Information Security

Studie über Kinder- und Jugendschutzprogramme

Evaluierung ausgewählter Kinder- und Jugendschutzlösungen auf Basis der Wirksamkeit technischer Maßnahmen

Diplomarbeit

zur Erlangung des akademischen Grades

Diplom-Ingenieur/in

eingereicht von

Lukas Schmalzbauer, BSc.

1610619525

im Rahmen des

Studienganges Information Security an der Fachhochschule St. Pölten

Betreuung

Betreuer/in: Ing. Dipl.-Ing. Richard Thron, BSc, CISSP

St. Pölten, 5. Juni 2018 _____ _____

(Unterschrift Verfasser/in) (Unterschrift Betreuer/in)

*

Ehrenwörtliche Erklärung

Ich versichere, dass

- ich diese Diplomarbeit selbständig verfasst, andere als die angegebenen Quellen und Hilfsmittel nicht benutzt und mich sonst keiner unerlaubten Hilfe bedient habe.
- ich dieses Diplomarbeitsthema bisher weder im Inland noch im Ausland einem Begutachter/einer Begutachterin zur Beurteilung oder in irgendeiner Form als Prüfungsarbeit vorgelegt habe.
- diese Arbeit mit der vom Begutachter/von der Begutachterin beurteilten Arbeit übereinstimmt.

Der Studierende/Absolvent räumt der FH St. Pölten das Recht ein, die Diplomarbeit für Lehre- und Forschungstätigkeiten zu verwenden und damit zu werben (z.B. bei der Projektevernissage, in Publikationen, auf der Homepage), wobei der Absolvent als Urheber zu nennen ist. Jegliche kommerzielle Verwertung/Nutzung bedarf einer weiteren Vereinbarung zwischen dem Studierenden/Absolventen und der FH St. Pölten.

Ort, Datum *Unterschrift*

Kurzfassung

Das Internet ist zu einem stetigen Begleiter im Leben Vieler geworden, denn weltweit besitzen im Jahre 2017 bereits über die Hälfte der Haushalte einen Internetzugang [1]. Weiterführend zeigt eine Studie von "Bitkom Research", dass bereits knapp die Hälfte der befragten Kinder im Alter von 6 bis 7 Jahren zumindest gelegentlich online sind [2]. Dieser Sachverhalt nimmt die Eltern mit in die Verantwortung, für die Filterung von Inhalten, die nicht für die jeweilige Altersgruppe geeignet sind, zu sorgen.
Diese Diplomarbeit zielt darauf ab, einen Vergleich zwischen unterschiedlichen Kinderschutzprogrammen für die Betriebssysteme Windows 7, Windows 10, Android 7.1.1 und iOS 11.1 herzustellen und dem Leser anhand eines ausgearbeiteten Kriterien- und Bewertungskataloges klar darzulegen, welches der jeweiligen Produkte für die Aufgabe der Filterung von Inhalten besonders geeignet ist. Einhergehend wurde der Begriff "Kinderschutz" definiert und die Kriterien zur Kategorisierung von Kinderschutzsoftware anhand eines Schemas abgeleitet sowie entsprechende technische Schutzmaßnahmen definiert als auch gewichtet. Entsprechend führte dies von einer breiten Vorauswahl zu jeweils fünf unterschiedlichen Softwareprodukten pro Betriebssystem, welche im Detail einem praktischen, auf gewichteten Kriterien basierenden Testverfahren einschließlich definierter Umgehungsszenarien unterzogen wurden. Abschließend wurden die Testszenarien der einzelnen Anwendungen ausgewertet und miteinander verglichen.

Abstract

The internet has become a constant companion in the life of many people, as in the year 2017 more than half of households worldwide have internet access [1]. Furthermore a study conducted through "Bitkom Research", shows that nearly half of the children aged 6 to 7 years old are online occasionally [2]. This circumstance makes parents responsible for taking precautions against inappropriate content for any specific age bracket.

The aim of this thesis is to create a comparison between various child-protection applications on different operating systems, being Windows 7, Windows 10, Android 7.1.1 and iOS 11.1. By providing a well-elaborated list of criteria and an evaluation catalogue, it is clear to the reader which products are working well for filtering inappropriate content. Furthermore the term "child protection" was defined and the various methods of protection mechanisms were derived from an elaborated schema. This resulted in a broad pre-selection for the aforementioned operating systems, which was conlusively narrowed down to five different softwareproducts per OS. Then these products were installed and tested practically including scenarios, concering the possibilty to bypass the protection mechanism of the software. Finally, this resulted into a statistical comparison of the products

Inhaltsverzeichnis

1 Einführung und statistische Betriebssystemanalyse

1.1 Definition

Unter dem Wort ”Kinderschutzprogramm” finden sich viele als Synonym verwendete Begrifflichkeiten, wie ”Jugendschutzfilter” [3], ”Kindersicherung” [4] und ”Elternkontrollsoftware” (im Englischen auch ”Parental Control Software” genannt) [5]. Dementsprechend schließt der rechtliche Begriff ”Jugendschutz” die Thematik des Kinderschutzes im Allgemeinen mit ein, wodurch eine weitergehende Begriffsdefinition durch Rechtstexte durchaus möglich ist.
Laut §11 der "Rechtsvorschrift für das Niederösterreichische Jugendgesetz" sind die Ziele des Jugendschutzes, dass

> “a) junge Menschen sich gesund entwickeln können und zwar in körperlicher, geistiger, seelischer, ethischer, religiöser, sozialer und demokratischer Hinsicht. (...)
>
> c) junge Menschen vor Gefahren geschützt werden, denen Sie auf Grund ihres Alters und Entwicklungsstandes nicht gewachsen sind (...)” [6]

1.2 Risiken

Die in dem Gesetzestext sogenannten "Gefahren" beziehungsweise Risiken können auch im Zusammenspiel mit der Verwendung des Internets auftreten. Zur Konkretisierung jener, wird eine Studie herangezogen, in welcher mehr als 25.000 Kinder im Alter von 9 bis 16 Jahren inklusive einem Elternteil zu ihren Internetaktivitäten befragt wurden. In jener fand eine Klassifizierung der Risiken denen Kinder im Internet ausgesetzt sind statt. Grundsätzlich umfasst die genannte Klassifizierung die folgenden drei Bereiche:

- Inhaltliche Risiken, denen Kinder ausgesetzt sind
- Kontaktbezogene Risiken, an denen Kinder selbst beteiligt sind

- Durchführungsbezogene Risiken, welche durch Kinder selbst erzeugt werden [7]

Die nachfolgende Matrix zeigt anhand von diversen Beispielen, welchen konkreten Risiken ein Kind nach der zuvor genannten Klassifizierung im Internet ausgesetzt sein kann.

	INHALT	**KONTAKT**	**DURCHFÜHRUNG**
AGGRESSIV	Gewalt	Belästigung, Stalking	Mobbing, feindseliges Verhalten
SEXUELL	Pornografie	”Grooming”, sexueller Missbrauch	Sexuelle Belästigung, ”Sexting”
IDEOLOGIE	Rassismus	Von einer Ideologie überzeugen	Potenziell gefährdender Benutzerinhalt
KOMMERZIELL	Eingebettetes Marketing	Missbrauch von persönlichen Daten	Glücksspiel, Urheberrechtsverletzung

Tabelle 1.1: Risiken-Matrix für Kinder im Internet (in Anlehnung an [7])

Für jeden Bereich in dieser Tabelle wurden entsprechende Fragen an die Probanden in der Studie gestellt und ausgewertet. Nachfolgende Statistik zeigt, wie viele der über 25.000 Kinder bzw. Jugendlichen bereits ungeeigneten Inhalten ausgesetzt waren.

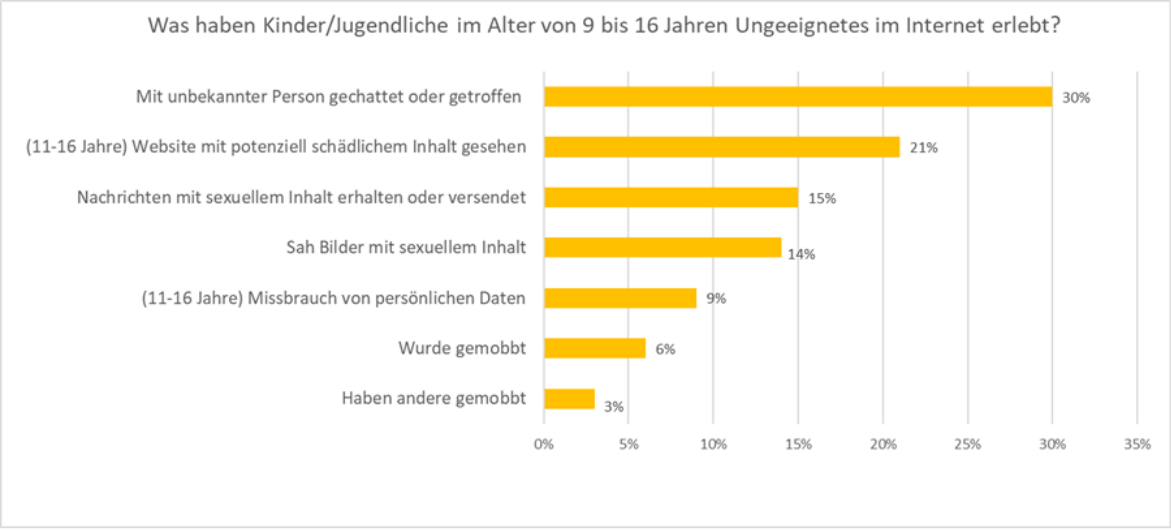

Abbildung 1.1: Prozentsätze der Kinder und Jugendlichen, welche bereits ungeeigneten Inhalten im Internet ausgesetzt waren (Daten aus [7])

Zum Schutz vor diesen Risiken können technische Maßnahmen in Form von Kinderschutzprogrammen getroffen werden. Um jedoch nun konkrete Programmvorschläge bieten zu können, ist es wichtig zu wissen, welche internetfähigen Geräte ein Kind besitzt und verwendet. Dafür wurde die nachfolgende Statistik genauer betrachtet.

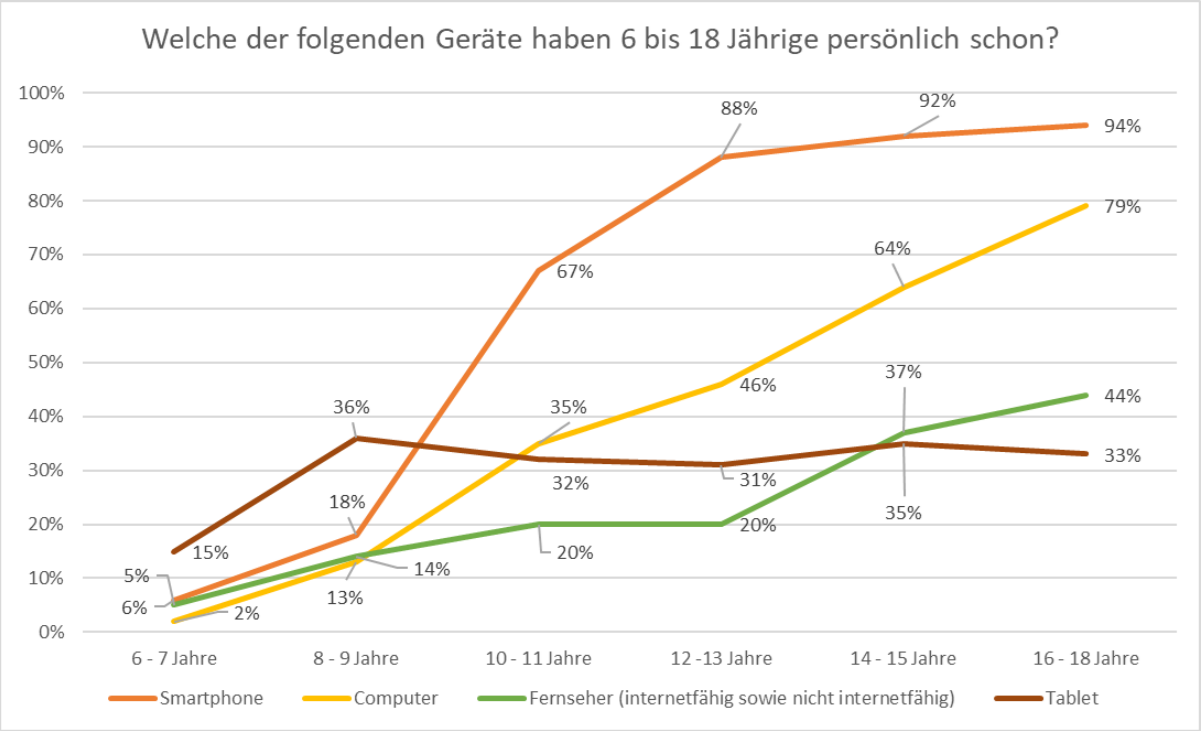

Abbildung 1.2: Technische Geräte der Kinder/Jugendlichen im Alter von 6-18 Jahren (in Anlehnung an [2])

Die zuvor genannte Statistik zeigt, dass

- Kinder im Alter von 6 bis 9 Jahren hauptsächlich ein Tablet besitzen
- über die Hälfte der Kinder im Alter von 10 bis 11 Jahren ein Smartphone hat und dieser Prozentsatz mit steigendem Alter weiter bis zu 94% ansteigt
- nur 13% der Kinder im Alter von 8 bis 9 Jahren einen Computer besitzen.

Daraus lässt sich grundsätzlich schließen, dass sich hierbei eher eine Tendenz zu mobilen als zu stationären Geräten bezüglich des Besitzes zeigt.

Für die genauere Analyse des Nutzungsverhaltens von Geräten für den Zugriff auf das Internet, wurde die nachfolgende Statistik herangezogen.

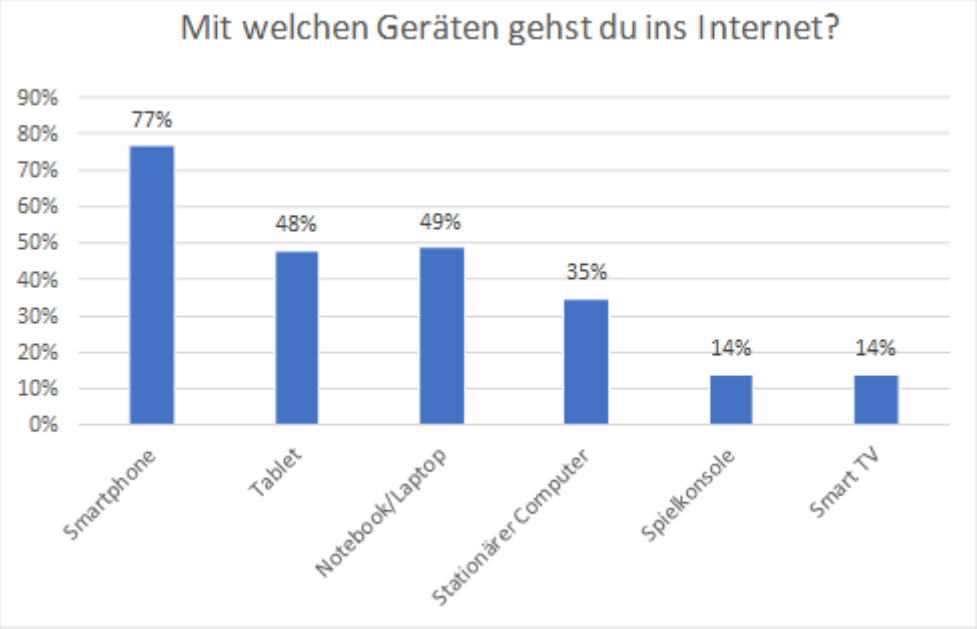

Abbildung 1.3: Statistik über die Internetnutzung von Kindern/Jugendliche durch welche Geräte (in Anlehnung an [2])

Aus den Ergebnissen kann man ablesen, dass hierbei zu einem größeren Anteil mobile Endgeräte verwendet werden, wie auch die Statistik bezüglich des Besitzes klar darlegt. Das bedeutet jedoch nicht, dass diese unbedingt eine höhere Relevanz aufweisen. Die Statistik zeigt ebenso, dass ein Kind mehrere Arten von Geräten simultan verwendet, weshalb Schutzmechanismen auf jeglichen Gerätetyp implementiert werden müssen, um einen effektiven Schutz gewährleisten zu können. Faktisch könnte ein Kind oder ein Jugendlicher sein Zweitgerät verwenden, um beispielsweise eine Website mit nicht altersgerechtem Inhalt aufzurufen.

1.3 Statistische Betriebssystemanalyse

Um nun passende Kinderschutzlösungen auswählen zu können, muss ermittelt werden, welche Betriebssysteme derzeit am häufigsten genutzt werden. In diesem Zusammenhang wurde der angebotene Service von “StatCounter Global Stats ”genutzt. Hierbei handelt es sich um einen Dienst, welcher anhand von über 10 Milliarden Seitenaufrufen auf 2 Millionen Websites, Statistiken zur aktuellen Verwendung von Betriebssystem und Browsern bietet [8]. Insgesamt sind folgende Produkte mit ihren dazugehörigen Marktanteilen im Dezember 2017 wie folgt vertreten:

- Microsoft Windows (36,07% Marktanteil) im stationären Bereich

  davon Windows 7 mit 41,89% [9] (entspricht 15,11% des absoluten Marktanteils von Microsoft Windows) und

  Windows 10 mit 41,69% (entspricht 15,04% des absoluten Marktanteils von Microsoft Windows)

- Google's Android (39,98% Marktanteil) im mobilen Bereich

  davon Android 7.1 Nougat mit 5,18% [10] (entspricht 2,07% des absoluten Marktanteils von Google's Android)

- Apple's iOS (13,22% Marktanteil) im mobilen Bereich

  davon iOS 11.1 mit 33,44% [11] (4,42% des absoluten Marktanteils von Apple's iOS) % [12]

Da mit diesen Herstellern ein Marktanteil von 90,98% (36,07% + 41,69% + 13,22%) erreicht wird und sich die einzelnen, genannten Produkte derzeit heruntergerechnet auf 36,64% (15,11% + 15,04% + 2,07% + 4,42%) des absoluten Marktanteils der einzelnen Hersteller dieser Betriebssystemgruppen belaufen, bezieht sich somit diese Arbeit auf Kinderschutzlösungen für eben jene genannten Produkte, da dadurch über ein Drittel an den derzeit verwendeten Betriebssystemen abgedeckt wird.

2 Definition der Kriterien zur Kategorisierung von Kinderschutzsoftware

Zur Definition von Kriterien zur Kategorisierung von Kinderschutzsoftware wurde der nachfolgende Prozess gewählt, welcher in den weiterführenden Unterkapiteln im Detail erläutert wird:

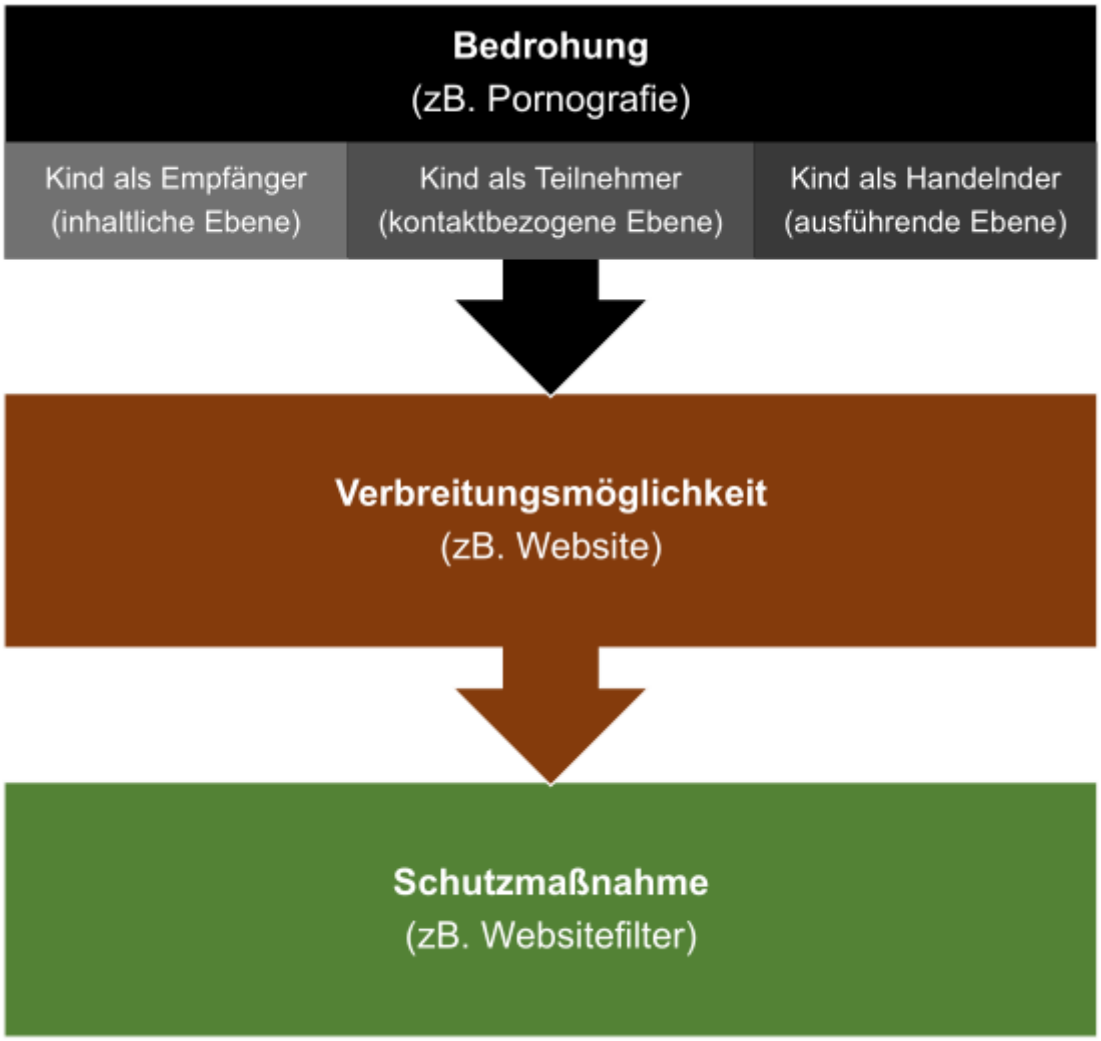

Abbildung 2.1: Prozess zur Definition von Kriterien für die Vorauswahl von Kinderschutzsoftware (in Anlehnung an [13])

2.1 Rollen des Kindes und Bedrohungen

In den Ausarbeitungen "E-Safety and Web2.0 for children aged 11-16" [14], "Risks and safety on the internet: The perspective of European children" [7] finden sich nachfolgende Bedrohungen, denen Kinder und Jugendliche im Web ausgesetzt sind. Zudem wurden in der Studie "Safer Children in a digital world" [13], neben der Nennung von weiteren Bedrohungen, Kinder und Jugendliche anhand der entsprechenden Bedrohungsszenarien grundsätzlich in die nachfolgenden drei Kategorien eingeteilt:

- Kind als Empfänger: Das Kind beziehungsweise der Jugendliche ist der passive Teilnehmer und die Bedrohung stellt die aktive Komponente dar. Dabei ist die Darstellung eines Inhaltes unpassend für die betroffene Person (z.B. Darstellung von Werbung auf einer Website).

- Kind als Teilnehmer: Das Kind beziehungsweise der Jugendliche wird durch eine Interaktion mit einer anderen Person oder einer Website im Internet in irgendeiner Art und Weise durch ein anderes Individuum geschädigt (z.B. Mobbing).

- Kind als Handelnder: Das Kind beziehungsweise der Jugendliche wird durch die Ausführung einer Tätigkeit selbst zum schädigenden Individuum (z.B. Upload von urheberrechtlich geschütztem Material).

Nachfolgend finden sich die Bedrohungen welche identifiziert werden konnten und bei Bedarf die entsprechenden, dazugehörigen Erläuterungen:

- Angebot von Drogen

- Anleitung zum Suizid: Das Web stellt Anleitungen bereit, wie man sich das Leben mittels verschiedener Methoden nehmen kann, [15] was Kinder bzw. Jugendliche dazu bekräftigen bzw. beraten kann, Selbstmord zu begehen.

- Anstößiger Inhalt: Da das Internet normalerweise nicht unter einer Zensur steht, können Inhalte verfügbar gemacht werden, die für Kinder bzw. Jugendliche im Allgemeinen anstößig sein können. Als konkretes Beispiel könnte hierbei der erfolgreiche YouTube-Star Felix Kjellberg, alias "Pewdiepie" genannt werden, welcher in mehreren seiner YouTube-Videos Witze über Juden und Nationalsozialisten gemacht hatte [16].

- Auslesen von persönlichen Daten durch Dritte: Wenn Kinder oder Jugendliche persönliche Daten, wie deren Namen, Geburtsdatum und/oder Adresse in einem sozialen Netzwerk oder auf einer Website angeben, können diese Daten in weiterer Folge durch Dritte missbraucht werden.

- Bereitstellung von irreführenden Informationen und Ratschlägen: Kinder bzw. Jugendliche können wissentlich gefälschte Informationen oder Ratschläge an Dritte weitergeben und dadurch einen Schaden für andere Personen oder sich selbst erzeugen.
- Darstellung von Gewalt / Selbstverletzung: Inhalte im Web, wie beispielsweise Forenbeiträge, Videos oder Blogs sowie Anwendungen oder Computerspiele können Gewalt oder Selbstverletzung beinhalten, was für Kinder bzw. Jugendliche verstörend wirken kann.
- Erhalt von Nachrichten mit sexuellem Inhalt
- Erstellung und Upload von unpassendem Material: Wenn Kinder oder Jugendliche im Web unpassende Nachrichten, Bilder oder Videos hochladen, ist ihnen Folgendes meist nicht bewusst: "Was einmal online gestellt wurde, bleibt auch online". Dies kann direkt im näheren, sozialen Umfeld oder im späteren Berufsleben zu weitreichenden Problemen führen. [17]
- Finanzieller Betrug: Durch die Weitergabe oder Verwendung von sensiblen Zahlungsinformationen wie beispielsweise einer Bankverbindung oder einer Kreditkartennummer, unabhängig davon ob es die des Kindes bzw. des Jugendlichen oder jene der Eltern ist, kann ein finanzieller Schaden entstehen.
- Förderung oder Verharmlosung von Adipositas / Anorexie: Die Studie "e-Ana and e-Mia: A Content Analysis of Pro-Eating Disorder Web Sites" [18] besagt, dass im Internet Websites bzw. Foren [19] [20] existieren, welche darauf abzielen Essstörungen zu unterstützen und weitergehend zu fördern. Entsprechend kann dies gesundheitlich weitreichende Folgen für ein Kind bzw. einen Jugendlichen haben.
- Glücksspiel
- Illegale Downloads: Da das Downloaden von urheberrechtlich geschütztem Material unter Strafe steht, wenn eine "... offensichtlich rechtswidrig hergestellte oder öffentlich zugänglich gemachte Vorlage verwendet wird." [21], können hierbei auf Kinder und Jugendliche bzw. deren Eltern hohe Folgekosten zukommen. Als Beispiel kann hier ein aktueller Fall zu dem Film "Suburbicon" genannt werden, in welchem die Kanzlei Waldorf Frommer in Deutschland abmahnt und 915€ in Rechnung stellt. [22]
- Kontaktaufnahme und Misshandlung von Kindern durch Fremde (z.B. Grooming): Bei Grooming handelt es sich um die Kontaktaufnahme zu Kindern, um diese sexuell zu missbrauchen, was bedingt durch die hohe Anzahl an Jugendlichen und Kindern in sozialen Netzwerken [23], als Risiko nicht zu missachten ist.

- Mobbing: Unter Mobbing versteht man, wenn eine einzelne Person systematisch, beinahe täglich, über einen längeren Zeitraum physisch und/oder psychisch schikaniert und dessen Ruf zerstört wird. [24] Da sich Mobbing hauptsächlich auf den Arbeitsplatz bezogen hat, wurde durch die Kommunikation über das Internet sowie den sozialen Netzwerken, ein neuer Begriff geprägt, nämlich "Cyber-Bullying". Dabei handelt es sich um eine Form des Mobbings, welche über Informations- und Kommunikationstechnologien, wie soziale Netzwerke, Chats, Smartphones etc. durchgeführt wird. [25] Dies stellt für ein Kind bzw. einen Jugendlichen einen äußerst hohen Bedrohungsgrad dar, da durch "Cyber-Bullying" bereits Selbstmorde [26] begangen wurden.
- Pornografie
- Rassismus: Es finden sich Websites [27] oder Inhalte, die rassistisches Verhalten propagieren und unterstützen. Dies kann sich auf das Verhalten eines Kindes oder Jugendlichen auswirken und Rassismus bei dem Betrachtenden fördern.
- Spam: Wenn Spam-Nachrichten durch Kinder oder Jugendliche angeklickt werden, kann neben Betrug und der Weitergabe von persönlichen, sensiblen Daten auch Malware [28] auf den betroffenen Computer gelangen.
- Stalking: Der Begriff "Cyber-Stalking" wird als eine Erweiterung des traditionellen Stalkings angesehen, in welcher der Verfolger hochtechnologische Mittel einsetzt, um ein Verbrechen zu verüben. [29] Das Internet, insbesondere soziale Netzwerke, erleichtern das Sammeln von persönlichen Informationen und dementsprechend ist es wichtig, dass Kinder und Jugendliche vor solch einer Gefahr bewahrt werden. Wie wichtig, wird dadurch erläutert, dass Opfer von Cyberstalking eindeutig schlechter im "WHO-5 well-being Index" abschneiden, als Menschen die nie unter dem Einfluss von Stalking litten. [30]
- Terrorismus: Entsprechend dem Artikel von Heise "Terroristen online: Der Islamist von nebenan" [31], wird das Potential von sozialen Netzwerken und dem Web zur Rekrutierung von neuen Anhängern beispielsweise für den "Islamischen Staat" (IS) beschrieben. Entsprechend können Kinder, aber viel mehr Jugendliche durch solche Online-Inhalte dazu bewogen werden, einer terroristischen Vereinigung beizutreten.
- Vernachlässigung des sozialen Umfelds / schulischen Pflichten: Durch die exzessive Verwendung eines Computers oder Smartphones, kann dies in weiterer Folge zu einer Vernachlässigung des sozialen Umfeldes beziehungsweise der schulischen Pflichten führen.
- Werbung für nicht altersgerechte Inhalte

- Weitergabe von persönlichen Daten / Passwörtern

Dementsprechend wurden die Bedrohungen den einzelnen Kategorien zugeordnet und die nachfolgende Tabelle erstellt.

Rolle des Kindes	Bedrohungen
Kind als Empfänger (inhaltliche Ebene)	• Angebot von Drogen • Anleitung zum Suizid • Anstößiger Inhalt • Darstellung von Gewalt • Darstellung von Selbstverletzung • Förderung oder Verharmlosung von Adipositas • Förderung oder Verharmlosung von Anorexie • Pornografie • Rassismus • Spam • Werbung für nicht altersgerechte Inhalte
Kind als Teilnehmer (kontaktbezogene Ebene)	• Auslesen von persönlichen Daten durch Dritte • Erhalt von Nachrichten mit sexuellem Inhalt • Kontaktaufnahme und Misshandlung von Kindern durch Fremde (zB. Grooming) • Mobbing • Stalking
Kind als Handelnder (ausführende Ebene)	• Bereitstellung von irreführenden Informationen und Ratschlägen • Erstellung und Upload von unpassendem Material • Finanzieller Betrug • Glücksspiel • Illegale Downloads • Mobbing • Terrorismus • Vernachlässigung des sozialen Umfeldes • Vernachlässigung von schulischen Pflichten • Weitergabe von Passwörtern • Weitergabe von persönlichen Daten

Tabelle 2.1: Ableitung der Bedrohungen von den Rollen des Kindes

2.2 Bedrohungen und Verbreitungsmöglichkeiten

Von den zuvor definierten Bedrohungen wurden entsprechende Verbreitungsmethoden und die dazugehörigen Schutzmaßnahmen, welche durch Kinderschutzsoftware gegeben sein sollten, abgeleitet. Die Auflistung der Ableitungen von Bedrohungen zu Verbreitungsmöglichkeiten, finden Sie auf den nachfolgenden Seiten.

Verbreitungsart ► Bedrohungen ▼	Website	Chat	Anwendung	Foren	SMS MMS	Soziale Netzwerke	Anruf	Mail	Daten-träger	Download	File-Sharing	Pop-Up	Sucht
Angebot von Drogen	X	X		X	X	X	X	X				X	X
Anleitung zum Suizid	X	X		X		X							
Anstößiger Inhalt	X	X	X	X	X	X		X	X	X	X	X	
Auslesen von persönlichen Daten durch Dritte	X	X	X	X	X	X	X	X				X	
Bereitstellung irreführender Informationen und Ratschlägen	X	X		X	X	X	X	X	X				
Darstellung von Gewalt	X	X	X	X	X	X		X	X	X	X	X	
Darstellung von Selbstverletzung	X	X	X	X	X	X		X				X	
Erhalt von Nachrichten mit sexuellem Inhalt	X	X	X	X	X	X	X	X				X	
Erstellung und Upload von unpassendem Material	X	X	X	X		X		X			X		
Finanzieller Betrug	X	X	X	X	X	X	X	X		X		X	

Verbreitungsart ► Bedrohungen ▼	Website	Chat	Anwendung	Foren	SMS MMS	Soziale Netzwerke	Anruf	Mail	Daten-träger	Download	File-Sharing	Pop-Up	Sucht
Förderung oder Verharmlosung von Adipositas	X	X		X	X	X		X				X	
Förderung oder Verharmlosung von Anorexie	X	X		X	X	X		X				X	
Glücksspiel	X		X		X	X	X	X				X	X
Illegale Downloads	X	X	X	X		X		X		X	X	X	
Kontaktaufnahme und Misshandlung von Kindern durch Fremde (z.B. Grooming)	X	X	X	X	X	X	X	X					
Mobbing	X	X	X	X	X	X	X	X					
Pornografie	X	X	X	X	X	X		X	X	X	X	X	X
Rassismus	X	X	X	X	X	X	X	X	X	X	X	X	
Spam	X	X		X	X	X		X				X	
Stalking	X	X	X	X	X	X	X	X					
Terrorismus	X	X	X	X	X	X	X	X		X		X	
Vernachlässigung des sozialen Umfelds	X	X	X	X	X	X	X	X					X

Verbreitungsart ► Bedrohungen ▼	Website	Chat	Anwendung	Foren	SMS MMS	Soziale Netzwerke	Anruf	Mail	Daten-träger	Download	File-Sharing	Pop-Up	Sucht
Vernachlässigung von schulischen Pflichten	X	X	X	X	X	X	X	X					X
Weitergabe von Passwörtern	X	X	X	X	X	X	X	X				X	
Weitergabe von persönlichen Daten	X	X	X	X	X	X	X	X				X	
Werbung für nicht altersgerechte Inhalte	X	X	X	X	X	X		X				X	

Tabelle 2.2: Ableitung der Verbreitungsmöglichkeiten von Bedrohungen

2.3 Ableitung der Schutzmaßnahmen von Verbreitungsmöglichkeiten und Bedrohungen

Entsprechend der vorhergehenden Matrix zu Bedrohungen und Verbreitungsmöglichkeiten wurden weitergehend passende Schutzmaßnahmen abgeleitet. Die nachstehenden Maßnahmen sollte eine Kinderschutzsoftware besitzen, um einen effizienten und gesamtheitlichen Ansatz hinsichtlich des Schutzes eines Kindes im Internet zu gewährleisten:

- Anwendungsblocker: Die Software bietet eine Funktion, die es erlaubt die Ausführung einer oder mehrerer Anwendungen zu blockieren. Diese Funktionalität wird beispielsweise durch Bitdefender geboten. Dort fügt man Applikationen zu einer Blacklist hinzu, um die Ausführung zu verhindern (z.B. wird eine Chatanwendung wie ICQ [32] blockiert). [33]

- Blockieren der Ausführung von bestimmten Dateitypen: Die Software besitzt eine Funktion, welche es ermöglicht, dass Dateien eines bestimmten Typs (wie beispielsweise .exe) [34] blockiert werden können.

- Loggingfunktion: Die Software hat eine Funktion implementiert, welche die Verwendung des Rechners aufzeichnet und es den Eltern damit ermöglicht, den Verlauf einer Computernutzung durch eine Person nachzuvollziehen (z.B. Aufzeichnung eines Regelverstoßes oder der aufgerufenen Websites bzw. Programme). Als Beispiel kann hier die Kindersicherung von macOS Sierra genannt werden, welche Protokolle zu Aktivitäten, Anwendungen sowie besuchte Websites in einem bestimmten Zeitraum anzeigt. [35]

- Websitefilter: Die Software hat eine Funktion, die es erlaubt ausgewählte Websites zu blockieren. Zum Beispiel können die Eltern ein spezifisches soziales Netzwerk zur Liste hinzufügen, um die Verwendung durch das Kind zu unterbinden.

- Downloadblocker: Die Software verhindert nach Aktivierung der Funktion, automatisch den Download von Dateien. Als Beispiel kann hier die Anwendung "BrowseControl" von "CurrentWare" [36] genannt werden, welche es ermöglicht, einen Filter für bestimmte Dateitypen zu erstellen und den Download entsprechend zu unterbinden.

- Spamfilter für Maildienste: Die Software hat einen integrierten Spamfilter für Maildienste.

- Blockieren von USB-Schnittstellen und integrierten Laufwerken: Die Software erlaubt es interne Laufwerke und anschließbare Wechselmedien (z.B. USB-Sticks) zu blockieren.

- Spieleblocker: Die Software bietet einen dezidierten Spieleblocker an. Dabei unterscheidet sich diese Form des Blockers vom Anwendungsblocker insofern, dass jener entsprechende Anwendungen automatisch als Computerspiele erkennt und weitergehend blockiert. Beispielhaft bietet Windows 7 über die integrierte Kindersicherung einen Spieleblocker, welcher Computerspiele im Allgemeinen oder entsprechend einer definierten Alterseinstufung blockiert [37], um zu vermeiden, dass nicht altersgerechte Computerspiele durch das Kind bzw. den Jugendlichen konsumiert werden.

- Ad-Blocker: Die Software bietet einen integrierten Ad-Blocker an, welcher unerwünschte Werbung und Pop-Ups im Internet blockiert. Anzumerken ist, dass 34% der Internet-Anwender ungewollt pornografische Inhalte über Werbung, Pop-Ups, falsche Links oder E-Mails zu Gesicht bekamen. [38]

- Verwendung einer sicheren und kindgerechten Suchmaschine: Die Software bietet eine Funktion an, die es ermöglicht eine sichere Suchmaschine [39] auszuwählen und festzulegen (hierunter fällt auch die Option von Safe-Search [40] für Suchmaschinen)

- Zeitkonto: Die Software bietet eine Funktion an ein Zeitkonto zu aktivieren. Dadurch können Eltern einen "Zeitbetrag" (z.B. eine Stunde pro Tag) oder einen Zeitrahmen (z.B. jeweils eine Stunde Computerzeit von Freitag bis Sonntag) definieren. Sobald jenes Zeitguthaben aufgebraucht wurde, schaltet sich die Internetverbindung, die Anwendung oder der gesamte Computer ab. Beispielhaft lässt sich unter Windows 10 ein Zeitrahmen setzen, in welchen ein spezifischer Account verwendet werden darf [41]

- Portblocker: Die Software erlaubt es spezifische Netzwerkports zu definieren, welche geblockt werden sollen [42] (z.B. eine bestimmter Netzwerkport für ein Online-Computerspiel)

Für ein mobiles Gerät sind noch zusätzlich zu den zuvor genannten Schutzmaßnahmen, weitergehend relevant:

- SMS/MMS von Dritten blockieren: Dies erlaubt es einem Anwender SMS/MMS von Dritten zu blockieren. Dies kann zum Einen durch ein Whitelisting-Verfahren geschehen, in welchem alle explizit erlaubten Kontakte, wie beispielsweise die Familie oder Freunde, einer Liste hinzugefügt werden. Darauffolgend werden alle anderen Mobiltelefonnummern gesperrt. Der andere Ansatz, welcher gewählt werden kann, wäre eine Blacklist, zu welcher Telefonnummern hinzugefügt werden können, die explizit ausgeschlossen werden. Hierfür muss jedoch die Telefonnummer bekannt

sein. Beide Modi sind mit dem bekannten White- bzw. Blacklisting von Firewalls [43] vergleichbar.

- Anrufe von Dritten blockieren: Die Erläuterung entspricht "SMS/MMS von Dritten blockieren", jedoch werden hierbei Anrufe und nicht SMS/MMS gefiltert.

Die nachstehende Matrix zeigt im Detail, für welche Art der Verbreitungsmöglichkeit, welche entsprechende Schutzmaßnahme angewandt werden kann:

Verbreitungsart ► Schutzmaßnahme ▼	Website	Chat	Anwendung	Foren	SMS MMS	Soziale Netzwerke	Anruf	Mail	Daten-träger	Download	File-Sharing	Pop-Up	Sucht
Ad-Blocker												X	
Anrufe blockieren							X						X
Anwendungsblocker		X	X								X		X
Blockieren von Laufwerken									X				
Blockieren von USB-Schnittstellen									X				
Downloadblocker										X			
Kindgerechte Suchmaschine integriert	X			X		X					X		
Loggingfunktion	X	X	X	X	X	X	X	X	X	X	X		
Portblocker			X								X		
SMS/MMS blockieren					X								X
Spamfilter								X					
Spieleblocker			X										
Websitefilter	X	X		X		X		X				X	X
Zeitkonto													X

Tabelle 2.3: Ableitung Schutzmaßnahmen anhand Verbreitungsmöglichkeiten

3 Vorauswahl der Kinderschutzsoftware

3.1 Aktuelle Kinderschutzlösungen am Markt

Im Internet findet sich eine hohe Anzahl an verschiedensten Kinderschutzlösungen mit unterschiedlichsten Ausprägungen in Hinblick auf deren Funktionalitäten. Um einen Vergleich herstellen und eine Vorauswahl treffen zu können, wurden die einzelnen, auf der Herstellerwebsite bzw. die des Hosters [44–76] gegebenen Beschreibungen zu den angebotenen Kinderschutzlösungen mit den abgeleiteten Schutzmaßnahmen verglichen. Zudem wurden hierbei noch allgemeine Informationen wie das Vorhandensein einer Testversion und die Kosten für das Programm dargestellt. Faktisch soll diese Diplomarbeit einen guten Überblick über das derzeitige Angebot an Software bieten. Die Sammlung an den aktuellen Produkten finden sich in den nachfolgenden Unterkapiteln.

3.1.1 Kinderschutzlösungen für Windows 7 und Windows 10

Dieser Abschnitt enthält Produkte, welche zumindest für die Betriebssysteme Windows 7 und Windows 10 verwendet werden können. Ebenso bieten einige Hersteller eine Version für mobile Endgeräte an, worüber die Zeile "Betriebssysteme" in der Tabelle Auskunft gibt.

Hersteller	AG KinderServer	Ars Nova Systems	Bitdefender	Blue Coat
Produkt	KinderServer	Parentsaround	Internet Security 2018	K9 Web Protection
Betriebssysteme (A, i => Android, iOS)	Win7	Win7, Win10, A, i	Win7, Win10, A, i	Win7, Win10, A, i
Funktionalitäten				
Ad-Blocker				
Anwendungsblocker		JA	JA	
Ausführung v. Dateitypen blockieren			JA	
USB-Schnittstellen blockieren				
Laufwerke blockieren				
Downloadblocker				
Loggingfunktion		JA	JA	JA
Portblocker				
Spamfilter f. Maildienste			JA	
Dezidierter Spieleblocker			JA	
Kindgerechte Suchmaschine integriert	JA		JA	JA
Websitefilter	JA	JA	JA	JA
Zeitkonto		JA	JA	JA
Funktionalitäten (mobile Geräte)				
SMS/MMS von Dritten blockieren			JA	
Anrufe von Dritten blockieren			JA	
Installationsart				
lokale Anwendung ohne Remotesteuerung	JA			JA
lokale Anwendung mit Remotesteuerung		JA	JA	
Cloud-basierte Anwendung				
Routereinstellung				
Allgemeine Informationen				
Voll funktionsfähige Testversion und Dauer		30 Tage	30 Tage	
Eingeschränkte Testversion und Dauer				
Kosten (G = Geräte)	Kostenlos	39,00€ / Jahr / 10G	64,99€ / Jahr / 3G	Kostenlos

Hersteller	Bullguard	Buhl Data Service GmbH	Content Watch Holding	Cybits AG
Produkt	Internet Security 2018	WISO Internet Security	Net Nanny	Surf Sitter
Betriebssysteme (A, i => Android, iOS)	Win7, Win10, A	Win7, Win10, A,	Win7, Win10, A, i	Win7, Win10
Funktionalitäten				
Ad-Blocker	JA			JA
Anwendungsblocker	JA	JA		JA
Ausführung v. Dateitypen blockieren	JA			
USB-Schnittstellen blockieren				
Laufwerke blockieren				
Downloadblocker				
Loggingfunktion	JA		JA	
Portblocker				
Spamfilter f. Maildienste		JA		
Dezidierter Spieleblocker	JA			
Kindgerechte Suchmaschine integriert		JA		
Websitefilter	JA	JA	JA	JA
Zeitkonto	JA	JA	JA	JA
Funktionalitäten (mobile Geräte)				
SMS/MMS von Dritten blockieren		JA		
Anrufe von Dritten blockieren		JA		
Installationsart				
lokale Anwendung ohne Remotesteuerung		JA		JA
lokale Anwendung mit Remotesteuerung	JA		JA	
Cloud-basierte Anwendung				
Routereinstellung				JA
Allgemeine Informationen			Keine Testversion	
Voll funktionsfähige Testversion und Dauer	60 Tage	30 Tage		30 Tage
Eingeschränkte Testversion und Dauer				
Kosten (G = Geräte)	59,95€ / Jahr / 3G	39,95€ / Jahr / 3G	10,00$ / Jahr / 1G	39,95€ / Jahr / 1G

Hersteller	die4reuthers	Entensys	eset	F-Secure
Produkt	Aus die Maus	Kindergate Parental Control	Internet Security	SAFE
Betriebssysteme (A, i => Android, iOS)	Win7, Win10	Win7, Win10	Win7, Win10	Win7, Win10, A, i
Funktionalitäten				
Ad-Blocker				
Anwendungsblocker				JA
Ausführung v. Dateitypen blockieren				
USB-Schnittstellen blockieren				
Laufwerke blockieren				
Downloadblocker		JA		
Loggingfunktion		JA	JA	JA
Portblocker				
Spamfilter f. Maildienste				
Dezidierter Spieleblocker		JA		JA
Kindgerechte Suchmaschine integriert		JA		
Websitefilter		JA	JA	JA
Zeitkonto	JA			JA
Funktionalitäten (mobile Geräte)				
SMS/MMS von Dritten blockieren				JA
Anrufe von Dritten blockieren				JA
Installationsart				
lokale Anwendung ohne Remotesteuerung	JA		JA	
lokale Anwendung mit Remotesteuerung		JA		JA
Cloud-basierte Anwendung				
Routereinstellung				
Allgemeine Informationen				
Voll funktionsfähige Testversion und Dauer		30 Tage	30 Tage	30 Tage
Eingeschränkte Testversion und Dauer				
Kosten (G = Geräte)	Kostenlos	19,00€ / Jahr / 1G	34,95€ / Jahr / 1G	59,90€ / Jahr / 3G

Hersteller	G Data	Infoweise	JusProg e.V.	Kaspersky
Produkt	Multi Device Security	SecureTeen Parental Control	JusProg	Safe Kids
Betriebssysteme (A, i => Android, iOS)	Win7, Win10, A, i	Win7, Win10, A, i	Win7, Win10, iOS	Win7, Win10, A, i
Funktionalitäten				
Ad-Blocker				
Anwendungsblocker	JA	JA		JA
Ausführung v. Dateitypen blockieren				JA
USB-Schnittstellen blockieren	JA			
Laufwerke blockieren	JA			
Downloadblocker		JA	JA	JA
Loggingfunktion	JA	JA		JA
Portblocker			JA	
Spamfilter f. Maildienste	JA			JA
Dezidierter Spieleblocker				JA
Kindgerechte Suchmaschine integriert		JA	JA	JA
Websitefilter	JA	JA	JA	JA
Zeitkonto	JA	JA	JA (Premium)	JA
Funktionalitäten (mobile Geräte)				
SMS/MMS von Dritten blockieren	JA	JA		
Anrufe von Dritten blockieren	JA	JA		
Installationsart				
lokale Anwendung ohne Remotesteuerung	JA		JA	
lokale Anwendung mit Remotesteuerung		JA		JA
Cloud-basierte Anwendung				
Routereinstellung				
Allgemeine Informationen				
Voll funktionsfähige Testversion und Dauer	30 Tage	30 Tage		
Eingeschränkte Testversion und Dauer			Kostenlos	Unbegrenzt
Kosten (G = Geräte)	49,95€ / Jahr / 2G	39,99$ / Jahr / 3G	19,90€ / Jahr / 1G	14,99€ / Jahr / 1G

Hersteller	McAffee	Michael Müller	Microsoft	Microsoft
Produkt	Safe Family	Parents-Friend	Family Safety	Live Family Safety
Betriebssysteme (A, i => Android, iOS)	Win7, Win10, A, i	Win7	Win10	Win7
Funktionalitäten				
Ad-Blocker				
Anwendungsblocker	JA	JA	JA	JA
Ausführung v. Dateitypen blockieren				
USB-Schnittstellen blockieren				
Laufwerke blockieren				
Downloadblocker				JA
Loggingfunktion	JA	JA	JA	
Portblocker				JA
Spamfilter f. Maildienste				
Dezidierter Spieleblocker			JA	JA
Kindgerechte Suchmaschine integriert				
Websitefilter	JA	JA	JA	JA
Zeitkonto	JA	JA	JA	JA
Funktionalitäten (mobile Geräte)				
SMS/MMS von Dritten blockieren	JA			
Anrufe von Dritten blockieren	JA			
Installationsart				
lokale Anwendung ohne Remotesteuerung				JA
lokale Anwendung mit Remotesteuerung	JA	JA	JA	
Cloud-basierte Anwendung				
Routereinstellung				
Allgemeine Informationen				
Voll funktionsfähige Testversion und Dauer	30 Tage			
Eingeschränkte Testversion und Dauer		Kostenlos		ohne Dauer
Kosten (G = Geräte)	107,40€ / Jahr / 3G	5,00€ einmalig	Kostenlos	19,90€ / Jahr / 1G

Hersteller	Mobicip	Norton	OpenDNS	ProtectCom
Produkt	Mobicip	Family Premier	Family Shield	Orvell Monitoring
Betriebssysteme (A, i => Android, iOS)	Win7, Win10, A, i	Win7, Win10, A, i	Win7, Win10, A, i	Win7, Win10
Funktionalitäten				
Ad-Blocker				
Anwendungsblocker	JA	JA		
Ausführung v. Dateitypen blockieren				
USB-Schnittstellen blockieren				JA
Laufwerke blockieren				JA
Downloadblocker				
Loggingfunktion	JA	JA	JA	JA
Portblocker				
Spamfilter f. Maildienste				
Dezidierter Spieleblocker		JA		
Kindgerechte Suchmaschine integriert				JA
Websitefilter	JA	JA	JA	JA
Zeitkonto	JA	JA		
Funktionalitäten (mobile Geräte)				
SMS/MMS von Dritten blockieren	JA	JA		
Anrufe von Dritten blockieren	JA	JA		
Installationsart				
lokale Anwendung ohne Remotesteuerung				
lokale Anwendung mit Remotesteuerung	JA	JA		JA
Cloud-basierte Anwendung				
Routereinstellung			JA	
Allgemeine Informationen				Keine Testversion
Voll funktionsfähige Testversion und Dauer	7 Tage	30 Tage		
Eingeschränkte Testversion und Dauer	ohne Dauer		ohne Dauer	
Kosten (G = Geräte)	39,99$ / Jahr / 5G	39,99€ / Jahr /∞G	19,95$ / Jahr / 1G	59,95€ / einmalig / 1G

Hersteller	Quick Heal	Qustodio	SafeDNS	Salfeld
Produkt	Total Security	Qustodio	SafeDNS	Kindersicherung
Betriebssysteme (A, i => Android, iOS)	Win7, Win10, A	Win7, Win10, A, i	Win7, Win10, A, i	Win7, Win10, A
Funktionalitäten				
Ad-Blocker			JA	
Anwendungsblocker	JA	JA		JA
Ausführung v. Dateitypen blockieren				
USB-Schnittstellen blockieren				
Laufwerke blockieren				
Downloadblocker				
Loggingfunktion		JA		JA
Portblocker				
Spamfilter f. Maildienste				
Dezidierter Spieleblocker	JA	JA		JA
Kindgerechte Suchmaschine integriert		JA	JA	
Websitefilter	JA	JA	JA	JA
Zeitkonto	JA	JA	JA	JA
Funktionalitäten (mobile Geräte)				
SMS/MMS von Dritten blockieren		JA		
Anrufe von Dritten blockieren		JA		
Installationsart				
lokale Anwendung ohne Remotesteuerung	JA			JA
lokale Anwendung mit Remotesteuerung		JA		
Cloud-basierte Anwendung			JA	
Routereinstellung			JA	
Allgemeine Informationen				
Voll funktionsfähige Testversion und Dauer	30 Tage		15 Tage	15 Tage
Eingeschränkte Testversion und Dauer		ohne Dauer		
Kosten (G = Geräte) *	74,00$ / Jahr / 1G	42,95€ / Jahr / 5G	19,95$ / Jahr / 3G	14,98€ / Jahr / 1G

Hersteller	SentryPC	Telekom	Trend Micro	TuEagles
Produkt	SentryPC	Kinderschutz Software	Internet Security 2017	Anti-Porn
Betriebssysteme (A, i => Android, iOS)	Win7, Win10	Win7, Win10	Win7, Win10	Win7
Funktionalitäten				
Ad-Blocker				
Anwendungsblocker	JA		JA	JA
Ausführung v. Dateitypen blockieren				
USB-Schnittstellen blockieren	JA			
Laufwerke blockieren	JA			
Downloadblocker				
Loggingfunktion	JA		JA	JA
Portblocker				
Spamfilter f. Maildienste			JA	
Dezidierter Spieleblocker				JA
Kindgerechte Suchmaschine integriert				
Websitefilter	JA	JA	JA	JA
Zeitkonto	JA	JA	JA	JA
Funktionalitäten (mobile Geräte)				
SMS/MMS von Dritten blockieren				
Anrufe von Dritten blockieren				
Installationsart				
lokale Anwendung ohne Remotesteuerung			JA	JA
lokale Anwendung mit Remotesteuerung	JA			
Cloud-basierte Anwendung	JA			
Routereinstellung				
Allgemeine Informationen				
Voll funktionsfähige Testversion und Dauer			30 Tage	30 Tage
Eingeschränkte Testversion und Dauer	nur Online Demo			
Kosten (G = Geräte) *	59,95$ / Jahr / 1G	Kostenlos	32,46€ / Jahr / 1G	29,97$ / einmalig / 1G

Hersteller	Witigo
Produkt	Parental Filter
Betriebssysteme (A, i => Android, iOS)	Win7, Win10, A
Funktionalitäten	
Ad-Blocker	
Anwendungsblocker	JA
Ausführung v. Dateitypen blockieren	
USB-Schnittstellen blockieren	
Laufwerke blockieren	
Downloadblocker	
Loggingfunktion	JA
Portblocker	
Spamfilter f. Maildienste	
Dezidierter Spieleblocker	
Kindgerechte Suchmaschine integriert	
Websitefilter	JA
Zeitkonto	JA
Funktionalitäten (mobile Geräte)	
SMS/MMS von Dritten blockieren	JA
Anrufe von Dritten blockieren	JA
Installationsart	
lokale Anwendung ohne Remotesteuerung	
lokale Anwendung mit Remotesteuerung	JA
Cloud-basierte Anwendung	
Routereinstellung	
Allgemeine Informationen	
Voll funktionsfähige Testversion und Dauer	30 Tage
Eingeschränkte Testversion und Dauer	
Kosten (G = Geräte) *	49,99$ / Jahr / 3G

Tabelle 3.1: Vorauswahl von verfügbaren Kinderschutzlösungen für Windows 7 und Windows 10

3.1.2 Dedizierte Kinderschutzlösungen für Android und iOS

In der nachfolgenden Tabelle findet sich die Vorauswahl zu den Kinderschutzlösungen für Android und iOS. Bezogen wurden die Informationen über die entsprechenden Herstellerwebsites, den "Google Play Store" und den "App Store" [77–99] Nicht aufgenommen wurden hierbei die zuvor aufgelisteten Hersteller, welche ebenso für die genannten mobilen Betriebssysteme eine App anbieten, um Redundanzen zu vermeiden. Dies wird jedoch in der Endauswertung der zu testenden Applikationen berücksichtigt.

Hersteller	Antropia	Avira	Bear Lock	Deity Kids
Produkt	Care4Kids - Kindersicherung	App Lock+	App Sperre	Kinderland
Betriebssysteme (A, i => Android, iOS)	A	A	A	A
Funktionalitäten				
Ad-Blocker				JA
Appblocker		JA	JA	JA
Downloadblocker				
Loggingfunktion			JA	
Dezidierter Spieleblocker				
Kindgerechte Suchmaschine integriert				
Websitefilter				
Zeitkonto	JA	JA		JA
Sperrung von unbekannten Kontakten				
SMS/MMS von Dritten blockieren				JA
Anrufe von Dritten blockieren				JA
Installationsart				
lokale Anwendung ohne Remotesteuerung	JA	JA	JA	JA
lokale Anwendung mit Remotesteuerung				
Cloud-basierte Anwendung				
Allgemeine Informationen				
Voll funktionsfähige Testversion und Dauer	3 Tage			
Eingeschränkte Testversion und Dauer		Unbegrenzt	Unbegrenzt	Unbegrenzt
Kosten (G = Gerät/Geräte)	1,50€ / einmalig / 1G	1,50€-2,51€ / einmalig / 1G	0,89€-11,99€ / einmalig / 1G	0,90€ - 2,89€ / einmalig / 1G

Hersteller	eScan	Eturi Corp.	Funamo Inc	IT HK Service Limited
Produkt	Mobile Security	OurPact	Funamo Kindersicherung	Kid-Modus - Kindersicherung
Betriebssysteme (A, i => Android, iOS)	A, i	A, i	A	A
Funktionalitäten				
Ad-Blocker				
Appblocker	JA	JA	JA	JA
Downloadblocker	JA			
Loggingfunktion			JA	
Dezidierter Spieleblocker				
Kindgerechte Suchmaschine integriert			JA	
Websitefilter	JA	JA	JA	
Zeitkonto		JA	JA	
Sperrung von unbekannten Kontakten				
SMS/MMS von Dritten blockieren	JA			
Anrufe von Dritten blockieren	JA			
Installationsart				
lokale Anwendung ohne Remotesteuerung	JA			JA
lokale Anwendung mit Remotesteuerung		JA	JA	
Cloud-basierte Anwendung				
Allgemeine Informationen				
Voll funktionsfähige Testversion und Dauer		7 Tage	2 Tage	
Eingeschränkte Testversion und Dauer		Unbegrenzt		Unbegrenzt
Kosten (G = Gerät/Geräte)	Kostenlos	23,88$ oder 83,88$ / 1G / Jahr	19,99$ / einmalig / 1G	4,99€ / einmalig / 1G

Hersteller	Jelly Ansns	JoLo Software	Kiddoware	KIDOZ
Produkt	Child Lock	JoLo Kindersicherung	Kids Place Parental Control	KIDOZ Kinder Spiele & Videos
Betriebssysteme (A, i => Android, iOS)	A	A	A	A
Funktionalitäten				
Ad-Blocker				JA
Appblocker		JA	JA	JA
Downloadblocker				
Loggingfunktion				
Dezidierter Spieleblocker				
Kindgerechte Suchmaschine integriert				JA
Websitefilter			JA	JA
Zeitkonto	JA	JA	JA	JA
Sperrung von unbekannten Kontakten				
SMS/MMS von Dritten blockieren				
Anrufe von Dritten blockieren				
Installationsart				
lokale Anwendung ohne Remotesteuerung	JA		JA	JA
lokale Anwendung mit Remotesteuerung		JA		
Cloud-basierte Anwendung				
Allgemeine Informationen				
Voll funktionsfähige Testversion und Dauer				
Eingeschränkte Testversion und Dauer		Unbegrenzt	Unbegrenzt	Unbegrenzt
Kosten (G = Gerät/Geräte)	Kostenlos	2,39€ bis 4,99€ / Jahr / 1G	5,46€ / einmalig / 1G	10,00€ / Jahr / 1G

Hersteller	Mobile Fence	M-Way Solutions	ootpapps	Protect Your Kid
Produkt	Parental Control	familee kids	Kids Zone Kindersicherung	protect your kid
Betriebssysteme (A, i => Android, iOS)	A	A, i	A	A
Funktionalitäten				
Ad-Blocker			JA	
Appblocker	JA	JA	JA	JA
Downloadblocker				
Loggingfunktion	JA	JA		
Dezidierter Spieleblocker			JA	JA
Kindgerechte Suchmaschine integriert				JA
Websitefilter		JA		JA
Zeitkonto	JA	JA	JA	JA
Sperrung von unbekannten Kontakten				
SMS/MMS von Dritten blockieren	JA			
Anrufe von Dritten blockieren	JA			
Installationsart				
lokale Anwendung ohne Remotesteuerung		JA	JA	JA
lokale Anwendung mit Remotesteuerung	JA			
Cloud-basierte Anwendung				
Allgemeine Informationen				
Voll funktionsfähige Testversion und Dauer	30 Tage	30 Tage		20 Tage
Eingeschränkte Testversion und Dauer			Unbegrenzt	
Kosten (G = Gerät/Geräte)	36,00$ / Jahr / 3G	23,99€ / Jahr / 1G	0,68€ bis 3,39€ / einmalig / 1G	46,92€ / Jahr / 1G

Hersteller	Safe Lagoon Software Inc.	SaferKid	Samsung Electronics Co., Ltd.	Screen Time Labs
Produkt	Safe Lagoon Kindersicherung	SaferKid	Kindermodus	Screen Time Elternaufsicht
Betriebssysteme (A, i => Android, iOS)	A, i (Windows-Version noch nicht verfügbar – Stand: 14.01.18)	A, i	A	A, i
Funktionalitäten				
Ad-Blocker				
Appblocker		JA	JA	JA
Downloadblocker				
Loggingfunktion	JA	JA		JA
Dezidierter Spieleblocker				JA
Kindgerechte Suchmaschine integriert				
Websitefilter	JA	JA		
Zeitkonto	JA	JA	JA	JA
Sperrung von unbekannten Kontakten				
SMS/MMS von Dritten blockieren	JA		JA	
Anrufe von Dritten blockieren	JA		JA	
Installationsart				
lokale Anwendung ohne Remotesteuerung			JA	
lokale Anwendung mit Remotesteuerung	JA	JA		JA
Cloud-basierte Anwendung				
Allgemeine Informationen				
Voll funktionsfähige Testversion und Dauer	7 Tage		Unbegrenzt	14 Tage
Eingeschränkte Testversion und Dauer	Unbegrenzt			Unbegrenzt
Kosten (G = Gerät/Geräte)	47,40$ / Jahr / 5G	199,98$ / Jahr / ∞G	Kostenlos	33,99€ / Jahr / ∞G

Hersteller	ThraceCode Inc	Trend Micro	Whispers Arts
Produkt	Kinder Sperre, Kinder Barriere	Mobile Security	Kid's Shell – Safe Kids-Modus
Betriebssysteme (A, i => Android, iOS)	A	A, i	A
Funktionalitäten			
Ad-Blocker	JA	JA	
Appblocker	JA	JA	JA
Downloadblocker			
Loggingfunktion			
Dezidierter Spieleblocker			
Kindgerechte Suchmaschine integriert		JA	
Websitefilter		JA	
Zeitkonto	JA		JA
Sperrung von unbekannten Kontakten			
SMS/MMS von Dritten blockieren		JA	
Anrufe von Dritten blockieren		JA	
Installationsart			
lokale Anwendung ohne Remotesteuerung	JA	JA	JA
lokale Anwendung mit Remotesteuerung			
Cloud-basierte Anwendung			
Allgemeine Informationen			
Voll funktionsfähige Testversion und Dauer	Unbegrenzt	7 Tage	
Eingeschränkte Testversion und Dauer		Unbegrenzt	Unbegrenzt
Kosten (G = Gerät/Geräte)	1,12€ / einmalig / 1G	19.95€ / Jahr / 1G	9,99€ / einmalig / 1G

Tabelle 3.2: Vorauswahl von verfügbaren Kinderschutzlösungen für Android und iOS

3.1.3 Ausgenommene Produkte

Einige angebotene Kinderschutzlösungen wurden nicht in die Vorauswahl mitaufgenommen. Diese sind mit Begründung nachfolgend aufgeführt.

- Kinderschutzlösungen bestimmter Mobilfunkanbieter: Beispielhaft wurde die tele.ring Kinderschutzlösung nicht in die Vorauswahl miteinbezogen, da jene nur im Zusammenspiel mit einem tele.ring Vertrag funktioniert [100]. Somit ist diese Lösung nicht der breiten Masse zugänglich und wurde deshalb ausgeschlossen. Als valides Programm, welches in die Vorauswahl miteinbezogen wurde, ist hierbei die Kinderschutz Software der deutschen Telekom zu nennen, da jene ohne entsprechenden Vertrag mit dem Anbieter verwendet werden kann.

- Kinderschutzbrowser und -suchmaschine: Diese alleinige Art der Kindersicherung ist ungenügend, denn eine einzelne Browseranwendung, ohne weiterführende Schutzmaßnahmen, kann ohne Probleme umgangen werden. Es stellt sich weiterführend nämlich die Frage, was ein Kind dazu zwingt, dass es den Kinderschutzbrowser bzw. die Kindersuchmaschine verwendet und nicht den Standardbrowser des jeweiligen Betriebssystems. Dies kann nur über entsprechende Funktionalitäten in der Kinderschutzanwendung abgebildet werden.

- Überwachungssoftware für Mitarbeiter und Spionagesoftware: Hierbei handelt es sich um eine Studie über den Vergleich von Kinderschutzanwendungen, worunter eine zweckentfremdete Mitarbeiterüberwachungssoftware oder eine Spionagesoftware nicht in den entsprechenden Scope dieser Diplomarbeit fällt.

3.2 Filterung der Vorauswahl

Die Vorauswahl besteht nun aus folgender Anzahl an kompatiblen Programmen für das jeweilige Betriebssystem:

- Android: 42 Programme (19 Programme aus der Tabelle "Windows 7 und Windows 10" und 23 Programme aus der Tabelle "Android und iOS")

- Windows 7: 32 Programme

- Windows 10: 29 Programme

- iOS: 21 Programme (14 Programme aus der Tabelle "Windows 7 und Windows 10" und 7 Programme aus der Tabelle "Android und iOS")

Anhand der vorhergehenden Tabellen wird erkenntlich, dass nicht jede Kinderschutzlösung denselben Funktionalitätsumfang bietet. Dementsprechend wird die Vorauswahl gefiltert, bevor weitergehend ein praktischer Test vollzogen wird. Dies geschieht anhand der nachfolgenden Kriterienkataloge für die verschiedenen Betriebssysteme.

3.2.1 Kriterienkatalog Windows 7 und Windows 10

Weiterführend findet eine Bewertung der Kinderschutzprogramme für die Betriebssysteme Windows 7 sowie Windows 10 statt.

Bewertung anhand der Kritikalität

Jede Funktionalität, welche in der Vorauswahl definiert und zur Bewertung herangezogen wurde, weist eine unterschiedliche Kritikalität in Hinblick auf den Nutzen und Schutz einer Kinderschutzlösung auf. Für die weitere Auswahl der Windows 7 und Windows 10 Produkte, werden die Funktionalitäten für mobile Geräte ignoriert, da diese hierfür nicht relevant sind. Dies ergibt nachfolgende Tabelle:

Funktionalität	**Kritikalität**
Ad-Blocker	Niedrig
Anwendungsblocker	Hoch
Ausführung v. Dateitypen blockieren	Mittel
USB-Schnittstellen blockieren	Niedrig
Laufwerke blockieren	Niedrig
Downloadblocker	Mittel
Loggingfunktion	Hoch
Portblocker	Mittel
Spamfilter f. Maildienste	Niedrig
Dezidierter Spieleblocker	Niedrig
Kindgerechte Suchmaschine integriert	Niedrig
Websitefilter	Hoch
Zeitkonto	Mittel

Tabelle 3.3: Gewichtung des Kriterienkataloges für Windows 7 sowie Windows 10

Begründet wird dies wie folgt:

- Ad-Blocker: Stellt nur eine niedrige Kritikalität dar, da bereits effiziente Third-Party Lösungen

existieren, welche Werbung und Pop-Ups blockieren und als Browser-Plugin installiert werden können. Die Stiftung Warentest [101] hat dazu bereits einen Test zu solchen Anwendungen wie uBlock Origin [102] oder AdBlock-Plus [103] veröffentlicht.

- Anwendungsblocker [104]: Weist eine hohe Kritikalität auf, da durch die Installation und/oder Ausführung von Anwendungen, der Kinderschutz oder Teile davon je nach Art des ausgeführten Programmes umgangen werden kann. Beispielsweise kann eine kostenlose VPN-Anwendung (wie TunnelBear [105]) verwendet werden, um den Webfilter zu umgehen.

- Ausführung von Dateitypen blockieren: Dies weist eine mittlere Kritikalität auf, da somit ein Installieren von Programmen verhindert wird, wenn die entsprechenden Dateiendungen wie .exe oder .msi, für Kinder oder Jugendliche blockiert [106] werden. Unter Aufsicht kann in weiterer Folge natürlich die Kindersicherung mittels des Elternpassworts/Elternkontos deaktiviert und die Blockierung aufgehoben werden.

- USB-Schnittstellen blockieren [107]: Dies weist eine niedrige Kritikalität auf, da zwar durch externe Medien beispielsweise portable Anwendungen wie ein Browser (z.B. Opera Portable [108]) zur Umgehung des Kinderschutzes durch Dritte heruntergeladen und über einen USB-Stick auf den Computer gebracht werden kann, aber dafür natürlich ein Zugriff auf eine weiteres, ungeschütztes Gerät gegeben sein muss. Weiterführend können neben dem Browser auch Keylogger [109] auf den geschützten Rechner gebracht werden, wodurch ein Aufzeichnen des Passwortes für den Elternbereich einer Kinderschutzsoftware und somit dessen Umgehung möglich wird.

- Laufwerk blockieren [110]: Wenn beispielsweise ein CD-Laufwerk eingebaut ist oder durch ein Kind bzw. einen Jugendlichen nachgerüstet wird, kann dies ebenfalls ein Problem darstellen. Entsprechend der Beschreibung im vorhergehenden Punkt können Anwendungen auf den Rechner gebracht werden mit welchen eine Umgehung der Kindersicherung möglich wird. Aber auch hier wird nur eine niedrige Kritikalität vergeben, da ebenso ein Zugriff auf ein externes, ungeschütztes Gerät gegeben sein muss.

- Downloadblocker [36]: Stellt eine mittlere Kritikalität dar, da durch Downloads von Websites Malware, jugendgefährdendes/urheberrechtlich geschütztes Material oder Anwendungen zur Umgehung von Kinderschutzsoftware auf das jeweilige System heruntergeladen werden können.

- Loggingfunktion: Die Kritikalität ist hierbei als Hoch zu bewerten. Nur durch das Logging kann herausgefunden werden, mit welchen Thematiken sich ein Kind bzw. ein Jugendlicher beschäftigt [111]. Wenn es sich bei diesen Thematiken um jugendgefährdendes Material oder Mobbing

handelt, kann dies mittels einer geeigneten Logging-Methode festgestellt werden. Im Anschluss können Elternteile über eben jene Geschehnisse mit ihren Kindern sprechen und diese Themen mittels eines konstruktiven Gesprächs behandeln.

- Portblocker: Dabei handelt es sich um eine Funktionalität mit mittlerer Kritikalität. Der Portblocker dient dazu, spezifische Verbindungen, welche von einem bestimmten Netzwerkport vom jeweiligen Rechner ein- bzw. ausgehen, zu blockieren. Eine Anwendung könnte hier ein Peer-To-Peer Programm [112] zum Download von urheberrechtlich geschütztem Material sein.

- Spamfilter f. Maildienste: Dies weist eine niedrige Kritikalität auf, da Anbieter von E-Mail-Diensten (wie beispielsweise GMail [113] oder GMX [114]) häufig bereits einen Spam-Filter integriert haben und somit ein abermaliger Schutz in dieser Hinsicht nicht zwingend nötig ist.

- Dezidierter Spieleblocker: Diese Funktionalität stellt eine niedrige Kritikalität dar, da selbst bei einem gut funktionierenden Spieleblocker nur ein marginaler Teil an möglicherweise problematischen Anwendungen für ein Kind bzw. einen Jugendlichen blockiert wird. Konkret bedeutet dies, dass trotz eines dezidierten Spieleblockers, Anwendungen zur Umgehung der Kindersicherung heruntergeladen und ausgeführt werden können.

- Kindgerechte Suchmaschine integriert: Weist eine niedrige Kritikalität auf, da eine entsprechend passende Suchmaschine (wie FragFinn [115]) ebenso im Nachhinein mittels geeigneter Schutzmethodiken im Browser definiert werden kann und dabei Anleitungen für nicht technikaffine Personen bestehen. [116]

- Websitefilter: Bei dieser Funktionalität handelt es sich um den Kern einer Kinderschutzsoftware, ergo wird diese mit einer hohen Kritikalität eingestuft.

- Zeitkonto: Jene Funktionalität wird mit einer mittleren Kritikalität eingestuft, da eine exzessive Nutzung eines Gerätes zwar weitreichende Folgen haben kann [117], aber der konsumierte Inhalt dabei stark ins Gewicht fällt [118]. Das Zeitkonto bietet dementsprechend Schutz vor einer zu extensiven Nutzung des jeweiligen Gerätes, des Internetanschlusses oder einer bestimmten Anwendung.

Weiterführend werden nun die einzelnen Kinderschutzprogramme der Vorauswahl wie folgt beurteilt und mittels Punkten bewertet. Die fünf "besten" sowie die fünf "schlechtesten" Anwendungen werden nachfolgend einem Praxistest anhand definierten Testszenarien und -kriterien unterzogen. Dabei werden fünf in Windows 7 und fünf in Windows 10 getestet.

- Werden Funktionalitäten, welche eine hohe Kritikalität besitzen, erfüllt, dann erhält die Anwendung drei Punkte.
- Werden Funktionalitäten, welche eine mittlere Kritikalität besitzen, erfüllt, dann erhält die Anwendung zwei Punkte.
- Werden Funktionalitäten, welche eine niedrige Kritikalität besitzen, erfüllt, dann erhält die Anwendung einen Punkt.
- Eine Anwendung, welche eine Remotesteuerung über ein anderes Gerät zulässt (entspricht den Funktionalitäten "lokale Anwendung mit Remotesteuerung", [59] "Cloud-basierte Anwendung" [71] und "Routereinstellung" [119]), erhält einen Punkt, da dadurch die Installation und Wartung sowie die Anpassung von entsprechenden Regeln auf mehreren Geräten deutlich vereinfacht wird.
- Anwendungen die kostenlos sind erhalten einen Punkt.

Eine beispielhafte Auswertung erfolgt nun anhand von "Kaspersky Safe Kids":

- Ad-Blocker - Kritikalität: Niedrig - Nicht angegeben - 0/1 Punkte
- Anwendungsblocker - Kritikalität: Hoch - 3/3 Punkte
- Ausführung v. Dateitypen blockieren - Kritikalität: Mittel - 2/2 Punkte
- USB-Schnittstellen blockieren - Kritikalität: Niedrig - Nicht angegeben - 0/1 Punkten
- Laufwerke blockieren - Kritikalität: Niedrig - Nicht angegeben - 0/1 Punkten
- Downloadblocker - Kritikalität: Mittel - 2/2 Punkte
- Loggingfunktion - Kritikalität: Hoch - 3/3 Punkte
- Portblocker - Kritikalität: Mittel - Nicht angegeben - 0/2 Punkte
- Spamfilter f. Maildienste - Kritikalität: Niedrig - 1/1 Punkt
- Dezidierter Spieleblocker - Kritikalität: Niedrig - 1/1 Punkt
- Kindgerechte Suchmaschine integriert - Kritikalität: Niedrig - 1/1 Punkt
- Websitefilter - Kritikalität: Hoch - 3/3 Punkte
- Zeitkonto - Kritikalität: Mittel - 2/2 Punkte

- Anwendung mit Remotesteuerung - 1/1 Punkt
- Nicht kostenlos - 0/1 Punkt
- Erreichte Gesamtpunktezahl: 19/25

Nach der Anwendung des genannten Bewertungsschemas auf die Tabelle 3.1 der Vorauswahl , erhalten die Programme unter Windows 7 sowie Windows 10 folgende Punktezahlen:

Hersteller	**Programm**	**Punktezahl**
AG Kinder Server	KinderServer	5/25
Ars Nova Systems	Parentsaround	12/25
Bitdefender	Internet Security 2018	17/25
Blue Coat	K9 Web Protection	10/25
Bullguard	Internet Security	16/25
Buhl Data Service GmbH	WISO Internet Security	10/25
Content Watch Holding	Net Nanny	9/25
Cybits AG	Surf Sitter	10/25
die4reuters	Aus die Maus	3/25
Entensys	Kindergate Parental Control	11/25
eset	Internet Security	6/25
F-Secure	SAFE	13/25
G Data	Multi Device Security	14/25
Infoweise	SecureTeen Parental Control	15/25
JusProg e.V.	JusProg	10/25
Kaspersky	Safe Kids	19/25
McAffee	Safe Family	12/25
Michael Müller	ParentsFriend	12/25
Microsoft	Family Safety	14/25
Microsoft	Live Family Safety	13/25
Mobicip	Mobicip	12/25
Norton	Family Premier	13/25
OpenDNS	Family Shield	7/25
ProtectCom	Orvell Monitoring	10/25
Quick Heal	Total Security	9/25

Hersteller	Programm	Punktezahl
Qustodio	Qustodio	14/25
SafeDNS	SafeDNS	8/25
Salfeld	Kindersicherung	12/25
SentryPC	SentryPC	14/25
Telekom	Kinderschutz Software	6/25
Trend Micro	Internet Security 2017	12/25
TuEagles	Anti-Porn	12/25
Witigo	Parental Filter	12/25

Tabelle 3.4: Kinderschutzlösungen unter Windows 7 sowie Windows 10 mit Punktebewertung

3.2.2 Kriterienkatalog Android und iOS

Für die weitere Auswahl der Android und iOS Produkte wird, wie zuvor bei den Produkten für Windows, die entsprechende Kritikalität pro Funktionalität bestimmt. Die Liste ist wie folgt:

Funktionalität	Kritikalität
Ad-Blocker	Niedrig
Appblocker	Hoch
Downloadblocker	Mittel
Loggingfunktion	Hoch
Dezidierter Spieleblocker	Niedrig
Kindgerechte Suchmaschine integriert	Niedrig
Websitefilter	Hoch
Zeitkonto	Mittel
SMS/MMS von Dritten blockieren	Hoch
Anrufe von Dritten blockieren	Hoch

Tabelle 3.5: Gewichtung des Kriterienkataloges für Android sowie iOS

Hierbei hat keine Änderung der Kritikalität stattgefunden, da die Funktionalitäten als gleichwertig anzusehen sind, wie unter Windows 7 oder Windows 10. Die Funktionalitäten sind dieselben, nur wurde "Appblocker" synonym für "Anwendungsblocker" verwendet und zusätzlich wurde die Kategorie "Sperrung von unbekannten Kontakten" in die Auswertung miteinbezogen, da dies nur mobile Geräte betrifft. Eine Erörterung bezüglich der gewählten Kritikalität ist wie folgt:

- SMS/MMS von Dritten blockieren: Diese Funktionalität weist eine hohe Kritikalität auf, da mittels Mobilfunk ein großes Risiko durch Dritte im Allgemeinen entsteht. Unter anderem ist hierbei Telefonterror mittels zahlreichen SMS/MMS oder Werbenachrichten, welche über eine Rückantwort zu einem ungewollten Kaufvertrag [120] führen können, als konkretes Problem zu nennen. Ebenso kann über das Medium Mobilfunk seelischer Missbrauch, Belästigung oder Stalking [121] durchgeführt werden (siehe Tabelle 2.2).
- Anrufe von Dritten blockieren: Diese Funktionalität weist eine hohe Kritikalität auf. Die Rechtfertigung dafür, entspricht dem vorhergehenden Unterpunkt, nur wird dies auf Anrufe bezogen.

Eine beispielhafte Auswertung wird nachfolgend anhand der App "Mobicip" durchgeführt:

- Ad-Blocker - Kritikalität: Niedrig - Nicht angegeben - 0/1 Punkt
- Appblocker - Kritikalität: Hoch - 3/3 Punkte
- Downloadblocker - Kritikalität: Mittel - Nicht angegeben - 0/2 Punkte
- Loggingfunktion - Kritikalität: Hoch - 3/3 Punkte
- Dezidierter Spieleblocker - Kritikalität: Niedrig - Nicht angegeben - 0/1 Punkt
- Kindgerechte Suchmaschine integriert - Kritikalität: Niedrig - Nicht angegeben - 0/1 Punkt
- Websitefilter - Kritikalität: Hoch - 3/3 Punkte
- Zeitkonto - Kritikalität: Mittel - 2/2 Punkte
- SMS/MMS von Dritten blockieren - Kritikalität: Hoch - 3/3 Punkte
- Anrufe von Dritten blockieren - Kritikalität: Hoch - 3/3 Punkte
- Anwendung mit Remotesteuerung - 1/1 Punkt
- Nicht kostenlos - 0/1 Punkt
- Erreichte Gesamtpunktezahl: 18/24

Nach der Anwendung des Bewertungsschemas auf die Tabelle 3.1 sowie die Tabelle 3.2 ergeben sich für die nachfolgenden Anwendungen die entsprechenden Punktezahlen:

Hersteller	**Programm**	**Punktezahl**
Antropia	Care4Kids - Kindersicherung	2/24

Hersteller	**Programm**	**Punktezahl**
Ars Nova Systems	Parentsaround	12/24
Avira	App Lock+	5/24
Bear Lock	App Sperre	6/24
Bitdefender	Internet Security 2018	20/24
Blue Coat	K9 Web Protection	10/24
Bullguard	Internet Security 2018	14/24
Buhl Data Service GmbH	WISO Internet Security	15/24
Content Watch Holding	Net Nanny	9 /24
Deity Kids	Kinderland	12/24
Eturi Corp	OurPact	9 /24
eScan	Mobile Security	15/24
F-Secure	SAFE	19/24
Funamo Inc	Funamo Kindersicherung	13/24
G Data	Multi Device Security	17/24
Infoweise	SecureTeen Parental Control	21/24
IT HK Service Limited	Kid-Modus - Kindersicherung	3/24
Jelly Ansns	Child Lock	3/24
JoLo Software	JoLo Kindersicherung	6/24
JusProg e.V.	JusProg	8/24
Kaspersky	Safe Kids	16/24
Kiddoware	Kids Place Parental Control	8/24
KIDOZ	KIDOZ Kinder Spiele & Videos	10/24
McAffee	Safe Family	12/24
Mobicip	Mobicip	18/24
Mobile Fence	Parental Control	15/24
M-Way Solutions	familee Kids	11/24
Norton	Family Premier	19/24
ootpapps	Kid Zone Kindersicherung	7/24
Open DNS	Family Shield	7/24
Protect Your Kid	protect your kid	10/24
Quick Heal	Total Security	9/24

Hersteller	Programm	Punktezahl
Qustodio	Qustodio	20/24
SafeDNS	SafeDNS	8/24
Safe Lagoon Software Inc.	Safe Lagoon Kindersicherung	15/24
SaferKid	SaferKid	12/24
Salfeld	Kindersicherung	12/24
Samsung Electronics Co., Ltd.	Kindermodus	12/24
Screen Time Labs	Screen Time Elternaufsicht	10/24
ThraceCode Inc	Kinder Sperre, Kinder Barriere	6/24
Trend Micro	Mobile Security	14/24
Whispers Arts	Kid's Shell - Safe Kids-Modus	5/24
Witigo	Parental Filter	18/24

Tabelle 3.6: Kinderschutzlösungen unter Android und/oder iOS mit Punktebewertung

3.2.3 Finale Vorauswahl der Produkte für den Praxistest

Aus jeder Tabelle werden nun entsprechend die "besten" sowie die "schlechtesten" fünf Produkte ausgewählt und einem Praxistest unterzogen. Der Grund für diese Art der Auswahl ist zum Einen, dass ein klarer Kontrast zu den "besten" Produkten hergestellt werden soll und zum Anderen kann es durchaus sein, dass ein Produkt eine nicht aussagekräftige Beschreibung durch den Hersteller besitzt und somit schlecht in der Vorauswahl bewertet wurde. Faktisch kann es sich somit bei den "schlechtesten" Produkten, um sehr gute Kinderschutzlösungen handeln und um dies stichprobenartig zu überprüfen, werden jene entsprechend ausgewählt.

Damit sind die zu testenden Produkte wie folgt für Windows 7 und Windows 10 definiert:

Hersteller	Programm	Punktezahl
Kaspersky	Safe Kids	19/25
Bitdefender	Internet Security 2018	17/25
Bullguard	Internet Security	16/25
Infoweise	SecureTeen Parental Control	15/25
G Data	Multi Device Security	14/25
OpenDNS	Family Shield	7/25
Telekom	Kinderschutz Software	6/25

Hersteller	Programm	Punktezahl
eset	Internet Security	6/25
AG Kinder Server	KinderServer	5/25
die4reuters	Aus die Maus	3/25

Tabelle 3.7: Finale Vorauswahl der Produkte zum Praxistest unter Windows 7 und Windows 10

Nach der Vorauswahl erreichen die vier Produkte "Family Safety", "SentryPC", "Multi Device Security" und "Qustodio" einen Gleichstand von 14 Punkten. Für den weiteren Verlauf wurde das Programm "Multi Device Security" von "G Data" ausgewählt, da jenes die höchste Kompatiblitätsbandbreite neben dem Produkt "Qustodio" besaß. Weiterführend wird "Qustodio" unter den mobilen Betriebssystemen getestet. Nun findet sich die Produktauswahl zu Android und iOS. Um Redundanzen hinsichtlich der Umgehungsszenarien und der Bewertungskriterien zu vermeiden, wurden die Apps "Secure Teen Parental Control" von "Infoweise" und "Internet Security 2018" von "Bitdefender" nicht in die Liste der zu testenden Apps mitaufgenommen, da diese bereits unter Windows dem Praxistest unterzogen werden. Die Anwendungen wurden durch die Produkte "Parental Filter" und "Mobicip" ersetzt. Doch während der Ausführung des Tests zeigte sich, dass die Anwendung "Witigo" nicht mehr gewartet wird und keine Funktion aufweist. Das letzte Update fand im Jahre 2017 statt und unterstützt somit die auf dem Testgerät vorhandene iOS Version 11.1 nicht mehr [122]. Dahingehend wurde auch dieses Programm aus dem weiteren Testverfahren ausgeschlossen und wurde durch "Parental Control" von "Safe Lagoon" ersetzt. Somit ist die Produktauswahl wie folgt:

Hersteller	Programm	Punktezahl
Qustodio	Qustodio	20/24
Norton	Family Premier	19/24
F-Secure	SAFE	19/24
Safe Lagoon	Parental Control	15/24
Mobicip	Mobicip	18/24
Whispers Arts	Kid’s Shell - Safe Kids-Modus	5/24
Avira	App Lock+	5/24
Jelly Ansns	Child Lock	3/24
IT HK Service Limited	Kid-Modus - Kindersicherung	3/24
Antropia	Care4Kids - Kindersicherung	2/24

Tabelle 3.8: Finale Vorauswahl der Produkte zum Praxistest unter Android und iOS

4 Testumgebungen und Kriterien

In diesem Kapitel wird der Aufbau der einzelnen Testumgebungen und der dazugehörigen verwendeten Hardware erläutert.

4.1 Aufbau der Testumgebungen

Für den Praxistest wurden unter Windows 7 sowie Windows 10 virtuelle Maschinen und unter Android sowie iOS physische Geräte benutzt. Es wurde das Programm "Virtualbox" von Oracle [123] in der Version 5.2.6 verwendet. In den nachfolgenden Unterkapiteln findet man den Aufbau der verschiedenen Testumgebungen.

4.1.1 Windows 10 Enterprise

Für die Darstellung der Testabläufe unter Windows 10 wurde eine virtuelle Maschine verwendet. Dieses läuft unter folgenden Systemangaben:

- Prozessor - physisch: Intel Core i5-4690K CPU - 4 Kerne mit jeweils 3.50 GHZ
- Grafikkarte - physisch : HD Graphics 4600
- Arbeitsspeicher - virtuell : 4096 MB
- Netzwerkkarte virtuell: Intel PRO/1000 MT Desktop
- Netzwerkkarte physisch: Intel Ethernet Connection I217-V
- System-Version - virtuell: 10.0.15063 Build 15063
- Systemtyp - virtuell: 64 Bit

4.1.2 Windows 7 Enterprise

Die Testumgebung entspricht jener von Windows 10, jedoch wurde hierbei ein Windows 7 64-Bit Image verwendet. Die System-Version ist "6.1.7601 Service Pack 1 Build 7601".

4.1.3 Android

Als Testumgebung wurde ein Nexus 5x von LG mit der Android-Version 7.1.1 und der Kernelversion 4.4.1 verwendet.

4.1.4 iOS

Für den Praxistest unter iOS wurde ein iPhone 7 mit der Version 11.1 verwendet.

4.2 Praxistestkatalog und Umgehungsszenarien

Nachfolgend wurde ein weiterführender Bewertungskatalog definiert, anhand welchem die 10 Produkte, welche aus der finalen Vorauswahl resultierten, getestet werden. Der Praxistestkatalog wurde anhand der Funktionalitäten welche in der Vorauswahl definiert wurden erstellt und weiterführend ergänzt. Die weiteren Kriterien wurden anhand des Produktes mit den meisten und kritischsten Funktionalitäten in der Vorauswahl, welches in diesem Falle "Safe Kids" unter Windows 7 und Windows 10 und "Qustodio" unter Android sowie iOS waren, eruiert. Weiterführend wurde ein ergänzender Bereich zum Praxistest hinzugefügt: die sogenannten "Umgehungsszenarien". Dabei handelt es sich um Testfälle, welche zur Umgehung der Kinderschutzsoftware verwendet werden können und welche bei jedem Programm überprüft wurden.
Die Punktebewertung ist dabei wie folgt:

- Eine Kritikalitätseinstufung des Kriteriums mit "Hoch" bedeutet eine Multiplikation der erhaltenen Punkt mit dem Faktor 3
- Eine Kritikalitätseinstufung des Kriteriums mit "Mittel" bedeutet eine Multiplikation der erhaltenen Punkte mit dem Faktor 2
- Eine Kritikalitätseinstufung des Kriteriums mit "Niedrig" führt zu keiner Multiplikation.

Da einige Anwendungen ihre Filter an dem Alter des Kindes ausrichten, wurde als Testgrundlage angenommen, dass es sich bei dem definierten Benutzer um einen 8 Jährigen handelt. Zudem wird ein Benutzerkonto unter Windows 7 und Windows 10 nach folgenden Kriterien eingerichtet:

- Weist die Software im Installationsprozess darauf hin, dass ein eingeschränktes Benutzerkonto für das Kind bzw. den Jugendlichen verwendet werden soll oder richtet es automatisch ein, dann wird im weiteren Testverlauf ein eingeschränktes Benutzerkonto verwendet.

- Weist die Software im Installationsprozess nicht darauf hin, dass ein eingeschränktes Benutzerkonto verwendet werden soll, wird ein Administrationskonto verwendet.

Das iOS Betriebssystem unterstützt sogenannte "Einschränkungen" [124]. Dabei handelt es sich um einen Elternmodus, welcher durch eine vierstellige PIN geschützt. Darin gibt es die Funktion "App löschen", welche deaktiviert werden kann, um zu verhindern, dass ein Kind eine Kinderschutzanwendung löscht. Da man nicht davon ausgehen kann, dass ein Elternteil automatisch weiß, dass es die Funktionalität gibt und diese aktiviert werden muss, werden die Anwendungen wie folgt getestet:

- Weist die App darauf hin, dass die definierte Einschränkung "App löschen" aktiviert werden muss, wird dies auch im Zuge des Testszenarios berücksichtigt und durchgeführt.
- Weist die App nicht darauf hin, wird keine Einschränkung aktiviert.

Weiterführend ist anzumerken, dass Apple den Zugriff mittels iTunes auf Apps auf mobilen Endgeräten ab der Version 12.7 nicht mehr ermöglicht [125]. Somit ist, betreffend dem Szenario "App löschen" nur ein Test des Löschens am Gerät selbst möglich.

4.2.1 Praxistestkatalog - Windows 7 und Windows 10

Nachfolgend finden sich der Bewertungskatalog für Kinderschutzsoftware und anschließend die Umgehungsszenarien unter den Betriebssystemen Windows 10 sowie Windows 7. Die Maximalpunktezahl setzt sich wie folgt zusammen:

- 5 Punkte in allen Funktionalitäten gemeinsam mit "Niedrig" als Kritikalität.
- 8 Punkte mal Faktor 2 für die Gewichtung ergibt 16 Punkte in allen Funktionalitäten gemeinsam mit "Mittel" als Kritikalität.
- 9 Punkte mal Faktor 3 für die Gewichtung ergibt 27 Punkte in allen Funktionalitäten gemeinsam mit "Hoch" als Kritikalität

Insgesamt ergibt dies eine maximal erreichbare Gesamtbewertung von 48 Punkten.

Kriterium	Beschreibung des Bewertungskriteriums	Kritikalität	Punkte
1. Accounts	Die Software bietet die Funktion mehrere Accounts für Kinder bzw. Jugendliche im Haushalt anzulegen und entsprechend unterschiedliche Filter zu definieren.	Mittel	1
	Die Software bietet einen Kindermodus der für alle im Haushalt befindlichen Kinder bzw. Jugendlichen derselbe ist und somit keine unterschiedlichen Filter definiert werden können.		0
2. Ausführung von spezifischen Dateitypen blockieren	Die Software kann spezifische Dateitypen (beispielsweise .exe oder .jpeg) blockieren.	Mittel	1
	Die Software kann keine spezifischen Dateitypen blockieren.		0
3. Beratungsfunktion	Die Software gibt Eltern konkrete Tipps, wie sie die Einführung einer Kinderschutzsoftware mit ihren Kindern bzw. Jugendlichen besprechen, um die Akzeptanz zu fördern.	Niedrig	1
	Die Software gibt Eltern keine Hilfestellung bei der Einführung einer Kinderschutzsoftware.		0
4. Deinstallationsschutz	Die Software wird mittels eines Passworts und/oder Zwei-Faktor Authentifizierung vor einer Deinstallation und/oder einer Löschung von relevanten Programmdateien zur Ausführung geschützt.	Hoch	1
	Die Software besitzt keinen Schutz vor Deinstallation oder Löschung von essentiellen Programmdaten.		0
5. Downloadblocker	Die Software bietet eine Funktionalität Downloads, welche über einen Browser ausgeführt werden, zu blockieren.	Mittel	1
	Die Software bietet keine Funktionalität Downloads zu blockieren.		0

Kriterium	Beschreibung des Bewertungskriteriums	Kritikalität	Punkte
6. Einrichtungsassistent	Die Software bietet einen Assistenten, welcher bei der Einrichtung der Software unterstützt und Hilfestellungen bietet. Zudem wird ein ausführliches Handbuch oder ein Web-Wiki angeboten.	Mittel	1
	Die Software bietet ein Web-Wiki an und hat entsprechende Hilfefunktionen in der Software integriert.		0,75
	Es wird keine Hilfestellung für die Software geboten.		0
7. Eingeschränkte Benutzerkonten	Die Software legt neue Benutzerkonten für Kinder bzw. Jugendliche, welche keine Admin-Rechte besitzen, sondern eingeschränkten Benutzerkonten entsprechen	Hoch	1
	Die Software weist darauf hin, dass für Kinder bzw. Jugendliche eingeschränkte Benutzerkonten verwendet werden sollen, um eine Umgehung der Kinderschutzsoftware zu erschweren.		0,75
	Die Software legt keine Benutzerkonten oder Konten mit Admin-Rechten für Kinder bzw. Jugendliche an. Ebenso weist die Software beim manuellen Anlegen der Benutzeraccounts nicht darauf hin, dass eingeschränkte Benutzerkonten für Kinder bzw. Jugendliche verwendet werden sollen.		0
8. Installation	Die Installation ist einfach und verständlich formuliert und die Software bietet mehrere Auswahlmöglichkeiten bezüglich des Installationsortes. Zusätzlich werden Tipps & Tricks zum Kinderschutz angezeigt.	Niedrig	1
	Die Installation ist einfach durchführbar und weist keine Komplexität auf.		0,75
	Die Installation ist aufwändig und komplex oder es werden weitere Softwareprodukte /Adware im Installer verpackt, welche entsprechend abgewählt werden müssen.		0

Kriterium	Beschreibung des Bewertungskriteriums	Kritikalität	Punkte
9. Kategoriefilter Web	Die Software bietet verschiedene Filter nach Kategorien für Websites und Inhalte (zB. Pornografie, Einkaufen, Gaming, etc.), welche explizit an das Alter des Kindes bzw. Jugendlichen angepasst werden können.	Hoch	1
	Die Software bietet einen vordefinierten Kategoriefilter, welcher selbst angepasst werden kann, jedoch für alle Benutzer der Kinderschutzsoftware derselbe ist.		0,5
	Die Software bietet keinen variablen Kategoriefilter an.		0
10. Kategoriefilter Anwendungen	Die Software bietet verschiedene Filter nach Kategorien für Anwendungen und Inhalte welche explizit an das Alter des Kindes bzw. Jugendlichen angepasst werden können.	Hoch	1
	Die Software bietet einen vordefinierten Kategoriefilter, welcher selbst angepasst werden kann, jedoch für alle Benutzer der Kinderschutzsoftware derselbe ist.		0,5
	Die Software bietet keinen variablen Kategoriefilter an.		0
11. Laufwerke blockieren	Die Software kann Laufwerke blockieren, um das Einbinden von Festplatten über die internen SATA-Schnittstellen oder das Einlegen von CDs bzw. DVDs zu unterbinden.	Niedrig	1
	Die Software kann keine Laufwerke blockieren.		0
12. Loggingfunktion	Die Software bietet eine Loggingfunktion an, welche relevante Informationen, wie die Ausführung von Programmen, besuchte Websites und versendete Nachrichten sowie Postings in sozialen Netzwerken protokolliert und sichert. Zusätzlich werden Logs automatisch analysiert und das Elternteil bei verdächtigen Aktivitäten (zB. Mobbing) sofort per E-Mail oder SMS gewarnt.	Hoch	1
	Die Software bietet eine Loggingfunktion an, welche relevante Informationen protokolliert und speichert.		0,75
	Die Software bietet keine Loggingfunktion an.		0

Kriterium	Beschreibung des Bewertungskriteriums	Kritikalität	Punkte
13. Portblocker	Die Software bietet die Funktion spezifische Ports zu blocken, um beispielsweise Filesharing oder bestimmte Online-Spiele zu unterbinden.	Mittel	1
	Die Software bietet keinen Portblocker an.		0
14. Prozessschutz	Jegliche Prozesse der Kinderschutzsoftware werden vor einer Beendigung mittels des Taskmanagers geschützt.	Hoch	1
	Die Prozesse der Kinderschutzsoftware werden vor Beendigung nicht geschützt.		0
15. Soziale Netzwerke	Die Software bietet Funktionalitäten hinsichtlich sozialer Netzwerke, wie die Überwachung eingehender Nachrichten oder Postings durch das Kind bzw. den Jugendlichen.	Mittel	1
	Die Software bietet keine spezifischen Funktionalitäten hinsichtlich sozialer Netzwerke.		0
16. Spamfilter für Maildienste	Die Software hat einen Filter integriert, welche Spam in Mailpostfächern erkennt und entsprechend entfernt bzw. kennzeichnet.	Niedrig	1
	Die Software hat keinen Spamfilter integriert.		0
17. Sperren von Anwendungen	Die Software erlaubt es spezifische Anwendungen zu blockieren.	Hoch	1
	Die Software kann keine spezifischen Anwendungen blockieren.		0
18. Sperren von Websites	Die Software erlaubt es spezifische Websites zu blockieren.	Hoch	1
	Die Software kann keine spezifischen Websites sperren.		0

Kriterium	Beschreibung des Bewertungskriteriums	Kritikalität	Punkte
19. Suchmaschine	Die Software bindet eine kindgerechte Suchmaschine wie „FragFinn“ oder „Blinde Kuh“ ein.	Mittel	1
	Die Software verwendet Safe-Search für allgemeine Suchmaschinen, wie Google oder Yahoo.		0,5
	Die Software beschränkt Suchmaschinen nicht und bietet auch keine Safe Search Funktion an.		0
20. USB Schnittstellen blockieren	Die Software kann USB Schnittstellen blockieren, um das Anschließen von USB-Wechselmedien zu unterbinden.	Niedrig	1
	Die Software kann keine USB Schnittstellen blockieren.		0
21. Verwaltung im Web	Die Software erlaubt eine Verwaltung der Kinderschutzsoftware auf einem oder mehreren Endgeräten über ein Onlinekonto und den Login in eine Weboberfläche.	Mittel	1
	Die Software wird lokal verwaltet.		0
22. Zeitbeschränkung	Man kann mittels der Software einen Zeitplan mit Wochentags- und/oder Datumsangabe sowie eine bestimmte Anzahl an Stunden pro Tag definieren. Sobald das Zeitguthaben aufgebraucht wurde, lässt sich der Rechner durch diesen Nutzer nicht mehr verwenden.	Hoch	1
	Die Software erlaubt es eine bestimmte Stundenanzahl pro Tag zu definieren. Sobald das Zeitguthaben aufgebraucht wurde, lässt sich der Rechner durch diesen Nutzer nicht mehr verwenden.		0,5
	Die Software hat keine Einstellung für eine Zeitbeschränkung.		0

Tabelle 4.1: Bewertungskriterien im Praxistest mit Gewichtung - Windows 7 und Windows 10

4.2.2 Umgehungsszenarien - Windows 7 und Windows 10

Nachfolgend finden sich die erstellten Umgehungsszenarien, unter Windows 7 und Windows 10.

1. Szenario: **Änderung der Systemzeit** [126, 127]
   - Betroffene Kriterien: Zeitbeschränkung (möglicherweise gesamte Kindersicherung, wenn es zu Lizenzproblemen durch die Umstellung der Systemzeit kommt)
   - Beschreibung: Das Testszenario beinhaltet dabei den Versuch, ob es im Windows-Betriebssystem möglich ist, die Systemzeit zu ändern. In weiterer Folge soll die Kindersicherung entweder den Änderungsversuch bemerken und unterbinden oder zumindest nicht dadurch gestört sein.
2. Szenario: **Anonymisierender Webproxy** [128, 129]
   - Betroffene Kriterien: Kategoriefilter Web, Sperren von Websites und Suchmaschine
   - Beschreibung: Das Testszenario besteht dabei aus einem HTTP oder HTTPS Zugriff auf fünf verschiedene Web-Proxy Dienste. Diese sind:
     - hide.me
     - hidester.com
     - proxysite.com
     - kproxy.com
     - anonymouse.org

     Dabei wird überprüft, ob auf mindestens einen davon zugegriffen werden kann und ob damit ein Zugriff auf eine normalerweise blockierte Domäne möglich ist.
3. Szenario: **Bruteforce-Angriff** [130–132]
   - Betroffene Kriterien: Gesamte Kindersicherung
   - Beschreibung: Die Kinderschutzsoftware kann möglicherweise umgangen werden, indem das Passwort zum Elternmodus der Software erraten wird. Das Testszenario besteht darin zehn Mal das falsche Passwort einzutippen, um so quasi einen Bruteforce- Angriff zu simulieren. Dabei muss die Kinderschutzsoftware in der Lage sein den Angriff zu unterbinden und bei einer bestimmten Anzahl an fehlgeschlagenen Versuchen eine E-Mail/SMS an die hinterlegte E-Mail Adresse/Telefonnummer des Elternteils zu senden.
4. Szenario: **Essentielle Dateien der Kinderschutzsoftware umbenennen/löschen**
   - Betroffene Kriterien: Gesamte Kindersicherung

- Beschreibung: Die Kinderschutzsoftware kann möglicherweise umgangen werden, indem für die Ausführung essentielle Dateien der Kinderschutzanwendung gelöscht oder umbenannt werden. Das Testszenario besteht dabei aus dem Versuch wichtige Dateien der Kinderschutzanwendung entweder zu löschen oder umzubenennen. Wenn dies nicht möglich ist, wird dies ein weiteres Mal im abgesicherten Modus versucht. Dabei sollte die Kinderschutzanwendung die Manipulation bemerken und diese unterbinden.

5. Szenario: **Keylogger** [133]
   - Betroffene Kriterien: Gesamte Kindersicherung
   - Beschreibung: Die Kinderschutzsoftware kann möglicherweise umgangen werden, indem ein Keylogger durch das Kind bzw. Jugendlichen in dem Account installiert wird und der Erwachsene sich dann mit dem Passwort in den Elternmodus einloggt. Das Testszenario besteht dabei aus der Verwendung von zwei portablen Keyloggern, welche durch die Kinderschutzanwendung blockiert werden müssen. Diese sind:
     - „Wolfeye Keylogger“ [134]
     - „Bester Keylogger“ [135]
6. Szenario: **MAC-Spoofing** [136]
   - Betroffene Kriterien: Kategoriefilter Web, Sperren von Websites und Suchmaschine
   - Beschreibung: Das Testszenario besteht darin, dass entweder eine zufällig generierte MAC-Adresse zugewiesen oder die MAC-Adresse eines unbeschränkten Gerätes imitiert wird. Dabei soll die Kinderschutzanwendung den Manipulationsversuch erkennen und unterbinden.
7. Szenario: **Prozess beenden**
   - Betroffene Kriterien: Gesamte Kindersicherung, Zeitbeschränkung
   - Beschreibung: Die Kinderschutzsoftware kann möglicherweise komplett umgangen werden, indem ein- oder mehrere für die Software essentielle Prozesse beendet werden. Das Testszenario besteht dabei aus zwei verschiedenen Abläufen eine Beendigung des Prozesses zu erzielen Dies geschieht dabei: - über den Taskmanager - über ein offenes Paint-Dokument, welches nicht gespeichert wurde und der Rechner den Herunterfahrprozess einleitet [137]
8. Szenario: **Portable Anwendung**
   - Betroffene Kriterien: Downloadblocker, Kategoriefilter Web, Kategoriefilter Anwendungen, Sperren von Websites Teile der Kindersicherung können möglicherweise umgangen werden,

indem nicht ein, mittels einer Setup-Datei zu installierendes Programm, sondern eine sogenannte „portable“ Anwendung ausgeführt wird. Das Testszenario besteht dabei aus zwei verschiedenen portablen Anwendungen, wo eine Ausführung versucht wird. Diese sind:

- das portable Spiel "Assault Cube" [138], welches repräsentativ einem Ego-Shooter ab 18 Jahren entspricht,
- dem "SR-Iron Browser" [139], welcher einen weiteren, alternativen Browser darstellt und eventuell den Webfilter umgehen kann

9. Szenario: **SafeSearch oder Kindersuchmaschine** [140]
   - Betroffene Kriterien: Kategoriefilter Web, Sperren von Websites
   - Beschreibung: SafeSearch oder die eingerichtete Kindersuchmaschine kann möglicherweise umgangen werden, indem alternative Suchmaschinen zu Bing, Yahoo! oder Google verwendet werden. Das Testszenario besteht dabei aus der Eingabe eines anstößigen Suchbegriffes (zB. Porno) in drei unterschiedliche Suchmaschinen. Diese sind:
     - "DuckDuckGo" [141]
     - "IxQuick" [142]
     - "Qwant" [143]

     Dabei werden Links, Bilder und Videos, welche die Suchmaschine retour gibt, angesehen und darauf untersucht, ob sich anstößige Inhalte zu dem Suchbegriff finden.
10. Szenario: **USB-Tethering** [144]
    - Betroffene Kriterien: Kategoriefilter Web, Sperren von Websites, Zeitbeschränkung
    - Beschreibung: Eine Umgehung der genannten Kriterien kann stattfinden, indem das Kind oder der Jugendliche sich mittels USB-Tethering zu einem ungeschützten und filterfreien Netz verbindet. Für das Testszenario wird ein Smartphone mittels eines USB-Kabels mit dem Rechner verbunden und USB- Tethering aktiviert. Nachfolgend wird versucht sich auf eine normalerweise blockierte Website zu verbinden.
11. Szenario: **Wayback Machine** [144]
    - Betroffene Kriterien: Kategoriefilter Web, Sperren von Websites
    - Beschreibung: Bei diesem Testszenario handelt es sich um den Versuch auf eine Website zu gelangen, welche in periodischen Zeitabständen sogenannte „Snapshots“, also Abbilder von anderen Websites generiert und diese zur Verfügung stellt. Für das Testszenario wird versucht

sich auf die Website der Wayback-Machine [145] zu verbinden und weiterführend über einen Snapshot auf eine normalerweise gesperrte Website zu gelangen.

4.2.3 Praxistestkatalog und Umgehungsszenarien - Android 7.1.1 und iOS 11.1

Nachfolgend finden sich der Bewertungskatalog für Kinderschutzsoftware und anschließend die Umgehungsszenarien unter den Betriebssystemen Android 7.1.1 sowie iOS 11.1. Die Maximalpunktezahl setzt sich wie folgt zusammen:

- 4 Punkte in allen Funktionalitäten gemeinsam mit "Niedrig" als Kritikalität.
- 6 Punkte mal Faktor 2 für die Gewichtung ergibt 12 Punkte in allen Funktionalitäten gemeinsam mit "Mittel" als Kritikalität.
- 9 Punkte mal Faktor 3 für die Gewichtung ergibt 27 Punkte in allen Funktionalitäten gemeinsam mit "Hoch" als Kritikalität

Insgesamt ergibt dies eine maximal erreichbare Gesamtbewertung von 43 Punkten.

Kriterium	Beschreibung des Bewertungskriteriums	Kritikalität	Punkte
1. Anrufe von Dritten blockieren	Die Anwendung erlaubt es, den Empfang von Anrufen von unbekannten Kontakten automatisch zu blockieren.	Hoch	1
	Das Empfangen von Anrufen von bekannten Kontakten kann nach explizitem Hinzufügen zu einer Liste entsprechend gesperrt werden.		0,5
	Das Empfangen von Anrufen kann nicht gesperrt werden.		0
2. Ausführung von spezifischen Dateitypen blockieren	Die Software kann spezifische Dateitypen (beispielsweise .apk oder .jpeg) blockieren.	Mittel	1
	Die Software kann keine spezifischen Dateitypen blockieren.		0
3. Beratungsfunktion	Die Software gibt Eltern konkrete Tipps, wie sie die Einführung einer Kinderschutzsoftware mit ihren Kindern bzw. Jugendlichen besprechen, um die Akzeptanz zu fördern.	Niedrig	1
	Die Software gibt Eltern keine Hilfestellung bei der Einführung einer Kinderschutzsoftware.		0
4. Datenübertragung über Lightning Connector / USB blockieren	Die Software kann die Datenübertragung über den USB-Port / Lightning Connector blockieren, um Datenübertragungen von anderen Medien zu unterbinden.	Niedrig	1
	Die Software kann keine Datenübertragungen über den USB-Port / Lightning Connector blockieren.		0
5. Deinstallationsschutz	Die Software wird mittels eines Passworts und/oder Zwei-Faktor Authentifizierung vor einer Deinstallation geschützt.	Hoch	1
	Die Software besitzt keinen Schutz vor einer Deinstallation.		0

Kriterium	Beschreibung des Bewertungskriteriums	Kritikalität	Punkte
6. Einrichtungsassistent	Die App bietet einen Assistenten, welcher bei der Einrichtung unterstützt und Hilfestellungen bietet. Zudem wird ein ausführliches Handbuch oder ein Web-Wiki angeboten.	Mittel	1
	Die App bietet ein Web-Wiki an und hat entsprechende Hilfefunktionen in der Software integriert.		0,75
	Es wird keine Hilfestellung für die Anwendung geboten.		0
7. Installation	Die Installation ist einfach durchführbar und weist keine Komplexität auf.	Niedrig	1
	Die Installation ist aufwändig und komplex oder es werden weitere Softwareprodukte /Adware mitinstalliert oder vorgeschlagen.		0
8. Kategoriefilter Apps	Die Software bietet verschiedene Filter nach Kategorien für Anwendungen und Inhalte (zB. Pornografie, Einkaufen, Gaming, etc.), welche explizit an das Alter des Kindes bzw. Jugendlichen angepasst werden können.	Hoch	1
	Die Software bietet keinen variablen Kategoriefilter an.		0
9. Kategoriefilter Web	Die Software bietet verschiedene Filter nach Kategorien für Websites und Inhalte (zB. Pornografie, Einkaufen, Gaming, etc.), welche explizit an das Alter des Kindes bzw. Jugendlichen angepasst werden können	Hoch	1
	Die Software bietet keinen variablen Kategoriefilter an.		0

Kriterium	Beschreibung des Bewertungskriteriums	Kritikalität	Punkte
10. Loggingfunktion	Die Software bietet eine Loggingfunktion an, welche relevante Informationen, wie die Ausführung von Programmen, besuchte Websites und versendete Nachrichten sowie Postings in sozialen Netzwerken protokolliert und speichert. Zudem wird das Elternteil bei verdächtigen Aktivitäten (zB. Mobbing) sofort per E-Mail oder SMS gewarnt.	Hoch	1
	Die Software bietet eine Loggingfunktion an, welche relevante Informationen protokolliert und speichert.		0,75
	Die Software bietet keine Loggingfunktion an.		0
11. SMS von Dritten blockieren	Die Anwendung erlaubt es, den Empfang von SMS von unbekannten Kontakten automatisch zu blockieren.	Hoch	1
	Das Empfangen von SMS von bekannten Kontakten kann nach explizitem Hinzufügen zu einer Liste entsprechend gesperrt werden.		0,5
	Das Empfangen von SMS kann nicht gesperrt werden.		0
12. Soziale Netzwerke	Die Software bietet Funktionalitäten hinsichtlich sozialer Netzwerke, wie die Überwachung eingehender Nachrichten oder Postings durch das Kind bzw. den Jugendlichen.	Mittel	1
	Die Software bietet keine spezifischen Funktionalitäten hinsichtlich sozialer Netzwerke.		0
13. Spamfilter für Maildienste	Die Software hat einen Filter integriert, welche Spam in Mailpostfächern erkennt und entsprechend entfernt bzw. kennzeichnet.	Niedrig	1
	Die Software hat keinen Spamfilter integriert.		0

Kriterium	Beschreibung des Bewertungskriteriums	Kritikalität	Punkte
14. Sperren von Apps	Die Software erlaubt es Anwendungen einer Whitelist hinzuzufügen und fremde Apps somit automatisch zu blockieren.	Hoch	1
	Die Software erlaubt es spezifische Anwendungen zu blockieren.		0,75
	Die Software kann keine spezifischen Anwendungen blockieren.		0
15. Sperren von Websites	Die Software erlaubt es spezifische Websites zu blockieren.	Hoch	1
	Die Software kann keine spezifischen Websites sperren.		0
16. Store-Blocker	Die Software bietet eine Funktionalität Downloads aus dem Apple App-Store / Google Play Store zu unterbinden.	Mittel	1
	Die Software bietet keine Funktionalität Downloads aus dem Apple App-Store / Google Play Store zu unterbinden.		0
17. Suchmaschine	Die Software bindet eine kindgerechte Suchmaschine wie „FragFinn“ oder „Blinde Kuh“ ein.	Mittel	1
	Die Software verwendet Safe-Search für allgemeine Suchmaschinen, wie Google oder Yahoo.		0,5
	Die Software beschränkt Suchmaschinen nicht und bietet auch keine Safe Search Funktion an.		0

Kriterium	Beschreibung des Bewertungskriteriums	Kritikalität	Punkte
18. Verwaltung im Web	Die Software erlaubt eine Verwaltung der Kinderschutzsoftware auf einem oder mehreren Endgeräten über ein Onlinekonto und den Login in eine Weboberfläche.	Mittel	1
	Die Software wird lokal verwaltet.		0
19. Zeitbeschränkung	Man kann mittels der Software einen Zeitplan mit Wochentags- und/oder Datumsangabe sowie eine bestimmte Anzahl an Stunden pro Tag definieren. Sobald das Zeitguthaben aufgebraucht wurde, lässt sich das Smartphone durch diesen Nutzer nicht mehr verwenden.	Hoch	1
	Die erlaubt es eine bestimmte Stundenanzahl pro Tag zu definieren. Sobald das Zeitguthaben aufgebraucht wurde, lässt sich das Smartphone durch diesen Nutzer nicht mehr verwenden.		0,5
	Die Software hat keine Einstellung für eine Zeitbeschränkung.		0

Tabelle 4.2: Bewertungskriterien im Praxistest mit Gewichtung - Android und iOS

4.2.4 Praxistestkatalog und Umgehungsszenarien - Android 7.1.1 und iOS 11.1

Nachfolgend finden sich die erstellten Umgehungsszenarien, unter Android 7.1.1 und iOS 11.1.

1. Szenario: **Änderung der Systemzeit** [146]
   - Betroffene Kriterien: Zeitbeschränkung (möglicherweise gesamte Kindersicherung, wenn es zu Lizenzproblemen durch die Umstellung der Systemzeit kommt)
   - Beschreibung: Das Testszenario beinhaltet dabei den Versuch, ob es unter Android oder iOS möglich ist, die Systemzeit zu ändern. Die Kinderschutzsoftware soll den Änderungsversuch bemerken und unterbinden.
2. Szenario: **Anonymisierender Webproxy** [128, 129]
   - Betroffene Kriterien: Kategoriefilter Web, Sperren von Websites und Suchmaschine
   - Beschreibung: Das Testszenario besteht dabei aus einem HTTP oder HTTPS Zugriff auf fünf verschiedene Web-Proxy Dienste. Diese sind:
     - hide.me
     - hidester.com
     - proxysite.com
     - kproxy.com
     - anonymouse.org

     Dabei wird überprüft, ob auf mindestens einen davon zugegriffen werden kann und ob damit ein Zugriff auf eine normalerweise blockierte Domäne möglich ist.
3. Szenario: **Anwendung beenden**
   - Betroffene Kriterien: Gesamte Kindersicherung
   - Beschreibung: Das Testszenario besteht dabei aus dem Versuch die Kinderschutzapp zu beenden. Dabei wird zuerst versucht die Anwendung mittels des integrierten Taskmanagers zu beenden. Schlägt dieser Versuch fehl, wird versucht nach einem Neustart des Smartphones die App am Starten zu hindern. Beide Versuche sollen durch die Kinderschutzanwendung unterbunden werden.
4. Szenario: **App löschen**
   - Betroffene Kriterien: Gesamte Kindersicherung

- Beschreibung: Das Testszenario besteht dabei aus dem Versuch die Kinderschutzapp zu löschen. Dabei wird zuerst versucht über die systemeigenen Funktionen die Anwendung zu deinstallieren. Falls dies nicht funktioniert, wird das Smartphone an einen Rechner per USB/Lightning-Connector angeschlossen und es wird dann versucht die Anwendung per manuellem Zugriff zu löschen. Die Kinderschutzanwendung sollte beide Versuche unterbinden.

5. Szenario: **Bruteforce-Angriff** [130–132]
   - Betroffene Kriterien: Gesamte Kindersicherung
   - Beschreibung: Die Kinderschutzsoftware kann möglicherweise umgangen werden, indem das Passwort zum Elternmodus der Software erraten wird. Das Testszenario besteht darin zehn Mal das falsche Passwort einzutippen, um so quasi einen Bruteforce- Angriff zu simulieren. Dabei muss die Kinderschutzsoftware in der Lage sein den Angriff zu unterbinden und bei einer bestimmten Anzahl an fehlgeschlagenen Versuchen eine E-Mail/SMS an die hinterlegte E-Mail Adresse/Telefonnummer des Elternteils zu senden.
6. Szenario: **SafeSearch oder Kindersuchmaschine** [140]
   - Betroffene Kriterien: Kategoriefilter Web, Sperren von Websites
   - Beschreibung: SafeSearch oder die eingerichtete Kindersuchmaschine kann möglicherweise umgangen werden, indem alternative Suchmaschinen zu Bing, Yahoo! oder Google verwendet werden. Das Testszenario besteht dabei aus der Eingabe eines anstößigen Suchbegriffes (zB. Porno) in drei unterschiedliche Suchmaschinen. Diese sind:
     - "DuckDuckGo" [141]
     - "IxQuick" [142]
     - "Qwant" [143]

     Dabei werden Links, Bilder und Videos, welche die Suchmaschine retour gibt, angesehen und darauf untersucht, ob sich anstößige Inhalte zu dem Suchbegriff finden.
7. Szenario: **Wayback Machine** [144]
   - Betroffene Kriterien: Kategoriefilter Web, Sperren von Websites
   - Beschreibung: Bei diesem Testszenario handelt es sich um den Versuch auf eine Website zu gelangen, welche in periodischen Zeitabständen sogenannte „Snapshots“, also Abbilder von anderen Websites generiert und diese zur Verfügung stellt. Für das Testszenario wird versucht sich auf die Website der Wayback-Machine [145] zu verbinden und weiterführend über einen Snapshot auf eine normalerweise gesperrte Website zu gelangen.

5 Ergebnisse aus dem Praxistest und den Umgehungsszenarien unter Windows 10 und Windows 7

Nachfolgend werden die Ergebnisse aus dem Praxistest aufgeführt. Da insgesamt zehn Anwendungen unter Windows 7 sowie Windows 10 dem Praxistest unterzogen werden, wurden pro Betriebssystem jeweils fünf Anwendungen getestet.

Kaspersky Safe Kids 1.0.3.326 – Praxistestkatalog – Windows 10			
Kriterium	**Beschreibung des Bewertungskriteriums**	**Kritikalität**	**Punkte**
1. Accounts	Kaspersky SafeKids erlaubt das Anlegen von Benutzerkonten für mehrere Jugendliche bzw. Kinder und erlaubt eine entsprechende Anpassung der Altersgruppe	Mittel	1
2. Ausführung von spezifischen Dateitypen blockieren	Spezifische Dateitypen können in der Anwendung nicht blockiert werden.	Mittel	0
3. Beratungsfunktion	Die Software steht Eltern beratend zur Seite und empfiehlt eine selektive Verwendung der erhaltenen Informationen durch die Kinderschutzsoftware. Dabei ist der grundlegende Gedanke, dass hierbei sehr vorsichtig und sensibel mit den erhaltenen Informationen umgegangen werden soll.	Niedrig	1
4. Deinstallationsschutz	Um die Konfiguration von Kaspersky Safe Kids ändern zu können benötigt die Software sowohl im Eltern Benutzerkonto als auch dem Kinder bzw. Jugendlichen Konto ein Passwort. Zudem können Dateien nicht ohne Admin-Rechte entfernt werden und ebenso wird bei der Deinstallation der Anwendung über die Systemsteuerung ein Passwort abgefragt.	Hoch	1
5. Downloadblocker	Die Software bietet keine Funktionalität Downloads zu blockieren.	Mittel	0
6. Einrichtungassistent	Die Anwendung bietet einen Einrichtungsassistenten an, welcher auf unkomplizierte Art und Weise die essentiellen Funktionalitäten der Software erläutert und es einem direkt erlaubt ein Konto für das Kind bzw. den Jugendlichen einzurichten. Zudem wird ein ausführliches Web-Wiki geboten, das die Software weitergehend erläutert und eine Hilfestellung bei der weiterführenden Einrichtung bietet.	Mittel	1

Kriterium	Beschreibung des Bewertungskriteriums	Kritikalität	Punkte
7. Eingeschränkte Benutzerkonten	Wenn über Kaspersky Safe Kids ein Kind bzw. Jugendlicher angelegt wird, muss dabei das Geburtsdatum und der Name angegeben werden. Weiterführend kann in der Software direkt ein Benutzerkonto für die Person angelegt und jene auch damit verknüpft werden. Dabei handelt es sich um ein eingeschränktes Benutzerkonto. Anzumerken ist, dass es ebenso möglich ist einem Kind ein Administrationskonto zuzuweisen, was jedoch durchaus gewollt sein kann.	Hoch	1
8. Installation	Die Anwendung führt den Anwender auf einfache Art und Weise durch die Installation. Dabei kann der Installationsort ausgewählt werden und zudem werden Ratschläge an Eltern gegeben, wie sie die Software einsetzen sollten.	Niedrig	1
9. Kategoriefilter Web	Die Software bietet verschiedenste Kategoriefilter (Inhalte für Erwachsene, Karrierenetzwerke, Anonymisierer etc.) an, welche für jeden Benutzer unterschiedlich sein können. Die breite Auswahl ermöglicht eine feingranulare Filterung von Webinhalten.	Hoch	1
10. Kategoriefilter Anwendungen	Entsprechend dem kategorischen Webfilter werden in diesem Bereich verschiedenste Arten von Filterkategorien angeboten (Browser, Spiele, FTP-Clients etc.), wodurch auch hier eine feingranulare Filterung der zugelassenen Inhalte möglich ist. Die Filterung geschieht auch hier auf Benutzerkonten-Ebene.	Hoch	1
11. Laufwerke blockieren	Die Software kann keine Laufwerke blockieren.	Niedrig	0

Kriterium	Beschreibung des Bewertungskriteriums	Kritikalität	Punkte
12. Loggingfunktion	Kaspersky Safe Kids loggt die verwendeten Anwendungen sowie die Nutzungsdauer. Ebenso werden jegliche Websiteaufrufe, egal ob jene erfolgreich, geblockt oder der Benutzer gewarnt wurde inklusive Timestamp geloggt. Ebenso ermöglicht die Software, dass die Verbindung mit einem Facebook-Konto des Kindes vebunden wird. Dabei ist jedoch eine Aktivierung des Kindes mit dem entsprechenden Account nötig.	Hoch	0,75
13. Portblocker	Die Anwendung bietet keinen Portblocker an.	Mittel	0
14. Prozessschutz	Selbst mit Admin-Rechten lässt sich der Prozess der Software nicht stoppen.	Hoch	1
15. Soziale Netzwerke	Eine Überwachung der sozialen Netzwerke ist mit Kaspersky Safe Kids möglich (siehe Loggingfunktion). Da das entsprechende Facebook-Konto jedoch über einen Aktivierungslink, welcher vom entsprechenden Account des Kindes bzw. Jugendlichen akzeptiert werden muss, verbunden wird, ist es fraglich inwiefern diese Funktionalität sinnvoll ist. Hierbei ist es möglich, dass ein Zweitaccount vom Kind bzw. Jugendlichen geführt wird, welcher nicht überwacht wird. Trotzdessen wird die Funktionalität erfüllt, und die Anwendung erhält den entsprechenden Punkt.	Mittel	1
16. Spamfilter für Maildienste	Die Software hat keinen Spamfilter integriert.	Niedrig	0
17. Sperren von Anwendungen	Die Software kann eine spezifische Anwendung erlauben, komplett blockieren oder das Programm zeitlich beschränken, was beispielsweise bei Computerspielen zur Suchtvermeidung sinnvoll ist.	Hoch	1

Kriterium	Beschreibung des Bewertungskriteriums	Kritikalität	Punkte
18. Sperren von Websites	Die Software ermöglicht es Websites explizit freizugeben oder zu sperren.	Hoch	1
19. Suchmaschine	Kaspersky Safe Kids ermöglicht es die sichere Suche von Suchmaschinen wie Google, Bing, Yahoo! oder Yandex zu aktivieren.	Mittel	0,5
20. USB Schnittstellen blockieren	Die Software kann keine USB Schnittstellen blockieren.	Niedrig	0
21. Verwaltung im Web	Eine Verwaltung über eine Weboberfläche ist in dem Falle von Kaspersky Safe Kids gegeben. Dabei lassen sich mehrere Geräte, inklusive der mobilen Geräte, in die Web-Steuerung einpflegen und verwalten.	Mittel	1
22. Zeitbeschränkung	Die Zeitkontofunktion findet sich unter dem Punkt „Geräteverwendung“. Dabei lassen sich für jedes einzelne eingepflegte Benutzerkonto eigene Zeitkonten einrichten. Die Funktionalität ist äußerst feingranular gestaltet. Entweder kann man die Computernutzung pro Tag auf eine bestimmte Anzahl von Stunden begrenzen, oder es lässt sich ein Zeitplan erstellen, zu welchem die Computernutzung zu bestimmten Zeiten an gewählten Tagen, erlaubt wird. das heißt es lässt sich die Computernutzung entweder pro einzelnem Tag	Hoch	1
Gesamtbewertung	**Hoch 8,75x3 + Mittel 4,5x2 + Niedrig 2x1 = 37,25/48**		

Tabelle 5.1: Ergebnis - Kaspersky Safe Kids - Praxistestkatalog

Kaspersky Safe Kids – Umgehungsszenarien – Windows 10 – Konto ohne Admin-Rechte		
Szenario	**Beschreibung**	**Bewertung**
Änderung der Systemzeit	Unter Windows 10 lässt sich ohne Administrationsrechte die Systemzeit nicht ändern. Da Kaspersky Safe Kids normalerweise eingeschränkte Benutzerkonten einrichtet, ist somit keine Änderung in Windows selbst möglich. Wenn es zu einer Änderung kommt, warnt Kaspersky den Elternaccount über eine Benachrichtigung und man kann die Systemzeit wieder korrigieren.	Bestanden
Anonymisierender Webproxy	Kaspersky Safe Kids hat in den Standardeinstellungen automatisch alle fünf Web-Proxy Dienste komplett blockiert.	Bestanden
Bruteforce-Angriff	**Kaspersky Safe Kids warnt die Eltern nicht per E-Mail oder SMS und nach über 10 fehlgeschlagenen Versuchen ist weiterhin ein Login möglich.**	**Nicht bestanden**
Essentielle Dateien der Kinderschutzsoftware umbenennen / löschen	Die Dateien können nicht ohne Administrationsrechte im Account des Kindes gelöscht werden. Selbst im abgesicherten Modus ist ohne Administrationsrechte unter Windows 10 keine Änderung möglich. **Über den abgesicherten Modus mit Netzwerktreibern wird verhindert, dass die Kinderschutzanwendung Safe Kids ausgeführt wird. Dadurch wurde der gesamte Schutzmechanismus ausgehebelt und es ist ein Zugriff auf jegliche gesperrten Websites und Anwendungen ohne Überwachung und ohne Logging möglich.**	**Nicht bestanden**
Keylogger	Unter Windows 10 wurde der Keylogger als Virus erkannt und automatisch entfernt. Da dies nicht der Verdienst von Kaspersky Safe Kids war, wurde der Windows Defender deaktiviert. **Danach konnte der Wolfeye Keylogger ohne Weiteres gestartet und zum Auslesen des Passworts verwendet werden. Ebenso konnte der zweite Keylogger installiert und ausgeführt werden. Auch hier war ein Auslesen des Passworts möglich.**	**Nicht bestanden**

Szenario	Beschreibung	Bewertung
MAC-Spoofing	Eine Zuweisung einer anderen MAC-Adresse ist ohne Admin-Rechte nicht möglich. Trotz Eingabe des Admin-Passworts und einer nachfolgenden Änderung der MAC-Adresse, greift der Webfilter noch immer.	Bestanden
Prozess beenden	Der Prozess lässt sich weder mit noch ohne Admin-Rechte beenden. Wenn der Herunterfahrprozess eingeleitet wird, während ein bearbeitetes, ungespeichertes Paint-Dokument offen ist und danach der Abschaltprozess unterbrochen wird, ist der Kinderschutzprozess weiterhin aktiv und somit ist ein durchgehender Schutz gewährleistet.	Bestanden
Portable Anwendung	• Assault Cube: Die Website zu der portablen Anwendung „Assault Cube“ wurde nicht gesperrt. Dies erlaubte weiterführend einen Download des portablen Spiels. Darauffolgend wurde das Programm im Dokumentenbereich des Benutzers installiert, wofür keine Admin-Rechte nötig waren. **Eine Ausführung war ebenso ohne Weiteres möglich, da das Spiel als ein 0+ Titel erkannt wurde.** Ein Ego-Shooter sollte mindestens ab 16 bzw. 18 Jahren freigegeben sein. **Zudem ist anzuführen, dass das Programm in „Lernsoftware 5000“ umbenannt werden konnte und auch als solches im Logging von Kaspersky Safe Kids aufscheint. Ein unwissendes Elternteil könnte somit denken, dass es sich wirklich um eine Lernsoftware handelt.** • SR Ware Iron Browser: Der Zugriff auf srware.net wird nicht blockiert und die portable Version des Browsers kann ohne Weiteres heruntergeladen und ausgeführt werden. **Eingegebene Suchbegriffe werden nicht geloggt und der Webfilter greift in diesem Falle gar nicht – es ist ein Zugriff auf alle normalerweise blockierten Websites möglich.**	**Nicht bestanden**

Szenario	Beschreibung	Bewertung
SafeSearch oder Kindersuchmaschine	• duckduckgo**: Safe Search ist zwar standardmäßig aktiv, lässt sich aber deaktivieren. Wenn dabei ein Suchbegriff eingegeben wird, der anstößig ist, werden Bilder angezeigt.** • ixquick.com: **Safe Search ist auch hier zwar standardmäßig aktiv, lässt sich jedoch ebenso deaktivieren. Abermals werden Bilder zu anstößigen Inhalten angezeigt.** • qwant.com: **Auch hier lässt sich Safe Search deaktivieren und es werden anstößige Bilder nach Eingabe eines anstößigen Suchbegriffes angezeigt**	**Nicht bestanden**
USB-Tethering	USB-Tethering hat keinen Einfluss auf die Funktionalität des Webfilters.	Bestanden
Wayback Machine	Auf web.archive.org konnte zugegriffen werden und **Snapshots von normalerweise blockierten Seiten konnten aufgerufen werden.**	**Nicht bestanden**
Gesamtbewertung	**6 (54,55%) von 11 Szenarien wurden nicht bestanden.**	

Tabelle 5.2: Ergebnis - Kaspersky Safe Kids - Umgehungsszenarien

5.0.1 Fazit - Kaspersky Safe Kids

Als Vorreiter mit dem ersten Rang unter Windows 7 sowie Windows 10 in der Vorauswahl prämiert und ebenso weitergehend ein sehr gutes Ergebnis mit 37,25 von 48 Punkten im Praxistestkatalog erzielend, enttäuscht das Programm mit 6 von 11 nicht bestandenen Umgehungsszenarien. Dabei wird in zwei Umgehungsszenarien, nämlich dem Szenario "Bruteforce-Angriff" und "Essentielle Dateien der Kinderschutzsoftware umbenennen/löschen" das Logging der Software komplett umgangen bzw. es wurde im Falle des Bruteforce-Angriffes überhaupt nicht implementiert. Im Szenario "Essentielle Dateien der Kinderschutzsoftware umbenennen/löschen" ist die Bootoption "Sicherer Modus mit Netzwerk" das Hauptproblem. Dabei werden nur essentielle Dienste unter Windows gestartet, wovon Kaspersky Safe Kids keiner ist. Zwar kann das Programm ohne Admin-Rechte nicht gelöscht werden, faktisch lässt sich damit jedoch das gesamte Logging, sowie der Anwendungs- und Webfilter umgehen, was das Programm in diesem Falle komplett unbrauchbar macht. Das Booten in diesen Modus ist mit einem äußerst geringen Aufwand verbunden und ohne Admin-Rechte durchführbar.

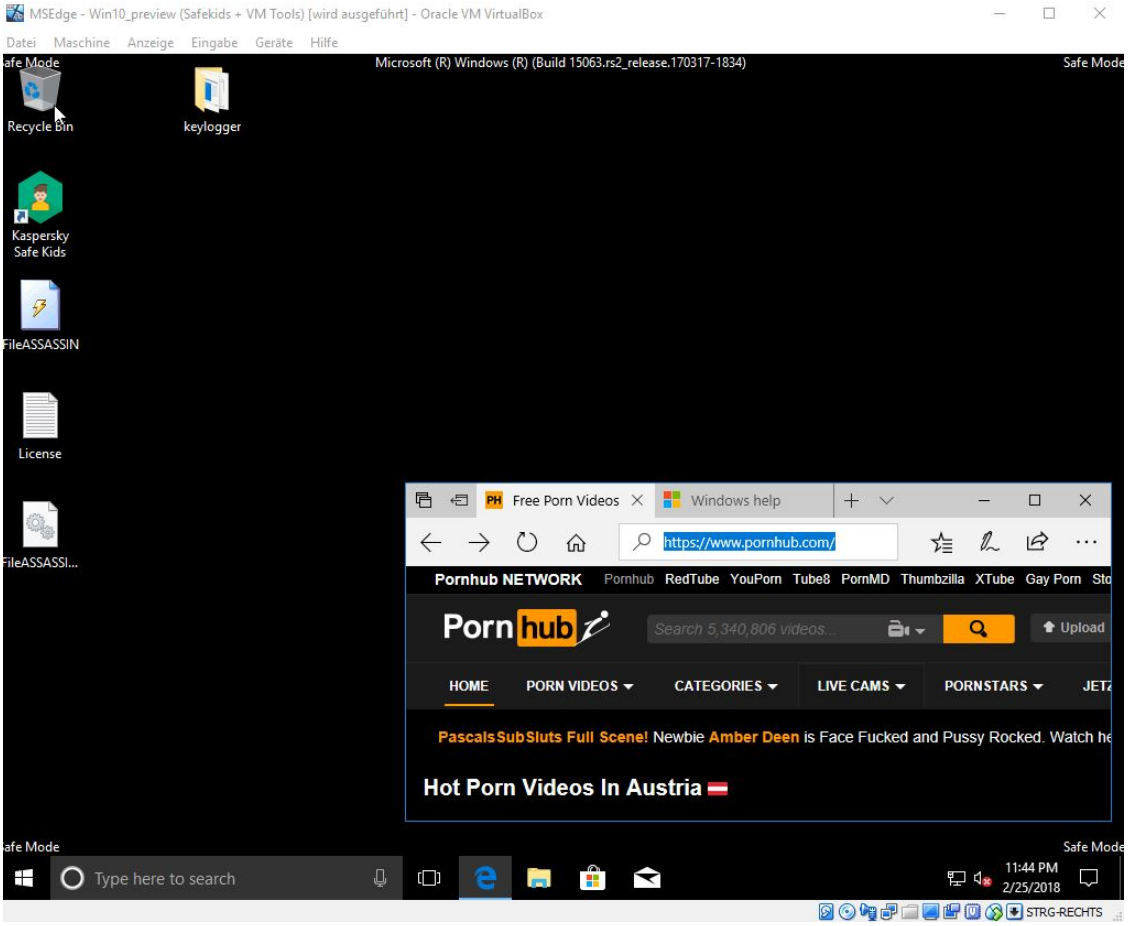

Abbildung 5.1: Ergebnis des Umgehungsszenarios "Essentielle Dateien der Kinderschutzsoftware umbenennen/löschen"

Weiterführend finden sich Screenshots aus anderen Umgehungsszenarien, welche erfolgreich waren:

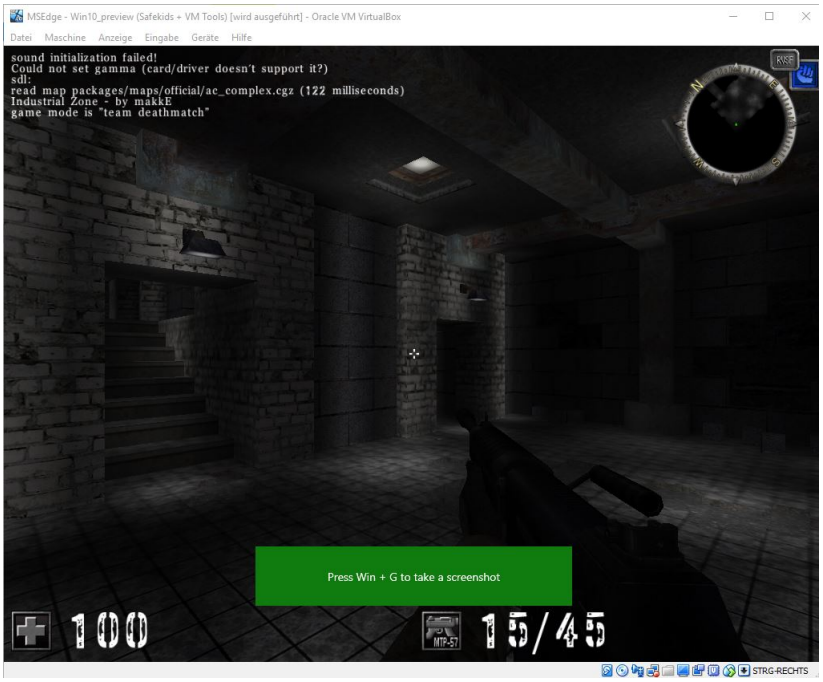

Abbildung 5.2: Umgehungsszenario "Portable Anwendungen" - Ausführung des 18+ Spiels "Assault Cube"

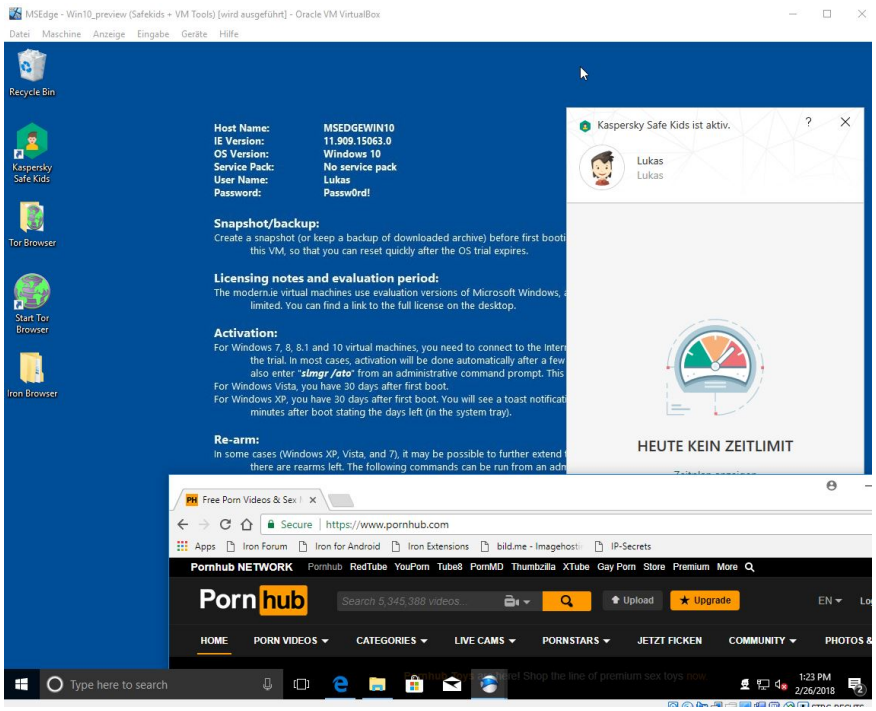

Abbildung 5.3: Umgehungsszenario „Portable Anwendungen“- Webfilter-Umgehung mittels „SRWare Iron Browser“

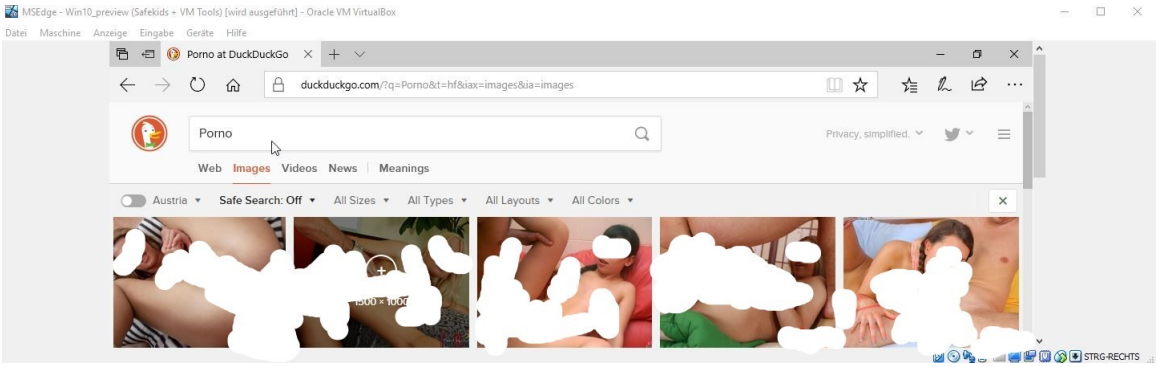

Abbildung 5.4: Umgehungsszenario „SafeSearch oder Kindersuchmaschine “- Webfilter-Umgehung mittels duckduckgo, einer der drei getesteten Suchmaschinen

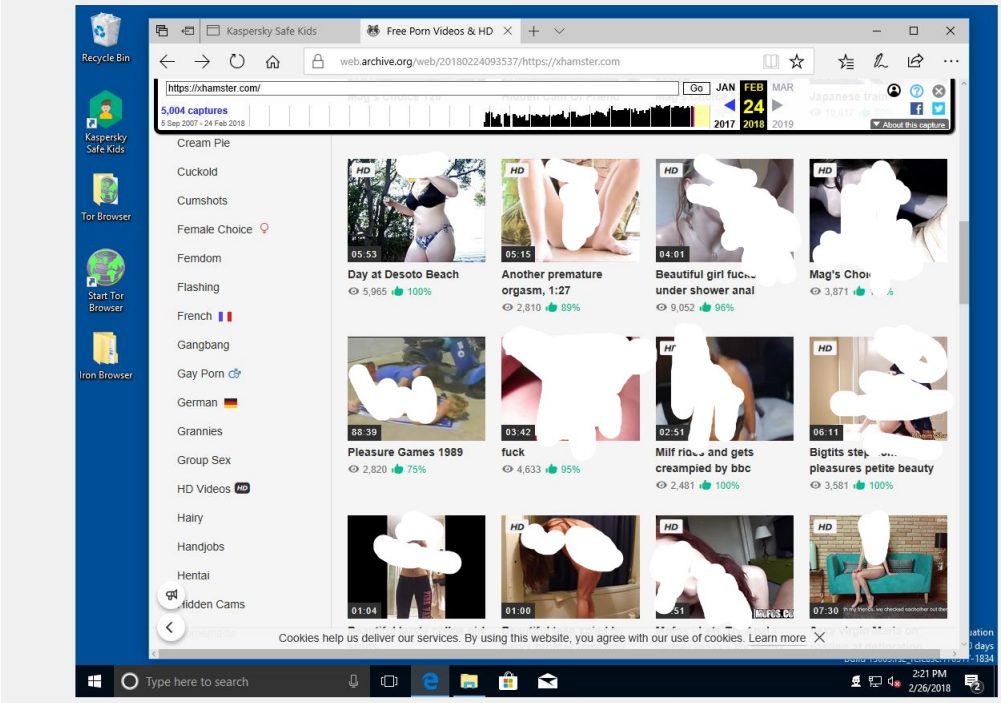

Abbildung 5.5: Umgehungsszenario „Waybackmachine “- Webfilter-Umgehung mittels der Verwendung eines Snapshots von web.archive.org

Bitdefender Internet Security 2018 22.0.21.297 – Praxistestkatalog – Windows 7			
Kriterium	**Beschreibung des Bewertungskriteriums**	**Kritikalität**	**Punkte**
1. Accounts	Mehrere Accounts können angelegt und dabei unterschiedliche Filterkategorien aktiviert werden.	Mittel	1
2. Ausführung von spezifischen Dateitypen blockieren	Spezifische Dateitypen können mittels Bitdefender Internet Security 2018 nicht blockiert werden.	Mittel	0
3. Beratungsfunktion	Bezüglich der Einführung der Kindersicherung bietet die Software keine Hilfestellung	Niedrig	0
4. Deinstallationsschutz	Die Software bietet zwar einen Passwortschutz an, jedoch ist dieser optional und es wird **NICHT** darauf hingewiesen, dass ein Passwort gesetzt werden sollte. Ergo wird bei einer Standardinstallation kein Passwort gesetzt, weshalb keine Punkte vergeben werden.	Hoch	0
5. Downloadblocker	Bitdefender Internet Security 2018 bietet keine Option, Downloads im Allgemeinen zu unterbinden.	Mittel	0
6. Einrichtungsassistent	Die Kindersicherung bietet während der Erstellung überhaupt keine Hilfestellung bezüglich der Einrichtung an. Es kann zwar ein Kinderaccount eingerichtet werden, jedoch wird in keiner Weise erklärt, welche Funktionalitäten wichtig sind und wie die Oberfläche zu bedienen ist. Insgesamt wirkt die Weboberfläche unausgereift und kompliziert.	Mittel	0
7. Eingeschränkte Benutzerkonten	Bitdefender Internet Security 2018 kann keine Benutzerkonten direkt anlegen und weist auch nicht darauf hin, dass eingeschränkte Benutzerkonten verwendet werden sollen.	Hoch	0

Kriterium	Beschreibung des Bewertungskriteriums	Kritikalität	Punkte
8. Installation	Die Installation ist äußerst einfach durchführbar, liefert jedoch keine Hinweise zum Kinderschutz. Zudem wirkt die GUI unübersichtlich und die Kindersicherungsfunktionalität (genannt „Elternberater“) ist schwer auffindbar.	Niedrig	0,75
9. Kategoriefilter Web	Bitdefender Internet Security 2018 bietet verschiedenste Kategoriefilter an, welche individuell an- und abwählbar sind. Zudem können für jeden Kinderaccount eigene Filter festgelegt werden.	Hoch	1
10. Kategoriefilter Anwendungen	Ein kategorischer Anwendungsfilter existiert nicht. Es können nur Anwendungen blockiert werden, die einmal ausgeführt wurden.	Hoch	0
11. Laufwerke blockieren	Die Software kann keine Laufwerke blockieren.	Niedrig	0
12. Loggingfunktion	Bitdefender Internet Security 2018 bietet diverse Funktionalitäten im Bereich des Loggings. Hierbei können zum Beispiel versuchte Aufrufe von blockierten Websites und Apps als Bericht direkt per E-Mail an das Elternteil weitergeleitet werden.	Hoch	1
13. Portblocker	Über die integrierte Firewall-Funktion lassen sich spezifische Ports blockieren.	Mittel	1
14. Prozessschutz	Der Prozess „bdparentalservice.exe“, welcher für die Kindersicherung zuständig ist, lässt sich beenden, wodurch der Schutz ausgehebelt werden kann.	Hoch	0
15. Soziale Netzwerke	Die Anwendung bietet eine Facebook-App an, welche mit dem Facebook-Account des Kindes verbunden werden kann, wodurch eine Überwachung dieses sozialen Netzwerkes möglich wird.	Mittel	1

Kriterium	Beschreibung des Bewertungskriteriums	Kritikalität	Punkte
16. Spamfilter für Maildienste	Eine Erkennungsfunktion von Spam ist durch die Anwendung gegeben.	Niedrig	1
17. Sperren von Anwendungen	Die Software erlaubt es spezifische Anwendungen über die Weboberfläche zu blockieren.	Hoch	1
18. Sperren von Websites	Spezifische Websites können entweder auf eine Whitelist oder Blacklist gesetzt werden.	Hoch	1
19. Suchmaschine	Bitdefender Internet Security 2018 bietet weder eine Safe-Search Funktion noch integrierte eine kindergerechte Suchmaschine an	Mittel	0
20. USB Schnittstellen blockieren	Die Software kann keine USB Schnittstellen blockieren.	Niedrig	0
21. Verwaltung im Web	Die Verwaltung von Bitdefender Internet Security 2018 erfolgt über einen Login in die Weboberfläche.	Mittel	1
22. Zeitbeschränkung	Die Zeitbeschränkung kann für bestimmte Tage sowie darunterliegenden Zeiträumen und/oder ein Gesamtzeitguthabenkonto definiert werden. Ebenso können Tage komplett von der Zeitbeschränkung ausgenommen werden. Ein Zusatzfeature ist die sogenannte „Schlafenszeit“: Hierbei kann ein Zeitraum definiert werden, in welchen das Gerät nicht verwendet werden darf.	Hoch	1
Gesamtbewertung	**Hoch 5x3 + Mittel 4x2 + Niedrig 1,75x1 = 24,75 / 48**		

Tabelle 5.3: Ergebnis - Bitdefender Internet Security 2018 - Praxistestkatalog

Bitdefender Internet Security 2018 – Umgehungsszenarien – Windows 7 – Admin-Rechte		
Szenario	**Beschreibung**	**Bewertung**
Änderung der Systemzeit	Die Systemzeit wird bei einer Änderung automatisch wieder zurückgestellt.	Bestanden
Anonymisierender Webproxy	**Auf einen der fünf Proxy-Dienste, nämlich hide.me, konnte zugegriffen werden. Zudem wurde der Webtraffic weiterführend nicht gefiltert, weshalb ein Zugriff auf normalerweise blockierte Websites möglich war.**	**Nicht bestanden**
Bruteforce-Angriff	**Das Passwort kann öfter als 10 Mal eingegeben werden, ohne dass irgendeine Meldung an die Eltern geschieht. Der Passwortschutz ist optional und es wird auch nicht darauf hingewiesen, dass ein Passwort verwendet werden sollte.** Des Weiteren kann als Passwort „12345678“ gewählt werden, was durch eine Passwortpolicy unbedingt verhindert werden sollte.	**Nicht bestanden**
Essentielle Dateien der Kinderschutzsoftware umbenennen / löschen	Bitdefender Internet Security 2018 ermöglicht es, trotz gesetztem Passwort, **die Anwendung zu deinstallieren, ohne ein Passwort eingeben zu müssen. Des Weiteren lassen sich selbst ohne abgesicherten Modus, Dateien des „Parental Advisors“, also der Kindersicherung, löschen, was bei einem Neustart dazu führt, dass die Anwendung zwar intakt wirkt, jedoch keine Filterfunktionalität mehr gegeben ist. Ein Test im abgesicherten Modus muss auf Grund dieses Ergebnisses nicht mehr durchgeführt werden.**	**Nicht bestanden**
Keylogger	Der Wolfeye Keylogger wird zwar erkannt, **der „Bester Keylogger“ von hw-suite jedoch nicht, wodurch das Passwort des Elternmodus aufgezeichnet werden kann.**	**Nicht bestanden**
MAC-Spoofing	Das Zuweisen einer neuen MAC-Adresse ändert nichts am Filterverhalten des Parental Advisors.	Bestanden

Szenario	Beschreibung	Bewertung
Prozess beenden	**Der Parental Advisor Service (bdparentalservice.exe) lässt sich im Taskmanager ohne Weiteres beenden und somit lässt sich der gesamte Filtermechanismus umgehen.** Das Umgehungsszenario funktioniert jedoch nicht mittels des offenen Paint-Dokuments.	**Nicht bestanden.**
Portable Anwendung	• **Assault Cube: Das Spiel lässt sich ohne Weiteres ausführen und wird nur dann erkannt, wenn es bereits einmal ausgeführt wurde. Weitergehend muss das Programm dann manuell durch das Elternteil im „Parental Advisor“ blockiert werden.** • SR-Iron Browser: Der Webfilter wird durch diese portable Anwendung nicht ausgehebelt.	**Nicht bestanden.**
SafeSearch oder Kindersuchmaschine	Es konnte auf keine der drei angegebenen Suchmaschinen zugegriffen werden, da diese blockiert wurden. **Jedoch ist bei Google SafeSearch standardmäßig deaktiviert und bei Bing kann dies deaktiviert werden. Weitergehend werden bei der Eingabe eines anstößigen Suchbegriffes, darauffolgend anstößige Inhalte retourniert.**	**Nicht bestanden**
USB-Tethering	USB-Tethering hat keine Auswirkung auf die Funktionalität des Filters.	Bestanden
Wayback Machine	Die Website „web.archive.org“ wird ausnahmslos durch Bitdefender Internet Security 2018 blockiert.	Bestanden
Gesamtbewertung	**7 (63,63%) von 11 Szenarien wurden nicht bestanden.**	

Tabelle 5.4: Ergebnis - Bitdefender Internet Security 2018 - Umgehungsszenarien

5.0.2 Fazit - Bitdefender

Als Zweitplatzierter in der Vorauswahl, zeigt sich im Praxistest, dass das Programm viele Versprechen bezüglich der gegebenen Funktionalitäten geboten hat. Faktisch hat das Programm jedoch nur 24,75 von 48 Punkten im Praxistestkatalog erzielt, da viele Funktionen nicht gegeben waren. Bei den Umgehungsszenarien hat das Programm 7 von 11 Szenarien nicht bestanden. Als besonders hervorzuheben ist, dass unter dem Punkt "Anonymsierender Webproxy" ein äußerst bekannter Dienst, in diesem Falle hide.me, nicht gesperrt wurde und ein Zugriff auf normalerweise blockierte Websites möglich war.

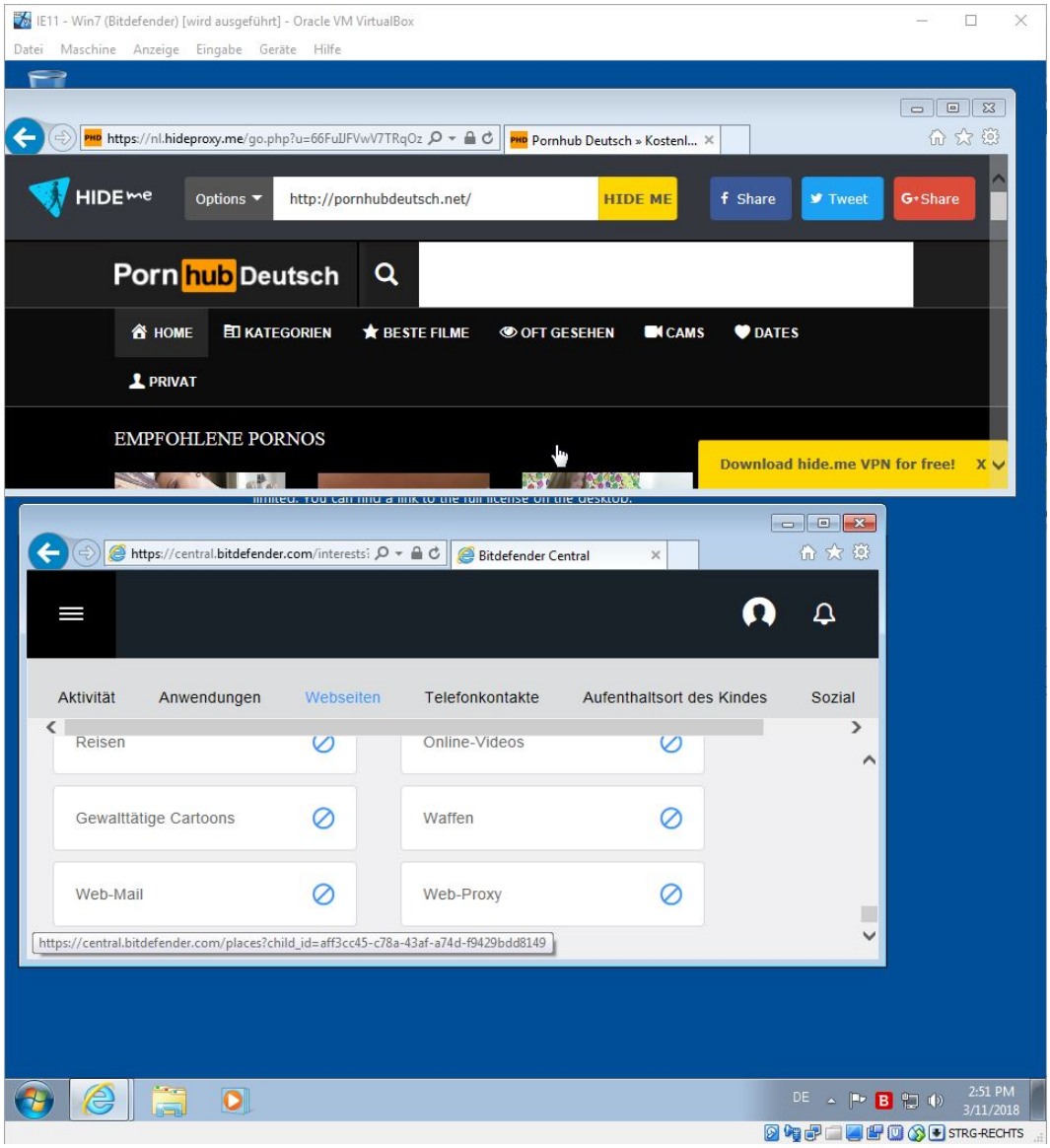

Abbildung 5.6: Ergebnis des Umgehungsszenarios "Anonymisierender Webproxy"

Außerdem könnte man sich auch hier per "Bruteforce-Angriff" einen Zugriff auf den Elternmodus verschaffen. Dies wird dadurch erleichtert, dass keine ordentliche Passwortpolicy hinterlegt ist und es mög-

lich ist ein rein aus Ziffern und aus 8 Zeichen bestehendes Passwort (z.B. "12345678") zu wählen. Interessant war zudem auch, dass unter dem Szenario "SafeSearch oder Kindersuchmaschine" alle drei alternativen Suchmaschinen, trotz standardmäßiger Freigabe im Parental Advisor von Bitdefender Internet Security 2018, blockiert waren. Jedoch war SafeSearch in der Suchmaschine "Google" standardmäßig deaktiviert und man konnte nach einem anstößigen Begriff suchen und es wurden dementsprechend auch anstößige Inhalte zurückgeliefert. Dasselbe galt für die Suchmaschine "Bing", wo SafeSearch nur deaktiviert werden musste.

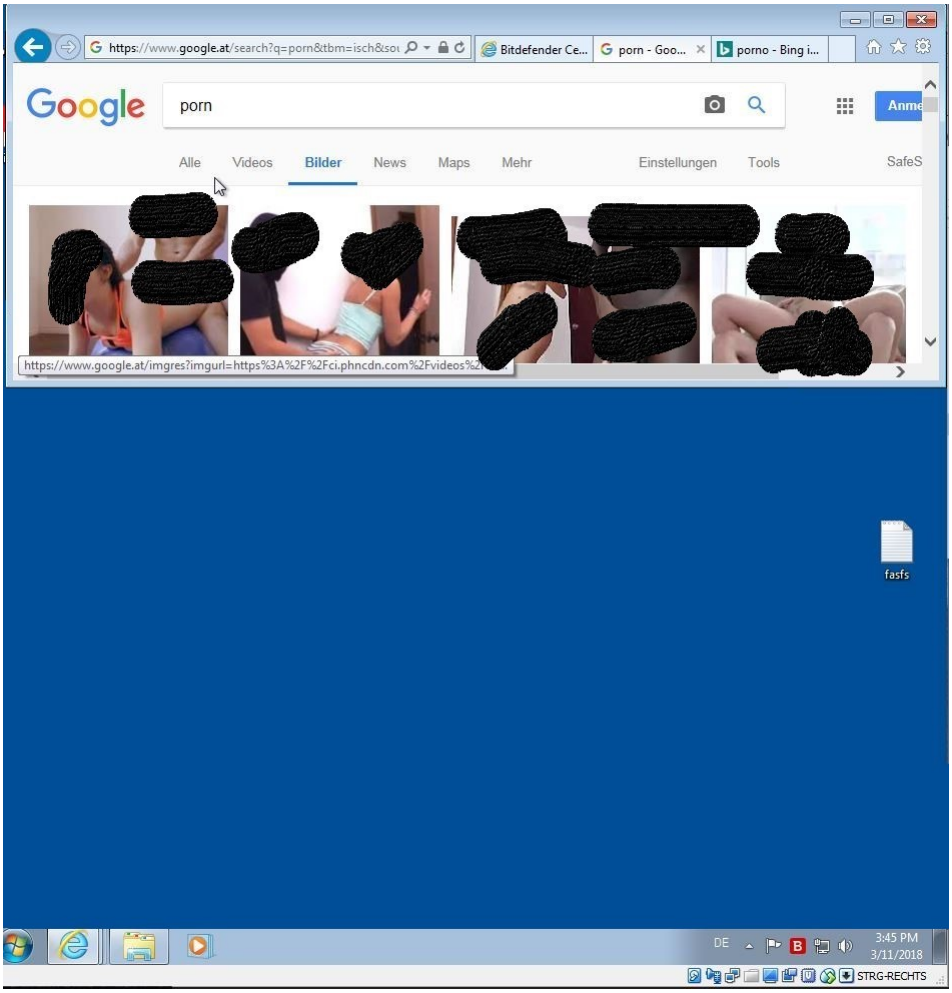

Abbildung 5.7: Ergebnis des Umgehungsszenarios "SafeSearch oder Kindersuchmaschine"

Besonders interessant war jedoch das Umgehungsszenario "Prozess beenden". Dabei stellte sich heraus, dass der Prozess "bdparentalservice.exe" keinen besonderen Schutz aufweist, wodurch jener ohne Weiteres im Benutzerkonto des Kindes beendet werden konnte. Dies hatte zur Folge, dass damit jeglicher Filterungsschutz umgangen werden konnte.

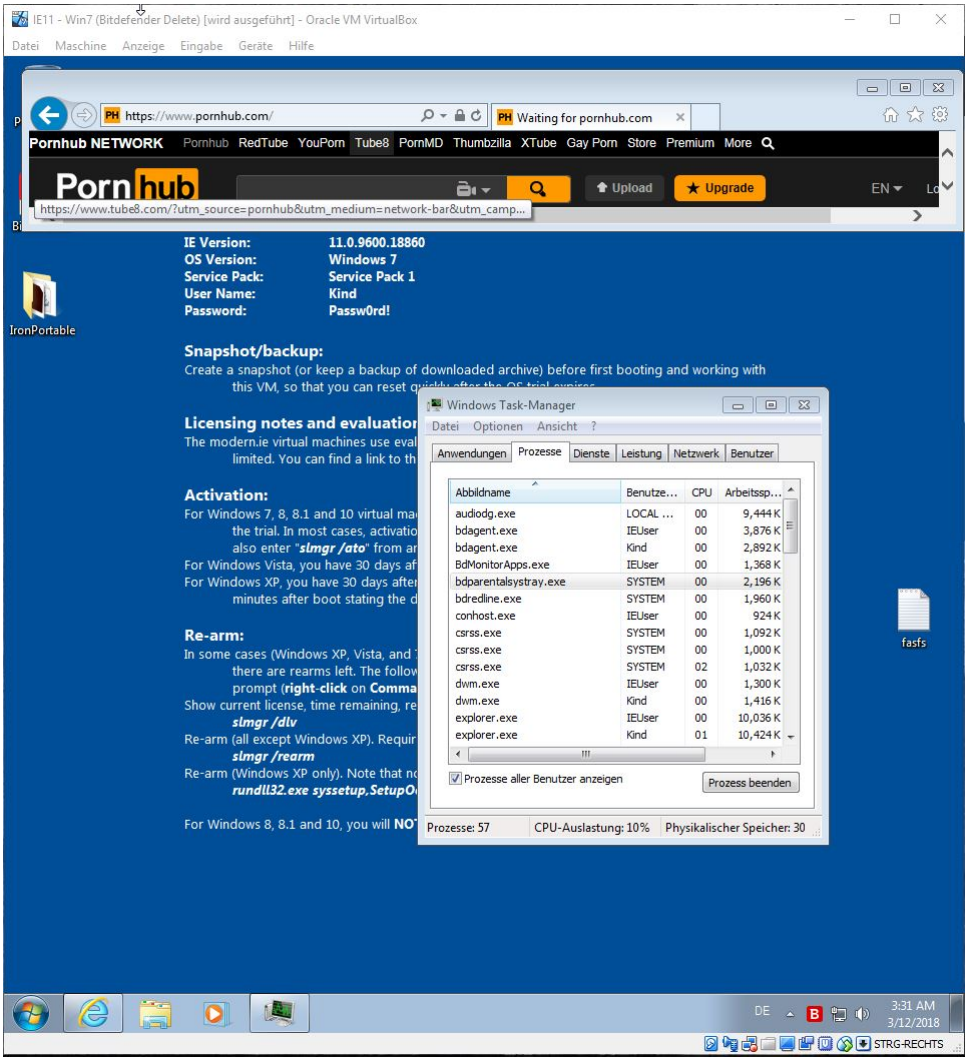

Abbildung 5.8: Ergebnis des Umgehungsszenarios "Prozess beenden"

Bullguard Internet Security 2018 18.0.347.4 – Praxistestkatalog – Windows 7			
Kriterium	**Beschreibung des Bewertungskriteriums**	**Kritikalität**	**Punkte**
1. Accounts	Mittels Bullguard Internet Security 2018 können mehrere Benutzerprofile für unterschiedliche Altersgruppen der Kinder angelegt werden.	Mittel	1
2. Ausführung von spezifischen Dateitypen blockieren	Spezifische Dateitypen können nicht blockiert werden.	Mittel	0
3. Beratungsfunktion	Die Anwendung bietet keine Beratungsfunktion für Eltern an und erläutert auch nicht, wie man am besten die Einführung einer Kindersicherung bespricht.	Niedrig	0
4. Deinstallationsschutz	Das Programm wird nicht durch ein Passwort oder eine Multifaktorauthentifizierung vor einer Deinstallation geschützt.	Hoch	0
5. Downloadblocker	Die Software bietet keine Funktionalität an, um Downloads zu blockieren.	Mittel	0
6. Einrichtungsassistent	Die Anwendung bietet ein ausführliches Web-Wiki an in welchem erläutert wird, wie die Kindersicherung einzurichten ist.	Mittel	0,75
7. Eingeschränkte Benutzerkonten	Bullguard Internet Security 2018 verlinkt zwar auf die Benutzerkonten von Windows, weist jedoch nicht darauf hin, dass kein Admin-Konto für Kinder verwendet sollte.	Hoch	0
8. Installation	Die Installation lässt sich mittels wenigen Klicks durchführen und ist äußerst einfach.	Niedrig	0,75
9. Kategoriefilter Web	Es werden unterschiedlichste Filterkategorien im Bereich Web angeboten. Mittels vordefinierter Profile können allgemeine Beschränkungen festgelegt und darauffolgend individuell weitere Kategorien blockiert oder freigegeben werden.	Hoch	1

Kriterium	Beschreibung des Bewertungskriteriums	Kritikalität	Punkte
10. Kategoriefilter Anwendungen	Ein Filter für Anwendungen existiert zwar, jedoch können Anwendungen nicht nach Kategorien blockiert, sondern müssen explizit ausgewählt und gesperrt werden. Eine Vorfilterung nach Kategorien ist somit nicht möglich.	Hoch	0
11. Laufwerke blockieren	Laufwerke können über Bullguard Internet Security 2018 nicht blockiert werden.	Niedrig	0
12. Loggingfunktion	Über die „Bericht“-Funktion kann ein umfassendes Logging abgerufen werden. Dabei werden Informationen wie die besuchten Websites, verwendeten Anwendungen und die Anmeldeversuche in den Elternmodus geloggt.	Hoch	0,75
13. Portblocker	Bullguard Internet Security 2018 arbeitet mit der integrierten Windowsfirewall, welche es ermöglicht Ports zu blockieren.	Mittel	1
14. Prozessschutz	Die essentiellen Prozesse der Anwendung werden vor einer Beendigung im Taskmanager geschützt.	Hoch	1
15. Soziale Netzwerke	Soziale Netzwerke können zwar über den Webfilter blockiert werden, jedoch ist es nicht möglich ein Online-Konto des Kindes über die Software zu beobachten.	Mittel	0
16. Spamfilter für Maildienste	Ein Spamfilter ist nicht in die Anwendung integriert.	Niedrig	0
17. Sperren von Anwendungen	Bullguard Internet Security 2018 erlaubt ein Sperren von spezifischen Anwendungen, bietet jedoch keinen kategorischen Anwendungsfilter.	Hoch	1
18. Sperren von Websites	Ein Sperren bzw. ein Erlauben von spezifischen Websites ist möglich.	Hoch	1

Kriterium	Beschreibung des Bewertungskriteriums	Kritikalität	Punkte
19. Suchmaschine	Im Profil des Kindes wird SafeSearch für bekannte Suchmaschinen wie Google, Yahoo und Bing aktiviert.	Mittel	0,5
20. USB Schnittstellen blockieren	Ein Blockieren von USB-Schnittstellen ist über Bullguard Internet Security 2018 nicht möglich.	Niedrig	0
21. Verwaltung im Web	Ein Verwalten der Software ist nur lokal am Rechner, auf welchem das Programm installiert wurde, möglich.	Mittel	0
22. Zeitbeschränkung	Ein feingranularer Zeitplan lässt sich für jeden Wochentag und eine bestimmte Uhrzeit einstellen.	Hoch	1
Gesamtbewertung	**Hoch 5,75x3 + Mittel 3,25x2 + Niedrig 0,75x1 = 24,5/48**		

Tabelle 5.5: Ergebnis - Bullguard Internet Security 2018 - Praxistestkatalog

Bullguard Internet Security 2018 – Umgehungsszenarien – Windows 7 – Admin-Konto		
Szenario	**Beschreibung**	**Bewertung**
Änderung der Systemzeit	Die Systemzeit wird automatisch auf das korrekte Datum sowie die korrekte Zeit angepasst.	Bestanden
Anonymisierender Webproxy	Alle Webproxyseiten wurden durch Bullguard Internet Security 2018 standardmäßig blockiert.	Bestanden
Bruteforce-Angriff	Ein Zugriffsversuch auf den Elternmodus wird über die Berichtefunktion mitgeloggt, j**edoch wird keine Warnung per Mail oder SMS an die Eltern versendet und ein Login ist auch nach 10 Versuchen noch möglich.**	**Nicht bestanden**
Essentielle Dateien der Kinderschutzsoftware umbenennen / löschen	Über das Benutzerkonto des Kindes lassen sich keine relevanten Daten der Kinderschutzanwendung löschen. **Im abgesicherten Modus lassen sich die Dateien jedoch ohne Weiteres löschen.**	**Nicht bestanden**
Keylogger	Der Wolfeye-Keylogger wird von Bullguard Internet Security 2018 direkt erkannt und gelöscht. **Jedoch lässt sich der „Bester Keylogger“ von hw-suite ohne Weiteres ausführen und installieren. Dabei können die Benutzerdaten zum Elternkonto ausgelesen werden.**	**Nicht bestanden**
MAC-Spoofing	Trotz dem Zuweisen einer neuen MAC-Adresse, ist der Webfilter weitergehend aktiv.	Bestanden
Prozess beenden	Die Prozesse der Anwendung lassen sich weder über den Taskmanager, noch über das offene Paint-Dokument sowie den eingeleiteten Herunterfahrprozess, beenden.	Bestanden
Portable Anwendung	• **Assault Cube: Lässt sich ohne Weiteres ausführen und wird von der Kindersicherung nicht blockiert.** • SR-Iron Browser: Der Webfilter greift weitergehend auch in dem alternativen Browser.	**Nicht bestanden**
SafeSearch oder Kindersuchmaschine	**Bei allen drei alternativen Suchmaschinen musste nur SafeSearch deaktiviert werden, damit man nach anstößigen Inhalten suchen konnte und entsprechende Ergebnisse angezeigt bekam.**	**Nicht bestanden**

Szenario	Beschreibung	Bewertung
USB-Tethering	Trotz USB-Tethering ist der Websitefilter weitergehend wirksam.	Bestanden
Wayback Machine	**Über web.archive.org ist auf Snapshots von normalerweise gesperrten Seiten ein Zugriff möglich.**	**Nicht bestanden**
Gesamtbewertung	**6 (54,55%) von 11 Szenarien wurden nicht bestanden.**	

Tabelle 5.6: Ergebnis - Bullguard Internet Security 2018 - Umgehungsszenarien

5.0.3 Fazit - Bullguard

Bullguard Internet Security 2018 erreichte im Praxistestkatalog 24,5 von 48 Punkten. Ebenso waren bei den Umgehungszenarien 6 von 11 erfolgreich. Hier zeigt sich hauptsächlich dasselbe Bild wie bei den vorhergehenden Kindersicherungsprogrammen. Faktisch liegt folgendes vor:

- Bei einem Bruteforce-Angriff bzw. bei vielen fehlgeschlagenen Anmeldeversuchen, werden die Eltern nicht aktiv per Mail oder SMS informiert.
- Die Anwendung lässt sich im abgesicherten Modus ohne Weiteres löschen.
- Es lässt sich ein Keylogger, in diesem Falle auch der "Bester Keylogger" von hw-suite, installieren, welcher nicht blockiert wird.
- Die Ausführung des portablen Spiels "Assault Cube" wird nicht blockiert.
- Alternative Suchmaschinen werden nicht blockiert und SafeSearch kann einfach deaktiviert werden.
- Mittels web.archive.org ist ein Zugriff auf Snapshots von normalerweise blockierten Websites ohne Weiteres möglich.

Nachfolgend finden sich auszugsweise Screenshots aus den erfolgreichen Umgehungsszenarien.

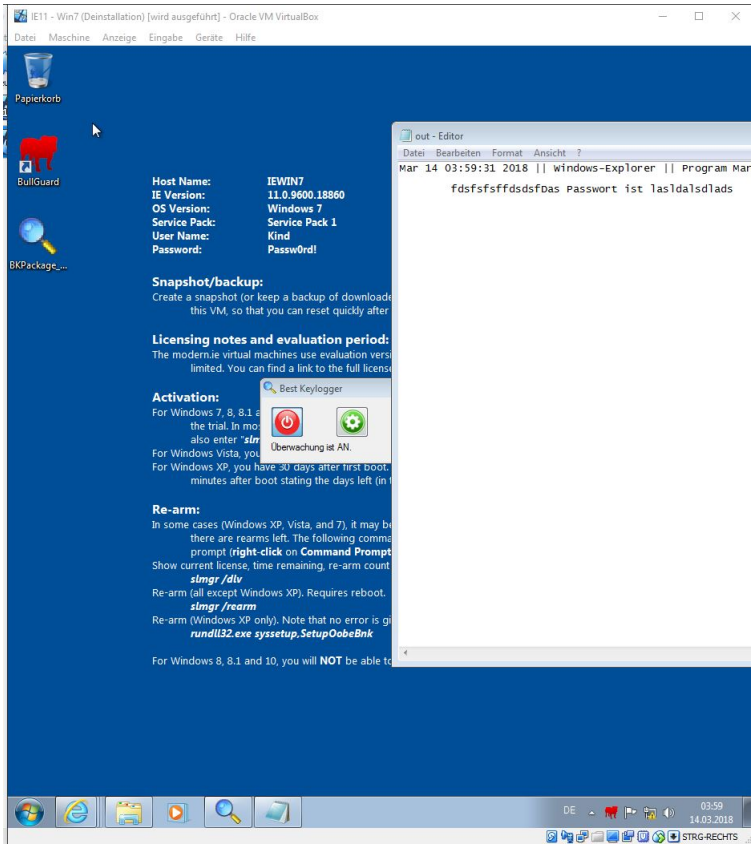

Abbildung 5.9: Ergebnis des Umgehungsszenarios "Keylogger"

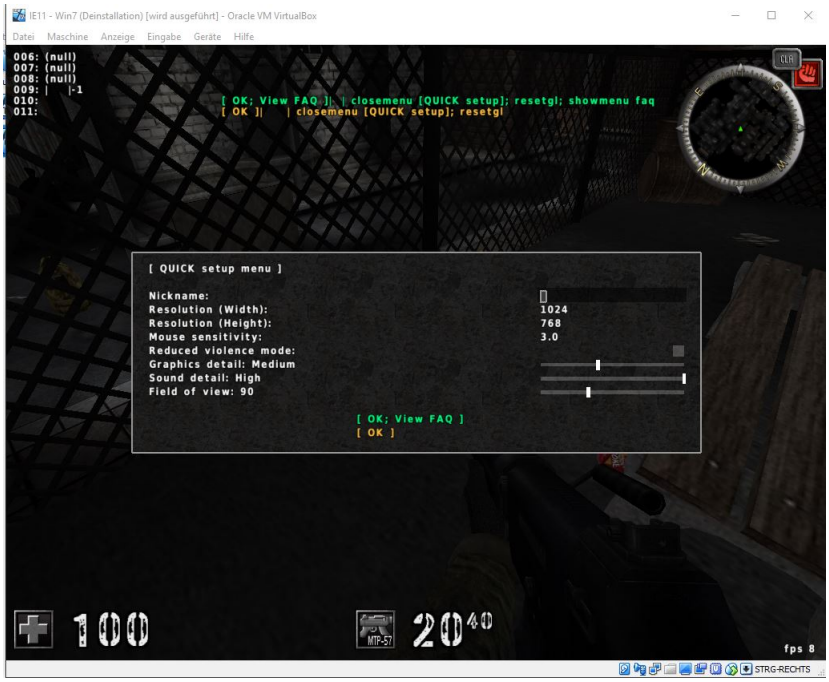

Abbildung 5.10: Ergebnis des Umgehungsszenarios "Portable Anwendungen"

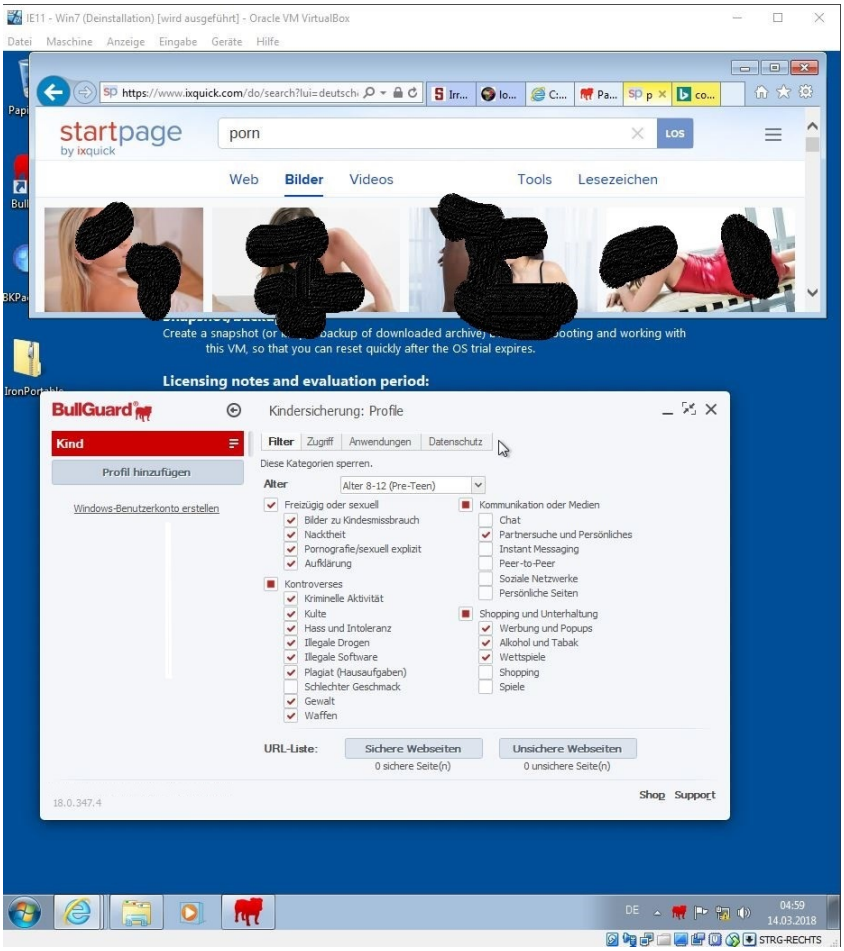

Abbildung 5.11: Ergebnis des Umgehungsszenarios "Safe Search"

SecureTeen Parental Control 1.2 – Praxistestkatalog – Windows 10			
Kriterium	**Beschreibung des Bewertungskriteriums**	**Kritikalität**	**Punkte**
1. Accounts	Secure Teen Parental Control bietet die Option an, entweder jeweils separate Benutzerkonten mit unterschiedlichen oder alle Konten mit den gleichen Filtereinstellungen zu versehen. Ebenso lassen sich unterschiedliche Filter für unterschiedliche Altersgruppen definieren.	Mittel	1
2. Ausführung von spezifischen Dateitypen blockieren	Die Software kann keine spezifischen Dateitypen blockieren.	Mittel	0
3. Beratungsfunktion	Die Software gibt Eltern keine Hilfestellung bei der Installation einer Kinderschutzsoftware.	Niedrig	0
4. Deinstallationsschutz	Die Deinstallation der Software erfolgt über eine herunterladbare .bat Datei, welche nach einem korrekten Benutzernamen und Passwort fragt, bevor die Deinstallation der Anwendung eingeleitet wird. Zudem muss dies mit Administratorrechten geschehen.	Hoch	1
5. Downloadblocker	Es können keine Downloads mittels SecureTeen Parental Control blockiert werden.	Mittel	0
6. Einrichtungsassistent	Der Einrichtungsassistent, welcher während der Installation direkt aufgerufen wird, enthält alle wichtigen Einstellungen und erläutert diese im Detail.	Mittel	1
7. Eingeschränkte Benutzerkonten	Es können direkt über die GUI der Anwendung entsprechende Standardbenutzerkonten angelegt und mit angepassten Profilen der Kinder verbunden werden	Hoch	1
8. Installation	Direkt während der Installation von SecureTeen Parental Control wird ein Einrichtungsassistent aufgerufen, welcher durch alle relevanten Einstellungen für den Kinderschutz führt und die vorhandenen Optionen im Detail erklärt. Die Installation ist einfach durchführbar.	Niedrig	0,75

Kriterium	Beschreibung des Bewertungskriteriums	Kritikalität	Punkte
9. Kategoriefilter Web	SecureTeen Parental Control bietet verschiedenste kategorische Webfilter an, welche individuell für jeden Kinderaccount gesetzt werden können. **Unverständlich hierbei ist jedoch, warum als standardmäßigen Filter nur 6 Kategorien blockiert werden, wobei beispielsweise die Kategorien Drogen, Alkohol, Hacking und Obszönität explizit erlaubt wurden?**	Hoch	1
10. Kategoriefilter Anwendungen	Die Software besitzt keinen Kategoriefilter für Anwendungen.	Hoch	0
11. Laufwerke blockieren	Die Software kann keine Laufwerke blockieren.	Niedrig	0
12. Loggingfunktion	Über die Reports-Funktion wird angezeigt welche Websites blockiert oder erlaubt wurden. Zudem lassen sich die Facebook-Aktivitäten und Nachrichten überwachen. Eine Warnung per SMS oder Email bei verdächtigen Aktivitäten wurde nicht implementiert.	Hoch	0,75
13. Portblocker	Ports können nicht über die Anwendung blockiert werden.	Mittel	0
14. Prozessschutz	Einer der beiden Prozesse, welche während der Ausführung der Anwendung erzeugt werden, lässt sich zwar beenden, jedoch hat dies keinen Einfluss auf die Filterfunktion der Anwendung.	Hoch	1
15. Soziale Netzwerke	SecureTeen Parental Control bietet die Überwachung des Facebookprofils des Kindes an, jedoch muss jenes über die Eingabe der entsprechenden Benutzerkontodaten mit der Anwendung verbunden werden.	Mittel	1

Kriterium	Beschreibung des Bewertungskriteriums	Kritikalität	Punkte
16. Spamfilter für Maildienste	Die Software hat keinen Spamfilter integriert.	Niedrig	0
17. Sperren von Anwendungen	Die Software kann keine spezifischen Anwendungen blockieren.	Hoch	0
18. Sperren von Websites	Spezifische Websites können explizit erlaubt bzw. gesperrt werden.	Hoch	1
19. Suchmaschine	SecureTeen Parental Control bietet keine Optionen bezüglich einer kindgerechten Suchmaschine oder zur Aktivierung von SafeSearch an.	Mittel	0
20. USB Schnittstellen blockieren	Die Software kann keine USB Schnittstellen blockieren.	Niedrig	0
21. Verwaltung im Web	SecureTeen Parental Control wird auf den einzelnen Endgeräten installiert, mit einem Benutzerkonto verbunden und kann dann nur über dieses Benutzerkonto über eine Weboberfläche gesammelt gesteuert werden.	Mittel	1
22. Zeitbeschränkung	Die Anwendung bietet verschiedene Methodiken zur Steuerung der Zeitbeschränkung. Zum Einen können spezifische Zeiten an bestimmten Wochentagen freigegeben werden, zum Anderen lassen sich auch erweiterte Regeln(in Bezug auf die Blockierung von Anwendungen oder Websites während den Lern- und Schulzeiten) festlegen	Hoch	1
Gesamtbewertung	**Hoch 6,75x3 + Mittel 4x2 + Niedrig 0,75x1 = 29 / 48**		

Tabelle 5.7: Ergebnis - Infoweise SecureTeen Parental Control - Praxistestkatalog

SecureTeen Parental Control – Umgehungsszenarien – Windows 10 – Konto ohne Admin-Rechte		
Szenario	**Beschreibung**	**Bewertung**
Änderung der Systemzeit	Eine Änderung der Systemzeit ist nicht möglich. Der Zugriff auf diese Funktionalität ist nur mittels Admin-Rechten durchführbar.	Bestanden
Anonymisierender Webproxy	Ein Verbindungsaufbau zu jedem der anonymisierenden Webproxies wird durch die Filterfunktion von SecureTeen Parental Control unterbunden.	Bestanden.
Bruteforce-Angriff	**Nach 10 fehlgeschlagenen Anmeldeversuchen, passiert nichts. Eine Funktionalität zur Warnung bei vielen fehlgeschlagenen Loginversuchen per Mail oder SMS, wurde nicht implementiert.**	**Nicht bestanden**
Essentielle Dateien der Kinderschutzsoftware umbenennen / löschen	Im Standardbenutzerkonto lässt sich die Datei mspdbsrv.exe, welche den Namen „Program Database (32 Bit)“ im Taskmanager besitzt und durch die Firma „Infoweise“, also dem Hersteller von SecureTeen Parental Control signiert wurde, nach Beendigung des Prozesses löschen. Dies hatte jedoch keinen Einfluss auf die Funktionalität der Software und da zum Beenden des Prozesses „System Device Enumeration Control“ die Berechtigungen fehlen, wurde in den abgesicherten Modus gewechselt. Auch hier war es nicht möglich, ohne Admin-Rechte die Datei zu löschen. **Aber: Der abgesicherte Modus mit Netzwerkzugriff ermöglicht es, auf alle normalerweise blockierten Websites zuzugreifen, da die Kindersicherung nicht mitgestartet wird.**	**Nicht bestanden**
Keylogger	Für den Test wurde der Windows 10 Defender deaktiviert, da die Kindersicherung selbst den Keylogger blockieren muss. **Jedoch wird weder der „Wolfeye-Keylogger“ noch der „Bester Keylogger“ erkannt und blockiert. Somit kann das Passwort eines Elternteils bei Eingabe mitgeschnitten werden.**	**Nicht bestanden**
MAC-Spoofing	Der Zugriff auf die Netzwerkeinstellungen ist nur mittels Administratorrechten möglich, somit kann die MAC-Adresse in diesem Falle nicht geändert werden.	Bestanden

Szenario	Beschreibung	
Prozess beenden	Der Hauptprozess („System Device Enumeration Control“) lässt sich weder über den Taskmanager noch über ein offenes Paint-Dokument sowie den eingeleiteten Herunterfahrprozess, beenden. Faktisch bleibt der Schutz durch die Kindersicherung erhalten.	Bestanden
Portable Anwendung	• **Assault Cube: Da das Programm keinen Anwendungsfilter besitzt, lässt sich Assault Cube ohne Weiteres ausführen.** • SR-Iron Browser: Der Webfilter ist auch weiterführend in dem alternativen Browser aktiv.	**Nicht bestanden**
SafeSearch oder Kindersuchmaschine	**In den Suchmaschinen qwant und ixquick muss nur SafeSearch deaktiviert werden, um anstößige Inhalte zu finden.** Bei duckduckgo kann man SafeSearch zwar deaktivieren, jedoch wird die Bildersuche darauffolgend entsprechend gefiltert.	**Nicht bestanden**
USB-Tethering	Die Verwendung von USB-Tethering beeinflusst die Funktionalität des Webfilters nicht.	Bestanden
Wayback Machine	Der Zugriff auf web.archive.org wird durch die Anwendung blockiert.	Bestanden
Gesamtbewertung	**5 (45,45%) von 11 Szenarien wurden nicht bestanden.**	

Tabelle 5.8: Ergebnis - Infoweise SecureTeen Parental Control - Umgehungsszenarien

5.0.4 Fazit - Infoweise SecureTeen Parental Control

Der Viertplatzierte der Vorauswahl hat eine Gesamtbewertung mit 29 von 48 Punkten erreicht und 5 von 11 Umgehungsszenarien nicht bestanden. Zusammengefasst zeigt sich auch hier, dass:

- Bruteforce-Angriffe auf den Elternmodus des Programmes ohne Weiteres möglich sind.
- das Löschen oder Umbenennen von relevanten Dateien im abgesicherten Modus zwar nicht möglich war, jedoch die Kindersicherung in diesem Modus nicht mitgestartet wird und somit ein unregulierter Zugriff auf das Web möglich ist.
- keiner der beiden Keylogger durch die Kindersicherung erkannt und blockiert wurde.
- das portable 18+ Spiel "Assault Cube" ohne Weiteres ausführbar war.
- bei zwei der drei alternativen Suchmaschinen nach anstößigen Inhalten gesucht werden konnte und entsprechende Inhalte auch zurückgeliefert wurden.

Weiterführend finden sich auszugsweise Screenshots aus den Umgehungsszenarien:

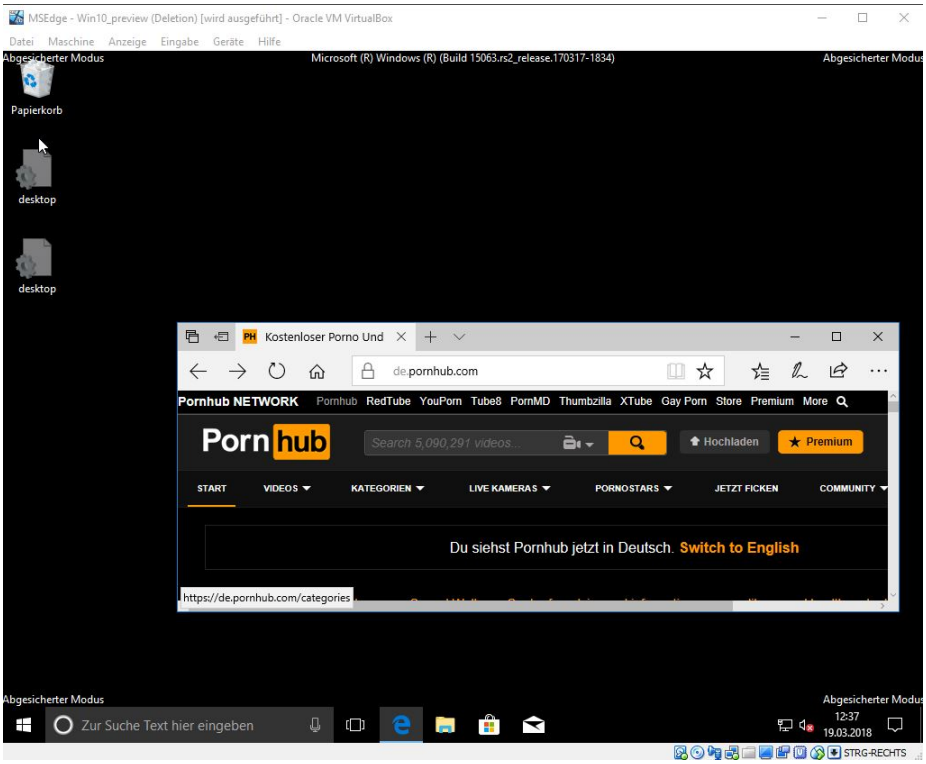

Abbildung 5.12: Ergebnis des Umgehungsszenarios "Essentielle Dateien der Kinderschutzsoftware umbenennen/löschen"

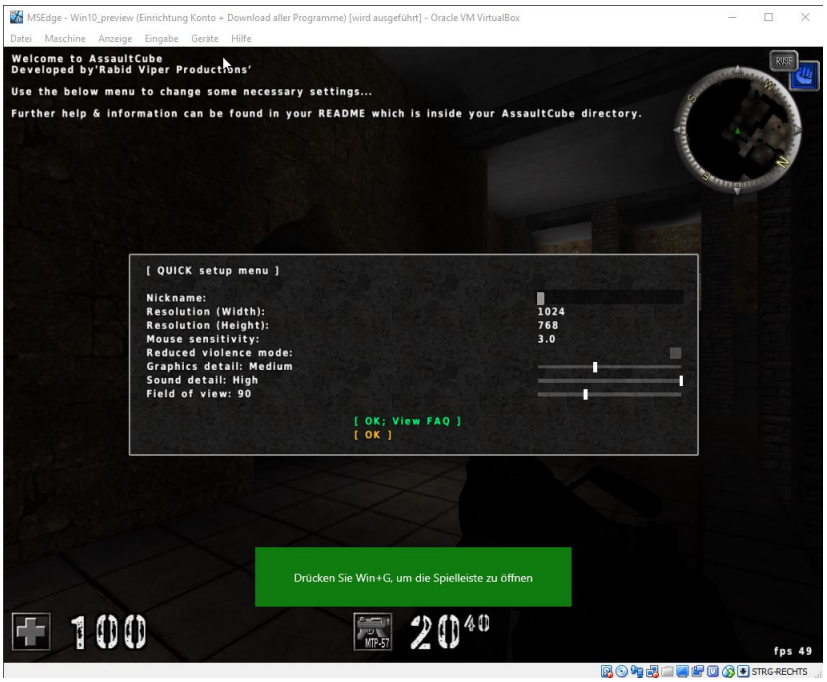

Abbildung 5.13: Ergebnis des Umgehungsszenarios "Portable Anwendungen"

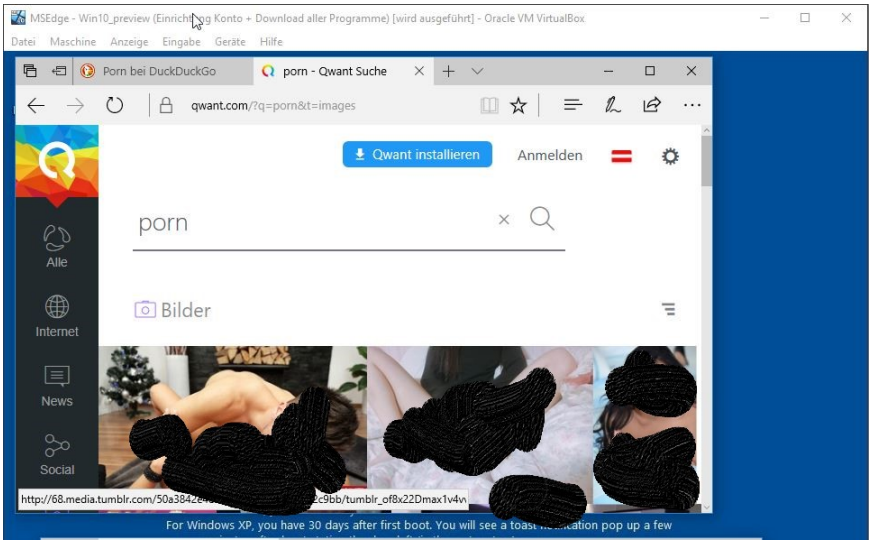

Abbildung 5.14: Ergebnis des Umgehungsszenarios "Safe Search"

G Data Multi Device (Internet) Security 25.4.0.3 – Praxistestkatalog – Windows 7			
Kriterium	**Beschreibung des Bewertungskriteriums**	**Kritikalität**	**Punkte**
1. Accounts	Es können unterschiedliche Filter für unterschiedliche Benutzerkonten am Rechner definiert werden.	Mittel	1
2. Ausführung von spezifischen Dateitypen blockieren	Die Software kann keine spezifischen Dateitypen blockieren.	Mittel	0
3. Beratungsfunktion	Bei G Data Internet Security wird keine Beratung bezüglich der Installation einer Kindersicherung gegeben.	Niedrig	0
4. Deinstallationsschutz	Da Benutzerkonten für Kinder bzw. Jugendliche über die GUI von G Data Internet Security angelegt werden können und es sich dabei um eingeschränkte Konten handelt, lässt sich die Anwendung nicht deinstallieren, da die Admin-Rechte fehlen. Somit ist das Programm vor Deinstallation geschützt.	Hoch	1
5. Downloadblocker	Die Software bietet keine Funktionalität Downloads zu blockieren.	Mittel	0
6. Einrichtungsassistent	Über den Button „?“ wird man zu einem Web-Wiki weitergeleitet, welches die Funktionalitäten der Kindersicherung im Detail erläutert.	Mittel	0,75
7. Eingeschränkte Benutzerkonten	Über die GUI von G Data Internet Security lässt sich direkt ein neues, eingeschränktes Benutzerkonto für ein Kind anlegen.	Hoch	1
8. Installation	Die Installation ist nicht komplex und einfach durchführbar. Der Ort der Installation lässt sich ebenso auswählen und anpassen und zudem wird auf die Kinderschutzfunktionalität hingewiesen.	Niedrig	1

Kriterium	Beschreibung des Bewertungskriteriums	Kritikalität	Punkte
9. Kategoriefilter Web	Jedes Benutzerkonto kann mit unterschiedlichen kategorischen Filtereinstellungen versehen und dementsprechend an das Alter des Kindes angepasst werden.	Hoch	1
10. Kategoriefilter Anwendungen	G Data Internet Security bietet keinen Filter für Anwendungen an.	Hoch	0
11. Laufwerke blockieren	Die Software kann keine Laufwerke blockieren.	Niedrig	0
12. Loggingfunktion	Über die Protokollfunktion findet sich ein simplistisches Logging über die Benutzer, welche versucht haben blockierte Webinhalte aufzurufen.	Hoch	0,75
13. Portblocker	G Data Internet Security bietet die Funktionalität Ports über die integrierte Firewall zu blockieren.	Mittel	1
14. Prozessschutz	Alle Prozesse von G Data Internet Security werden vor einer Beendigung im Task-Manager geschützt.	Hoch	1
15. Soziale Netzwerke	Die Software bietet keine spezifischen Funktionalitäten hinsichtlich sozialer Netzwerke.	Mittel	0
16. Spamfilter für Maildienste	E-Mails werden sowohl auf Malware, als auch auf Spam überprüft.	Niedrig	1
17. Sperren von Anwendungen	Die Software kann keine spezifischen Anwendungen blockieren, da kein Anwendungsfilter in G Data Internet Security implementiert wurde.	Hoch	0
18. Sperren von Websites	Websites können entweder explizit freigegeben oder blockiert werden.	Hoch	1

Kriterium	Beschreibung des Bewertungskriteriums	Kritikalität	Punkte
19. Suchmaschine	Über den Menüpunkt „Erlaubte Inhalte“ lässt sich eine Whitelist definieren, welche nur explizit definierte Websites zulässt. Hierbei ist die Suchmaschine „FragFINN“ standardmäßig auswählbar.	Mittel	1
20. USB Schnittstellen blockieren	Wechselmedien können zwar auf Malware automatisch untersucht werden, jedoch bietet die Anwendung keine Funktionalität um USB-Schnittstellen zu sperren.	Niedrig	0
21. Verwaltung im Web	Die Verwaltung der Software erfolgt lokal über die GUI.	Mittel	0
22. Zeitbeschränkung	G Data Internet Security bietet entweder ein spezifisches Zeitguthaben, welches beliebig verbraucht werden kann oder die alternative ist das Beschränken der Nutzung des Internets oder des Computers an definierbaren Wochentagen und Uhrzeiten.	Hoch	1
Gesamtbewertung	**Hoch 6,75x3 + Mittel 3,75x2 + Niedrig 2x1 = 29,75 / 48**		

Tabelle 5.9: Ergebnis - G Data Multi Device (Internet) Security - Praxistestkatalog

G Data Multi Device (Internet) Security – Umgehungsszenarien – Windows 7 – Konto ohne Admin-Rechte		
Szenario	**Beschreibung**	**Bewertung**
Änderung der Systemzeit	Die Systemzeit kann ohne Admin-Rechte nicht angepasst werden.	Bestanden
Anonymisierender Webproxy	**Der Zugriff auf alle fünf Dienste wurde nicht durch den Webfilter blockiert. Weitergehend war es möglich mit drei von fünf Webproxies, konkret „hide.me“, „hidester.com“ und „proxysite.com“ den Filter zu umgehen.**	**Nicht bestanden**
Bruteforce-Angriff	Ein Bruteforceangriff auf die Anwendung selbst kann in diesem Falle nicht geschehen, da kein Passwort abgefragt wird, sondern ob der Benutzer ein Administrator ist. Wenn der Nutzer kein Administrator ist, kann er die Kindersicherung nicht deaktivieren. Da mit G Data Internet Security eingerichtete Benutzerkonten automatisch eingeschränkt sind, gilt das Szenario als bestanden.	Bestanden
Essentielle Dateien der Kinderschutzsoftware umbenennen / löschen	Die Programmdateien lassen sich im eingeschränkten Benutzerkonto des Kindes weder umbenennen noch löschen. **Im abgesicherten Modus lässt sich die Anwendung zwar nicht deinstallieren, da Admin-Rechte erforderlich sind, jedoch wird die Anwendung nicht gestartet, wodurch ein Zugriff auf das Web ohne Filterung über das Benutzerkonto des Kindes möglich ist.**	**Nicht bestanden**
Keylogger	Der „Wolfeye Keylogger“ wird als Keylogger erkannt und durch G Data Internet Security blockiert. Der „Bester Keylogger“ von HW-Suite wird nicht erkannt und lässt sich ohne Weiteres ausführen. Da es jedoch nötig ist sich über ein Administratorkonto anzumelden (das heißt man muss das Benutzerkonto wechseln) um die Einstellung der Kindersicherung zu ändern, ist der Keylogger für den Kinderaccount nutzlos. Somit gilt dieses Szenario als bestanden.	Bestanden
MAC-Spoofing	Zur Änderung der MAC Adresse sind Admin-Rechte nötig. Somit gilt das Szenario als bestanden.	Bestanden

Szenario	Beschreibung	
Prozess beenden	Die Anwendung kann weder über den Task-Manager noch über ein offenes Paint-Dokument und dem eingeleiteten Herunterfahrprozess zum Beenden gezwungen werden	Bestanden
Portable Anwendung	• **Assault Cube: Da kein Anwendungsfilter implementiert wurde, ist eine Ausführung der Anwendung ohne Weiteres möglich.** • SR-Iron Browser: Der Webfilter greift weiterhin in dem alternativen Browser.	**Nicht bestanden**
SafeSearch oder Kindersuchmaschine	**Nach der Deaktivierung von SafeSearch in allen drei Suchmaschinen, werden anstößige Inhalte, nach der Eingabe eines Suchbegriffes, zurückgeliefert.**	**Nicht bestanden**
USB-Tethering	USB-Tethering beeinflusst die Funktionalität des Webfilters nicht.	Bestanden**.**
Wayback Machine	**Ein Zugriff auf web.archive.org ist möglich und in Zuge dessen kann man ebenso auf Websites zugreifen, die normalerweise gesperrt sein sollten.**	**Nicht bestanden**
Gesamtbewertung	**5 (45,45%) von 11 Szenarien wurden nicht bestanden.**	

Tabelle 5.10: Ergebnis - G Data Multi Device (Internet) Security - Umgehungsszenarien

5.0.5 Fazit - G Data

Platz fünf der Vorauswahl zeichnet sich durch eine Gesamtbewertung mit 29,75 von 48 Punkten aus und hat 5 von 11 Umgehungsszenarien nicht bestanden. Zusammengefasst zeigt sich weiterführend auch hier, dass:

- keiner der Webproxy-Dienste blockiert wurde und mit dreien davon eine Umgehung des Webfilters möglich war.
- ein unregulierter Zugriff auf das Web im abgesicherten Modus ohne Weiteres möglich ist.
- ein fehlender Anwendungsfilter es äußerst leicht macht, nicht altersgerechte Programme zu installieren und auszuführen.
- in allen drei alternativen Suchmaschinen nach anstößigen Inhalten gesucht werden konnte und entsprechende Inhalte auch zurückgeliefert wurden.
- über die Wayback-Machine ein Zugriff auf normalerweise blockierte Inhalte möglich ist.

Nachfolgend finden sich auszugsweise Screenshots aus den erfolgreichen Umgehungsszenarien:

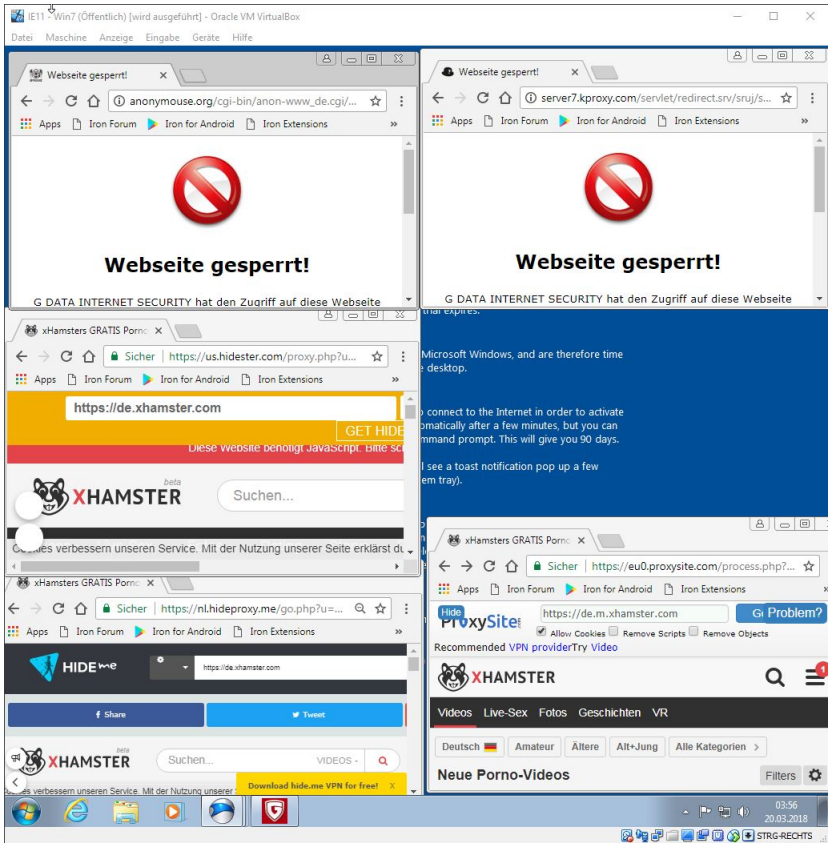

Abbildung 5.15: Ergebnis des Umgehungsszenarios "Anonmysierender Webproxy"

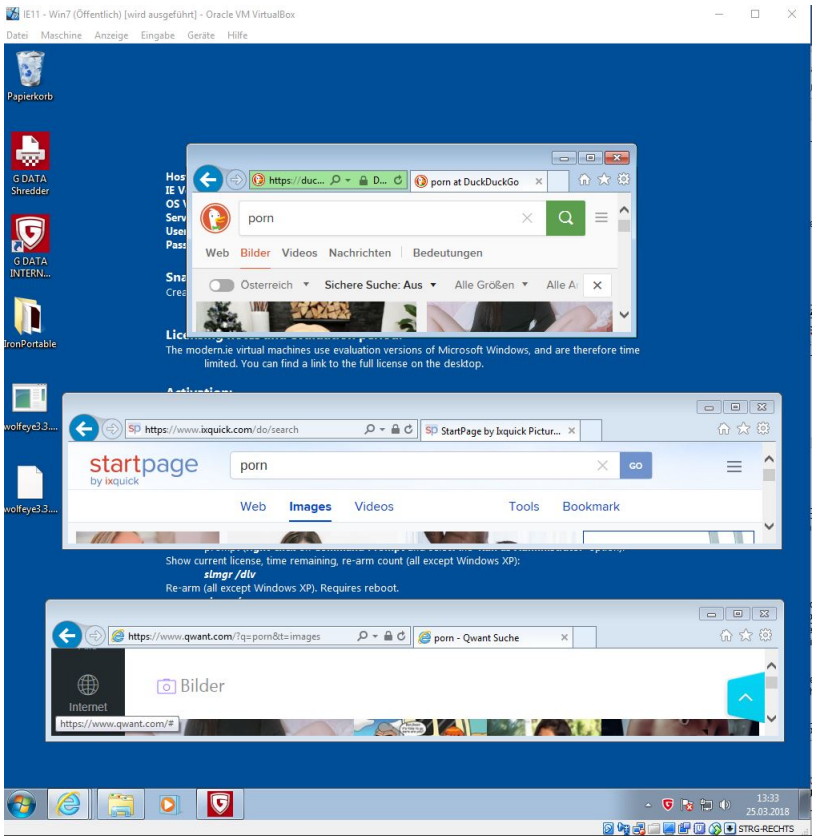

Abbildung 5.16: Ergebnis des Umgehungsszenarios "SafeSearch oder Kindersuchmaschine"

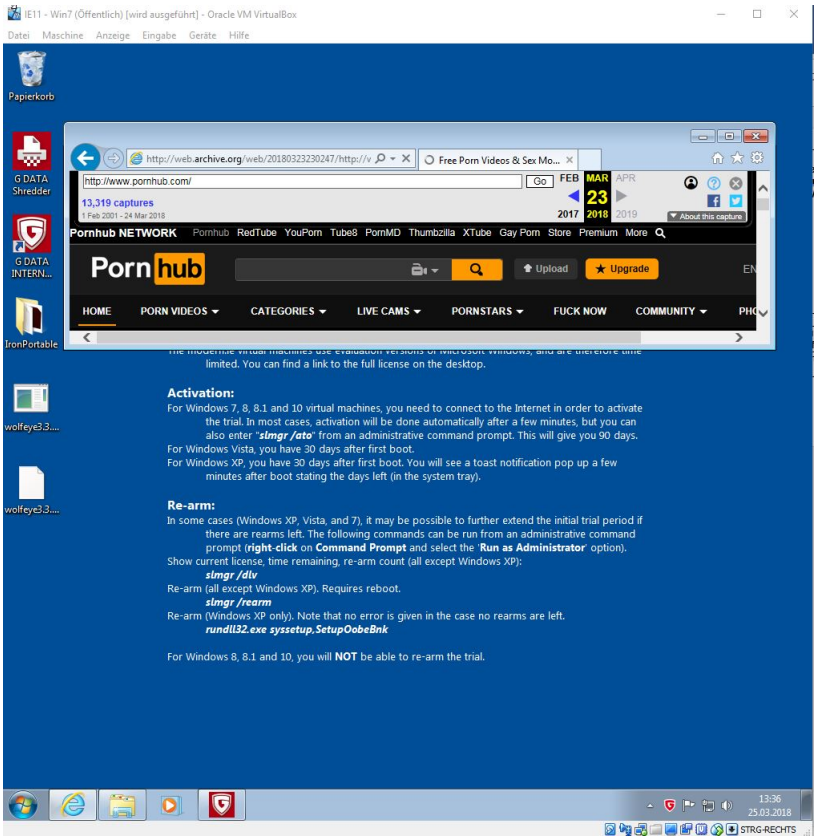

Abbildung 5.17: Ergebnis des Umgehungsszenarios "Wayback Machine"

OpenDNS Family Shield – Praxistestkatalog – Windows 10			
Kriterium	**Beschreibung des Bewertungskriteriums**	**Kritikalität**	**Punkte**
1. Accounts	Open DNS Family Shield wird laut Empfehlung am besten auf Router-Ebene installiert. Dabei gibt es keine Benutzerkonten oder individuelle Filter, wodurch jedes Benutzerkonto gleichermaßen gefiltert wird.	Mittel	0
2. Ausführung von spezifischen Dateitypen blockieren	Die Software kann keine spezifischen Dateitypen blockieren.	Mittel	0
3. Beratungsfunktion	Die Software gibt Eltern keine Hilfestellung bei der Einführung einer Kinderschutzsoftware.	Niedrig	0
4. Deinstallationsschutz	**Wenn OpenDNS auf einem Router installiert wird:** Hierbei liegt die Verantwortung des Setzens eines vernünftigen Passworts für den entsprechenden Router beim Anwender. Da oft ein Standardpasswort oder überhaupt kein Kennwort gesetzt wird, ist der Schutz vor einer Änderung sehr zu hinterfragen. **Wenn OpenDNS am Client installiert wird:** Da OpenDNS nicht darauf hinweist, dass ein eingeschränktes Benutzerkonto verwendet werden sollte, um eine Änderung des DNS Servers zu vermeiden, ist praktisch kein Deinstallationsschutz gegeben.	Hoch	0
5. Downloadblocker	Die Software bietet keine Funktionalität Downloads zu blockieren.	Mittel	0
6. Einrichtungassistent	OpenDNS bietet einen äußerst knappen Einrichtungsleitfaden an, welcher die wichtigsten Schritte zur Einrichtung dokumentiert.	Mittel	0,75

Kriterium	Beschreibung des Bewertungskriteriums	Kritikalität	Punkte
7. Eingeschränkte Benutzerkonten	Es wird während des äußerst kurzen Einrichtungsleitfadens, insbesondere bei der lokalen Eintragung des DNS-Servers, nicht darauf hingewiesen, dass unbedingt ein eingeschränkte Benutzerkonten verwendet werden sollte, um eine Umgehung des DNS-Filters zu vermeiden.	Hoch	0
8. Installation	Es wurde versucht, OpenDNS auf Router-Ebene zu konfigurieren, was jedoch trotz einiger Anläufe nicht funktioniert hat. Bei dem verwendeten Router handelt es sich um einen Huawei B315s-22. Trotz dem expliziten Setzen eines DNS Servers, wurde die Einstellung nicht angenommen, weshalb auf das lokale Eintragen eines DNS-Servers am Client zurückgegriffen werden musste. Da die Installation nur sehr knapp beschrieben ist und zudem nicht funktioniert hat, wird hier kein Punkt vergeben.	Niedrig	0
9. Kategoriefilter Web	OpenDNS Family Shield bietet nur einen vordefinierten Inhaltsfilter.	Hoch	0
10. Kategoriefilter Anwendungen	Anwendungen können mittels OpenDNS nicht blockiert werden.	Hoch	0
11. Laufwerke blockieren	Die Software kann keine Laufwerke blockieren .	Niedrig	0
12. Loggingfunktion	Die Software bietet keine Loggingfunktion an.	Hoch	0
13. Portblocker	Die Software bietet keinen Portblocker an.	Mittel	0

Kriterium	Beschreibung des Bewertungskriteriums	Kritikalität	Punkte
14. Prozessschutz	OpenDNS bietet keinen „Prozess“ der beendet werden kann – da die Änderung des DNS-Servers jedoch ohne Weiteres möglich ist, ist kein Schutz in diesem Sinne gegeben.	Hoch	0
15. Soziale Netzwerke	Die Software bietet keine spezifischen Funktionalitäten hinsichtlich sozialer Netzwerke.	Mittel	0
16. Spamfilter für Maildienste	Die Software hat keinen Spamfilter integriert.	Niedrig	0
17. Sperren von Anwendungen	Die Software kann keine spezifischen Anwendungen blockieren.	Hoch	0
18. Sperren von Websites	Die Software kann keine spezifischen Websites sperren.	Hoch	0
19. Suchmaschine	Die Software beschränkt Suchmaschinen nicht und bietet auch keine Safe Search Funktion an.	Mittel	0
20. USB Schnittstellen blockieren	Die Software kann keine USB Schnittstellen blockieren.	Niedrig	0
21. Verwaltung im Web	Da eine Installation am Router nicht möglich war, wurde die Software lokal installiert. Weil die Anwendung jedoch grundsätzlich eine kollektive Verwaltung bietet, wird hierbei ein Punkt vergeben.	Mittel	1
22. Zeitbeschränkung	Die Software hat keine Einstellung für eine Zeitbeschränkung.	Hoch	0
Gesamtbewertung	**Hoch 0x3 + Mittel 1,75x2 + Niedrig 0x1 = 3,5 / 48**		

Tabelle 5.11: Ergebnis - OpenDNS Family Shield - Praxistestkatalog

OpenDNS Family Shield– Umgehungsszenarien – Windows 10 – Admin-Rechte		
Szenario	**Beschreibung**	**Bewertung**
Änderung der Systemzeit	Die Änderung der Systemzeit hat keine Auswirkungen auf den Filter.	Bestanden
Anonymisierender Webproxy	OpenDNS Family Shield hat alle Webproxy-Seiten blockiert.	Bestanden
Bruteforce-Angriff	***Da der DNS-Server manuell in den Einstellungen am Client gesetzt wurde und nicht darauf hingewiesen wurde, dass ein eingeschränktes Benutzerkonto für das Kind verwendet werden soll, ist ein Bruteforce-Angriff nicht notwendig, da der DNS-Server einfach in den Einstellungen mittels Admin-Rechten geändert werden kann.*** ***Selbst wenn der DNS-Server am Router gesetzt werden würde, wird oftmals das Standardpasswort oder auch kein Passwort für den Admin-Zugang zum Router belassen bzw. gesetzt, was den Zugang sehr einfach macht. Ein Logging der Loginversuche ist abhängig vom Routermodell. Somit wäre ein Bruteforce-Angriff möglich und sogar äußerst einfach durchführbar.***	***Nicht anwendbar***
Essentielle Dateien der Kinderschutzsoftware umbenennen / löschen	***Der DNS-Server Eintrag kann am Client geändert werden, wodurch eine Umgehung des Kinderschutzes auf einfache Art und Weise möglich ist. Selbst am Router könnte dies über einen Werksreset einfach durchgeführt werden.***	***Nicht anwendbar***
Keylogger	**Da nur auf DNS-Ebene gefiltert wird und kein Anwendungsfilter verfügbar ist, lassen sich beide Anwendungen logischerweise ohne Einschränkungen installieren. Ein Login in den Router im Kinderaccount könnte somit über den Keylogger mitgeschnitten werden.**	**Nicht bestanden**
MAC-Spoofing	Trotz dem Ändern der MAC-Adresse greift der Webfilter weiterhin.	Bestanden

Szenario	Beschreibung	
Prozess beenden	***Da es sich hierbei um eine DNS-Einstellung handelt, gibt es keinen „Prozess“, welcher beendet werden kann. Jedoch kann der DNS-Server aufgrund der Admin-Rechte einfach geändert werden.***	***Nicht anwendbar***
Portable Anwendung	• **Assault Cube: Die Anwendung kann ohne Weiteres ausgeführt werden, da dies nur das Web und keine lokalen Anwendungen filtert.** • SR Iron Browser: Der Webfilter wird durch den alternativen Browser nicht umgangen.	**Nicht bestanden**
SafeSearch oder Kindersuchmaschine	**Nach der Deaktivierung des SafeSearch Filters in allen drei alternativen Suchmaschinen, werden entsprechende anstößige Inhalte, nach Eingabe des Suchbegriffes, zurückgeliefert.**	**Nicht bestanden**
USB-Tethering	**Da über USB-Tethering ein neuer Netzwerkadapter eingespeist wird, greifen die lokal definierten DNS-Einstellungen nicht mehr, was dazu führt, dass der Webfilter ausgehebelt wird. Dasselbe würde auch bei der Definition des DNS-Servers am Router selbst passieren, da quasi das USB-Tethering-Gerät den neuen Router bzw. den neuen Zugang zum Web darstellt.**	**Nicht bestanden**
Wayback Machine	Die Wayback Machine wird als Proxy/Anonymizer deklariert und in weiterer Folge blockiert.	Bestanden
Gesamtbewertung	**4 (50,00%) von 8 Szenarien wurden nicht bestanden. 3 Szenarien sind nicht anwendbar**	

Tabelle 5.12: Ergebnis - OpenDNS Family Shield - Umgehungsszenarien

5.0.6 Fazit - OpenDNS

Ein äußerst bedenkenswertes Ergebnis liefert Family Shield von OpenDNS. Jene Anwendung erreicht nur 3,5 von möglichen 48 Punkten in der Gesamtbewertung. Der Sinn hinter OpenDNS wäre gewesen, dass eine effektive Filterung von Erwachseneninhalten stattfindet. Jedoch hat die Anwendung bedingt durch die fehlenden Konfigurations- sowie Filtermöglichkeiten und den Problemen bei der Installation am Router einen entsprechend hohen Punkteverlust zu verantworten. Weiterführend zeichnet sich auch in den Umgehungsszenarien ein weniger hervorragendes Ergebnis mit 4 von 8 nicht bestandenen Umgehungsszenarien ab. Ein weiteres Problem liegt in der hohen Abhängigkeit von gegebenen technischen Geräten - in diesem Falle den Router betreffend. Bei dem eingesetzten Modell haben die DNS-Einstellungen nicht funktioniert, was dazu geführt hat, dass der DNS-Server lokal am Client eingestellt werden musste.

Da nicht darauf hingewiesen wird, dass ein eingeschränktes Benutzerkonto für Kinder bzw. Jugendliche verwendet werden sollte, lassen sich mit den gegebenen Admin-Rechten die DNS-Einstellungen leicht ändern. Außerdem ist dies die erste Anwendung, bedingt durch das DNS-basierte Webfiltering, die mittels USB-Tethering umgehbar ist.

Positiv anzumerken ist, dass OpenDNS die Waybackmachine als "Proxy/Anonymizer" deklariert und automatisch blockiert.

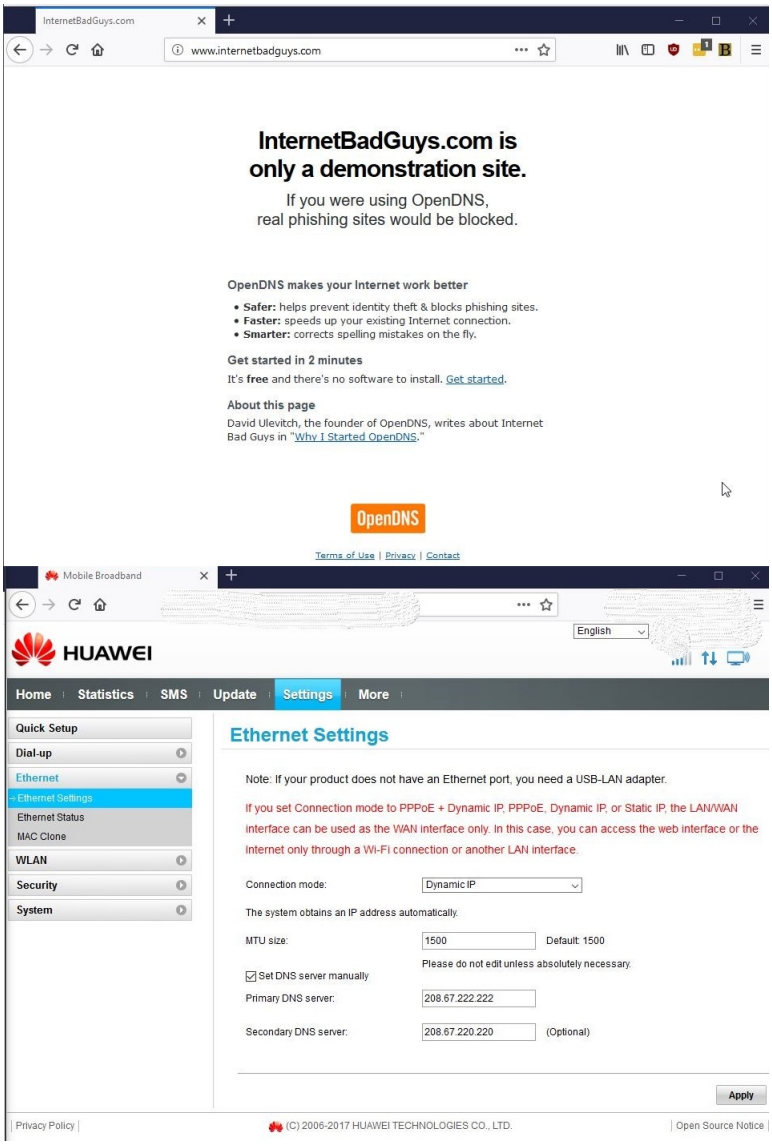

Abbildung 5.18: OpenDNS funktioniert auf Router-Ebene nicht

Telekom Kinderschutz Software 4.00.0070 – Praxistestkatalog – Windows 10			
Kriterium	**Beschreibung des Bewertungskriteriums**	**Kritikalität**	**Punkte**
1. Accounts	Es können Profile für Kinder direkt in der Anwendung angelegt werden und unterschiedliche Filter für die unterschiedlichen Kinderkonten definiert werden.	Mittel	1
2. Ausführung von spezifischen Dateitypen blockieren	Die Software kann keine spezifischen Dateitypen blockieren.	Mittel	0
3. Beratungsfunktion	Bereits während der Installation werden die Eltern bezüglich der Ver- und Anwendung der Kinderschutzsoftware beraten.	Niedrig	1
4. Deinstallationsschutz	Bei der Einrichtung der Software muss direkt ein Passwort für den Elternbereich definiert und ein entsprechendes Benutzerkonto des Elternteils ausgewählt werden. Ebenso lässt sich eine Sicherheitsfrage hinterlegen, welche auch selbst gewählt werden kann.	Hoch	1
5. Downloadblocker	Das Herunterladen von spezifischen Dateitypen (Video, Musik, Programm, Dokumente..) kann blockiert werden.	Mittel	1
6. Einrichtungsassistent	Die Telekom Kinderschutz Software bietet einen Einrichtungsassistenten an, welcher jeden relevanten Bereich genau erörtert. Zudem werden Tooltips angeboten, die jedes Feld und jeden Text nochmals im Detail erläutern.	Mittel	1
7. Eingeschränkte Benutzerkonten	Während der Einrichtung wird über die Hilfe-Funktion drauf hingewiesen, dass unbedingt ein eingeschränktes Benutzerkonto für das Kind verwendet werden sollte.	Hoch	0,75

Kriterium	Beschreibung des Bewertungskriteriums	Kritikalität	Punkte
8. Installation	Bereits während der Installation werden die Funktionalitäten des Kinderschutzes und die notwendigen Schritte zur Einrichtung erläutert.	Niedrig	0,75
9. Kategoriefilter Web	Der Kategoriefilter für das Web wird automatisch auf das entsprechende Alter des Kindes zugeschnitten. Dabei werden verschiedenste Haupt- und Unterkategorien angeboten, welche ein Einstellen eines feingranularen Filters erlauben.	Hoch	1
10. Kategoriefilter Anwendungen	Die Software bietet keinen variablen Anwendungskategoriefilter an.	Hoch	0
11. Laufwerke blockieren	Die Software kann keine Laufwerke blockieren.	Niedrig	0
12. Loggingfunktion	Die Software bietet keine Loggingfunktion an.	Hoch	0
13. Portblocker	Die Software bietet keinen Portblocker an.	Mittel	0
14. Prozessschutz	Der Service der Anwendung lässt sich nicht ohne Admin-Rechte beenden. Der zweite Prozess der Kindersicherung jedoch schon. Dabei kann aber weiterführend keine Verbindung mit dem Internet mehr aufgebaut werden.	Hoch	1
15. Soziale Netzwerke	Die Software bietet keine spezifischen Funktionalitäten hinsichtlich sozialer Netzwerke.	Mittel	0
16. Spamfilter für Maildienste	Spam-URLs werden durch die Anwendung automatisch blockiert.	Niedrig	1
17. Sperren von Anwendungen	Spezifische Anwendungen lassen sich in der Anwendung blockieren.	Hoch	1

Kriterium	Beschreibung des Bewertungskriteriums	Kritikalität	Punkte
18. Sperren von Websites	Die Software erlaubt es spezifische Websites zu blockieren oder explizit freizugeben.	Hoch	1
19. Suchmaschine	Es wird auf die Verwendung der Suchmaschine „FragFinn“ verwiesen, wenn eine Website angesurft wird, die gesperrt wurde.	Mittel	0,5
20. USB Schnittstellen blockieren	Die Software kann keine USB Schnittstellen blockieren.	Niedrig	0
21. Verwaltung im Web	Die Software wird lokal verwaltet.	Mittel	0
22. Zeitbeschränkung	Es lässt sich pro Tag ein gewisser Zeitraum und eine Anzahl an Stunden, in welcher das Internet verwendet werden darf, definieren.	Hoch	1
Gesamtbewertung	**Hoch 6,75x3 + Mittel 3,5x2 + Niedrig 2,75x1 = 30 / 48**		

Tabelle 5.13: Ergebnis - Telekom Kinderschutz Software - Praxistestkatalog

Telekom Kinderschutz Software – Umgehungsszenarien – Windows 10 – Konto ohne Admin-Rechte		
Szenario	**Beschreibung**	**Bewertung**
Änderung der Systemzeit	Bedingt durch die fehlenden Admin-Rechte, lässt sich die Systemzeit nicht ändern.	Bestanden
Anonymisierender Webproxy	**Beim Webfilter wurde eine Sperrung von HTTPs Seiten automatisch aktiviert. Dieser Filter stellt keine Kindersicherung in diesem Sinne dar, da damit generisch alle Websites die verschlüsselten Traffic generieren automatisch gesperrt werden. Zudem werden ständig Meldungen mit „Nicht erlaubt“ generiert. Darauffolgend wurde dieser Teil des Webfilters deaktiviert.** Alle fünf Webproxy-Dienste wurden durch die Kindersicherung blockiert.	Bestanden
Bruteforce-Angriff	**Die fehlgeschlagenen Zugriffsversuche werden nicht mitgeloggt und das Elternteil wird auch nicht darüber informiert. Außerdem gibt es eine Sicherheitsfrage, welche das Zurücksetzen des Passwortes ermöglicht. Bei Fragen wie „Wo haben Sie Ihren Partner kennengelernt?“ oder „Wie heißt Ihr bester Kindheitsfreund?“ kann es äußerst schnell passieren, dass unwissende Eltern die passende Antwort herausgeben, wenn Kinder danach fragen.**	**Nicht bestanden**
Essentielle Dateien der Kinderschutzsoftware umbenennen / löschen	Das Löschen bzw. Umbenennen von relevanten Dateien ist im Account des Kindes nicht möglich, da dafür Admin-Rechte benötigt werden. **Jedoch startet die Kinderschutzanwendung im abgesicherten Modus nicht mit, wodurch ein filterfreier Zugang zum Web ohne Weiteres möglich ist.**	**Nicht bestanden**
Keylogger	**Da die Telekom Kindersicherung keinen Anwendungsfilter besitzt, konnten beide Keylogger ohne Weiteres am Client installiert und genutzt werden.**	**Nicht bestanden**
MAC-Spoofing	Eine neue MAC-Adresse kann ohne Admin-Rechte nicht zugewiesen werden.	Bestanden

Szenario	Beschreibung	
Prozess beenden	- Taskmanager: Einer der beiden Kinderschutzprozesse kann beendet werden. Dies führt jedoch dazu, dass keine Internetverbindung mehr aufbaubar ist. - Paint-Dokument: Das offene und bearbeitete Dokument sowie der Herunterfahrprozess haben keine Auswirkungen auf die Funktionalität der Kindersicherung.	Bestanden
Portable Anwendung	• **Assault Cube: Da die Kindersicherung keinen Anwendungsblocker besitzt, kann Assault Cube ausgeführt werden.** • SR-Iron Browser: Der Webfilter greift auch in dem alternativen Browser.	**Nicht bestanden**
SafeSearch oder Kindersuchmaschine	DuckDuckgo wurde von der Kindersicherung blockiert. **Jedoch lässt sich bei ixquick sowie qwant der SafeSearch-Filter deaktivieren, was dazu führt, dass anstößige Suchbegriffe eingegeben werden können und entsprechende Resultate zurückgeliefert werden.**	**Nicht bestanden**
USB-Tethering	USB Tethering beeinflusst die Funktionalität des Webfilters nicht.	Bestanden
Wayback Machine	Die Wayback-Machine wird durch die Kindersicherung blockiert.	Bestanden
Gesamtbewertung	**5 (45,45%) von 11 Szenarien wurden nicht bestanden.**	

Tabelle 5.14: Ergebnis - Telekom Kinderschutz Software - Umgehungsszenarien

5.0.7 Fazit - Telekom

Die Kindersicherung der Telekom erreicht 30 von 48 möglichen Punkten im Praxistestkatalog und 5 von 11 Umgehungsszenarien wurden nicht bestanden. Bedingt durch den fehlenden Anwendungsfilter, lassen sich Keylogger sowie portable Anwendungen, welche nicht altersgerecht sind, ausführen. Ebenso lassen sich alternative Suchmaschinen aufrufen, welche nach der Deaktivierung von SafeSearch, anstößige Inhalte zurückliefern. Abschließend wird die Anwendung im abgesicherten Modus nicht mitgestartet, wodurch ein ungefilterter Zugang zum Web möglich ist.

Nachfolgend finden sich abermals auszugsweise Screenshots aus den erfolgreichen Umgehungsszenarien:

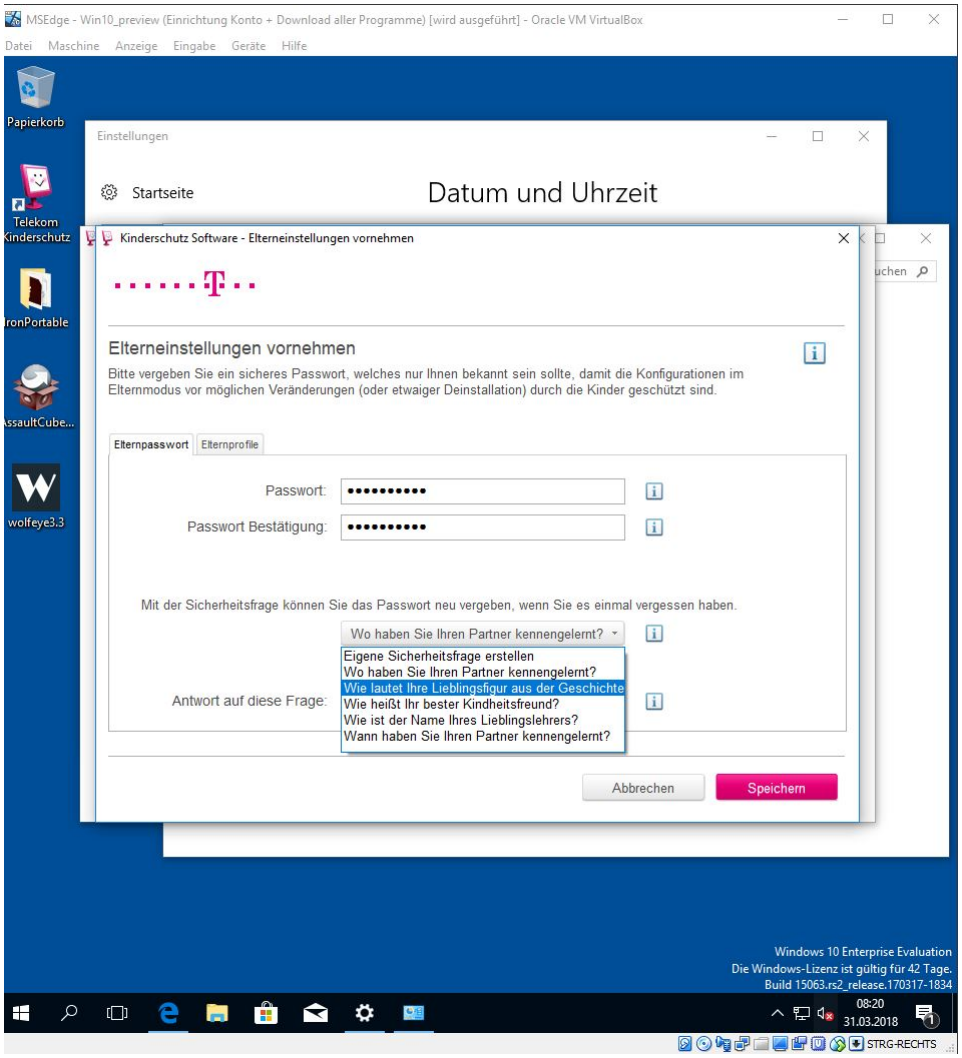

Abbildung 5.19: Ergebnis des Umgehungsszenarios "Bruteforce-Angriff"

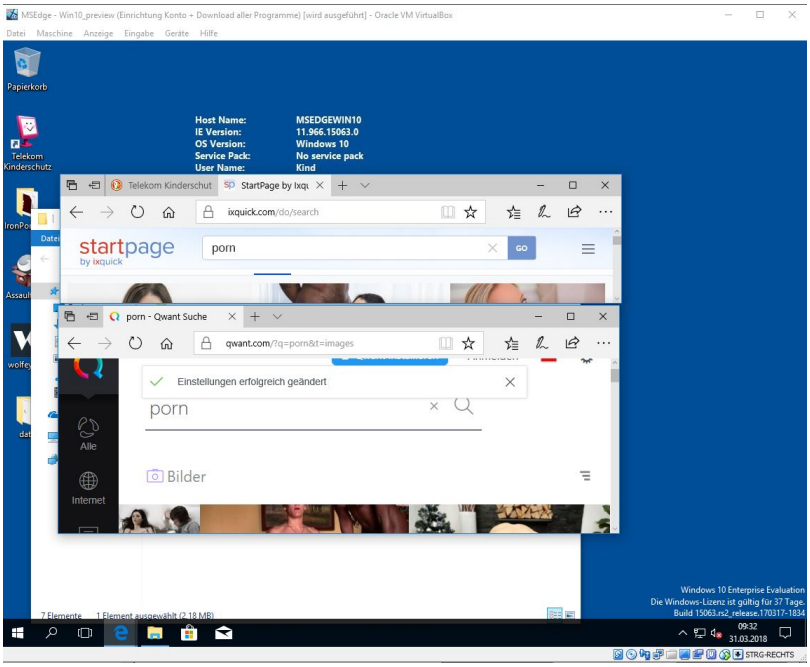

Abbildung 5.20: Ergebnis des Umgehungsszenarios "SafeSearch oder Kindersuchmaschine"

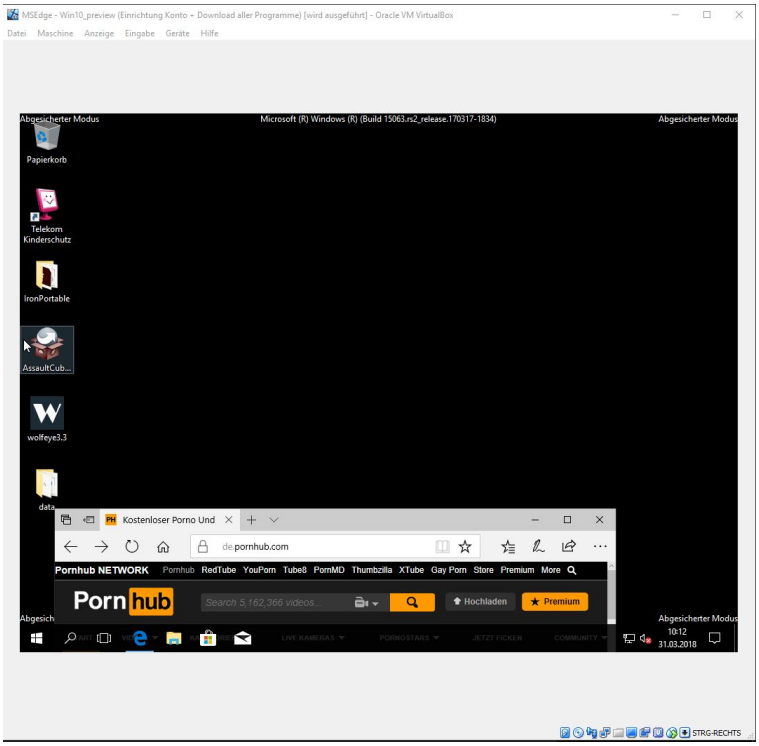

Abbildung 5.21: Ergebnis des Umgehungsszenarios "Essentielle Dateien der Kinderschutzsoftware umbenennen/löschen"

5.0.8 Fazit - KinderServer

Wie man den nachfolgenden Screenshots entnehmen kann, hat es sich herausgestellt, dass der Proxy-Server der Anwendung nicht mehr aktiv ist. Somit kann das Programm nicht mehr eingesetzt werden, da die Anwendung selbst nur einen Webfilter und weder eine Zeitkontofunktion noch einen zusätzlichen Anwendungsfilter besitzt. Faktisch liefert somit die Anwendung überhaupt keinen Schutz in diesem Sinne mehr, weshalb die Anwendung mit 0 Punkten bewertet wird.

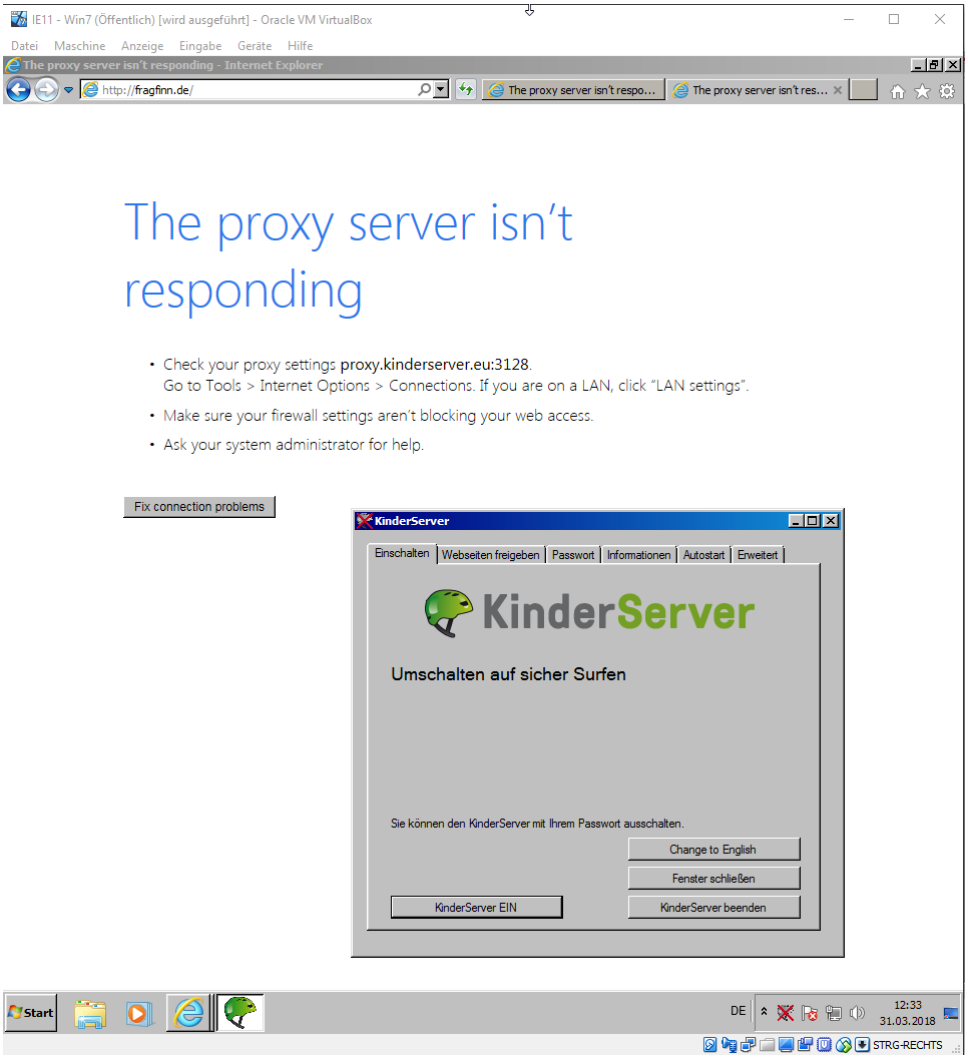

Abbildung 5.22: KinderServer - Proxy Server nicht verfügbar

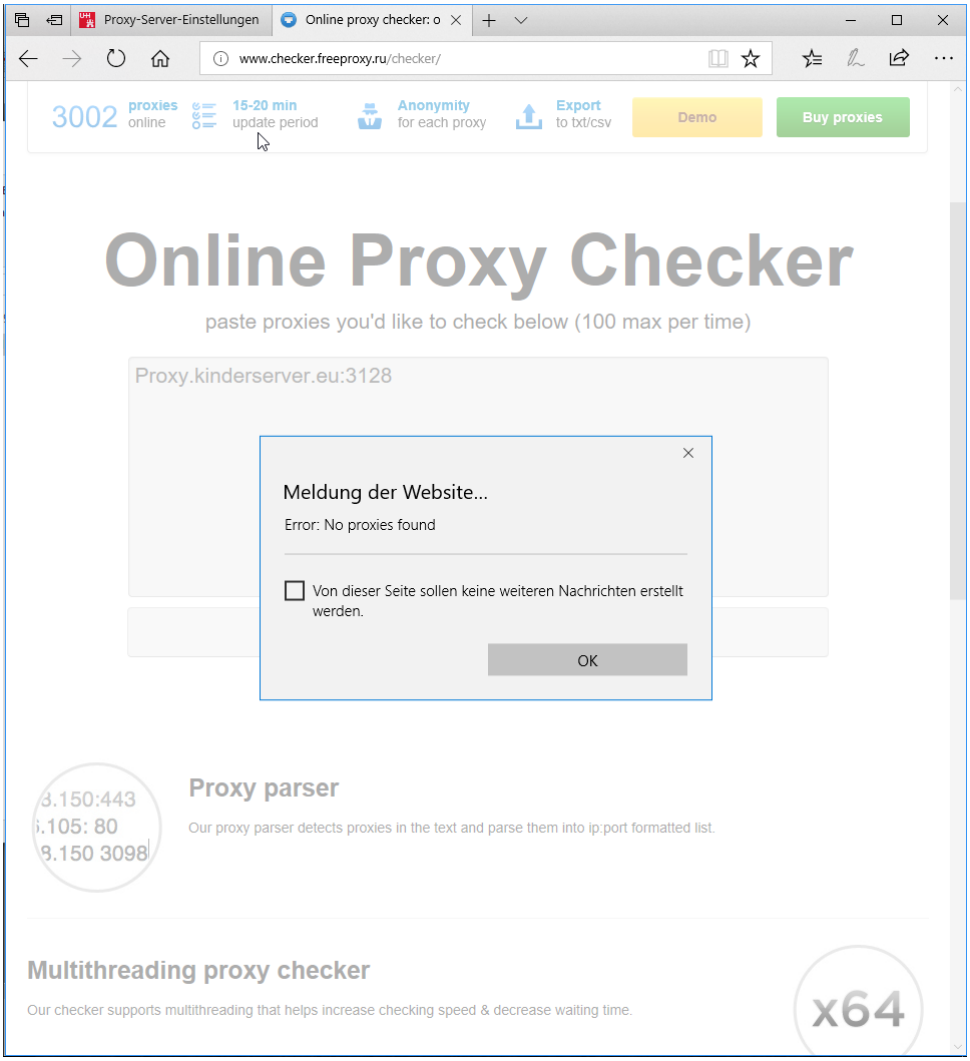

Abbildung 5.23: KinderServer - Proxy Server nicht verfügbar

ESET Internet Security 11.0.159.9 – Praxistestkatalog – Windows 10			
Kriterium	**Beschreibung des Bewertungskriteriums**	**Kritikalität**	**Punkte**
1. Accounts	Benutzeraccounts lassen sich zwar nicht über das Softwareinterface anlegen, jedoch können jedem Benutzerkonto unter Windows 10 eigene Filter- und Profileinstellungen zugewiesen werden.	Mittel	1
2. Ausführung von spezifischen Dateitypen blockieren	ESET Internet Security erlaubt kein Blockieren von spezifischen Dateiendungen.	Mittel	0
3. Beratungsfunktion	Eine Beratungsfunktion für Eltern, wie mit den, durch die Kindersicherung erhaltenen Informationen umzugehen ist, ist durch die Software nicht gegeben.	Niedrig	0
4. Deinstallationsschutz	Das Setzen eines Passwortes ist optional und während der Einrichtung wird auch nicht darauf hingewiesen, dass ein Passwort gesetzt werden sollte. Dies führt dazu, dass in den Standardeinstellungen eine Deinstallation der Software ohne Weiteres möglich ist. Mit dem Setzen eines Passwortes, wird auch die Deinstallation geschützt.	Hoch	0
5. Downloadblocker	Downloads können mittels ESET Internet Security nicht blockiert werden.	Mittel	0
6. Einrichtungassistent	ESET Internet Security bietet ein äußerst kurzgehaltenes Web-Wiki an. Weitere Hilfestellungen werden nicht angeboten.	Mittel	0,75
7. Eingeschränkte Benutzerkonten	ESET bietet nicht die Möglichkeit an direkt über das Softwareinterface einen Benutzeraccount anzulegen, weshalb dies über die Benutzerkontensteuerung von Windows 10 geschehen muss. Dabei ist dieser Weg fehleranfällig, da es dazu führen kann, dass das Elternteil bei der Einrichtung gewollt oder auch ungewollt ein Konto mit Admin-Rechten anlegt, was eine Umgehung der Software für das Kind erleichtert. Zudem wird auf diesen Sachverhalt nicht durch die Software hingewiesen.	Hoch	0

Kriterium	Beschreibung des Bewertungskriteriums	Kritikalität	Punkte
8. Installation	ESET Internet Security lässt sich einfach installieren, jedoch werden keine unterstützenden Hinweise zur Einrichtung der Kindersicherung gegeben.	Niedrig	0,75
9. Kategoriefilter Web	Die Software bietet verschiedenste Kategorien, nach denen gefiltert werden kann. Zudem wird der Filter bereits im Vorhinein an das Alter des Kindes bzw. des Jugendlichen durch die Eingabe eines Geburtsdatums angepasst.	Hoch	1
10. Kategoriefilter Anwendungen	ESET Internet Security bietet keine Option an Anwendungen nach Kategorien zu blockieren. Insgesamt gibt es keine Funktion, Anwendungen zu blockieren.	Hoch	0
11. Laufwerke blockieren	Ein Blockieren von eingelegten Datenträgern wie einer CD/DVD ist möglich.	Niedrig	1
12. Loggingfunktion	Besuchte Websites werden durch die Anwendung geloggt und können gefiltert werden.	Hoch	0,75
13. Portblocker	Über die mitgelieferte Firewall Funktion der Software lassen sich spezifische Anwendung und/oder Ports blockieren.	Mittel	1
14. Prozessschutz	Die Prozesse, welche durch die Ausführung von ESET Internet Security erzeugt werden, werden geschützt.	Hoch	1
15. Soziale Netzwerke	Eine Funktion zur Sperrung von sozialen Netzwerken ist vorhanden, mit welcher jedoch auch gleichzeitig Chats gesperrt werden.	Mittel	1
16. Spamfilter für Maildienste	Ein Spam-Filter ist in ESET Internet Security integriert und automatisch aktiv.	Niedrig	1
17. Sperren von Anwendungen	ESET Internet Security bietet keine Option Anwendungen zu sperren.	Hoch	0

Kriterium	Beschreibung des Bewertungskriteriums	Kritikalität	Punkte
18. Sperren von Websites	Die Software kann Ausnahmen generieren und somit spezifische Websites sperren oder zulassen.	Hoch	1
19. Suchmaschine	Es wird keine kindersichere Suchmaschine oder Safe-Search Funktion angeboten.	Mittel	0
20. USB Schnittstellen blockieren	Die Software erlaubt es verschiedenste Schnittstellen am Rechner (USB-Sticks, CDs/DVDs, Drucker, ...) zu sperren.	Niedrig	1
21. Verwaltung im Web	ESET Internet Security wird nur lokal installiert und hat keine Weboberfläche zur Verwaltung.	Mittel	0
22. Zeitbeschränkung	Die Software hat keine Einstellung für eine Zeitbeschränkung.	Hoch	0
Gesamtbewertung	**Hoch 3,75x3 + Mittel 3,75x2 + Niedrig 3,75x1 = 22,5 / 48**		

Tabelle 5.15: Ergebnis - ESET Internet Security - Praxistestkatalog

ESET Internet Security – Umgehungsszenarien – Windows 10 – Admin-Rechte		
Szenario	**Beschreibung**	**Bewertung**
Änderung der Systemzeit	Die Systemzeit wird automatisch auf die derzeit gültige Zeit zurückgesetzt, obwohl die Datums- und Uhrzeitsynchronisation von Windows 10 deaktiviert wurde. Zu Testzwecken wurde ebenso für kurze Zeit der Netzwerkadapter deaktiviert, um eine Synchronisation über das Web zu vermeiden. Weiterführend wurde das Datum und die Uhrzeit trotzdem zurückgesetzt.	Bestanden
Anonymisierender Webproxy	ESET Internet Security hat alle fünf Web-Proxy Dienste blockiert.	Bestanden
Bruteforce-Angriff	**Als erstes ist anzumerken, dass das Setzen eines Passwortes bei ESET für die Kindersicherung optional ist.** Es wird zwar eine Warnung angezeigt, jedoch sollte ein Passwort verpflichtend sein, wenn schon nicht darauf hingewiesen wird, dass ein eingeschränktes Benutzerkonto für den Kinder- bzw. Jugendlichen-Account verwendet werden soll. **Zudem gibt es keine Passwort Policies, ergo kann ein Passwort mit nur einer einzigen Ziffer eingegeben und gesetzt werden. Faktisch werden die fehlgeschlagenen Loginversuche nicht geloggt und es kann zudem beliebige Male versucht werden, das Passwort zu knacken.**	**Nicht bestanden**
Essentielle Dateien der Kinderschutzsoftware umbenennen / löschen	Die Software benötigt SYSTEM-Rechte – mit reinen Admin-Rechten funktioniert ein Löschen der Software über den Explorer nicht. **Anders hingegen sieht es über die Systemsteuerung aus: wenn das optionale Passwort nicht gesetzt wurde, ist eine Deinstallation ohne Weiteres möglich.** **Im abgesicherten Modus lässt sich die Anwendung einfach im Explorer in den Papierkorb schieben und löschen. Ein Unterbinden durch die Software ist in diesem Falle nicht möglich.**	**Nicht bestanden**
Keylogger	Der „Wolfeye-Keylogger“ wurde von ESET sofort als Malware erkannt sowie entfernt und konnte somit gar nicht installiert werden. **Der „Bester Keylogger“ von hwsuite wird hingegen nicht erkannt und kann durch die Admin-Rechte auf jeglichen Benutzerkonten installiert werden. Auch nach der Ausführung und dem Mitschnitt von Eingaben, wird der Keylogger nicht erkannt.**	**Nicht bestanden**

Szenario	Beschreibung	
MAC-Spoofing	Das Spoofen der MAC-Adresse ist bedingt durch die Admin-Rechte möglich, jedoch bleiben Websites die gesperrt sind, weiterhin blockiert.	Bestanden
Prozess beenden	Der Prozess kann trotz Admin-Rechten im Taskmanager nicht beendet werden. Wenn der Herunterfahrprozess eingeleitet wird, wird zwar die GUI-Anwendung geschlossen, jedoch bleibt der ESET-Service weiterhin bestehen, wodurch der Kinderschutz weiterhin greift.	Bestanden
Portable Anwendung	• **Assault Cube: Das Spiel ab 18+ kann ohne Weiteres ausgeführt werden, da ESET keinen Anwendungsfilter besitzt.** • SR-Iron Browser: Der Webfilter kann mittels des portablen Browsers nicht umgangen werden. Der Webfilter greift weiterhin.	**Nicht bestanden**
SafeSearch oder Kindersuchmaschine	• **duckduckgo.com: SafeSearch muss nur deaktiviert werden, danach kann nach anstößigen Inhalten gesucht werden und weiterführend werden die Suchergebnisse ungefiltert auch an das Kind bzw. den Jugendlichen weitergeleitet.** • **ixquick.com: Auch hier muss SafeSearch nur deaktiviert werden – die Suchergebnisse werden daraufhin nicht mehr gefiltert.** • **qwant.com: Nach einer Deaktivierung von SafeSearch werden anstößige Inhalte ungefiltert angezeigt.**	**Nicht bestanden**
USB-Tethering	Trotz USB-Tethering greift der Webfilter weiterhin.	Bestanden
Wayback Machine	**Ein Zugriff auf Snapshots von normalerweise gesperrten Websites ist ohne Weiteres möglich. Der Websitefilter von ESET Internet Security greift nicht.**	**Nicht bestanden**
Gesamtbewertung	**6 (54,55%) von 11 Szenarien wurden nicht bestanden.**	

Tabelle 5.16: Ergebnis - ESET Internet Security - Umgehungsszenarien

5.0.9 Fazit - ESET

Die Anwendung nahm den vorletzten Platz in der Vorauswahl ein, hat jedoch ein definitiv besseres Ergebnis im Praxistest erlangt. Dabei erhielt das Programm 22,5 von 48 möglichen Punkten und hat insgesamt 6 von 11 Umgehungsszenarien nicht bestanden. Ein Auszug aus den Umgehungsszenarien zeigt die bereits bekannten Probleme, welche nachfolgend aufgeführt werden:

- Bruteforce-Angriffe werden nicht geloggt und ebenso nicht unterbunden.
- Da das Passwort zum Elternmodus nur optional ist, lässt sich die Kinderschutzanwendung einfach deinstallieren. Ebenso führt der abgesicherte Modus dazu, dass die Anwendung nicht ausgeführt wird und somit ein ungefilterter Zugang zum Web möglich ist.
- Ein Keylogger wird nicht detektiert, wodurch ein Mitschneiden jeglicher Passwörter auf allen Konten möglich ist.
- Alternative Suchmaschinen werden nicht geblockt und SafeSearch kann in allen deaktiviert werden.
- Ein Zugriff auf Snapshots von normalerweise gesperrten Websites des Webarchives ist ohne Weiteres möglich.

Nachfolgend finden sich noch auszugsweise Screenshots der erfolgreichen Umgehungsszenarien:

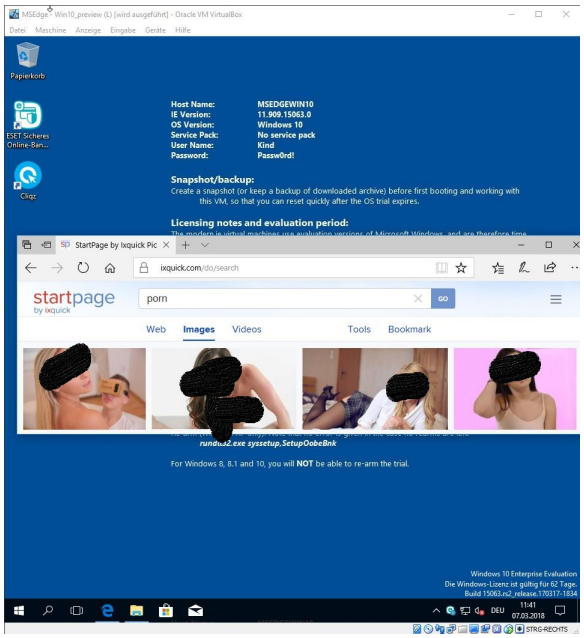

Abbildung 5.24: Ergebnis des Umgehungsszenarios "SafeSearch oder Kindersuchmaschine"

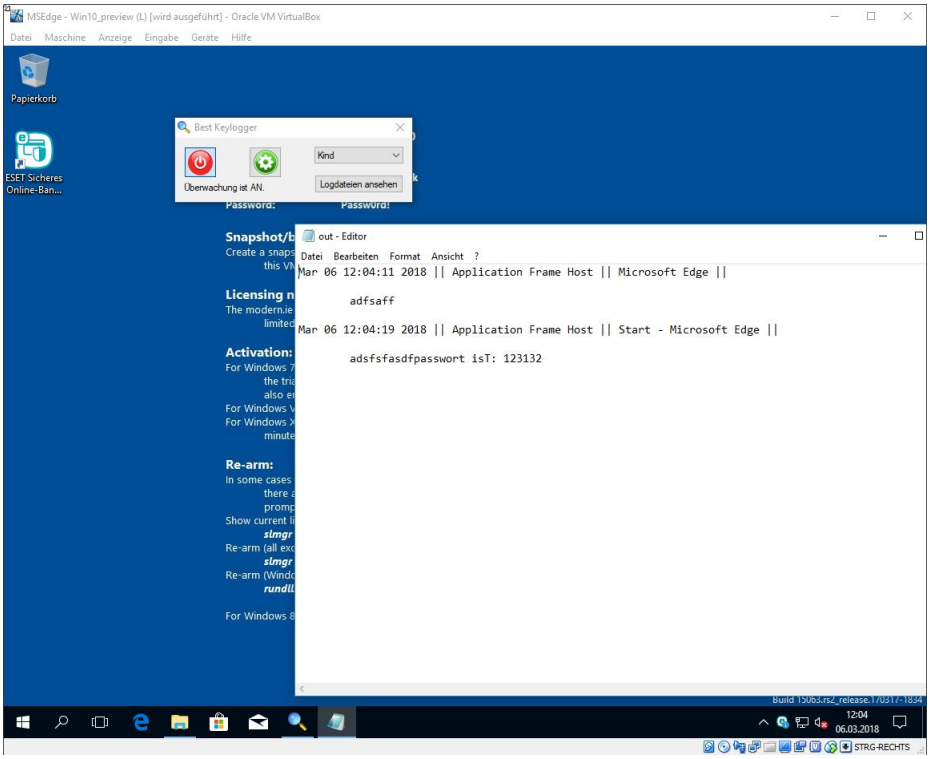

Abbildung 5.25: Ergebnis des Umgehungsszenarios "Keylogger"

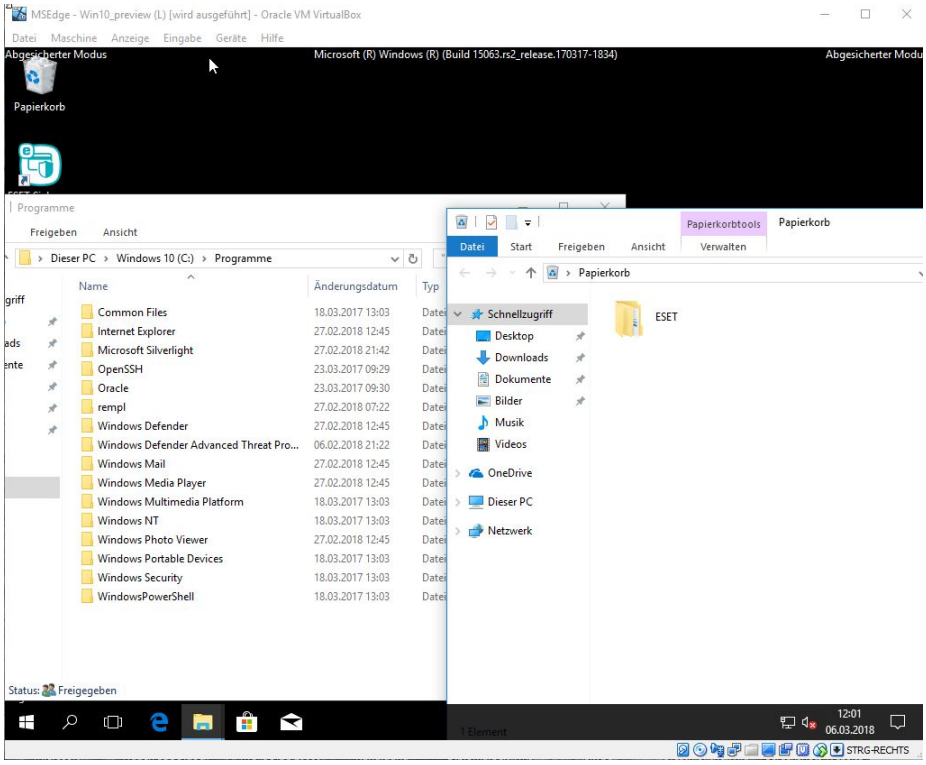

Abbildung 5.26: Ergebnis des Umgehungsszenarios "Essentielle Dateien der Kinderschutzsoftware umbenennen/löschen"

Aus die Maus! 1.7.4.0 – Praxistestkatalog – Windows 7			
Kriterium	**Beschreibung des Bewertungskriteriums**	**Kritikalität**	**Punkte**
1. Accounts	Das Zeitkontoguthaben kann pro Account definiert werden.	Mittel	1
2. Ausführung von spezifischen Dateitypen blockieren	Die Software kann keine spezifischen Dateitypen blockieren.	Mittel	0
3. Beratungsfunktion	Es werden keine Empfehlungen zur Einführung der Kindersicherung durch den Hersteller gegeben.	Niedrig	0
4. Deinstallationsschutz	Die Anwendung kann ohne Weiteres gelöscht werden.	Hoch	0
5. Downloadblocker	Die Software bietet keine Funktionalität Downloads zu blockieren.	Mittel	0
6. Einrichtungsassistent	Es wird keine weiterführende Hilfestellung für die Anwendung geboten.	Mittel	0
7. Eingeschränkte Benutzerkonten	Es wird nicht darauf hingewiesen, dass für Kinder eingeschränkte Benutzerkonten verwendet werden sollten.	Hoch	0
8. Installation	Die Installation selbst ist einfach durchführbar und selbsterklärend. Ebenso lässt sich der Installationsort auswählen.	Niedrig	0,75
9. Kategoriefilter Web	Die Software bietet keinen variablen Kategoriefilter an.	Hoch	0

Kriterium	Beschreibung des Bewertungskriteriums	Kritikalität	Punkte
10. Kategoriefilter Anwendungen	Die Software bietet keinen variablen Kategoriefilter an.	Hoch	0
11. Laufwerke blockieren	Die Software kann keine Laufwerke blockieren.	Niedrig	0
12. Loggingfunktion	Die Software bietet keine Loggingfunktion an.	Hoch	0
13. Portblocker	Die Software bietet keinen Portblocker an.	Mittel	0
14. Prozessschutz	Die Anwendung lässt sich über den Taskmanager beenden.	Hoch	0
15. Soziale Netzwerke	Die Software bietet keine spezifischen Funktionalitäten hinsichtlich sozialer Netzwerke.	Mittel	0
16. Spamfilter für Maildienste	Die Software hat keinen Spamfilter integriert.	Niedrig	0
17. Sperren von Anwendungen	Die Software kann keine spezifischen Anwendungen blockieren.	Hoch	0
18. Sperren von Websites	Die Software kann keine spezifischen Websites sperren.	Hoch	0
19. Suchmaschine	Die Software beschränkt Suchmaschinen nicht und bietet auch keine Safe Search Funktion an.	Mittel	0
20. USB Schnittstellen blockieren	Die Software kann keine USB Schnittstellen blockieren.	Niedrig	0
21. Verwaltung im Web	Die Software wird lokal verwaltet.	Mittel	0

Kriterium	Beschreibung des Bewertungskriteriums	Kritikalität	Punkte
22. Zeitbeschränkung	Es lässt sich pro Tag eine Anzahl an Minuten definieren, welche der entsprechende Account am Rechner verbringen darf.	Hoch	0,5
Gesamtbewertung	**Hoch 0,5x3 + Mittel 1x2 + Niedrig 0,75x1 = 4,25 / 48**		

Tabelle 5.17: Ergebnis - Aus die Maus! - Praxistestkatalog

Aus die Maus! – Umgehungsszenarien – Windows 7 – Admin-Rechte		
Szenario	**Beschreibung**	**Bewertung**
Änderung der Systemzeit	Die Änderung der Systemzeit hat keine Auswirkungen auf die Funktionalität des Zeitguthabens.	Bestanden
Anonymisierender Webproxy	**Da die Anwendung keinen Webfilter besitzt, gilt das Szenario automatisch als „Nicht bestanden“.**	**Nicht bestanden**
Bruteforce-Angriff	**Die Anzahl der fehlgeschlagenen Loginversuche wird nicht mitgeloggt und man kann beliebig viele Versuche starten, um das Passwort via Bruteforce zu knacken.**	**Nicht bestanden**
Essentielle Dateien der Kinderschutzsoftware umbenennen / löschen	**Die Anwendung lässt sich über den integrierten Uninstaller einfach deinstallieren. Dies ist unabhängig davon, ob ein Passwort für den Elternmodus gesetzt wurde oder nicht.**	**Nicht bestanden**
Keylogger	**Da die Anwendung keinen Anwendungsfilter oder Anti-Virenschutz besitzt, kann ohne Weiteres ein Keylogger installiert werden.**	**Nicht bestanden**
MAC-Spoofing	Die MAC-Adresse beeinflusst nicht die Zeitkontofunktion der Anwendung.	Bestanden
Prozess beenden	**Der Prozess der Kinderschutzanwendung lässt sich einfach über den Task-Manager beenden.**	**Nicht bestanden**
Portable Anwendung	**Da die Anwendung keine Filterfunktionalitäten besitzt, gilt das Szenario automatisch als „Nicht bestanden“**	**Nicht bestanden**
SafeSearch oder Kindersuchmaschine	**Da die Anwendung keine Filterfunktionalitäten besitzt, gilt das Szenario automatisch als „Nicht bestanden“**	**Nicht bestanden**

Szenario	Beschreibung	Bewertung
USB-Tethering	USB-Tethering beeinflusst die Zeitkontofunktionalität nicht.	Bestanden
Wayback Machine	**Da die Anwendung keinen Webfilter besitzt, gilt das Szenario automatisch als „Nicht bestanden“.**	**Nicht bestanden**
Gesamtbewertung	**8 (72,73%) von 11 Szenarien wurden nicht bestanden.**	

Tabelle 5.18: Ergebnis - Aus die Maus! - Umgehungsszenarien

5.0.10 Fazit - Aus die Maus!

Das Schlusslicht bildet hierbei "Aus die Maus!", da es im Grunde nur eine einzige Funktionalität bietet, nämlich das Zeitkonto. Wenn dieses aufgebraucht wurde, beginnt automatisch ein Abmeldeprozess vom Benutzerkonto. Wenn man ausgeloggt wurde, kann man sich zwar dann in weiterer Folge wieder einloggen, jedoch wird dann abermals nach wenigen Sekunden der Abmeldeprozess eingeleitet. Weiterführend wurden keine Anwendungs- oder Webfilteralgorithmen implementiert, weshalb das Programm nur 4,25 von 48 Punkten im Praxistestkatalog erhalten und 8 von 11 Umgehungsszenarien nicht bestanden hat. Abgesehen von der fehlenden Funktionalität, lässt sich das Programm sehr einfach umgehen, da der Prozess der Anwendung nicht geschützt wird und einfach beendet werden kann. Außerdem lässt sich "Aus die Maus!" direkt über den Uninstaller deinstallieren. Nachfolgend finden sich Screenshots aus den genannten Umgehungsszenarien:

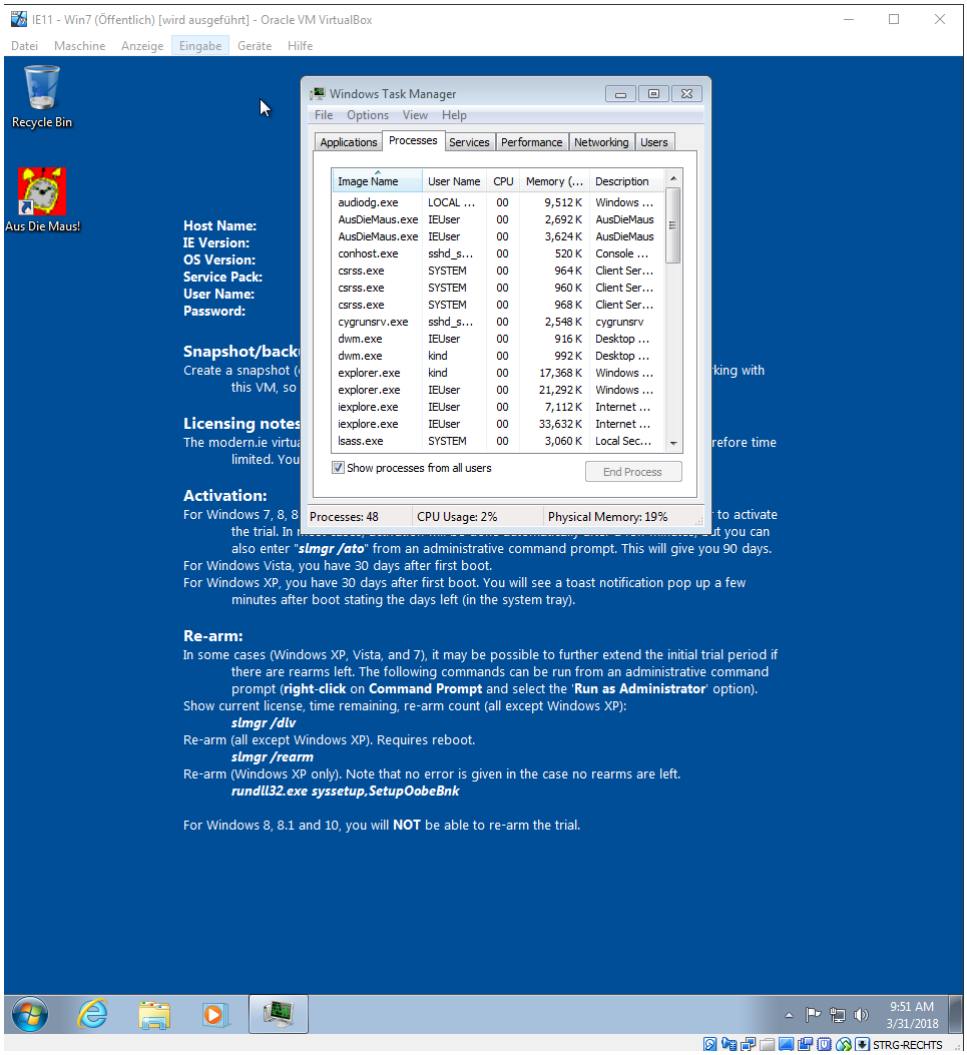

Abbildung 5.27: Ergebnis des Umgehungsszenarios "Prozess beenden" - Aus die Maus!

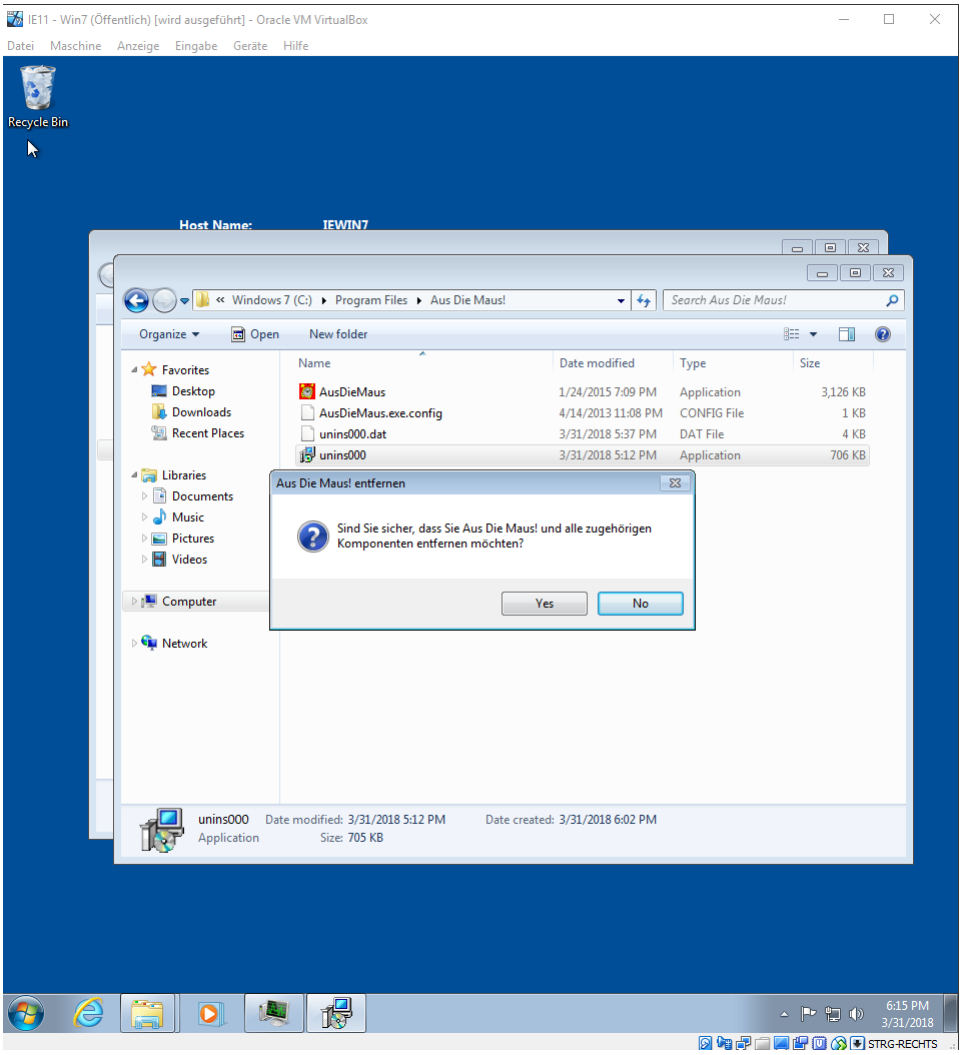

Abbildung 5.28: Ergebnis des Umgehungsszenarios ""Essentielle Dateien der Kinderschutzsoftware umbenennen/löschen" - Aus die Maus!

6 Ergebnisse aus dem Praxistest und den Umgehungsszenarien unter Android 7.1.1 und iOS 11.1

Nachfolgend werden die Ergebnisse aus dem Praxistest aufgeführt. Dabei wurden fünf Anwendungen unter Android 7.1.1 und fünf Anwendungen unter iOS 11.1 getestet.

Qustodio 180.23.1 - Praxistestkatalog – iOS 11.1			
Kriterium	**Beschreibung des Bewertungskriteriums**	**Kritikalität**	**Punkte**
1. Anrufe von Dritten blockieren	Qustodio bietet zwar die Funktionalität Anrufe zu überwachen und zu blockieren, jedoch nur unter Android	Hoch	0
2. Ausführung von spezifischen Dateitypen blockieren	Die Software kann keine spezifischen Dateitypen blockieren.	Mittel	0
3. Beratungsfunktion	Die Software gibt Eltern keine Hilfestellung bei der Einführung einer Kinderschutzsoftware.	Niedrig	0
4. Datenübertragung über Lightning Connector / USB blockieren	Die Software kann keine Datenübertragungen über den USB-Port / Lightning Connector blockieren.	Niedrig	0
5. Deinstallationsschutz	Die Anwendung beschreibt im Einrichtungsassistenten nicht, dass der in iOS integrierte „Einschränkungen“-Modus verwendet werden sollte, um eine Löschung der App zu verhindern. Somit ist kein Deinstallationsschutz gegeben.	Hoch	0
6. Einrichtungsassistent	Der Einrichtungsassistent ist einfach aufgebaut und wird detailliert erläutert. Zudem gibt es das sogenannte „Help Center“, welches eine Sammlung an abrufbaren Informationen zu dem Programm bietet.	Mittel	1
7. Installation	Die Installation ist einfach durchführbar und weist keine Komplexität auf.	Niedrig	1

Kriterium	Beschreibung des Bewertungskriteriums	Kritikalität	Punkte
8. Kategoriefilter Apps	Die Software bietet keinen variablen Kategoriefilter an.	Hoch	0
9. Kategoriefilter Web	Der Kategoriefilter unter Qustodio erlaubt eine feingranulare Auswahl von Themen, welche blockiert, erlaubt oder mit einer Warnung versehen werden sollen. Ebenso lassen sich Websites, die in keine der Kategorien fallen, automatisch blockieren.	Hoch	1
10. Loggingfunktion	Die Software bietet eine Loggingfunktion an, welche relevante Informationen protokolliert und speichert.	Hoch	0,75
11. SMS von Dritten blockieren	Das Empfangen von SMS kann nicht gesperrt werden.	Hoch	0
12. Soziale Netzwerke	Facebook kann mittels Qustodio überwacht werden, jedoch muss sich das Kind in den entsprechenden Account einloggen und die Qustodio-Anwendung akzeptieren.	Mittel	1
13. Spamfilter für Maildienste	Die Software hat keinen Spamfilter integriert.	Niedrig	0
14. Sperren von Apps	Spezifische Apps können nach der ersten Ausführung blockiert werden.	Hoch	0,75
15. Sperren von Websites	Das Definieren von Ausnahmen und expliziten Sperren ist mit der Anwendung möglich.	Hoch	1

Kriterium	Beschreibung des Bewertungskriteriums	Kritikalität	Punkte
16. Store-Blocker	Mittels der Anwendungsregeln kann der App-Store blockiert werden.	Mittel	1
17. Suchmaschine	Die Anwendung bietet die Option „SafeSearch“ automatisch zu aktivieren.	Mittel	0,5
18. Verwaltung im Web	Die Anwendung kann über eine Weboberfläche verwaltet werden.	Mittel	1
19. Zeitbeschränkung	Qustodio erlaubt es, einen Wochenplan mit entsprechenden Uhrzeiten zu erstellen, an welchen das Gerät genutzt werden darf. Ebenso lässt sich ein Zeitguthaben einstellen, welches beliebig pro Tag eingesetzt werden kann. Außerdem ist die Art der Sperre des Gerätes (nur Online-Sperre oder Sperren des gesamten Gerätes) möglich.	Hoch	1
Gesamtbewertung	**Hoch 4,5x3 + Mittel 4,5x2 + Niedrig 1x1 = 23,5 / 43**		

Tabelle 6.1: Ergebnis - Qustodio - Praxistestkatalog

Qustodio - Umgehungsszenarien – iOS 11.1		
Szenario	**Beschreibung**	**Bewertung**
Änderung der Systemzeit	Das Datum sowie die Uhrzeit können zwar geändert werden, was jedoch keinen Einfluss auf die Zeitkontofunktionalität hat.	Bestanden
Anonymisierender Webproxy	Alle fünf Web-Proxy-Dienste wurden blockiert.	Bestanden
Anwendung beenden	Die App kann nicht über den Taskmanager beendet werden, da es sich dabei um eine VPN Verbindung sowie einem konfigurierten MDM-Profil handelt. Auch bei einem Neustart und einem direkten Start des Browsers sowie dem Ansurfen einer normalerweise blockierten URL, greift die Kindersicherung weitergehend.	Bestanden
App löschen	**Die Anwendung kann einfach deinstalliert und das MDM-Profil sowie der eingerichtete VPN gelöscht werden.**	**Nicht bestanden**
Bruteforce-Angriff	**Der Login zum Eltern-Dashboard kann via eines Bruteforce-Angriffs geknackt werden, da die Anwendung die fehlgeschlagenen Loginversuche nicht mitloggt und auch keine Warnung an das Elternteil per E-Mail oder SMS versendet.**	**Nicht bestanden**
SafeSearch oder Kindersuchmaschine	**In allen drei Suchmaschinen kann SafeSearch deaktiviert und nach anstößigen Inhalten gesucht werden. Entsprechende Ergebnisse werden nicht gefiltert und an das Kind bzw. den Jugendlichen zurückgegeben.**	**Nicht bestanden**
Wayback Machine	**Die Wayback-Machine wird nicht blockiert und es ist ein Zugriff auf Snapshots von normalerweise gesperrten Websites möglich.**	**Nicht bestanden**
Gesamtbewertung	**4 (57,14%) von 7 Szenarien wurden nicht bestanden.**	

Tabelle 6.2: Ergebnis - Qustodio - Umgehungsszenarien

6.0.1 Fazit - Qustodio

Die Erstplatzierte mobile Kindersicherung der Vorauswahl erreicht nur 23,5 von 43 möglichen Punkten im Praxistestkatalog und hat insgesamt 4 von 7 Umgehungsszenarien nicht bestanden. Entsprechend schwach zeigt sich die Anwendung hinsichtlich des Schutzes vor einer Deinstallation, da die App samt Einstellungen nicht geschützt wird und auch nicht darauf hingewiesen wird, dass der "Einschränkungen"-Modus des iOS Betriebssystems verwendet werden sollte. Außerdem zeigt sich auch hier ein bekanntes Bild von den Kindersicherungen unter Windows:

- Ein Bruteforce-Angriff auf die Login-Credentials ist ohne Weiteres möglich, da keine Loginversuche mitgeloggt oder die Eltern gewarnt werden.
- SafeSearch ist äußerst einfach in den alternativen Suchmaschinen deaktivierbar.
- Die Wayback-Machine erlaubt einen ungefilterten Zugriff auf die Snapshots von gesperrten Websites.

Nachfolgend finden sich auszugsweise Screenshots aus den genannten sowie erfolgreichen Umgehungsszenarien:

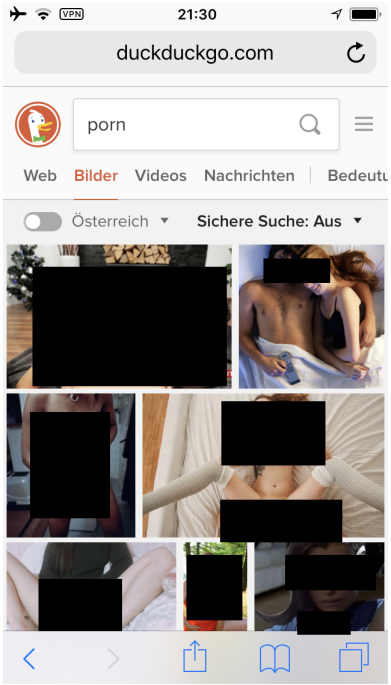

Abbildung 6.1: Ergebnis des Umgehungsszenarios "SafeSearch oder Kindersuchmaschine"

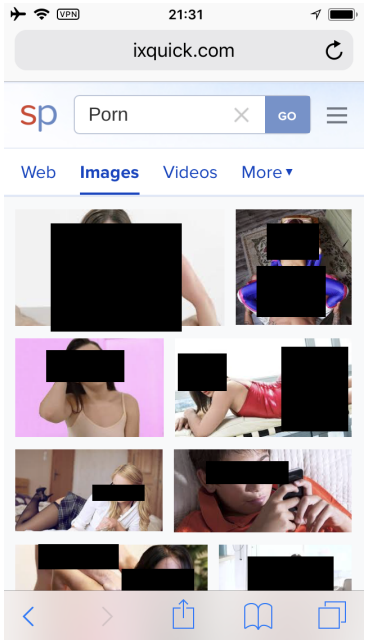

Abbildung 6.2: Ergebnis des Umgehungsszenarios "SafeSearch oder Kindersuchmaschine"

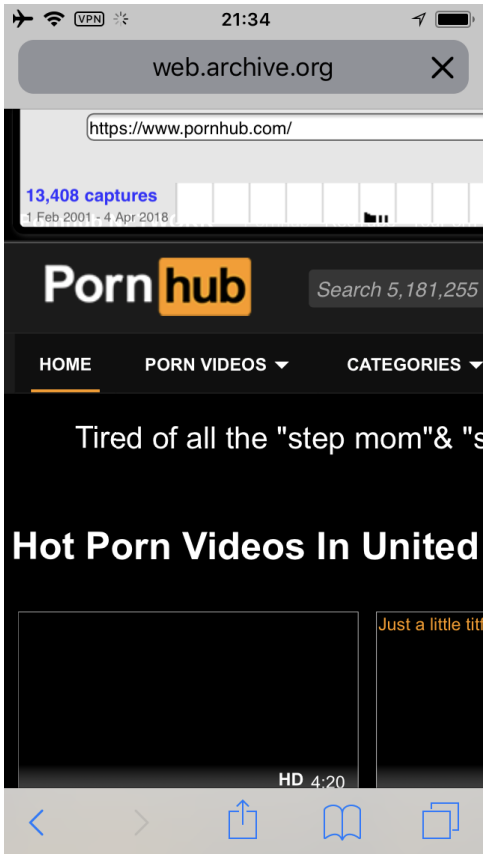

Abbildung 6.3: Ergebnis des Umgehungsszenarios "Wayback Machine"

Norton Family 1.7.1 - Praxistestkatalog – iOS 11.1			
Kriterium	**Beschreibung des Bewertungskriteriums**	**Kritikalität**	**Punkte**
1. Anrufe von Dritten blockieren	Das Empfangen von Anrufen kann nicht gesperrt werden.	Hoch	0
2. Ausführung von spezifischen Dateitypen blockieren	Die Software kann keine spezifischen Dateitypen blockieren.	Mittel	0
3. Beratungsfunktion	Die Software gibt Eltern keine Hilfestellung bei der Einführung einer Kinderschutzsoftware.	Niedrig	0
4. Datenübertragung über Lightning Connector / USB blockieren	Die Software kann keine Datenübertragungen über den USB-Port / Lightning Connector blockieren.	Niedrig	0
5. Deinstallationsschutz	Die App weist darauf hin, dass der „Einschränkungen“-Modus verwendet werden soll, um die App zu schützen.	Hoch	1
6. Einrichtungsassistent	Die App bietet zahlreiche Hilfestellungen und der Einrichtungsassistent erweist sich als unkompliziert und vielseitig.	Mittel	1
7. Installation	Insgesamt war eine hohe Verständlichkeit der Angaben durch die Software während der Installation gegeben. Die Komplexität ist, bedingt durch den wertvollen Einrichtungsassistenten, äußerst niedrig.	Niedrig	1
8. Kategoriefilter Apps	Die Anwendung bietet keinen Kategoriefilter für Apps unter iOS an.	Hoch	0

Kriterium	Beschreibung des Bewertungskriteriums	Kritikalität	Punkte
9. Kategoriefilter Web	Der Kategoriefilter Web, ist äußerst extensiv gehalten worden, da jener 27 einzeln an- oder abwählbare Kategorien umfasst.	Hoch	1
10. Loggingfunktion	Über das Dashboard der Anwendung kann ein detailliertes Logging hinsichtlich besuchter Websites und verbrachter Zeit mit dem Smartphone abgerufen werden.	Hoch	0,75
11. SMS von Dritten blockieren	Eine Überwachung von SMS ist nur in den USA, in Kanada und in Großbritannien möglich.	Hoch	0
12. Soziale Netzwerke	Soziale Netzwerke können unter iOS nicht überwacht werden, sondern nur unter Windows.	Mittel	0
13. Spamfilter für Maildienste	Die Software hat keinen Spamfilter integriert.	Niedrig	0
14. Sperren von Apps	Apps lassen sich unter iOS nicht über die Anwendung sperren. Das Feature wird nur unter Android unterstützt.	Hoch	0
15. Sperren von Websites	Websites lassen sich entweder explizit einer Whitelist oder einer Blacklist hinzufügen.	Hoch	1
16. Store-Blocker	Die Software bietet keine Funktionalität Downloads aus dem Apple App-Store / Google Play Store zu blockieren.	Mittel	0
17. Suchmaschine	Die Anwendung unterstützt eine SafeSearch Funktionalität für gängige Suchmaschinenanbieter wie Google, bing oder Yahoo!	Mittel	0,5

Kriterium	Beschreibung des Bewertungskriteriums	Kritikalität	Punkte
18. Verwaltung im Web	Die Software erlaubt eine Verwaltung der Kinderschutzsoftware auf einem oder mehreren Endgeräten über ein Onlinekonto und den Login in eine Weboberfläche.	Mittel	1
19. Zeitbeschränkung	Über das Dashboard lassen sich pro Tag Uhrzeiten einstellen, an welchen das Smartphone verwendet werden darf und ebenso wie lange.	Hoch	1
Gesamtbewertung	**Hoch 4,75x3 + Mittel 2,5x2 + Niedrig 1x1 = 20,25 / 43**		

Tabelle 6.3: Ergebnis - Norton Family - Praxistestkatalog

Norton Family - Umgehungsszenarien – iOS 11.1		
Szenario	**Beschreibung**	**Bewertung**
Änderung der Systemzeit	**Auf dem iOS-Testgerät funktioniert die Zeitkontofunktionalität nicht. Trotz dem Sperren eines ganzen Tages, greift die Beschränkung nicht und somit ist diese Funktionalität nicht gegeben.**	**Nicht bestanden**
Anonymisierender Webproxy	Normalerweise werden alle fünf Web-Proxy-Dienste gesperrt, **aber die Norton Browser App hat hierbei scheinbar einen Bug: Über den „Zurück"-Button lässt sich die normalerweise gesperrte Website manchmal anzeigen. Hierbei zeigt sich, dass der Web-Schutz nicht ordentlich funktioniert.**	**Nicht bestanden**
Anwendung beenden	Die Sicherheit der App liegt dabei im Verwenden des „Einschränkungen"-Modus von iOS. Dabei wurde die Option „App löschen" deaktiviert sowie ein Alterslimit für Apps von 7 Jahren definiert, welches verhindern soll, dass ein ungefilterter Browser am Gerät installiert wird. Faktisch sind ungefilterte Browser erst ab 17 Jahren im App Store verfügbar. Da für den Zugang in den „Einschränkungen"-Modus ein vierstelliger PIN-Code nötig ist, ist ein Beenden dieses Modus nicht möglich.	Bestanden
App löschen	Bedingt durch den Hinweis während der Einrichtung, dass die Kindersicherung mittels der Deaktivierung der „App löschen" Funktionalität geschützt wird, ist das Entfernen nicht möglich.	Bestanden
Bruteforce-Angriff	Ab sechs Versuchen sich in das Norton-Online Konto einzuloggen, wird ein Captcha aktiviert um einen automatisierten Bruteforce-Angriff zu unterbinden. Ebenso wird, wenn es ein weiteres Mal versucht wird, sich in das Konto einzuloggen, das Konto selbst für eine Stunde gesperrt, was weiterführend zu einer Warnung per E-Mail führt.	Bestanden
SafeSearch oder Kindersuchmaschine	**Bei allen drei Suchmaschinen kann SafeSearch deaktiviert und nach entsprechend anstößigen Inhalten gesucht werden. Entsprechend anstößige Ergebnisse werden an den Anwender zurückgeliefert.**	**Nicht bestanden**
Wayback Machine	Web.archive.org wird durch Norton Family als Web-Proxy erkannt und blockiert.	Bestanden
Gesamtbewertung	**3 (42,86%) von 7 Szenarien wurden nicht bestanden.**	

Tabelle 6.4: Ergebnis - Norton Family - Umgehungsszenarien

6.0.2 Fazit - Norton

Als Zweitplatzierte mobile Kindersicherung der Vorauswahl hat die Anwendung insgesamt 20,25 von 43 möglichen Punkten im Praxistestkatalog erreicht und nur 3 von 7 Umgehungsszenarien nicht bestanden. Trotz dessen ist die Wirksamkeit des Webfilters äußerst fraglich, da sich jene mittels des "Zurück"-Buttons des Browsers zum Teil aushebeln ließ.

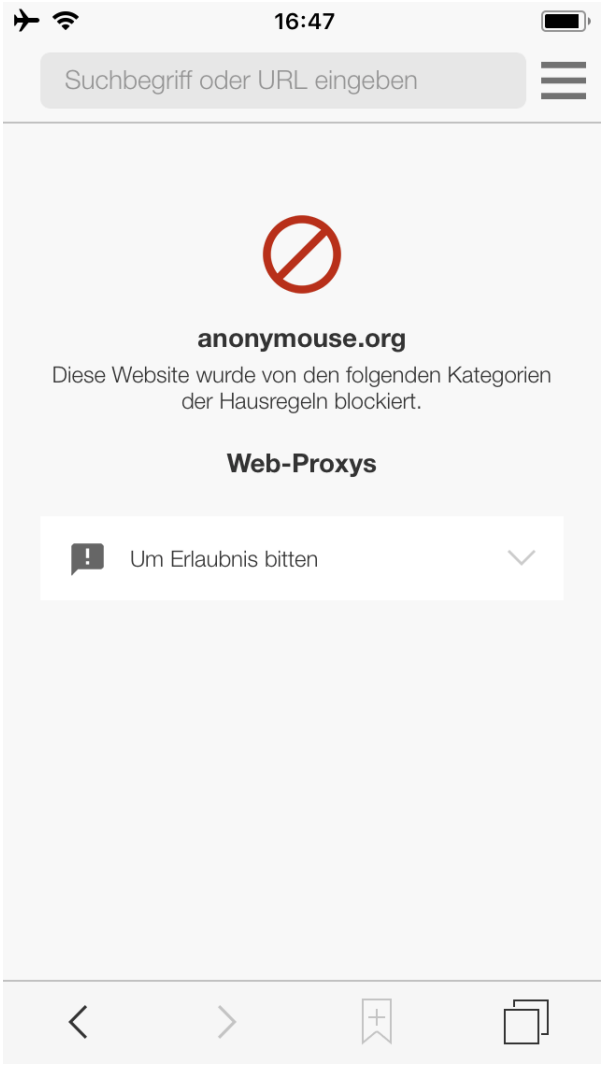

Abbildung 6.4: Anonymouse.org wird im Normalfall blockiert

Abbildung 6.5: Der Webfilter ließ sich mittels des "Zurück-Buttons" aushebeln

Außerdem konnte man die SafeSearch Funktionalität in allen getesteten alternativen Suchmaschinen deaktivieren.

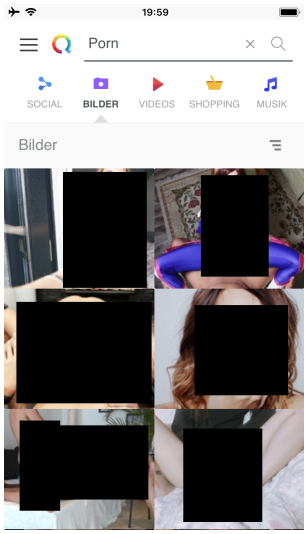

Abbildung 6.6: Ergebnis des Umgehungsszenarios "SafeSearch oder Kindersuchmaschine"

F-Secure SAFE 17.3.241201 - Praxistestkatalog – iOS 11.1			
Kriterium	**Beschreibung des Bewertungskriteriums**	**Kritikalität**	**Punkte**
1. Anrufe von Dritten blockieren	Das Empfangen von Anrufen kann nicht gesperrt werden.	Hoch	0
2. Ausführung von spezifischen Dateitypen blockieren	Die Software kann keine spezifischen Dateitypen blockieren.	Mittel	0
3. Beratungsfunktion	Die App weist darauf hin, dass man zumindest mit seinen Kindern über die Einführung der Kindersicherung sprechen sollte.	Niedrig	1
4. Datenübertragung über Lightning Connector / USB blockieren	Die Software kann keine Datenübertragungen über den USB-Port / Lightning Connector blockieren.	Niedrig	0
5. Deinstallationsschutz	F-Secure SAFE weist darauf hin, dass die App mittels des „Einschränkungen“-Modus geschützt werden soll.	Hoch	1
6. Einrichtungsassistent	Der Assistent ist selbsterklärend und weist auf die gegebenen Features hin.	Mittel	0,75
7. Installation	Die Installation ist einfach durchführbar und weist keine Komplexität auf.	Niedrig	1
8. Kategoriefilter Apps	Die App bietet keinen variablen Kategoriefilter an.	Hoch	0
9. Kategoriefilter Web	Die Anwendung bietet 15 verschiedene Kategoriefilter, welche an- oder abgewählt werden können.	Hoch	1
10. Loggingfunktion	Die Software bietet keine Loggingfunktion an.	Hoch	0

Kriterium	Beschreibung des Bewertungskriteriums	Kritikalität	Punkte
11. SMS von Dritten blockieren	Das Empfangen von SMS kann nicht gesperrt werden.	Hoch	0
12. Soziale Netzwerke	Die Software bietet keine spezifischen Funktionalitäten hinsichtlich sozialer Netzwerke.	Mittel	0
13. Spamfilter für Maildienste	Die Software hat keinen Spamfilter integriert.	Niedrig	0
14. Sperren von Apps	Die Software kann keine spezifischen Anwendungen blockieren.	Hoch	0
15. Sperren von Websites	Die Software kann keine spezifischen Websites sperren.	Hoch	0
16. Store-Blocker	Die Software bietet keine Funktionalität Downloads aus dem Apple App-Store / Google Play Store zu blockieren.	Mittel	0
17. Suchmaschine	Die Software beschränkt Suchmaschinen nicht und bietet auch keine Safe Search Funktion an.	Mittel	0
18. Verwaltung im Web	Die Software erlaubt eine Verwaltung der Kinderschutzsoftware auf einem oder mehreren Endgeräten über ein Onlinekonto und den Login in eine Weboberfläche.	Mittel	1
19. Zeitbeschränkung	Es kann ein Zeitplan mit der täglichen Gerätenutzung sowie komplementär dazu die sogenannte „Schlafenszeit“ definiert werden, welche das Gerät zu bestimmten Zeiten sperrt.	Hoch	1
Gesamtbewertung	**Hoch 3x3 + Mittel 1,75x2 + Niedrig 2x1 = 14,5 / 43**		

Tabelle 6.5: Ergebnis - F-Secure SAFE - Praxistestkatalog

F-Secure SAFE - Umgehungsszenarien – iOS 11.1		
Szenario	**Beschreibung**	**Bewertung**
Änderung der Systemzeit	**Die Zeitkontofunktionalität lässt sich durch die Änderung der Uhrzeit umgehen. Das heißt: wenn beispielsweise eine Schlafenszeit von 21:00 bis 07:00 definiert wurde und es im Moment 21:01 ist, schließt sich die App automatisch und lässt sich nicht mehr öffnen. Nun muss nur die Uhrzeit umgestellt werden und schon lässt sich die App abermals verwenden.**	**Nicht bestanden**
Anonymisierender Webproxy	Alle fünf Webproxy-Dienste werden automatisch blockiert.	Bestanden
Anwendung beenden	Das Beenden der App funktioniert zwar, stoppt dabei jedoch nur Um einen ungefilterten Browser zu installieren, muss man auf den „Einschränkungen“-Modus gelangen, welcher durch eine vierstellige PIN gesichert ist.	Bestanden
App löschen	Das Löschen der App ist zwar möglich, jedoch hat man darauffolgend keinen Browser mehr, um zu surfen. Ebenso ist die Funktionalität „App löschen“ über den „Einschränkungen“-Modus blockierbar.	Bestanden
Bruteforce-Angriff	Nach sieben Versuchen wird ein Captcha aktiviert, welches dazu führt, dass automatisierte Angriffe zwar blockiert werden, **ein manueller Angriff ist jedoch weiterhin möglich**. **Ebenso wird ein Elternteil darauffolgend nicht über die vielen fehlgeschlagenen Loginversuche informiert.**	**Nicht bestanden**
SafeSearch oder Kindersuchmaschine	**Man kann auf jede der drei alternativen Suchmaschinen zugreifen und SafeSearch deaktivieren. Weiterführend werden bei anstößigen Suchbegriffen auch anstößige Inhalte an den Benutzer zurückgeliefert.**	**Nicht bestanden**
Wayback Machine	**Ein Zugriff auf normalerweise blockierte Websites über die Wayback-Machine ist ohne Weiteres möglich.**	**Nicht bestanden**
Gesamtbewertung	**4 (57,14%) von 7 Szenarien wurden nicht bestanden.**	

Tabelle 6.6: Ergebnis - F-Secure SAFE - Umgehungsszenarien

6.0.3 Fazit - F-Secure

Der Drittplatzierte in der Vorauswahl erreichte 14,5 von 43 möglichen Punkten im Praxistestkatalog und hat insgesamt 4 von 7 Umgehungsszenarien nicht bestanden. Erstaunlich ist, dass es sich hierbei um die erste Anwendung im Allgemeinen handelt, welche am Szenario "Änderung der Systemzeit" gescheitert ist. Hierbei ließ sich die Zeitkontofunktion äußerst leicht aushebeln, indem man nur die Uhrzeit und/oder das Datum am Gerät änderte.

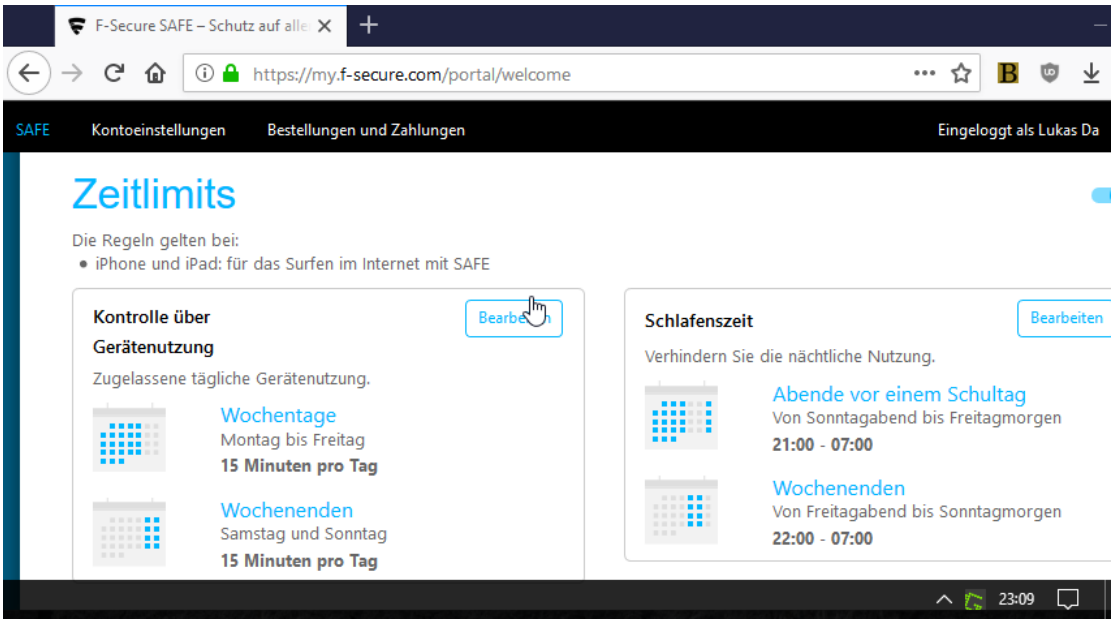

Abbildung 6.7: Zeitkonto-Einstellungen hinsichtlich "Schlafenszeit" und aktuelle sowie korrekte Systemzeit

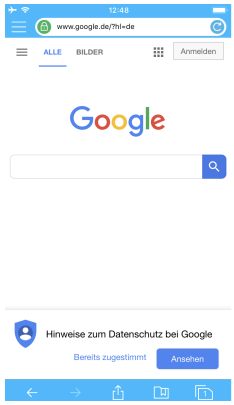

Abbildung 6.8: Änderung der Uhrzeit am Gerät führt zu funktionierendem Browser trotz aktiver "Schlafenszeit"

Ein Auszug an Screenshots aus den weiteren erfolgreichen Umgehungsszenarien findet sich nachfolgend:

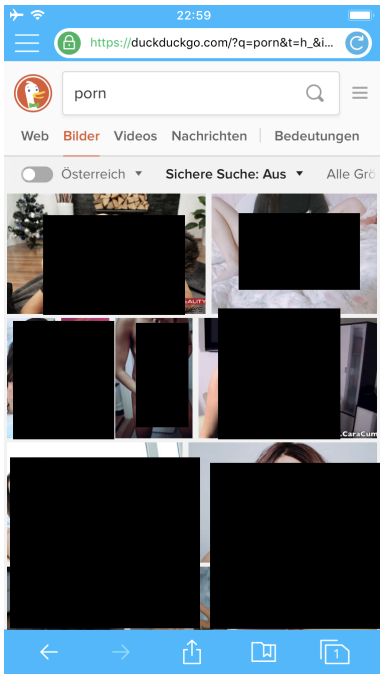

Abbildung 6.9: Ergebnis des Umgehungsszenarios "SafeSearch oder Kindersuchmaschine"

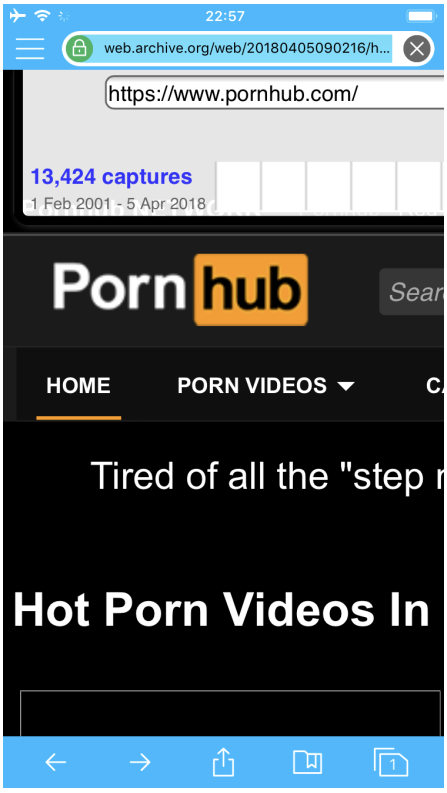

Abbildung 6.10: Ergebnis des Umgehungsszenarios "Wayback Machine"

Mobicip 4.8 - Praxistestkatalog – iOS 11.1			
Kriterium	**Beschreibung des Bewertungskriteriums**	**Kritikalität**	**Punkte**
1. Anrufe von Dritten blockieren	Das Empfangen von Anrufen kann nicht gesperrt werden.	Hoch	0
2. Ausführung von spezifischen Dateitypen blockieren	Die Software kann keine spezifischen Dateitypen blockieren.	Mittel	0
3. Beratungsfunktion	Die Software gibt Eltern keine Hilfestellung bei der Einführung einer Kinderschutzsoftware.	Niedrig	0
4. Datenübertragung über Lightning Connector / USB blockieren	Die Software kann keine Datenübertragungen über den USB-Port / Lightning Connector blockieren.	Niedrig	0
5. Deinstallationsschutz	Es wird darauf hingewiesen, dass der „Einschränkungen“-Modus und die Einstellungen „Apps löschen“, „Apps installieren“ und „Safari“ deaktiviert werden sollen. Somit ist ein Schutz der Anwendung gegeben.	Hoch	1
6. Einrichtungsassistent	Die Funktionalitäten der App werden im Detail erläutert.	Mittel	0,75
7. Installation	Direkt nach der Erstellung eines Accounts und dem Login wird darauf verwiesen, dass der „Einschränkungen“-Modus aktiviert werden soll. Weiterführend ist die Installation äußerst einfach und nicht komplex.	Niedrig	1
8. Kategoriefilter Apps	Apps können selbst in der Premiumversion nicht nach Kategorien gefiltert werden.	Hoch	0

Kriterium	Beschreibung des Bewertungskriteriums	Kritikalität	Punkte
9. Kategoriefilter Web	Der Filter basiert auf drei verschiedenen Filterarten (Strict, Moderate und Mature) die eingestellt werden können. In der Premium-Version ist ein feingranulares Filtern möglich.	Hoch	1
10. Loggingfunktion	In der Premium-Version wird detailliertes Logging über besuchte und/oder blockierte Websites geboten.	Hoch	0,75
11. SMS von Dritten blockieren	Das Empfangen von SMS kann nicht gesperrt werden.	Hoch	0
12. Soziale Netzwerke	Die Software bietet keine spezifischen Funktionalitäten hinsichtlich sozialer Netzwerke.	Mittel	0
13. Spamfilter für Maildienste	Die Software hat keinen Spamfilter integriert.	Niedrig	0
14. Sperren von Apps	Spezifische Apps können nach der Installation am Gerät blockiert werden. Dafür muss jedoch die Premium-Version verwendet werden.	Hoch	0,75
15. Sperren von Websites	In der Premium-Version können Websites blockiert werden.	Hoch	1
16. Store-Blocker	Der App-Store kann über die entsprechende „Sperren von Apps“-Funktionalität blockiert werden.	Mittel	1
17. Suchmaschine	Die Software beschränkt Suchmaschinen nicht und bietet auch keine Safe Search Funktion an.	Mittel	0

Kriterium	Beschreibung des Bewertungskriteriums	Kritikalität	Punkte
18. Verwaltung im Web	Die Software erlaubt eine Verwaltung der Kinderschutzsoftware auf einem oder mehreren Endgeräten über ein Onlinekonto und den Login in eine Weboberfläche.	Mittel	1
19. Zeitbeschränkung	Es lassen sich pro Tag entsprechende Uhrzeiten definieren wo das Internet für das Gerät blockiert wird.	Hoch	1
Gesamtbewertung	**Hoch 5,5x3 + Mittel 2,75x2 + Niedrig 1x1 = 23 / 43**		

Tabelle 6.7: Ergebnis - Mobicip - Praxistestkatalog

Mobicip - Umgehungsszenarien – iOS 11.1		
Szenario	**Beschreibung**	**Bewertung**
Änderung der Systemzeit	***Da die Funktionalität nur mittels Premium-Modus testbar ist, wird hier keine Bewertung vorgenommen***	***Nicht anwendbar***
Anonymisierender Webproxy	Der Zugriff auf 3 von 5 Webproxies, nämlich hide.me, hidester.com und kproxy.com, war möglich, jedoch konnte man sich nicht auf eine gesperrte Website verbinden.	Bestanden
Anwendung beenden	Ein Beenden der App ist in diesem Sinne nicht möglich, da es sich dabei um den Browser selbst handelt. Wenn dieser beendet wird, ist auch kein Zugriff mehr auf das Web möglich, da der Safari-Browser bereits am Anfang über den „Einschränkungen“-Modus blockiert wurde.	Bestanden
App löschen	Ein Löschen der Anwendung ist nicht möglich, da der „Einschränkungen“-Modus aktiv ist und „App löschen“ deaktiviert wurde.	Bestanden
Bruteforce-Angriff	**Nach 10 fehlgeschlagenen Versuchen kann man sich weiterhin in die Weboberfläche einloggen. Das Elternteil wird in diesem Falle weder darauf hingewiesen noch davor gewarnt, dass jemand versucht hat sich mehrere Male in den Account einzuloggen**	**Nicht bestanden**
SafeSearch oder Kindersuchmaschine	SafeSearch kann zwar deaktiviert werden und der Zugriff ist nur auf qwant und duckduckgo möglich, jedoch wird bei der Suche nach „Porn“ automatisch die Website blockiert. **Dementsprechend wurde der Suchbegriff auf „Po rn Se x“ abgeändert, was jedoch nur bei duckduckgo zu entsprechenden anstößigen Inhalten geführt hat.**	**Nicht bestanden**
Wayback Machine	Der Zugriff auf web.archive.org ist zwar möglich, jedoch werden blockierte Websites weiterhin gesperrt.´	Bestanden
Gesamtbewertung	**2 (33,33%) von 6 Szenarien wurden nicht bestanden. 1 Szenario war nicht anwendbar.**	

Tabelle 6.8: Ergebnis - Mobicip - Umgehungsszenarien

6.0.4 Fazit - Mobicip

Als äußerst robust zeigte sich die App "Mobicip", welche sich im Mittelfeld von Android- und iOS-Programmen in der Vorauswahl befand. Im Praxistestkatalog erreichte die Anwendung 23 von möglichen 43 Punkten und hat insgesamt nur 2 von 6 Umgehungsszenarien nicht bestanden. 1 Umgehungsszenario war nicht testbar, da die Zeitkontofunktionalität nur in der Premium-Version verfügbar war und man diese nicht ohne Angabe einer Kreditkartennummer testen kann. Faktisch könnte ein Bruteforce-Angriff auf das Elternkonto Erfolg versprechen. Letztendlich war es jedoch nur möglich über eine der drei alternativen Suchmaschine sowie einer Abänderung des Suchbegriffes an anstößige Inhalte zu gelangen.

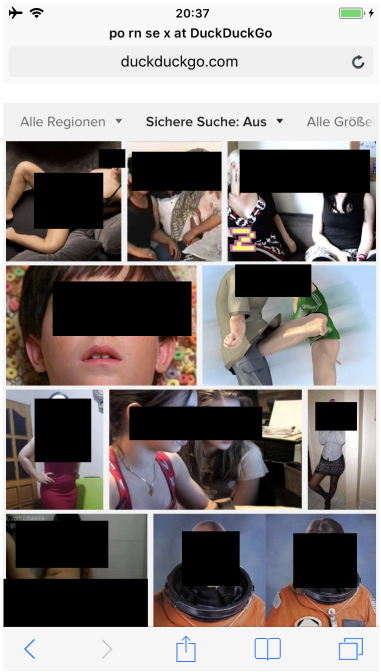

Abbildung 6.11: Ergebnis des Umgehungsszenarios "SafeSearch oder Kindersuchmaschine"

Safe Lagoon Parental Control 1.0.40 - Praxistestkatalog – iOS 11.1			
Kriterium	**Beschreibung des Bewertungskriteriums**	**Kritikalität**	**Punkte**
1. Anrufe von Dritten blockieren	Das Empfangen von Anrufen kann nicht gesperrt werden.	Hoch	0
2. Ausführung von spezifischen Dateitypen blockieren	Die Software kann keine spezifischen Dateitypen blockieren.	Mittel	0
3. Beratungsfunktion	Die Software gibt Eltern keine Hilfestellung bei der Einführung einer Kinderschutzsoftware.	Niedrig	0
4. Datenübertragung über Lightning Connector / USB blockieren	Die Software kann keine Datenübertragungen über den USB-Port / Lightning Connector blockieren.	Niedrig	0
5. Deinstallationsschutz	Auf den „Einschränkungen“-Modus wurde während der Installation nicht hingewiesen, wodurch kein Deinstallationsschutz gegeben ist.	Hoch	0
6. Einrichtungsassistent	Über den Einrichtungsassistenten wird alles im Detail erläutert. Aber die Übersetzung der Anwendung ins Deutsche ist teilweise sehr gewöhnungsbedürftig.	Mittel	0,75
7. Installation	Die Installation war insgesamt äußerst aufwändig, da sowohl unter iOS als auch an einem Rechner eine Anwendung installiert werden musste. Ebenso war es nötig für bestimmte Monitoring-Funktionen wie Youtube-Überwachung und iTunes entsprechende Accounts einzurichten und einzugeben. Zudem mussten bestimmte Features wie „Find my iPhone“ und „Device Management“ deaktiviert werden.	Niedrig	0

Kriterium	Beschreibung des Bewertungskriteriums	Kritikalität	Punkte
8. Kategoriefilter Apps	Die Anwendung besitzt keinen kategorischen Appblocker.	Hoch	0
9. Kategoriefilter Web	Safe Lagoon verfolgt einen äußerst interessanten Ansatz: Websites aus den Kategorien Pornografie, Suizid oder Abtreibung werden automatisch blockiert und lassen sich als Filter nicht deaktivieren. Darauffolgend sind noch weitere 12 Kategorien auswählbar, welche gesperrt werden können.	Hoch	1
10. Loggingfunktion	Die App loggt den Besuch von allen Websites sowie Anrufen und SMS.	Hoch	0,75
11. SMS von Dritten blockieren	Das Empfangen von SMS kann nicht gesperrt werden.	Hoch	0
12. Soziale Netzwerke	Die Anwendung unterstützt das Verbinden mit dem YouTube-, Instagram-, VK- und dem iCloud-Account des Kindes.	Mittel	1
13. Spamfilter für Maildienste	Die Software hat keinen Spamfilter integriert.	Niedrig	0
14. Sperren von Apps	Apps können nachdem jene von der Kindersicherung erkannt wurden, entweder komplett blockiert oder freigegeben werden. Ebenso lässt sich die Kategorie, welcher die Anwendung zugeordnet werden soll, auswählen.	Hoch	0,75

Kriterium	Beschreibung des Bewertungskriteriums	Kritikalität	Punkte
15. Sperren von Websites	Websites lassen sich über die Weboberfläche entweder explizit blockieren oder freigeben.	Hoch	1
16. Store-Blocker	Die Software bietet keine Funktionalität Downloads aus dem Apple App-Store zu blockieren.	Mittel	0
17. Suchmaschine	Die Software beschränkt Suchmaschinen nicht und bietet auch keine Safe Search Funktion an.	Mittel	0
18. Verwaltung im Web	Die Software erlaubt eine Verwaltung der Kinderschutzsoftware auf einem oder mehreren Endgeräten über ein Onlinekonto und den Login in eine Weboberfläche.	Mittel	1
19. Zeitbeschränkung	SafeLagoon erlaubt eine Zeitsperre betreffend bestimmter Apps, Kategorien oder dem Internetzugang. Zudem sind Wochentage und Uhrzeiten einstellbar, zu welchen der Zugriff ermöglicht wird. Ebenso gibt es die Option ein Zeitlimit pro Tag einzustellen.	Hoch	1
Gesamtbewertung	**Hoch 4,5x3 + Mittel 2,75x2 + Niedrig 0x1 = 19 / 43**		

Tabelle 6.9: Ergebnis - Safe Lagoon Parental Control - Praxistestkatalog

Safe Lagoon Parental Control - Umgehungsszenarien – iOS 11.1		
Szenario	**Beschreibung**	**Bewertung**
Änderung der Systemzeit	Die Änderung der Systemzeit beeinflusst die Funktionalität des Zeitkontos bzw. der Beschränkung von Apps nicht.	Bestanden
Anonymisierender Webproxy	**Der Zugriff auf kproxy.com war trotz aktiver Kindersicherung möglich.**	**Nicht bestanden**
Anwendung beenden	**Wenn die SafeLagoon Kindersicherungsapp angestartet und nachfolgend beendet wird, lassen sich über ein kurzes Zeitfenster normalerweise blockierte Websites ohne Weiteres aufrufen.**	**Nicht bestanden**
App löschen	**Da auf den „Einschränkungen“-Modus nicht hingewiesen wurde, lässt sich die App deinstallieren und es besteht kein Schutz.**	**Nicht bestanden**
Bruteforce-Angriff	**Nach zehn Versuchen sind weitere Logins möglich. Das Elternteil wird hierbei nicht über einen möglichen Bruteforce-Angriff durch das Kind informiert.**	**Nicht bestanden**
SafeSearch oder Kindersuchmaschine	**In allen drei alternativen Suchmaschinen lässt sich SafeSearch deaktivieren und man kann nach anstößigen Inhalten suchen und bekommt jene auch zurückgeliefert.**	**Nicht bestanden**
Wayback Machine	**Die Wayback Machine wird zuerst blockiert, jedoch sobald man auf den Refresh-Button drückt, wird die Website manchmal angezeigt. Weiterführend kann man auch auf andere blockierte Seiten zugreifen.**	**Nicht bestanden**
Gesamtbewertung	**6 (85,71%) von 7 Szenarien wurden nicht bestanden.**	

Tabelle 6.10: Ergebnis - Safe Lagoon Parental Control - Umgehungsszenarien

6.0.5 Fazit - Safe Lagoon

Die letzte zu testende App unter iOS, "Parental Control" von der Firma "Safe Lagoon", erreichte im Praxistestkatalog 23 von 43 möglichen Punkten, konnte jedoch 6 von 7 möglichen Umgehungsszenarien nicht bestehen. Äußerst verwunderlich war, dass der Webfilter nur sporadisch funktionierte und gesperrte Websites teilweise nach einer Aktualisierung im Browser anzeigte, wie die nachfolgenden Screenshots beweisen:

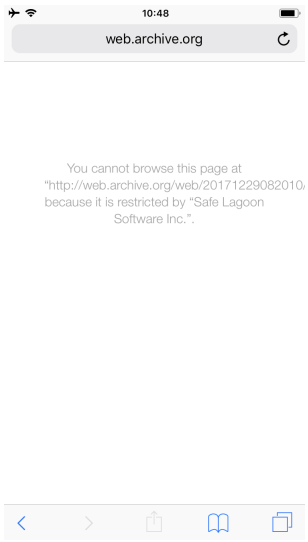

Abbildung 6.12: Website web.archive.org gesperrt

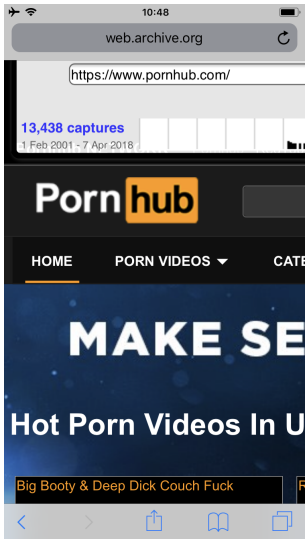

Abbildung 6.13: Durch einen Refresh im Browser war die Website plötzlich verfügbar und ein Zugriff auf Snapshots von blockierten Websites ebenso.

Zudem war äußerst interessant, dass ein Aufrufen und ein Beenden der App per Taskmanager dazu führte, dass der Webfilter für kurze Zeit ausfiel:

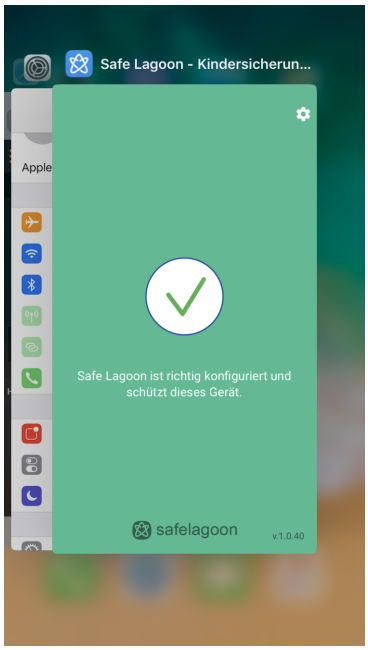

Abbildung 6.14: Ergebnis des Umgehungsszenarios "App beenden"

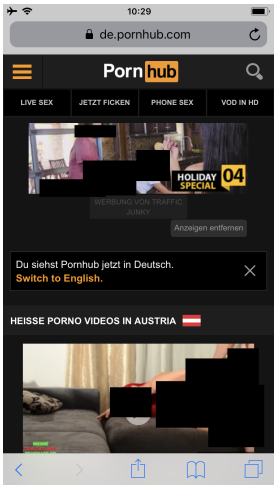

Abbildung 6.15: Ergebnis des Umgehungsszenarios "App beenden"

Whisper's Arts Kid's Shell 2.3.3 - Praxistestkatalog – Android 7.1.1			
Kriterium	**Beschreibung des Bewertungskriteriums**	**Kritikalität**	**Punkte**
1. Anrufe von Dritten blockieren	Das Empfangen von Anrufen kann nicht gesperrt werden.	Hoch	0
2. Ausführung von spezifischen Dateitypen blockieren	Die Software kann keine spezifischen Dateitypen blockieren.	Mittel	0
3. Beratungsfunktion	Die Software gibt Eltern keine Hilfestellung bei der Einführung einer Kinderschutzsoftware.	Niedrig	0
4. Datenübertragung über Lightning Connector / USB blockieren	Die Software kann keine Datenübertragungen über den USB-Port / Lightning Connector blockieren.	Niedrig	0
5. Deinstallationsschutz	Die Anwendung lässt sich nicht ohne das festgelegte Elternpasswort deinstallieren, wenn die Kid's Shell entsprechend eingerichtet wurde.	Hoch	1
6. Einrichtungsassistent	Die App bietet ein kurzes Tutorial, mit welchem sich die App einrichten lässt.	Mittel	0,75
7. Installation	Die Installation der App selbst ist einfach. Weiterführend können weitere Apps die zB. den Bereich des Browsings abdecken, heruntergeladen werden.	Niedrig	1
8. Kategoriefilter Apps	Die Software bietet keinen variablen App-Kategoriefilter an.	Hoch	0
9. Kategoriefilter Web	Die Software bietet keinen variablen Web-Kategoriefilter an.	Hoch	0
10. Loggingfunktion	Die Software bietet keine Loggingfunktion an.	Hoch	0
11. SMS von Dritten blockieren	Das Empfangen von SMS kann nicht gesperrt werden.	Hoch	0

Kriterium	Beschreibung des Bewertungskriteriums	Kritikalität	Punkte
12. Soziale Netzwerke	Die Software bietet keine spezifischen Funktionalitäten hinsichtlich sozialer Netzwerke.	Mittel	0
13. Spamfilter für Maildienste	Die Software hat keinen Spamfilter integriert.	Niedrig	0
14. Sperren von Apps	Apps müssen explizit erlaubt werden, um von dem Kind genutzt werden zu können.	Hoch	1
15. Sperren von Websites	Websites müssen manuell durch ein Elternteil hinzugefügt werden und nur jene können dann durch die Kinder besucht werden.	Hoch	1
16. Store-Blocker	Solange der Play-Store nicht explizit erlaubt wurde, ist jener gesperrt.	Mittel	1
17. Suchmaschine	Die Software beschränkt Suchmaschinen nicht und bietet auch keine Safe Search Funktion an.	Mittel	0
18. Verwaltung im Web	Die Software wird lokal verwaltet.	Mittel	0
19. Zeitbeschränkung	Es lassen sich Uhrzeiten eintragen, an welchen das Smartphone verwendet werden darf. Diese können beliebig oft erzeugt und entsprechend ausgedehnt werden.	Hoch	1
Gesamtbewertung	**Hoch 4x3 + Mittel 1,75x2 + Niedrig 1x1 = 16,5 / 43**		

Tabelle 6.11: Ergebnis - Whispers Arts Kids Shell - Praxistestkatalog

Whisper's Arts Kid's Shell - Umgehungsszenarien – Android 7.1.1		
Szenario	**Beschreibung**	**Bewertung**
Änderung der Systemzeit	Keine Änderung möglich, da der Zugriff auf die Einstellungen blockiert wird.	Bestanden
Anonymisierender Webproxy	Kein Zugriff möglich, da die Websites rein Whitelist-basierend sind.	Bestanden
Anwendung beenden	Sobald der Taskmanager geöffnet wird, wird ein Sperrbildschirm angezeigt. Unabhängig davon wie oft man auf diesen Button drückt oder man es schafft alle Apps zu schließen, startet sich die App abermals. Nach einem Neustart wird die App ebenso sofort mitgestartet und es ist kein Ausbrechen aus dem Kindermodus möglich.	Bestanden
App löschen	Die App kann nicht deinstalliert werden, da kein Zugriff auf die Einstellungen möglich ist. Beim Anschließen an den Rechner liegt das Problem darin, dass das Smartphone nicht den Datentransfermodus automatisch aktiviert. Im Kindermodus ist kein Zugriff auf diese Funktionalität möglich.	Bestanden
Bruteforce-Angriff	**Die Loginversuche werden nicht mitprotokolliert. Weiterführend können ohne Verzögerungen unterschiedlichste Passwortkombinationen ausprobiert werden.**	**Nicht bestanden**
SafeSearch oder Kindersuchmaschine	**Für dieses Testszenario wurde einfach Google explizit als Suchmaschine freigegeben um einen Zugriff drauf zu ermöglichen. Hierbei ist SafeSearch nicht aktiv und es kann nach entsprechend anstößigen Inhalten über die Bilder-Funktion gesucht werden.**	**Nicht bestanden**
Wayback Machine	Kein Zugriff möglich, da die Websites rein Whitelist-basierend sind.	Bestanden
Gesamtbewertung	**2 (28,57%) von 7 Szenarien wurden nicht bestanden.**	

Tabelle 6.12: Ergebnis - Whispers Arts Kids Shell - Umgehungsszenarien

6.0.6 Fazit - Whisper's Arts

Die Anwendung "Kid's Shell" von der Firma "Whisper's Arts" erhielt, bedingt durch die gegebene Funktionalität im Praxistestkatalog 16,5 von 43 möglichen Punkten. Fakt ist, dass bei dieser Anwendung zwar nur 2 von 7 Umgehungsszenarien erfolgreich waren, dies aber an der sehr starken Restriktion hinsichtlich Geräte- und Webnutzung für das Kind liegt. Gesurft werden kann nur auf explizit freigegebenen Websites. Apps müssen ebenso im Elternmodus aktiv freigegeben werden. Wenn ein Elternteil nun jedoch zum Beispiel Google als Suchmaschine freigibt, ist hier keine SafeSearch-Funktion aktiv, weshalb nach anstößigen Inhalten ohne Weiteres gesucht werden kann.

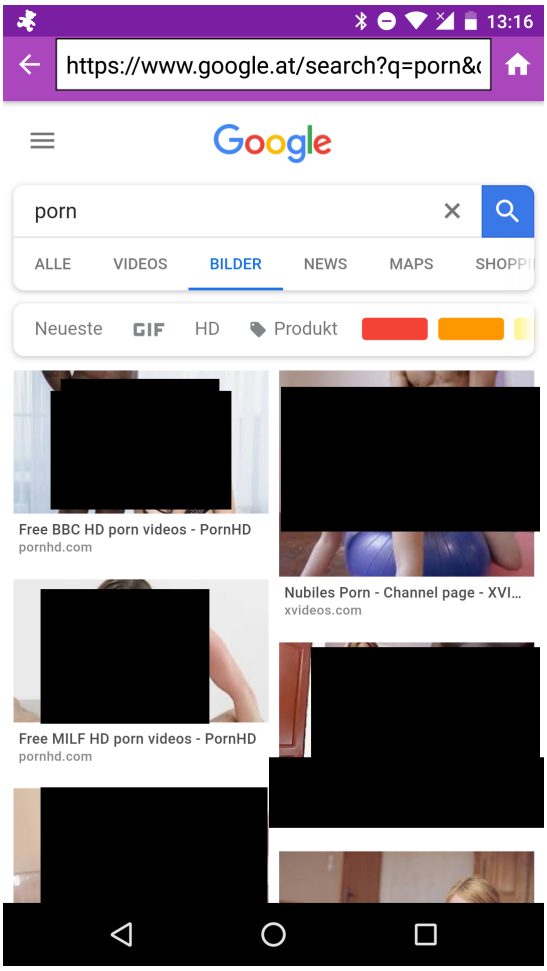

Abbildung 6.16: Ergebnis des Umgehungsszenarios "SafeSearch oder Kindersuchmaschine"

Avira AppLock+ 1.0.6 - Praxistestkatalog – Android 7.1.1			
Kriterium	**Beschreibung des Bewertungskriteriums**	**Kritikalität**	**Punkte**
1. Anrufe von Dritten blockieren	Das Empfangen von Anrufen kann nicht gesperrt werden.	Hoch	0
2. Ausführung von spezifischen Dateitypen blockieren	Die Software kann keine spezifischen Dateitypen blockieren.	Mittel	0
3. Beratungsfunktion	Die Software gibt Eltern keine Hilfestellung bei der Einführung einer Kinderschutzsoftware.	Niedrig	0
4. Datenübertragung über Lightning Connector / USB blockieren	Die Software kann keine Datenübertragungen über den USB-Port / Lightning Connector blockieren.	Niedrig	0
5. Deinstallationsschutz	Bevor die Software deinstalliert werden kann, muss eine entsprechende PIN eingegeben werden, um auf die Einstellungen zugreifen zu können.	Hoch	1
6. Einrichtungsassistent	Die Einrichtung erfolgt nach der Installation über ein selbsterläuterndes Tutorial. Alle relevanten Funktionalitäten werden im Detail erläutert.	Mittel	0,75
7. Installation	Die Installation ist einfach durchführbar und weist keine Komplexität auf.	Niedrig	1
8. Kategoriefilter Apps	Die Software bietet keinen variablen Kategoriefilter an.	Hoch	0
9. Kategoriefilter Web	Die Software bietet keinen variablen Kategoriefilter an.	Hoch	0
10. Loggingfunktion	Die Software bietet keine Loggingfunktion an.	Hoch	0

Kriterium	Beschreibung des Bewertungskriteriums	Kritikalität	Punkte
11. SMS von Dritten blockieren	Das Empfangen von SMS kann nicht gesperrt werden.	Hoch	0
12. Soziale Netzwerke	Die Software bietet keine spezifischen Funktionalitäten hinsichtlich sozialer Netzwerke.	Mittel	0
13. Spamfilter für Maildienste	Die Software hat keinen Spamfilter integriert.	Niedrig	0
14. Sperren von Apps	Anwendungen können mittels einer PIN versehen werden, welches die ungewünschte Ausführung vermeiden soll.	Hoch	0,75
15. Sperren von Websites	Die Software kann keine spezifischen Websites sperren.	Hoch	0
16. Store-Blocker	Der Play-Store kann als ganzheitliche Anwendung mit einem PIN versehen und somit blockiert werden.	Mittel	1
17. Suchmaschine	Die Software beschränkt Suchmaschinen nicht und bietet auch keine Safe Search Funktion an.	Mittel	0
18. Verwaltung im Web	Die Software wird lokal verwaltet.	Mittel	0
19. Zeitbeschränkung	Die Premium-Funktionalität „Zeitplan-Sperre“ ermöglicht es pro Tag Zeiträume zu definieren, zu welchen bestimmte Apps verwendet werden dürfen.	Hoch	1
Gesamtbewertung	**Hoch 2,75x3 + Mittel 1,75x2 + Niedrig 1x1 = 12,75 / 43**		

Tabelle 6.13: Ergebnis - Avira AppLock+ - Praxistestkatalog

Avira AppLock+ - Umgehungsszenarien – Android 7.1.1		
Szenario	**Beschreibung**	**Bewertung**
Änderung der Systemzeit	***Die Zeitkontofunktion ist ein Premium-Feature und nicht kostenlos. Somit kann dieses Umgehungsszenario nicht getestet werden.***	***Nicht anwendbar***
Anonymisierender Webproxy	**Die Anwendung besitzt keinen Webfilter, wodurch keine Umgehung nötig ist. Das Szenario gilt automatisch als „Nicht bestanden".**	**Nicht bestanden**
Anwendung beenden	Das Beenden der App über den Taskmanager beeinflusst die Funktionalität nicht. Die Kinderschutzanwendung kann möglicherweise beendet werden. **Jedoch ist nach einem Neustart die Anwendung nicht aktiv und es kann ohne PIN für einen kurzen Zeitraum auf jede App zugegriffen werden.**	**Nicht bestanden**
App löschen	**Die Anwendung kann nach einem Neustart entfernt werden, da die Anwendung zu spät startet. Ebenso lässt sich dies auch ohne Neustart durchführen, wenn man die App auf den „Deinstallieren"-Button zieht und dann schnell bei der auftretenden Meldung, ob man die Anwendung deinstallieren möchte, auf „Ja" klickt.**	**Nicht bestanden**
Bruteforce-Angriff	**Ein Bruteforce-Angriff ist ohne Weiteres möglich, da weder eine Zeitsperre bei zu vielen fehlgeschlagenen Versuchen aktiviert wird, noch eine Warnung an die hinterlegte E-Mail-Adresse versendet wird.**	**Nicht bestanden**
SafeSearch oder Kindersuchmaschine	**Die Anwendung besitzt keinen Webfilter, wodurch keine Umgehung nötig ist. Das Szenario gilt automatisch als „Nicht bestanden".**	**Nicht bestanden**
Wayback Machine	**Die Anwendung besitzt keinen Webfilter, wodurch keine Umgehung nötig ist. Das Szenario gilt automatisch als „Nicht bestanden".**	**Nicht bestanden**
Gesamtbewertung	**6 (100%) von 6 Szenarien wurden nicht bestanden. 1 Szenario waren nicht anwendbar.**	

Tabelle 6.14: Ergebnis - Avira AppLock+ - Umgehungsszenarien

6.0.7 Fazit - Avira

"AppLock+" von "Avira" erreichte 12,75 von 43 Punkten im Praxistestkatalog und hat 6 von 6 Umgehungsszenarien nicht bestanden. Das Szenario "Änderung der Systemzeit" konnte nicht getestet werden, da die Zeitkontofunktionalität kostenpflichtig war. Weiterführend war es möglich die App zu umgehen, indem man das Gerät neugestartet hat und direkt danach die normalerweise gesperrte App aufrief.

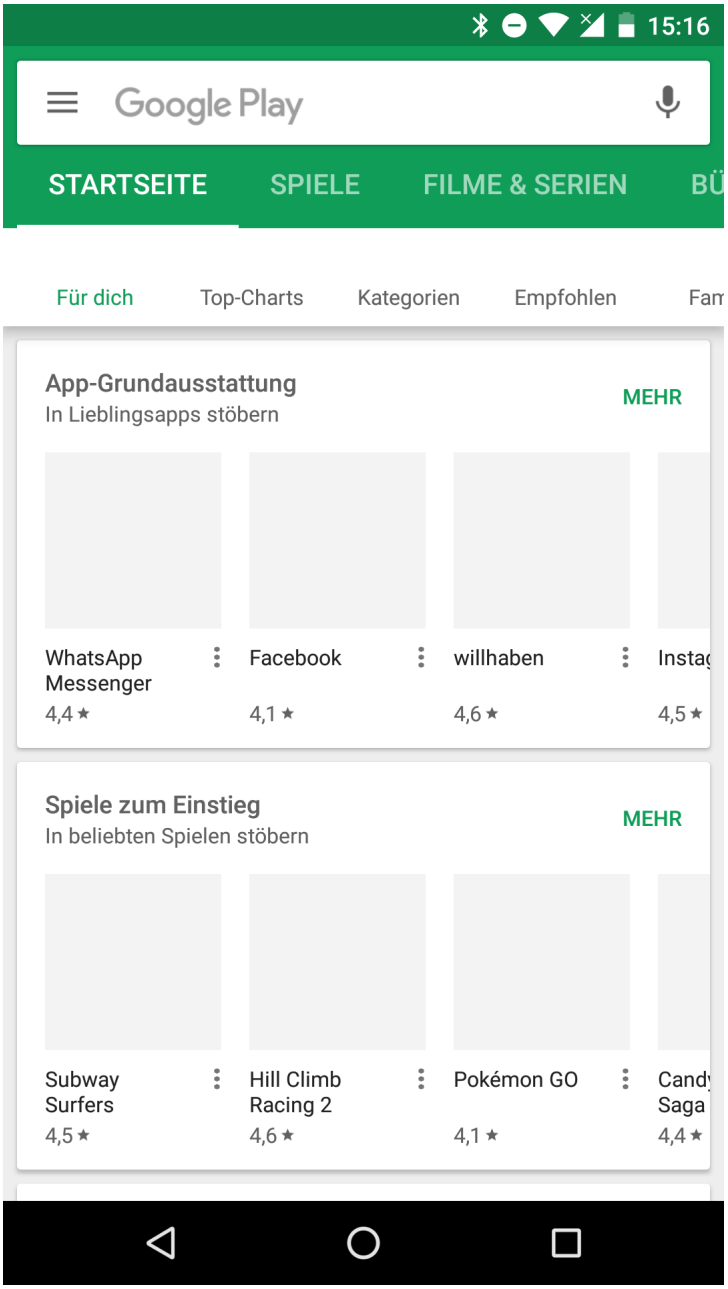

Abbildung 6.17: Ergebnis des Umgehungsszenarios "Anwendung beenden"

Ebenso war es möglich die App direkt nach dem Neustart einfach vom Gerät zu entfernen.

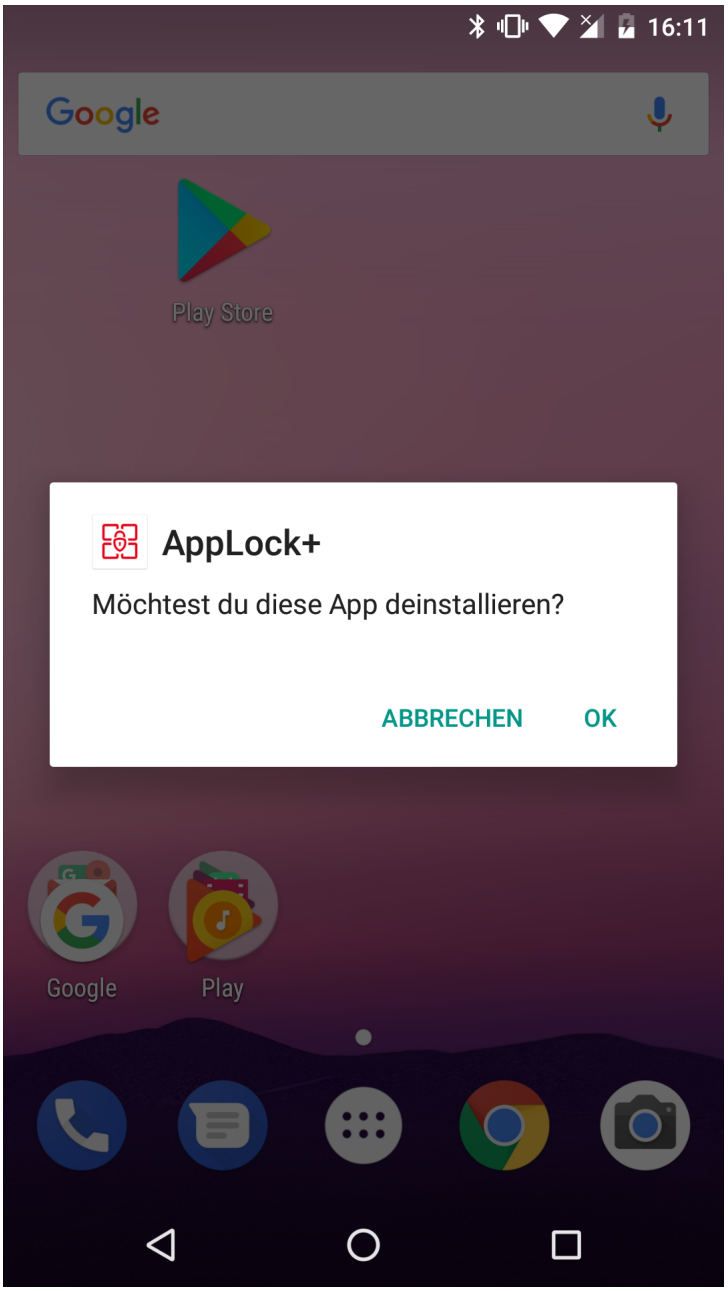

Abbildung 6.18: Ergebnis des Umgehungsszenarios "App löschen"

Auch während die Kindersicherung auf dem Gerät lief, ließ sich jene entfernen. Dafür war es nötig die Anwendung auf "Deinstallieren" zu ziehen und dann direkt danach bei der auftretenden Meldung, ob man die App deinstallieren wolle, auf "OK" zu klicken.

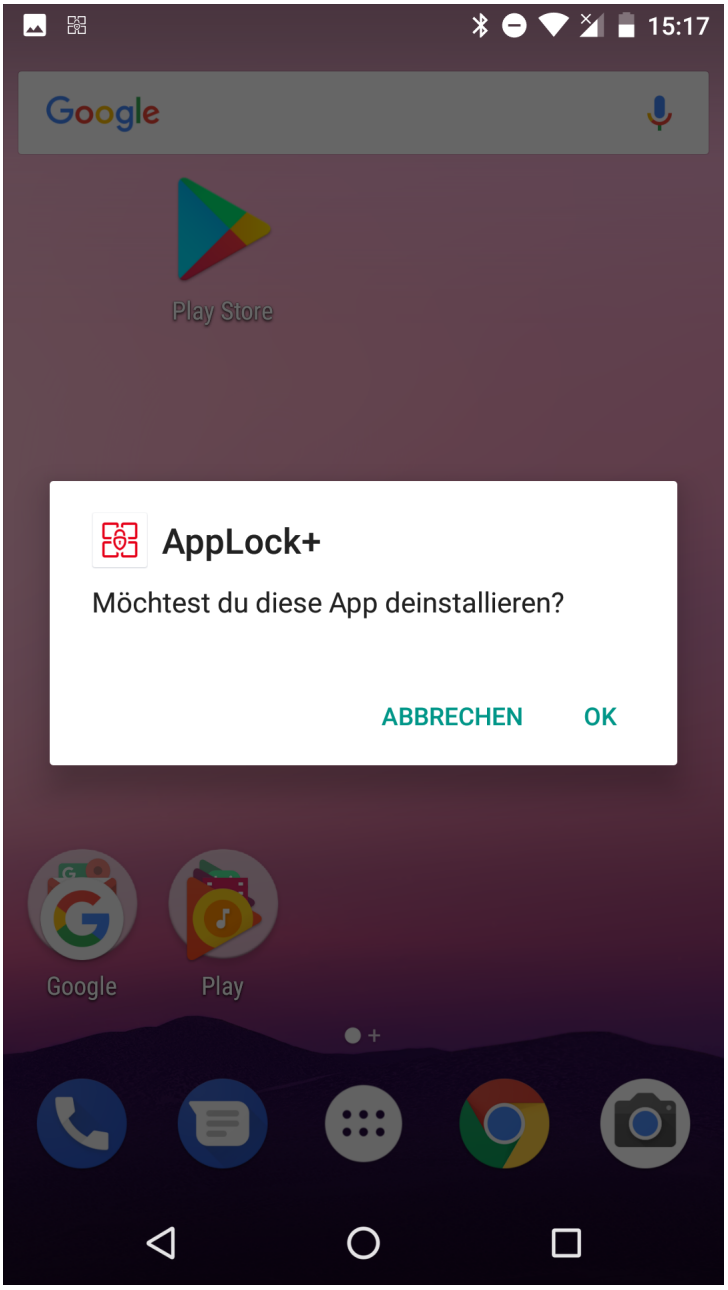

Abbildung 6.19: Ergebnis des Umgehungsszenarios "App löschen"

Jelly Ansns Child Lock 2 - Praxistestkatalog – Android 7.1.1			
Kriterium	**Beschreibung des Bewertungskriteriums**	**Kritikalität**	**Punkte**
1. Anrufe von Dritten blockieren	Das Empfangen von Anrufen kann nicht gesperrt werden.	Hoch	0
2. Ausführung von spezifischen Dateitypen blockieren	Die Software kann keine spezifischen Dateitypen blockieren.	Mittel	0
3. Beratungsfunktion	Die Software gibt Eltern keine Hilfestellung bei der Einführung einer Kinderschutzsoftware.	Niedrig	0
4. Datenübertragung über Lightning Connector / USB blockieren	Die Software kann keine Datenübertragungen über den USB-Port / Lightning Connector blockieren.	Niedrig	0
5. Deinstallationsschutz	Die Software besitzt keinen Schutz vor einer Deinstallation.	Hoch	0
6. Einrichtungsassistent	Es wird keine Hilfestellung für die Anwendung geboten.	Mittel	0
7. Installation	Die Installation ist einfach durchführbar und weist keine Komplexität auf.	Niedrig	1
8. Kategoriefilter Apps	Die Software bietet keinen variablen Kategoriefilter an.	Hoch	0
9. Kategoriefilter Web	Die Software bietet keinen variablen Kategoriefilter an.	Hoch	0
10. Loggingfunktion	Die Software bietet keine Loggingfunktion an.	Hoch	0
11. SMS von Dritten blockieren	Das Empfangen von SMS kann nicht gesperrt werden.	Hoch	0

Kriterium	Beschreibung des Bewertungskriteriums	Kritikalität	Punkte
12. Soziale Netzwerke	Die Software bietet keine spezifischen Funktionalitäten hinsichtlich sozialer Netzwerke.	Mittel	0
13. Spamfilter für Maildienste	Die Software hat keinen Spamfilter integriert.	Niedrig	0
14. Sperren von Apps	Die Software kann keine spezifischen Anwendungen blockieren.	Hoch	0
15. Sperren von Websites	Die Software kann keine spezifischen Websites sperren.	Hoch	0
16. Store-Blocker	Die Software bietet keine Funktionalität Downloads aus dem Google Play Store zu blockieren.	Mittel	0
17. Suchmaschine	Die Software beschränkt Suchmaschinen nicht und bietet auch keine Safe Search Funktion an.	Mittel	0
18. Verwaltung im Web	Die Software wird lokal verwaltet.	Mittel	0
19. Zeitbeschränkung	Es lässt sich ein sogenannter „Alarm“ einstellen, welcher bis zur bestimmten Uhrzeit gilt. Danach wird das Gerät gesperrt und es muss der zuvor definierte 4-stellige PIN eingegeben werden.	Hoch	0,5
Gesamtbewertung	**Hoch 0,5x3 + Mittel 0x2 + Niedrig 1x1 = 2,5 / 43**		

Tabelle 6.15: Ergebnis - Jelly Ansns Child Lock - Praxistestkatalog

Jelly Ansns Child Lock- Umgehungsszenarien – Android 7.1.1		
Szenario	**Beschreibung**	**Bewertung**
Änderung der Systemzeit	**Solange die Sperrung durch Zeitablauf nicht ausgelöst wurde, kann einfach die Uhrzeit geändert werden und die Kindersicherung wird dadurch umgangen.**	**Nicht bestanden**
Anonymisierender Webproxy	**Die Anwendung besitzt keinen Webfilter, wodurch keine Umgehung nötig ist. Das Szenario gilt automatisch als ,,Nicht bestanden".**	**Nicht bestanden**
Anwendung beenden	Die Kindersicherung kann nachdem jene ausgelöst wurde, nicht über den Taskmanager beendet werden. **Jedoch hebt ein Neustart die Sperre auf und das Gerät kann ohne Limitierung weiterverwendet werden.**	**Nicht bestanden**
App löschen	**Die Kindersicherung wird nicht geschützt und ist daher ohne Weiteres deinstallierbar.**	**Nicht bestanden**
Bruteforce-Angriff	**Ein Bruteforce-Angriff ist möglich, da keine zeitliche Sperre bei zu vielen Versuchen integriert wurde. Ebenso wird keine Warnung an ein Elternteil versendet.**	**Nicht bestanden**
SafeSearch oder Kindersuchmaschine	**Die Anwendung besitzt keinen Webfilter, wodurch keine Umgehung nötig ist. Das Szenario gilt automatisch als ,,Nicht bestanden".**	**Nicht bestanden**
Wayback Machine	**Die Anwendung besitzt keinen Webfilter, wodurch keine Umgehung nötig ist. Das Szenario gilt automatisch als ,,Nicht bestanden".**	**Nicht bestanden**
Gesamtbewertung	**7 (100%) von 7 Szenarien wurden nicht bestanden.**	

Tabelle 6.16: Ergebnis - Jelly Ansns Child Lock - Umgehungsszenarien

6.0.8 Fazit - Jelly Ansns

"Child Lock" von "Jelly Ansns" erreichte nur 2,5 von 43 Punkten im Praxistestkatalog und alle Umgehungsszenarien waren erfolgreich. Die Anwendung bietet nur eine Funktionalität, nämlich die des Zeitkontos und selbst diese wurde äußerst schlecht ausgeführt. Der sogenannte "Alarm" lässt sich einfach umgehen, indem man die Uhrzeit umstellt, damit der Alarm nicht ausgelöst wird. Und selbst wenn die Sperre greift, muss man nur das Smartphone neustarten, um jene zu umgehen. Weiterführend waren daher drei der Umgehungsszenarien nicht anwendbar, da die Funktionalität des Webfilters nicht gegeben war.

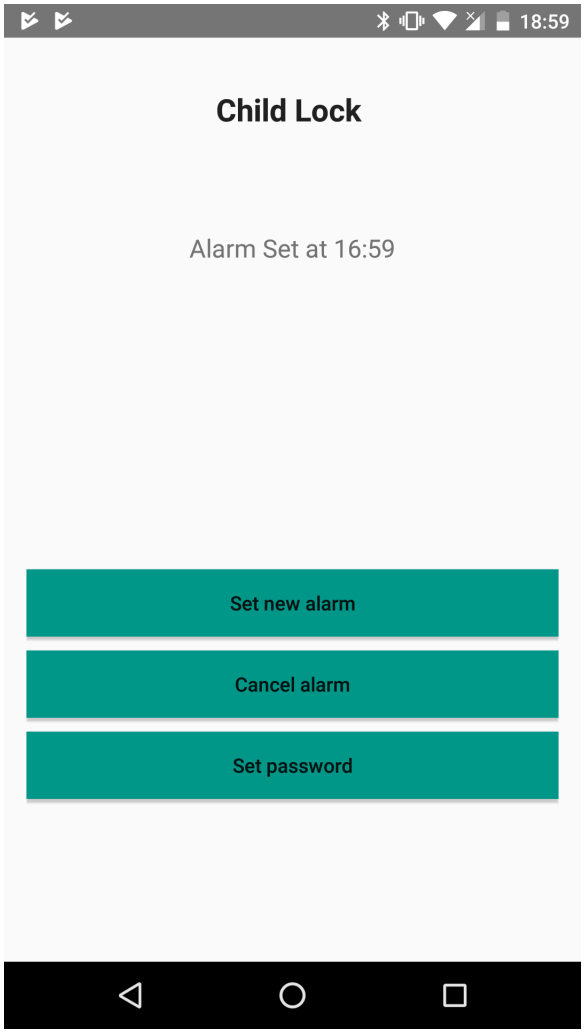

Abbildung 6.20: Ergebnis des Umgehungsszenarios "Änderung der Systemzeit"

Außerdem besitzt die Anwendung keinen Deinstallationsschutz und lässt sich somit einfach vom Gerät entfernen.

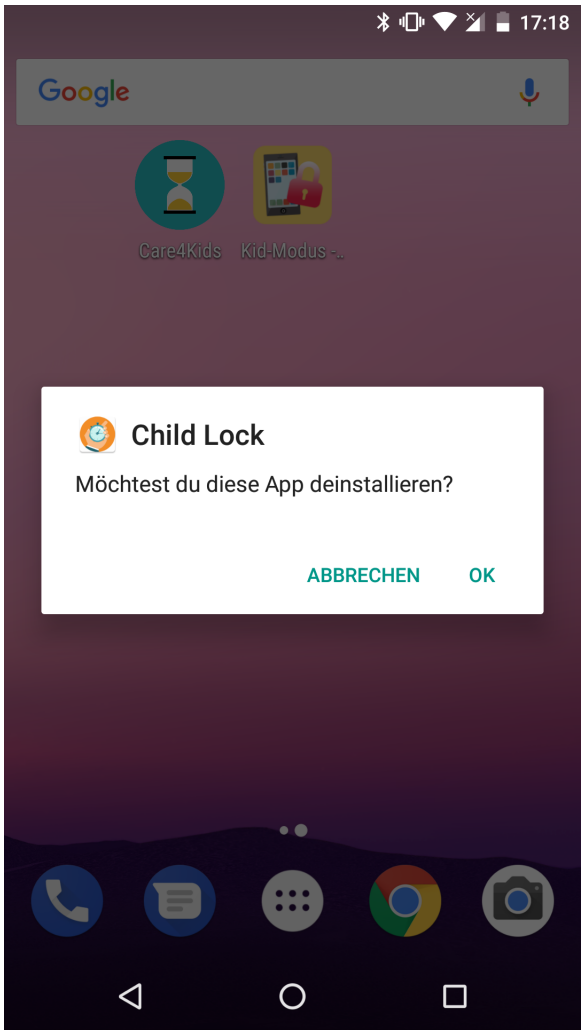

Abbildung 6.21: Ergebnis des Umgehungsszenarios "App löschen"

IT HK Service Limited Kid-Modus Kindersicherung 1.3 - Praxistestkatalog – Android 7.1.1			
Kriterium	**Beschreibung des Bewertungskriteriums**	**Kritikalität**	**Punkte**
1. Anrufe von Dritten blockieren	Das Empfangen von Anrufen kann nicht gesperrt werden.	Hoch	0
2. Ausführung von spezifischen Dateitypen blockieren	Die Software kann keine spezifischen Dateitypen blockieren.	Mittel	0
3. Beratungsfunktion	Die Software gibt Eltern keine Hilfestellung bei der Einführung einer Kinderschutzsoftware.	Niedrig	0
4. Datenübertragung über Lightning Connector / USB blockieren	Die Software kann keine Datenübertragungen über den USB-Port / Lightning Connector blockieren.	Niedrig	0
5. Deinstallationsschutz	Die Software besitzt keinen Schutz vor einer Deinstallation.	Hoch	0
6. Einrichtungsassistent	Das angegebene Tutorial ist in einem unverständlichen und äußerst gebrochenen Deutsch beschrieben, wodurch die Funktionsweise am Anfang nicht direkt verständlich ist.	Mittel	0
7. Installation	Die Installation ist einfach durchführbar und weist keine Komplexität auf.	Niedrig	1
8. Kategoriefilter Apps	Die Apps, welche angezeigt werden sollen, können nur an- oder abgewählt werden	Hoch	0
9. Kategoriefilter Web	Die Software bietet keinen variablen Kategoriefilter an.	Hoch	0
10. Loggingfunktion	Die Software bietet keine Loggingfunktion an.	Hoch	0

Kriterium	Beschreibung des Bewertungskriteriums	Kritikalität	Punkte
11. SMS von Dritten blockieren	Das Empfangen von SMS kann nicht gesperrt werden.	Hoch	0
12. Soziale Netzwerke	Die Software bietet keine spezifischen Funktionalitäten hinsichtlich sozialer Netzwerke.	Mittel	0
13. Spamfilter für Maildienste	Die Software hat keinen Spamfilter integriert.	Niedrig	0
14. Sperren von Apps	Apps können explizit zu den erlaubten Anwendungen hinzugefügt werden.	Hoch	1
15. Sperren von Websites	Die Software kann keine spezifischen Websites sperren.	Hoch	0
16. Store-Blocker	Der Play-Store kann entsprechend blockiert werden, indem er nicht zu den erlaubten Apps hinzugefügt wird.	Mittel	1
17. Suchmaschine	Die Software beschränkt Suchmaschinen nicht und bietet auch keine Safe Search Funktion an.	Mittel	0
18. Verwaltung im Web	Die Software wird lokal verwaltet.	Mittel	0
19. Zeitbeschränkung	Die Software hat keine Einstellung für eine Zeitbeschränkung.	Hoch	0
Gesamtbewertung	**Hoch 1x3 + Mittel 1x2 + Niedrig 1x1 = 6 / 43**		

Tabelle 6.17: Ergebnis - IT HK Service Limited Kid-Modus Kindersicherung - Praxistestkatalog

IT HK Service Limited Kid-Modus Kindersicherung - Umgehungsszenarien – Android 7.1.1		
Szenario	**Beschreibung**	**Bewertung**
Änderung der Systemzeit	**Die Anwendung besitzt keine Zeitkontofunktionalität, wodurch keine Umgehung nötig ist. Das Szenario gilt automatisch als „Nicht bestanden“.**	**Nicht bestanden**
Anonymisierender Webproxy	**Die Anwendung besitzt keinen Webfilter, wodurch keine Umgehung nötig ist. Das Szenario gilt automatisch als „Nicht bestanden".**	**Nicht bestanden**
Anwendung beenden	Die Anwendung lässt sich nicht über den Taskmanager beenden und auch beim Neustart startet die App direkt mit, wodurch ein Beenden nicht möglich ist.	Bestanden
App löschen	**Die App kann gelöscht werden indem die Benachrichtigungsleiste geöffnet wird und man dann auf das Zahnradsymbol klickt, wodurch man in die Einstellungen gelangt. Unter Apps lässt sich die Anwendung dann ohne PIN-Eingabe deinstallieren.**	**Nicht bestanden**
Bruteforce-Angriff	**Ein Bruteforce-Angriff auf den PIN ist ohne Einschränkungen möglich. Ein Elternteil wird dabei ebenso nicht gewarnt.**	**Nicht bestanden**
SafeSearch oder Kindersuchmaschine	**Die Anwendung besitzt keine Zeitkontofunktionalität, wodurch keine Umgehung nötig ist. Das Szenario gilt automatisch als „Nicht bestanden“.**	**Nicht bestanden**
Wayback Machine	**Die Anwendung besitzt keinen Webfilter, wodurch keine Umgehung nötig ist. Das Szenario gilt automatisch als „Nicht bestanden".**	**Nicht bestanden**
Gesamtbewertung	**6 (85,71%) von 7 Szenarien wurden nicht bestanden.**	

Tabelle 6.18: Ergebnis - IT HK Service Limited Kid-Modus Kindersicherung - Umgehungsszenarien

6.0.9 Fazit - IT HK Service Limited

Die vorletzte Anwendung im Praxistest, nämlich "Kid-Modus Kindersicherung" von "IT HK Service Limited" erhielt nur 6 von 43 möglichen Punkten im Praxistestkatalog und hat insgesamt 6 von 7 Umgehungsszenarien nicht bestanden. Mittels der Anwendung soll es möglich sein, dass nur gewisse Apps für das Kind bzw. den Jugendlichen freigegeben werden. Jedoch lässt sich die Anwendung einfach löschen, indem die Benachrichtigungsleiste heruntergezogen und dann über die Einstellungen die Anwendung entfernt wird.

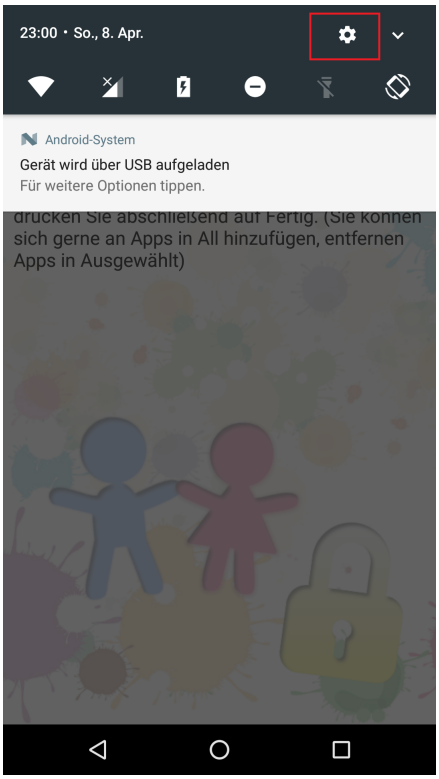

Abbildung 6.22: Ergebnis des Umgehungsszenarios "App löschen"

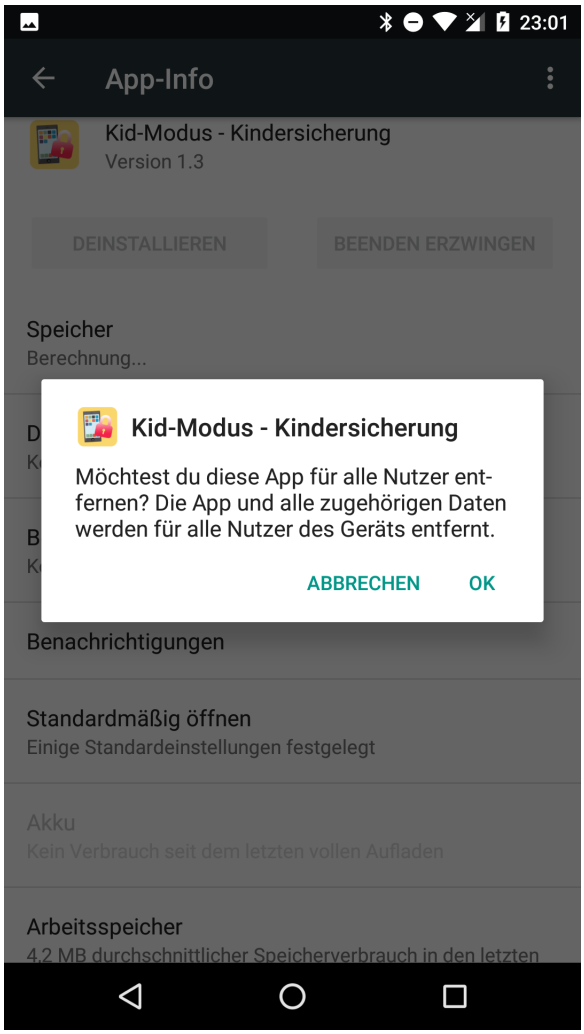

Abbildung 6.23: Ergebnis des Umgehungsszenarios "App löschen"

Antropia Care4Kids 1.0.7 - Kindersicherung - Praxistestkatalog – Android 7.1.1			
Kriterium	**Beschreibung des Bewertungskriteriums**	**Kritikalität**	**Punkte**
1. Anrufe von Dritten blockieren	Das Empfangen von Anrufen kann nicht gesperrt werden.	Hoch	0
2. Ausführung von spezifischen Dateitypen blockieren	Die Software kann keine spezifischen Dateitypen blockieren.	Mittel	0
3. Beratungsfunktion	Die Software gibt Eltern keine Hilfestellung bei der Einführung einer Kinderschutzsoftware.	Niedrig	0
4. Datenübertragung über Lightning Connector / USB blockieren	Die Software kann keine Datenübertragungen über den USB-Port / Lightning Connector blockieren.	Niedrig	0
5. Deinstallationsschutz	Die Software besitzt keinen Schutz vor einer Deinstallation.	Hoch	0
6. Einrichtungsassistent	Die Anwendung bietet eine kurze Erläuterung der wichtigsten Funktionalitäten sowie der Bedienungsweise der App.	Mittel	0,75
7. Installation	Die Installation ist einfach durchführbar und weist keine Komplexität auf.	Niedrig	1
8. Kategoriefilter Apps	Die Software bietet keinen variablen Kategoriefilter an.	Hoch	0
9. Kategoriefilter Web	Die Software bietet keinen variablen Kategoriefilter an.	Hoch	0
10. Loggingfunktion	Die Software bietet keine Loggingfunktion an.	Hoch	0
11. SMS von Dritten blockieren	Das Empfangen von SMS kann nicht gesperrt werden.	Hoch	0

Kriterium	Beschreibung des Bewertungskriteriums	Kritikalität	Punkte
12. Soziale Netzwerke	Die Software bietet keine spezifischen Funktionalitäten hinsichtlich sozialer Netzwerke.	Mittel	0
13. Spamfilter für Maildienste	Die Software hat keinen Spamfilter integriert.	Niedrig	0
14. Sperren von Apps	Apps können nicht vollkommen gesperrt werden, da eine Mindestnutzungszeit von einer Minute gegeben sein muss, um eine Beschränkung erstellen zu können.	Hoch	0
15. Sperren von Websites	Die Software kann keine spezifischen Websites sperren.	Hoch	0
16. Store-Blocker	Die Software bietet keine Funktionalität Downloads aus dem Google Play Store zu blockieren.	Mittel	0
17. Suchmaschine	Die Software beschränkt Suchmaschinen nicht und bietet auch keine Safe Search Funktion an.	Mittel	0
18. Verwaltung im Web	Die Software wird lokal verwaltet.	Mittel	0
19. Zeitbeschränkung	Die Dauer der Nutzung jeder App kann separat definiert werden. Nach Ablauf der Zeit erscheint ein Pop-Up, welches die Verwendung der App unterbindet.	Hoch	0,5
Gesamtbewertung	**Hoch 0,5x3 + Mittel 0,75x2 + Niedrig 1x1 = 4 / 43**		

Tabelle 6.19: Ergebnis - Antropia Care4Kids - Kindersicherung - Praxistestkatalog

Antropia Care4Kids - Umgehungsszenarien – Android 7.1.1		
Szenario	**Beschreibung**	**Bewertung**
Änderung der Systemzeit	**Durch die Änderung der Systemzeit lässt sich die Zeitkontofunktionalität der Anwendung umgehen.**	**Nicht bestanden**
Anonymisierender Webproxy	**Die Anwendung besitzt keinen Webfilter, wodurch keine Umgehung nötig ist. Das Szenario gilt automatisch als ,,Nicht bestanden".**	**Nicht bestanden**
Anwendung beenden	**Wenn das Smartphone neugestartet wird, nachdem die Zeit für eine App abgelaufen ist, kann man die App wiederverwenden und es erscheinen keine Pop-Ups mehr.**	**Nicht bestanden**
App löschen	**Die Anwendung ist nicht extra abgesichert, wodurch eine Deinstallation der App einfach möglich ist.**	**Nicht bestanden**
Bruteforce-Angriff	**Passwörter können ohne Weiteres mehr als 10 Mal nacheinander ausprobiert werden. Dies führt weder zu einer zeitlichen Sperrung von Loginversuchen noch wird ein Elternteil vor dem Bruteforce-Angriff gewarnt.**	**Nicht bestanden**
SafeSearch oder Kindersuchmaschine	**Die Anwendung besitzt keinen Webfilter, wodurch keine Umgehung nötig ist. Das Szenario gilt automatisch als ,,Nicht bestanden".**	**Nicht bestanden**
Wayback Machine	**Die Anwendung besitzt keinen Webfilter, wodurch keine Umgehung nötig ist. Das Szenario gilt automatisch als ,,Nicht bestanden".**	**Nicht bestanden**
Gesamtbewertung	**7 (100%) von 7 Szenarien wurden nicht bestanden.**	

Tabelle 6.20: Ergebnis - Antropia Care4Kids - Kindersicherung - Umgehungsszenarien

6.0.10 Fazit - Antropia

Die letzte Anwendung im Praxistest, nämlich "Care4Kids - Kindersicherung" von "Antropia" erreichte nur 4 von 43 Punkten und hat alle Umgehungsszenarien nicht bestanden. Die Anwendung soll es ermöglichen, die zeitliche Nutzung jeder App am Smartphone einzuschränken. Jedoch ist diese Funktionalität durch die Änderung der Systemzeit umgehbar. Ebenso ist die App nicht weiter abgesichert und kann einfach gelöscht werden.

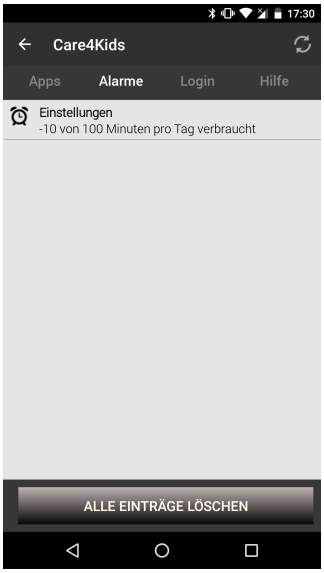

Abbildung 6.24: Ergebnis des Umgehungsszenarios "Änderung der Systemzeit"

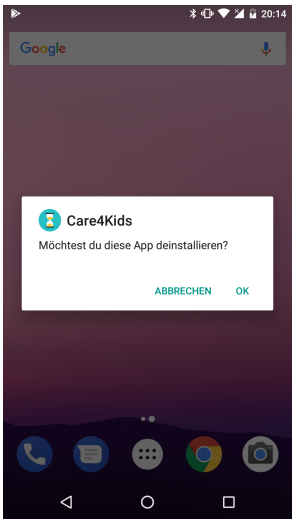

Abbildung 6.25: Ergebnis des Umgehungsszenarios "App löschen"

7 Gesamtresümee

Zusammenfassend finden sich nun die Ergebnisse aus allen Programmen:

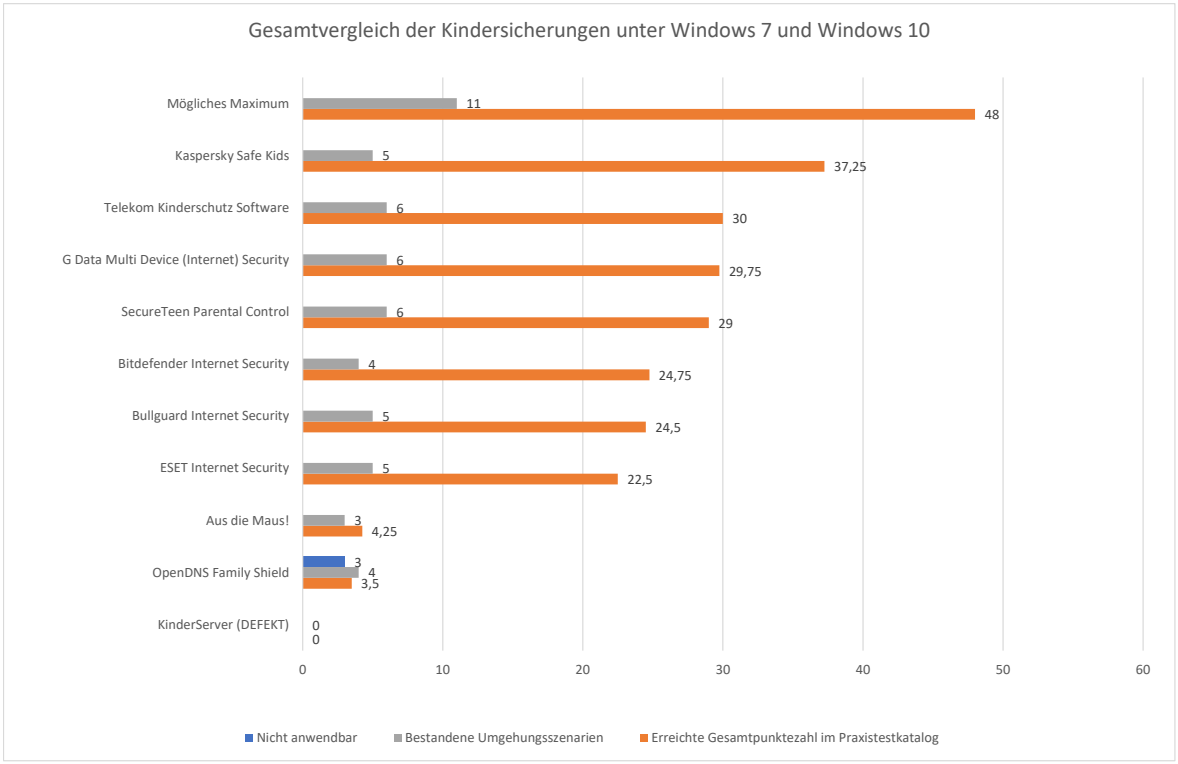

Abbildung 7.1: Gesamtvergleich der Kindersicherungen - Windows 7 und Windows 10

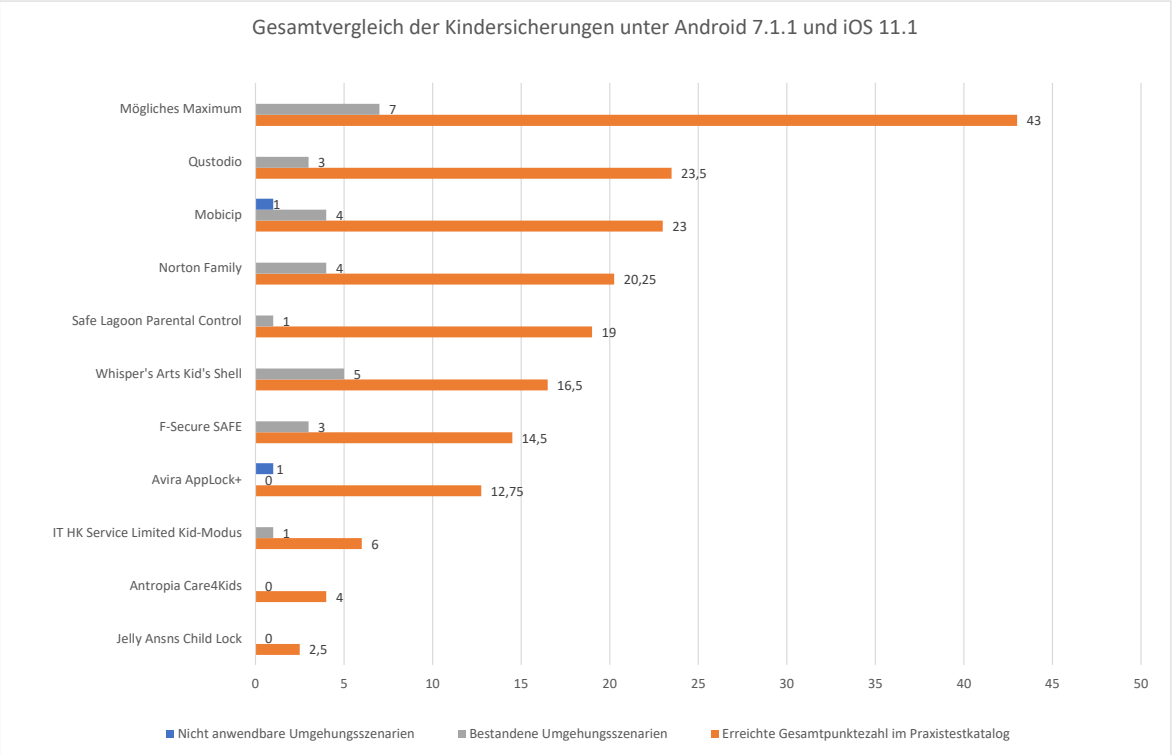

Abbildung 7.2: Gesamtvergleich der Kindersicherungen - Android 7.1.1 und iOS 11.1

Es zeigt sich, dass jede der 20 Anwendungen in zumindest einer Art und Weise umgehbar war. Faktisch gibt es keinen Schutz, welcher zu 100% undurchdringbar war. Außerdem legen die vorhergehenden Tests klar dar, dass sich die Anwendungen deutlich in der Funktionalitätsbandbreite unterscheiden.

7.1 Erkenntnisse und Empfehlungen

Nachfolgend finden sich die Schlussfolgerungen aus dem Praxistest und den Umgehungsszenarien.

7.1.1 Kindersicherungen - Windows 7 und Windows 10

Summa summarum lassen sich aus den Ergebnissen des Praxistests unter Windows 7 und Windows 10 folgende Erkenntnisse schließen:

- Viele der getesteten Anwendungen schützen meist nur ungenügend vor den zahlreichen, exis-

tierenden Gefahren, da Schutzmechanismen zu bestimmten Gefahrenquellen nicht implementiert wurden. Als Beispiel kann man hier die Anwendung "Parental Control" von "Secure Teen" heranziehen, welche 29 von möglichen 48 Punkten erreicht hat. Da die Kindersicherung keine Features hinsichtlich der Sperrung von Anwendungen bietet, sind insgesamt 6 Punkte (2 Punkte x 3 Gewichtung) abgezogen worden. Weiterführend verlor die Anwendung 2 Punkte, da weder eine Laufwerkssperrung [147] noch ein Blockieren von USB-Schnittstellen [148] möglich ist. Entsprechend hat die Anwendung somit effektiv 17% seiner Gesamtbewertung dahingehend verloren. Dasselbe gilt für die Anwendung "Multi Device (Internet) Security" von "G Data". Entsprechend kann hier der Schluss gezogen werden, dass unbedingt ein gesamtheitlicher Schutzansatz verfolgt werden und auch hinsichtlich der Bedrohungsszenarien eine umfassende Analyse geschehen muss, um etwaige Einfallstore für Gefahren mittels der Kindersicherung schließen zu können.

- Die Anwendungen müssen im Allgemeinen einen höheren Beratungsaufwand vor, während und nach der Installation aufweisen, damit Eltern mit den gegebenen Informationen über die Computernutzung des Kindes bzw. Jugendlichen richtig umgehen können. Weiterführend kann es nämlich bei der falschen Verwendung der entsprechenden Informationen, welche über die Kindersicherungssoftware mitgeloggt werden, schnell zu einem Vertrauensbruch bzw. -verlust [149] seitens des Kindes bzw. Jugendlichen kommen.

- Ein großes Manko bei dem Großteil der Anwendungen ist, dass nicht darauf hingewiesen wird, dass ein eingeschränktes Benutzerkonto für ein Kind verwendet werden soll und in weiterer Folge der Deinstallationsschutz fehlt. Dies macht eine Entfernung oder Manipulation der Anwendung äußerst einfach. Als Beispiel kann man hier die getestete Anwendung "Internet Security" von "ESET" nennen. Bei jener wurde nicht darauf geachtet, dass unbedingt ein Passwort für das Programm gesetzt werden sollte, um eine Deinstallation durch ein Kind bzw. einen Jugendlichen zu erschweren. In weiterer Folge wurde ebenso nicht darauf hingewiesen, dass eingeschränkte Benutzerkonten verwendet werden sollten, was sich im erfolgreichen Umgehungsszenario "Essentielle Dateien der Kinderschutzsoftware umbenennen/löschen" widergespiegelt hat.

- Äußerst bedenklich ist, dass nur zwei Anwendungen, nämlich "G Data Multi Device Internet Security" und "Telekom Kinderschutz Software" auf die standardmäßige Verwendung einer Kindersuchmaschine wie "FragFinn" [115] hingewiesen haben. Hierbei sollte dringend nachgebessert werden, da sich im Laufe der Arbeit herausgestellt hat, dass die SafeSearch-Funktion der Suchmaschinen äußerst einfach deaktivierbar war. Abgesehen davon ist anzumerken dass, "SafeSearch [...] nicht zu 100% treffsicher [...]" [40] ist.

- Hinsichtlich eines Bruteforce-Angriffs auf die Kindersicherung gibt es nur eine Anwendung, nämlich "Norton Family", welche eine Login-Sperre nach 7 Versuchen eingerichtet und entsprechend das Elternteil dann per E-Mail über die Sperrung des Kontos informiert hat. Solch eine Warnung ist äußerst wichtig, da dies darauf hindeuten kann, dass das Kind bzw. der Jugendliche gerade versucht, die Anwendung zu umgehen. In weiterer Folge sollte entsprechend das Gespräch durch die Eltern gesucht werden, um klar darzulegen, warum die Kindersicherung verwendet wird und was man tun kann, um solch ein Vorgehen in weiterer Folge zu verhindern.

- Das Umgehungsszenario zu anonymisierenden Webproxies wurde unter Windows 7 sowie Windows 10 insgesamt 3 mal aus 9 getesteten Anwendungen nicht bestanden ("KinderServer" wird dabei nicht beachtet, da die Anwendung generell keine Funktionalität aufwies). Das bedeutet, dass ein Drittel der getesteten Anwendungen zumindest einen der fünf getesteten Webproxies nicht kannte und in weiterer Folge nicht blockiert hat. Entsprechend ist als Empfehlung zu geben, dass entweder eine Blacklist mit den Webproxy-Servern erzeugt und regelmäßig gewartet wird oder entsprechendes Keyword-Filtering [150] in die Kindersicherung implementiert wird.

- Eine Kindersicherung sollte unbedingt jegliche Art von Keylogger sperren, wenn diese durch ein Kind bzw. einen Jugendlichen auf den Rechner gebracht wird.

- Bei Kindersicherungen, welche auf einem Router installiert werden, ist darauf zu achten, dass es durchaus große technische Unterschiede geben kann. Dies kann dazu führen, dass auf gewissen Geräten die benötigte Konfigurationsmethodik überhaupt nicht möglich ist oder nicht funktioniert, wie man an dem Beispiel von "OpenDNS Family Shield" im Zusammenspiel mit dem Huawei B315s-22 Router erkennen konnte.

- Bei 2 der 9 getesten Programme unter Windows 7 und Windows 10 war es möglich den Prozess der Kindersicherung zu beenden (konkret waren dies "Aus die Maus!" und "F-Secure SAFE"). Da dies eine äußerst einfache Methodik ist das Programm zu umgehen, ist dementsprechend ein hoher Wert auf einen Schutz vor Beendigung des Prozesses der Anwendung zu legen.

- Final ist anzumerken, dass jedes Programm unter Windows 7 sowie Windows 10 mittels des abgesicherten Modus ausgehebelt werden konnte. Eine Ausführung der Kindersicherung kann jedoch mittels eines Registry-Eintrags [151] erzwungen werden. Falls dies als weiterführender Schutz nicht ausreichend ist, kann erwogen werden, ob man den abgesicherten Modus komplett blockiert. Dies wäre zum Beispiel über die Anwendung "NoSafeMode" [152] feingranular auf Benutzerkontenebene oder über einen Registry-Eintrag [153] möglich.

7.1.2 Kindersicherungen - Android und iOS

Die Erkenntnisse aus dem Praxistest unter Android 7.1.1 und iOS 11.1 lassen sich wie folgt zusammenfassen:

- Bei keiner der getesteten Apps war es möglich Anrufe oder SMS von unbekannten Kontakten zu blockieren, obwohl entsprechend der abgeleiteten Bedrohungen, ein hohes Gefahrenpotential von diesen Funktionalitäten ausgeht. Entsprechende Anwendungen [154–156] existieren bereits und sollten dementsprechend in eine Kindersicherung implementiert werden.

- Zwei der getesteten Anwendungen unter iOS wiesen nicht auf den standardmäßig verfügbaren "Einschränkungen"-Modus [124] auf dem iPhone hin (konkret "Qustodio" und "Safe Lagoon Parental Control"), was konkret dazu führte, dass das "App löschen" Umgehungsszenario erfolgreich war. Ergo hatten die Anwendungen keinen Schutz vor einer Deinstallation. Dementsprechend ist es wichtig, dass die App darauf hinweist, dass die interne Kindersicherungsfunktion aktiviert wird.

- Wie unter Windows 7 und Windows 10 gilt auch bei den mobilen Anwendungen, dass dringend an der Beratungsfunktion sowie dem Deinstallationsschutz bei den getesteten Applikationen gearbeitet und auch ein gesamtheitlicher Ansatz, mit entsprechend implementierten Funktionalitäten, angewandt werden muss. In weiterer Folge trägt dies dazu bei einen effektiven Schutz vor den unterschiedlichen Bedrohungsquellen gewährleisten zu können.

- Bei vier der getesteten Applikationen ("Antropia Care4Kids", "IT HK Service Limited Kid-Modus Kindersicherung", "Jelly Ansns Child Lock" und "F-Secure SAFE") konnte die Zeitkontofunktionalität umgangen werden, indem die Systemzeit geändert wurde. Ein entsprechender Schutz vor einer Änderung der Uhrzeit ist in diesem Falle zu implementieren, um eine Umgehung auf diese Art und Weise zu unterbinden.

- Ein Neustart des Gerätes oder ein Beenden der App hat bei 4 von 10 Apps dazu geführt, dass die Anwendung für zumindest einen kurzen Zeitraum ausgefallen ist und in weiterer Folge die Kindersicherung umgangen werden konnte. Dies muss ebenso entsprechend unterbunden werden, da ein Neustart die Wirksamkeit einer Kindersicherung nicht beeinflussen darf.

7.2 Kritik und Ausblick

Aufbauend auf diese Diplomarbeit gilt es nun ein valides Modell zur Vermeidung von unpassenden Inhalten für entsprechende Altersgruppen zu entwickeln und umzusetzen. Hauptaugenmerk sollte hierbei

auf die zuvor erwähnten, nötigen technischen Maßnahmen und insbesondere den Einfluss der Kommunikation und Beratung durch Eltern mit den betroffenen Kindern und Jugendlichen gelegt werden, da eine Umgehung bei den getesteten Anwendungen immer möglich war. Natürlich bedeutet dies nicht, dass Kinderschutzsoftware sinnlos ist, denn der "versehentliche" Konsum von unpassenden Inhalten kann dadurch natürlich reduziert werden. Sobald jedoch eine Umgehung vom Sprössling gewünscht wird, ist diese bis dato auch realistisch durchsetzbar.

Weiterführend gilt hauptsächlich zu bedenken, dass sobald ein Kind bzw. ein Jugendlicher genügend Geld besitzt um sich entsprechend ein eigenes Gerät zu kaufen wovon die Eltern nichts wissen, sei es ein Notebook, Tablet oder ein Smartphone, ist jeglicher technische Schutz automatisch umgangen. Dasselbe gilt hier auch für Router-Lösungen, da sich das Kind bzw. der Jugendliche selbst eine SIM-Karte mit einem Datentarif und einem entsprechenden Modem zulegen kann oder indem jener einfach außerhalb der eigenen vier Wände surft. Entsprechend ist auch auszuführen, dass es im Umfeld des Kindes oder Jugendlichen durchaus Freunde oder Bekannte geben kann, welche das Web sowie Software, wie Computerspiele, ungefiltert konsumieren können.

Abbildungsverzeichnis

Tabellenverzeichnis

Literaturverzeichnis

[1] Statista, "Anteil der Haushalte weltweit mit Internetzugang von 2002 bis 2017," https://de.statista.com/statistik/daten/studie/187116/umfrage/anteil-der-haushalte-mit-internetzugang/, 2017, (Abgerufen am 09/26/2017).

[2] Bitkom Research, "Kinder und Jugend in der digitalen Welt," https://www.bitkom.org/Presse/Anhaenge-an-PIs/2017/05-Mai/170512-Bitkom-PK-Kinder-und-Jugend-2017.pdf, pp. 2–6, 2017, (Abgerufen am 09/26/2017).

[3] T. Günter and F. Schindler, "Technische möglichkeiten des jugendschutzes im internet," pp. 341–350, 2006.

[4] T. König and T. Schmid, "Kim-studie 2010," https://www.mpfs.de/fileadmin/files/Studien/KIM/2010/KIM_Studie_2010.pdf, p. 39, 2011, (Abgerufen am 09/26/2017).

[5] J. G. Noll, C. E. Shenk, J. E. Barnes, and K. J. Haralson, "Association of maltreatment with high-risk internet behaviors and offline encounters," *Pediatrics*, vol. 131, no. 2, pp. e510–e517, 2013, (Abgerufen am 09/30/2017). [Online]. Available: http://pediatrics.aappublications.org/content/131/2/e510

[6] Bundeskanzleramt Österreich, "Landesrecht konsolidiert Niederösterreich: Gesamte Rechtsvorschrift für NÖ Jugendgesetz, Fassung vom 29.08.2017," https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=LrNO&Gesetzesnummer=20000556#header, 2013, (Abgerufen am 09/26/2017).

[7] S. Livingstone, L. Haddon, A. Görzig, and K. Ólafsson, "Risks and safety on the internet: the perspective of european children: full findings and policy implications from the eu kids online survey of 9-16 year olds and their parents in 25 countries," pp. 13–101, 2011.

[8] StatCounter, "About statcounter," 2017, (Abgerufen am 01/05/2018). [Online]. Available: http://gs.statcounter.com/about

[9] ——, "Desktop windows version market share worldwide," 2017, (Abgerufen am 05/21/2018). [Online]. Available: http://gs.statcounter.com/os-version-market-share/windows/desktop/worldwide

[10] ——, "Mobile & tablet android version market share worldwide," 2017, (Abgerufen am 05/21/2018). [Online]. Available: http://gs.statcounter.com/os-version-market-share/android/mobile-tablet/worldwide

[11] ——, "Mobile & tablet ios version market share worldwide," 2017, (Abgerufen am 05/21/2018). [Online]. Available: http://gs.statcounter.com/os-version-market-share/ios/mobile-tablet/worldwide

[12] ——, "Operating system market share worldwide," 2017, (Abgerufen am 01/05/2018). [Online]. Available: http://gs.statcounter.com/os-market-share

[13] T. Byron, "Safer children in a digital world: The report of the byron review: Be safe, be aware, have fun," 2008.

[14] M. Sharples, R. Graber, C. Harrison, and K. Logan, "E-safety and web 2.0 for children aged 11–16," *Journal of Computer Assisted Learning*, vol. 25, no. 1, pp. 70–84, 2009.

[15] "Endegut.info," Feb 2015, (Abgerufen am 05/21/2018). [Online]. Available: http://www.endegut.info

[16] P. Hernandez. (2017) Pewdiepie says he's going to stop making nazi jokes after charlottesville. (Abgerufen am 05/21/2018). [Online]. Available: https://kotaku.com/pewdiepie-says-hes-going-to-stop-making-nazi-jokes-afte-1797904266

[17] G. S. O'Keeffe, K. Clarke-Pearson *et al.*, "The impact of social media on children, adolescents, and families," *Pediatrics*, vol. 127, no. 4, pp. 800–804, 2011.

[18] D. L. Borzekowski, S. Schenk, J. L. Wilson, and R. Peebles, "e-ana and e-mia: A content analysis of pro–eating disorder web sites," *American journal of public health*, vol. 100, no. 8, pp. 1526–1534, 2010.

[19] (2018) mpa. (Abgerufen am 05/21/2018). [Online]. Available: http://www.myproana.com/index.php/forum/62-anorexia-discussions/

[20] (2018) Wohlbeleibt.de - ein forum für wohlbeleibte - und für deren verehrer. (Abgerufen am 05/21/2018). [Online]. Available: http://www.wohlbeleibt.de/phpBB3/viewforum.php?f=15

[21] Bundesministerium für Digitalisierung und Wirtschaftsstandort, "RIS - Urheberrechtsgesetz - Bundesrecht konsolidiert, Fassung vom 22.05.2018," Mai 2018, (Abgerufen am 05/21/2018). [Online]. Available: https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10001848

[22] C. Herrle. (2018) Abmahnung für george clooneys kriminaldrama „suburbicon". (Abgerufen am 05/21/2018). [Online]. Available: https://www.anwalt.de/rechtstipps/abmahnung-fuer-george-clooneys-kriminaldrama-suburbicon_134457.html

[23] K.-K. R. Choo and A. I. of Criminology, *Online child grooming: a literature review on the misuse of social networking sites for grooming children for sexual offences*. Australian Institute of Criminology Canberra, 2009, vol. 103.

[24] H. Leymann, "The content and development of mobbing at work," *European journal of work and organizational psychology*, vol. 5, no. 2, pp. 165–184, 1996.

[25] M. A. Campbell, "Cyber bullying: An old problem in a new guise?" *Journal of Psychologists and Counsellors in Schools*, vol. 15, no. 1, pp. 68–76, 2005.

[26] J. Krebs. (2017) Suizid von sabrina (†13): Das sagt gerichtspsychiater josef sachs über das «du wirst sterben»-video. (Abgerufen am 05/21/2018). [Online]. Available: https://www.aargauerzeitung.ch/schweiz/suizid-von-sabrina-13-das-sagt-gerichtspsychiater-josef-sachs-ueber-das-du-wirst-sterben-video-131793312

[27] San Jose State University. Links to hate groups. (Abgerufen am 05/21/2018). [Online]. Available: http://www.sjsu.edu/faculty/Brent/190/hatelinks.html

[28] D. A. Herati, A. Bojamma, and M. I. Gandhi, "Countermeasures to ransomware threats," 04 2018.

[29] M. L. Pittaro, "Cyber stalking: An analysis of online harassment and intimidation," *International Journal of Cyber Criminology*, vol. 1, no. 2, pp. 180–197, 2007.

[30] H. Dressing, A. Anders, C. Gallas, and J. Bailer, "Cyberstalking: Prevalence and impact on victims," *Psychiatrische Praxis*, vol. 38, no. 7, pp. 336–341, 2011.

[31] T. Kleinz. (2017) Terroristen online: Der islamist von nebenan. (Abgerufen am 05/21/2018). [Online]. Available: https://www.heise.de/newsticker/meldung/Terroristen-online-Der-Islamist-von-nebenan-3708980.html

[32] LLC Mail Ru. (2018) Icq with voice and video calls, free messages. (Abgerufen am 05/23/2018). [Online]. Available: https://icq.com/windows/de

[33] Bitdefender. (2018) How can i block certain apps with parental control? (Abgerufen am 05/23/2018). [Online]. Available: https://www.bitdefender.com/support/how-can-i-block-certain-apps-with-parental-control-1196.html

[34] Forcepoint. (2018) Blocking by file extension. (Abgerufen am 05/26/2018). [Online]. Available: https://www.websense.com/content/support/library/web/hosted/admin_guide/exten_block.aspx

[35] Apple Inc. (2018) macOS Sierra: Logs dialog of Parental Controls System Preferences. (Abgerufen am 05/23/2018). [Online]. Available: https://support.apple.com/kb/PH25531?viewlocale=en_US&locale=en_US

[36] CurrentWare. (2018) Block downloads from the internet. (Abgerufen am 05/23/2018). [Online]. Available: http://www.currentware.com/block-downloads-from-internet

[37] Windows 7 Teacher, "Allow or block games in parental control | windows 7 teacher," Mai 2018, (Abgerufen am 05/23/2018). [Online]. Available: http://www.windows7teacher.com/security-tutorials/621/allow-or-block-games-in-parental-control.html

[38] Webroot, "Internet pornography by the numbers a significant threat to society," Mai 2018, (Abgerufen am 05/23/2018). [Online]. Available: https://www.webroot.com/us/en/resources/tips-articles/internet-pornography-by-the-numbers

[39] klicksafe.de, "So suchen kinder und jugendliche," Mai 2018, (Abgerufen am 05/23/2018). [Online]. Available: https://www.klicksafe.de/themen/suchen-recherchieren/suchmaschinen/so-suchen-kinder-und-jugendliche

[40] Google. (2018) Anstößige suchergebnisse auf google mit safesearch blockieren - android-gerät - hilfe für google-suche. (Abgerufen am 05/23/2018). [Online]. Available: https://support.google.com/websearch/answer/510?co=GENIE.Platform%3DAndroid&hl=de

[41] W. Glenn, "How to set time limits for a regular account in windows 10," April 2016, (Abgerufen am 05/23/2018). [Online]. Available: https://www.howtogeek.com/250224/how-to-set-time-limits-for-a-regular-account-in-windows-10

[42] R. Ranbe. (2018) How to block ports on a computer | chron.com. (Abgerufen am 05/26/2018). [Online]. Available: http://smallbusiness.chron.com/block-ports-computer-54658.html

[43] Comodo. Whitelist vs blacklist. (Abgerufen am 05/23/2018). [Online]. Available: https://securebox.comodo.com/whitelist-vs-blacklist/

[44] S. Mueller. Kinderserver. (Abgerufen am 05/23/2018). [Online]. Available: https://www.blinde-kuh.de/jugendschutz/kinderserver.html

[45] Ars Nova Systems. (2017) Parentsaround.com. (Abgerufen am 05/23/2018). [Online]. Available: https://www.parentsaround.com/

[46] Bitdefender. (2018) Internet security multi-device 2018. (Abgerufen am 05/23/2018). [Online]. Available: https://www.bitdefender.de/solutions/internet-security.html

[47] Symantec Corporation. (2018) News und events. (Abgerufen am 05/23/2018). [Online]. Available: http://www1.k9webprotection.com/

[48] Bullguard. (2018) Kindersicherung – Übersicht. (Abgerufen am 05/23/2018). [Online]. Available: https://www.bullguard.com/support/product-guides/internet-security/guides-for-current-version/parental-control.aspx

[49] BUHL Data Service GmbH. (2018) Schutz vor viren und datendiebstahl wiso internet security 2018. (Abgerufen am 05/23/2018). [Online]. Available: https://www.buhl.de/produkte/wiso-internet-security

[50] Content Watch Holdings, Inc. (2017) The most-trusted parental control software, helping millions of parents since 1996. (Abgerufen am 05/23/2018). [Online]. Available: https://www.netnanny.com/

[51] J. Beineke. (2015) Surf-sitter 6. (Abgerufen am 05/23/2018). [Online]. Available: https://www.heise.de/download/product/surf-sitter-89685

[52] U. Reuther. (2015) Aus die maus! - computerzeitbegrenzung für kinder. (Abgerufen am 05/23/2018). [Online]. Available: http://ausdiemaus.die4reuthers.de/

[53] E. Corporation. (2018) Sicheres surfen im netz für ihre kinder. (Abgerufen am 05/23/2018). [Online]. Available: https://www.entensys.com/de/products/kindergate-parental-control/overview

[54] ESET, spol. s r.o. (2018) Sicher im netz unterwegs. (Abgerufen am 05/23/2018). [Online]. Available: https://www.eset.com/de/home/internet-security/

[55] F-Secure. (2018) F-secure safe — internet security for all devices. (Abgerufen am 05/23/2018). [Online]. Available: https://www.f-secure.com/en/web/home_global/safe

[56] G DATA Software AG. (2018) Multi device security für windows, macos und android | g data. (Abgerufen am 05/23/2018). [Online]. Available: https://www.gdata.at/shop/multi-device-security

[57] Infoweise. (2018) Ultimate parental control software. (Abgerufen am 05/23/2018). [Online]. Available: https://www.secureteen.com/

[58] JusProg. (2018) Für eltern. (Abgerufen am 05/23/2018). [Online]. Available: https://www.jugendschutzprogramm.de/

[59] K. Lab, "Kaspersky safe kids," 2017, (Abgerufen am 08/28/2017). [Online]. Available: https://www.kaspersky.de/safe-kids

[60] McAfee, LLC. . (2018) Safe family. (Abgerufen am 05/23/2018). [Online]. Available: https://family.mcafee.com/

[61] M. Müller. Parents friend -die sicherheitszentrale für den pc-. (Abgerufen am 05/23/2018). [Online]. Available: http://www.parents-friend.de

[62] Microsoft. (2017) Was ist microsoft family? (Abgerufen am 05/23/2018). [Online]. Available: https://support.microsoft.com/de-de/help/12413/microsoft-account-what-is-family

[63] Mobicip, LLC. (2018) Trusted and most advanced parental controls for your family's devices. (Abgerufen am 05/23/2018). [Online]. Available: http://www.mobicip.com/

[64] Symantec Corporation. (2018) Norton family premier. (Abgerufen am 05/23/2018). [Online]. Available: https://at.norton.com/norton-family-premier

[65] Cisco. (2018) Family shield by opendns. (Abgerufen am 05/23/2018). [Online]. Available: https://signup.opendns.com/familyshield/

[66] ProtectCom GmbH. (2018) Das ultimative tool zur pc Überwachung. (Abgerufen am 05/23/2018). [Online]. Available: https://www.protectcom.de/orvell-monitoring/

[67] Quick Heal Technologies Limited. (2018) Quick heal total security. (Abgerufen am 05/23/2018). [Online]. Available: https://www.quickheal.co.in/home-users/quick-heal-total-security

[68] Qustodio LLC. (2018) Die beste kostenlose app für elternkontrolle im internet. (Abgerufen am 05/23/2018). [Online]. Available: https://www.qustodio.com/de/

[69] SafeDNS, Inc. (2018) Secure internet for home and business | safedns. (Abgerufen am 05/23/2018). [Online]. Available: https://www.safedns.com/de/parental-controls/

[70] Salfeld Computer GmbH. (2018) Kindersicherung für pcs, smartphones und tablets. (Abgerufen am 05/23/2018). [Online]. Available: https://salfeld.de/kindersicherung/

[71] SentryPC. (2018) Monitor. filter. control. (Abgerufen am 05/23/2018). [Online]. Available: https://www.sentrypc.com/

[72] Grote, Matthias. (2015) Telekom kinderschutz software 4. (Abgerufen am 05/23/2018). [Online]. Available: https://www.heise.de/download/product/telekom-kinderschutz-software-95842

[73] Trend Micro Incorporated. (2018) Internet security-software – internetschutz. (Abgerufen am 05/23/2018). [Online]. Available: http://www.trendmicro.de/produkte/internet-sicherheitssoftware/index.html

[74] Tueagles. (2014) Anti porno - blockieren pornoseiten - internetsperren und filter-software. (Abgerufen am 05/23/2018). [Online]. Available: http://www.tueagles.com/anti-porn/de/

[75] EPTIMUM. Witigo logiciel contrôle parental windows 7 8 10. (Abgerufen am 05/23/2018). [Online]. Available: http://www.witigo.eu/produits/witigo-parental-filter-pour-windows

[76] S. Chen. (2018) 10 best parental controls software for both mobile and pc. (Abgerufen am 05/23/2018). [Online]. Available: https://webcache.googleusercontent.com/search?q=cache:aPeE4jiSP50J:https://www.spyzie.com/parental-controls/parental-control-software.html+&cd=2&hl=de&ct=clnk&gl=at&client=firefox-b-ab

[77] Antropia. (2016) Care4kids - kindersicherung – apps bei google play. (Abgerufen am 05/26/2018). [Online]. Available: https://play.google.com/store/apps/details?id=com.antropia.care4kids&hl=de

[78] Avira Operations GmbH & Co. KG. (2018) Avira applock+ – schützen sie ihre apps mit einem pin-code. (Abgerufen am 05/26/2018). [Online]. Available: https://www.avira.com/de/avira-applock-plus

[79] Bear Lock Applock. (2018) App Sperre - Applock, Kindersicherung - Apps bei Google Play. (Abgerufen am 05/26/2018). [Online]. Available: https://play.google.com/store/apps/details?id=com.bear.applock

[80] Deity Kids. (2016) Kinderland – apps bei google play. (Abgerufen am 05/26/2018). [Online]. Available: https://play.google.com/store/apps/details?id=net.godsof.kidsworld&hl=de_AT

[81] MicroWorld Tech Inc. (2018) escan mobile security – apps bei google play. (Abgerufen am 05/26/2018). [Online]. Available: https://play.google.com/store/apps/details?id=com.eScan.main&hl=de_AT

[82] Eturi Corp. (2016) Ourpact everywhere. (Abgerufen am 05/26/2018). [Online]. Available: https://ourpact.com/

[83] Funamo, Inc. (2018) Funamo kindersicherung – apps bei google play. (Abgerufen am 05/26/2018). [Online]. Available: https://play.google.com/store/apps/details?id=funamo.funamo&hl=de_AT

[84] IT HK SERVICE LIMITED. (2017) Kid-modus - kindersicherung – apps bei google play. (Abgerufen am 05/26/2018). [Online]. Available: https://play.google.com/store/apps/details?id=hk.ithkservice.kidlock&hl=de_AT

[85] Jelly Ansns. (2016) Child lock – apps bei google play. (Abgerufen am 05/26/2018). [Online]. Available: https://play.google.com/store/apps/details?id=com.jelly.timelock.newtimelockwithads

[86] J. Lochmann. Jolo kindersicherung. (Abgerufen am 05/26/2018). [Online]. Available: https://jolo.software/de/kindersicherung/

[87] kiddoware. (2018) Kids place mit kindersicherung und -sperre – apps bei google play. (Abgerufen am 05/26/2018). [Online]. Available: https://play.google.com/store/apps/details?id=com.kiddoware.kidsplace&referrer=utm_source%3Dkiddoware_website%26utm_medium%3Dwebsite%26utm_caign%3Dwebsite

[88] KIDOZ. (2018) Kidoz kinder spiele & videos – apps bei google play. (Abgerufen am 05/26/2018). [Online]. Available: https://play.google.com/store/apps/details?id=com.kidoz

[89] Mobile Fence. (2018) Mobile fence parental control – apps bei google play. (Abgerufen am 05/26/2018). [Online]. Available: https://play.google.com/store/apps/details?id=com.mobilefence.family&hl=gsw

[90] M-Way Solutions GmbH. (2018) familee kids – apps bei google play. (Abgerufen am 09/26/2017). [Online]. Available: https://play.google.com/store/apps/details?id=com.familee.kid&hl=de

[91] Out of the Park Apps. (2018) Kids zone - kindersicherung & android-jugendschutz – apps bei google play. (Abgerufen am 05/26/2018). [Online]. Available: https://play.google.com/store/apps/details?id=com.ootpapps.kids.zone.app.lock&hl=de_AT

[92] protectyourkid. (2018) Die kindersicherung und all-in-one kinderschutz-app für android handys/smartphones und tablets. (Abgerufen am 05/26/2018). [Online]. Available: http://www.protectyourkid.de/

[93] Safe Lagoon Software. (2017) Healthy online experiences and digital protection for your children. (Abgerufen am 05/26/2018). [Online]. Available: https://safelagoon.com/de/

[94] SaferKid. (2016) Protect children from meeting strangers online with saferkid™. (Abgerufen am 05/26/2018). [Online]. Available: https://www.saferkid.com/

[95] Samsung Electronics Co., Ltd. (2018) Kindermodus – apps bei google play. (Abgerufen am 05/26/2018). [Online]. Available: https://play.google.com/store/apps/details?id=com.sec.android.app.kidshome&hl=de_AT

[96] Screen Time Labs. (2018) Screen time elternaufsicht – apps bei google play. (Abgerufen am 05/26/2018). [Online]. Available: https://play.google.com/store/apps/details?id=com.screentime.rc

[97] ThraceCode Inc. (2015) Kinder sperre, kinder barriere – apps bei google play. (Abgerufen am 05/26/2018). [Online]. Available: https://play.google.com/store/apps/details?id=com.thracecodeinc.LittleHands&hl=de

[98] Trend Micro. (2018) Mobile security & antivirus – apps bei google play. (Abgerufen am 05/26/2018). [Online]. Available: https://play.google.com/store/apps/details?id=com.trendmicro.tmmspersonal&hl=de

[99] Whisper Arts. (2018) Kid's shell - safe kids-modus – apps bei google play. (Abgerufen am 05/26/2018). [Online]. Available: https://play.google.com/store/apps/details?id=com.whisperarts.kidsshell

[100] tele.ring, "Schlauberger machen sicheres surfen zum kinderspiel," (Abgerufen am 01/15/2018). [Online]. Available: https://www.telering.at/kinderschutz/

[101] Stiftung Warentest. (2018) Tracking: Wie unser surfverhalten überwacht wird – und was dagegen hilft. (Abgerufen am 05/26/2018). [Online]. Available: https://www.test.de/Tracking-Wie-unser-Surfverhalten-ueberwacht-wird-und-was-dagegen-hilft-5221609-0/

[102] R. Hill, "uBlock - Home," https://www.ublock.org/, 2017, (Abgerufen am 01/20/2018).

[103] eyeo GmbH, “Adblock plus - für ein web ohne nervige werbung!” https://adblockplus.org/de/, 2017, (Abgerufen am 01/20/2018).

[104] W. Glenn. (2016) How to block (or allow) certain applications for users in windows. (Abgerufen am 05/26/2018). [Online]. Available: https://www.howtogeek.com/howto/8739/restrict-users-to-run-only-specified-programs-in-windows-7/

[105] TunnelBear Inc., “Tunnelbear: Secure vpn service,” https://www.tunnelbear.com/, 2018, (Abgerufen am 01/20/2018).

[106] M. O’Neill. (2015) How to block users from installing software on your windows computer. (Abgerufen am 05/26/2018). [Online]. Available: https://www.makeuseof.com/tag/block-users-installing-software-windows-computer/

[107] Computer Hope. (2018) How to disable the usb ports. (Abgerufen am 05/26/2018). [Online]. Available: https://www.computerhope.com/issues/ch001554.htm

[108] Opera Software, “Browser opera portable,” http://www.opera.com/de/computer/portable, 2017, (Abgerufen am 01/20/2018).

[109] Refog, “Keylogger downloaden kostenlos! german-deutsch,” https://de.refog.com/keylogger/, 2017, (Abgerufen am 01/20/2018).

[110] M. Anastasiou. (2018) How to enable or disable cd/dvd rom (win xp/vista/7/8). (Abgerufen am 05/26/2018). [Online]. Available: http://michael.anastasiou.me/how-to-enable-or-disable-cd-dvd-rom/

[111] ESET. (2018) Funktionen der kindersicherung in eset smart security premium, eset smart security und eset internet security. (Abgerufen am 05/23/2018). [Online]. Available: https://support.eset.com/kb3074/?locale=en_US&viewlocale=de_DE

[112] Symantec Corporation. (2009) What do p2p applications do and how to block peer to peer applications (p2p) using symantec endpoint protection? (Abgerufen am 05/26/2018). [Online]. Available: https://www.symantec.com/connect/articles/what-do-p2p-applications-do-and-how-block-peer-peer-applications-p2p-using-symantec-endpoin

[113] Google. (2018) Einstellungen für den spamfilter individuell anpassen - hilfe für g suite-administrator. (Abgerufen am 05/26/2018). [Online]. Available: https://support.google.com/a/answer/2368132?hl=de

[114] GMX. (2018) Spamschutz-einstellungen - gmx hilfe. (Abgerufen am 05/26/2018). [Online]. Available: https://hilfe.gmx.net/email/spam-und-viren/spamschutz-einstellungen.html

[115] fragFINN e.V., "fragfinn - die suchmaschine für kinder," https://www.fragfinn.de/, 2018, (Abgerufen am 01/20/2018).

[116] ——. (2018) fragfinn-suchmaschine als startseite einrichten. (Abgerufen am 05/26/2018). [Online]. Available: https://eltern.fragfinn.de/eltern/fragfinn-als-startseite/anleitung-fuer-chrome/

[117] S. Kosta, "Computersucht bei übergewichtigen/adipösen kindern und jugendlichen," Ph.D. dissertation, uniwien, 2008.

[118] C. A. Anderson, A. Sakamoto, D. A. Gentile, N. Ihori, A. Shibuya, S. Yukawa, M. Naito, and K. Kobayashi, "Longitudinal effects of violent video games on aggression in japan and the united states," *Pediatrics*, vol. 122, no. 5, pp. e1067–e1072, 2008.

[119] OpenDNS. (2018) Familyshield router configuration instructions. (Abgerufen am 05/26/2018). [Online]. Available: https://support.opendns.com/hc/en-us/articles/228006487-FamilyShield-Router-Configuration-Instructions

[120] Frankfurter Allgemeine Zeitung GmbH. (2017) Lka warnt vor neuer betrugsmasche via telefon. (Abgerufen am 04/22/2018). [Online]. Available: http://www.faz.net/aktuell/gesellschaft/kriminalitaet/lka-warnt-vor-neuer-betrugsmasche-via-telefon-14925168.html

[121] C. Southworth, J. Finn, S. Dawson, C. Fraser, and S. Tucker, "Intimate partner violence, technology, and stalking," *Violence against women*, vol. 13, no. 8, pp. 842–856, 2007.

[122] A. Inc. (2016) Screenshots. [Online]. Available: https://itunes.apple.com/ch/app/witigo-content-filter/id1130261635?mt=8

[123] ORACLE, "Virtualbox," 2017, (Abgerufen am 09/10/2017). [Online]. Available: https://www.virtualbox.org/

[124] Apple Inc. (2018) Kindersicherung auf dem iphone, ipad oder ipod touch ihres kindes verwenden. (Abgerufen am 05/27/2018). [Online]. Available: https://support.apple.com/de-at/HT201304

[125] ——, "Managing apps with itunes 12.7 or later," 2018, (Abgerufen am 04/05/2018). [Online]. Available: https://discussions.apple.com/docs/DOC-12234

[126] Anne Va. (2011) Parental control time-limits being bypassed. (Abgerufen am 05/28/2018). [Online]. Available: https://answers.microsoft.com/en-us/windows/forum/windows_vista-security/parental-control-time-limits-being-bypassed/15ee8532-8167-4ebd-aa96-8909e72379da

[127] hcornea. (2015) Device time change to get around curfews win7 x64. (Abgerufen am 05/26/2018). [Online]. Available: https://community.norton.com/en/forums/device-time-change-get-around-curfews-win7-x64

[128] G. Phillips. (2016) 7 ways your children might bypass parental control software. (Abgerufen am 05/28/2018). [Online]. Available: https://www.makeuseof.com/tag/7-ways-children-might-bypass-parental-control-software/

[129] B. Collins. (2015) How your kids are beating your parental controls and is there anything you can do? (Abgerufen am 05/28/2018). [Online]. Available: http://www.expertreviews.co.uk/software/internet-security/1402585/how-your-kids-are-beating-your-parental-controls-and-is-there

[130] Beginner_Hacks. (2015) Any ideas for hacking parental controls? (Abgerufen am 05/28/2018). [Online]. Available: https://null-byte.wonderhowto.com/forum/any-ideas-for-hacking-parental-controls-0163701/

[131] P. Meserole. Is it possible for children to hack screen time? (Abgerufen am 05/28/2018). [Online]. Available: https://www.quora.com/Is-it-possible-for-children-to-hack-screen-time

[132] King406. (2016) My parents have a long history of using parental controls on my pc. recently, it's gotten to the breaking point. (Abgerufen am 05/28/2018). [Online]. Available: https://www.reddit.com/r/pcmasterrace/comments/4mtp6k/my_parents_have_a_long_history_of_using_parental/

[133] Jabari. (2017) 4 ways teens bypass parental control software and how you can battle back. (Abgerufen am 05/28/2018). [Online]. Available: http://www.pdlsolutions.com/parent-resources/4-ways-teens-bypass-parental-control-software-and-how-you-can-battle-back/

[134] A. Gonzalez. (2017) Überwachen sie alles was am pc und internet gemacht wird! (Abgerufen am 05/28/2018). [Online]. Available: https://www.windows-keylogger.com/

[135] HeavenWard. (2018) Bester keylogger | der mächtige, kleine keylogger. (Abgerufen am 05/28/2018). [Online]. Available: http://www.hwsuite.de/besterkeylogger-ist-der-m%C3%A4chtige-kleine-keylogger-f%C3%BCr-windows-8.php

[136] C. Hoffman. (2014) Why you shouldn't use mac address filtering on your wi-fi router. (Abgerufen am 05/28/2018). [Online]. Available: https://www.howtogeek.com/204458/why-you-shouldn%E2%80%99t-use-mac-address-filtering-on-your-wi-fi-router/

[137] Nilsz12345. (2012) Wer kennt sich mit salfeld kindersicherung aus? (Abgerufen am 05/28/2018). [Online]. Available: https://www.gutefrage.net/frage/wer-kennt-sich-mit-salfeld-kindersicherung-aus

[138] Rabid Viper Productions. (2017) Assaultcube. (Abgerufen am 05/26/2018). [Online]. Available: https://assault.cubers.net/

[139] SRWare. (2016) Srware iron: Der browser der zukunft. (Abgerufen am 05/26/2018). [Online]. Available: https://www.srware.net/software_srware_iron.php

[140] M. Maciej. (2015) Google safesearch ausschalten, deaktivieren und sperren: Jugendschutzeinstellungen für die suche. (Abgerufen am 05/28/2018). [Online]. Available: https://www.giga.de/webapps/google-suche/tipps/google-safesearch-ausschalten-deaktivieren-und-sperren-jugendschutzeinstellungen-fuer-die-suche/

[141] (2018) Duckduckgo. (Abgerufen am 05/28/2018). [Online]. Available: https://duckduckgo.com/

[142] (2018) Lassen sie startpage für ihre privatsphäre arbeiten. (Abgerufen am 05/28/2018). [Online]. Available: https://www.startpage.com/

[143] (2018) Qwant internet. (Abgerufen am 05/28/2018). [Online]. Available: https://www.qwant.com/

[144] Kasperle. (2014) fritzbox 7240 wlan, heimnetz ip´s sperren, kindersicherung, jugendschutz. (Abgerufen am 05/28/2018). [Online]. Available: https://www.ip-phone-forum.de/threads/fritzbox-7240-wlan-heimnetz-ip%C2%B4s-sperren-kindersicherung-jugendschutz.259733/

[145] (2018) Wayback Machine. (Abgerufen am 05/28/2018). [Online]. Available: https://web.archive.org

[146] Screentime. (2018) My children are able to use their devices longer than the daily limit i set. (Abgerufen am 05/28/2018). [Online]. Available: https://screentimelabs.com/de/help/daily-limit-exceeded/

[147] Z. Karbhari. (2016) Device control software. (Abgerufen am 05/30/2018). [Online]. Available: http://www.copynotify.com/DeviceControl.html

[148] C. Lestoc. (2018) 5 best software to block usb ports and prevent instruders. (Abgerufen am 05/30/2018). [Online]. Available: https://windowsreport.com/block-usb-ports-software/

[149] C. C. Andrews. Spying on your child: the good, the bad, and the ugly - educate empower kids. (Abgerufen am 05/30/2018). [Online]. Available: https://educateempowerkids.org/spying-child-good-bad-ugly/

[150] C. Hoffman. (2013) What parents need to know about web filtering and parental controls. (Abgerufen am 05/31/2018). [Online]. Available: https://www.howtogeek.com/177469/what-parents-need-to-know-about-web-filtering-and-parental-controls/

[151] Microsoft. (2018) Run and runonce registry keys. (Abgerufen am 05/31/2018). [Online]. Available: https://msdn.microsoft.com/en-us/library/windows/desktop/aa376977(v=vs.85).aspx

[152] PLJ Soft. (2018) Nosafemode. (Abgerufen am 05/31/2018). [Online]. Available: http://www.pljsoft.fr/NoSafeMode_Main.html

[153] admin. Disable windows safe mode. (Abgerufen am 05/31/2018). [Online]. Available: http://thetechnologygeek.org/disable-windows-safe-mode/

[154] T. Nimmerjahn. (2018) Whitelist call blocker - apps on google play. (Abgerufen am 05/31/2018). [Online]. Available: https://play.google.com/store/apps/details?id=de.tn_software.callblocker&hl=en_US

[155] A. Kaliturin. (2017) Blacklist call & sms blocker. (Abgerufen am 05/31/2018). [Online]. Available: https://play.google.com/store/apps/details?id=com.kaliturin.blacklist

[156] iDevBR Team. (2015) iblacklist for iphone. (Abgerufen am 05/31/2018). [Online]. Available: http://www.iblacklist.com.br/