FERDINAND PORSCHE
FERN FH

Gefahren im Internet für ältere Menschen durch Malware

Bachelorarbeit I

am

Studiengang „Aging Services Management“
an der Ferdinand Porsche FernFH

Verena Kis, BA
11716439

Begutachter: Ing. DI Andreas Eisenbock, BA MA

Schönkirchen-Reyersdorf, Februar 2022

Eidesstattliche Erklärung

Ich erkläre hiermit, dass ich die vorliegende Arbeit selbstständig und ohne Benutzung anderer als der angegebenen Quellen und Hilfsmittel angefertigt habe. Alle Stellen, die wörtlich oder sinngemäß übernommen wurden, habe ich als solche kenntlich gemacht. Die Arbeit wurde in gleicher oder ähnlicher Form noch keiner anderen Prüfungsbehörde vorgelegt oder veröffentlicht.

06.02.2022 Unterschrift: 

Abstract

Das Ziel der vorliegenden Arbeit ist es, die Gefahren von bösartiger Software für ältere Menschen aufzuzeigen und geeignete Schutzmaßnahmen vorzustellen. Dadurch ergeben sich folgende Forschungsfragen: Welche Gefahren birgt Malware für ältere Menschen, die wenig Erfahrung und Kenntnis in der Internetnutzung haben und worauf ist dabei zu achten? Welche Maßnahmen können zur Prävention und zum Schutz gesetzt werden?

Um die Forschungsfragen zu beantworten, wurde eine Literaturanalyse gemacht, die sich vor allem am deutschsprachigen Raum orientiert. Gerade ältere Menschen mit wenig Erfahrung im Internet sind durch ihr Nutzungsverhalten gefährdeter, durch E-Mails oder Internetlinks ihre Computer durch Malware zu infizieren. Die Beschreibungen und Erklärungen der bekanntesten Malware-Typen, wie Computerviren, Trojaner und Computerwürmer, ergibt unterschiedliche Infizierungsmethoden, die von den Nutzer*innen erkannt und präventiv vermieden werden können. Durch geeignete Schutzmaßnahmen wie integrierte Firewalls, Antivirenprogramme und eine gesunde Skepsis gegenüber E-Mail-Anhängen, können sich auch ältere Menschen gut und einfach vor Malware schützen.

Schlüsselbegriffe: Malware, Senior*innen, Internet, Datensicherheit, Cybergefahr;

Abstract (englisch)

The aim of the work is to show the dangers of malicious software for older people and to present suitable protective measures. This results in the following research questions: What are the dangers of malware for older people who have little experience and knowledge of using internet and what to watch out for? Which measures are to use for prevention and protection? In order to answer the research questions, a literature analysis was written. The literature analysis concentrates mainly on the German-speaking world. Especially older people with only little experience on the internet are at risk of infecting their computers with malware through their usage behavior by sending e-mails or opening internet links. The descriptions and explanations of the most well-known malware types, such as computer viruses, Trojans and computer worms, result in different infection methods that can be detected by users and preventively avoided. With appropriate protective measures such as built-in firewalls, antivirus programs and a healthy skepticism about e-mail attachments, even older people can protect themselves well and easily against malware.

Key words: malware, elderly people, internet, data security, cyber-crime;

Inhalt

Inhalt **4**

1. Einleitung **1**

1.1. Problemstellung und Forschungsfrage 1
1.2. Zielsetzung und Aufbau der Arbeit 2
1.3. Methode 4

2. Ältere Menschen im Internet **5**

2.1. Zahlen und Fakten 5
2.2. Nutzungsverhalten 7
2.3. Ängste und Sorgen älterer Menschen bei der Internetnutzung 9

3. Malware **11**

3.1. Computerviren 13
3.2. Würmer 14
3.3. Trojaner 16
3.4. Bots 17
3.5. Adware 18
3.6. Spyware 19
3.7. Phishing 19

4. Schutz und Gegenmaßnahmen **21**

4.1. Präventionsmaßnahmen speziell für ältere Menschen 21
4.2. Gefahren durch Malware erkennen 22
4.3. Gefahren durch Malware vermeiden 24
4.3.1. Antiviren-Programme 24
4.3.2. Firewall 25
4.3.3. Browser 25
4.3.4. Datensicherheit 27
4.4. Schadensbegrenzung betreiben 28

5. Diskussion und Beantwortung der Forschungsfragen **29**

6. Fazit und weiterer Ausblick **30**

7. Literaturverzeichnis 32

1. Einleitung

Die vorliegende Arbeit und die enthaltene Problemstellung sind gekennzeichnet durch Aktualität, Medienpräsenz und dem Anspruch, älteren Menschen die Gefahren des Internets zu erläutern, sowie Schutzmaßnahmen aufzuzeigen. Die Arbeit grenzt die Gefahren im Internet auf Malware ein und kommt somit auf folgenden Titel:

Gefahren im Internet für ältere Menschen durch Malware

„Malware“, also bösartige Software- „malicious“= bösartig, kann für jede und jeden Internetnutzer*in schwere technische Probleme hervorrufen. Schon in den Anfängen des Internets gab es erste Computerviren, die Schäden auf den betroffenen Geräten anrichteten. Malware wurde mit der vermehrten Internetnutzung immer größer, raffinierter und schwerer zu beseitigen. Malware bezeichnet nicht nur Computerviren, sondern auch Trojanische Pferde, Würmer, Bots und Spyware (Itzel, 2007, S.12ff).

Das Ziel all dieser Programme ist immer bösartiger Natur und dient meistens dazu, die arglosen Internetnutzer*innen um ihre persönlichen und sensiblen Daten zu erleichtern oder sich in private Computer einzuschleichen um dort verbotene Aktivitäten durchzuführen (Chatfield, 2013, S.80ff).

Malware ist also eine nicht zu unterschätzende Gefahr für alle Internetnutzer*innen weltweit. Doch während jüngere Menschen mit dem Wissen über diese Gefahren, mit Lösungsansätzen und Strategien gegen Gefahren im Internet aufwachsen, sind ältere Menschen oft mit diesen Themen überfordert und allein gelassen. Das Internet hat in der heutigen Gesellschaft einen hohen Stellenwert eingenommen und beeinflusst viele Bereiche unseres Lebens (Feuersinger, 2004, S.20ff).

1.1. Problemstellung und Forschungsfrage

Auch wenn die Internetnutzung und die selbstständige Zuhilfenahme von technischen Geräten für viele ältere Menschen eine große Erleichterung darstellen würde, so überwiegt oftmals noch die Angst vor Gefahren im Internet und das Unwissen, diese zu umgehen. Zum einen wird das Problem der „Digital Divide“, also der digitalen Spaltung zwischen den Generationen verdeutlicht, da ältere Menschen weniger vertraut mit der Internetnutzung sind, zum anderen das Problem der stetig präsenten Gefahren durch Malware im Internet.

Nach heutigen Forschungsständen verwenden immer mehr ältere Menschen das Internet und die Anzahl der Internetnutzer*innen steigt stetig. Um gerade diese Personengruppe vor Datendiebstahl, Hard- & Softwareproblemen und Viren zu schützen, braucht es mehr Maßnahmen und Strategien, wie ältere Menschen sich vor bösartiger Software schützen können. Diese eng miteinander verbundenen Probleme bringen mich zu folgender Forschungsfrage:

> *Welche Gefahren birgt Malware für ältere Menschen, die wenig Erfahrung und Kenntnis in der Internetnutzung haben und worauf ist dabei zu achten?*
> *Welche Maßnahmen können zur Prävention und zum Schutz gesetzt werden?*

1.2. Zielsetzung und Aufbau der Arbeit

In dieser Arbeit sollen die Gefahren für Internetnutzer*innen aufgezeigt werden, die durch bösartige Software ausgelöst werden und die gerade für (in der Internetnutzung unerfahrene) ältere Menschen eine nicht unerhebliche Gefahr für Datensicherheit und in weiterer Folge für ihre finanzielle Sicherheit, ihre Anonymität im Internet und ihre Geräte darstellt. Ziel ist insbesondere das Wissen, mit welcher Gefahr Nutzer*innen im Internet konfrontiert sind, sowie das Aufzeigen von Gegenmaßnahmen und wie diese zum Schutz etabliert werden können. Das Wissen über die bekanntesten Typen von bösartiger Software trägt dazu bei, die Funktionsweise zu verstehen, die Übertragungsweise zu erkennen und die persönlichen Daten zu schützen.

Medienberichte und Sensationsartikel schüren die Angst vor Computerviren oder Datendiebstahl und verleiten gerade unerfahrene Internetnutzer*innen dazu, sich gar nicht erst mit der Materie auseinanderzusetzen. Die Arbeit soll älteren Menschen dabei helfen, ohne Furcht das Medium Internet zu benutzen und ihnen das Wissen zu geben, wie sie sich, ihre Daten und ihre Geräte vor bösartigen Programmen schützen können. Durch das Studium “Aging Services Management” wurde ein besonderes Augenmerk auf die Personengruppe der älteren Menschen gelegt.

In der vorliegenden Arbeit wird zunächst erläutert, welche Rolle ältere Menschen im Internet spielen und warum gerade diese Gruppe gefährdet ist, Opfer von Malware-Angriffen zu werden. Auch eine Definition, welche Personengruppe in der vorliegenden Arbeit behandelt wird und warum das Alter eine wichtige Rolle spielt, wird im ersten Kapitel erläutert. Das Nutzungsverhalten im Internet von älteren Menschen unterscheidet sich gravierend von den jüngeren Generationen. Außerdem muss hier bedacht werden, dass jüngere Menschen von klein

auf mit dem Medium Internet, den Gefahren und den zu treffenden Schutzmaßnahmen aufwachsen, während viele ältere Menschen erst im höheren Alter mit dem Internet konfrontiert wurden und werden. Die Aktualität der Arbeit ist vor allem durch die Corona-Pandemie geprägt, da die Bevölkerung durch die verschiedensten Maßnahmen gezwungen ist, mehr Zeit zu Hause zu verbringen und es in den letzten Monaten vermehrt zu Kontaktbeschränkungen kam. Da Besuche bei Freunden und Familie nicht möglich waren, mussten auch ältere Menschen auf virtuelle Treffen im Internet umsteigen, wenn sie ihre Familie und Freunde sehen wollten. Das Risiko, auf fragwürdige Kommunikationsanbieter zu treffen, ist durch diese virtuellen Treffen während der Corona-Pandemie deutlich erhöht.

Das darauffolgende Kapitel widmet sich ganz dem Thema Malware. Beinahe jede*r Internetnutzer*in hat bereits theoretische Kenntnisse über bösartige Software oder wurde schon Opfer von Malware-Angriffen. Damit ist nicht zwingend ein Virus-Befall oder ein eingenisteter Trojaner gemeint, sondern auch verschiedenste Arten von Spyware und personalisierter Werbung, die garantiert jede*n Internetnutzer*in schon einmal betroffen haben. Das Kapitel zeigt die verschiedenen Arten von Malware auf und geht auf die Unterschiede ein, wie sie ein Gerät infizieren und wie sie sich vermehren. Auch Software, die primär keine Gefahr darstellt und nicht bösartig ist, sondern unerwünscht, wird in diesem Kapitel beschrieben, da die Vorgehensweise und die Verbreitungsart ähnlich zu den verschiedenen Malware-Typen ist und potenziell dabei hilft, Malware in ein Gerät einzuschleusen. Die Kenntnis über die Infizierungsmethode hilft dabei, Malware vorzubeugen und zu vermeiden.

Die Vermeidung und Prävention von Malware wird in Kapitel 4- Schutz und Gegenmaßnahmen eingehend beschrieben. Durch das Wissen über die Infizierungsmethoden und Merkmale der Malware-Typen, kann Malware auch von Menschen mit wenig Internet- und Technikerfahrung erkannt werden. Gerade ältere Menschen, die vermehrt E-Mail-Programme nutzen, können so einen Großteil aller schädlichen Angriffe schon frühzeitig abwenden. Trotz aller Vorsicht kann es nichtsdestotrotz passieren, dass bösartige Software einen Weg findet, das Gerät zu infizieren. Wird diese nicht von den technischen Abwehrprogrammen wie Firewall und Antiviren-Programmen abgehalten, sind die persönlichen Daten in Gefahr. Um diese zu schützen, wird auch kurz auf die Thematik Datenschutz, Datensicherheit und die Schadensbegrenzung eingegangen.

Zuletzt werden die aufgestellten Forschungsfragen beantwortet, sowie ein weiterer Ausblick gegeben, wie es in Zukunft mit den Gefahren, die von Malware ausgehen, weitergeht und welche

Angebote es für ältere Menschen gibt, die sich weiter mit dem Thema Internet und dessen Gefahren auseinandersetzen möchten.

1.3. Methode

Die vorliegende Bachelorarbeit ist eine Literaturanalyse und wurde mithilfe wissenschaftlicher Artikel, akademischer Abschlussarbeiten und Monografien, sowie Sammelbänden geschrieben. Die Literatur wurde in wissenschaftlichen Datenbanken und Bibliotheken recherchiert und gesammelt und ist am Ende in einem Literaturverzeichnis nach gängigen Zitierregeln angeführt. Durch die gewählte Methode erschafft die vorliegende Arbeit einen Zusammenhang zwischen den bereits veröffentlichten Werken und der aktuellen Problemstellung. Durch das Hinzuziehen aktueller Datenlagen und Fakten, wird die Aktualität der Arbeit hervorgehoben.

Schlüsselbegriffe/ Keywords: Nutzungsverhalten, Internet, Malware, Antivirenprogramme, Digitale Gefahren, Netzsicherheit, Ältere Menschen, Digital Divide

2. Ältere Menschen im Internet

Obwohl das Internet als Massenmedium gilt, werden ältere Menschen als Zielgruppe oft noch zu wenig beachtet. Durch technische Schwierigkeiten, Unwissenheit und dadurch, dass viele ältere Menschen den praktischen Nutzen und Sinn des Internets noch nicht kennen, ist eine Eingliederung des Internets in die Haushalte älterer Menschen schwieriger, als bei jüngeren Nutzer*innen.

Dieses Kapitel dient dazu, den Unterschied zwischen älteren und jüngeren Internetnutzer*innen aufzuzeigen. In dieser Arbeit werden ältere Personen aufgrund ihres chronologischen bzw. kalendarischen Alters charakterisiert, weshalb nur von Menschen ausgegangen wird, die zum Zeitpunkt der Befragungen über 65 Jahre alt waren. Diese Personengruppe ist deshalb so interessant, da sie einerseits noch vital ist und zu großen Teilen in Gesundheit lebt und sich andererseits in einem Alter befindet, in welchem die Menschen nicht mit dem Medium Internet aufgewachsen sind und in vielen Fällen auch in ihrer Erwerbstätigkeit und in ihrem Alltag noch nicht viel damit zu tun hatten. Ältere Menschen machen einen Großteil der Weltbevölkerung aus und dieser Anteil wird durch den demografischen Wandel in den nächsten Jahren noch weiter steigen. Umso wichtiger ist es, älteren Menschen, die noch nie oder nur wenig mit dem Internet zu tun hatten, die Vorteile und die Innovation des Netzes zu zeigen. Durch verschiedene Projekte im deutschsprachigen Raum wird und wurde erfolgreich versucht, interessierten älteren Menschen einen einfachen Einstieg ins Internet zu ermöglichen. Hierbei zeigte sich, dass ältere Menschen keineswegs uninteressiert an diesen Themen sind, sondern die technischen Hürden und die Unerfahrenheit eine zu große Angst mit sich bringen. Die Skepsis älterer Menschen gegenüber dem Internet wird oft fehlinterpretiert, da bedacht werden muss, dass sich viele ältere Menschen allem Neuen und Unbekanntem vergleichsmäßig skeptisch und vorsichtig verhalten- nicht nur der Technik und dem Internet gegenüber (Feuersinger, 2004, S.21).

2.1. Zahlen und Fakten

Das Internet hat in den letzten Jahren in allen Altersgruppen an Bedeutung zugenommen und spiegelt sich deutlich im Nutzungsverhalten wider. Massenmedien und das Internet nehmen an Bedeutung zu, wobei die Nutzer*innen sich je nach Altersgruppe in ihrem Nutzungsverhalten, in der Nutzungsdauer und der Nutzungshäufigkeit unterscheiden. Im Folgenden werden einige

Zahlen präsentiert, welche belegen, wie schnell sich auch ältere Menschen mit dem Thema Internet auseinandergesetzt haben und dieses regelmäßig nutzen.

Tabelle 1: Internetnutzer*innen 2021 in Österreich

Alter	Personen, die das Internet in den letzten 3 Monaten genutzt haben in %	Personen, die das Internet noch nie genutzt haben in %
16 bis 24 Jahre	100 %	-
25 bis 34 Jahre	99,8 %	0,2 %
35 bis 44 Jahre	98,9 %	0,4 %
45 bis 54 Jahre	97,1 %	2,0 %
55 bis 64 Jahre	88,9 %	7,9 %
65 bis 74 Jahre	65,5 %	29,8 %

(Statistik Austria, 2021)

Wie in Tabelle 1 gut ersichtlich ist, gibt es kaum Personen unter 50 Jahren in Österreich, die das Internet nicht als Medium nutzen. Im Vergleich zu Personen über 65 Jahren, wo knapp ein Drittel noch nie das Internet genutzt hat, ist dies ein signifikanter Unterschied. Hierbei ist zu beachten, dass die meisten Menschen, die aktuell über 65 Jahre alt sind, die meiste Lebenszeit und die längsten Jahre ihrer Erwerbstätigkeit nicht mit dem Internet und mit Computern verbracht haben.

Betrachtet man die Entwicklung der Internetnutzer*innen über die letzten 15 Jahre, so zeigt sich jedoch ein mehr als deutlicher Anstieg der Personen im höheren Alter:

Tabelle 2: Internetnutzer*innen 2005, 2010, 2015 und 2020 in Österreich

Alter	**2005**	2010	2015	2020
16 bis 24 Jahre	83,8 %	95,2 %	99,3 %	99,6 %
25 bis 34 Jahre	75,7 %	91,8 %	98,9 %	97,7 %
35 bis 44 Jahre	64,9 %	85,9 %	94,1 %	95,7 %
45 bis 54 Jahre	51,7 %	76,8 %	87,0 %	91,5 %
55 bis 64 Jahre	26,4 %	52,8 %	69,4 %	78,2 %

65 bis 74 Jahre	8,5 %	28,2 %	46,0 %	57,4 %

(Statistik Austria, 2021)

Gerade in den letzten 15 Jahren kam es zu einem rasanten Anstieg der Internetnutzer*innen über 65 Jahren. Ältere Menschen greifen aus den verschiedensten Gründen vermehrt auf das Internet zurück, was in Kapitel 2.2 noch genauer erörtert wird.

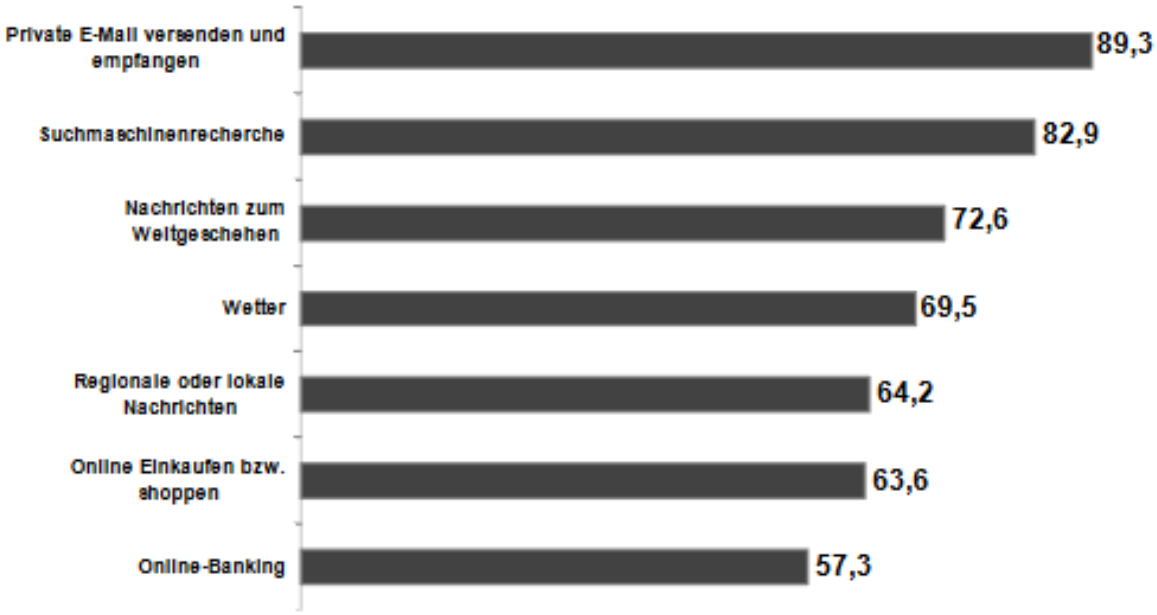
Nicht nur das Alter, auch das Geschlecht spielt in der Häufigkeit der Internetnutzung eine Rolle. Bei älteren Menschen sind über die Hälfte der Männer im Internet unterwegs, während bei den Frauen nur 34,3% online surfen (Donnerstag et al., 2012, S.251f).

Das Jahr 2020 und 2021 war geprägt durch die Corona-Pandemie, Lockdowns und das massive Einschränken des Alltags. Durch diese Maßnahmen verbrachten viele Menschen mehr Zeit in ihren Wohnungen und Häusern als in den Jahren zuvor. Dies spiegelt sich laut Statistik Austria auch in der Internetnutzung wider, wobei der Zuwachs der Internetnutzung auf ältere Menschen zurückzuführen ist. Nicht nur die Anzahl der älteren Internetanwender*innen, sondern auch die Häufigkeit der Internetnutzung ist in diesen zwei Jahren deutlich gestiegen. Durch die Pandemie verwenden demnach mehr ältere Leute das Internet als jemals zuvor und sie nutzen es viel häufiger als zuvor. Durch die Integration des Internets in den Alltag wurde bei vielen User*innen ein praktischer Nutzen und eine sinnvolle Beschäftigung entdeckt, sodass davon auszugehen ist, dass die Anzahl an Anwender*innen auch nach der Pandemie gleichbleibend hoch ausfällt.

2.2. Nutzungsverhalten

Zu Beginn lassen sich gravierende Unterschiede in der Nutzung des Internets auch zwischen gleichaltrigen Älteren feststellen. Diese liegen vor allem in der Vergangenheit der älteren Menschen und in der Technikaffinität. Ältere Menschen, die vor ihrer Pensionierung schon mit Computern und dem Internet zu tun hatten, unterscheiden sich häufig in ihrem Nutzungsverhalten nicht von jüngeren Generationen. Doch ältere Menschen, die nur wenig Vertrauen in Technik haben und die die Nutzung des Internets neu erlernen müssen und mussten, haben meist größere Zweifel und mehr Schwierigkeiten. In Abbildung 1 sind die Hauptgründe, für welche Tätigkeiten und Aufgaben ältere Menschen das Internet benutzen, angeführt.

Abbildung 1:



(Donnerstag et al., 2012, S.252)

Für ältere Menschen spielt vor allem der praktische Nutzen im Internet eine große Rolle. Anders als jüngere Anwender*innen, welche das Internet vor allem zur Kommunikation und zum Vergnügen verwenden, steckt bei älteren Menschen oft ein Informationsgewinn und der Erwerb von Wissen hinter ihrer Internetnutzung. Vor allem der E-Mail-Verkehr, welcher im privaten Bereich bei jüngeren Menschen abgenommen hat, ist für ältere Personen ein wichtiger Nutzungsbereich.

2010 führten private E-Mails, Tagesnachrichten aus aller Welt, das Wetter und Online-Banking die Liste der meistverwendeten Seiten von älteren Anwender*innen an. Auch regionale Nachrichten, sowie Veranstaltungen in der Nähe sind oft besuchte Webseiten bei älteren Internetnutzer*innen (Latzer et al, 2013, S.12 ff). Der Fakt, dass ältere Menschen mehr E-Mails verschicken und empfangen als die jüngere Generation, spielt beim Thema Malware noch eine große Rolle. Ältere Menschen werden somit durch ihr Nutzungsverhalten automatisch zu Zielen von Hackern und von bösartigen Programmen. In Kapitel 4.1.1 wird auf diesen Fakt noch genauer eingegangen.

Das Verwenden von Suchmaschinen wie beispielsweise Google ist - altersunabhängig - bei allen User*innen sehr häufig und beliebt. Gerade bei diesen Online-Recherchen und beim Einkaufsverhalten zeigt sich, dass ältere Menschen gegenüber Jüngeren öfter Preise vergleichen

und mehrere Webseiten zum selben Thema besuchen, bevor sie sich für ein Produkt oder eine Dienstleistung entscheiden. Auch Gesundheit steht bei älteren Menschen als Suchbegriff im Mittelpunkt. Ärztesuchen, Informationen über medizinische Beschwerden und Symptome, sowie Informationen über Medikamente werden häufig von älteren Nutzer*innen gesucht (Fittkau & Harms, 2012, S. 37).

2.3. Ängste und Sorgen älterer Menschen bei der Internetnutzung

Generell lässt sich sagen, dass es sowohl bei älteren als auch bei jüngeren Menschen zu Ängsten und Sorgen bezüglich der Internetnutzung kommt, wobei die Sorgen mit dem Alter ansteigen. Durch meist negative Schlagzeilen in Medien wird bei vielen Menschen, die noch nicht mit dem Internet in Kontakt waren, große Furcht und Angst vor negativen Konsequenzen ausgelöst (Ott & Hennewig, 2012, S.314f). Schon die Zugangsbarrieren, um überhaupt ins Internet zu gelangen, machen vielen älteren Menschen Sorgen. Zunächst benötigen sie zwangsweise eine (für sie meist teure) Hardware, die mit den oft kleinen Pensionen eine gut zu überlegende Investition darstellt. Wird davon ausgegangen, dass ältere Menschen nicht mit dem Smartphone im Internet surfen, brauchen sie ein internetfähiges Gerät zu Hause, wie beispielsweise einen Stand-PC oder einen Laptop. Hinzu kommen die Gebühren, um überhaupt das Internet nutzen zu können. Die Anschaffung und Inbetriebnahme der Geräte stellen eine erste Hürde dar, der sich viele Menschen noch nicht gewachsen fühlen. Hier ist die Mehrheit entweder auf technisch versierte Verwandte und Bekannte oder auf Fachleute angewiesen.

2013 wurde an der Universität Zürich eine landesweite Befragung durchgeführt, in welcher Personen aller Altersgruppen über ihre Sorgen und über mögliche Risiken der Internetnutzung befragt wurden. Hierbei zeigte sich, dass vor allem ältere Menschen, die wenig bis gar nicht das Internet nutzen, überdurchschnittlich besorgt waren. Sorgen machten sie sich demnach beispielsweise über wenig Glaubwürdigkeit der Internetmedien, sowie über den Missbrauch ihrer Daten. Im Umkehrschluss bedeutet das, dass Menschen, die vermehrt das Internet nutzen und sich Wissen darüber aneignen, sich weniger Sorgen um ihre Daten oder über einen möglichen Betrug machen (Latzer et al., 2013, S. 5ff).

Die Sorge über den Missbrauch von privaten Daten ist weit verbreitet und betrifft fast jede*n Internetnutzer*in mindestens einmal. Interessant hierbei ist, dass ältere Anwender*innen zwar statistisch besorgter in der Internetnutzung sind als Jüngere, jedoch nicht beim Thema Datenmissbrauch. Darunter wird verstanden, dass personenbezogene Daten wie Namen, Passwörter, Kontaktdaten oder Kontodaten, ohne Erlaubnis weitergegeben werden. Die größten

Sorgen bei Älteren sind demnach die Angst vor einer Kontrolle durch die Regierung und durch Unternehmen, sowie Sorge über das Bezahlen im Internet mit einer Kreditkarte. Hier haben die Anwender*innen jedoch nicht unbedingt Sorge um die Weitergabe der Kontodaten, sondern Angst, dass das Geld nicht beim gewünschten Empfänger bzw. bei der gewünschten Empfängerin ankommt. Obwohl den älteren Menschen die Angst vor den Gefahren im Internet in den letzten Jahren ein wenig genommen werden konnte, ist diese immer noch sehr hoch (Latzer et al., 2013, S.14ff).

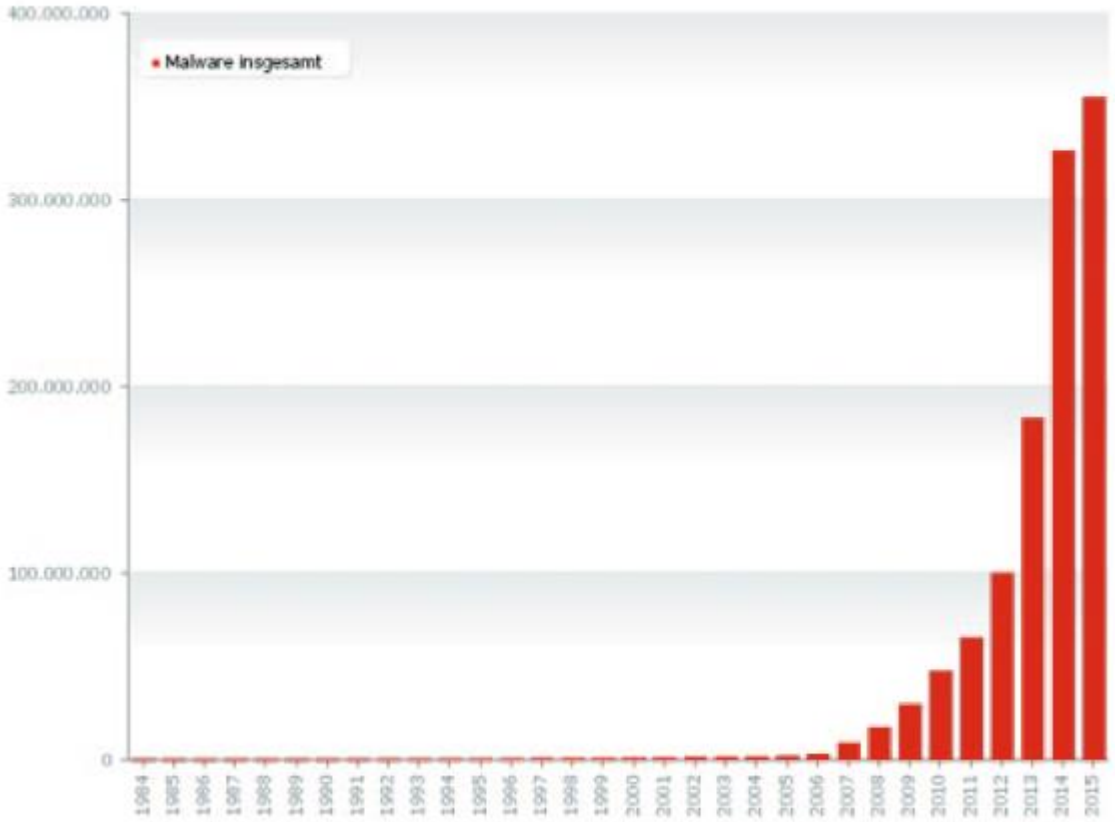
Spannend in diesem Rahmen ist, dass die Angst vor Malware als Begriff nicht stark vertreten ist. Dies liegt vermutlich daran, dass dieser für ältere Menschen nicht greifbar ist, nur schwer zu erkennen ist und erst zum Problem wird, wenn sich eine bösartige Software im System einnistet. Malware als Überbegriff ist im gesellschaftlichen Alltag noch nicht stark verbreitet, Computerviren und Trojanische Pferde hingegen schon, wobei die wenigsten diese voneinander unterscheiden können. Die Ängste und Sorgen über Datenmissbrauch und Malware lassen sich nur durch gezielte Aufklärung lösen, weshalb im Folgenden die Unterschiede der Malware-Arten erläutert werden.

3. Malware

Wie bereits in der Einleitung beschrieben, handelt es sich bei Malware um bösartige Software [Malicious Software]. Malware ist jedoch nur der Überbegriff von vielen schädlichen Programme, die sich auf Computern oder mobilen Geräten mit Internetzugang einnisten. Jedes dieser Programme kann unangenehme Folgen für die Nutzer*innen haben und wird ohne Zustimmung auf den Geräten installiert (Chatfield, 2013, S.80).
Wie bereits in Kapitel 2 beschrieben, ist die Angst vor Datenmissbrauch, vor Viren und Trojanern, sowie die Sorge etwas falsch zu machen, bei älteren Menschen sehr präsent. Gerade diese Unwissenheit und die Angst vor Fehlern, begünstigt die Verbreitung von Malware, da genau auf diese Sorgen gesetzt wird. Malware kann demnach vertrauenswürdig und sicher aussehen, sodass sich die Anwender*innen in Sicherheit wiegen. Viele Nutzer*innen haben Schwierigkeiten, Malware bei Updates oder Installationen von neuen Programmen und Software zu erkennen. Gerade für ältere, wenig mit dem Internet vertraute Personen, stellen demnach schon die regelmäßig durchzuführenden Updates der Geräte eine Herausforderung dar.

Malware wächst mit der Nutzung des Internets: Mehr User*innen begünstigen eine Vermehrung von schädlicher Software. Bereits in den Anfängen des Internets, 1971, konnten Programme identifiziert werden, welche sich bereits selbst auf Geräten vermehren konnten. Einige Jahre später gab es den ersten Trojaner und Angreifer gingen dazu über, Malware über Mail-Anhänge oder Internet-Links zu verbreiten (Chatfield, 2013, S. 80ff).
In Abbildung 2 wird deutlich, dass Malware in den letzten Jahren exponentiell gestiegen ist und vermutlich auch in den nächsten Jahren noch steigen wird.

Abbildung 2: Malware Wachstum



(Willems, 2013, S.11)

Die Gefahren von Malware für die einzelnen Internetnutzer*innen sind vielfältig und greifen in die verschiedensten Programme ein. Je nach Typus kommt es bei einem Malware-Angriff zum Ausspionieren von persönlichen Daten, bzw. das Merken von Tastenkombinationen wie Passwörter und PINs oder zur Überwachung aller Aktivitäten, die von den Nutzer*innen getätigt werden. Häufig wird auch von den betroffenen Geräten eine wahre Flut an Spam-Mails verschickt und der Rechner somit aus der Ferne manipuliert. Ebenso kommt es zur Manipulation von Sicherheitsprogrammen, Firewalls und Schutzmechanismen, sodass diese vom Schadprogramm deaktiviert oder beschädigt werden. Auch die Verschlüsselung der eigenen Daten mit darauffolgender Erpressung der User*innen ist eine Gefahr von Malware (Heuveline, 2015, S.102).

Die verbreitetsten und bekanntesten Malware-Typen werden im Folgenden vorgestellt.

3.1. Computerviren

Ein Computervirus ist die bekannteste Art von Malware und vermutlich auch die älteste. Zu Beginn waren Computerviren nicht bösartig und die Erzeuger*innen hatten keine kriminellen Absichten. Computerviren ähneln in vielen Zügen Krankheitsviren, da sie sich ebenso in einen Wirt einnisten und diesen infizieren. Nach der Infektion kann ein Virus sich selbstständig und ohne Zutun der Nutzer*innen reproduzieren und andere Dateien auf dem Gerät infizieren. Die Infektion erfolgt dabei auf verschiedene Arten. Schätzungsweise 16% der durch Malware infizierten Computer sind durch Computerviren entstanden (Heuveline, 2015, S. 102).

Arbeitsweise

Die einfachste Methode stellt hierbei das Überschreiben von Dateien dar, bzw. das Ersetzen eines Dateicodes durch den Viruscode. Ein Virus erstellt demnach Kopien seines eigenen Programmcodes und pflanzt diese in immer mehr Dateien und Programme auf dem Gerät ein. Am weitesten verbreitet sind sogenannte parasitäre Viren, welche die ursprüngliche Wirtsdatei meist vollständig funktional belassen und der Datei- bzw. Programmcode wird nicht wie oben beschrieben vollständig ersetzt, sondern der Virencode setzt sich an den Datei-Anfang oder ans Datei-Ende fest. Seltener sind jene Viren anzutreffen, die ihren Eintrittspunkt im Code verschleiern und womöglich Jahre in einer Datei verweilen können, bis sie aktiviert werden. Diese Infizierungsmethoden passieren meist unbemerkt, sodass es für Menschen ohne notwendiger technischer Ausbildung nur schwer möglich ist, diese als infizierte Dateien zu identifizieren. Durch die Weitergabe dieser Dateien verbreitet sich ein Computervirus auf anderen Geräten. Diese Weitergabe kann durch das Verschicken von E-Mails mit Dateianhang oder die Weitergabe von Dateien über Discs und USB-Sticks erfolgen und gibt somit die infizierten Dateien an andere Geräte weiter. Ist ein Gerät mit einem Computervirus infiziert, so kann dieser Veränderungen am Betriebssystem oder an Anwendungssoftware vornehmen (Kaspersky, 2008, S. 51ff).

Obwohl es inzwischen tausende verschiedene Arten von Viren gibt, richten die Folgenden, abgesehen von den bereits beschriebenen parasitären Viren, die meisten Schäden an:

- **Boot-Viren**: Diese Viren infizieren den Boot-Sektor von Festplatten oder anderen Datenträgern. Dadurch werden sie beim Starten eines Geräts aktiviert, noch bevor die Sicherheitssysteme geladen wurden (Klau, 2002, S.39).
- **Datei-Viren**: Hierbei hängen die Viren ihren eigenen Programmcode an den Code von Dateien an, welche dann verschickt werden. Häufig wird der Dateicode auch durch den

Viruscode ersetzt. Die Dateien sind somit unbrauchbar und es ist nicht möglich, sie wiederherzustellen (Kaspersky, 2008, S.58).

- **Makroviren**: Bekannt wurden diese Viren durch ihre Verbreitung über Microsoft Office, da sie sich vor allem in Word, Excel und PowerPoint Dateien einnisteten. Makroviren sind keine eigenständigen Programme, sondern benötigen zur Ausführung einen Interpreter (Klau, 2002, S.39).

Gefahr durch Computerviren

Ähnlich zu biologischen Viren können auch Computerviren mutieren und sind somit für Anti-Viren-Programme schwer zu bekämpfen. Diese Mutationen sind jedoch vom jeweiligen Programmierer, von der jeweiligen Programmiererin erzeugt und vorgegeben. Computerviren benötigen für ihre Reproduktion immer ihren Wirt, beziehungsweise ihr zu infizierendes Gerät und dessen Programme und können somit- anders als Computerwürmer- ohne Wirt nicht überleben. Ein Virus verbreitet sich somit immer mit dem aktiven Zutun der Nutzer*innen, wie dem Öffnen von Programmen und Dateien oder dem Öffnen von Mailanhängen und Internetlinks. Die Gefahr von Computerviren ist, dass sie einerseits Programme verlangsamen und vergrößern, andererseits aber auch Datenbestände verändern oder sogar löschen können (Ball, 2021, S.87ff).

Da E-Mail-Programme zu den von älteren Menschen am häufigsten genutzten Programmen zählen, geht von diesen ein großes Risiko aus. Infektionen durch E-Mails und deren Anhänge sind nach wie vor der größte Infektionsherd.

3.2. Würmer

Ein Computerwurm, kurz Wurm genannt, ist ebenfalls ein bösartiges Programm mit der großen Eigenschaft, dass es sich wie ein Virus selbst reproduzieren und zusätzlich auch selbst verbreiten kann. Ein Computerwurm benötigt kein Wirtsprogramm, sondern ist bereits ein eigenständiges Schadprogramm. Würmer können sich selbstständig im ganzen Netz verbreiten und dort große Schäden anrichten. Im Gegensatz zu anderen Malware-Typen, sind Würmer selten geworden, beziehungsweise können schon gut erkannt und frühzeitig gestoppt werden, sodass schätzungsweise nur 8% der schadhaften Software im Netz den Würmern zuzuschreiben sind (Heuveline, 2015, S. 102f).
Anders als Viren und Trojaner, welche von Nutzer*innen oder Hackern unbemerkt aktiviert werden, machen Würmer dies ohne aktives menschliches Zutun und können so unbemerkt in

andere Geräte eindringen. Das Eindringen in andere Geräte erfolgt auf unterschiedliche Arten. Nach dieser Art des Eindringens benannt (Ball, 2021, S.90).

Arbeitsweise

- **E-Mail-Würmer**: Die klassische Infektionsmethode besteht für diese Würmer darin, sich in E-Mails an Dateianhang oder als Internetlink zu verbergen. Durch das Öffnen der Mailanhänge werden bösartige Programme heruntergeladen. Beim Klicken auf den Internetlink wird die Datei ebenfalls heruntergeladen und der Computerwurm aktiviert. Die Mails mit Wurmanhang werden hierbei nicht aktiv von den Nutzer*innen versandt, sondern bereits durch den Wurm selbst, der mit den befallenen Dateien seine eigene Kopie verschickt. Ein Computerwurm kann sich selbstständig an alle Kontakte des Adressbuches versenden. Durch öffentliche E-Mail-Datenbanken und durch den Faktor, dass sich immer mehr Menschen auf diversen Internetseiten mit ihrer Mail-Adresse registrieren, landen nach und nach immer öfter private Mail-Adressen im Netz, welche von den Würmern verwendet werden und sich so rasend schnell ausbreiten können (Klau, 2002, S.22; Kaspersky, 2008, S.53).
- **Würmer durch Systemlücken**: Diese Würmer verbreiten sich nicht über E-Mail Anhänge, sondern suchen sich selbstständig Schwachstellen im Betriebssystem, um so von einem Server zum nächsten zu gelangen. In einem Peer-to-Peer Netzwerk schlüpfen Computerwürmer in freigegebene Dateien oder suchen sich eine Sicherheitslücke, um andere Geräte im gleichen Netzwerk zu befallen (Klau, 2002, S.23f).
- **Parasitäre-Würmer**: Diese Würmer nisten sich, ähnlich wie manche Viren, in Trojanische Pferde ein, um so in andere Geräte transportiert zu werden. Bereits von Trojanern oder Viren infizierte Rechner sind für Würmer leicht erkennbar und bieten somit ebenfalls ein leichtes Ziel (Kaspersky, 2008, S.55).

In den Anfängen der Office-Programme stellten Würmer ein großes Problem dar, da sich viele Dateien im Mailprogramm von selbst öffneten und ohne aktives Zutun den Download starteten. Was als Vereinfachung für Nutzer*innen gedacht war, stellte vor allem für Würmer ein einfaches Eindringen dar. Da fast jede*r Windowsanwender*in ein Office Programm besitzt, wurde dies zur liebsten Verbreitungsart von Computerwürmern (Klau, 2002,S.24).

Oftmals verbreiten sich Computerwürmer gleich über mehrere Methoden und erhöhen so ihre Chance, in ein Netzwerk eindringen zu können. Die Schäden, die Würmer in den betroffenen Geräten anrichten, sind ident zu den Schäden von Viren.

3.3. Trojaner

Ein Trojanisches Pferd, im Folgenden Trojaner genannt, ist mit 70% die am häufigsten anzutreffende Art von Malware im Internet. Trojaner haben vielfältige Einsatzmöglichkeiten und verbinden oftmals mehrere Malware-Typen miteinander. Sie können auch andere Programme wie Adware und Spyware auf den betroffenen Geräten installieren und scheinen auf den ersten Blick oftmals nicht unerwünscht auf, da sie scheinbar nützliche Programme in ein Gerät einschleusen, auf welchen meistens bereits ein Virus sitzt (Heuveline, 2015, S.102; Ball, 2021, S.89).

Arbeitsweise und Gefahren

Trojanische Pferde transportieren, wie der Name vermuten lässt, feindliche Software und bösartige Programme in ein Gerät. Sie dienen als Transportmittel für Computerviren und Würmer und können sich im Gegensatz zu diesen, nicht selbstständig reproduzieren, sondern sind ein eigenständiges Programm. Trojaner können, sobald sie auf einem Gerät installiert wurden, sämtliche Vorgänge beobachten, speichern und verfolgen. Es gibt verschiedene Typen von Trojanischen Pferden, wobei die bekanntesten Folgende sind:

- **Trojaner zur Fernverwaltung**: Trojaner diesen Typs können aus der Ferne von Hackern gesteuert und kontrolliert werden. Die Installation dieser Trojaner erfolgt wie bei fast allen Trojanischen Pferden unbemerkt und hat zur Folge, dass Angreifer den gesamten Rechner unter Kontrolle bringen können. Angreifer können somit über Trojanische Pferde die Systeme der betroffenen Nutzer*innen fernsteuern. Dies kann vom Versenden von Mails und Nachrichten über das Löschen von persönlichen Daten und Informationen auf dem Gerät, sowie das Öffnen und Deinstallieren von Dateien und Programmen gehen (Kaspersky, 2008, S.63).
  Diese Art der Trojanischen Pferde gelten als sehr gefährlich, da die Hacker die betroffenen Geräte vollständig kontrollieren können.

- **Trojan PSW**: „Password Stealing Ware“ bezeichnet Trojanische Pferde, die es sich zur Aufgabe gemacht haben, Passwörter, PINs, vertrauliche Daten und Zugangsdaten ausfindig zu machen. Diese ausgespähten Informationen und gestohlenen Daten werden dann an die Hacker übermittelt (Kaspersky, 2008, S.64).
- **Angriffs-Trojaner**: Diese Trojaner installieren sich auf mehreren Geräten von unwissenden Privatpersonen und können zu einem vom Schöpfer des Trojaners ausgewählten Zeitpunkt einen Massenangriff im Internet starten. Die Nutzer*innen der betroffenen Geräte sind somit unwissende Angreifer auf meist gut gesicherte und wichtige Server. Die Massenangriffe dienen meist der Erpressung der Server-Betreiber und überlasten die gesamte betroffene Infrastruktur. Mit steigender Popularität von IOT-Geräten (Internet of things) – Smarthome-Systeme, internetfähige Haushaltsgeräte- steigt die Angriffskraft eines solchen Trojaners, da sich in einem einzigen Haushalt gleich mehrere netzwerkfähige Geräte befinden (Kaspersky, 2008, S.63ff; Klau, 2002, S.46).

Die Schwierigkeit bei Trojanischen Pferden ist der Tarneffekt. Trojaner schauen nicht nur für Nutzer*innen mit wenig Technikerfahrung aus wie nützliche Programme, sondern können auch technisch versierte Personen mit viel Erfahrung täuschen. Trojaner können jedoch durch eine plötzlich auftretende Verlangsamung der Arbeitsgeschwindigkeit, welche sich durch eine große Auslastung der CPU äußert, auffallen. Auch merkwürdige Fehlermeldungen von anderen Programmen und plötzlich aufscheinende Dateien sind typische Merkmale eines Trojaners. Malware beschränkt sich in den meisten Fällen auf Schädigungen und Auffälligkeiten der Software. Es gibt jedoch bei Trojanischen Pferden manchmal Merkmale an der Hardware, wie beispielsweise das von Nutzer*innen ungewollte Öffnen und Schließen des CD-Laufwerks (Klau, 2002, S.45).

3.4. Bots

Bots werden manchmal auch „Drohnen“ oder „Zombies“ genannt. Ein „Bot“ ist eine unspezifische Bezeichnung für Roboter, welche auf den Geräten eine Möglichkeit für einen externen Zugriff installieren und somit fremdgesteuert werden können. Gefährlich werden Bots meistens erst im Zusammenhang mit vielen anderen, ebenfalls infizierten Geräten. Einzelne Bots werden zu einem Botnet [Robot + Network] zusammengeschlossen und können, ähnlich wie Angriffs-Trojaner, einen Massenangriff im Netzwerk tätigen. Zusammengeschlossene Bots können für eine Flut von Spam-Mails oder andere großflächige Cyber-Angriffe verantwortlich sein oder stellen den

Angreifern den Speicherplatz der betroffenen Geräte zur Verfügung (Kaspersky, 2008, S.63ff; Itzel, 2007, S.2).

3.5. Adware

Adware [advertisement + Software], also Werbesoftware, gehört eigentlich nicht zu den klassischen Typen von Malware, da es sich bei Adware primär um keine bösartige Software handelt. Adware möchte, im Gegensatz zu den bisher genannten Programmen, primär keinen Schaden an fremden Geräten anrichten. Trotzdem wird Adware häufig mit Malware in Verbindung gebracht, da die Programme ähnlich aufgebaut sind, häufig die gleichen Anwendungsmerkmale besitzen und Adware oft mit Malware-Typen kombiniert wird.

Das Ziel von Adware ist es, Werbungen anzuzeigen und Nutzer*innen gezielt auf Werbe-Webseiten zu lotsen. Ähnlich wie bei Malware, ist Adware für die meisten Menschen nicht sichtbar installiert und arbeitet im Hintergrund. Die gezeigten Werbungen sind durch das Verhalten bei Suchmaschinen oder ähnlichem auf die individuellen Anwender*innen angepasst, werden personifiziert und verändern sich mit dem Nutzungsverhalten (Bühler et al., 2019, S.84).
Wie bereits in Kapitel 2 festgestellt, unterscheidet sich dieses Verhalten von jüngeren Anwender*innen. Ältere Menschen surfen auf vielen unterschiedlichen Seiten und vergleichen die Produkte und Dienstleistungen miteinander. Doch gerade Webseiten, beispielsweise Online-Magazine, welche Adbanner verwenden, um Werbungen zu schalten, bieten ein erhöhtes Risiko, auf Adware zu treffen. Seriöse Webseiten verringern das Risiko auf gefährliche Werbeanzeigen zu stoßen und sich somit einen Typ von Malware einzufangen. Dies sollte ältere Menschen keinesfalls vom Internet abschrecken oder Ängste schüren. In der Arbeit werden auch Strategien aufgezeigt, wie sich die Nutzer*innen vor Adware und Spyware schützen können, um unbesorgter im Internet zu surfen.

Adware ist zwar nicht unbedingt bösartig, jedoch mühselig und lästig. Die Werbeanzeigen können in Form von Pop-up-Fenstern aufscheinen oder auf Webseiten eingebettet sein. Zwar werden die persönlichen Daten – anders als bei Spyware- nicht ausspioniert, der Browserverlauf und der Standort bieten den Werbebetreibern jedoch ein gutes Bild vom Such- und Nutzungsverhalten. Adware fällt in vielen Fällen nicht unter den Begriff Malware, da sie oft mit der Zustimmung der Nutzer*innen installiert wird. Adware gelangt häufig durch Lücken im System in die betroffenen

Geräte oder bedient sich eines Trojaners, um in ein Netzwerk zu gelangen (Kaspersky, 2008, S.73f).

3.6. Spyware

Spyware, also ausspionierende Software, kommt auch in einigen Trojanern und in vielen Adware-Programmen vor. Der Unterschied zur Adware, welche vor allem das Nutzerverhalten erkennt und dementsprechende Werbeanzeigen schaltet, ist, dass Spyware vertrauliche Daten, Tastenanschläge, Passwörter und PINs ausspioniert.
Spyware gelangt häufig durch das Herunterladen von Gratis-Software, Gratis-Spielen oder anderen kostenlosen Programmen auf die Geräte. Spyware informiert die Anwender*innen darüber, dass sie bestimmte Daten der Anwender*innen weitergeben dürfen oder für eigene Zwecke benutzen dürfen. Meist werden diese Informationen in den seitenlangen Nutzungsbedingungen versteckt, sodass nur die wenigsten Menschen diese tatsächlich lesen. Durch die Registrierung bei verschiedenen Programmen gelangen so die ersten Benutzerdaten ins System. Doch nicht nur persönliche Daten, auch die Weitergabe aller aufgesuchten Webseiten an Werbetreibende fällt unter Spyware. Durch Spyware können auch Sicherheitslücken im Abwehrsystem der Geräte auftreten, die es so anderen Malware-Typen einfach machen, sich in den Geräten einzunisten (Klau, 2002, S.125ff).

3.7. Phishing

Ziel von Phishing ist es, durch gefälschte Webseiten, aber auch durch das vermeintlich seriöse Auftreten in sozialen Netzwerken durch Kurznachrichten, User*innen an persönliche Daten zu gelangen.
Gerade Personen, die viele E-Mails erhalten und mehrere E-Mail-Dienstleister nutzen, kennen die Problematik von Phishing. Ältere Menschen nutzen E-Mail-Programme wesentlich häufiger als andere Programme und liegen im Gegensatz zu jüngeren Nutzer*innen beim Empfang und Versenden von Mails im privaten Bereich über dem Durchschnitt. Der Begriff „Phishing“ setzt sich aus dem englischen „Password“ und „Fishing“ zusammen und bedeutet genau das: Das Fischen von Passwörtern und persönlichen Daten. Phishing Mails leiten die Anwender*innen durch das Klicken des mitgeschickten Links auf täuschend echte, nachgeahmte Webseiten von Banken, Shops oder anderen wichtigen Seiten um. Den User*innen werden Komplikationen vorgetäuscht und sie werden gebeten, ihre persönlichen Bankdaten einzugeben. Zwar beschränken sich

Phishing-Mail nicht auf die Erlangung von Bankdaten, sie machen aber den weitaus größten Teil der Phishing-Mails aus. Durch das Erlangen von Bankdaten können Hacker die Konten der Betroffenen leeren oder große Geldbeträge überweisen (Speichert, 2007, S.313f).

4. Schutz und Gegenmaßnahmen

Der zuvor aufgezeigte Überblick über die verschiedenen Malware-Typen und bösartigen Programme macht deutlich, dass gerade E-Mail Anhänge eine große Gefahr für Geräte und Nutzer*innen darstellen. Um die in Kapitel 3 beschriebenen Folgen von Malware zu verhindern, gibt es ein paar einfache, jedoch wirksame Gegenmaßnahmen, die jede*r Internetnutzer*in verwenden sollte. Obwohl sich die Malware-Programme voneinander unterscheiden, werden sie vom technischen Blickwinkel aus gesehen alle ähnlich bekämpft und ferngehalten. Die Gegenmaßnahmen sind durch ihre Einfachheit besonders dazu geeignet, sie Älteren näherzubringen, da sie klar strukturiert sind und auch einfach in das Internetverhalten zu integrieren sind. Bevor die technischen Maßnahmen zum Tragen kommen, braucht es jedoch ein Grundwissen, wie die Programme funktionieren und wie sie installiert werden können. Da es gerade bei älteren Menschen viele Einsteiger*innen in die Thematik Internet gibt, braucht es spezielle Angebote, um sie bei der ersten Schritten zu begleiten und zu unterstützen.

4.1. Präventionsmaßnahmen speziell für ältere Menschen

Neben technischen Möglichkeiten, wie die Installation der Antiviren-Programme, der Firewall und das Nutzen des Browser, brauchen gerade ältere Menschen mit wenig Technikerfahrung Unterstützung, um die Thematik zu verstehen und umzusetzen. Gerade für Menschen, die keinen technikaffinen Verwandtschaftskreis und keine Freunde in der IT-Branche haben, sind vor allem die ersten Schritte im Internet schwierig zu bewältigen. Für diesen Bedarf gibt es jedoch einige Angebote, auf die ältere Menschen zurückgreifen können.

- Internetschulungen für Anfänger*innen in Bildungseinrichtungen wie in Volkshochschulen und spezielle Schulungen für Senioren wie das Seniorencolleg in Wien, welche den älteren Menschen die Grundlagen des Internet näherbringen (vhs.at, seniorencolleg.at).
- Kleinstunternehmen, die sich zum Ziel gesetzt haben (älteren) Menschen mit wenig Technikerfahrung und Problemen bei technischen Geräten wie Computern und Laptops zu helfen. Bei Anbietern wie Helferline und TechChild kommen geschulte Mitarbeiter*innen sogar zu den Unterstützungssuchenden nach Hause (Helferline.at, TechChild.at).

- Workshops für die Generation 60+ an speziell eingerichteten Standorten wie fit4internet im Kaffee Digital an mehreren Standorten Österreichs oder die A1 Seniorenakademie (fit4internet.at, a1seniorenakademie.at)
- Computerkurse für Senior*innen beim Arbeiter-Samariter-Bund in Deutschland, an welchen sowohl Ersteinsteiger*innen als auch schon technisch versiertere Nutzer*innen teilnehmen können (asb.de).
- Spezielle E-Mail-Kurse und EDV-Schulungen im Land Salzburg in der 50Plus GmbH für alle Menschen ab dem 50. Lebensjahr (50pluscenter.at)

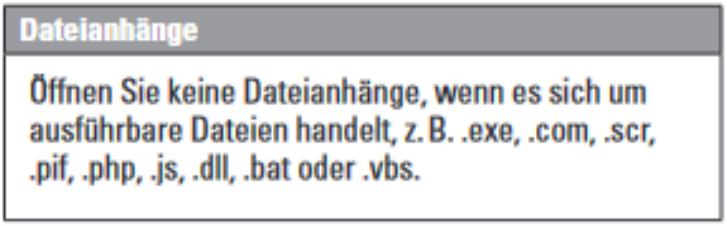
4.2. Gefahren durch Malware erkennen

Durch die meist illegale Installation von Schadsoftware im Hintergrund bekommen die wenigsten Nutzer*innen mit, dass ihre Geräte von Malware infiziert sind. Glücklicherweise gibt es auch für wenig technikaffine Menschen, oder ältere Menschen, die noch wenig Erfahrung im Internet sammeln konnte, die Möglichkeit, Viren, Würmer oder Trojaner zu erkennen. Wie bereits in den vorigen Kapiteln aufgezeigt, sind vor allem Anhänge aus E-Mails, Überträger von Malware. Doch auch die Sicherheitswarnungen von Antiviren-Programmen lassen erkennen, dass gerade ein bösartiges Programm abgewehrt wurde. Auch der Browser selbst kann einige Arten von Malware erkennen und die Anwender*innen so vor böser Software schützen.

E-Mail-Anhänge

In den meisten Fällen verraten sich schädliche Mail-Anhänge durch die E-Mail an sich. E-Mails mit Anhängen, deren Herkunft unklar ist, also von fremden Firmen, Privatpersonen oder Dienstleistern, sollten nicht einfach geöffnet und heruntergeladen werden. Doch selbst wenn die E-Mail aus einer scheinbar vertrauenswürdigen Quelle stammt, beispielsweise Bekannten, Banken oder bekannten Firmen, sollte der mitgeschickte Anhang nicht bedenkenlos geöffnet werden (Bühler et al., 2019, S.85).

Abbildung 3: Potenziell gefährliche Dateianhänge



(Bühler et al., 2019, S.85)

Mit ausführbaren Dateien sind vor allem Dateien mit den oben gezeigten Endungen gemeint, die jedoch oftmals nicht direkt in der E-Mail angezeigt werden. Durch das Öffnen dieser Anhänge beginnt eine mögliche Schadsoftware, sich selbstständig herunterzuladen, sich zu installieren, andere Programme auszuführen und so Malware auf das Gerät einzuschleusen. Um sicher zu gehen, dass es sich bei der erhaltenen E-Mail um keinen Versuch von Hackern handelt, sollte immer direkt beim vermeintlichen Absender nachgefragt werden. Diese Nachfrage darf nicht unbedacht über die E-Mailadresse erfolgen sondern sollte vorher auf beispielsweise Firmenwebseiten recherchiert werden. Oftmals kommen verdächtige E-Mails von Freunden und Bekannten, wobei nur Kleinigkeiten in der Absenderadresse von den Hackern geändert wurden, sodass ein Betrug nur bei genauem Hinschauen erkannt wird. Plumpe Betreffzeilen, unpersönliche Anreden und Fehler in der Rechtschreibung deuten darauf hin, dass sich im E-Mail-Anhang ein bösartiges Programm verbirgt.

Auch Links, die sich in E-Mails befinden, sollten nicht unbedacht angeklickt werden. Vor allem die bereits genannten Phishing-Mails versuchen Nutzer*innen auf gefälschte Webseiten umzuleiten. Gerade bei E-Mails von Banken, Kreditinstituten oder Firmen, bei welchen ein Benutzerkonto angelegt ist, ist Vorsicht geboten. Seriöse Banken informieren ihre Kund*innen meist telefonisch oder per Kundennachrichten im Konto-Bereich. Niemals würden Banken von ihren Kund*innen verlangen, ihre Daten aufgrund von Sicherheitslücken, Änderungen am Online-Banking oder sonstiger Probleme, in einer E-Mail oder einem mitgeschickten Link einzugeben. Verdächtige E-Mails oder Spam Mails mit unerwünschten Inhalten können ohne Bedenken gelöscht werden.

Spam- Mails machen bereits über die Hälfte aller Mails aus. In den meisten E-Mail-Programmen werden diese schon vor dem Lesen durch Spamfilter gelotst und kommen gar nicht in den Posteingang. Immer wieder rutschen jedoch auch wichtige E-Mails in den Spam-Ordner, weshalb dieser regelmäßig kontrolliert werden sollte (Bühler et al., 2019, S. 85f).

4.3. Gefahren durch Malware vermeiden

Viele Malware-Angriffe können durch Vorsicht und gesunde Skepsis bei E-Mails und beim Herunterladen von Software vermieden werden. Trotzdem sollte jede*r User*in einen Virenschutz besitzen und diesen regelmäßig updaten. Im Internet lassen sich hunderte Antiviren-Programme finden, die in unterschiedlicher Stärke gegen die meisten Malware-Angriffe schützen. Abgesehen von automatisiert arbeitenden Möglichkeiten wie Antiviren-Programmen und Firewalls, müssen die Nutzer*innen das verwendete Betriebssystem regelmäßig updaten und auf den neuesten Stand bringen, um einen größtmöglichen Malware-Schutz zu gewährleisten (Chatfield, 2013, S. 82f).

4.3.1. Antiviren-Programme

Im Gegensatz zu Firewalls, arbeitet Antivirensoftware mit den Dateien und Programmen, die sich bereits auf dem Rechner befinden. Diese Daten werden gescannt und überprüft, um Anzeichen von Malware herauszufiltern. Dies geschieht, indem das Antiviren-Programm die bekanntesten schädlichen Softwarecodes mit den Daten auf den Geräten vergleicht, weshalb diese Programme immer auf dem neuesten Stand sein sollten (wko, 2017).

Anwender*innen, die Windows als Betriebssystem nutzen, haben bereits ein Antiviren-Programm installiert und müssen sich nicht mit der Vielfalt an Programmen, die es im Internet zu finden gibt, beschäftigen. Nutzer*innen mit Geräten von Apple sind von Grund auf etwas mehr geschützt als Windows-User*innen, da die Apple Software seltener Malware-Angriffen ausgesetzt ist als Windows. Das liegt daran, dass es deutlich mehr Windows-User*innen gibt und somit die Chance für Hacker, neue Geräte zu infizieren, deutlich höher ist. Doch auch Apple-User*innen werden zunehmend Opfer von Malware, die speziell für Apple-Geräte geschrieben wurde. Da Apple keine eigene Antiviren-Software anbietet, sind die Nutzer*innen auf Lösungen aus dem Internet angewiesen (Bühler, 2019, S.89).
Mittlerweile sind die meisten Programme gegen den Großteil der Malware-Arten geschützt. Die Schwierigkeit für die Hersteller von Antivirenprogrammen liegt darin, dass täglich bis zu 500 neue Viren, Würmer und Trojaner fabriziert werden, gegen die nicht alle Antivirenprogramme geschützt sind. Daher ist es essenziell, immer auf die neueste Version des Antiviren-Programms upzudaten und die Warnhinweise von Browsern und Betriebssystemen zu beachten (Chatfield, 2013, S. 83; Kaspersky, 2008, S.82f).

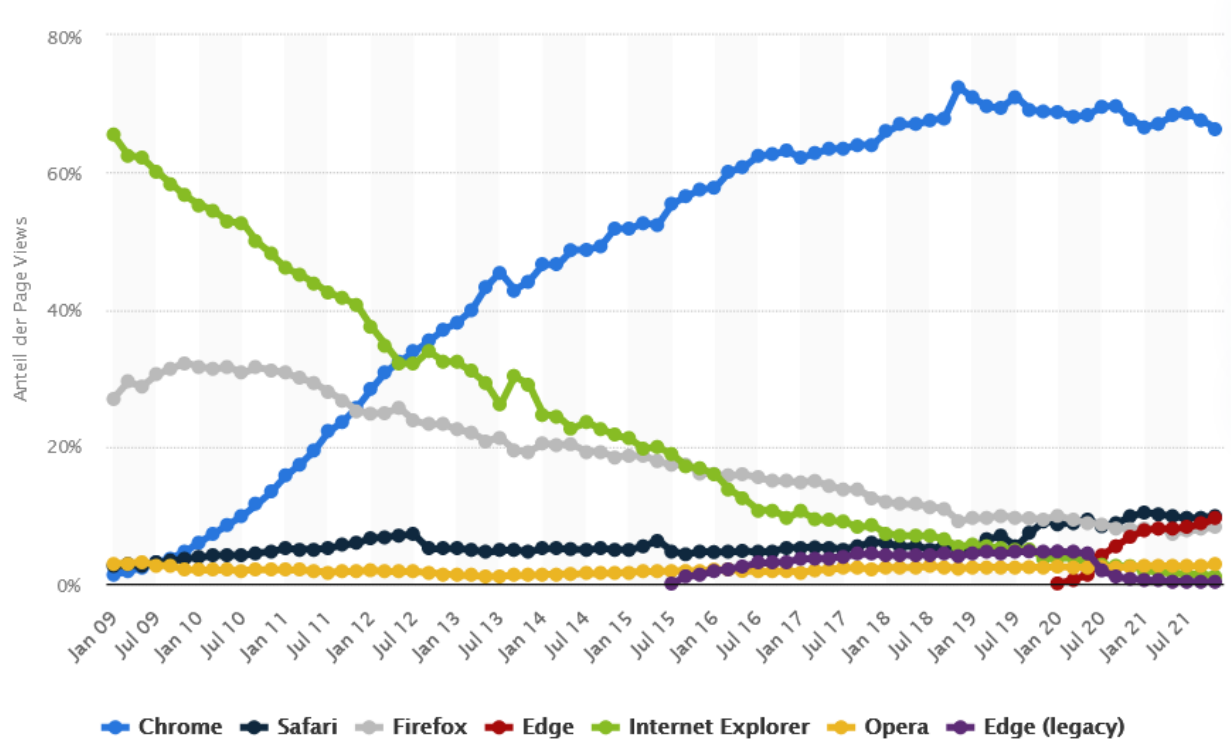
4.3.2. Firewall

Jeder Computer sollte, um gegen Malware geschützt zu sein, eine Firewall installiert haben. Bei den gängigsten Betriebssystemen wie Windows, Linux oder den OS-Betriebssystemen auf Apple-Geräten, ist meist eine Firewall vorinstalliert.
Firewall bedeutet sinngemäß Brandschutzmauer und sorgt dafür, dass keine Viren, Würmer, Trojaner oder andere Malware-Typen auf das Gerät gelangen. Firewalls prüfen alle ein- und ausgehenden Dateien, Nachrichten und Datenpakete auf Bedrohungen und blockieren diese. Dabei wird vor allem die IP-Adresse des Absenders überprüft und eine inbegriffene Block-Funktion wehrt jene Versuche von außen ab, die das Gerät auf Sicherheitslücken hin untersuchen wollen. Firewalls überwachen außerdem die Kommunikation des Geräts, damit dieses nicht unerwünscht und unerlaubt mit anderen Geräten kommuniziert (Bühler, 2019, S.90; Klau, 2002, S.74f).
Heutzutage prüfen sowohl Firewalls, als auch viele Browser die Aktivitäten und geben, wenn nötig, eine Sicherheitswarnung an die Nutzer*innen. Eine Firewall schlägt Alarm, wenn die Arbeitsgeschwindigkeit plötzlich langsamer wird oder wenn auf nicht benutzten Kanälen der Datenverkehr anschwillt (Klau, 2002, S.45)..

4.3.3. Browser

Der Browser ist nicht nur die erste Verteidigungslinie jedes Geräts, sondern öffnet auch Tür und Tor für alle möglichen Arten von Malware. Browser werden zum Ansteuern, Öffnen und Darstellen von Webseiten und zum Herunterladen von Dateien und zum Streamen von Multimedia verwendet. Die am häufigsten verwendeten Browser sind, wie in Abbildung 4 ersichtlich, mittlerweile Google Chrome, Safari auf Apple-Geräten, Mozilla Firefox und Microsoft Edge.

Abbildung 4:



(de.statista.com)

All diese Browser verfügen selbst über die Möglichkeit, bestimmte Webseiten zu blockieren oder die Nutzer*innen über eine mögliche Gefahr zu informieren. Aufgerufene Webseiten werden mehrfach vom Browser überprüft, ob es sich um sichere Verbindungen handelt. Sichere Verbindungen sind erkennbar durch „https“ in der URL-Leiste. Seiten, welche nur „http“ verwenden, haben keine verschlüsselte Verbindung und gelten als unsicher. Durch verschiedene Schutzmaßnahmen, beispielsweise das Blockieren von verseuchten Webseiten, können User*innen vor Malware verschont werden. Diese verseuchten Seiten werden durch Cloud-Technologien erkannt und der Zugriff durch den Browser blockiert (Willems, 2013, S.67f).
Zusätzlich können Anwender*innen Plug-Ins (kleine Softwareprogramme, die in größeren Programmen integriert sind) für Browser installieren, um die Sicherheit und den Schutz noch weiter zu erhöhen.

4.3.4. Datensicherheit

Malware lässt sich in den meisten Fällen von den oben genannten Programmen erfolgreich abwehren. Um die möglichen Folgen von Malware gering zu halten, gibt es einige wichtige Maßnahmen, die jede*r Internetnutzer*in befolgen sollte.
Jede*r Internetuser*in ist auf mehreren Webseiten, Dienstleistern und Programmen angemeldet. Meist geschieht dies durch die Eingabe eines Passwortes. Viele Menschen schützen ihre privaten Computer nur unzureichend und machen es Hackern leicht, Passwörter und PINs zu knacken. Wie schon bei gefährlichen E-Mail-Anhängen erwähnt, fragen seriöse Webseiten niemals Kennwörter oder PINs über Mails ab. Auch außerhalb dieser Mail-Anhänge sollten Passwörter niemals weitergegeben werden. Gerade ältere Menschen haben oftmals Angst, ihre Passwörter zu vergessen und schreiben sie deshalb auf oder teilen sie mit Verwandten und Freunden.
Auffallend ist außerdem, dass immer mehr Menschen das gleiche Passwort auf vielen unterschiedlichen Plattformen verwenden, was die Möglichkeit eines Hacker-Angriffs deutlich erhöht. Um die eigenen Daten zu sichern, sollten deshalb verschiedene, sichere Passwörter gewählt werden, die beim kleinsten Verdacht auf einen externen Zugriff, geändert werden sollten (Bühler et al.,2019, S86).
In folgender Tabelle sind die bekanntesten Passwörter aufgelistet, wobei diese von Hackern in meist wenigen Sekunden zu knacken sind.
Tabelle 3: Passwortschutz

Passwort	Geknackt in...
Passwort	0,0001 Sekunden
12345678	0,0002 Sekunden
Pasw00rt	53,9 Sekunden
Klammeraffe	5 Monate
Kl@mmer@ffe	10 Monate
$Kl@mmer@ffe$	895 Jahre

(Willems, 2013, S.114)

Passwörter sollten daher niemals den „Klassikern“ entsprechen und möglichst kompliziert - mit Sonderzeichen und Zahlen versehen - jedoch einfach zu merken sein.

4.4. Schadensbegrenzung betreiben

So sehr Antivirenschutzprogramme und Firewalls helfen und so groß die Skepsis gegenüber dubioser E-Mail auch ist: Jede*r Internetnutzer*in kann von Malware angegriffen werden.
Den größten Schaden, den Malware auf privaten Geräten anrichten kann, ist das Löschen und der Missbrauch von privaten Daten.
Gute Möglichkeiten, sich vor diesen Szenarien bestmöglich abzusichern, ist entweder das Sichern von Dateien auf externen Trägern wie Festplatten oder mobilen Datenträgern oder das Sichern von Dateien in Cloudspeichern. Somit kann immer eine Kopie der Datei gemacht werden, die bei Bedarf abgerufen werden kann. Der Nachteil an Backups auf externen Festplatten ist die beschränkte Größe. Obwohl es mittlerweile Festplatten mit mehreren Terrabyte Speicherplatz gibt, sind diese anfällig für menschliches Versagen wie Verlust, unachtsamer Umgang oder für äußerliche Einflüsse. Externe Datenträger müssen außerdem immer zum Ort der Verwendung mitgenommen werden. Cloud-Speicher hingegen können von jedem Gerät abgerufen werden und haben eine große Speicherkapazität. Der Nachteil an Backups auf Cloud-Speichern ist jedoch, dass diese ebenfalls durch Malware-Angriffe gehackt werden können. Die sicherste Lösung für Daten stellt deshalb eine Mischform aus beiden Varianten dar (Willems, 2013, S.114f).

5. Diskussion und Beantwortung der Forschungsfragen

Die zu Beginn der Arbeit gestellten Forschungsfragen, nämlich:

> *Welche Gefahren birgt Malware für ältere Menschen, die wenig Erfahrung und Kenntnis in der Internetnutzung haben und worauf ist dabei zu achten?*
> *Welche Maßnahmen können zur Prävention und zum Schutz gesetzt werden?*

können nach sorgfältiger Recherche und nach dem Verfassen dieser Arbeit beantwortet werden. Die Gefahren durch Malware spiegeln sich auch in den Ängsten und Sorgen der älteren Menschen wider. Die Sorge um Datenmissbrauch, um das „Stehlen“ der privaten Daten und die Sorgen um das Löschen aller privaten Dateien machen vielen Internetnutzer*innen Angst. Viele Typen von Malware zielen auf genau diese Ängste ab und stehlen, missbrauchen oder löschen Daten von infizierten Geräten. Ältere Menschen mit wenig Interneterfahrung trifft Malware statistisch gesehen deshalb öfter, da die Verbreitungsart der meisten Malware-Typen immer noch durch E-Mail-Anhänge und Links in E-Mails geschieht. E-Mails werden im privaten Bereich überdurchschnittlich oft von älteren Menschen genutzt und erhöhen somit das Risiko einer Infektion. Beachtet werden muss hier jedoch der Umstand, dass eine Infektion durch Malware auch erfahrene User*innen treffen kann. Gefährlich wird Malware nicht nur im Zusammenhang mit den privaten Daten, sondern auch durch Fernsteuerung durch Hacker. Wie in Kapitel 3.3 beschrieben, können viele Menschen ohne ihr aktives Zutun und meist ohne ihr Wissen an Massenangriffen im Internet auf große und wichtige Server beteiligt sein.
Durch Erfahrung und Interesse an der Materie können viele Malware-Angriffe durch die Nutzer*innen erkannt werden und schon frühzeitig blockiert werden. Immer mehr Firmen und Einrichtungen spezialisieren sich auf Computerschulungen für Senior*innen und bieten Workshops, kostenlose Broschüren und Hilfestellungen bei technischen Schwierigkeiten an. Doch auch technische Lösungen wie gute Antiviren-Programme und eine eingebaute Firewall helfen beim Schutz vor bösartiger Software. Gerade für ältere Menschen mit wenig Kenntnis in der Internetnutzung empfiehlt sich eine gesunde Skepsis E-Mails gegenüber, auch wenn diese augenscheinlich von Bekannten und Verwandten verschickt wurden. Auch beim Surfen im Internet ist die Gefahr von Malware stets präsent. Durch Vorsicht, gute Browsereinstellungen und das Updaten der technischen Sicherheitsvorkehrungen können sich jedoch auch unerfahrene und ängstliche Internetnutzer*innen ins Netz wagen und gleichzeitig die Gefahr von Malware verringern.

6. Fazit und weiterer Ausblick

Zusammenfassend leitet sich aus dieser Arbeit ab, dass Malware für alle Internetnutzer*innen, insbesondere jedoch für ältere Menschen, die aufgrund ihrer geringen Vorerfahrung, den technischen Schwierigkeiten und ihrem Nutzungsverhalten, eine ernstzunehmende Gefahr darstellt. Wie in Abbildung 1 ersichtlich, steigt die Anzahl von Malware Angriffen exponentiell und wird auch weiter zunehmen. Täglich werden hunderte Arten von Computerviren, Würmern und Trojanern hergestellt, um Computer zu infizieren. Auch die Einsatzgebiete vergrößern sich, gehen von privaten Geräten über streng gesicherte Firmenserver und beschränken sich nicht mehr nur auf Angriffe einzelner Geräte, sondern tätigen auch Massenangriffe von tausenden Geräten. Der Befall des eigenen Computers muss keinesfalls einen Grund zur Panik darstellen, wenn richtig reagiert wird.
Gerade Menschen mit wenig Erfahrung im Internet - und das sind oft ältere Personen - haben oftmals mehr Angst vor Datenmissbrauch, Hackern und Datenräubern, als diese Art von Gefahr tatsächlich darstellt. Aus der recherchierten Datenlage wird ersichtlich, dass vor allem das Nutzungsverhalten der Älteren den Unterschied macht, ob eine größere Gefahr von Malware ausgeht. Die Arbeit beleuchtet einerseits die Arbeits- und Wirkungsweise von Computerviren, Würmern und Trojanern, als auch die Verbreitung dieser. Obwohl viele Programme ähnlich funktionieren und mit ähnlichen Mechanismen in die Geräte gelangen, macht es Sinn, sich die kleinen Unterschiede vor Augen zu führen. Durch die erworbenen Erkenntnisse wird die Gefahr geringer, auf potenziell gefährliche E-Mail Anhänge und Links zu klicken. Durch das Wissen, wie die häufigsten Arten von Malware in die Geräte gelangen, können viele Programme schon im Vorhinein abgefangen werden. Computerviren und andere bösartige Software sind weniger beängstigend, wenn es geeignete Schutzmaßnahmen gibt, die die Geräte vor Angriffen bewahren.

Der notwendige Schutz, um Malware vorzubeugen ist einfach genug, damit auch unerfahrene Internetnutzer*innen ihn benutzen und warten können und ist gleichzeitig effektiv genug, um die meisten Arten von Malware frühzeitig abzufangen und zu bekämpfen. Dadurch, dass die meisten Betriebssysteme bereits eine integrierte Firewall besitzen, brauchen sich auch Menschen mit wenig Technikerfahrung, keine Sorge um die erste Verteidigungslinie ihres Geräts machen. Bei Windows ist auch ein Antivirensystem enthalten, welches von den User*innen nur regelmäßig auf Updates überprüft werden muss, um zu funktionieren und um potenziell gefährliche Programme und Dateien auf dem Gerät zu entdecken. User*innen von Apple Produkten müssen auf dem

gewaltigen Markt an Antiviren-Programmen im Internet ein passendes Produkt aussuchen, um ihre Geräte zu schützen. Zusammenfassend lässt sich jedoch sagen, dass es auch für unerfahrene Internetnutzer*innen genügend Schutzmaßnahmen gibt, um Malware von den eigenen Geräten fernzuhalten. Für jene Personen, denen die Schutzmaßnahmen zu komplex sind und die noch Grundkenntnisse in der IT benötigen, gibt es geeignete Präventionskonzepte und Schulungen, die sich speziell auf ältere Menschen fokussieren. Das Angebot an Workshops und Unterstützung für Senior*innen, die sich technisch weiterbilden wollen, steigt kontinuierlich an.

Durch die schiere Menge an bösartigen Programmen, die es inzwischen im Internet gibt, wird es auch in Zukunft ein Wettlauf zwischen Hackern und Antivirensoftware-Herstellern sein, der darüber entscheidet, wie gefährlich Malware für die einzelnen Nutzer*innen sein wird. Durch Mutationen, die durch Rechenfehler von Geräten, aber auch durch menschliche Hand gemacht werden, könnte Malware die Oberhand gewinnen und Antiviren-Herstellern das Leben schwer machen (Heuveline, 2015, S.104).

Auch die Gefahr von mobiler Malware wird nicht lange auf sich warten lassen. Der Umstand, dass mehr Menschen das Smartphone für den Einstieg ins Internet nutzen, macht mobile bösartige Software in Form von Apps für Hacker interessant und lukrativ. Diese Arten von bösartigen Programmen ließ sich bisher gut abfangen, da auf Smartphones jedes Programm (jede APP) ausdrücklich die Zustimmung der Anwender benötigt, um sich zu installieren. Hacker sind sich diesem Problem bewusst und werden mit Sicherheit Möglichkeiten finden, diese Hürden zu umgehen und ein Sicherheitsloch zu finden (Willems, 2013, S.163f).

Die Sicherheitslücke, welche jedoch immer besteht und durch keine technische Applikation zu ersetzen ist, ist die Person vor dem Gerät selbst. Durch uninformierte, unerfahrene Internetnutzer*innen wird es auch in Zukunft schwer sein, Geräte vor Malware ausreichend zu schützen. Die vorliegende Arbeit soll jedoch einen ersten Schritt im gemeinsamen Kampf gegen Malware darstellen.

7. Literaturverzeichnis

Ball, R. (2021). *Viren in allen Dimensionen. Wie ein Informationscode Viren, Software und Mikroorganismen steuert.* Springer Verlag.

Blödorn, S. (2009). Die Bedeutung der Massenmedien für ältere Menschen. In B. Schorb, A. Hartung, W. Reißmann, (Hrsg.) *Medien und höheres Lebensalter* (S.157-171). VS Verlag.

Bühler, P., Schlaich, P., Sinner, D. (2019). *Datenmanagement. Daten-Datenbanken-Datensicherheit.* Springer Verlag

Chatfield, T. (2013). *Digitale Kultur. 50 Schlüsselideen*. Springer Verlag.

Donnerstag, J., Mika, C. & Pfleiderer, R. (2012): Alter und Zeitunglesen? Nur Print gefragt?. In B. Kampmann, B.Keller, M. Knippelmeyer & F.Wagner (Hrsg.), *Die Alten und das Netz* (S. 249-265). Springer.

Feuersinger, D. (2004). *Internet für Senioren. Anspruch und Wirklichkeit seniorengerechter Webseiten* [Diplomarbeit, Universität Wien]. https://www.feuersinger.com/danielafeuersinger/files/Dipl_feuersinger2.pdf

Fittkau S., Harms A. (2012). Silver Surfer – Profile, Nutzungsverhalten und -bedürfnisse. In B. Kampmann, B. Keller, M. Knippelmeyer & F. Wagner (Hrsg.) *Die Alten und das Netz. Angebote und Nutzung jenseits des Jugendkults.* (S. 52-71). Springer.

Hembach, M. (2001). *Möglichkeiten und Grenzen der Internetnutzung bei Senioren. Eine empirische Studie* [Diplomarbeit, Heinrich Heine Universität Düsseldorf]. https://www.socialnet.de/materialien/attach/53.pdf

Heuveline, V. (2015). Infiziertes Netz. Virtuelle Krankmacher. *Ruperto Carola Forschungsmagazin, 6*, 100-107.

Itzel, L.-A. (2007). *Eine Infrastruktur zur Einschätzung des aktuellen Gefährdungslevels durch Malware* [Diplomarbeit, Universität Mannheim]. http://www.dihe.de/docs/docs/diplomarbeit-2007-itzel.pdf

Kaspersky, E. (2008). *Malware. Von Viren, Würmern, Hackern und Trojanern und wie man sich vor ihnen schützt.* Carl Hanser Verlag.

Klau, P. (2002). *Hacker, Cracker, Datenräuber. Datenschutz selbst realisieren, akute Gefahren erkennen, jetzt Abhilfe schaffen.* Vieweg Verlag.

Latzer, M., Just, N., Metreveli, S. & Saurwein, F. (2013). Vertrauen und Sorgen bei der Internetnutzung in der Schweiz 2013. *Themenbericht aus dem World Internet Project – Switzerland 2013*. Universität Zürich, Zürich. http://www.mediachange.ch/media/pdf/publications/Vertrauen_Sorgen_2013.pdf

Ott, D. & Hennewig, S. (2012): 50plus- Internetnutzung und gesellschaftlicher Auftrag. In B. Kampmann, B.Keller, M. Knippelmeyer & F.Wagner (Hrsg.), *Die Alten und das Netz* (S. 305-339). Springer.

Speichert, H. (2007). Praxis des IT-Rechts. Praktische Rechtsfragen der iT-Sicherheit und Internetnutzung. In P. Hohl (Hrsg.) *Edition <kes>.* Vieweg Verlag.

Willems, E. (2013). *Cybergefahr. Wie wir uns gegen Cyber-Crime und Online-Terror wehren können.* Springer.

Online-Quellen:

50Plus GmbH. https://www.50pluscenter.at/content/ [Abruf am 06.01.2022]

A1 Seniorenakademie: https://a1seniorenakademie.at/ [Abruf am 06.01.2022]

Arbeiter-Samariter-Bund. https://www.asb.de/ [Abruf am 06.01.2022]

Haesner, M., Steinert, A., O'Sullivan, J. & Steinhagen-Thiessen, E. (2015). Analyse des Umgangs älterer Internetnutzer mit unerwarteten Situationen. *Z Gerontol Geriat* (48) 715–721. https://doi.org/10.1007/s00391-014-0838-z [Abruf am 18.12.2021]

Helferline: https://helferline.at/ [Abruf am 06.01.2022]

Kaspersky Labs GmbH (23.04.2021). *Ransomware 2019-2021: Zielgerichtete Angriffe auf hochrangige Organisationen um fast das Achtfache gestiegen.* https://www.kaspersky.de/about/press-releases/2021_ransomware-2019-2020-zielgerichtete-angriffe-auf-hochrangige-organisationen-um-fast-das-achtfache-gestiegen [Abruf am 22.12.2021]

SeniorenColleg. Computer-Handy- & Tablet Schule für Senior*innen https://www.seniorencolleg.at/

TechChild. https://www.techchild.at/techhelp [Abruf am 06.01.2022]

Verein zur Steigerung der digitalen Kompetenzen in Österreich. https://www.fit4internet.at/page/home [Abruf am 06.01.2022]

Volkshochschulen. Computer, Internet und Multimedia. https://www.vhs.at/de/k/computer-internet-und-multimedia [Abruf am 06.01.2022]

WKO (31.05.2017): Virenschutz und Firewall. https://www.wko.at/service/innovation-technologie-digitalisierung/Virenschutz-und-Firewall.html [Abruf am 22.12.2021]

Abbildungsverzeichnis

Abbildung 1:

Donnerstag, J., Mika, C. & Pfleiderer, R. (2012): Alter und Zeitunglesen? Nur Print gefragt?. In B. Kampmann, B.Keller, M. Knippelmeyer & F.Wagner (Hrsg.), *Die Alten und das Netz* (S. 249-265). Springer. S.252

Abbildung 2:

Willems, E. (2013): *Cybergefahr. Wie wir uns gegen Cyber-Crime und Online-Terror wehren können.* Springer. S.11

Abbildung 3:

Bühler, P., Schlaich, P., Sinner, D. (2019). *Datenmanagement. Daten-Datenbanken-Datensicherheit.* Springer Verlag. S.85

Abbildung 4:

Browser-Nutzung weltweit auf Desktop/Laptops

https://de.statista.com/statistik/daten/studie/157944/umfrage/marktanteile-der-browser-bei-der-internetnutzung-weltweit-seit-2009/#professional [Aufruf am 27.12.2021]

Tabellenverzeichnis

Tabelle 1 und 2:

Statistik Austria. (2021). *Internetnutzerinnen und Internetnutzer 2021. Internetnutzerinnen und Internetnutzer 2005 bis 2021*

https://www.statistik.at/web_de/statistiken/energie_umwelt_innovation_mobilitaet/informationsgesellschaft/ikt-einsatz_in_haushalten/index.html [Aufruf am 03.11.2021]

Tabelle 3:

Willems, E. (2013): *Cybergefahr. Wie wir uns gegen Cyber-Crime und Online-Terror wehren können.* Springer.