



G Data
Security Studie 2011

Wie schätzen Nutzer die Gefahren
im Internet ein?

Inhalt

1 Zusammenfassung.....	2
1.1 Umfang und Zweck der Studie.....	2
1.2 Wie gut kennen Surfer die Gefahren im Internet?.....	2
2 Methodik der Studie	3
3 Ergebnisse der G Data Security Studie 2011	4
3.1 Wie schützen sich Anwender vor den Gefahren?	5
3.1.1 Wie bewerten Anwender die Leistungsfähigkeit von kostenlosen Virenschutz- Lösungen?	6
3.1.2 Anzahl ungeschützter PCs.....	8
3.1.3 Security-Suite oder reiner Virenschutz?.....	9
3.2 Wo erwarten Internet-Surfer die meisten Gefahren?	11
3.2.1 Die elf Thesen der Internet-Sicherheit	11
3.2.2 Wer ist besser informiert: jüngere oder ältere Internetnutzer?.....	17
3.2.3 In welchem Land sind die Internetnutzer am besten über die Gefahren informiert?	19
3.2.4 Sind Männer die besseren Surfer?	20
3.3 Verhalten in sozialen Netzwerken.....	22
3.3.1 Wer verhält sich sicherer in sozialen Netzwerken: Männer oder Frauen?.....	24
3.3.2 Nutzen jüngere Anwender soziale Netzwerke sicherer als ältere Nutzer?.....	25
4 Schlussfolgerungen	26
Anhang	29
G Data Software AG.....	29
Survey Sampling International.....	31
Glossar.....	31

1 Zusammenfassung

1.1 Umfang und Zweck der Studie

Täglich berichten Medien über neue Angriffe auf Internetnutzer und Unternehmen, über Datendiebstahl, neue Computerschädlinge und die Strukturen der eCrime-Kartelle. Privatanwender geraten dabei immer stärker in den Fokus der Täter und werden immer häufiger Opfer der weltweit agierenden Cyber-Banden. Der Schutz der digitalen Identität ist im Zeitalter des Internets daher gesellschaftsübergreifend von elementarer Bedeutung. Zur Absicherung des Personal Computers stehen Anwendern dabei unterschiedlichste IT-Sicherheitslösungen zur Verfügung. Doch wie gut sind Nutzer wirklich über die wahren Gefahren im Internet und die Methoden der Täter informiert? Haben jüngere oder ältere Anwender in puncto IT-Security die Nase vorn – sind Frauen oder Männer die besseren Internetnutzer? In der großen länderübergreifenden Security Studie 2011 geht G Data diesen und vielen weiteren Fragen nach, stellt IT-Security-Mythen auf den Prüfstand und zeigt, wie Nutzer die Gefahren im Internet wirklich einschätzen.

1.2 Wie gut kennen Surfer die Gefahren im Internet?

In der G Data Security Studie 2011 wurden die Umfrageergebnisse, d.h. die eigene Wahrnehmung und Einschätzung der Gefahren, mit der tatsächlichen Bedrohungslage verglichen. Die Analyse zeigt, dass die Kenntnisse der Internetnutzer in vielen Bereichen immer noch unzureichend und veraltet sind.

Fast alle Umfrageteilnehmer haben eine generelle Vorstellung darüber, dass Gefahren im Internet lauern und versuchen ihren PC davor entsprechend abzusichern. Das Wissen spiegelt jedoch nur selten ein realistisches Abbild der wirklichen Gefahren wider. So nehmen neun von zehn PC-Nutzern an, dass eine Malware-Infektion vom Anwender bemerkt wird. Diese äußern sich nach Einschätzung der Umfrageteilnehmer durch merkwürdige Pop-ups, eine Verlangsamung des Computers oder das dieser überhaupt nicht mehr funktioniert. Die Mehrheit der Umfrageteilnehmer geht fest davon aus, dass zumindest eines dieser Symptome auftritt.

Online-Kriminelle haben jedoch das Ziel, möglichst viel Geld zu verdienen, d.h. der Nutzer soll möglichst lange nichts von einer Infektion bemerken. In der Regel werden alle Daten, wie Kreditkarteninformationen, Bankdaten, Zugangsdaten zu Onlineshops und E-Mail-Konten etc., bei der Erstinfektion gestohlen. Anschließend erfolgt in der Regel die Einbindung der Rechner in Botnetze, um diese unbemerkt vom Anwender als Spam-Schleudern oder für DDoS-Angriffe in Untergrundforen zu vermieten.

Bei der Verbreitung von Schadcode setzen die Täter seit längerem auf soziale Netzwerke, um dort Links zu präparierten Webseiten zu publizieren. Die Verbreitung per Spam-Mail und infiziertem Dateianhang kommt zwar immer noch vor, ist entgegen der Meinung vieler Umfrageteilnehmer aber überholt. Spam wird beim Verbreitungskonzept von Computerschädlingen genutzt, um Empfänger auf Schadcode-Webseiten zu locken und dann PCs per Drive-by-Download zu infizieren (s. Abschnitt 3.2.1: Die elf Mythen der IT-Sicherheit - und wo Internetnutzer falsch liegen).

Der Vertrauensvorschuss in sozialen Netzwerken ist bei den Nutzern immens: 35 Prozent vertrauen veröffentlichten Links innerhalb ihres Netzwerkes und gut 19 Prozent wählen Links an, egal von

wem sie stammen und machen sich so leicht zur Zielscheibe von Cyberkriminellen und ihren illegalen Handlungen.

Doch wie schützen sich Anwender vor den Angriffen? Die gute Nachricht: Lediglich elf Prozent aller Internetnutzer gehen nahezu ungeschützt ins Internet – und verzichten gänzlich auf funktionstüchtige Virenschutzlösungen oder Internet-Sicherheitspakete. 48 Prozent der Umfrageteilnehmer nutzen kostenfreie Virenschutzprogramme und verzichten dabei auf den Einsatz einer separaten Firewall, http-Schutz, CloudSecurity, Antispyware oder Antispam-Module. Über 50 Prozent dieser Nutzer gehen davon aus, ein vollständiges Programmpaket mit diesen notwendigen Schutztechnologien installiert zu haben (s. hierzu Abschnitt 3.1: Wie schützen sich Anwender vor den Gefahren?).

Kurzfasit: Die G Data Security Studie 2011 zeigt, dass Anwender die wirklichen Gefahren im Internet falsch einschätzen und ein großer Prozentsatz der Privatanwender ihre Computer nicht effektiv absichern. Die Konsequenz liegt auf der Hand: Zu viele Menschen laufen Gefahr, dass ihre Computer ungewollt mit Malware infiziert werden. Das Fehlen von Wissen spielt Cyberkriminellen und Malware-Autoren doppelt in die Hände.

2 Methodik der Studie

Die G Data Security Studie 2011 "Wie schätzen Nutzer die Gefahren im Internet ein?" basiert auf einer internationalen Online-Umfrage. In elf Ländern nahmen daran insgesamt 15.559 Internet-Nutzer im Alter zwischen 18 und 64 Jahren teil. Die Teilnehmer beantworteten Fragen zum Thema Online-Gefahren im Internet, ihrem Surf-Verhalten, dem Einsatz von Sicherheitslösungen sowie ihrem Sicherheitsbewusstsein im Internet. Für jedes Land wurde dabei eine eigene Internetseite in der Landessprache mit identischem Fragenkatalog erstellt. Die Befragten verfügten alle über einen eigenen PC mit eigenem Internetzugang. Die Erhebung der Daten erfolgte in den Monaten Februar bis März 2011 und wurde von Survey Sampling International¹ im Auftrag der G Data Software AG durchgeführt. Die Auswertung und Analyse der Daten fand im April und Mai 2011 statt.

Tabelle 1: Altersverteilung und Geschlecht der Befragten

Alter	Männer	Frauen	Total
18-24	1.273	1.430	2.703
25-34	1.636	1.796	3.432
35-44	1.603	1.784	3.387
45-54	1.585	1.647	3.232
55-64	1.381	1.424	2.805
Gesamt	7.478	8.081	15.559

Tabelle 2: Befragte pro Land

Land	Männer	Frauen	Total
Belgien	432	496	928
Deutschland	591	603	1.194
Frankreich	582	622	1.204
Großbritannien	545	561	1.106
Italien	575	563	1.138
Niederlande	336	367	703
Österreich	343	425	768
Russland	503	582	1.085
Schweiz	346	333	679
Spanien	579	579	1.158
Vereinigte Staaten von Amerika	2.646	2.958	5.604
Gesamt	7.478	8.081	15.559

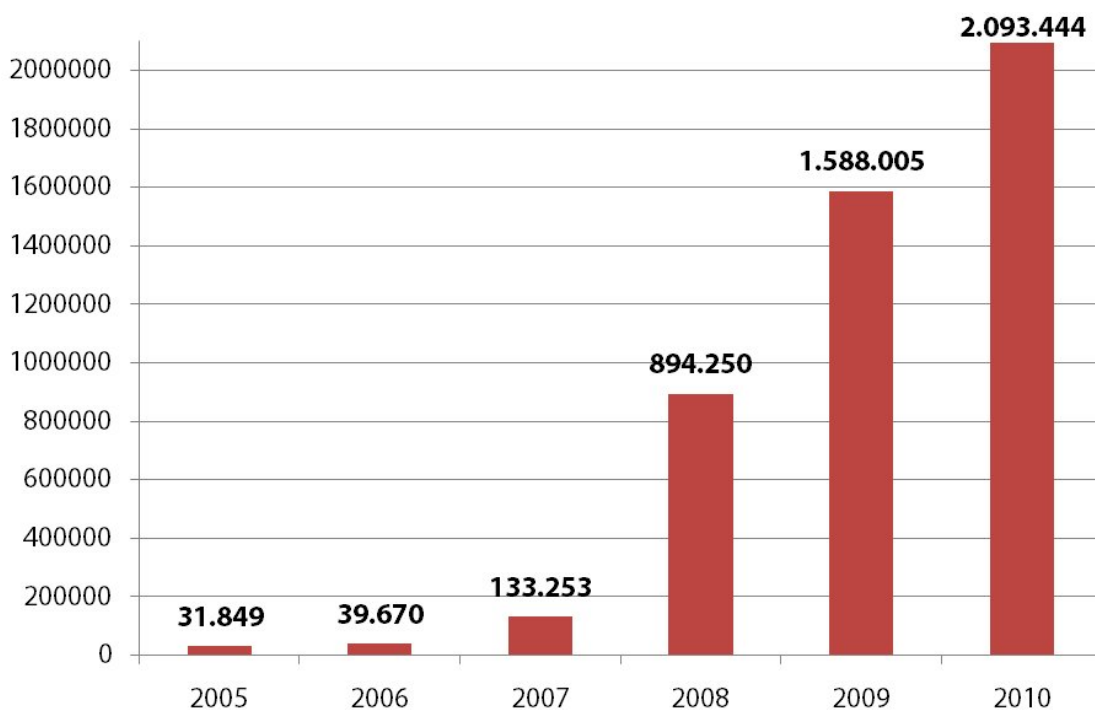
¹ Weitere Informationen über Survey Sampling International sind im Anhang zu finden.

3 Ergebnisse der G Data Security Studie 2011

Die Angriffe auf Unternehmen und Privatanwender haben in den vergangenen Jahren deutlich zugenommen. Online-Kriminalität ist unlängst zu einem profitablen Geschäft herangewachsen und die Täter setzen bei Ihren Angriffen unterschiedlichste Methoden ein, um Rechner mit Computerschädlingen zu infizieren und den Opfern alle erdenklichen Daten zu stehlen und diese gewinnbringend weiterzuverkaufen.

Allein im vergangenen Jahr registrierte G Data mehr als zwei Millionen neue Schadprogramme für Windows-Systeme.²

Diagramm 1: Anzahl neuer Malware pro Jahr seit 2005



Schadcode wird von Kriminellen über mehrere Wege verbreitet: Eine Möglichkeit ist das Hinterlegen von schädlichen Programmen auf Internetseiten. Schon der reine Besuch einer verseuchten Webseite reicht dabei aus, um den Computer über sogenannte Drive-by-Downloads mit Viren, Trojanern, Spionageprogrammen und weiterer Malware zu infizieren. Auf diese tückischen Internetseiten trifft der Nutzer entweder beim Surfen im Netz oder die URLs werden von den Tätern z. B. in sozialen Netzwerken oder durch Nachrichten in Chat-Programmen publiziert. Online-Kriminelle nutzen auch weiterhin Spam-Mails, um Anwender mittels Links auf präparierte Webseiten zu locken oder sie zu animieren verseuchte Dateianhänge zu öffnen. Im Mail-Anschreiben ist dann beispielsweise die Rede von einer vermeintlichen Rechnung oder Mahnung oder es werden exklusive Fotos zu einem aktuellen Ereignis versprochen. Kommen die Anwender der Aufforderung nach, gelangen sie direkt auf die Schadcode-Seiten und fangen sich unbeabsichtigt einen Computerschädling ein.

Nutzer können sich nur mit Hilfe einer umfangreichen Security-Sicherheitslösung und einem umsichtigen Umgang mit dem Medium Internet vor diesen Gefahren schützen.

² Vgl. G Data Malware Report 2/2010, <http://www.gdata.de/virenforschung/info/whitepaper.html>

3.1 Wie schützen sich Anwender vor den Gefahren?

Das Ergebnis der G Data Security-Studie 2011 zeigt, dass von den mehr als 15.500 befragten Anwendern mehr als 89 Prozent eine Sicherheitssoftware auf ihrem System einsetzen und davon 48 Prozent auf kostenfreie Programme vertrauen.

Diagramm 2: Welche Sicherheitslösung haben Anwender auf ihren Systemen installiert?

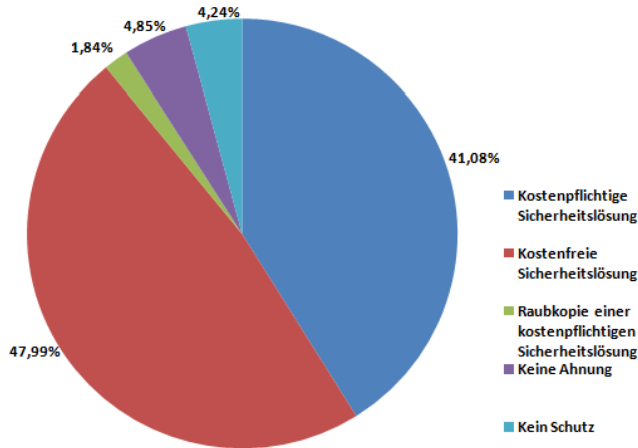


Tabelle 3: Ergebnisse der Frage, welche Sicherheitslösung Anwender installiert haben

Wie schützen Sie Ihren PC?					
	Kostenpflichtige Sicherheitslösung	Kostenfreie Sicherheitslösung	Raubkopie einer kostenpflichtigen Sicherheitslösung	Keine Ahnung	Kein Schutz
Männer (18-24)	39,83%	43,99%	4,08%	4,87%	7,23%
Männer (25-34)	42,60%	47,37%	2,14%	2,87%	5,01%
Männer (35-44)	42,98%	47,16%	1,62%	3,93%	4,30%
Männer (45-54)	42,15%	50,41%	1,32%	2,84%	3,28%
Männer (55-64)	44,97%	48,08%	1,16%	2,68%	3,11%
Gesamt Männer	42,55%	47,53%	2,01%	3,40%	4,52%
Frauen (18-24)	34,69%	51,47%	2,10%	6,08%	5,66%
Frauen (25-34)	40,81%	47,05%	2,62%	5,57%	3,95%
Frauen (35-44)	42,60%	46,92%	1,51%	5,44%	3,53%
Frauen (45-54)	40,80%	48,33%	1,09%	6,86%	2,91%
Frauen (55-64)	38,48%	49,02%	1,05%	7,30%	4,14%
Gesamt Frauen	39,71%	48,41%	1,70%	6,20%	3,98%
Gesamt	41,08%	47,99%	1,84%	4,85%	4,24%

Im Vergleich mit dem Gesamtergebnis der Security Studie schneidet Großbritannien überdurchschnittlich gut ab: über 94 Prozent der Befragten nutzen eine Sicherheitslösung. Den niedrigsten Anteil hat Russland mit knapp 83 Prozent. Damit nutzen durchweg mindestens vier Fünftel der Befragten in den einzelnen Ländern eine Security-Software.

Diagramm 3: Welche Sicherheitslösung haben Anwender in den einzelnen Ländern auf ihren Systemen installiert?

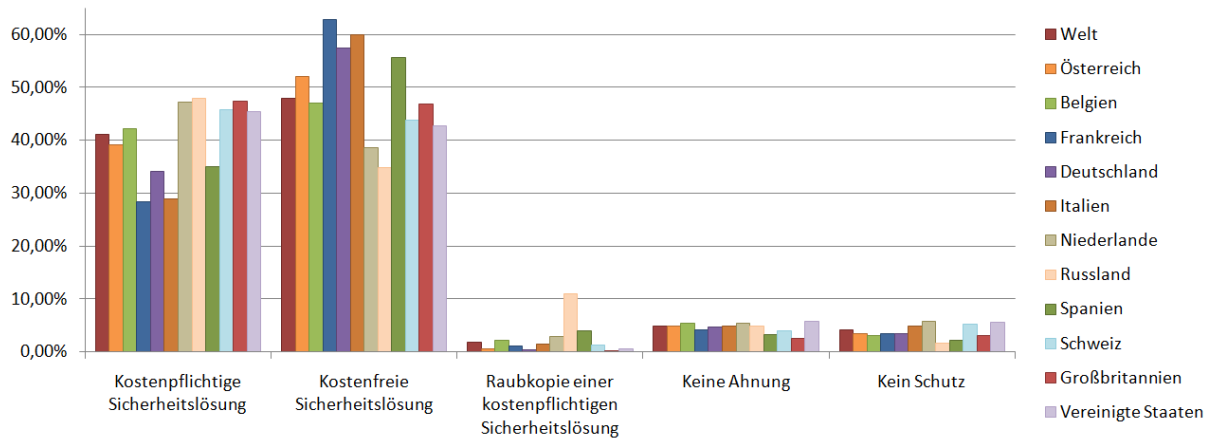


Tabelle 4: Ergebnisse der Länder im Detail: Welche Sicherheitslösung haben die Anwender installiert?

Wie schützen Sie Ihren PC?					
	Kostenpflichtige Sicherheitslösung	Kostenfreie Sicherheitslösung	Raubkopie einer kostenpflichtigen Sicherheitslösung	Keine Ahnung	Kein Schutz
Welt	41,08%	47,99%	1,84%	4,85%	4,24%
Belgien	42,24%	47,09%	2,16%	5,39%	3,13%
Deutschland	34,09%	57,37%	0,34%	4,77%	3,43%
Frankreich	28,41%	62,79%	1,16%	4,24%	3,41%
Großbritannien	47,29%	46,84%	0,27%	2,53%	3,07%
Italien	28,82%	60,01%	1,40%	4,92%	4,83%
Niederlande	47,23%	38,55%	2,99%	5,41%	5,83%
Österreich	39,19%	51,95%	0,52%	4,95%	3,39%
Russland	47,83%	34,84%	10,97%	4,79%	1,57%
Schweiz	45,76%	43,80%	1,26%	3,92%	5,26%
Spanien	34,96%	55,57%	4,00%	3,22%	2,26%
Vereinigte Staaten	45,40%	42,74%	0,55%	5,71%	5,60%

Anwender können kostenlose Antiviren-Software mit anderen kostenfreien Tools kombinieren. Problematisch ist jedoch eine mögliche Inkompatibilität der einzelnen Programme mit der eingesetzten Sicherheitslösung.

Zu den wichtigsten Bestandteilen für eine effektive Absicherung des Rechners gehören neben dem Virenschutz eine Personal Firewall, ein Spam-Filter und nicht zuletzt ein geeigneter Webschutz. G Data bietet in diesem Bereich mit G Data CloudSecurity ein kostenfreies Browser-Plugin, das mit allen Antivirenschutz-Lösungen kompatibel ist.³

3.1.1 Wie bewerten Anwender die Leistungsfähigkeit von kostenlosen Virenschutz-Lösungen?

Die Einfallstore für eine Infektion des eigenen PCs sind, wie oben bereits erwähnt, unterschiedlich. Moderne Sicherheitslösungen sollten jedoch aufeinander abgestimmt sein, um vor allen Gefahren schützen zu können. Kostenlose Virenschutzprogramme sind, einzeln betrachtet, hierzu nicht in der Lage. Denn sie enthalten nicht die Schutztechnologien, die für einen weitreichenden Schutz von

³ Weitere Informationen zum kostenfreien Webschutz unter: <http://www.free-cloudsecurity.com>

elementarer Bedeutung sind. Darunter fallen AntiSpam, Webfilter, Firewall, verhaltensbasierte Erkennung von Schadcode und Cloud Security.

Vor diesem Hintergrund wurden die Anwender über ihre Einschätzung des Leistungsumfanges und der Qualität kostenfreier Schutzprogramme befragt. Knapp 44 Prozent der Umfrageteilnehmer sehen den Leistungsumfang und die Qualität kostenloser Sicherheitssoftware auf dem Niveau kostenpflichtiger Lösungen.

Diagramm 4: Bewertung der Leistungsfähigkeit: Ist kostenfreie Security-Software genau so gut wie eine kostenpflichtige Sicherheitslösung?

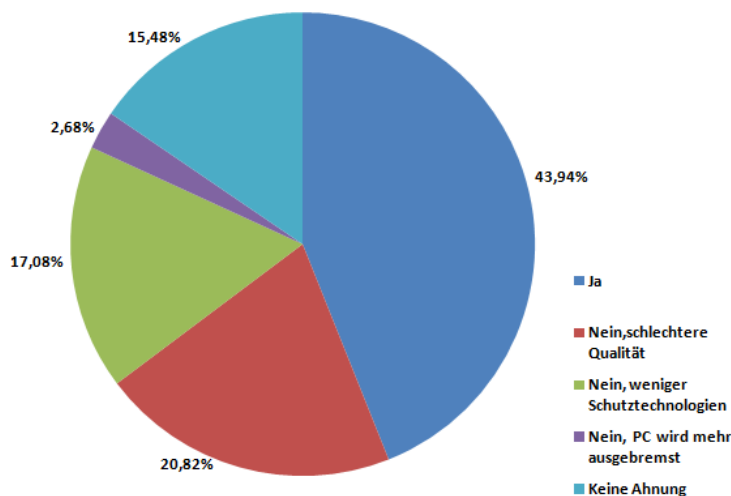


Tabelle 5: Ergebnisse der Frage im Detail: Sehen die Anwender kostenfreie und kostenpflichtige Security-Lösungen in Bezug auf die Qualität und den Umfang als gleichwertig an?

Ist kostenlose Virenschutzsoftware genauso leistungsfähig, wie kostenpflichtige Sicherheitsprogramme?					
	Ja	Nein, schlechtere Qualität	Nein, weniger Schutztechnologien	Nein, PC wird mehr ausgebremst	Keine Ahnung
Männer (18-24)	42,42%	25,69%	17,67%	2,83%	11,39%
Männer (25-34)	46,03%	23,96%	17,30%	3,30%	9,41%
Männer (35-44)	45,60%	22,46%	17,90%	2,87%	11,17%
Männer (45-54)	42,84%	22,02%	19,05%	2,52%	13,56%
Männer (55-64)	42,87%	20,71%	19,48%	2,32%	14,56%
Gesamt Männer	44,06%	22,92%	18,27%	2,78%	11,97%
Frauen (18-24)	43,64%	22,10%	17,97%	2,45%	13,85%
Frauen (25-34)	44,82%	21,27%	16,31%	3,29%	14,31%
Frauen (35-44)	43,39%	20,74%	15,92%	2,30%	17,66%
Frauen (45-54)	43,47%	16,03%	15,48%	2,19%	22,83%
Frauen (55-64)	43,75%	13,55%	14,26%	2,67%	25,77%
Gesamt Frauen	43,83%	18,87%	15,99%	2,59%	18,72%
Gesamt	43,94%	20,82%	17,08%	2,68%	15,48%

Spitzenreiter im Vergleich der Länder ist Frankreich: Für 53 Prozent der Umfrageteilnehmer besteht kein Unterschied zwischen kostenfreien und kostenpflichtigen Security-Lösungen. Eine gänzlich andere Einschätzung haben niederländische Internetnutzer: Knapp 65 Prozent der Niederländer sehen deutliche Unterschiede in der Leistungsfähigkeit von kostenfreien und kostenlosen Sicherheitsprogrammen.

Diagramm 5: Bewertung der Leistungsfähigkeit kostenfreier Security-Lösungen im Ländervergleich

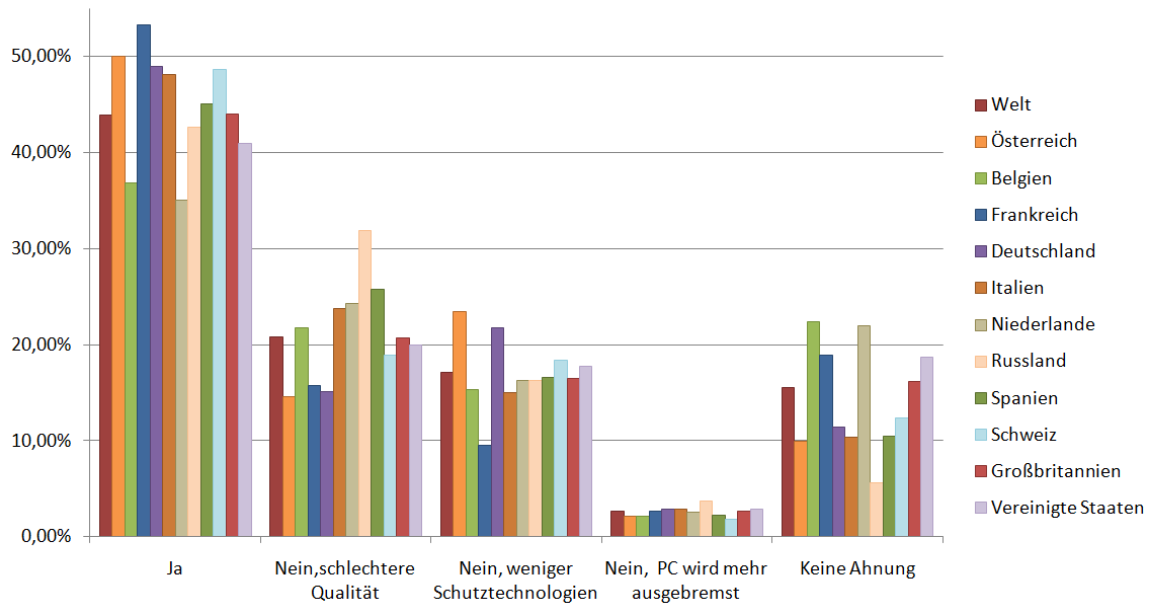


Tabelle 6: Ergebnisse in den einzelnen Ländern: Ist kostenfreie Security-Software für die Befragten gleichwertig mit kostenpflichtigen Sicherheitslösungen?

Ist kostenlose Virenschutzsoftware genauso leistungsfähig, wie kostenpflichtige Sicherheitsprogramme?					
	Ja	Nein, schlechtere Qualität	Nein, weniger Schutztechnologien	Nein, PC wird mehr ausgebremst	Keine Ahnung
Welt	43,94%	20,82%	17,08%	2,68%	15,48%
Belgien	36,85%	21,77%	15,30%	2,16%	22,41%
Deutschland	48,91%	15,08%	21,78%	2,85%	11,39%
Frankreich	53,32%	15,70%	9,47%	2,66%	18,85%
Großbritannien	44,03%	20,71%	16,46%	2,62%	16,18%
Italien	48,15%	23,72%	14,94%	2,81%	10,37%
Niederlande	34,99%	24,32%	16,22%	2,56%	21,91%
Österreich	50,00%	14,58%	23,44%	2,08%	9,90%
Russland	42,58%	31,89%	16,22%	3,69%	5,62%
Schweiz	48,60%	18,85%	18,41%	1,77%	12,37%
Spanien	45,04%	25,74%	16,52%	2,26%	10,43%
Vereinigte Staaten	40,94%	19,91%	17,68%	2,82%	18,65%

3.1.2 Anzahl ungeschützter PCs

Das Bewusstsein für die Notwendigkeit der Absicherung des eigenen Personal Computers scheint bei den Anwendern generell vorhanden zu sein. Bei allen Umfrageteilnehmern lag die Anzahl der ungesicherten Rechner relativ niedrig und betrug lediglich gut vier Prozent oder umgerechnet 659 befragten Anwender - soweit die gute Nachricht. Weitere knapp fünf Prozent der Anwender konnten jedoch keine Angaben dazu machen, ob überhaupt eine Sicherheitslösung auf ihrem System installiert ist. Zudem gaben fast zwei Prozent der befragten Personen zu Raubkopien einzusetzen. So kann man insgesamt davon ausgehen, dass rund elf Prozent aller Interviewten ungeschützt im Internet unterwegs sind. Außerdem liegt die Vermutung nah, dass die Befragten, die nicht wissen, ob sie eine Sicherheitslösung verwenden, ebenfalls ungeschützt sind.

Geringes Security-Bewusstsein bei den russischen Anwendern

Im Vergleich zu allen anderen Ländern sind in Russland die meisten Computer ungeschützt. Hier werden mit einem Anteil von fast elf Prozent auch die meisten illegalen Versionen kostenpflichtiger Sicherheitslösungen von den Anwendern eingesetzt. Insgesamt sind in Russland 17 Prozent der PCs nicht ausreichend vor den lauernden Gefahren des Internets abgesichert. Spitzenreiter im positiven Sinne ist Großbritannien. Hier machen nur knapp sechs Prozent der Interviewten Angaben, die darauf schließen lassen, dass sie nicht abgesichert sind.

3.1.3 Security-Suite oder reiner Virenschutz?

Diagramm 6: Welche Sicherheitslösung haben die Anwender installiert?

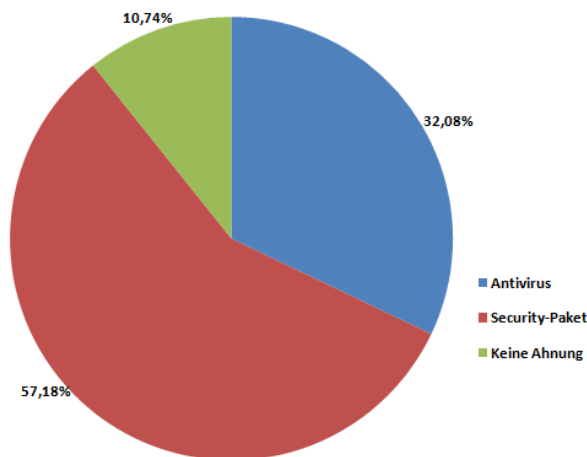


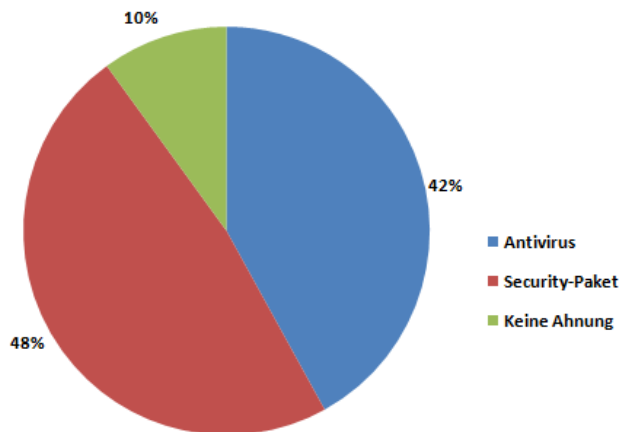
Tabelle 7 Ergebnisse der Frage nach der installierten Sicherheitslösung im Detail

Was für eine Sicherheitslösung haben sie installiert?			
	Antivirus	Security-Paket	Keine Ahnung
Männer (18-24)	37,00%	55,29%	7,71%
Männer (25-34)	35,52%	59,52%	4,95%
Männer (35-44)	32,46%	60,69%	6,84%
Männer (45-54)	29,55%	63,54%	6,91%
Männer (55-64)	29,67%	62,93%	7,40%
Gesamt Männer	32,73%	60,57%	6,69%
Frauen (18-24)	36,03%	52,34%	11,64%
Frauen (25-34)	33,86%	53,39%	12,75%
Frauen (35-44)	29,92%	56,13%	13,95%
Frauen (45-54)	28,71%	56,29%	15,01%
Frauen (55-64)	29,23%	51,36%	19,41%
Gesamt Frauen	31,49%	54,05%	14,46%
Gesamt	32,08%	57,18%	10,74%

Die Internetnutzer wissen, dass unterschiedliche Gefahren im Internet lauern und sie sich dagegen schützen müssen – oder vielleicht doch nicht? Stellt man die Ergebnisse der zuvor gestellten Frage (vgl. Diagramm 2) in Bezug zur Frage „Was für eine Sicherheitssoftware haben Sie auf Ihrem Rechner installiert?“, so ergibt sich ein bemerkenswerter Widerspruch – denn:

Bei kostenfreien Sicherheitslösungen handelt es sich ausschließlich um reine Virenschutzlösungen, ohne weitere Schutztechnologien wie Firewall, Antispam oder Webschutz. Kostenfreie Sicherheitspakete existieren auf dem Markt aktuell nicht. Trotzdem gab die Mehrzahl der Umfrageteilnehmer (vgl. Diagramm 7), die zuvor noch angegeben hatten Nutzer einer kostenlosen Virenschutzlösung zu sein, an, eine Internetsicherheits-Suite mit Personal Firewall, Antispam und Webschutz im Einsatz zu haben.

Diagramm 7: Installierte Sicherheitslösung der Nutzer, die angaben, eine kostenfreie Sicherheitslösung zu nutzen.



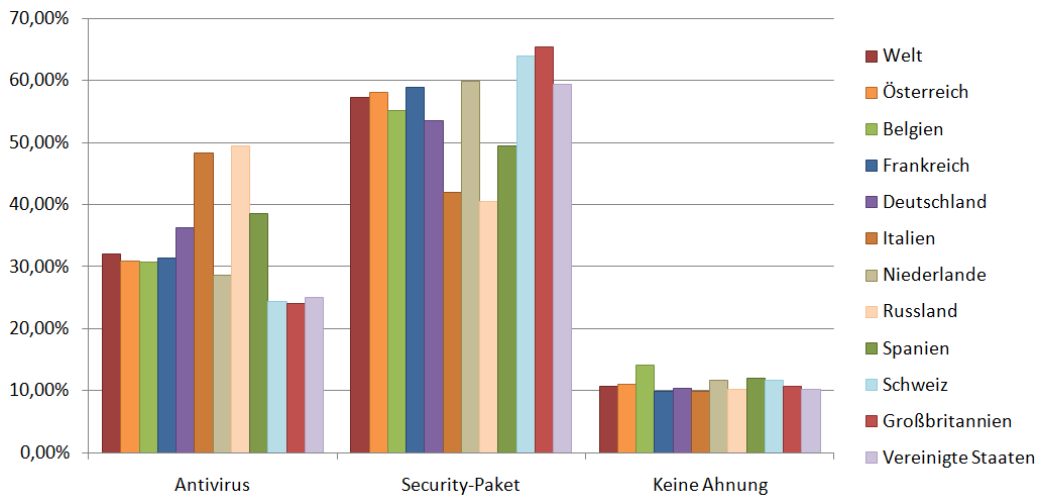
Was zeigt dieser scheinbare Widerspruch? Die Mehrzahl der befragten Endanwender schätzen die Leistungsmerkmale reiner Virenschutzprogramme im Vergleich zu Internetsicherheits-Suiten anscheinend falsch ein und scheinen über die integrierten Schutztechnologien nicht ausreichend informiert zu sein. Kostenloser Virenschutz und Internetsicherheitspakete werden von der Mehrzahl somit unabhängig von den technologischen Unterschieden als gleichwertig betrachtet. Eine Fehleinschätzung, die Internetnutzer teuer zu stehen kommen kann, wenn man die unterschiedlichen Verbreitungswege von Schadcode betrachtet.

Tabelle 8: Installierte Security-Lösungen in den einzelnen Ländern

Was für eine Sicherheitslösung haben Sie installiert?			
	Antivirus	Security-Paket	Keine Ahnung
Welt	32,08%	57,18%	10,74%
Belgien	30,70%	55,17%	14,13%
Deutschland	36,17%	53,51%	10,32%
Frankreich	31,30%	58,90%	9,80%
Großbritannien	24,04%	65,33%	10,63%
Italien	48,30%	41,92%	9,78%
Niederlande	28,55%	59,82%	11,63%
Österreich	30,86%	58,09%	11,05%
Russland	49,44%	40,45%	10,11%
Schweiz	24,42%	63,92%	11,66%
Spanien	38,52%	49,47%	12,01%
Vereinigte Staaten	24,93%	59,35%	10,12%

In den meisten Ländern ergab sich ein ähnliches Bild: Der größte Anteil der Teilnehmer gab vor eine Security-Suite zur Absicherung des Computers installiert zu haben. Lediglich in Italien und Russland war dies nicht der Fall. Hier gaben die meisten Teilnehmer an, kostenfreie Virenschutz-Lösungen einzusetzen.

Diagramm 8: Installierte Security-Lösungen im Ländervergleich

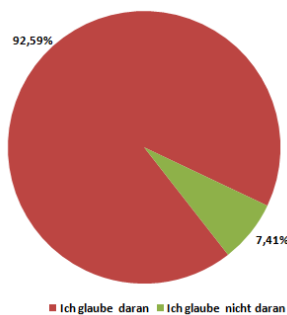


3.2 Wo erwarten Internet-Surfer die meisten Gefahren?

Um einen Überblick darüber zu erhalten, wovor sich Internet-Nutzer im Hinblick auf Cyberkriminalität fürchten, hat G Data den Befragten unter anderem elf falsche Aussagen vorgelegt. Wie sich herausstellte, hielten einige der Befragten alle diese falschen Annahmen für richtig. Daher bezeichnen wir diese Aussagen als die elf Thesen der Internet-Sicherheit.

3.2.1 Die elf Thesen der Internet-Sicherheit

These 1: Wenn mein System mit Malware infiziert ist, merke ich dies in irgendeiner Weise an meinem PC (93 Prozent).



Die erste These ist am weitesten verbreitet. Fast alle Internetnutzer (93 Prozent) weltweit sind davon überzeugt, dass Schadprogramme eine bestimmte spürbare Auswirkung auf den PC haben. So vermuten über 45 Prozent aller Befragten, dass der Computer im Falle eines Malware-Befalls sofort abstürzt. Fast 57 Prozent sind der Auffassung, dass zumindest einige Funktionen gestört sind oder bestimmte Software-Produkte nicht mehr funktionieren. 58 Prozent sind davon überzeugt, dass der Computer verschiedene Popups anzeigt und merkwürdige Geräusche von sich gibt, wenn er infiziert ist. Schließlich glauben fast

57 Prozent der Befragten, dass der Computer sehr langsam wird. Weniger als 7,5 Prozent sind der Meinung, dass im Falle einer Infektion nichts Auffälliges festzustellen sein wird, obwohl genau dies in den meisten Fällen zutrifft (vgl. Tabelle 9).

Tabelle 9: Was passiert nach Ansicht der Befragten, wenn der Computer infiziert ist? – Mehrere Antwortmöglichkeiten konnten von den Befragten gewählt werden.

Was passiert, wenn Ihr Computer mit Schadcode infiziert ist?					
	PC stürzt ab	PC funktioniert nicht mehr richtig	Pop-ups, komische Geräusche usw.	PC wird langsamer	Nichts erkennbares
Männer (18-24)	43,52%	52,24%	56,64%	58,84%	10,45%
Männer (25-34)	43,52%	57,46%	58,31%	59,96%	8,37%
Männer (35-44)	46,35%	56,33%	58,58%	57,70%	7,99%
Männer (45-54)	41,83%	54,57%	58,36%	57,03%	8,83%
Männer (55-64)	37,44%	57,42%	54,89%	55,10%	7,10%
Gesamt Männer	42,65%	55,71%	57,46%	57,77%	8,50%
Frauen (18-24)	48,46%	58,18%	64,06%	62,52%	6,43%
Frauen (25-34)	50,17%	59,30%	64,37%	58,13%	5,57%
Frauen (35-44)	47,48%	57,51%	57,12%	55,27%	7,29%
Frauen (45-54)	46,81%	57,86%	56,22%	53,25%	5,65%
Frauen (55-64)	46,00%	57,23%	50,56%	48,17%	7,16%
Gesamt Frauen	47,85%	58,05%	58,62%	55,53%	6,40%
Gesamt	45,35%	56,93%	58,06%	56,60%	7,41%

In der Vergangenheit wurden Schädlinge von Entwicklern geschrieben, die ihre technischen Fähigkeiten unter Beweis stellen wollten. Gelingt eine Infektion, war diese für das Opfer auch ersichtlich und zwar in Form von Popups, Funktionsausfällen oder durch den plötzlichen Absturz des PC. Offenbar erinnern sich viele Menschen noch gut an diese Dinge.

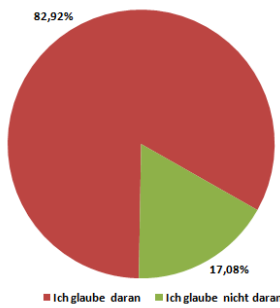
Heute wird Schadcode von professionellen und technisch sehr versierten Kriminellen mit dem Ziel programmiert, möglichst viel Geld zu verdienen. Ein gut programmierter Schädling bringt auf dem Online-Schwarzmarkt viel Geld ein. Dabei wird der Programmcode von anderen Kriminellen aufgekauft, die diesen beispielsweise für den Aufbau eines Botnetzes nutzen, um so auf eine möglichst große Rechenleistung weltweit infizierter PCs zugreifen zu können. Mit solchen Botnetzen lassen sich beispielsweise sogenannte DDoS-Attacken durchführen, Computerschädlinge verbreiten oder man kann damit Spam versenden. Diese Art der Schattenwirtschaft ist weit entwickelt: Entwickler und Administratoren von Botnetzen bieten ihr Know-how und ihre Dienste als Spezialdienstleistungen in speziellen Untergrundforen an. Andere Kriminelle kaufen diese Dienstleistungen oder Schadcode auf diesen Plattformen ein, z. B. um einen Angriff auf die Website eines Unternehmens durchführen zu lassen oder um eine große Spam-Versandaktion zu starten. Dazu ist kein eigenes technisches Know-how erforderlich.⁴

Die Entwickler und Administratoren der Botnetze achten daher darauf, dass das Botnetz möglichst groß und stabil ist. Dies bedeutet, dass jeder PC, der aus einem Verbund abgezogen wird – z. B. wenn die Infektion des PCs entdeckt und beseitigt worden ist – für den Cyberkriminellen einen wirtschaftlichen Verlust darstellt. Schadprogramme sind von den Malware-Autoren daher so konstruiert, dass die Infektion vom Nutzer nicht wahrgenommen werden kann. Daher ist es heute sehr unwahrscheinlich, dass eine Infektion des PCs durch Abstürze, eingeschränkte Rechenleistung, verdächtige Pop-up-Fenster oder andere Merkmale ersichtlich ist. Diese Entwicklung ist für den PC-Nutzer sehr gefährlich, denn nur eine Infektion die schnell auffällt, kann auch schnell behoben werden. Nicht gerade zur Besserung der Situation trägt bei, dass immer noch neun von zehn Nutzern der Meinung

⁴ Weitere Information über die Untergrund Ökonomie im G Data Whitepaper Underground Economy unter: <http://www.gdata.de/virenforschung/info/whitepaper.html>

sind, Malware sei leicht zu entdecken. Diese Nutzer gehen nämlich bei einer einwandfreien Funktionsweise ihres Computers davon aus, dass dieser nicht infiziert sein kann. Daher passt diese These Cyberkriminellen voll und ganz ins Konzept.

These 2: Kostenlose Virenschutzsoftware und kostenpflichtige Softwarepakete bieten dieselben Schutzfunktionen (83 Prozent).

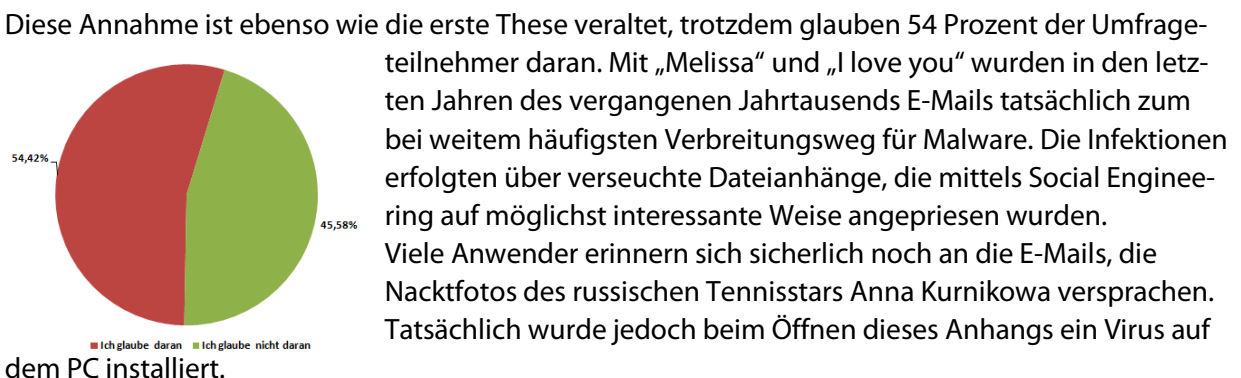


Diese falsche Aussage wird mit 83 Prozent ebenfalls von einer großen Mehrheit der Befragten unterstützt. Obwohl mit 56 Prozent die Mehrheit der Interviewten bei der Frage nach den Qualitätsunterschieden zwischen kostenfreien und kostenpflichtigen Security-Lösungen (vgl. Tabelle 6) Zweifel daran äußert, dass die Qualität beider Arten von Schutzsoftware vergleichbar ist, können die meisten der Befragten die Unterschiede im Einzelnen nicht nennen. 15 Prozent gaben zu keine Ahnung davon zu haben, wie kostenfreie Sicherheitsprodukte im Vergleich zu kommerziellen Lösungen hinsichtlich ihrer Leistungsfähigkeit abschneiden.

Fast drei Prozent der Befragten vertreten die Auffassung, dass der Unterschied in der Belastung des Systems liegt: Die kostenlosen Produkte würden das System stärker als die kostenpflichtigen Lösungen belasten.

Der große Unterschied zwischen kostenfreien und kostenpflichtigen Angeboten liegt darin, welche Security-Technologien sie umfassen. Kostenfreie Sicherheitssoftware bietet lediglich einen reinen Virenschutz. Kostenpflichtige Security-Software umfasst mehrere Sicherheitselemente: Neben dem Virenschutz beinhalten die Lösungen in der Regel einen http-Filter, eine Firewall, ein AntiSpam-Modul und eine verhaltensbasierte Erkennung von Schadcode. Das wissen nur 17 Prozent der Interviewten bei dieser gestellten Frage.

These 3: Die meiste Malware wird per E-Mail verbreitet (54 Prozent).

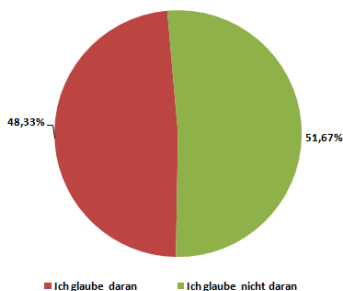


Diese Annahme ist ebenso wie die erste These veraltet, trotzdem glauben 54 Prozent der Umfrageteilnehmer daran. Mit „Melissa“ und „I love you“ wurden in den letzten Jahren des vergangenen Jahrtausends E-Mails tatsächlich zum bei weitem häufigsten Verbreitungsweg für Malware. Die Infektionen erfolgten über verseuchte Dateianhänge, die mittels Social Engineering auf möglichst interessante Weise angepriesen wurden. Viele Anwender erinnern sich sicherlich noch an die E-Mails, die Nacktfotos des russischen Tennisstars Anna Kurnikowa versprochen. Tatsächlich wurde jedoch beim Öffnen dieses Anhangs ein Virus auf dem PC installiert.

Seit ca. sechs Jahren werden Dateianhänge in E-Mails vermehrt durch Links auf Dateien innerhalb von Webseiten ersetzt. Diese Taktik ermöglichte es den Tätern, ihre Mails an den sehr wirkungsvollen Spamfiltern vorbei zu führen und sie so den ahnungslosen Nutzern zuzustellen. Auf der anderen Seite sind viele Anwender sehr vorsichtig geworden, wenn sie E-Mails von unbekanntem Absendern erhalten und löschen diese im besten Fall sofort, ohne sie vorher zu öffnen. Links in E-Mails verweisen mittlerweile in den meisten Fällen auf schädliche Webseiten. Das bietet auch weitere Möglichkeiten, Opfer zu finden: z. B. über soziale Netzwerke (vgl. Abschnitt 3.3), Optimierung von Suchan-

fragen, „Vertipper-Domains“ usw. Die Schadprogramme sind auf Webseiten umgezogen und Webseiten sind mittlerweile Infektionsfaktor Nummer eins.

These 4: Ein PC kann nicht lediglich durch das Laden einer infizierten Webseite selbst infiziert werden (48 Prozent).

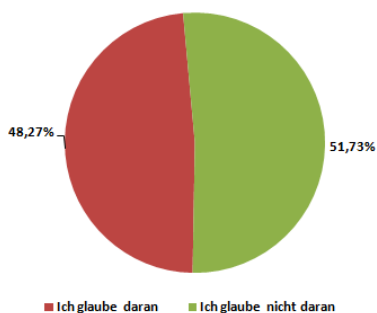


Es ist schockierend, dass fast die Hälfte der Internet-Nutzer diese Aussage für korrekt hält. Über Drive-by-Downloads ist es schon seit Jahren möglich, seinen Computer mit Schadcode zu verseuchen. Der Besuch einer entsprechenden Internetseite reicht für eine solche Infektion schon aus. Die Annahme, dass das Laden allein nicht ausreicht, erweist sich daher als gefährlicher Trugschluss, denn diese Art des Angriffs wird tagtäglich im großen Maßstab praktiziert.

Es existieren zwei Varianten von Drive-by-Infektionen: Zum einen gibt es Webseiten, die mit dem Ziel entwickelt wurden, PCs zu infizieren. Die Cyberkriminellen versuchen durch die Veröffentlichung des interessant beschriebenen Links in sozialen Netzwerken, mit Hilfe von Bannerwerbung oder über E-Mails, in denen der Link eingebunden ist, die Opfer auf die infizierte Webseite zu locken.

Die andere Variante ist raffinierter: Auf einer eigentlich vertrauenswürdigen und beliebten Internetseite wird Schadcode eingeschleust. So wird beispielsweise ein für den Internetnutzer unsichtbares, z. B. 0 x 0 Pixel großes Fenster geöffnet. Hierdurch wird jedoch ein Download gestartet, der den PC des Besuchers automatisch und im Verborgenen mit Schadprogrammen infiziert. Für die Cyberkriminellen besteht der Vorteil dieser zweiten Methode insbesondere darin, dass sie keine Werbung für die Webseite machen müssen. Um sie zu erreichen, müssen die Täter lediglich in diese Webseite eindringen und sie dahingehend manipulieren. Ist diese gut geschützt, was übrigens nur für einen kleinen Teil der Webseiten im Internet zutrifft, ist dies unter Umständen sehr schwierig.

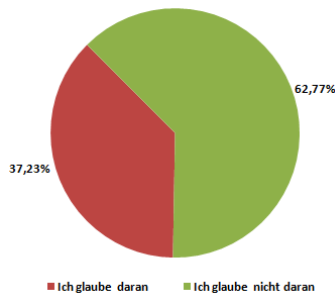
These 5: Die meisten Viren und Computerschädlinge verbreiten sich durch infizierte Dateien in Tauschbörsen wie Peer-2-Peer-Netzwerken und Torrent-Webseiten (48 Prozent).



Unstrittig ist, dass über Tausch-Plattformen wie Torrent-Webseiten und Peer-2-Peer-Netzwerke viele Schadprogramme verbreitet werden. Daher ist es nicht verwunderlich, dass 48 Prozent der Umfrageteilnehmer der Meinung sind, dass diese Methode die wichtigste für die Verbreitung von Malware ist. Eventuell hat der ein oder andere Nutzer sein System durch die Aktivitäten auf solchen Seiten bereits einmal mit Schadcode infiziert.

Doch auch diese These ist falsch und daher ein Mythos, denn die meisten Schadprogramme werden (wie bereits dargestellt) über schädliche Webseiten verbreitet.

These 6: Bei Porno-Webseiten ist die Gefahr höher auf Malware zu treffen, als beispielsweise beim Besuch von Webseiten über den Reitsport oder über Reisen (37 Prozent).

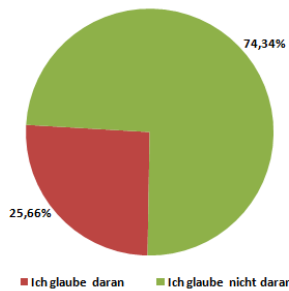


gesichert.

Die Pornografie hat einen zwielichtigen Ruf. Daher ist es auch hier nicht verwunderlich, dass viele Menschen (37 Prozent der Befragten) hier einen Zusammenhang mit Internetkriminalität vermuten. Allerdings ist es fraglich, ob pornografische Seiten tatsächlich häufiger verseucht sind als Internetseiten, die den Reitsport oder andere Freizeit-Themen aufgreifen. In der Pornobranche wird viel Geld verdient. Für die Betreiber stellt die Internetseite ihre Haupteinnahmequelle dar. Daher wird diese in der Regel von Profis entwickelt, gepflegt und

gesichert. Ein zahlender Kunde, der seinen PC durch den Besuch mit Malware infiziert, wäre für den Betreiber ein verlorener Kunde und dies würde finanzielle Einbußen zur Folge haben. Ein Hobby-Betreiber einer Internetseite ist vielleicht kein professioneller Web-Designer und spielt daher nicht regelmäßig alle neuen Softwareupdates und -patches ein, die nötig sind, um Sicherheitslücken zu schließen. Für Kriminelle ist es daher viel einfacher in solche Webseiten einzudringen und dort Schadcode einzuschleusen, als bei professionell abgesicherten Webseiten von Erotik-Anbietern. Darüber hinaus sind diese nicht ausreichend geschützten Webseiten ganz einfach per Google auszumachen: Man braucht nur den Namen einer der Anwendungen und eine Sicherheitslücke darin zu kennen. Auf diese Weise lassen sich viele Webseiten finden, die leicht zu manipulieren sind. Porno-Webseiten können insgesamt aber ein höheres Risiko bergen, wenn sie von zwielichtigen Anbietern stammen. Bei seriösen Erotik-Seiten ist das Gefahrenpotential dagegen geringer.

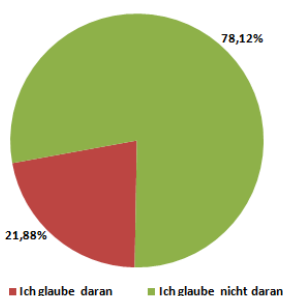
These 7: Meine Firewall schützt mich vor Drive-by-Download-Angriffen (26 Prozent).



An diese Aussage glauben rund 26 Prozent der Befragten. Diese These ist falsch. Firewalls sind zwar ein wichtiger Bestandteil eines Schutzkonzeptes für einen Computer. Allerdings ist es nicht möglich, einen PC alleine durch eine Firewall wirksam vor Drive-by-Infektionen zu schützen.

Für eine effektive und ausreichende Absicherung ist ein Internetnutzer zusätzlich auf eine umfassende Sicherheitslösung mit einem integrierten Web-Schutz angewiesen. Selbst bei einer erfolgreichen Infektion kann eine Firewall nicht immer verhindern, dass das Schadprogramm seine schädlichen Aufgaben ausführt und z. B. bei Spionageprogrammen sensible Daten an den Kriminellen sendet.

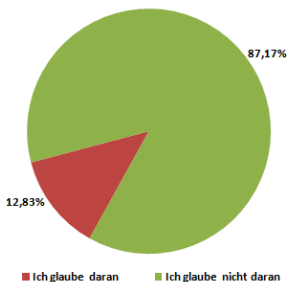
These 8: Wenn man keine infizierten Dateien öffnet, kann der PC nicht infiziert werden (22 Prozent).



Diese Aussage basiert, wie einige andere der hier vorgestellten Behauptungen, auf veralteten Tatsachen, die sich in Form von Halbwissen bis heute gehalten haben und an die in diesem Fall fast 22 Prozent der Umfrageteilnehmer glauben. Natürlich erfolgen Infektionen auch immer noch durch das Öffnen infizierter Dateianhänge. Eine automatische Ausführung von schädlichen Dateien ist allerdings nur dann möglich, wenn bestehende Sicherheitslücken von

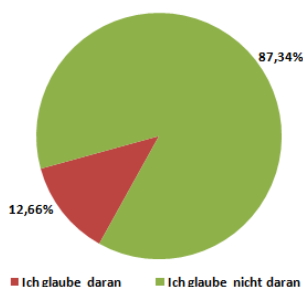
den Angreifern ausgenutzt werden. In diesem Fall würde sich der Schadcode ohne ein Anklicken der verseuchten Datei automatisiert aktivieren. Daher sollte grundsätzlich von einer Gefahr durch infizierte Dateien ausgegangen werden.

These 9: Die meiste Malware wird über USB-Sticks verbreitet (13 Prozent)



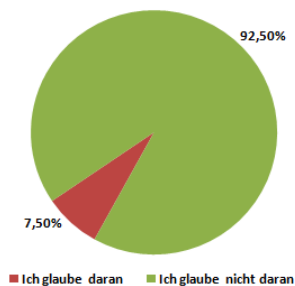
In der Zwischenzeit ist klar geworden, dass die meisten Schadprogramme über schädliche Webseiten verbreitet werden, andere Infizierungswege aber möglich sind. In den 1980er und -90er-Jahren, in denen das Internet noch nicht so allgegenwärtig war, stellten Disketten noch häufige Infektionsquellen dar. In den letzten Jahren ist die Popularität von USB-Sticks und anderen USB-Wechselmedien bei Cyberkriminellen deutlich gestiegen. Hier werden die Autostart-Funktionen von Datenträgern missbraucht, um Schadprogramme beim Anschließen an den PC auszuführen. Prominentestes Beispiel ist der Conficker-Wurm. Daher ist dringend zu empfehlen, die Funktion des Betriebssystems für die automatische Wiedergabe zu deaktivieren. So wird vermieden, dass ein Wurm beim Verbinden des USB-Sticks mit dem Computer automatisch installiert wird.

These 10: Ich besuche keine seltsamen Webseiten. Deswegen bin ich nicht gefährdet, was Drive-by-Infektionen betrifft (13 Prozent).



Diese Aussage kann auf dieselbe Weise wie die sechste These („Bei Porno-Webseiten ist die Gefahr höher auf Malware zu treffen, als beispielsweise beim Besuch von Webseiten über den Reitsport oder über Reisen“) widerlegt werden. Cyberkriminelle achten nicht auf das Thema einer Website. Für sie ist nur interessant, wo sie mit möglichst geringem Aufwand viele Besucher mit Schadcode infizieren können. Dies gelingt den Kriminellen u. a. über die Manipulation von Werbebannern und das ständige Attackieren von großen Domains. Wenn sie erfolgreich sind und einen Zugang erlangen, wird mit Hilfe von sogenannten Web Exploit Toolkits auch ohne Fachwissen Schadcode eingespielt. Webseiten, die seit Jahren sehr vertrauenswürdig sind, können so plötzlich gehackt werden und damit die Gefahr einer Infektion bergen. An diese These glauben allerdings nur fast 13 Prozent der Befragten.

These 11: Cyberkriminelle interessieren sich nicht für die Computer von Privatpersonen (8 Prozent).



Glücklicherweise wird dieser Annahme von allen Aussagen am wenigsten Glauben geschenkt. Nur fast 8 Prozent halten diese These für korrekt. Auch hierbei handelt es sich um einen falsche Annahme. Selbstverständlich sind Unternehmensnetze für Cyberkriminelle sehr interessant. Im Allgemeinen sind sie aber auch schwieriger zu infizieren. Auch Privatcomputer sind heute sehr leistungsfähig und eignen sich somit sehr gut als Komponenten für Botnetze. Außerdem sind auf ihnen oft viele interessante personenbezogene Daten wie Zugänge zu Online Shops, sozialen Netzwerken und E-Mail-Accounts oder Kreditkartenin-

formationen gespeichert, aus denen Cyberkriminelle Nutzen ziehen können. Daher sollte die Bedeutung von Privatcomputern für Cyberkriminelle nicht unterschätzt werden.

3.2.2 Wer ist besser informiert: jüngere oder ältere Internetnutzer?

Die jüngeren Internet-Nutzer im Alter zwischen 18 und 25 Jahren sind weitgehend mit dem Computer und dem Internet aufgewachsen. Darüber hinaus ist diese Gruppe im Internet sehr aktiv. Anders stellt sich die Situation bei den ältesten Befragten im Alter von 55 bis 64 Jahren dar. Die Untersuchung wurde ausschließlich online durchgeführt. Folglich sind alle Befragten im Internet aktiv. Für viele ältere Umfrageteilnehmer ist das Medium jedoch relativ neu. Es wäre daher durchaus denkbar, dass die jüngere Generation viel mehr über die Gefahren im Internet weiß, als die ältere Generation. Eine andere Hypothese besagt jedoch, dass die ältere Generation gerade durch die relative Unvertrautheit mit dem Internet und dem Computer überall Gefahren wittert und deshalb im Netz viel vorsichtiger ist.

Um herauszufinden, wie es um den Informationsstand der jüngsten und der ältesten Generation der Internetnutzer steht, wurde untersucht, inwieweit diese beiden Gruppen den genannten Thesen Glauben schenken. Die folgende Tabelle liefert einen entsprechenden Überblick.

Tabelle 10: Wer glaubt eher an die vorgelegten Thesen: jüngere oder ältere Nutzer?

These	In Altersklasse 18-25 glauben dies:	In Altersklasse 55-64 glauben dies:	Von allen Befragten glauben dies:
1) Wenn mein System mit Malware infiziert ist, merke ich dies in irgendeiner Weise an meinem PC.	91,68%	92,87%	92,59%
2) Kostenlose Virenschutzsoftware und kostenpflichtige Softwarepakete bieten dieselben Schutzfunktionen.	82,17%	83,17%	82,92%
3) Die meiste Malware wird per E-Mail verbreitet.	46,54%	61,46%	54,42%
4) Ein PC kann nicht lediglich durch das Laden einer infizierten Webseite selbst infiziert werden.	53,42%	46,67%	48,33%
5) Die meisten Viren und Computerschädlinge verbreiten sich durch infizierte Dateien in Tauschbörsen wie Peer-2-Peer-Netzwerken und Torrent-Webseiten.	53,42%	45,67%	48,27%
6) Bei Porno-Webseiten ist die Gefahr höher auf Malware zu treffen, als beispielsweise beim Besuch von Webseiten über den Reitsport oder über Reisen.	32,89%	17,47%	25,66%
7) Meine Firewall schützt mich vor Drive-by-Download-Angriffen	39,18%	35,40%	37,23%
8) Wenn man keine infizierten Dateien öffnet, kann der PC nicht infiziert werden.	22,42%	25,13%	21,88%
9) Die meiste Malware wird über USB-Sticks verbreitet.	16,91%	9,02%	12,83%
10) Ich besuche keine seltsamen Webseiten. Deswegen bin ich nicht gefährdet, was Drive-by-Downloads betrifft.	14,39%	13,69%	12,66%
11) Cyberkriminelle interessieren sich nicht für die Computer von Privatpersonen.	10,03%	6,77%	7,50%

Wenn man in der Tabelle die Spalte der jüngeren Nutzer betrachtet, ist das Ergebnis zunächst positiv. Die jüngeren glauben weniger stark an die drei größten Thesen (Nr. 1-3 in Tabelle 10), unterscheiden sich darin allerdings nur minimal vom durchschnittlichen Befragten. Doch an die vierte

These, die einen sehr gefährlichen Irrtum darstellt, da diese die Existenz und die Effizienz von Drive-by-Infektionen in Frage stellt, glauben die jungen Menschen weit häufiger als andere Befragte. Dies gilt auch für die fünfte These über Malware auf Tauschbörsen wie Torrent-Seiten und Peer-2-Peer-Netzwerken. Der Grund liegt möglicherweise darin, dass die jüngere Generation sehr viele Dateien von solchen Webseiten herunterlädt und dabei bereits auf infizierte Dateien gestoßen ist. Auch vermuten jüngere Befragte bei Porno-Webseiten eine etwas höhere Gefahr als ältere Befragte. Die jüngere Generation ist offenbar noch schlechter informiert, was die Funktionen einer Firewall betrifft. Dies passt nicht zu der Hypothese, dass jüngere Nutzer die Technologien mit denen sie aufgewachsen sind gut kennen.

Die Jugendlichen sind sich auch weniger der Tatsache bewusst, dass es für eine Infektion nicht unbedingt erforderlich ist, eine Datei zu öffnen. Darüber hinaus glauben die jüngsten Befragten mehr als der Durchschnitt daran, dass USB-Sticks die wichtigste Quelle für Malware-Infektionen sind. Die jüngeren Teilnehmer überschätzen mehr als andere Altersgruppen ihr Wissen darum, wie sie Drive-by-Downloads verhindern können. Außerdem nehmen sie in stärkerem Maße als der Durchschnitt der Befragten an, dass ihre Privatcomputer für Cyberkriminelle uninteressant sind.

Zwischenfazit: Generation „Silversurfer“ leicht vorn

Insgesamt schneiden die jüngeren Befragten also nicht besonders gut ab. Ihr Kenntnisstand ist noch geringer als der des durchschnittlichen Internet-Nutzers und die Hypothese, dass junge Menschen das Internet besser kennen müssten als der Bevölkerungsdurchschnitt, da sie mit dieser Technologie aufgewachsen sind, ist daher unhaltbar.

Wenn wir unsere Aufmerksamkeit auf die Spalte der älteren Befragten richten, wird indes klar, dass diese den drei größten Thesen in noch stärkerem Maße Glauben schenken als der Durchschnitt aller Nutzer.

Bei der vierten These, bei der es um die Drive-by-Download-Angriffe geht, ergibt sich allerdings ein anderes Bild. Ältere Befragte sind offenbar besser als die Befragten der jüngeren Altersgruppen, vor allem besser als die ganz jungen Nutzer, über die Gefahren dieser Angriffe informiert. Dies ist jedoch kein Grund zur Erleichterung, denn auch unter den Älteren glaubt fast jeder zweite Befragte, dass es Drive-by-Downloads nicht gibt. Überdurchschnittlich viele ältere Umfrageteilnehmer vertreten die Auffassung, dass Filesharing-Seiten die wichtigste Quelle für Malware-Infektionen sind. Die Differenz zum Durchschnitt ist jedoch gering. Auch Porno-Webseiten stoßen bei den Älteren auf weniger Misstrauen als beim Durchschnitt der Befragten. Die Älteren vertrauen viel weniger auf die Schutzfunktionen von Firewalls gegen Drive-by-Downloads als die jüngsten Befragten und auch als der Durchschnitt der Interviewten. Hingegen sind ältere Internetnutzer häufiger der Meinung, dass es unmöglich ist infiziert werden, wenn keine Datei geöffnet wird, was der zuvor geäußerten Überzeugung der Gefahr von Drive-by-Infektionen eigentlich widerspricht.

USB-Sticks sehen die älteren Nutzer weniger oft als häufigste Quelle der Malware-Verbreitung an, womit sie richtig liegen. Weniger gerechtfertigt ist hingegen das überdurchschnittliche Vertrauen in die Sicherheit der eigenen Surfgewohnheiten, das ältere Menschen vor Drive-by-Download-Angriffen schützen soll. Die älteren Menschen sind dabei jedoch noch etwas weniger leichtsinnig als die Jugendlichen. Positiv ist hingegen, dass ältere Anwender mehr als der Durchschnitt erkennen, dass ihre PCs für Cyberkriminelle von Interesse sein können.

Die Generation „Silversurfer“ hat in diesem Vergleich die Nase gegenüber den jüngsten Teilnehmern leicht vorn. Jedoch schneiden auch die älteren Menschen nicht als beste ab, obwohl sie offenbar

etwas besser mit den Gefahren des Internets umgehen als die jüngsten Befragten. Die Ergebnisse der Studie zeigen, dass die Altersgruppe der 25 bis 54-Jährigen über den besten Kenntnisstand in puncto aktuelle Internetgefahren verfügt.

3.2.3 In welchem Land sind die Internetnutzer am besten über die Gefahren informiert?

Es bestehen viele Vorurteile darüber, in welchen Ländern Nutzer besser bzw. schlechter informiert sind. So werden beispielsweise einige Menschen vermuten, dass Internetnutzer aus IT-Technologie-Nationen, wie z. B. den Vereinigten Staaten oder Großbritannien gut über drohende Gefahren im Internet informiert sind. Um herauszufinden, ob es Länder gibt, in denen Internet-Nutzer viel besser bzw. schlechter über die tatsächlichen Gefahren im Internet informiert sind, wurden die prozentualen Ergebnisse der Befragten, die an die vorgegebenen Aussagen glauben, in Tabelle 11 aufgeführt. Grün zeigt an, in welchen Ländern der These am wenigsten Glauben geschenkt wird. Rot zeigt an, wo die These die größte Zustimmung findet.

Tabelle 11: In welchem Land wird den Thesen am meisten Glauben geschenkt?

These	Niederlande	Belgien	Frankreich	Spanien	Vereinigte Staaten von Amerika	Italien	Deutschland	Russland	Großbritannien	Österreich	Schweiz	Welt
1) Infektionen ersichtlich	86,63%	93,97%	92,28%	95,30%	94,29%	94,38%	83,17%	97,88%	91,40%	86,46%	90,13%	92,59%
2) Kostenfreie Sicherheitslösungen so gut wie kostenpflichtige	83,78%	83,19%	90,53%	83,48%	82,32%	85,06%	78,22%	83,78%	83,54%	76,56%	81,59%	82,92%
3) Größte Schadcode-Verbreitung per E-Mail	58,89%	62,18%	57,64%	58,61%	52,37%	58,88%	52,85%	38,80%	52,89%	55,47%	57,73%	54,42%
4) Keine Infektion nur vom Laden einer infizierten Webseite	51,49%	49,03%	49,25%	57,83%	40,95%	63,44%	62,90%	48,48%	42,85%	60,68%	54,93%	48,33%
5) Größte Schadcode-Verbreitung über Tauschbörsen	43,53%	46,76%	48,17%	52,43%	52,73%	45,52%	35,26%	49,49%	48,73%	41,02%	44,48%	48,27%
6) Porno-Webseiten gefährlicher als Reitsport-Internetseiten	25,32%	34,27%	31,89%	32,43%	40,13%	32,25%	30,65%	60,18%	35,80%	34,11%	36,23%	37,23%
7) Firewall schützt vor Drive-by-Downloads	31,44%	28,34%	18,77%	26,78%	24,32%	28,03%	29,31%	17,05%	24,95%	28,26%	29,16%	25,66%
8) Keine Infektion, wenn infizierte Dateien nicht geöffnet werden	16,50%	26,29%	23,59%	30,78%	18,18%	30,67%	13,32%	38,53%	20,43%	14,06%	18,56%	21,88%
9) Größte Schadcode-Verbreitung durch USB-Sticks	8,11%	10,67%	17,28%	20,09%	9,92%	15,38%	8,38%	30,05%	10,49%	8,72%	8,98%	12,83%
10) Sicher, wenn keine seltsamen Seiten angeklickt werden	18,07%	13,69%	14,78%	14,00%	10,79%	17,84%	11,81%	11,89%	9,67%	12,50%	14,14%	12,66%
11) Kriminelle nicht interessiert an Privat-PCs	5,12%	6,90%	5,98%	8,87%	7,50%	8,35%	7,20%	6,54%	8,77%	9,90%	6,63%	7,50%

Zwischenfazit: Deutsche Internetnutzer am besten informiert

Diese Tabelle zeigt, dass die Befragten aus Deutschland offenbar am besten über die im Internet lauenden Gefahren informiert sind. Von allen Ländern schenken sie drei der Thesen am wenigsten Glauben. Dasselbe gilt auch für die Niederländer. Dabei ist jedoch anzumerken, dass die Niederländer bei der Einschätzung der Aussagen zwei Mal am weitesten von der Wahrheit entfernt lagen. Interessanterweise weisen die US-Amerikaner, von denen man vielleicht das beste Abschneiden erwartet hätte, nur bei der vierten These den niedrigsten Anteil der Befürworter auf. Am meisten Glauben schenken amerikanische Internetnutzer der These, dass über Tauschbörsen der meiste Schadcode verbreitet wird. Doch es sind nicht die US-Amerikaner, die über die Gefahren des Internets am schlechtesten informiert sind: Das Schlusslicht bildet Russland. Von allen Nationalitäten schenken russische Anwender vier der elf falschen Aussagen am meisten Glauben. Dass sie andererseits zwei anderen Aussagen am wenigsten Glauben schenken, bewahrt sie nicht vor dem letzten Platz in diesem Ranking.

3.2.4 Sind Männer die besseren Surfer?

Die Annahme, Männer seien technisch versierter als Frauen, ist bei vielen Menschen (unbewusst) tief verankert. Sollte dies stimmen, müssten Männer auch besser darüber informiert sein als Frauen, wo die wirklichen Gefahren des Internets liegen und welche Ängste veraltet bzw. unrealistisch sind. Ist das wirklich so? Die folgende Tabelle zeigt, wie es um die Einschätzungen bei Männern und Frauen in puncto Internet-Mythen steht.

Tabelle 12: Wer glaubt eher an die Aussagen: Männer oder Frauen?

These	Männer	Frauen	Total
1) Wenn mein System infiziert ist, merke ich dies in irgendeiner Weise an meinem PC.	91,50%	93,60%	92,59%
2) Kostenlose Virenschutzsoftware und kostenpflichtige Softwarepakete bieten dieselben Schutzfunktionen.	84,01%	81,73%	82,92%
3) Die meiste Malware wird per E-Mail verbreitet.	54,53%	54,31%	54,42%
4) Ein PC kann nicht lediglich durch das Laden einer infizierten Webseite selbst infiziert werden.	48,19%	48,46%	48,33%
5) Die meisten Computerschädlinge verbreiten sich über infizierte Dateien in Tauschbörsen wie Peer2Peer-Netzwerken oder Torrent-Webseiten.	49,13%	47,47%	48,27%
6) Bei Porno-Webseiten ist die Gefahr höher auf Malware zu treffen, als beispielsweise beim Besuch von Webseiten über den Reitsport oder übers Reisen.	43,88%	31,07%	37,23%
7) Meine Firewall schützt mich vor Drive-by-Download-Attacken.	26,02%	25,32%	25,66%
8) Wenn man keine infizierten Dateien öffnet, kann der PC nicht infiziert werden.	22,65%	21,16%	21,88%
9) Die meiste Malware wird über USB-Sticks verbreitet.	13,47%	12,24%	12,83%
10) Ich besuche keine seltsamen Webseiten. Deswegen bin ich nicht gefährdet, was Drive-by-Downloads betrifft.	11,74%	13,51%	12,66%
11) Internetkriminelle interessieren sich nicht sehr für privat genutzte Computer.	8,75%	6,35%	7,50%

Die Auswertung zeigt, dass Frauen die Gefahren leicht besser einschätzen als Männer. Lediglich bei drei Aussagen lagen sie hinter den männlichen Internetnutzern. Betrachtet man alle Einschätzungen, so zeigt sich nur ein marginaler Unterschied von weniger als zwei Prozent. Ob Frauen somit besser informiert sind als Männer – oder umgekehrt – ist daher fraglich.

Wo liegen die Unterschiede?

Die deutlichsten Unterschiede zwischen Männern und Frauen zeigen sich bei der These „Bei Porno-Webseiten ist die Gefahr höher auf Malware zu treffen, als beispielsweise beim Besuch von Webseiten über den Reitsport oder über Reisen“. Warum diese falsche Aussage so viel häufiger von Männern vertreten wird, kann möglicherweise auf dieselbe Weise erklärt werden wie die Antworten der jüngeren Befragten, die der folgenden Aussage den stärksten Glauben schenken: „Die meisten Viren und Computerschädlinge verbreiten sich durch infizierte Dateien in Tauschbörsen wie Peer-2-Peer-Netzwerken und Torrent-Webseiten“.

Wo könnte der Grund für eine unterschiedliche Einschätzung liegen? Hat eine Zielgruppe mehr Erfahrung beim Umgang mit derartigen Webseiten, ist es in dieser Gruppe möglicherweise bereits öfter vorgekommen, dass sie auf diesen Webseiten auf Malware gestoßen sind? Dies ist jedoch kein Beweis dafür, dass die Aussage richtig ist. Denn haben die männlichen Befragten ebenso häufig Webseiten besucht, auf denen es um den Reitsport geht? Und selbst wenn dies der Fall wäre und dennoch auf keiner dieser Webseiten eine Infektion mit Schadsoftware aufgetreten ist: Könnte es nicht auch Zufall sein, dass in keinem dieser Fälle ein Drive-by-Infektion stattgefunden hat?

Frauen haben vermutlich weniger Erfahrung mit pornografischen Internetangeboten und haben deshalb möglicherweise noch keinen Drive-by-Download-Angriff auf einer solchen Webseite erlebt. Aus der Sicht der Frauen ist eine Porno-Webseite daher möglicherweise genauso gefährlich oder ungefährlich wie jede andere Internetseite. Eine weitere Erklärung für die unterschiedliche Bewertung könnte eine psychologische Betrachtungsweise liefern. Pornos empfinden die meisten Menschen als ungehörig und schlecht, also als etwas, was heimlich betrachtet werden muss. Wenn die Menschen das Gefühl haben, eigentlich etwas Unerlaubtes zu tun, sind sie möglicherweise eher darauf eingestellt sich eine Strafe für ihr Verhalten einzuhandeln: in diesem Fall eine Malware-Infektion. Es ist eine statistische Tatsache, dass mehr Männer als Frauen Pornos konsumieren und dass sie daher wohl vermuten, beim Besuch von Porno-Webseiten auf Schadcode zu treffen.

Neben dieser Frage nach den Erotikseiten gibt es noch eine weitere Aussage, dessen Beurteilung bei Männern und Frauen ziemlich unterschiedlich ausfällt: Männer glauben häufiger, dass ihr Privatcomputer für Cyberkriminelle uninteressant ist. Frauen fühlen sich hier weniger sicher. Möglicherweise liegt dies an der Tatsache, dass Frauen im Allgemeinen vorsichtiger mit ihrem PC umgehen – vielleicht, weil sie in dieser Hinsicht weniger Selbstvertrauen haben – und daran, dass Männer risikobereiter sind. Wahrscheinlich spricht aus dieser Annahme vor allem eine Hoffnung, die die männlichen Befragten hegen.

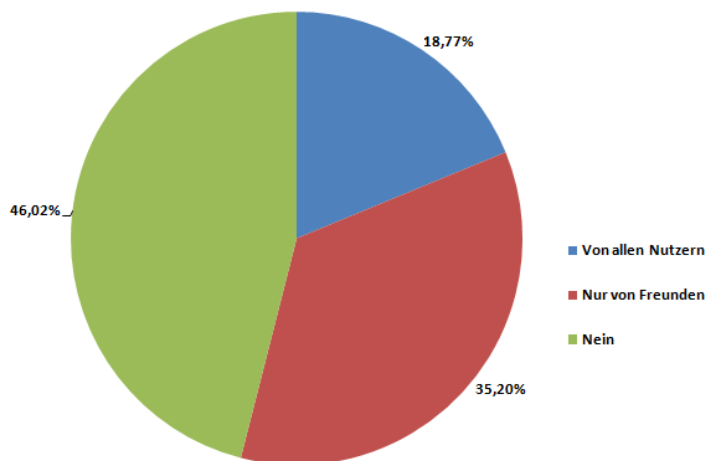
3.3 Verhalten in sozialen Netzwerken

Soziale Netzwerke werden immer populärer und sind so zu einem festen Bestandteil der Internetlandschaft geworden. In Facebook, Twitter und Co. präsentieren sich deren Nutzer und pflegen ein oftmals großes und internationales Freundesnetzwerk. Die große Beliebtheit der sozialen Netzwerke ruft allerdings zunehmend Kriminelle auf den Plan, die die sozialen Portale für ihre kriminellen Machenschaften missbrauchen.

Die Betrüger haben mehrere Möglichkeiten um Nutzer zu schädigen: Generell können die Zugangsdaten der Anwender zum Netzwerk über „klassisches“ Phishing mit Hilfe täuschend echt nachgebauter Webseiten oder über den Diebstahl der Zugangsdatenbank des Anbieters entwendet werden. Eine sehr gängige Masche der Kriminellen in sozialen Plattformen ist die Verbreitung von schadhafte Internetadressen via Pinnwandeintrag, Chat-Nachricht oder persönlicher Nachricht. Versprochen wird z. B. ein Link zu einem Video.

Die angesprochenen Webseitenadressen sind oft durch einen URL-Verkürzungsdienst so stark abgekürzt, dass ein Nutzer keinen Hinweis auf ein Risiko entdecken kann. Der Klick auf diese Links führt zu einer externen Internetseite, die entweder mit Schadcode verseucht ist, mittels Phishing Daten stiehlt oder das Opfer über Clickjacking zur Spam-Schleuder im sozialen Netzwerk macht. Dabei verbreitet der Nutzer ungewollt und für ihn nicht ersichtlich den Link in seinem Freundes-Netzwerk. Bei Links von Unbekannten ist daher Vorsicht geboten, aber auch Freunde können solche Internetadressen verbreiten, z. B. wenn das Benutzerkonto von einem Kriminellen gehackt und genutzt wird. Aufgrund des hohen Gefahrenpotentials enthielt die G Data Security Studie 2011 die Frage, ob die Anwender Links in sozialen Netzwerken anklicken.

Diagramm 9: Klickverhalten bei Webseiten-URLs in sozialen Netzwerken

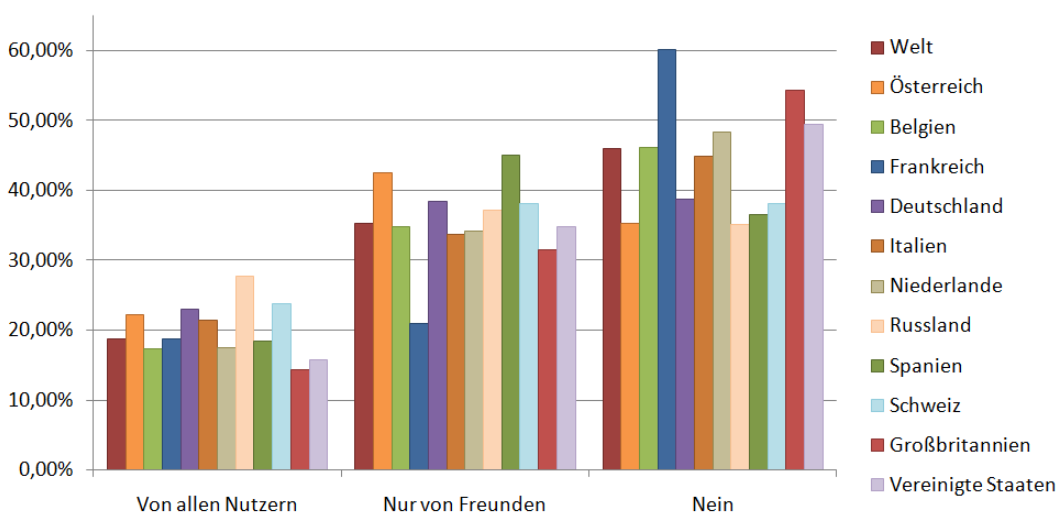


Die Mehrheit der in der Studie befragten Teilnehmer nutzt generell angebotene Links in sozialen Netzwerken. 46 Prozent aller Befragten klickt nicht auf Webseiten-URLs, unabhängig ob diese von Freunden oder Unbekannten stammen. Mehr als ein Drittel vertraut den Internetadressen die Freunde aus dem eigenen Netzwerk veröffentlicht haben. Lediglich gut 19 Prozent wählen alle Links an, egal von wem sie stammen und machen sich so leicht zur Zielscheibe von Cyberkriminellen und ihren illegalen Handlungen.

Im Ländervergleich sticht besonders Frankreich hervor

60 Prozent der Franzosen klicken nicht auf Links in sozialen Netzwerken. Dies ist im Vergleich zu allen anderen Ländern der höchste Wert. 18 Prozent klicken Internetseiten von allen Nutzern an. Dieser Wert ist exakt gleich mit dem Durchschnittswert aus dem Ländervergleich. Außerdem klicken nur 21 Prozent der Umfrageteilnehmer Webseiten an, die Mitglieder des Freundesnetzwerkes auf der sozialen Plattform gepostet haben. Im Vergleich zu anderen Ländern und dem Durchschnittswert ist dieser am niedrigsten. Die Franzosen erweisen sich demnach am sensibelsten für Gefahren von Verweisen auf Webseiten in sozialen Netzwerken.

Diagramm 10: Klickverhalten bei Webseiten-URLs in sozialen Netzwerken im Ländervergleich



Am wenigsten bewusst über die Gefahren von Links sind sich die Befragten aus Russland: Mehr als ein Viertel der Interviewten gab an URLs von allen bekannten und unbekanntem Nutzern des sozialen Netzwerkes anzuklicken und ist damit Spitzenreiter bei dieser Antwortmöglichkeit. Nur 35 Prozent klicken überhaupt keine Webseiten-URLs an. 37 Prozent der befragten Russen wählen nur Internetadressen von Freunden an.

Tabelle 13: Klickverhalten bei Webseiten-URLs in sozialen Netzwerken in den einzelnen Ländern

Klicken Sie auf Links, die in sozialen Netzwerken veröffentlicht werden?			
	Von allen Nutzern	Nur von Freunden	Nein
Welt	18,77%	35,20%	46,02%
Belgien	17,34%	34,80%	46,17%
Deutschland	22,95%	38,36%	38,69%
Frankreich	18,77%	21,01%	60,22%
Großbritannien	14,29%	31,46%	54,25%
Italien	21,44%	33,66%	44,90%
Niederlande	17,50%	34,14%	49,36%
Österreich	22,27%	42,45%	35,29%
Russland	27,74%	37,14%	35,12%
Schweiz	23,71%	38,14%	38,14%
Spanien	18,43%	45,04%	36,52%
Vereinigte Staaten	15,79%	34,80%	49,41%

3.3.1 Wer verhält sich sicherer in sozialen Netzwerken: Männer oder Frauen?

Bei der G Data Security Studie lässt sich tatsächlich ein Unterschied zwischen Frauen und Männern in Bezug auf die Nutzung von Links in sozialen Netzwerken erkennen. Dieser fällt nicht erwartungsgemäß aus, denn Frauen gehen in sozialen Communities grundsätzlich vorsichtiger vor.

Die Differenz fällt eher gering aus: 47 Prozent der Frauen vermeiden Links in sozialen Plattformen, während die Männer mit knapp 45 Prozent leicht darunter fallen. Dafür zeigen sich die männlichen Nutzer risikofreudiger beim Anklicken von Links unbekannter Quellen. Frauen klicken mehr als doppelt so häufig URLs von Freunden an, als Links von anderen Nutzern der sozialen Plattform. Bei den Männern bevorzugen etwa ein Drittel Internetadressen von Freunden.

Tabelle 14: Ergebnisse der Frage im Detail (Gesamtergebnisse aller Länder)

Klicken Sie auf Links, die in sozialen Netzwerken veröffentlicht werden?			
	Von allen Nutzern	Nur von Freunden	Nein
Männer (18-24)	26,24%	38,02%	35,74%
Männer (25-34)	25,92%	38,63%	35,45%
Männer (35-44)	21,09%	33,56%	45,35%
Männer (45-54)	18,23%	31,10%	50,66%
Männer (55-64)	15,93%	26,21%	57,86%
Gesamt Männer	21,46%	33,55%	44,99%
Frauen (18-24)	21,54%	45,38%	33,08%
Frauen (25-34)	20,43%	40,92%	38,64%
Frauen (35-44)	15,41%	35,59%	48,99%
Frauen (45-54)	13,72%	31,27%	55,01%
Frauen (55-64)	9,83%	30,48%	59,69%
Gesamt Frauen	16,29%	36,73%	46,99%
Gesamt	18,77%	35,20%	46,02%

Die Ergebnisse in den einzelnen Ländern geben, abgesehen von Italien, Belgien und Österreich ein ähnliches Bild ab:

Die Frauen gehen auch in diesen Ländern grundsätzlich vorsichtiger in sozialen Netzwerken vor und vermeiden das Anklicken von URLs entweder generell oder wenn sie den Absender nicht kennen. Im Vergleich zu den Männern tun sie dies häufiger, wenn auch die Differenz zwischen den Geschlechtern in der Regel nicht groß ist. Umgekehrte Verhältnisse zeigen die Ergebnisse der SecurityStudie in Italien, Belgien und Österreich: Hier scheinen die Männer geringfügig sensibler für Gefahren zu sein, die in sozialen Plattformen von Links ausgehen. Die Diskrepanz ist aber auch hier minimal.

Es zeigt sich also, dass die Unterschiede zwischen Männern und Frauen zwar vorhanden sind, aber sehr gering ausfallen. So kann als Schlussfolgerung nicht klar festgestellt werden, dass eines der beiden Geschlechter vorsichtiger im Umgang mit sozialen Netzwerken ist.

3.3.2 Nutzen jüngere Anwender soziale Netzwerke sicherer als ältere Nutzer?

Jüngere Internetnutzer sind bekanntermaßen häufiger in sozialen Netzwerken unterwegs und nutzen diese weitaus intensiver als ältere Surfer. Trotzdem ist die ältere Generation vorsichtiger im Umgang mit den sozialen Plattformen, wie das Gesamtergebnis der G Data Security Studie zeigt: Besonders vorsichtig sind bei Männern und Frauen gleichermaßen die beiden älteren Altersklassen von 45 bis 54 und 55 bis 64 Jahren (vgl. Tabelle 14).

Mehr als die Hälfte der Interviewpartner dieser Jahrgänge lehnt das Anklicken der URLs in sozialen Netzwerken kategorisch ab. Die Frauen dieser Generation sind sogar ein Stück kritischer als ihre männlichen Altersgenossen. Die drei jüngeren Altersklassen (bis 44 Jahre) bevorzugen dagegen erwartungsgemäß deutlich das Anklicken von geposteten Webseiten die von bekannten oder unbekanntem Anwendern stammen.

Fazit: Generation „Silversurfer“ hat die Nase vorn

Je älter die männlichen und weiblichen Befragten jeweils sind, desto seltener klicken diese in sozialen Netzwerken auf eingebundene Links zu externen Internetseiten. Dabei ist es irrelevant, ob diese von bekannten oder unbekanntem Personen stammen. Während Männer von 55 bis 64 Jahren das Anklicken zu fast 58 Prozent ablehnen, schlagen nur 36 Prozent der männlichen Altersklasse von 18 bis 24 Jahren das Anwählen aus. Bei den Frauen ist die Differenz noch größer: In der ältesten Jahrgangsklasse verneinen 60 Prozent das Anklicken im Gegensatz zu einem Drittel der 18- bis 24-jährigen Frauen. Im Umkehrschluss klicken weibliche Interviewte Links von Bekannten und Unbekannten vermehrt an je jünger sie sind. Das Gleiche gilt für Links von Bekannten aus dem Netzwerk-Freundeskreis.

Die Vorsicht der älteren Nutzer kann mehrere Ursachen haben. Sicherlich ist die ältere Generation im Regelfall unsicherer im Umgang mit sozialen Netzwerken. Diese Form des Mitmach-Web und der Online-Kommunikation ist ihnen nicht so geläufig wie der jüngeren Generation. Bei einigen älteren Menschen dürfte daher eine grundlegende Unsicherheit bei der Nutzung der sozialen Portale vorliegen. Die Älteren nutzen (wie oben schon angesprochen) soziale Netzwerke nicht in der Intensität wie es junge Nutzer tun und verbringen dort auch nicht so viel Zeit. Zudem besteht die Möglichkeit, dass die Kontakte in den Netzwerken dieser Altersgruppen keine oder kaum externe Links veröffentlichen und die Befragten so mit der Thematik nicht in Berührung kommen. Ein weiterer Aspekt liegt darin, dass junge Internetnutzer das Internet selbst und so auch soziale Netzwerke als eine Art Werkzeug sehen: Man kann Kontakte pflegen oder neue aufbauen, Zeit vertreiben und Persönliches preisgeben.

4 Schlussfolgerungen

IT-Security Know-how: Licht und Schatten

Die G Data Security Studie 2011 zeigt, dass die Mehrheit der Nutzer, unabhängig von Alter, Geschlecht oder Nationalität eine generelle Vorstellung über die Gefahren im Internet und über Computerschädlinge besitzt. Eine Sensibilisierung auf Anwenderseite scheint durch die stärkere Berichterstattung in den Medien somit erste Früchte zu tragen. Eine genaue Betrachtung zeigt jedoch ein ernüchterndes Bild: Nur die wenigsten Internetnutzer weltweit schätzen die Gefahren durch Malware (Computerschädlinge) und Cyberkriminelle richtig ein und wissen, wie sie ihre persönlichen Daten bzw. ihren Computer effektiv schützen.

Zwar glauben fast alle Umfrageteilnehmer zu wissen, was es mit Viren und anderem Schadcode auf sich hat, sie stützen sich dabei aber auf völlig veraltete Fakten. So bestehen viele Ängste vor Gefahren, die heute nur noch sehr selten auftreten. Etwa vor Malware, die massenhaft per E-Mail verbreitet wird (54 Prozent denken, dass die meisten Computerschädlinge auf diese Weise verteilt werden) oder die Vermutung, dass Malware den PC in seiner Funktionsweise für den Anwender offensichtlich beeinträchtigt (dies glauben 92 Prozent der Umfrageteilnehmer). Obwohl das in den 1990er-Jahren und teils auch im ersten Jahrzehnt des neuen Jahrtausends noch der Fall war, trifft dies heutzutage nicht mehr zu. Gerade letztere Fehleinschätzung birgt eine besondere Gefahr, denn: Solange diese Anwendergruppe an ihren PCs keine Auffälligkeiten feststellt, wiegt sie sich fälschlicherweise in Sicherheit. Die meisten Schadprogramme sind jedoch so geschickt programmiert, dass sie für den PC-Nutzer quasi unsichtbar sind. Eine der wenigen Ausnahmen bilden gefälschte Sicherheitsprogramme, sogenannte Rogueware, die eine angebliche Infektion des PCs vortäuschen. Der installierte Schädling ist so in der Lage, seinen Zweck lange im Sinne der Täter zu erfüllen.

Gefahrenquelle Internet: 48 Prozent liegen falsch

Die Verlagerung von Schadcode ins Internet, d. h. die Infizierung von Computern durch manipulierte Webseiten, gehört zu den erfolgreichsten Maschen der Täter und stellt derzeit die häufigste Methode zur Schadcode-Verbreitung dar. Der reine Besuch einer entsprechenden Webseite führt bei einem unzureichend abgesicherten System zur Infektion. Diese Form der Verbreitung von Schadprogrammen, also durch sog. Drive-by-Downloads (Drive-by-Infektionen), ist bei fast der Hälfte der Internetnutzer jedoch unbekannt – so das ernüchternde Ergebnis der G Data Security Studie 2011. 48 Prozent der Umfrageteilnehmer glauben demnach nicht daran, dass der eigene PC durch den Besuch einer verseuchten Webseite infiziert werden könnte. Die Internetnutzer, die von Drive-by-Infektionen gehört haben oder diese kennen, haben oft bestimmte Vorstellungen darüber, wo derartig infizierte Webseiten primär zu finden sind.

Vor allem Männer (fast 44 Prozent) vermuten, dass Webseiten mit pornografischen Inhalten überdurchschnittlich gefährlich sind. Dies impliziert jedoch auch, dass infizierte Webseiten nicht zufällig über das gesamte Web verstreut sind. Bei dieser Annahme wird außerdem nicht berücksichtigt, dass bekannte, vertrauenswürdige Webseiten gehackt und mit Schadcode infiziert werden könnten. Fast jede Woche findet man in den Medien Berichte über bedeutende Verbrauchermarken, deren Webseiten gehackt wurden. Und das sind nur die Fälle, die bekannt werden. Wer weiß, wie viele Fälle unentdeckt bleiben? Kurz gesagt: Für den Benutzer sind Drive-by-Infektionen, wie der Name schon sagt („Infektionen im Vorbeigehen“), nicht vorherzusehen. Folglich ist es nicht möglich, durch das eigene Verhalten zu vermeiden, dass der PC jemals damit in Berührung kommt.

Der effektivste Weg PCs vor Drive-by-Downloads (Drive-by-Infektionen) zu schützen, ist der Einsatz einer umfassenden Sicherheitslösung mit integriertem Webschutz (HTTP-Scan und Cloud basiertem Blacklisting), der Internetseiten auf Malware hin untersucht und diese automatisch blockt, bevor sie geladen werden. Kostenfreie Virenschutzlösungen enthalten diese Schutztechnologien nicht.

Wie das Ergebnis der Studie zeigt, liegt die Mehrheit der Anwender hier falsch: Nicht weniger als 62 Prozent der Nutzer kostenloser Virenschutzlösungen glauben, dass das Programm den PC vor Drive-by-Downloads schützt. 25 Prozent der Nutzer nehmen (fälschlicherweise) an, dass ihr PC durch die Firewall gegen Drive-by-Downloads geschützt sei. Viele dieser Anwender werden sich aufgrund ihrer falschen Annahmen nicht auf die Suche nach einem zusätzlichen Webschutz machen, um so vor infizierten Webseiten sicher zu sein. Ein Irrtum, der fatale Folgen haben kann.

Soziale Netzwerke: 46 Prozent klicken nicht auf Links

Der Schutz vor infizierten Webseiten ist gerade für Nutzer von sozialen Netzwerken sehr wichtig. In diesen Plattformen werden permanent Links zu externen Internetseiten mit witzigen oder informativen Inhalten oder zu Filmclips veröffentlicht. Gerade Funktionen wie diese machen Netzwerke wie Twitter und Facebook für ihre Anwender so attraktiv. Daher wäre es sehr schade, solche Links aus Sicherheitsgründen grundsätzlich unbeachtet zu lassen. Eine Vorsichtsmaßnahme, die jedoch 46 Prozent der Netzwerker laut Umfrageergebnis treffen. Ein großes Problem stellen dabei die verkürzten Links dar, da die kompletten Zieladressen für Anwender nicht mehr unmittelbar erkennbar sind. Diesen Umstand nutzen Online-Kriminelle vermehrt und locken Anwender so auf verseuchte Webseiten. In diesem Zusammenhang muss erwähnt werden, dass verkürzte Webseiten-URLs generell ein höheres Risiko mit sich bringen – und das nicht nur auf Social Media Plattformen. Anwender können die ursprüngliche Internetadresse mit speziellen Services wie <http://longurl.org> vorab ermitteln. Unabdingbar bleibt jedoch der Einsatz einer Sicherheitslösung die einen leistungsstarken Webschutz beinhaltet.

Gut informiert?

Die Auswertung der Studie zeigt, dass es keine Anwendergruppe gibt, die generell in allen Bereichen des IT-Security-Wissens die Nase vorn hat. Zwar hat die mittlere und hohe Altersgruppe zwischen 25 und 54 das größte Bewusstsein für Internetgefahren - allerdings haben sie oft auch Bedenken in Situationen, die kaum Gefahren bergen. Ob sie somit als die vernünftigeren Internet-Nutzer gelten können, ist daher zweifelhaft. Ebenso gilt dies für die „Generation Silversurfer“ im Vergleich zu den jüngsten Teilnehmern (vgl. hierzu Kap. 3.2.2 und 3.3.2).

Der Unterschied zwischen Männern und Frauen fällt ebenfalls sehr gering aus, auch wenn Frauen als Gesamtergebnis der G Data Security Studie 2011 minimal besser informiert zu sein scheinen. Eine allgemeine Schlussfolgerung, welches der beiden Geschlechter mehr Wissen über die Gefahrenpotenziale im Internet hat, kann daher nicht gezogen werden.

Auch wenn wir die Nationalität der Befragten betrachten, lässt sich kein eindeutiger Sieger ausmachen. In Deutschland und Großbritannien sind die Nutzer offenbar etwas besser darüber informiert, welche Internet-Bedrohungen real sind und welche nicht, doch auch hier sind die Unterschiede zum Gesamtdurchschnitt minimal.

Ein Land sticht bei der Umfrage deutlich hervor: In Russland ist die Unwissenheit über die Gefahren des Internets am größten. Glücklicherweise ist auf der anderen Seite der Anteil der russischen Surfer



die kostenpflichtige Security-Suiten nutzen im Ländervergleich der höchste. Anzumerken ist aber auch, dass in Russland die meisten Raubkopien kostenpflichtiger Security-Suiten im Einsatz sind.

Die Auswertung und Analyse aller Ergebnisse lässt insgesamt nur eine ernüchternde Schlussfolgerung zu: Trotz der intensiven Nutzung des Computers und des Internets ist das Wissen der meisten Anwender über die wirklichen Gefahren durch Computerschädlinge und deren technologische, sowie anwenderbasierte Abwehr weiterhin gering. Die weltweit agierenden und zum Teil gut organisierten Cyberkriminellen setzen bei einer Vielzahl ihrer Angriffskonzepte auf den Faktor Mensch. Eine kontinuierliche Aufklärung und Information der Internetnutzer scheint daher weiterhin dringend geboten und ist ein nicht zu unterschätzender Baustein für mehr Sicherheit im Internet und im Kampf gegen Online-Kriminalität. Der Einsatz moderner Sicherheitslösungen, die umfassende und aufeinander abgestimmte Schutztechnologien bieten, ist dabei obligatorisch.



Anhang

G Data Software AG

Die G Data Software AG, mit Unternehmenssitz in Bochum, ist ein innovatives und schnell expandierendes Softwarehaus mit Schwerpunkt auf IT-Sicherheitslösungen. Als Spezialist für Internetsicherheit und Pionier im Bereich Virenschutz entwickelte das 1985 in Bochum gegründete Unternehmen bereits vor mehr als 20 Jahren das erste Antiviren-Programm.

G Data ist damit eines der ältesten Security-Software-Unternehmen der Welt. Seit mehr als fünf Jahren hat zudem kein anderer europäischer Hersteller von Security-Software häufiger nationale und internationale Testsiege und Auszeichnungen errungen als G Data.

Das Produktportfolio umfasst Sicherheitslösungen für Endkunden, den Mittelstand und für Großunternehmen. G Data Security-Lösungen sind in weltweit mehr als 90 Ländern erhältlich.

Weitere Informationen zum Unternehmen und zu G Data Security-Lösungen finden Sie unter www.gdata.de

G Data Meilensteine

1986

Die CeBIT wird flügge und G Data stellt auf der Messepremiere das erste Konzept eines Virenschutzes für ATARI-Rechner vor.

1987

G Data entwickelt zahlreiche innovative Programme für den ATARI ST, darunter auch das erste Virenschutzprogramm weltweit: G Data AntiVirenKit.

1990

Die Verbreitung von Personal Computern schreitet rasant voran. G Data beginnt mit der Entwicklung von Software für MS-DOS. Das erste Projekt ist die Umsetzung des AntiVirenKits für PCs – damals ein Novum: die eigene grafische Benutzeroberfläche.

1991

G Data wächst kontinuierlich und bietet ein breites Spektrum unterschiedlicher Softwareprogramme für den ATARI ST.

1992

Neben Virenschutz-Programmen entwickelt G Data zahlreiche Anwendersoftware für MS-DOS und Windows. Besonders innovativ: Der Routenplaner GeoRoute – der erste PC Routenplaner mit interaktiver Karte.

1995

Eröffnung der ersten Auslandsniederlassung in Polen

1998

PowerRoute ist mit über 1 Mio. verkauften Stück der erfolgreichste PC-Routenplaner Deutschlands



2000

Umwandlung in eine Aktiengesellschaft: G Data Mitarbeiter werden an dem Unternehmen beteiligt. Bis heute gehören die Mehrheitsanteile den Mitarbeitern und den Firmengründern.

2001

Eintritt in den Netzwerk- und Business-Markt mit G Data AntiVirus Business und AntiVirus Enterprise.

2002

G Data entwickelt die DoubleScan-Technologie und schafft es als erster Hersteller, zwei Viren-Engines parallel in seinen Produkten einzusetzen.

2003

Going International: Markteintritt in Japan

2004

G Data präsentiert auf der CeBIT die erste Programmgeneration seines umfassenden Sicherheitspakets G Data InternetSecurity.

2005

Der Zeit voraus: G Data integriert in seine Schutzprogramme als eines der ersten Unternehmen weltweit Cloud-Security-Technologie. OutbreakShield schützt inhaltsunabhängig in Echtzeit vor Spam und unbekanntem Computerschädlingen.

Die Stiftung Warentest bewertet G Data InternetSecurity als bestes Sicherheitspaket.

Going International: Eröffnung der Niederlassungen in Frankreich und Italien

2006

Die Zahl der Computerschädlinge steigt - G Data reagiert: Mit stündlichen Signatur-Updates sind G Data Kunden schnell vor neuer Malware geschützt.

2007

Stiftung Warentest: Zum zweiten Mal in Folge gewinnt G Data InternetSecurity 2010 den ersten Platz im großen Vergleichstest des renommiertesten deutschen Verbrauchermagazins.

CeBit-Premiere 2007: G Data TotalCare

2008

Markteinführung einer speziellen Sicherheitslösung für Notebook-Besitzer: G Data NotebookSecurity vereint als leistungsstarke All-in-One-Lösung Virenschutz, Backup und Verschlüsselungstechnik.

2009

G Data Sicherheitslösungen sind weltweit in mehr als 60 Ländern erhältlich. Mit den Markteintritten in Südamerika, Russland, Süd-Afrika und China setzt G Data seine erfolgreiche Expansionspolitik fort.

2010

G Data feiert sein 25-jähriges Firmenjubiläum

CeBIT-Premiere: G Data EndpointProtection

2011

CeBIT Premiere G Data CloudSecurity – Kostenfreies Browser-Plugin zur Absicherung der Internetnutzung

Smarter Schutz für Android Smartphones und Tablet-PCs: G Data MobileSecurity

Survey Sampling International

SSI erfand im Jahr 1977 das kommerzielle Stichprobengeschäft in den USA. Wir bestimmen seit über drei Jahrzehnten den Standard für das Fachwissen und die Qualität von Stichproben- und dem Kundenservice im Bereich Marktforschung.

SSI bietet Zugriff auf über 6 Millionen Befragungsteilnehmer in 54 Ländern. Zu unseren Quellen gehören eigene SSI Panel-Communities in 27 Ländern, eine wachsende Zahl von uns geführter Tochterunternehmen und unser umfangreiches weltweites Netzwerk aus Partnerunternehmen. SSI arbeitet mit 400 firmeneigenen Mitarbeitern aus 50 Ländern, die 36 Sprachen sprechen, für über 1.800 Marktforschungskunden und drei Viertel der weltweit größten Marktforschungsunternehmen.

Das Unternehmen verfügt weltweit über 17 Geschäftsstellen: Peking, Frankfurt, London, Los Angeles, Madrid, Mexico City, Paris, Rotterdam, Seoul, Shanghai, Shelton (CT), Singapur, Stockholm, Sydney, Timisoara (Rumänien) Tokyo und Toronto. Zusätzlich finden Sie auch SSI Repräsentanten in Hong Kong.

Mehr über Survey Sampling International unter www.surveysampling.com

Glossar

Bot: Bots sind kleine Programme, die meist unbemerkt im Hintergrund auf den Rechnern der Opfer laufen und dort je nach Funktionsumfang diverse Dinge erledigen – von DDoS-Attacken über E-Mail-Spam bis zum Mitlesen von Tastatureingaben und vielem mehr. Der Funktionsumfang ist primär eine Frage wie viel Geld man für einen Bot anlegen möchte. Bots mit einem sehr großen Umfang sind naturgemäß teurer als eher einfache Bots, die nur wenig können. Verkauft werden sie unter anderem in Untergrundforen.

Botnets: Ein Botnetz ist ein Verbund aus so genannten Zombie-PCs. Zur Verwaltung des Botnetzes werden Command-and-Control-Server (C&C Server) genutzt. Botnetze werden unter anderem dafür benutzt, um gezielte Überlastangriffe auf Webserver zu starten (DoS- und DDoS-Attacken) und um Spam zu versenden.

DoS (Denial of Service): Bei einer Denial-of-Service-Attacke werden Rechner (meist Webserver) mit gezielten und/oder sehr vielen Anfragen bombardiert. Dadurch können sie ihre Dienste nicht mehr ausführen und brechen unter der Last zusammen.

DDoS (Distributed Denial of Service): Eine Distributed-Denial-of-Service-Attacke basiert auf demselben Prinzip wie eine normal DoS-Attacke, jedoch mit dem einzigen Unterschied, dass es sich hierbei um einen verteilten Angriff handelt. Oft werden diese Angriffe mit vielen tausend Zombie-PCs durchgeführt.

Drive-by-Infektion (Drive-by-Download): Bei einer Drive-by-Infektion wird beim Besuch einer präparierten Webseite unbemerkt Schadcode auf den Rechner heruntergeladen und ausgeführt. Die Täter nutzen für diese Attacke Sicherheitslücken im Browser und deren Plugins aus. Ein besonderes Augenmerk legen Angreifer auf die Schwachstellen in Funktionen zum Ausführen von aktiven Inhalten (z. B. JavaScript, Flash oder Java).

Exploit: Ein Programm, das eine bestehende Sicherheitslücke im Zielrechner ausnutzt, um beliebigen Programmcode auszuführen.

Phishing: Unter Phishing versteht man den Versuch persönliche Daten wie Login-Namen, Passwörter, Kreditkartennummern, Bankzugangsdaten etc. durch gefälschte Webseiten oder unerwünschte E-Mails zu erhalten. Meist richten sich Phishing-Versuche an Kunden von Banken mit Online-Banking-Angeboten (CityBank, Postbank), Bezahlendiensten (Paypal), Internet-Service-Providern (AOL) oder Online-Shops (eBay, Amazon). Dazu wird man in der Regel per Email oder Instant Messenger auf gefälschte Webseiten geleitet, die den Seiten der Vorbilder sehr genau nachempfunden sind.

Social Engineering: Als Social Engineering werden Überredungstaktiken bezeichnet, mit denen ein Hacker einen Anwender dazu veranlasst Informationen preiszugeben, die er dazu nutzen kann dem Anwender oder seiner Organisation Schaden zuzufügen. Oft wird dazu Autorität vorgespiegelt, um Zugangsdaten oder Passwörter zu erlangen.

Spam: Mitte der 90er Jahre bezeichnet Spam die übermäßige Verbreitung der gleichen Nachricht in Usenet-Foren. Der Begriff selbst geht auf einen Sketch von Monty Python zurück. Mittlerweile verwendet man Spam in mehreren Bedeutungen. Als Oberbegriff steht Spam für alle unaufgefordert zugesandten E-Mails. In einem engeren Sinn beschränkt sich der Begriff Spam auf Werbemails; das heißt: Würmer, Hoaxes, Phishing-Mails und AutoResponder werden nicht dazu gezählt.

Zombie-PC: Als Zombie bezeichnet man einen PC, der sich über eine Backdoor fernsteuern lässt. Analog zum filmischen Vorbild gehorcht der Zombie-PC nur noch dem verborgenen Master und führt dessen oftmals verbrecherischen Befehle aus. Viele Zombies werden zu sogenannten Botnetzen zusammengefasst.