

Inhalt

Sicherer Auftritt im Internet	4
So bewegen Sie sich sicher im Internet – 10 hilfreiche Tipps	6
Für Nutzer drahtloser Netzwerke	10
Übersicht über weit verbreitete Bedrohungen	12
Andere Arten von Bedrohungen	18
Verbreitungsmechanismen	22
Proaktive und traditionelle Antivirenlösungen im Vergleich	24

Sicherer Auftritt im Internet

Es ist keine leichte Aufgabe, mit den Entwicklungen auf dem Gebiet der IT-Sicherheit und -Kriminalität Schritt zu halten. Die Notwendigkeit für effektive Schutzmaßnahmen ist jedoch offensichtlich, und elementare Kenntnisse über die am häufigsten auftretenden Risiken sind unerlässlich. Dieses kleine grüne Buch soll Ihnen helfen, aktuelle und weit verbreitete Bedrohungen zu erkennen, die Auswirkungen von Malware auf den Benutzer einzuschätzen und geeignete Schutzmaßnahmen zu ergreifen.

Computerviren und andere Bedrohungen der IT-Sicherheit sind Probleme, die seit langer Zeit bekannt sind. Der erste Computervirus wurde vor mehr als 25 Jahren entdeckt, und die damit zusammenhängenden Probleme haben sich über die Jahre mit alarmierender Geschwindigkeit vervielfacht. Während die ersten Viren darauf abzielten, Systeme zu ruinieren und zum Absturz zu bringen, ist das Vorgehen heutiger Urheber von Schadprogrammen

(Malware) weitaus raffinierter und meist von wirtschaftlichem Interesse geprägt. Malware-Autoren sind meist gut organisiert und bedienen sich ausgeklügelter Methoden zur Verbreitung ihrer Software. Hacker stehlen private Daten, um sich zu bereichern oder überwachen Ihre Surfgewohnheiten im Internet, um Sie mit maßgeschneiderten Werbebotschaften zu „beglücken“. Einige Hacker sammeln außerdem Email-Adressen, die auf Ihrem System gespeichert sind, und verkaufen sie an andere Unternehmen.

Hinweis:

IT-Kriminalität bewegt sich zunehmend im organisierten Rahmen und verursacht immer komplexere Bedrohungsszenarien.

So schützen Sie sich

Im Internet lauern viele Gefahren. Nutzer von drahtlosen Netzwerken (WLAN) und bluetooth-fähigen Geräten sind diesen Gefahren in höherem Maße ausgesetzt als andere. Mobile Technologien sind extrem anfällig, und deren Nutzer müssen deshalb besonders wachsam sein. Sie sollten Bluetooth-Verbindungen abschalten, wenn sie nicht benötigt werden. Das Erste, wonach potenzielle Hacker bei

einem Bluetooth-Gerät Ausschau halten, ist der SSID (Service Set Identifier) – der schlichtweg nicht auffindbar ist, wenn die Verbindung deaktiviert wurde.

Der physische Verlust von Daten ist eine weitere Gefahr. Mit steigender Anzahl an Computerbenutzern, die zu Hause oder außerhalb der Büroräume arbeiten, wächst auch das Datendiebstahlrisiko. Achten Sie darauf, wo Sie Ihr Notebook abstellen oder Ihre externen Speichersticks deponieren. Sicherheitslücken und Malware, die diese Schwachstellen

ausnutzt, wurden auch bei Mobiltelefonen, Geldautomaten und Internetbanken festgestellt. Ein Beispiel ist der Cabir-Virus, der sich von einem Mobiltelefon auf andere ausbreiten kann. Es ist davon auszugehen, dass solche Geräte einem besonderen Risiko für Malware-Angriffe ausgesetzt sind, da sie im Zuge der technischen Weiterentwicklung durch den Einsatz von Computertechnologien immer ausgefeiltere Funktionalitäten aufweisen. Lesen Sie dazu auch den separaten Abschnitt für *Nutzer drahtloser Netzwerke* in diesem Dokument.



SO BEWEGEN SIE SICH SICHER IM INTERNET – 10 HILFREICHE TIPPS

1. Lassen Sie keine „Fremden“ hinein
Überprüfen Sie vor dem Zugriff auf das Internet sorgfältig die Konfiguration Ihres PCs. Achten Sie dabei insbesondere auf freigegebene Ordner und Ressourcen. Sie werden kaum daran interessiert sein, Ihre privaten Daten der gesamten Internet-Community zugänglich zu machen. Genau dies könnte aber passieren, wenn Sie allzu sorglos mit Ihren Daten umgehen. Freigegebene Daten sind eine der gefährlichsten Sicherheitslücken in Windows-Systemen, die sich Eindringlinge gerne zunutze machen. Sie sollten Ihren PC auch immer abschalten, wenn Sie ihn nicht benutzen.

2. Verwenden Sie professionelle Bereinigungsprogramme

Die Installation von Antiviren-Software ist eine unverzichtbare Sicherheitsmaßnahme. Ebenso wichtig ist, dass das Virenschutzprogramm in regelmäßigen Abständen aktualisiert wird – vorzugsweise automatisch beim Herstellen der Internetverbindung. Mit der Installation von Anti-Spyware- und Anti-Adware-Programmen halten Sie Ihr System frei

von Spyware und Adware. Eine weitere Sicherheitsmaßnahme ist die Überprüfung eingehender Email Nachrichten, bevor sie in Ihr System gelangen. Viele Hersteller von Antiviren-Software bieten diesen Service an.

3. Aktualisieren Sie Ihr Betriebssystem in regelmäßigen Abständen

Das Betriebssystem ist das Herzstück aller Aktivitäten auf dem Computer. Leider wurde bisher noch kein Betriebssystem erfunden, das zu 100% fehlerfrei ist. Virenautoren nutzen solche Software-Fehler oft für Angriffe. Stellen Sie deshalb sicher, dass stets alle wichtigen Sicherheitsupdates unmittelbar nach der Veröffentlichung heruntergeladen und so schnell wie möglich installiert werden.

4. Betrachten Sie Emails kritisch

Vertrauen Sie Ihrem gesunden Menschenverstand. Wenn nur eine der folgenden Situationen zutrifft, sollten Sie die Nachricht einfach löschen:

- Der Absender ist unbekannt.
- Der Betreff ergibt keinen Sinn.
- Die Email enthält verdächtige Anlagen.

-
- Die Email enthält einen Website-Link, von dem Sie nicht wissen, wohin er Sie führen wird.
 - Die Email als solche macht einen verdächtigen Eindruck.
 - Die Email scheint von einem Softwareanbieter zu stammen und enthält im Anhang ein Programm, das sich als Sicherheitsupdate ausgibt. Softwareanbieter versenden niemals Sicherheitsupdates per Email!
 - Die Verwendung der Vorschaufunktion in Email-Programmen ist ein Sicherheitsrisiko. Schalten Sie sie ab und löschen Sie unerwünschte Nachrichten sofort, ohne sie überhaupt zu öffnen.
 - Ein Spam-Filter erspart Ihnen viel Zeit (und Ärger), die Sie andernfalls mit dem Löschen unerwünschter Emails verbringen, die nicht selten auch Schadprogramme enthalten. Antworten Sie niemals auf Spam-Mails. Durch eine Antwort erhält der Sender die Bestätigung, dass die Email-Adresse tatsächlich gültig ist und verwendet wird.
 - Es empfiehlt sich, vertrauliche Informationen vor dem Senden zu verschlüsseln.

5. Engagieren Sie einen zuverlässigen „Türsteher“

Auf Ihrem Computer gibt es viele „Eingänge“ (Ports) für verschiedene Aufgaben. Offene Ports ermöglichen unter Umständen den uneingeschränkten Zugriff auf die Ressourcen Ihres Computers. Port 25 wird üblicherweise für Email verwendet und von den meisten Spammern genutzt. Port 80 ist der normale Zugang zum Web. Der Hauptzweck einer persönlichen Firewall besteht im Schutz des Computers gegen „unerwünschte Besucher“, Angreifer aus dem Internet. Firewalls können auch so konfiguriert werden, dass Daten von bestimmten Adressen blockiert werden.

6. Verschießen Sie „Aktenschränke“ mit vertraulichen Daten

Speichern Sie vertrauliche Daten an einem sicheren Ort. Auf tragbaren Computern, die leicht abhanden kommen, ist dies von besonderer Bedeutung. Die beste Lösung ist die Verwendung von Verschlüsselungsprogrammen, die auf komplette Ordner, aber auch auf einzelne Dateien angewendet werden können.



7. Geben Sie Eindringlingen keine Chance

Konfigurieren Sie Ihren Webbrowser so, dass bei „aktivem Inhalt“ die Nachfrage erfolgt, ob die Ausführung zugelassen werden soll. In vielen Websites sind Skripts und andere Programme integriert, um ein optimales Surferlebnis zu bieten. Dies birgt jedoch ein gewisses Sicherheitsrisiko, da dabei Programmcode auf Ihrem Computer ausgeführt wird. Seien Sie wählerisch, wenn es um die Frage geht, welchen Websites Sie Zugriff auf Ihren eigenen Computer erlauben, und haben Sie ein kritisches Auge auf Programme, die Sie aus dem Web oder aus Peer-to-Peer-Netzwerken (P2P) herunterladen.

8. Lassen Sie sich von erfahrenen IT-Mitarbeitern beraten

Wenn Sie bei Ihrer täglichen Arbeit einen tragbaren Computer verwenden, sollten Sie sich zuallererst mit den im Hinblick auf die IT-Sicherheit geltenden Regelungen und Richtlinien Ihres Arbeitgebers vertraut machen. Viele Probleme werden

erst gar nicht auftreten, wenn Sie die Ratschläge erfahrener IT-Mitarbeiter Ihres Unternehmens befolgen.

9. Verraten Sie so wenig wie möglich über sich

Geben Sie niemals persönliche Daten preis, wenn dies nicht absolut notwendig ist. Es empfiehlt sich zudem, für verschiedene Anfragen unterschiedliche Email-Adressen zu verwenden.

*Hinweis:
Geben Sie nicht
unbedacht persönliche
Daten im Internet preis..*

10. Sichern Sie wichtige Informationen

Daten können versehentlich gelöscht werden – durch Malware-Aktivität oder von Übeltätern, die Zugriff auf Ihre Daten erlangt haben. Sichern Sie daher wichtige Daten regelmäßig. Zu den wichtigsten Daten zählen jene Dateien, deren Erstellung Sie viel Zeit und Mühe gekostet hat. Software und andere Systemdateien können nach Beschädigung einfach neu installiert werden.

FÜR NUTZER DRAHTLOSER NETZWERKE

Nutzer drahtloser Netzwerke (WLAN) sollten besondere Vorsichtsmaßnahmen ergreifen, um sich zu schützen. Ein drahtloses Netzwerk lässt sich leicht verwalten und kann sehr effektiv genutzt werden. Der Zugang ist recht einfach. Andererseits birgt dies Risiken durch das Eindringen von illegalen Benutzern. Wenn Sie Ihr drahtloses Netzwerk nicht absichern, kann es heimlich für illegale Zwecke, wie etwa zum Download und Verteilen von Spam, genutzt werden. Im schlimmsten Fall können Angreifer Zugriff auf Ihren Computer erlangen.

Hier einige wichtige Tipps für Benutzer drahtloser Netzwerke:

1. Schützen Sie Ihr Netzwerk mit einem Autorisierungsschlüssel

In der Benutzerdokumentation finden Sie weitere Informationen zu diesem Thema. Es handelt sich um einen einfachen Vorgang, der von jedermann ausgeführt werden kann. Sie müssen lediglich den

korrekten Code eingeben, um den Zugriff auf das Netzwerk zu ermöglichen. Wenn Sie einen Autorisierungsschlüssel verwenden, gehen Sie sicher, dass nur Computer, die den richtigen Schlüssel besitzen, auf das private Netzwerk zugreifen können, und dass der Datenverkehr im Netzwerk verschlüsselt

*Hinweis:
Schalten Sie Ihren
Computer immer
aus, wenn Sie ihn
nicht benutzen.*

ist. Die gängigsten Verschlüsselungsmethoden sind WEP und WPA.

2. Verwenden Sie Antivirenprogramme

Wie alle Netzwerknutzer sollten sich WLAN-User durch Antivirenprogramme schützen. Drahtlose Netzwerke sind besonders anfällig, und Antivirenprogramme schützen Sie vor Viren, Würmern, Trojanern und anderem böserartigen Code. Die besten Lösungen sind proaktive Antivirenprogramme, die nicht auf herkömmlichen signaturbasierten Technologien beruhen. Proaktive Antivirenlösungen erkennen neue und unbekannte Viren und bieten somit den effektivsten Schutz für Ihren Computer.

3. Verwenden Sie Anti-Spyware- und Anti-Adware-Programme

Diese Programme entfernen Spyware und blockieren illegale Programme, die Ihre Internetaktivitäten ausspionieren.

4. Verschlüsseln Sie Ihre persönlichen Daten

Sicher möchten Sie Ihre Daten nicht jedermann zugänglich machen. Die beste Methode, Ihre Privatsphäre zu wahren, besteht in der Verschlüsselung Ihrer Daten. Sie können Verschlüsselungsprogramme installieren und so Email-Nachrichten, private Dateien, Unternehmensdaten, vertrauliche Aufzeichnungen und Email-Anhänge verschlüsseln.



ÜBERSICHT ÜBER WEIT VERBREITETE BEDROHUNGEN

Es gibt viele Bedrohungen, denen Sie als Computerbenutzer ausgesetzt sind.

Die häufigsten sind:

Malware

Computer-Malware („Malicious Software“ [Schadsoftware]) ist der allgemeine Begriff für bösartigen Programmcode, der darauf abzielt, ein Computersystem zu schädigen oder Störungen im Betrieb hervorzurufen. Im Folgenden finden Sie kurze Erläuterungen zu weit verbreiteten Schädlingen.

1. Virus

Ein Computervirus ist ein Programm, das sich – üblicherweise durch das Anhängen an Anwendungen – selbst reproduziert und verbreitet. Wenn eine infizierte Anwendung ausgeführt wird, kann sie andere Dateien infizieren. Viren können sich nur mit menschlicher Hilfe auf anderen Rechnern und Systemen ausbreiten. Übliche Verbreitungswege sind Download von Dateien, Austausch von CDs/DVDs und USB-Speichersticks, Kopieren von Daten von und auf Dateiserver oder das Öffnen infizierter Email-Anhänge.

Viren treten in unterschiedlicher Form auf:

Dateiviren:

Ein Dateivirus wird mit einer Programmdatei verknüpft. Er bedient sich verschiedener Techniken, um andere Programmdateien zu infizieren. Dieser Virustyp kann sich in Netzwerken und über alle Arten von (beschreibbaren) Speichermedien verbreiten.

Systemviren:

Systemviren – auch Bootviren genannt – können sich auf Bootgeräten (z.B. USB-Sticks und CDs) befinden, ohne dass der Benutzer dies bemerkt. Wird der Computer über das infizierte Gerät bzw. Speichermedium (neu) gestartet, infiziert der Systemvirus den Master-Boot-Sektor (MBS) und den System-Boot-Sektor (SBS).

Dropper-Viren:

Ein „Dropper“ ist ein eigens erstelltes oder modifiziertes Programm, das einen Virus auf dem Zielcomputer installiert. Er ist quasi der „Umschlag“, in dem sich der Virus verbirgt. Die Infektion findet statt, wenn der Virus auf dem Computer

installiert wird. Auch in diesem Fall reproduziert sich der Virus, nicht das Dropper-Programm. Oft wird eine Datei mit dem Namen README.exe oder LIESMICH.exe verwendet, die die Neugier des Benutzers erregen soll und so sicherstellt, dass dieser die Datei auch tatsächlich öffnet. Ein Dropper ist eigentlich eine Art trojanisches Pferd, das dem Zweck dient, einen Virus zu installieren.

Makroviren:

Makroviren können in Anwendungen eingeschleust werden, in denen eine Makrosprache integriert ist, beispielsweise Word, Excel und Access. Der Virus verbreitet sich von einem Dokument zum anderen, und die Infektion beginnt, wenn das Dokument geöffnet wird. Früher waren Makroviren eine sehr „beliebte“ Art von Malware. Heute ist diese Art von Viren nicht mehr weit verbreitet. Im Gegensatz zu anderen Malware-Arten treten nur wenige neue Varianten auf.

2. Würmer

Ein Netzwerkwurm infiziert andere Computer und verbreitet sich ohne

menschliches Zutun automatisch in Netzwerken. Die Tatsache, dass Würmer zur Verbreitung nicht auf menschliches Eingreifen angewiesen sind, führt zu einer sehr viel schnelleren Ausbreitung als bei Viren. Ein Netzwerkwurm kann auf vielfältige Weise in ein Netzwerk eingeschleust werden, beispielsweise über USB-Sticks oder als Email-Anhang. Email-Würmer werden oft ohne Wissen des betreffenden Benutzers übertragen. Kennzeichnend für Email-Würmer ist, dass sie sich selbst an alle Email-Adressen versenden, die sie auf dem infizierten PC vorfinden. Die Email scheint also von einem dem Empfänger bekannten Absender zu stammen, was häufig dazu führt, dass die üblichen Vorsichtsmaßnahmen außer Acht gelassen werden.

3. Trojaner

Ein Trojaner ist ein Programm, das auf den ersten Blick harmlos erscheint. Es tarnt sich als etwas Nützliches und verleitet Sie so dazu, es auszuprobieren. Sobald Sie das Programm gestartet haben, öffnet der Trojaner jedoch Hintertüren im

*Die besten Lösungen sind
proaktive Antivirenprogramme,
die nicht auf herkömmlichen
signaturbasierten
Technologien beruhen.*

System und ermöglicht Hackern den Zugriff. In der Regel ist der unmittelbare Schaden nicht der Rede wert; der Schutz Ihres Systems ist jedoch durchbrochen, und Kriminelle können vertrauliche Daten stehlen und/oder unbemerkt die Kontrolle über Ihren Rechner übernehmen und diesen für illegale Zwecke missbrauchen.

4. Spyware

Als Spyware bezeichnet man jegliche Methode, die zum Sammeln von Infor-

mationen über eine Person, ein Unternehmen oder eine Organisation ohne deren Wissen und Einwilligung dient. Spyware wird meist heimlich installiert, beispielsweise beim Herunterladen einer

Datei oder durch Anklicken eines Werbe-Popups im Internet.

Spyware kann neben dem Anzeigen von Werbung (online oder offline) Ihre

automatische Signatur zurücksetzen, installierte Komponenten deaktivieren oder umgehen, Tastenanschläge überwachen,

Hinweis:

*Die Mehrzahl der
Spyware-Programme ist
schwer zu entfernen.*

Dateien auf Laufwerken durchsuchen, auf Anwendungen zugreifen und Browser-Startseiten ändern.

Sie können Dateien lesen, schreiben oder löschen und sogar die Festplatte neu formatieren, während sie gleichzeitig einen stetigen Strom von Daten an die Personen übertragen, die das Spyware-Programm kontrollieren. Einmal installiert, können einige dieser Programme nicht mehr mit den üblichen Methoden aus dem System entfernt werden. Sie hinterlassen auch nach dem Löschen häufig Komponenten, die sich erneut installieren und weiterhin Ihre Verhaltensmuster überwachen.

5. Adware

Adware ist eng mit Spyware verbunden. Viele Spyware-Programme werden mit der Absicht installiert, Adware-Programme zu starten. Adware-Software ruft Werbebotschaften auf, häufig in der Form von Popup-Fenstern. Die Werbung ist auf den jeweiligen Benutzer zugeschnitten und basiert auf den Informationen, die mittels Spyware über das Surfverhalten des Benutzers in Erfahrung gebracht wurden.

6. Backdoor

Backdoor („Hintertür“) ist ein Programm, das Ihren Computer für Zugriffe öffnet, die Sie nicht autorisiert haben. Solche Hintertüren ermöglichen Remotezugriffe, da die vorhandenen Authentifizierungsmechanismen umgangen werden.

Backdoor-Programme öffnen in der Regel bestimmte Ports; anschließend versucht der Urheber des Programms eine Verbindung über diese Ports herzustellen. Wenn es jemand geschafft hat, mehrere Computer mit Backdoor-Programmen zu infizieren, kann er eine ganze Palette von Computern überprüfen, identifizieren und für bestimmte Zwecke, zum Beispiel als „Zombie-Computer“ (siehe unten), missbrauchen.

7. Kombinationen von Malware

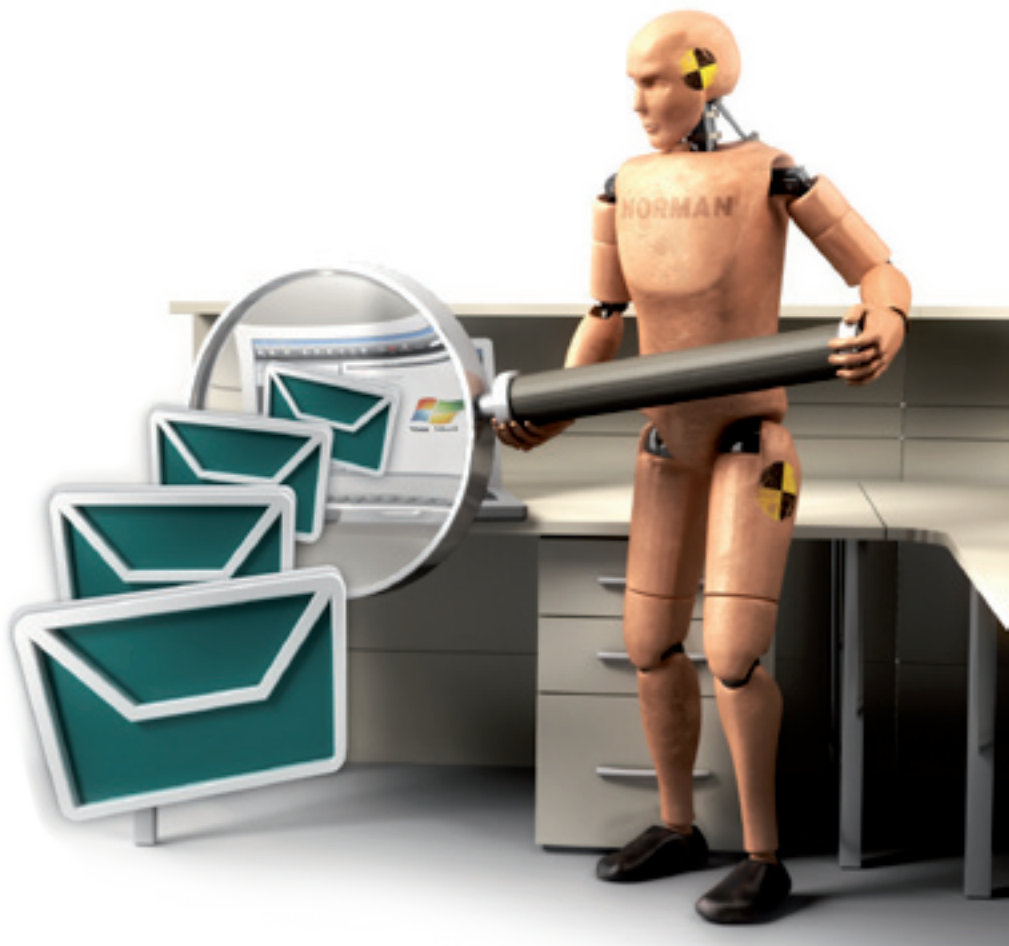
In letzter Zeit ist ein deutlich zunehmender Trend zu beobachten, mehrere der oben beschriebenen Methoden in einem Malware-Programm zu kombinieren. Würmer werden verwendet, um Viren zu verbreiten, die wiederum Backdoors und Spyware installieren, während Spyware-Programme dazu dienen, am Nutzerprofil

*Softwareanbieter
versenden niemals
Sicherheitsupdates
per Email!*

orientierte Werbebotschaften an den Mann zu bringen und ferngesteuerte PCs als Mailserver zum Versenden von Spam zu missbrauchen (siehe unten).

Besonders beachtenswert ist jedoch die Tatsache, dass sich die Malware selbstständig aktualisieren kann, indem neue Komponenten aus dem Internet heruntergeladen werden. Bei diesen neuen Modulen kann es sich um verschiedenste Arten von Schadsoftware handeln, die möglicherweise neue Funktionen umfassen.

Die Unterschiede zwischen den verschiedenen Bedrohungsarten verwischen in zunehmendem Maße. Die Malware-Autoren agieren heute zumeist aus wirtschaftlichem Interesse und verfügen über umfangreiche Ressourcen. Folglich wird Malware immer ausgereifter.



ANDERE ARTEN VON BEDROHUNGEN

1. Spam

Spam sind unerwünschte Emails, die wahllos in Massen versendet werden. Es ist eine äußerst effiziente und billige Methode, beliebige Produkte zu vermarkten. Studien belegen, dass mehr als die Hälfte aller Email-Nachrichten als Spam einzustufen ist, d.h. die meisten Benutzer sind davon betroffen.

Von Spam geht zwar keine unmittelbare Gefahr aus; der Umfang des erzeugten Email-Verkehrs und die Zeit, die Organisationen und die Nutzer aufwenden müssen, um den „Müll“ zu entsorgen, stellen aber allemal ein großes Ärgernis dar, welches langfristig kostspielig werden kann.

Spam wird auch zum Versenden verschiedener Arten von Malware verwendet (siehe oben).

2. Phishing

Als Phishing bezeichnet man eine Methode, bei der sich Kriminelle auf betrügerische Weise vertrauliche persönliche Daten (z.B. Kennwörter, Kreditkarteninformationen) aneignen. Sie

geben sich beispielsweise in einer offiziell wirkenden Email als vertrauenswürdige Person mit legitimen Anspruch auf die Informationen aus. Beliebte Ziele sind Nutzer von Online-Banking und Teilnehmer an Online-Auktionen.

Phisher versenden in der Regel Spam-Emails an eine große Anzahl potenzieller Opfer. Diese Emails dirigieren die Empfänger zu einer Webseite, die scheinbar zur offiziellen Online-Bank gehört, tatsächlich aber die Kontoinformationen für die illegalen Absichten des Phishers abfängt.

Eine spezielle Variante stellt das sogenannte „Spear Phishing“ dar, welches lediglich auf eine relativ kleine Gruppe von Benutzern (z.B. Geschäftsführer) abzielt. So lässt sich der Phishing-Versuch noch besser auf eine Zielgruppe zuschneiden.

3. Pharming

Pharming ist eine weiterentwickelte Form von Phishing. Pharmer machen sich das DNS-System zunutze, das dazu dient, Computer in IP-Adressen zu übersetzen.

Hinweis:

Studien belegen, dass mehr als die Hälfte aller Email-Nachrichten als Spam einzustufen ist.

Sie erstellen beispielsweise eine gefälschte Website, die der echten, z.B. einer Bankwebsite, täuschend ähnlich sieht und erfassen die Daten, die arglose Benutzer dort eingeben. Pharming wird auch als „DNS-Poisoning“ bezeichnet.

4. „Distributed Denial-of-Service“

Einige sehr bekannte Websites sind Opfer so genannter Distributed Denial-of-Service-Angriffe (DDoS) geworden. Diese Angriffe werden häufig von Bots (abgeleitet vom Begriff „Robot“) durchgeführt, die gleichzeitig riesige Mengen von Anforderungen an einen bestimmten Computer oder ein Netzwerk senden. Infolge der enormen Belastung bricht das Netzwerk oder das Computersystem zusammen und steht für die eigentlichen Zwecke nicht mehr zur Verfügung. Die angreifenden Computer (Bots) sind häufig Computer mit geöffneten Backdoors, die für solche illegalen Zwecke missbraucht werden. Die Eigentümer dieser Computer sind meist völlig

ahnungslose Mitwirkende bei diesen kriminellen Machenschaften. Die infizierten Computer werden deshalb häufig als „Zombie-Computer“ bezeichnet. Sie sind fertig präpariert und bereit zuzuschlagen, wenn Hacker per Fernsteuerung den richtigen Knopf drücken. Auch Ihr Computer kann für illegale Zwecke missbraucht werden.

5. Keylogger

Keylogger zeichnen die Tastenanschläge eines Benutzers in einer speziellen Anwendung oder auch systemweit auf. Die protokollierten Eingaben werden dann nach bestimmten Datenabschnitten durchsucht, die sich für die Aneignung der Identität des Benutzers, den Diebstahl geistigen Eigentums oder andere betrügerische Aktionen nutzen lassen. Kreditkartennummern, Kennwörter und andere vertrauliche Daten können damit in Erfahrung gebracht werden.

Hinweis:
Norman bietet verschiedene Produkte, die Sicherheit im Internet garantieren. Für Produktinformationen und Demoversionen: www.norman.com.

6. Browser Helper Object (BHO)

BHOs sind Plug-In-Komponenten für Internet Explorer und haben uneingeschränkten Zugriff auf alles, was in der aktuellen Browsersitzung geschieht.

Es „sieht“, welche Seiten angezeigt und wie diese dargestellt werden und kann die Seiten ändern, bevor sie überhaupt für den Benutzer sichtbar sind. Trotz ihres schlechten Rufs werden BHOs häufig für legitime Zwecke, z.B. zum Download, für QuickInfos und zum Entfernen von Popups verwendet.

7. Betrügerische Sicherheitssoftware

Eine besondere Art von Bedrohung bildet Software, die als Sicherheitsprogramm getarnt, tatsächlich aber Malware ist. Der Benutzer wird verleitet, die Software zu installieren und einen (geringen) Betrag zu zahlen, um sein System zu schützen. Dieser Schutz ist in Wahrheit nicht vorhanden. Es gibt zahlreiche Beispiele für diese Methode; besonders gängig sind Programme, die sich als Antispyware- oder Antiviren-Software ausgeben.

*Kreditkarten-
nummern,
Kennwörter und
andere vertrauliche
Daten können
mittels Keylogging
gestohlen werden.*



VERBREITUNGSMECHANISMEN

Früher wurden Computerviren hauptsächlich über Disketten verbreitet. Dieses Speichermedium wird heute kaum noch verwendet. An seine Stelle sind neuere und effektivere Verbreitungstechnologien getreten.

Heutzutage nutzen Malware-Programme zur Verbreitung häufig bekannte Sicherheitslücken in den verschiedenen Anwendungen und Betriebssystemen.

Email-Anlagen

Die Verbreitung von Malware in Form von Email-Anhängen war besonders Ende der 90er Jahre und Anfang dieses Jahrzehnts sehr populär. Bei dieser Methode wurde ein mit Malware infizierter Anhang per Email versendet und der Benutzer veranlasst, den Anhang per Mausclick zu öffnen. Durch das Öffnen des Anhangs wurde das System infiziert.

Für die Verbreitung von Malware per Email werden in vielen Fällen Würmer eingesetzt, die sich ohne Wissen des infizierten Benutzers automatisch durch Emails weiter ausbreiten.

Verbreitung über Netzwerke

Zu den gefährlichsten Malware-Verbreitungsmechanismen für Unternehmen zählen die Programme, die sich über Netzwerke verbreiten und Netzwerkfreigaben befallen. Innerhalb weniger Sekunden kann sich Malware von einem infizierten Computer aus im gesamten Netzwerk ausbreiten.

Da eine Netzwerkausbreitung schnell und effizient ist, gestaltet sich die Beseitigung solcher Malware extrem schwierig.

USB-Sticks

USB-Sticks könnte man als die Nachfolger der Disketten betrachten. Sie sind leicht in der Handhabung und bieten ausreichende Speicherkapazität für viele Anwendungsbereiche, bei denen Daten von einem Computer auf einen anderen übertragen werden sollen.

Leider machen diese Vorteile sie auch zu praktischen Werkzeugen für die Verbreitung von Malware, insbesondere wenn die automatische Ausführung auf dem jeweiligen Computer aktiviert ist. USB-Sticks als kleine tragbare Geräte

zum Anschluss an Computer werden häufig in den Sicherheitsrichtlinien von Unternehmen zur Nutzung neuer Geräte nicht berücksichtigt.

Infizierte Websites

Einer der gängigsten Verbreitungsmechanismen derzeit sind infizierte Websites. Normalerweise erfolgt die Infizierung ohne das Wissen des Website-Eigentümers,

beispielsweise über Sicherheitslücken in Anwendungen des Webservers.

Arglose Internetnutzer werden durch verschiedenste ausgeklügelte Tricks dazu gebracht, die infizierte Website aufzurufen. Infolgedessen wird der Computer des jeweiligen Benutzers ebenfalls infiziert.

Dieses Szenario wird oft als „Drive-by-Infektion“ bezeichnet.

*Sie können im Norman SandBox
Center verdächtige Dateien
kostenlos nach Viren überprüfen.
Testen Sie es unter
<http://sandbox.norman.no/>*

PROAKTIVE UND TRADITIONELLE ANTIVIRENLÖSUNGEN IM VERGLEICH

Der Unterschied zwischen traditionellen signaturbasierten Antivirenlösungen und der neuen proaktiven Antivirentechnologie kann über Leben und Tod Ihrer Computersysteme entscheiden.

Proaktive Lösungen sind in der Lage, neue Bedrohungen zu erkennen, vor denen signaturbasierte Programme

kapitulieren müssen. Virenautoren gehen von Mal zu Mal raffinierter vor und immer neue Virusvarianten überschwemmen das Internet – traditionelle Lösungen bieten keinen ausreichenden Schutz mehr. Der Ruf nach proaktiven Lösungen ist unüberhörbar.

Im Folgenden finden Sie eine kurze Beschreibung der beiden Technologien.

Traditionelle Antivirenlösungen

Die Wirksamkeit signaturbasierter Antivirenlösungen beruht auf der Grundvoraussetzung, dass ein Virus von jemandem entdeckt, als Virus identifiziert und analysiert wird. Danach können die Hersteller von Antivirenprogrammen für geeignete Schutzmaßnahmen sorgen. Erst nach Abschluss dieser vorbereitenden

Schritte kann eine Virussignaturdatei veröffentlicht werden. Im Schnitt vergehen sechs bis 24 Stunden, bis eine aktualisierte Signaturdatei verteilt werden kann.

Hinweis:

Proaktive Antivirenlösungen erkennen neue und unbekannte Viren.

Diese Datei aktualisiert die Antivirenprogramme sämtlicher Kunden, und erst ab diesem Zeitpunkt können die Programme Infektions-

versuche erkennen und verhindern. Ganz offenkundig besteht zwischen der Bekanntgabe des Virusfunds und der Veröffentlichung der aktualisierten Signaturdatei eine kritische Lücke, in der Benutzer dem Risiko ausgesetzt sind, sich mit dem Virus zu infizieren.

Proaktive Lösungen

Eine proaktive Antivirenlösung erkennt neue und unbekannte Viren auch ohne aktualisierte Signaturdateien. Norman bietet seinen Kunden einzigartige proaktive Lösungen.

Norman SandBox®

Norman SandBox® umfasst eine vollständig simulierte Computerumgebung, die von den produktiven Systemen völlig

isoliert ist. Alle eingehenden Dateien werden auf den simulierten Computer (die Sandbox) übertragen. Hier werden die Dateien überwacht. Wird eine verdächtige Aktion entdeckt, stoppt die Norman-Lösung die Datei und blockiert den Zugang zum echten System. Entspricht das tatsächliche Verhalten dem erwarteten Verhalten, wird die Übertragung der Datei auf das produktive System zugelassen. Sogenannte „Day Zero“-Angriffe stellen eine zunehmende Bedrohung dar. Bei diesen Angriffen wird an dem Tag, an dem eine Software-Schwachstelle öffentlich bekannt gegeben wird, ein Schadprogramm in Umlauf gebracht, dass diese Schwachstelle ausnutzt. Nur proaktive Lösungen können es mit dieser Art von Bedrohung aufnehmen.

Norman DNA Matching

Man kann sich den Computercode und die Anweisungen eines Programms wie einen Abschnitt eines DNA-Profiles vorstellen. Norman nutzt diesen Ansatz, um Malware zu erkennen und neue Malware aufzuhalten, die durch herkömmliche Methoden (durch Virensignaturen) noch

nicht registriert wurde. Falls neue Malware wie eine Mutation bereits bekannter Malware erscheint (d.h. es kommt ähnlicher oder identischer Schadcode zum Einsatz), lässt sich daraus schließen, dass es sich höchstwahrscheinlich um ein Malware-Programm derselben Familie handelt.

Wenn ein neues, unbekanntes Programm auftaucht und verbreitet wird, nutzt Norman die DNA Matching-Technologie, um festzustellen, ob die Software eventuell verdächtige oder schädliche Eigenschaften aufweist oder doch ganz unversehrlich ist. Wenn ein nicht unerheblicher Teil der DNA des neuen Programms als Schadcode eingestuft wird, ist davon auszugehen, dass es sich um Malware handelt.

Norman Exploit Detection

Dabei handelt es sich um eine Technologie zur Erkennung von Malware, die Sicherheitslücken in weit verbreiteten Dokumententypen wie OLE2 (Office), MDB (Access), WMF (Windows Media-Datei), JPEG (Bilder), RIFF (Windows Media-Metaformat) und SWF (Flash) nutzt.

Deutschland/Österreich

Norman Data Defense
Systems GmbH
Gladbecker Straße 3
40472 Düsseldorf

Fon: +49-211 / 586 99-0
Email: info@norman.de
www.norman.de
www.virenschutz.com

Norman Data Defense
Systems GmbH
Ludwigstraße 47
85399 Hallbergmoos

Fon: +49-811 / 541 84-0
Email: info@norman.de
www.norman.de
www.virenschutz.com

Schweiz

Norman Data Defense
Systems AG
Münchensteinerstrasse 43
4052 Basel

Fon: +41-61 317 25 25
Email: norman@norman.ch
www.norman.ch

Norman ASA übernimmt keinerlei Haftung für jegliche Art von Verlusten oder Schäden, die durch die Verwendung der Dokumentation oder durch darin enthaltene Fehler oder Mängel entstehen, einschließlich, aber nicht beschränkt auf Ertragsverluste.

Die Informationen in diesem Dokument können ohne Ankündigung geändert werden. Kein Teil dieser Dokumentation darf zu irgendeinem anderen Zweck als der persönlichen Verwendung durch den Käufer ohne ausdrückliche schriftliche Genehmigung von Norman ASA in irgendeiner Form oder mit irgendwelchen Mitteln, sei es elektronisch oder mechanisch, einschließlich der Erstellung von Fotokopien oder Aufzeichnungen oder der Verwendung von Systemen zur Datenspeicherung und -abrufung, reproduziert oder übertragen werden.

Das Norman-Logo ist eine eingetragene Marke von Norman ASA.

In dieser Dokumentation erwähnte Produktnamen sind entweder Marken oder eingetragene Marken der jeweiligen Eigentümer. Sie werden lediglich zu Identifizierungszwecken angegeben.

Copyright © 2010 Norman ASA.

Alle Rechte vorbehalten.

Norman ASA ist eines der weltweit führenden Unternehmen im Bereich Datensicherheit, Onlineschutz und Analyseanwendungen. Dank der SandBox®-Technologie bietet Norman im Gegensatz zu den Konkurrenten seinen Kunden einzigartigen und proaktiven Schutz.



Neben der stetigen Weiterentwicklung der proaktiven Antiviren-Technologie arbeitet Norman eng mit anderen Unternehmen zusammen, um den Kunden eine umfangreiche Palette an Datensicherheits-Lösungen anbieten zu können. Norman wurde im Jahre 1984 gegründet und hat seinen Hauptsitz in Norwegen. Die wichtigsten Märkte des Unternehmens bilden Europa, Großbritannien und die USA.

NORMAN®