Schreckxikon

Computer- und Datensicherheit von A bis Z

SOPHOS

Computer- und Datensicherheit von A bis Z

Ganz egal, ob Sie in der IT-Branche arbeiten, einfach nur einen Computer für die Arbeit nutzen oder in Ihrer Freizeit im Internet surfen: Dieser Leitfaden ist für alle da. Wir erklären Ihnen in einfachen, leicht verständlichen Worten, welchen Bedrohungen Ihr Computer und Ihre Daten ausgesetzt sind.

Sophos hält IT-Managern den Rücken frei, damit diese sich um wichtigere Unternehmensbelange kümmern können. Wir bieten Sicherheitslösungen für Computer (Endpoint), Verschlüsselung, E-Mail, Internet und Netzwerksicherheit. Lösungen, die einfach bereitzustellen, zu verwalten und zu benutzen sind. Über 100 Mio. Benutzer vertrauen bereits auf unsere Schutzlösungen gegen komplexe Bedrohungen und Analysten zählen uns zu den Marktführen.

Unser Unternehmen blickt auf mehr als zwei Jahrzehnte Erfahrung zurück. Dank unseres globalen Netzwerks aus Analysecentern können wir blitzschnell auf neue Bedrohungen reagieren. Dank seines einzigartigen Know-hows verzeichnet Sophos den branchenweit höchsten Grad an Kundenzufriedenheit. Unsere Hauptsitze befinden sich in Boston, USA, und Oxford, UK.

Inhalt

Einleitung

Über Computerviren weiß heutzutage jeder Bescheid. Zumindest glauben das viele.

Der erste Computervirus trat vor 30 Jahren auf: Wurde ein infizierter Computer zum 50. Mal hochgefahren, zeigte „Elk Cloner" ein kurzes Gedicht an. Seit dieser Zeit haben Cyberkriminelle Millionen von Viren und eine Unmenge weitere Malware entwickelt: E-Mail-Viren, Trojaner, Internetwürmer, Spyware und Keylogger. Einige davon haben sich weltweit verbreitet und Schlagzeilen gemacht.

Oft hört und liest man, dass Viren Dateien löschen oder den Bildschirm mit Nonsense-Nachrichten überfluten. Die Allgemeinheit bringt Malware immer noch mit dummen Streichen oder mit Sabotage in Verbindung. In den frühen 1990ern löste der Michelangelo-Virus sogar eine weltweite Panik aus. In den 2000ern wurden Millionen von Computern mit dem Sobig-F-Virus infiziert und so manipuliert, dass sie zu einem bestimmten Zeitpunkt unbekannte Programme aus dem Internet herunterluden. Antiviren-Unternehmen mussten Internetdienstanbieter dazu überreden, ihre Server abzuschalten, um diese Bedrohung abzuwenden. Hollywood-Filme wie „Independence Day" verstärkten die Vorstellung, dass Virenangriffe sich vor allem als blinkende Bildschirme und Alarm-Meldungen zeigen.

Die Realität sieht heute ganz anders. Die aktuellen Bedrohungen sind nach wie vor sehr real. Doch die Angriffe spielen sich oft unbemerkt im Hintergrund ab und verlaufen zielgerichtet. Sie dienen nicht mehr dazu, Chaos zu verbreiten; heute geht es vor allem ums Geldverdienen.

Es ist heutzutage eher unwahrscheinlich, dass Malware Ihre Festplatte zerstört, Dateien beschädigt oder eine Nachricht anzeigt. Der Cyber-Vandalismus von einst hat lukrativeren Angriffen Platz gemacht. Ein moderner Virus verschlüsselt zum Beispiel all Ihre Dateien und verlangt ein Lösegeld von Ihnen. Oder ein Hacker erpresst ein großes Unternehmen durch die Androhung eines Denial-of-Service-Angriffs, der die Kunden daran hindern würde, die Unternehmenswebseite zu nutzen.

Üblicherweise richten Viren heute keinen direkten oder offensichtlichen Schaden mehr an, sie machen sich im Gegenteil kaum noch bemerkbar. Stattdessen installiert zum Beispiel ein Virus in aller Stille einen Keylogger. Dieser wartet darauf, dass das Opfer eine Online-Banking-Webseite öffnet, zeichnet dann die Kontodetails und das Passwort des Benutzers auf und leitet diese Informationen über das Internet an einen Hacker

weiter. Der Hacker stiehlt so die Identität seines Opfers und nutzt die entwendeten Daten, um Kreditkarten zu fälschen oder Bankkonten zu plündern. Und der Betroffene bemerkt oft nicht einmal, dass sein Computer infiziert ist. Hat der Virus seinen Zweck erfüllt, zerstört er sich oftmals selbst, um seine Spuren dauerhaft zu verwischen.

Ein weiterer Trend: Malware übernimmt Computer und verwandelt sie in ferngesteuerte Zombies. Ohne Ihr Wissen versendet Ihr Computer dann millionenfach Spamnachrichten – für Cyberkriminelle ein einträgliches Geschäft. Oder die Schadsoftware startet von Ihrem Computer Malware-Angriffe auf andere arglose Computerbenutzer.

Nachdem soziale Netzwerke wie Facebook und Twitter immer beliebter werden, nutzen Hacker und Cyberkriminelle auch diese Wege, um Computer zu infizieren oder Identitäten zu stehlen.

Hacker richten Ihre Angriffe aber oft nicht mehr gegen eine große Anzahl potenzieller Opfer. Solche Massenangriffe erregen nämlich unerwünschtes Aufsehen und Antiviren-Unternehmen können weitverbreitete Malware in der Regel schnell neutralisieren. Groß angelegte Angriffe bringen Hackern zudem oft mehr Daten ein, als sie verarbeiten können. Daher gehen Angreifer heute immer zielgerichteter vor.

Spearphishing ist ein Beispiel dafür. Ursprünglich wurden beim Phishing Massen-E-Mails versendet, die scheinbar von Banken kamen und in denen die Kunden aufgefordert wurden, vertrauliche Daten neu einzugeben, die sich dadurch stehlen ließen. Beim Spearphishing hingegen erfolgt der Angriff auf eine geringe Anzahl an Personen, die meist im selben Unternehmen arbeiten. Sie erhalten eine E-Mail, die scheinbar von einem Kollegen aus einer vertrauenswürdigen Abteilung kommt und in der sie nach Passwörtern gefragt werden. Das Prinzip ist dasselbe wie beim Phishing, doch der Angriff hat mehr Chancen auf Erfolg, weil das Opfer die E-Mail für eine interne Nachricht hält und keinen Hinterhalt vermutet.

Klammheimlich und gezielt auf einen kleinen Personenkreis gerichtet – das sind die Sicherheitsbedrohungen von heute.

Was aber bringt die Zukunft? Die Entwicklung kommender Sicherheitsbedrohungen vorherzusagen ist beinahe unmöglich. In der Vergangenheit hieß es, es würde niemals mehr als einige Hundert Viren geben, und Microsoft- Chef Bill Gates erklärte einst, Spam würde im Jahr 2006 kein Problem mehr darstellen. Es ist schwer zu sagen, wie die Bedrohungen in Zukunft aussehen und wie schwerwiegend sie sein werden. Klar ist hingegen, dass Hacker und Kriminelle immer versuchen werden, Daten zu stehlen und zu missbrauchen – sofern sie daraus finanziellen Nutzen ziehen können.


AZ

Bedrohungen von A bis Z

Adware

Adware ist Software, die Werbung auf Ihrem Computer einblendet.

Adware wird auch als werbeunterstützte oder werbefinanzierte Software bezeichnet. Sie zeigt Werbebanner oder Pop-up-Fenster auf dem Computer an, wenn Sie eine Anwendung benutzen oder eine Webseite besuchen. Das ist nicht automatisch schlecht. Solche Werbung kann die Entwicklung nützlicher Software finanzieren, die dann kostenlos zur Verfügung steht. Viele Android-Anwendungen werden zum Beispiel durch Adware gesponsert.

In folgenden Fällen wird Adware jedoch zum Problem:

- Wenn sie sich von selbst und ohne Ihre Zustimmung auf Ihrem Computer installiert.
- Wenn sie sich nicht nur in der Anwendung installiert, mit der sie geliefert wurde, sondern ausufernd in anderen Anwendungen Werbung anzeigt.
- Wenn sie Ihren Webbrowser übernimmt, um noch mehr Werbung anzuzeigen (siehe **Browser-Hijacker**).
- Wenn sie ohne Ihre Zustimmung Daten zu Ihrem Surfverhalten sammelt und diese über das Internet an andere weiterleitet (siehe **Spyware**).
- Wenn sie so gestaltet ist, dass man sie nur schwer wieder deinstallieren kann.

Adware kann Ihren PC langsamer machen. Sie belastet durch das Herunterladen von Werbung unter Umständen auch Ihre Internetverbindung. Programmierfehler in Adware können dazu führen, dass der Computer instabil arbeitet.

Werbe-Pop-ups können ablenken und Zeit kosten, wenn diese erst geschlossen werden müssen, bevor Sie an Ihrem Computer weiterarbeiten können.

Einige Virenschutzprogramme erkennen Adware und melden sie als potenziell unerwünschte Anwendung: Sie können das Adware-Programm dann entweder autorisieren oder von Ihrem Computer entfernen. Einige Programme haben sich sogar auf die Adware-Erkennung spezialisiert.


TWO
FOR ON
BUY
ME

Anonymisierender Proxyserver

Anonymisierende Proxyserver ermöglichen dem Benutzer, seine Surfaktivität im Internet zu verbergen. Er kann damit Websicherheitsfilter umgehen und zum Beispiel mit einem Firmencomputer auf gesperrte Seiten zuzugreifen.

Anonymisierende Proxyserver sind für Unternehmen ein ernstes Risiko:

- Sicherheit: Der anonymisierende Proxyserver umgeht Maßnahmen für mehr Sicherheit im Web und ermöglicht Benutzern unter Umständen, auf infizierte Webseiten zuzugreifen.
- Haftung: Unternehmen können rechtlich haften, wenn ihre Computer zum Anzeigen pornografischer oder extremistischer Materialien zweckentfremdet werden oder illegales Verhalten fördern. Auch drohen Konsequenzen, wenn die Benutzer durch illegale MP3-, Film- und Software-Downloads die Rechte Dritter verletzen.
- Produktivität: Anonymisierende Proxyserver ermöglichen den Benutzern den Zugriff auf Webseiten, die zwar keine Gefahr darstellen, die aber ausschließlich rein privaten Zwecken dienen.

Advanced Persistent Threat (APT)

Der Advanced Persistent Threat ist ein gezielter Angriff durch Personen, die sowohl über die Zeit als auch die Mittel verfügen, über einen langen Zeitraum hinweg die Infiltration eines Netzwerks zu planen und umzusetzen.

Diese Angreifer dringen zunächst in das Netzwerk ein und steuern danach ihren Angriff ganz bewusst. Meist suchen sie nicht einfache Finanzdaten, sondern fundierte wirtschaftliche oder andere geschützte und möglichst interessante Informationen. APTs sind dauerhafte Bedrohungen, die oft einige Zeit im Netzwerk verbleiben, ehe sie Zugriff auf die gewünschten Daten erhalten und diese dann stehlen. APTs dürfen nicht mit gängigen Botnets verwechselt werden. Über Botnets laufen meist wahllose Angriffe ab, die einfach eine Gelegenheit nutzen und auf beliebige Opfer abzielen. APTs hingegen suchen zielstrebig nach ganz spezifischen Informationen.

AutoRun-Wurm

AutoRun-Würmer sind Schadprogramme, die sich die AutoRun-Funktion von Windows zunutze machen. Sie werden automatisch gestartet, wenn etwas an einen Computer angeschlossen wird.

AutoRun-Würmer werden normalerweise über USB-Datenträger verbreitet und infizieren Computer sofort nach dem Anschließen oder Einstecken. Bei AutoPlay handelt es sich um eine ähnliche Funktion wie AutoRun. Auf Wechselmedien fordert sie den Benutzer auf, Musik über den Standard- Mediaplayer zu hören oder im Windows-Explorer ein Laufwerk zu öffnen.

Die AutoPlay-Funktion wurde von Angreifern in ähnlicher Weise ausgenutzt, am erfolgreichsten mit dem Conficker-Wurm.

Bei gepatchten und neueren Betriebssystemen wurde die AutoRun-Funktion von Microsoft deaktiviert. Aus diesem Grund sollten AutoRun-Würmer in Zukunft eine geringere Bedrohung darstellen.

Backdoor-Trojaner

Mit Hilfe eines Backdoor-Trojaners kann ein Angreifer per Internet den Computer eines Benutzer übernehmen – ohne dessen Zustimmung.

Backdoor-Trojaner geben sich meist als legitime Software aus. Das soll den Benutzer dazu verleiten, die Software und damit den Trojaner zu starten. Immer häufiger gelangen solche Trojaner schon dann auf einen Computer, wenn der Benutzer einem Link in einer Spam-E-Mail folgt oder eine infizierte Webseite besucht.

Nachdem der Trojaner ausgeführt wird, fügt er sich selbst der Startroutine des Computers hinzu und kann dann den Computer überwachen. Geht der Computer online, kann die Person, die hinter dem Trojaner steckt, mit seiner Hilfe zahlreiche Aktionen durchführen. Er kann zum Beispiel Programme auf dem infizierten Computer ausführen, auf persönliche Dateien zugreifen, Dateien ändern und hochladen, die Tasteneingaben des Benutzers speichern oder Spam-E-Mails versenden.

Zu den bekannten Backdoor-Trojanern gehören Netbus, OptixPro, Subseven, BackOrifice und in jüngerer Zeit auch Zbot und ZeuS.

Um eine Infizierung mit Backdoor-Trojanern zu vermeiden, sollten Sie Ihre Computer mit den aktuellen Patches auf dem neuesten Stand halten, um Sicherheitslücken im Betriebssystem zu schließen. Installieren Sie außerdem Spamfilter und eine Virenschutzsoftware. Zudem empfiehlt sich eine Firewall: Sie hindert Trojaner daran, auf das Internet zuzugreifen und mit dem Hacker in Kontakt zu treten.

Bootsektor-Malware

Bootsektor-Malware verbreitet sich, indem sie das spezielle Startprogramm ändert, das den Computer hochfährt.

Wenn Sie einen Computer einschalten, sucht die Hardware automatisch im Bootsektor der Festplatte, der Diskette oder der CD nach einem speziellen Startprogramm. Dieses Programm lädt dann den Rest des Betriebssystems in den Speicher und startet so den Computer.

Bootsektor-Malware ersetzt den ursprünglichen Bootsektor mit einer abgeänderten Version (und verbirgt in der Regel das Original an einer anderen Stelle auf der Festplatte). Beim nächsten Hochfahren verwendet das System den infizierten Bootsektor und aktiviert so die Malware.

Malware verbreitet sich über Bootsektoren, weil sie auf diese Weise noch vor dem Betriebssystem geladen wird. Auf diese Weise kann die Malware ihre Anwesenheit besser verbergen (zum Beispiel TDL-Rootkit).

Botnet

Ein Botnet ist ein Verbund infizierter Computer, die von einem Hacker per Fernsteuerung kontrolliert werden.

Wenn ein Computer mit einem Bot infiziert ist, kann der Hacker das Gerät per Fernsteuerung über das Internet kontrollieren. Von diesem Zeitpunkt an folgt der Computer wie ein Zombie nur noch den Anweisungen des Hackers, während der Benutzer nicht das Geringste davon merkt. Die Gesamtheit der so kontrollierten Computer wird als Botnet bezeichnet.

Der Hacker kann den Zugriff auf das Botnet gegen Bezahlung für andere freigeben, so dass diese es für ihre kriminellen Zwecke nutzen können.

Ein Spammer kann ein Botnet zum Beispiel zum Versenden von Spam-E-Mails einsetzen. Bis zu 99 Prozent des gesamten Spam-Aufkommens werden auf diesem Weg erzeugt. Die Spammer schützen sich auf diese Weise auch vor Entdeckung und verhindern, dass ihre eigenen Server auf einer schwarzen Liste landen. Kosten sparen sie auch, denn für den Internetzugriff bezahlen ja die vielen Computerbesitzer.

Hacker nutzen Computer-Zombies auch für verteilte Denial-of-Service-Angriffe (DDoS). Sie bringen Tausende Computer dazu, gleichzeitig auf dieselbe Webseite zuzugreifen, damit der Webserver die unzähligen Aufrufe nicht mehr verarbeiten kann. Das hindert andere Besucher am Zugriff auf die Webseite. (Siehe **Zombie, Denial-of-Service-Angriff, Spam, Backdoor-Trojaner, Command and Control Center**)

Browser-Hijacker

Browser-Hijacker ändern ohne Ihre Zustimmung die Standard-Startseite und die Suchmaschine Ihres Webbrowsers.

Wurde Ihr Computer von einem Hijacker übernommen, lässt sich die Startseite Ihres Browsers unter Umständen nicht mehr ändern. Einige Hijacker bearbeiten dazu die Windows-Registry, so dass die Hijacking-Einstellungen bei jedem Neustart des Computers wiederhergestellt werden. Andere entfernen Optionen aus dem Browser-Menü „Extras“, so dass sich die Startseite mangels Zugriff auf die Einstellungen nicht zurücksetzen lässt.

Mit Browser-Hijacking sollen Werbeeinnahmen gesteigert werden, zum Beispiel bei der Verwendung von Blackhat-SEO. Damit werden die Richtlinien der Suchmaschinenoptimierung absichtlich umgangen und das Ranking einer Webseite in Suchergebnissen künstlich erhöht.

Browser-Hijacker können sehr hartnäckig sein und sehr heimtückisch agieren. Die Angreifer setzen auf eine Methode namens Clickjacking (auch unter der Bezeichnung „UI Redressing“ bekannt), bei der sie mehrere durchsichtige oder undurchsichtige Ebenen auf einer Webseite einfügen. Mit dieser Technik kann ein Benutzer dazu gebracht werden, auf einer Webseite auf Schaltflächen oder Links zu klicken, die er gar nicht anklicken wollte. Der Angreifer übernimmt die Klicks, die für eine bestimmte Seite vorgesehen waren, und leitet sie auf eine andere Seite um, die mit hoher Wahrscheinlichkeit zu einer anderen Anwendung, einer anderen Domäne (oder beidem) gehört.

Das bedroht zwar nicht direkt Ihren Computer, doch es stört Sie beim Surfen im Web.

Brute-Force-Angriff

Bei einem Brute-Force-Angriff probieren Angreifer eine große Anzahl an möglichen Stichwort- oder Passwort-Kombinationen durch, um unberechtigt Zugriff auf ein System oder eine Datei zu erlangen.

Brute-Force-Angriffe werden oft eingesetzt, um an passwortgeschützte, verschlüsselte Daten zu gelangen. Die Hacker bedienen sich dabei spezieller Computerprogramme, die automatisch eine immense Anzahl von Passwörtern durchprobieren, um eine Nachricht zu entschlüsseln oder auf ein System zugreifen zu können.

Um Brute-Force-Angriffe zu verhindern, müssen Sie Ihre Passwörter so sicher wie möglich gestalten. (Siehe **So wählen Sie sichere Passwörter**)

Buffer-/Pufferüberlauf

Ein Pufferüberlauf tritt ein, wenn ein Programm mit zu vielen Daten gefüttert wird. Dabei werden andere Teile des Computerspeichers überschrieben, was zu Fehlern oder Abstürzen führt.

Einige Programme sind nicht darauf ausgelegt, mehr Daten zu erhalten, als sie verarbeiten können. Wenn das passiert, geht ihnen der Speicherplatz aus und sie überschreiben versehentlich Teile des Speichers, die das Betriebssystem eigentlich für andere Zwecke vorgesehen hat. Pufferüberlauf-Angriffe nutzen diese Schwäche aus und versuchen gezielt, Programme mit Daten zu überfüttern.

Entgegen der verbreiteten Meinung kommt es nicht nur bei Windows-Diensten oder -Kernprogrammen zu Pufferüberläufen. Sie können in jeder Anwendung auftreten.

Ein möglicher Schutz ist die Buffer Overflow Protection (BOP). Sie sucht in Programmen nach Code, der absichtlich einen Pufferüberlauf erzeugen will, um auf diese Weise eine Sicherheitslücke auszunutzen. (Siehe **Exploit, Drive-by-Download**)

Chain letter/Kettenbrief

Ein elektronischer Kettenbrief ist eine E-Mail, die Sie dringlich auffordert, Kopien davon an andere Personen zu schicken.

Wie Viren-Hoaxes sind auch Kettenbriefe auf den Benutzer angewiesen, um sich verbreiten zu können. Folgende Typen lassen sich unterscheiden:

- Falschmeldungen (Hoaxes) über Terroristenangriffe, Betrügereien mit teuren Bezahlrufnummern, Diebstähle an Geldautomaten usw.
- Falsche Behauptungen, z.B. dass Ihnen Unternehmen kostenlose Flüge, Mobiltelefone oder sogar Bargeld anbieten, wenn Sie die E-Mail weiterleiten
- Nachrichten, die angeblich von Organisationen wie Geheimdiensten oder der Polizei stammen und die vor gefährlichen Kriminellen in Ihrer Region warnen
- Petitionen, die vor geraumer Zeit vielleicht sogar mal echt waren, aber schon lange abgelaufen sind
- Witze und Streiche (zum Beispiel die Behauptung, dass das Internet am 1. April zu Wartungszwecken abgeschaltet werden müsse)
- Postings bei sozialen Netzwerken wie Facebook, in denen Benutzer aufgefordert werden, Links zu teilen: Etwa das Bild eines kranken Kindes, das eine Herztransplantation benötigt, oder betrügerische Panikmache, dass Kindern Drogen mit Erdbeergeschmack angeboten werden

Kettenbriefe bedrohen nicht Ihre Sicherheit, aber sie verschwenden Zeit, verbreiten falsche Informationen und lenken die Benutzer von wichtigen E-Mails ab.

Sie erhöhen unnötig das E-Mail-Aufkommen und machen E-Mail-Server langsamer. Manchmal wird in Kettenbriefen aufgefordert, E-Mails an bestimmte Adressen zu senden, so dass diese mit unerwünschten Nachrichten überflutet werden.

Die Lösung des Kettenbriefproblems ist ganz einfach: Leiten Sie diese Nachrichten nicht weiter. (Siehe **Hoax**)

Command and Control Center

Ein Command and Control Center (C&C) ist ein Computer, der ein Botnet (also ein Netzwerk aus manipulierten Zombie-Computern) steuert. Einige Botnets weisen verteilte Command-and-Control-Systeme auf, was sie widerstandsfähiger macht.

Vom Command and Control Center aus können Hacker eine Vielzahl an Computern dazu bringen, die von ihnen gewünschten Aktivitäten auszuführen.

Command and Control Center werden oft für verteilte Denial-of-Service-Angriffe eingesetzt, da sie eine riesige Anzahl an Computern so steuern können, dass diese zur selben Zeit dieselbe Aktion ausführen. (Siehe **Botnet, Zombie, Denial-of-Service-Angriff**)

Cookie

Bei Cookies handelt es sich um Dateien, die auf Ihrem Computer abgelegt werden, damit Webseiten Informationen speichern können.

Jede Webseite kann beim Aufruf auf Ihrem Computer eine Datei ablegen, die als Cookie bezeichnet wird. In ihm speichert die Webseite einige Informationen und kann auf diese Weise Ihre Besuche nachverfolgen. Cookies bedrohen zwar Ihre Privatsphäre, nicht aber Ihre Daten.

Cookies wurden ursprünglich als nützliche Hilfe entwickelt. Wenn Sie zum Beispiel beim Besuch einer Webseite persönliche Informationen eingeben, kann ein Cookie diese Daten speichern, damit Sie diese beim nächsten Mal nicht erneut eingeben müssen. Cookies haben auch Vorteile für Webmaster, da sie zum Beispiel über die meistbesuchten Webseiten informieren, was bei der Umgestaltung von Internetauftritten helfen kann. Technisch gesehen sind Cookies kleine Textdateien, die Ihren Daten nicht schaden, jedoch Ihre Privatsphäre beeinträchtigen können.

Cookies werden ohne Ihr Wissen oder Ihre Zustimmung auf Ihrem Computer gespeichert. Sie enthalten Informationen über Sie in einer Form, auf die Sie nicht leicht zugreifen können. Wenn Sie dieselbe Webseite erneut besuchen, werden diese Daten an den Webserver zurückgegeben – erneut ohne Ihre Zustimmung.

Die Webseiten erstellen auf diese Weise nach und nach ein Profil Ihres Surfverhaltens und Ihrer Interessen. Diese Informationen können verkauft oder für andere Webseiten freigegeben werden. Werbebotschaften stimmen sich so auf Ihre Interessen ab oder bilden zusammengehörende Anzeigen auf verschiedenen Webseiten. Auch lässt sich damit prüfen, wie oft Sie eine Anzeige gesehen haben.

Wenn Sie lieber anonym bleiben möchten, können Sie Cookies in den Sicherheitseinstellungen Ihres Browsers deaktivieren.


Cookies

Datenlecks

Durch Datenlecks fließen Informationen auf unerwünschte Weise aus einem Unternehmen hinaus. Das kann absichtlich (Datendiebstahl) oder unabsichtlich (Datenverlust) geschehen.

Der Schutz vor Datenlecks steht bei allen Unternehmen ganz oben auf der Prioritätenliste, dennoch machen Skandale über Verletzungen der Datensicherheit häufig Schlagzeilen. Denn viele Unternehmen und Behörden schützen ihre Informationen nur unzureichend. Sie setzen damit die Vertraulichkeit personenbezogener Daten von Mitarbeitern, Kunden und der Öffentlichkeit aufs Spiel.

Für Benutzer ist der Umgang mit Daten alltäglich geworden, sie geben diese weiter und machen sich dabei zu wenig Gedanken über Verhaltensregeln und Vertraulichkeitsanforderungen.

Datenlecks können mit einer Reihe von Techniken verhindert werden. Hierzu zählen unter anderem Virenschutzsoftware, Verschlüsselung, Firewalls, Zugriffskontrolle, schriftlich festgehaltene Richtlinien und verbesserte Mitarbeiterschulungen. (Siehe **Datenverlust, Datendiebstahl, So sichern Sie Ihre Daten**)

Datendiebstahl

Von Datendiebstahl spricht man, wenn Daten nicht versehentlich verloren gehen, sondern absichtlich gestohlen werden.

Ein Datendiebstahl kann sowohl innerhalb eines Unternehmens (zum Beispiel von einem verärgerten Mitarbeiter) als auch durch Kriminelle außerhalb des Unternehmens begangen werden.

Im Jahr 2012 hackten sich Kriminelle in das System des belgischen Kreditanbieters Dexia. Sie forderten 150.000 EUR, andernfalls würden sie vertrauliche Daten veröffentlichen. Ein weiteres Beispiel sind die Mitarbeiter eines Call-Centers mit Sitz in Indien, die private Daten von fast 500.000 britischen Bürgern einschließlich Name, Adresse und Kreditkartennummern verkauft haben.

Weitere Datendiebstähle aus der jüngsten Zeit zählen zu den größten der Geschichte:

- 2007: Der Einzelhandelskonzern TJX Companies gibt bekannt, dass ihm 45,6 Mio. Debit- und Kreditkartennummern gestohlen wurden. Der Schaden betrug knapp 210 Mio. EUR.
- 2009: Heartland Payment Systems gibt den Diebstahl von 100 Mio. Datensätzen bekannt, was den Kreditkarten-Abrechnungsdienstleister fast 115 Mio. EUR kostete.
- 2011: Beim E-Mail-Marketing-Unternehmen Epsilon werden Millionen von Namen und E-Mail-Adressen aus Kundendatenbanken von Best Buy, Marks & Spencer und Chase Bank offengelegt. Die Kosten für anfängliche Kosteneingrenzung und Korrekturmaßnahmen werden auf über 180 Mio. EUR geschätzt, können jedoch auch auf bis zu 3,3 Mrd. EUR steigen.
- 2011: Die Sony Corporation erleidet Datenverluste, die ein Risiko für 100 Mio. Kundenkonten darstellen. Sie kosten das Unternehmen bis zu 1,6 Mrd. EUR.
- 2011: Die Server von Global Payments, einem Abrechnungsdienstleister von Visa, werden gehackt und die Daten von 7 Mio. Karteninhabern offengelegt.

Für den Zugriff auf Computer und den Datendiebstahl setzen Kriminelle oft Malware ein. Typisch ist, dass ein Trojaner eine Keylogging-Software installiert. Sie zeichnet auf, was der Benutzer eintippt, auch Benutzernamen und Passwörter, um damit auf das Bankkonto des Benutzers zuzugreifen.

Datendiebstahl liegt auch dann vor, wenn Geräte oder Medien, die Daten speichern (wie zum Beispiel Laptops oder USB-Laufwerke), gestohlen werden. (Siehe **Datenlecks, Datenverlust, So sichern Sie Ihre Daten**)

Datenverlust

Ein Datenverlust liegt vor, wenn Daten versehentlich (und nicht durch einen Diebstahl) an den falschen Ort geraten oder abhanden kommen.

Ein Datenverlust tritt oftmals auf, wenn das Gerät oder Medium, auf dem die Daten gespeichert sind, verloren geht. Gerne und leicht verschwinden Laptops, Tablet-PCs, CD-ROMs, Mobiltelefone oder USB-Sticks. In diesen Fällen besteht das Risiko, dass die Daten in falsche Hände geraten, wenn keine wirksame Datensicherheitstechnik zum Einsatz kommt. (Siehe **Datenlecks, Datendiebstahl, So sichern Sie Ihre Daten**)

Denial-of-Service-Angriff

Ein DoS-Angriff (Denial-of-Service) hindert die Benutzer daran, auf einen Computer zuzugreifen oder eine Webseite aufzurufen.

Bei einem DoS-Angriff versucht ein Hacker einen Dienst zu überlasten oder zu beenden, so dass legitime Benutzer nicht mehr darauf zugreifen können. Typische DoS-Angriffe richten sich gegen Webserver und sollen dafür sorgen, dass diese unerreichbar sind. Es werden zwar keine Daten gestohlen oder beschädigt, doch schon die Dienstunterbrechung selbst kann für das betroffene Unternehmen kostspielig sein.

Der gängigste Typ des DoS-Angriffs besteht darin, mehr Daten an einen Computer zu senden als dieser verarbeiten kann. Für DoS-Angriffe werden verschiedenste Methoden eingesetzt, die einfachste und am weitesten verbreitete ist jedoch die, einen Webserver über ein Botnet mit Anfragen zu überfluten. Dies wird als verteilter Denial-of-Service-Angriff (Distributed DoS, DDoS) bezeichnet. (Siehe **Backdoor-Trojaner, Zombie**)

DNS-Hijacking

Das Domain Name System (DNS) ist das Telefonbuch des Internets. Damit können Computer Namen von Webseiten wie www.sophos.com in IP-Adressen übersetzen und so miteinander kommunizieren.

Ein DNS-Hijacking-Angriff ändert die Computereinstellungen so, dass der Computer das DNS entweder ignoriert oder seine Informationen über einen böswillig gehackten DNS-Server bezieht. Die Angreifer können dann falsche IP-Adressen an den Computer senden und auf diese Weise seine Kommunikation umleiten. DNS-Hijacking wird in der Regel eingesetzt, um Benutzer auf gefälschte Anmeldeseiten für Banken und andere Online-Dienste umzuleiten und dort ihre Anmeldedaten zu stehlen. Mit einer ähnlichen Methode lassen sich Sicherheitswebseiten auf nicht vorhandene Server umleiten, so dass die betroffenen Benutzer ihre Sicherheitssoftware nicht aktualisieren können.

Dokument-Malware

Dokument-Malware nutzt eingebettete Skripts oder Makros in Dokument-Dateien, um sich zu verbreiten oder Schaden anzurichten.

Makro-Viren, die Microsoft Office-Dokumente infizieren, traten erstmals Mitte der 1990er Jahre auf und mauserten sich rasch zur gefährlichsten Bedrohung ihrer Zeit. In den letzten Jahren sind schädliche Inhalte, die spezielle Sicherheitslücken ausnützen, weitaus gängiger geworden als diese älteren Makro-Viren. Durch das Einbetten schädlicher Inhalte in Dokumente nutzen Hacker Sicherheitslücken in jenen Programmen aus, mit denen Sie verschiedenste Dokumente öffnen.
(Siehe **Exploit**)

Drive-by-Download

Beim Drive-by-Download wird ein Computer mit Malware infiziert, sobald der Benutzer eine schädliche Webseite aufruft.

Drive-by-Downloads laufen ohne Wissen oder Zutun des Benutzers ab. Schon das Aufrufen einer infizierten Webseite reicht aus, um die Malware auf seinen Computer zu laden und zu starten. Die Malware nutzt dann Sicherheitslücken im Browser (oder in den Browser-Erweiterungen) des Benutzers, um den Computer zu infizieren.

Jeden Tag manipulieren Hacker völlig legitime Webseiten und bauen schädlichen Code in ihre Seiten ein. Ruft ein Benutzer dann eine solche legitime (aber infizierte) Webseite auf, lädt sein Browser den Schadcode und startet so den Drive-by-Angriff. Auf diese Weise können Hacker Computer infizieren, ohne den Benutzer dazu erst auf eine bestimmte Webseite locken zu müssen.

Um sich vor Drive-by-Downloads zu schützen, installieren Sie eine Endpoint-Sicherheitssoftware gemeinsam mit Webschutzfiltern. (Siehe **Exploit**)

E-Mail-Malware

Bei E-Mail-Malware handelt es sich um Malware, die per E-Mail verbreitet wird.

In der Vergangenheit wurden einige der erfolgreichsten Virenarten (zum Beispiel Netsky oder SoBig) in Dateianhängen von E-Mails verbreitet. Wenn Empfänger den Anhang per Doppelklick öffneten, wurde der schädliche Code ausgeführt, der Computer infiziert und die Malware von diesem Computer aus an weitere E-Mail-Adressen verschickt.

Heutzutage konzentrieren sich Hacker bei der Verbreitung von Malware auf das Internet. E-Mail-Nachrichten bleiben eine Gefahr, dienen aber in erster Linie zum Versenden von Links auf schädliche Webseiten, nicht zum Verteilen schädlicher Dateianhänge. Dennoch gibt es auch heute noch Malware-Arten wie Bredo, die sich per E-Mail verbreiten und auf den Benutzergeräten schädlichen Code ausführen.

Ein strikter Spamschutz in Kombination mit einer Endpoint-Sicherheitssoftware schützt Sie vor E-Mail-Malware. Beständige Aufklärung der Benutzer schärft deren Auge, damit sie auch bei scheinbar ungefährlichen Anhängen von Fremden aufmerksam bleiben. (Siehe **Exploit, Botnet**)

Exploit

Bei einem Exploit wird eine vorhandene und bekannte Sicherheitslücke ausgenutzt, um auf einen Computer zuzugreifen oder diesen zu infizieren.

Ein Exploit nutzt in der Regel eine bestimmte Sicherheitslücke in einer Anwendung aus. Er wird hinfällig, wenn diese Lücke mit einem Patch geschlossen ist. Sogenannte Zero-Day-Exploits werden von Hackern möglichst früh genutzt oder weitergegeben, noch ehe der Softwareanbieter über die Sicherheitslücke Bescheid weiß und sie somit mit einem Patch schließen kann.

Um sich vor Exploits zu schützen, achten Sie stets darauf, dass Ihre Virenschutz- oder Endpoint-Sicherheitssoftware aktiviert ist und auf Ihrem Computer alle aktuellen Patches installiert sind. Dies betrifft das Betriebssystem genauso wie die Anwendungen. (Siehe **Sicherheitslücke, Drive-by-Download, Buffer-/Pufferüberlauf**)

Gefälschter Virenschutz

Einige Virenprogramme sind Fälschungen: Sie geben sich als Virenschutz aus, melden aber nicht existente Bedrohungen. Sie wollen den Benutzer verunsichern und ihn dazu bringen, echtes Geld für ein unnötiges, kostenpflichtiges Produkt auszugeben.

Gefälschter Virenschutz wird als Scareware bezeichnet. Er wird meist über schädliche Webseiten installiert und sieht aus wie ein Online-Scanner. Cyberkriminelle locken Besucher auf diese Webseiten, indem sie Spam-Nachrichten mit entsprechenden Links versenden oder legitime Webseiten hacken. Oftmals versuchen sie auch, die Ergebnisse beliebter Suchmaschinen zu manipulieren (Blackhat SEO), so dass Benutzer im Rahmen einer Suche unweigerlich auf Webseiten stoßen, über die der schädliche Code verbreitet wird.

Hinter Scareware und gefälschten Virenschutzprogrammen stecken reale finanzielle Interessen. Die enormen Einnahmen fließen in die Entwicklung und Verbreitung neuer gefälschter Virenschutzprogramme. Hackergruppen können heute schnell und einfach professionell wirkende Webseiten erstellen, die so wirken, als gehörten sie zu einem legitimen Sicherheitsanbieter.

Echte und stets aktuell gehaltene Virenschutz- oder Endpoint-Sicherheitssoftware schützt Sie vor solchen gefälschten Virenschutzprogrammen.

Hacktivismus

Hacktivisten sind meist politisch motiviert und greifen Unternehmen, Behörden, Institutionen und Privatpersonen an.

Politische Hacker verunstalten Webseiten, leiten Datenverkehr um, starten DoS-Angriffe und stehlen Daten.

Im Jahr 2011 machte die Hacktivisten-Gruppe LulzSec häufig Schlagzeilen mit Angriffen unter anderem auf Sony, PBS, den US-Senat, die CIA und die FBI-Tochter InfraGard. Nach 50 Tagen löste sich die Gruppe wieder auf.

Anonymous, ein lockerer Zusammenschluss international agierender Hacker, möchte mit seinen Aktionen nach eigener Aussage den zivilen Ungehorsam fördern. Anonymous stand beispielsweise im Verdacht, Webseiten in El Salvador, Israel und der Stadt Toronto über verteilte Denial-of-Service-Angriffe lahmgelegt zu haben. Der Gruppierung angehörende Hacker legten im Rahmen eines Angriffs auf Booz Allen Hamilton außerdem 90.000 E-Mail-Adressen von US-Militärangehörigen offen.

Die Vielfalt der Ziele deutet darauf hin, dass Hacktivismus nahezu alle Institutionen treffen kann, auch wenn bisher nur eine Minderheit wirklich betroffen war. Viele Mitglieder von LulzSec und Anonymous wurden inzwischen von den Strafverfolgungsbehörden verhaftet.

Verschlüsselung ist die beste Methode, um sich vor Hackern zu schützen und unbefugte Zugriffe auf sensible Daten zu verhindern.

Hoax

Hoaxes sind Berichte über erfundene Viren oder nicht existierende Gefahren.

Hoaxes sind typischerweise E-Mails mit Inhalten der folgenden Art:

- Sie warnen vor einer nicht erkennbaren, höchst schädlichen, neuen Malware.
- Sie fordern Sie auf, E-Mails mit einem bestimmten Betreff (zum Beispiel „Justin Bieber“) nicht zu lesen.
- Sie behaupten, die Warnung stamme von einem großen Softwareunternehmen, einem Internetdienstanbieter oder einer Regierungsbehörde (zum Beispiel von IBM, Microsoft, AOL oder der FCC).
- Sie behaupten, die neue Malware sei zu Unglaublichem in der Lage. Im Hoax „A moment of silence“ heißt es beispielsweise, es sei kein Datenaustausch erforderlich, um einen Computer zu infizieren.
- Es wimmelt von unsinnigen technischen Begriffen. So heißt es bei „Sector Zero“, die Malware könne den Nullsektor der Festplatte zerstören.
- Sie werden aufgefordert, die Warnung weiterzuleiten.
- Es wird behauptet, dass Sie, wenn Sie bei Facebook bei bestimmten Personen oder Geschichten auf „Gefällt mir“ klicken, für karitative Zwecke spenden, Geld oder sonstige Preise erhalten.

Wenn solche Hoax-Meldungen von vielen Benutzern weitergeleitet werden, kann dies eine Nachrichtenflut verursachen, die zu einer Überlastung der E-Mail-Server führt. Hoax-Nachrichten lenken unter Umständen auch von tatsächlichen Malware-Bedrohungen ab.

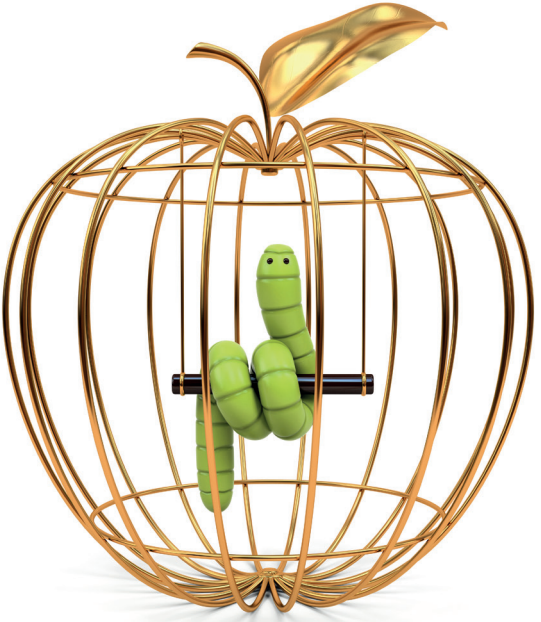
Da es sich bei Hoaxes nicht um Malware handelt, können diese auch nicht von Ihrer Virenschutz- oder Endpoint-Sicherheitssoftware erkannt werden.

Honeypot

Bei einem Honeypot handelt es sich um eine Falle: Sicherheitsexperten legen sie aus, um Hackerangriffe zu analysieren oder Malware-Samples zu sammeln.

Es gibt verschiedene Arten von Honeypots. Bei einigen werden Geräte an das Netzwerk angeschlossen, um Netzwerkwürmer zu erfassen. Bei anderen werden gefälschte Netzwerkdienste (zum Beispiel ein Webserver) bereitgestellt, um eingehende Angriffe zu protokollieren.

Sicherheitsexperten oder -forscher setzen Honeypots ein, um Daten zu aktuellen Bedrohungen und Angriffen zu sammeln.



Internetwurm

Würmer sind Viren, die sich im Internet oder in lokalen Netzwerken selbst kopieren und so verbreiten.

Würmer unterscheiden sich von Computerviren dadurch, dass sie sich selbst verbreiten können und weder Programme noch Dateien als Träger benötigen. Sie erstellen einfach exakte Kopien von sich selbst und verbreiten sich über die Kommunikation zwischen Computern.

Der Conficker-Wurm ist ein Beispiel für einen Internetwurm, der eine Sicherheitslücke im System ausnutzt, um Computer über das Netzwerk zu infizieren. Solche Würmer können sich sehr schnell verbreiten und eine große Anzahl an Computern infizieren.

Manche Würmer öffnen auch eine „Hintertür“ am Computer, durch die Hacker eindringen und das Gerät übernehmen können. Solche Computer können dann zum Versenden von Spam-E-Mails eingesetzt werden (siehe **Zombie**).

Betriebssystemanbieter veröffentlichen regelmäßig Patches, um Sicherheitslücken in ihrer Software zu schließen. Um geschützt zu bleiben, aktivieren Sie die automatischen Updates für Windows- oder Apple-Geräte.

In-the-Cloud-Erkennung

Bei der In-the-Cloud-Erkennung werden Daten in Echtzeit online überprüft, um mögliche Bedrohungen ausfindig zu machen.

In-the-Cloud-Erkennung dient vor allem dem Ziel, Sicherheitsprodukte möglichst schnell mit aktuellsten Malware-Signaturen auszustatten. Durch die Abfrage von online (das heißt „in der Cloud“) veröffentlichten Daten müssen Sicherheitsprodukte keine Signaturen an Computer senden.

Dank In-the-Cloud-Erkennung kann ein Virenschutz sehr schnell auf neu erkannte Bedrohungen reagieren. Der Nachteil liegt jedoch darin, dass für die Überprüfung eine Internetverbindung bestehen muss.

Keylogging

Beim Keylogging werden Ihre Tasteneingaben heimlich von nicht autorisierten Dritten aufgezeichnet.

Es handelt sich hierbei um einen gängigen Bestandteil von Malware. Denn mit ihm lassen sich Benutzernamen, Passwörter, Kreditkartendaten und andere vertrauliche Daten auf effektive Weise stehlen.

Malware

Malware ist eine allgemeine Bezeichnung für schädliche Software wie Viren, Würmer, Trojaner und Spyware. Viele verwenden die Begriffe Malware und Viren synonym.

Eine gute Virenschutzsoftware erkennt normalerweise eine breitere Palette an Bedrohungen als Viren sie darstellen.

Mobiltelefon-Malware

Bei Mobiltelefon-Malware handelt es sich um Schadsoftware, die speziell für die Ausführung auf mobilen Geräten entwickelt wurde. Es gibt sie vor allem auf Smartphones und PDAs.

Die ersten Beispiele für schädliche Programme auf Mobiltelefonen zeigten sich schon im Jahr 2004. Die Mobiltelefon-Malware richtete sich anfangs nur gegen das damals sehr verbreitete Betriebssystem Symbian, die prinzipielle Bedrohung durch mobile Malware nahm aber erst ihren Anfang.

Die Cyberkriminellen haben zwar relativ lange gebraucht, um mobile Malware in bedeutendem Umfang zu entwickeln. Doch seitdem die moderne Generation von Smartphones mit den Betriebssystemen Android und iOS populär wurde, reißt die Welle der Mobiltelefon-Malware nicht mehr ab. Seit Ende 2010, als man die ersten Malware-Samples für Android- und iOS-Geräte identifizierte, sind Tausende Varianten von mobiler Malware aufgetaucht.

Bis heute haben Malware-Experten deutlich mehr schädliche Apps für Android entdeckt als für iOS. Das liegt mit großer Wahrscheinlichkeit daran, dass sich auf Android-Geräten sehr leicht Apps installieren lassen, die nicht über den offiziellen Shop geladen werden. Tauschbörsen enthalten häufig schädliche Versionen beliebter Anwendungen und Spiele.

Ganz wie bei PC-Malware wollen Cyberkriminelle mit mobiler Malware vor allem das schnelle Geld machen. Ähnlich wie Windows-Malware verbreitet auch die mobile Malware gefälschte Virenschutzprogramme und stiehlt vertrauliche Daten. Andere Typen mobiler Malware senden SMS-Nachrichten oder rufen bei kostenpflichtigen Mehrwertdiensten an.

Auch vertrauenswürdige Quellen bieten Anwendungen an, die die Privatsphäre des Benutzers beeinträchtigen können. Viele sogenannte Advertising-Frameworks geben unter Umständen persönliche Daten von Benutzern weiter, etwa Standort oder Telefonnummer. Die Anwendungen können als potenziell unerwünschte Anwendungen (PUAs) eingestuft werden.

Damit Malware auf Ihrem Mobilgerät keine Chance hat, halten Sie das mobile Betriebssystem mit allen Sicherheitsupdates auf dem aktuellen Stand. Laden Sie Anwendungen nur aus vertrauenswürdigen Quellen herunter, etwa Google Play oder Apple iTunes. Für Geräte, auf denen Android ausgeführt wird, empfehlen wir die Installation einer Sicherheitssoftware, zum Beispiel Sophos Mobile Security.

Non-Compliance

Non-Compliance liegt vor, wenn gesetzliche oder branchenspezifische Datenschutzvorschriften nicht eingehalten werden.

Non-Compliance kann teuer werden. Unternehmen können rechtlich belangt und mit Bußgeldern belegt werden oder ihren guten Ruf verlieren.

Eine Studie des Ponemon Institute im Jahr 2012 ergab, dass sich die durchschnittlichen Kosten eines Datenlecks in den USA auf 6,7 Mio. USD (5,4 Mio. EUR) beliefen. Pro Kundendatensatz entspricht das durchschnittlich 204 USD.

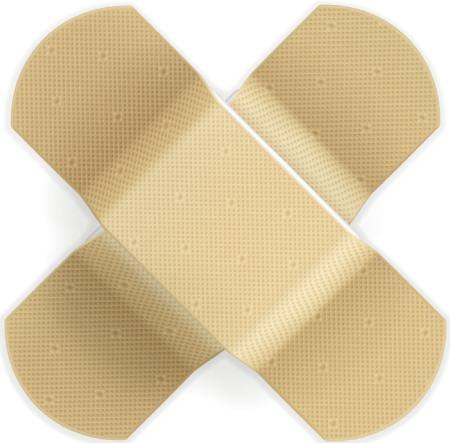
Parasitenvirus

Parasitenviren sind auch als Dateiviren bekannt und verbreiten sich, indem sie sich selbst an Programmdateien anhängen.

Wenn Sie ein mit einem Parasitenvirus infiziertes Programm starten, wird zuerst der parasitäre Virencode ausgeführt. Um seine Anwesenheit zu verbergen, übergibt der Virus danach die Kontrolle an das Originalprogramm zurück.

Das Betriebssystem auf Ihrem Computer betrachtet den Virus als Teil des Programms, das Sie ausführen wollten, und vergibt dafür dieselben Rechte. Diese Rechte ermöglichen dem Virus, sich selbst zu kopieren, sich im Speicher zu installieren oder Änderungen an Ihrem Computer vorzunehmen.

Parasitenviren traten in der Geschichte der Viren früh auf, wurden dann aber eher selten. Heutzutage werden sie wieder gängiger. Jüngste Beispiele dafür sind Sality, Virut und Vetor.



Patches

Patches sind Software-Flicken, die Fehler und Sicherheitsprobleme in Betriebssystemen oder Anwendungen beseitigen.

Für den Schutz vor Malware sind Patches für Sicherheitslücken von höchster Bedeutung. Viele ausgefeilte Bedrohungen nutzen Sicherheitslücken aus, zum Beispiel Conficker. Wenn Sie die aktuellen Patches nicht installiert haben, laufen Sie Gefahr, Ihren Computer angreifbar zu machen.

Viele Softwareanbieter geben regelmäßig neue Patches heraus: Microsoft veröffentlicht seine Fixes jeden zweiten Dienstag im Monat („Patch Tuesday"), Adobe gibt vierteljährliche Updates für Adobe Reader und Acrobat am zweiten Dienstag nach Quartalsbeginn heraus.

Abonnieren Sie entsprechende Mailing-Listen, um in Bezug auf Sicherheitslücken immer auf dem Laufenden zu bleiben. Die meisten seriösen Anbieter stellen einen solchen Service zur Verfügung. Die Sicherheitsbenachrichtigungen von Microsoft finden Sie beispielsweise unter www.microsoft.com/technet/security/bulletin/notify.mspx.

Benutzer von Microsoft Windows Home können automatische Updates mit Hilfe von Windows Update (Windows Vista/7) oder Security Center (Windows XP) aktivieren. Benutzer von Apple OS X können auf das Apple-Logo in der oberen linken Ecke ihres Desktops klicken und Software-Updates auswählen.

Unternehmen sollten sicherstellen, dass alle Computer, die mit ihrem Netzwerk verbunden sind, festgelegte Sicherheitsrichtlinien erfüllen. Dazu gehört, dass die aktuellen Sicherheitspatches für Betriebssysteme und Anwendungen installiert sind. (Siehe **Exploit, Sicherheitslücke**)


What's
your
name?

Phishing

Phishing ist der Versuch, Sie dazu zu bringen, vertrauliche Informationen an unbekannte Dritte weiter zu geben.

Typischerweise erhalten Sie eine E-Mail, die von einer seriösen Organisation zu kommen scheint, zum Beispiel von:

- Banken
- Sozialen Netzwerken (Facebook, Twitter)
- Online-Spielen
- Online-Diensten mit Zugriff auf Ihre Finanzdaten (zum Beispiel iTunes, Buchhaltungsdienstleister)
- Abteilungen in Ihrem eigenen Unternehmen (zum Beispiel vom technischen Support-Team, vom Systemadministrator oder Helpdesk)

In der E-Mail befindet sich ein Link, der scheinbar zur Webseite des Unternehmens führt. Folgen Sie jedoch dem Link, leitet dieser Sie auf eine betrügerische Kopie der Webseite weiter. Alle Daten, die Sie eingeben, zum Beispiel Kontonummern, PINs oder Passwörter, können von den Hintermännern der gefälschten Webseite gestohlen und missbraucht werden.

Manchmal führt der Link auch zur tatsächlichen Webseite, doch über ihr liegt ein gefälschtes Pop-up-Fenster. Sie sehen dann die Adresse der tatsächlichen Webseite im Hintergrund, doch die Daten, die Sie in das Pop-up- Fenster eingeben, lassen sich trotzdem stehlen.

Zum besseren Schutz gegen Phishing-Angriffe sollten Sie es grundsätzlich vermeiden, Links in E-Mail-Nachrichten anzuklicken. Geben Sie stattdessen manuell die Adresse der gewünschten Webseite in das Adressfeld ein, oder rufen Sie die Webseite über ein Lesezeichen oder einen Favoritenlink auf.

Phishing-Angriffe per E-Mail finden mittlerweile nicht mehr ausschließlich über das Internet statt, sondern schließen auch Offline-Medien ein. Es wurden bereits Phishing-Versuche gemeldet, bei denen neben Webseiten auch Telefon- und Faxnummern zum Einsatz kamen.

Virenschutzsoftware blockiert viele Phishing-E-Mails, Websicherheitssoftware verhindert den Zugriff auf Phishing-Webseiten.

Potenziell unerwünschte Anwendung (PUA)

Potenziell unerwünschte Anwendungen sind nicht unbedingt schädlich, eignen sich aber eher nicht zur Verwendung im Unternehmen.

Manche Anwendungen sind nicht schädlich und im richtigen Kontext möglicherweise sogar sinnvoll, doch für den Einsatz in einem Unternehmensnetzwerk sind sie nicht geeignet. Beispiele hierfür sind Adware, Dialer, unschädliche Spyware, Werkzeuge zur PC-Fernsteuerung und Hacking-Tools.

Bestimmte Virenschutz- und Endpoint-Sicherheitsprogramme erkennen und melden PUAs auf den Computern der Benutzer. Der Administrator kann die Anwendungen dann wahlweise autorisieren oder sie von den Computern entfernen.

Ransomware

Ransomware ist erpresserische Software. Sie versperrt Ihnen den Zugriff auf Ihre eigenen Dateien – bis Sie ein Lösegeld bezahlen.

Früher hat schädliche Software Ihre Daten beschädigt oder gelöscht. Heute nimmt sie Ihre Daten als Geisel. Der Trojaner Archiveus beispielsweise kopiert den Inhalt des Ordners „Eigene Dateien" in eine passwortgeschützte Datei und löscht dann die Originaldateien. Er hinterlässt danach eine Nachricht, in der er Ihnen mitteilt, dass Sie ein Passwort mit 30 Zeichen benötigen, um auf den Ordner zugreifen zu können, und dass Sie dieses Passwort erhalten, wenn Sie eine Bestellung bei einer Online-Apotheke in Auftrag geben.

In diesem wie in den meisten anderen Ransomware-Fällen sind Passwort oder Schlüssel im Code des Trojaners verborgen, so dass Malware-Analysten ihn abrufen können. Künftig könnten Hacker jedoch eine asymmetrische Chiffrierung (mit öffentlichem Schlüssel) nutzen, bei der ein Schlüssel zur Verschlüsselung der Daten, ein zweiter zur Entschlüsselung dient, so dass das Passwort dann nicht mehr auf Ihrem Computer zu finden ist.

Im Februar 2012 warnte beispielsweise die UK Metropolitan Police Windows-Benutzer vor einem Malware-Angriff, der sich als Nachricht der Polizeibehörde im Kampf gegen Computerkriminalität ausgibt. Ransomware sperrt Computer mit der Begründung, dass auf illegale Webseiten zugegriffen wurde. Erst nach dem Bezahlen einer Geldstrafe, behauptet die offiziell wirkende Nachricht, funktionieren die Computer wieder. Diese Drohungen entbehren jedoch jeglicher Grundlage, da Ransomware zu solchen Dingen nicht in der Lage ist.

Ransomware kann sich in der Zukunft allerdings zu einem Problem entwickeln, da Hacker immer neue Methoden finden, sich das Lösegeld überweisen zu lassen. Früher beschränkte die Bezahlung über SMS-Premiumdienste das Problem auf bestimmte geografische Bereiche.

Rootkit

Bei einem Rootkit handelt es sich um ein kleines Stück Software, das andere laufende Programme oder Prozesse verbirgt. So unterstützt es Computermissbrauch oder Datendiebstahl.

Ein relativ hoher Anteil der heute im Umlauf befindlichen Malware installiert nach der Infektion ein Rootkit, um damit seine Aktivität zu verbergen. Ein Rootkit kann Keylogger oder Passwortschnüffler tarnen, die vertrauliche Daten erfassen und sie per Internet an Hacker schicken. Es kann einem Hacker auch ermöglichen, den Computer für illegale Zwecke zu missbrauchen (zum Beispiel zum Starten eines Denial-of-Service-Angriffs gegen andere Computer oder zum Versenden von Spam-E-Mails), ohne dass sich der Benutzer dessen bewusst ist.

Endpoint-Sicherheitsprodukte erkennen und entfernen heute Rootkits wie TDL und ZAccess im Rahmen ihrer standardmäßigen Anti-Malware-Routinen. Für die wirksame Beseitigung einiger Rootkits ist jedoch ein spezielles Entfernungstool erforderlich.

Sicherheitslücke

Sicherheitslücken sind Fehler in Softwareprogrammen. Hacker nutzen die Fehler aus, um Computer anzugreifen oder zu infizieren.

Sicherheitslücken, die den Benutzer angreifbar machen, gibt es in jedem Softwareprodukt. Wenn die verantwortlichen Softwareanbieter von einem Problem erfahren, erstellen und veröffentlichen sie umgehend entsprechende Patches.

Manche Unternehmen beauftragen Sicherheitsexperten und sogenannte „ethische Hacker", um Sicherheitslücken für sie aufzuspüren. Es gibt aber auch Hacker, die das Wissen um neue Sicherheitslücken auf dem Schwarzmarkt verkaufen. Sogenannte Zero-Day-Angriffe versuchen Sicherheitslücken auszunutzen, ehe ein entsprechender Patch angeboten wird.

Um möglichst viele Sicherheitslücken zu schließen, sollten Sie stets alle aktuell verfügbaren Patches für Ihr Betriebssystem installieren und auch alle installierten Anwendungen stets auf dem neusten Stand halten. (Siehe **Exploit, Patches**)

Social Engineering

Social Engineering bezeichnet die Palette möglicher Tricks, mit denen Angreifer ihre Opfer zu bestimmten Handlungen verführen. Meist haben sie das Aufrufen einer schädlichen Webseite oder das Ausführen eines unerwünschten Dateianhangs zum Ziel.

Beim Social Engineering geht es sehr oft darum, Benutzer dazu zu bringen, Benutzernamen und Passwörter preiszugeben. Die Angreifer können diese Zugangsdaten benutzen, um Nachrichten zu verschicken, die scheinbar von einem internen Benutzer kommen. Auf diese Weise lässt sich ein Datendiebstahl leichter durchführen.

Im April 2012 starteten Hacker eine Malware-Kampagne: Sie teilte den Empfängern per E-Mail mit, man habe online ein privates Foto von ihnen veröffentlicht. Die einzelnen E-Mail-Nachrichten hatten jeweils verschiedene Nachrichtentexte, doch stets wurde im Anhang eine ZIP-Datei mit einem Trojaner versendet.

Die Betreffzeilen lauteten in etwa wie folgt:

RE: Bitte Anhang überprüfen – Auf dieses Foto musst Du reagieren!

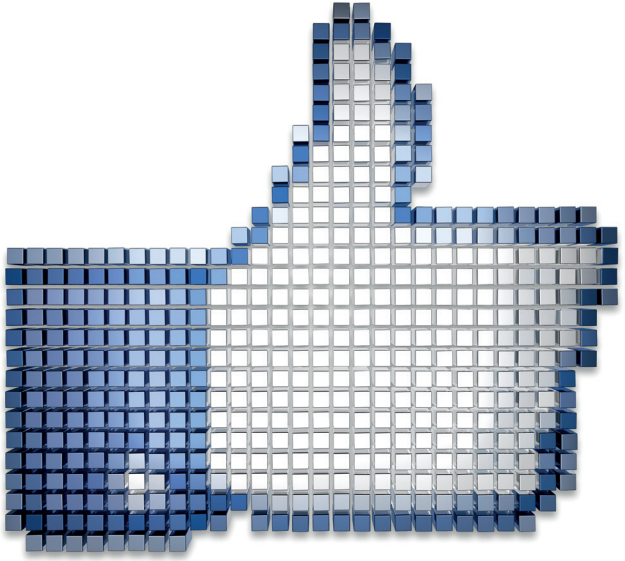
FW: Bitte Anhang überprüfen – Auf dieses Foto musst Du reagieren!

RE: Foto im Anhang UNBEDINGT ansehen

RE: Ein NACKTFOTO von Dir ist auf Facebook zu sehen!

RE: Warum hast Du dieses Foto ins Netz gestellt?

Wenn Sie Ihren gesunden Menschenverstand einsetzen und Ihre Virenschutzsoftware aktuell halten, haben Sie wenig zu befürchten.



Soziale Netzwerke

Über soziale Netzwerke können Sie kommunizieren und Informationen austauschen. Die Webseiten lassen sich jedoch auch dazu missbrauchen, Malware zu verbreiten und persönliche Daten zu stehlen.

Facebook, der Riese unter den sozialen Netzwerken, gab bekannt, dass von den über eine Milliarde Anmeldedaten jeden Tag ganze 0,06 Prozent geknackt werden. Das sind mehr als 600.000 Benutzerkonten jeden Tag – alle 140 Millisekunden wird ein Konto erobert! Nur zum Vergleich: Ein Augenzwinkern dauert 300-400 Millisekunden.

Überlegen Sie immer gut, auf welche Links Sie klicken, und geben Sie niemals persönliche Daten ein, wenn Sie nicht ganz sicher sind, sich auf einer legitimen Webseite zu befinden.
(Siehe **So bewegen Sie sich sicher im Internet**)

Spam

Bei Spam handelt es sich um unaufgefordert versandte Werbe-E-Mails, also der elektronischen Version unliebsamer Werbepost im Briefkasten.

Um Spam-Filter zu überlisten, tarnen Spammer häufig ihre E-Mails. Immer mehr Spam kommt von scheinbar normalen Absendern mit einer Yahoo!, Hotmail oder AOL E-Mail-Adresse, deren Benutzerkonten geknackt wurden. Auch die Menge an „Snowshoe Spam", der von gemieteten statischen IP-Adressen (VPS) oder Cloud-Diensten aus gesendet wird, nimmt immer mehr zu.

Spammer haben es auch auf große E-Mail-Dienstanbieter abgesehen und versuchen, mit ihrer Malware deren Mail Transfer Agents (MTA) zu manipulieren, um darüber Spam zu versenden.

Spamming kann sich lohnen. In einer einzigen Kampagne können für sehr wenig Geld Millionen von E-Mails verschickt werden. Und wenn auch nur einer von 10.000 Empfängern einen Kauf tätigt, macht der Spammer bereits einen Gewinn.,

Aber ist Spam denn so schlimm?

- Spam verschwendet Arbeitszeit. Benutzer ohne Spamschutz müssen Spam-E-Mails heraussuchen und löschen.
- In der Spam-Flut übersieht man leicht wichtige E-Mails oder löscht sie versehentlich, weil man sie für Spam hält.
- Genauso wie Hoaxes oder E-Mail-Viren verbraucht Spam Bandbreite und verschwendet Speicherplatz.
- Benutzer fühlen sich durch Spam belästigt. Die Schuld wird beim Arbeitgeber gesucht, da man von ihm erwartet, eine sichere Arbeitsumgebung zu gewährleisten.
- Spammer verschicken ihre E-Mails oft über die Computer anderer Benutzer (siehe **Zombie**).
- Spam wird oft zur Verbreitung von Malware genutzt (siehe **E-Mail-Malware**).

Spammer nutzen heute auch beliebte Dienste wie Twitter und oder Facebook, um Spamfilter zu umgehen und Benutzer dazu zu verleiten, persönliche und finanzielle Daten preiszugeben.


BLAH
BLAH BLAH
BLAH
BLAH BLAH BLAH BLAH BLAH BLAH BLAH

Spearphishing

Beim Spearphishing handelt es sich um gezieltes Phishing mit gefälschten E-Mails. Einzelne Mitarbeiter eines Unternehmens sollen dazu verleitet werden, vertrauliche Informationen oder Benutzerdaten offenzulegen.

Während Angreifer beim Phishing massenhaft und ziellos E-Mails versenden, gehen sie beim Spearphishing im kleinen Rahmen ganz gezielt vor. Der Spearphisher sendet E-Mails an ausgesuchte Mitarbeiter eines bestimmten Unternehmens. Diese E-Mails erwecken oft den Eindruck, sie kämen von einem anderen Mitarbeiter desselben Unternehmens. Sie bitten darum, einen Benutzernamen oder ein Passwort zu bestätigen.

Manchmal stammen die E-Mails scheinbar von einer vertrauenswürdigen Abteilung, die solche Informationen tatsächlich anfragen könnte, zum Beispiel von der IT- oder Personalabteilung. Links in den E-Mails leiten dann zu einer gefälschten Version der Unternehmenswebseite oder des Intranets weiter, wo weitere Benutzerdaten gestohlen werden. (Siehe **E-Mail-Malware**)

Spoofing

Beim E-Mail-Spoofing wird die Absenderadresse für Social-Engineering- Zwecke gefälscht.

Spoofing eignet sich für eine ganze Reihe bösartiger Absichten.

Phisher (Kriminelle, die Benutzer zur Preisgabe vertraulicher Informationen verleiten) fälschen Absenderadressen, um den Eindruck zu erwecken, die E-Mail stamme von einer vertrauenswürdigen Quelle, etwa Ihrer Bank. Die E-Mail leitet Sie auf eine gefälschte Webseite (zum Beispiel der Nachahmung einer Bank-Webseite) weiter, die Ihre Kontodetails und Ihr Passwort abfragt.

Manchmal senden Phisher auch E-Mails, die scheinbar aus dem Unternehmen stammen, in dem Sie arbeiten – zum Beispiel vom Systemadministrator. Sie fordern Sie zum Beispiel auf, Ihr Passwort zu ändern oder Ihre Daten zu bestätigen.

Kriminelle Onlinebetrüger verwischen mit gefälschten E-Mail-Adressen ihre Spuren und entgehen so der Entdeckung und Verfolgung.

Spammer erwecken durch gefälschte Absenderadressen den Eindruck, dass eine harmlose Einzelperson oder ein Unternehmen für den Spam verantwortlich ist. Ein weiterer Vorteil für die Absender ist, dass ihr eigenes Postfach nicht mit Nachrichten über fehlgeschlagene Zustellungen überflutet wird.
(Siehe **E-Mail-Malware**)

Spyware

Bei Spyware handelt es sich um Software, die Werbetreibenden oder Hackern ermöglicht, ohne Ihr Wissen an persönliche Daten zu gelangen.

Spyware kann auf Ihren Computer gelangen, wenn Sie bestimmte Webseiten besuchen. Möglicherweise werden Sie in einem Pop-up-Fenster dazu aufgefordert, ein notwendiges Software-Dienstprogramm herunterzuladen, oder es wird ohne Ihr Wissen automatisch Software heruntergeladen.

Ist die Spyware auf Ihrem Computer erst mal installiert, kann sie Ihre Aktivitäten protokollieren (zum Beispiel Ihre Besuche von Webseiten) und die Protokolle an nicht autorisierte Dritte (zum Beispiel Werbetreibende) schicken. Spyware verbraucht Speicher und Arbeitsspeicher, was zu einer Verlangsamung oder zum Absturz Ihres Computers führen kann.

Gute Virenschutz- und Endpoint-Sicherheitslösungen erkennen und entfernen Spyware-Programme und behandeln sie wie einen Trojaner.

SQL Injection

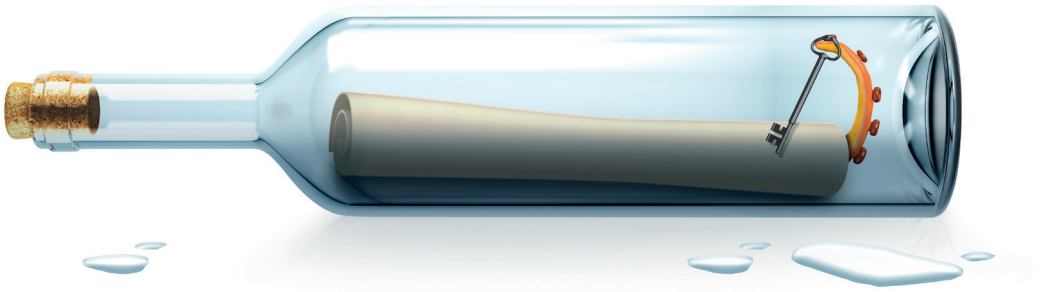
Die SQL Injection ist ein Exploit, der sich den Umstand zunutze macht, dass Software für Datenbankabfragen nicht immer gründlich prüft, ob eine Abfrage evtl. durch Formulareingaben eingeschleuste schädliche Kommandos enthält.

Würmer nutzen SQL Injection in Kombination mit Cross Site Scripting (XSS), um Webseiten zu knacken und dort Daten zu extrahieren oder schädlichen Code einzubetten.

Bei der SQL Injection werden Befehle an einen Webserver gesendet, der mit einer SQL-Datenbank verknüpft ist. Wenn der Server nicht richtig aufgesetzt und gehärtet ist, behandelt er Daten, die in ein Formularfeld eingegeben werden (zum Beispiel einen Benutzernamen) als Befehle, die auf dem Datenbankserver auszuführen sind. Ein Angreifer kann dadurch beispielsweise einen Befehl einschleusen, der den gesamten Inhalt der Datenbank (etwa Kundendatensätze und Zahlungsinformationen) herausgibt.

Das wohl bekannteste Datenloch, das per SQL Injection entstand, trat im März 2008 auf, als Hacker die Systeme des Zahlungsabwicklers Heartland Payment Systems knackten und 134 Mio. Kreditkartendaten stahlen.

Web Application Firewalls (WAFs) schützen vor dieser Art von Angriff mit einem hoch entwickelten System an Mustern, die an den Webserver übermittelte SQL-Befehle erkennen. Wie bei jedem musterbasierten System ist es für einen bestmöglichen Schutz auch hier erforderlich, die Muster regelmäßig zu aktualisieren, um neue, kreative Methoden zur Einbettung von SQL-Injection-Befehlen abzuwehren.



Trojaner (Trojanisches Pferd)

Trojaner sind Programme, die sich als legitime Software ausgeben, im Geheimen aber schädliche Funktionen ausführen.

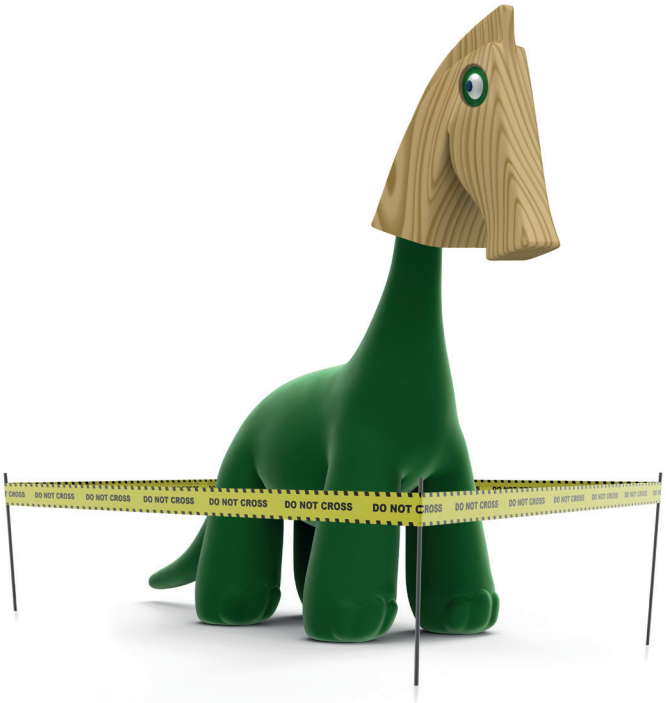
Der Sammelbegriff Trojaner umfasst viele verschiedene Arten von Malware: Bots, Backdoor-Trojaner und Download-Trojaner.

Bei einem hohen Prozentsatz der heutigen Malware handelt es sich um Trojaner.

Ein Trojaner-Programm gibt vor, eine bestimmte Aktion auszuführen, tut aber in Wahrheit etwas völlig anderes – meist ohne Wissen des Benutzers. Bekannte Beispiele sind Video-Codecs, die auf manchen Webseiten zum Anzeigen von Online-Videos erforderlich sind. Wenn ein Trojaner-Codec installiert wird, kann dieser auch Spyware oder andere schädliche Software installieren.

Ein anderes Beispiel ist ein Link, der angeblich zu einem tollen Spiel führt. Nach der Installation des Programms stellt sich heraus, dass es sich nicht etwa um ein Spiel handelt, sondern um einen Trojaner, der Ihren Computer beschädigt und die Daten auf Ihrer Festplatte löscht.

Trojaner werden oft mit raubkopierten Softwareanwendungen verbreitet oder mit Keygens, die illegale Lizenzcodes für herunterladbare Software generieren. (Siehe **Backdoor-Trojaner**)


DO NOT CROSS
DO NOT CROSS
DO NOT CROSS
DO NOT CROSS
DO NOT CROSS
DO NOT CROSS
DO NOT CROSS
DO NOT CROSS
DO NOT CROSS
DO NOT CROSS

Verdächtige Dateien und Verhaltensmuster

Bei einer Prüfung markiert eine Endpoint-Sicherheitslösung jede Datei als unbedenklich oder schädlich. Weist eine Datei eine Reihe bedenklicher Merkmale oder Verhaltensmuster auf, gilt sie als verdächtig.

Verdächtiges Verhalten bedeutet, dass Dateien bei der Ausführung auf einem Computer fragwürdige Dinge tun, wie zum Beispiel eine Kopie von sich selbst in einem Systemordner ablegen.

Laufzeitschutz hilft beim Schutz vor verdächtigen Dateien: Das Verhalten aller auf dem Computer ausgeführten Programme wird analysiert, und es werden alle Aktivitäten blockiert, die eventuell schädlich sein könnten.
(Siehe **Buffer-/Pufferüberlauf**)

Virus

Ein Virus ist ein Computerprogramm, das sich verbreitet, indem es sich selbst kopiert.

Computerviren verbreiten sich von Computer zu Computer und von Netzwerk zu Netzwerk, indem sie Kopien von sich selbst erstellen. Der Benutzer bekommt davon meist gar nichts mit.

Viren bewirken zuweilen, dass der Computer lästige Meldungen anzeigt. Sie helfen Hackern, Daten zu stehlen oder die Kontrolle über einen Computer zu übernehmen.

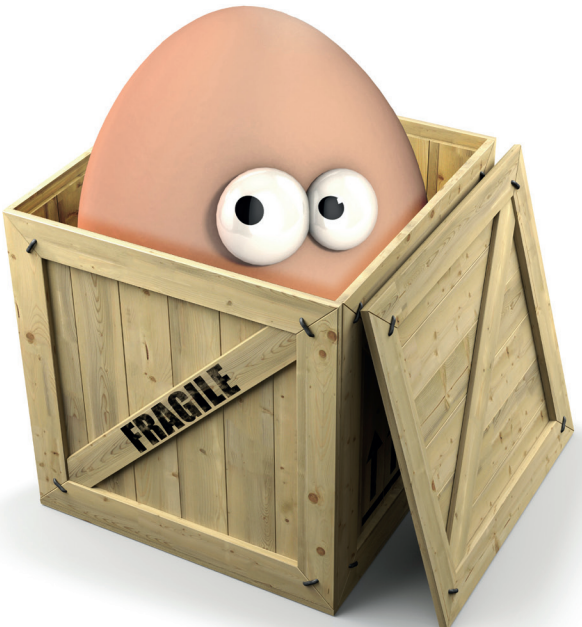
Viren können sich selbst an andere Programme anhängen. Sie verbergen sich außerdem in Code, der beim Öffnen bestimmter Dateitypen automatisch ausgeführt wird. Manchmal nutzen sie Sicherheitslücken im Computer-Betriebssystem, um sich automatisch auszuführen und zu verbreiten.

Eine mit einem Virus infizierte Datei gelangt auf verschiedenen Wegen zu Ihnen, zum Beispiel als E-Mail-Anhang, als Download aus dem Internet oder per USB-Datenträger. (Siehe **Parasitenvirus, E-Mail-Malware, Internetwurm, Malware**)

Zombie

Bei einem Zombie handelt es sich um einen infizierten Computer, der von einem Hacker ferngesteuert wird. Oft ist er bereits Teil eines Botnets, also eines Netzwerks aus vielen Zombie- oder Bot-Computern.

Wenn ein Hacker einen Computer über ein Botnet im Internet fernsteuern kann, nennt man den Computer einen Zombie. (Siehe **Botnet**)


FRAGILE

Sicherheits-software und -hardware


SOPHOS

Anti-Malware

Anti-Malware-Software und Malwareschutzpakete schützen Sie vor Viren und weiteren Bedrohungen wie Trojanern, Würmern und – je nach Produkt – auch vor Spyware.

Anti-Malware-Software besitzt immer auch einen Scanner. Er prüft Programme und stellt fest, ob sie möglicherweise oder tatsächlich schädlich sind. Scanner können Folgendes erkennen:

- Bekannte Malware: Der Scanner vergleicht die Dateien auf Ihrem Computer mit einer Bibliothek bekannter Malware-Dateien. Bei einer Übereinstimmung gibt der Scanner eine Warnung aus und blockiert den Zugriff auf diese Datei. Die Erkennung bekannter Malware setzt die möglichst häufige Aktualisierung einer lokalen Datenbank mit den aktuellen Virusidentitäten voraus, alternativ eine Verbindung zu einer cloud-basierten Malware-Datenbank.
- Bisher unbekannte Malware: Der Scanner analysiert das wahrscheinliche Verhalten eines Programms. Wenn es alle Kennzeichen eines Virus aufweist, wird der Zugriff blockiert, auch wenn die Datei keinem bekannten Virus entspricht.
- Verdächtige Dateien: Der Scanner analysiert das wahrscheinliche Verhalten eines Programms. Wird dieses Verhalten als unerwünscht eingestuft, dann warnt der Scanner, dass es sich um Malware handeln könnte. Die meisten Malwareschutzpakete beinhalten sowohl Scanner, die beim Dateizugriff prüfen (Zugriffsscanner), als auch solche, die nach Bedarf prüfen (On-Demand- Scanner).

Zugriffsscanner sind auf Ihrem Computer ständig im Hintergrund aktiv. Sie überprüfen automatisch alle Dateien, die Sie öffnen oder ausführen möchten, und können Sie am Zugriff auf infizierte Dateien hindern.

On-Demand-Scanner prüfen auf ausdrücklichen Wunsch ganz gezielt ausgesuchte Dateien, Verzeichnisse oder Laufwerke.

Anti-Spam

Spamfilter erkennen unerwünschte E-Mails und sortieren sie aus, damit sie nicht in den Posteingang des Empfängers gelangen.

Sie kombinieren verschiedene Methoden, um herauszufinden, welche E-Mail harmlos und welche E-Mail mit hoher Wahrscheinlichkeit Spam ist. Sie haben folgende Funktionen:

- Sie blockieren E-Mails von Computern, die sich auf einer schwarzen Liste befinden. Dies kann eine käuflich erwerbbare Liste sein oder eine lokale Liste der Adressen, von denen Ihr Unternehmen schon zuvor Spam erhalten hat.
- Sie blockieren E-Mails, in denen bestimmte Webadressen als Links genannt werden.
- Sie prüfen, ob eine E-Mail von einer legitimen Domäne oder Webadresse aus gesendet wurde. Spammer fälschen Absenderadressen, um Spamschutzprogramme zu umgehen.
- Sie suchen nach bestimmten Schlüsselwörtern oder Phrasen, die für Spamnachrichten (zum Beispiel „Kreditkarte“ oder „Abnehmen“) typisch sind.
- Sie suchen nach Mustern, die darauf hindeuten, dass der E-Mail-Absender versucht, bestimmte Schlüsselwörter zu tarnen (zum Beispiel „Hardc*re P0rn0“).
- Sie suchen in E-Mails nach unnötigem HTML-Code, der dazu dienen soll, Nachrichten zu verbergen und Spamschutzprogramme zu verwirren.
- Sie kombinieren alle gefundenen Informationen und entscheiden auf dieser Grundlage, mit welcher Wahrscheinlichkeit es sich bei einer E-Mail um Spam handelt. Ab einem bestimmen Wahrscheinlichkeitswert blockieren oder löschen sie die E-Mail, jeweils abhängig von den gewählten Einstellungen.

Spamschutzsoftware muss häufig mit neuen Regeln aktualisiert werden, damit sie die neuesten von Spammern eingesetzten Techniken erkennt.

Appliance

Appliances kombinieren Hardware und Software zu einer einzigen Sicherheitslösung. Appliances lassen sich einfach anschließen, es muss keine separate Software installiert werden.

Die gängigsten Typen sind Email Appliances, UTM Appliances (Unified Threat Management) und Web Appliances. Sie arbeiten am Übergang zwischen Internet und den IT-Systemen eines Unternehmens und filtern den Datenverkehr, um Malware und Spam zu blockieren und Datenverluste zu vermeiden. Email Appliances blockieren Spam, Phishing, Viren, Spyware und andere Malware und können – je nach Lösung – durch Inhaltsfilterung und Verschlüsselung auch die Preisgabe vertraulicher Daten per E-Mail verhindern.

Web Appliances stoppen Malware, Spyware, Phishing, anonymisierende Proxyserver und andere unerwünschte Anwendungen am Übergang zum Web. Gegebenenfalls bieten sie auch Tools, mit denen sich Internet-Nutzungsrichtlinien durchsetzen lassen.

UTM Appliances reduzieren den oft komplexen Aufwand, zahlreiche Einzellösungen für den Schutz Ihres Unternehmens vor Viren, Spam und Hackern auszurollen und zu verwalten.

Application Control

Mit Application Control legen Sie fest, welche Anwendungen auf Unternehmenscomputern und in Unternehmensnetzwerken laufen dürfen und welche nicht.

Eine bessere Kontrolle von Anwendungen verhindert, dass sich Malware ausbreitet oder die Produktivität des Netzwerks und seiner Benutzer leidet. Zu den kontrollierbaren Anwendungen zählen unter anderem Tauschbörsen-Programme, Spiele oder Media-Player.

Mit Application Control limitieren Sie den Zugriff der Benutzer auf ausgewählte Unternehmensanwendungen. Eine Richtlinie kann beispielsweise festlegen, dass nur der Internet Explorer gestartet werden darf, alle anderen Browser aber blockiert werden.

Zu den typischen Anwendungskategorien, die Unternehmen besser kontrollieren sollten, zählen Voice-over-IP-Programme (VoIP), Tools zur Fernsteuerung und Instant-Messaging-Clients.

So genannte Next Generation Firewalls können den Datenverkehr im Netzwerk auch nach der Art der transportierten Daten und der involvierten Ports filtern.

Device Control

Per Device Control lässt sich der Zugriff auf Wechseldatenträger, optische Medienlaufwerke und Drahtlosnetzwerkprotokolle kontrollieren.

Device Control ist ein wichtiges Element in jeder Strategie gegen Datenverluste. Sie verhindert, dass sich Malware ungehindert über USB-Datenträger verbreitet.

Viele Unternehmen setzen Device Control ein, um die bestehenden Richtlinien zur Verwendung von Wechseldatenträgern durchzusetzen. Je nach Lösung können Sie per Device Control mit einer zentralen Richtlinie entscheiden, welche Medien an Computer angeschlossen werden dürfen.

Encryption/Verschlüsselung

Verschlüsselungslösungen schützen Ihre Daten durch die Chiffrierung Ihrer PCs, Laptops, Wechseldatenträger, CDs, E-Mails, Netzwerkdateien, Cloud-Speicher uvm. Nur wer das richtige Passwort kennt, kann auf die Daten zugreifen.

Einige Verschlüsselungslösungen lassen sich so konfigurieren, dass Daten für autorisierte Benutzer automatisch entschlüsselt werden und sie keinen Verschlüsselungsschlüssel und kein Passwort eingeben müssen, um auf die Daten zuzugreifen.

Verschlüsselungslösungen bieten meist folgende Optionen: Schlüsselverwaltung (zur Vereinfachung von Speicherung, Austausch und Wiederherstellung von Schlüsseln), Durchsetzung von Verschlüsselungsrichtlinien, zentrale Verwaltung und Berichtsfunktionen.

Eine wichtige Sicherheitsmaßnahme ist die Verschlüsselung von Daten, die Sie in externen Speichern ablegen. Selbst mobile Mitarbeiter können unterwegs von ihren Mobilgeräten (einschließlich Smartphones und Tablet-PCs) auf verschlüsselte Daten zugreifen.

Mit Verschlüsselungslösungen können Sie Ihre vertraulichen Daten schützen und die gesetzlichen Vorgaben für die Datensicherheit einhalten.

Endpoint-Sicherheit

Endpoint-Sicherheitssoftware schützt Computer und andere Geräte vor zahlreichen Problemen in Sachen Sicherheit, Produktivität und Unternehmensrichtlinien. Sie ermöglicht die zentrale Verwaltung von Sicherheitslösungen auf verschiedenen Computern.

Endpoint-Sicherheitsprodukte fassen die einzelnen Produkte, die Sie zum Schutz vor modernen Bedrohungen benötigen, in einer Lösung zusammen. Sie integrieren den Schutz für mehrere Funktionen in einem Agenten oder in einer zentralen Konsole. Das vereinfacht Verwaltung und Berichterstattung. Endpoint-Sicherheitsprodukte können folgende Elemente beinhalten:

- Virenschutzsoftware
- Firewalls
- Device Control
- Network Access Control
- Application Control
- Laufzeitschutz
- Verschlüsselungstechnologie
- Websicherheit
- Patch Management
- Data Loss Prevention

Wir empfehlen den Einsatz von Endpoint-Sicherheitssoftware mit Funktionen zur Webinhaltsfilterung. Malware wird oftmals über Webseiten verbreitet. Erwägen Sie daher auch die Aktivierung der Sicherheitsfilterfunktionen in Ihrem Webbrowser.

Firewall

Firewalls prüfen Netzwerkzugriffe auf Computer oder Netzwerke und blockieren diese bei Bedarf.

Wie der Name schon andeutet, fungiert eine Firewall als Barriere zwischen Netzwerken oder Netzwerkbereichen. Sie blockiert schädlichen Datenverkehr und Hackerangriffe.

Eine Netzwerk-Firewall wird am Übergang zwischen zwei Netzwerken (in der Regel zwischen dem Internet und dem Unternehmensnetzwerk) installiert. Bei einer Firewall kann es sich um ein Hardware-Gerät handeln oder um Software, die auf einem Computer ausgeführt wird, der als Übergang zum Unternehmensnetzwerk arbeitet.

Eine Client-Firewall ist Software, die auf dem Computer eines Endbenutzers ausgeführt wird. Sie schützt nur dieses eine Gerät. Die Firewall untersucht den gesamten eingehenden und ausgehenden Datenverkehr und prüft diesen anhand bestimmter Kriterien. Werden bestimmte Kriterien erfüllt, wird der Datenverkehr zugelassen, andernfalls wird er blockiert.

Firewalls filtern Datenverkehr basierend auf folgenden Kriterien:

- Quell- und Zieladressen sowie Portnummern (Adressenfilterung)
- Art des Netzwerkverkehrs (zum Beispiel HTTP- oder FTP-Protokollfilterung)
- Attribute oder Status der gesendeten Informationspakete

Eine Client-Firewall kann den Benutzer warnen, wenn ein Programm versucht, eine Verbindung herzustellen. Der Benutzer kann entscheiden, ob er die Verbindung zulassen oder blockieren möchte. Aus den Antworten des Benutzers lernt die Firewall im Lauf der Zeit, welche Arten von Datenverkehr der Benutzer zulässt.

HTTPS-Scanning

Malware und sonstige Bedrohungen können sich im verschlüsselten Datenverkehr vertrauenswürdiger Webseiten verbergen. Beim HTTPS-Scanning werden diese Daten entschlüsselt, gescannt und wieder verschlüsselt.

Bei HTTPS-Scans werden schädliche Inhalte automatisch gefunden und entfernt, ohne dass jemand die Inhalte zu Gesicht bekommt. Auf diese Weise wird der Schutz des verschlüsselten Datenverkehrs garantiert.

IPS

Intrusion-Prevention-Systeme (IPS) überwachen Netzwerke und Systeme auf schädliche Aktivitäten.

IPS protokolliert Aktivitätsdaten und ist in der Lage, unerwünschte Aktivitäten zu blockieren und an die Netzwerkadministratoren zu melden, um Netzwerkinfektionen zu vermeiden.

IPsec

Mit IPsec wird jedes Internet-Protocol-Datenpaket (IP) einer Kommunikationssitzung authentifiziert und verschlüsselt.

IPsec ermöglicht die sichere Kommunikation über das eigentlich unsichere Internet Protocol (IP). Es beinhaltet unter anderem Protokolle, mit der sich Kommunikationspartner zu Beginn einer Sitzung authentifizieren, und tauscht den Schlüssel für die Chiffrierung der transportierten Daten aus.

Laufzeitschutz

Der Laufzeitschutz blockiert Zugriffsversuche auf gefährdete Bereiche Ihres Computers.

Der Laufzeitschutz analysiert das Verhalten aller auf dem Computer ausgeführten Programme und blockiert alle potenziell schädlichen Aktivitäten. Er überprüft beispielsweise an der Windows-Registrierung vorgenommene Änderungen. Diese könnten nämlich darauf hindeuten, dass sich Malware installiert, die dann beim Neustart des Computers automatisch gestartet wird.

Folgende Laufzeitschutzlösungen sind verfügbar:

Host Intrusion Prevention Systems (HIPS) überwachen das Verhalten von Code und stoppen Malware schon, bevor ein spezielles Erkennungs-Update zur Verfügung steht, das sie eindeutig identifiziert. Viele HIPS-Lösungen überwachen Code bei der Ausführung und schreiten ein, wenn der Code durch seine Aktivitäten als verdächtig oder schädlich eingestuft wird.

Buffer Overflow Prevention Systems (BOPS) erfassen Angriffe auf Sicherheitslücken sowohl in der Software des Betriebssystems als auch in Anwendungen. Sie registrieren den Versuch, einen laufenden Prozess mittels Pufferüberlaufmethoden zu missbrauchen, und melden ihn als Angriff.

Mobile Device Security

Mobile Geräte werden als Angriffsziel immer interessanter, je mehr wir mit ihnen Online-Banking und andere Transaktionen abwickeln.

Es wurde bereits Malware für Mobilgeräte beobachtet, die sich als eine Online-Banking-Anwendung tarnte und dem Zweck diente, Kunden- und Zugangsdaten zu stehlen, Authentifizierungstoken-Code über SMS abzufangen und Bankkonten zu plündern.

Der Conficker Working Group zufolge sind Smartphone-Viren immer noch relativ selten, während SMS-Attacken bereits zum Alltag gehören. Einige schädliche Apps senden automatisch SMS an Mehrwertdienste und verursachen so widerrechtlich hohe Gebühren. Vor allem Benutzer in Europa waren von Apps für SMS-Gebührenbetrug betroffen.

Verwaltungslösungen für mobile Geräte schützen Daten standort- und geräteunabhängig. Ihre Sicherheitslösung sollte verschiedene Mobilgeräte und Betriebssysteme unterstützen und deren Verwaltung über eine zentrale, webbasierte Konsole ermöglichen. Interessant ist auch die Möglichkeit, Ihre Daten mit einer Lösung zu schützen, die gestohlene oder verloren gegangene Geräte orten, sperren oder löschen kann.

Network Access Control (NAC)

Eine NAC-Lösung schützt das Netzwerk und die darin gespeicherten Daten vor Bedrohungen, die von seinen Benutzern oder angeschlossenen Geräten ausgehen.

NAC hat drei Hauptfunktionen:

- Authentifizierung von Benutzern und Geräten.
- Überprüfung von Computern, die versuchen, auf das Netzwerk zuzugreifen, um sicherzustellen, dass diese virenfrei sind und geltenden Sicherheitskriterien entsprechen.
- Durchsetzung von Richtlinien basierend auf den Benutzerrollen, so dass jeder Benutzer nur auf die seiner Rolle entsprechenden Daten zugreifen kann.

Reverse Proxy

Bei einem Reverse Proxy handelt es sich um einen Proxyserver, der im Auftrag eines Clients Ressourcen von anderen Servern abruft. Auf diese Weise bleibt nicht der Client, sondern der Zielserver im Verborgenen.

URL-Inhaltsfilterung

URL- oder Webinhaltsfilterung ist eine Technik, mit der Unternehmen Webseiten einzeln oder nach Themen blockieren können.

Hiermit können Sie verhindern, dass über das Unternehmensnetzwerk auf Webseiten zugegriffen wird, die der Produktivität schaden, illegal sind oder bekanntermaßen Malware verbreiten. Das erhöht die Produktivität und vermeidet Netzwerkinfektionen.

Unified Threat Management (UTM)

UTM kombiniert Schutzmechanismen für Netzwerk, Web, E-Mail und Computer (Endpoints) in einem Gateway und macht somit die Installation und Verwaltung mehrerer Einzellösungen überflüssig.

UTM-Lösungen verschaffen Ihnen vollständige Sicherheit für Ihr Netzwerk und jeden einzelnen Computer. Sie vereinfachen IT-Management-Aufgaben und schützen Sie vor Viren, Spam und Hackern. Somit bleiben Ihr Netzwerk und Ihre Daten vor Bedrohungen geschützt und zwar unabhängig davon, wo Ihre Mitarbeiter arbeiten, welche Geräte sie benutzen und von wo aus sie eine Verbindung herstellen.

VPN/SSL-VPN

Über ein Virtual Private Network (VPN) werden Remote-Standorte oder Remote-PCs an das zentrale Netzwerk angeschlossen.

Bei dieser Methode müssen sich die Benutzer typischerweise authentifizieren, indem sie Passwörter oder Schlüssel eingeben.

Web Application Firewall (WAF)

Hacker nutzen eine Reihe von Angriffsmethoden, um Ihre Webseite und Ihre Anwendungen still und heimlich auf Sicherheitslücken zu testen. Web Application Firewalls schützen Ihre Server, indem sie die Aktivitäten scannen und Angriffe erkennen.

Eine Web Application Firewall ist eine herkömmliche Firewall-Appliance, die jedoch zusätzlich Aufgaben übernimmt, die früher auf mehrere verschiedene Systeme verteilt waren. Dazu gehören zum Beispiel Inhaltsfilterung, Spamfilterung, Intrusion Detection und Virenschutz.

Eine All-in-One-Websicherheitslösung hat erhebliche Vorteile gegenüber kostspieligeren und komplexeren Webfilter-Lösungen, die sich auf eine einzige Funktionalität beschränken. Ein zentraler Steuerpunkt für den Webzugriff bietet folgende Vorteile:

Malwareschutz: Dämmen Sie von Malware, Spyware, Viren, Würmern und anderen Angriffen ausgehende Bedrohungen mit einer zuverlässigen ersten Schutzbarriere ein.

Kostenreduzierung: Reduzieren Sie IT-Verwaltungsaufgaben und vereinfachen Sie routinemäßige Wartungen und Updates durch eine zentral verwaltete Websicherheits-Appliance.

Legal Compliance: Sorgen Sie für die Einhaltung interner Richtlinien und rechtlicher Vorgaben, indem Sie den Zugriff auf unangemessene und illegale Webseiten blockieren.

Produktivitätssteigerung: Verhindern Sie, dass Mitarbeiter während der Arbeitszeit auf Webseiten zugreifen, die für die Arbeit nicht relevant sind. Reduzieren Sie gleichzeitig das Malware-Infektionsrisiko, das von bedenklichen Webseiten ausgeht. Damit unterbinden Sie auch netzwerkbelastende Aktivitäten wie Bitstreaming.

Web Application Control

Web Application Control blockiert Anwendungen wie P2P oder Instant Messaging, die rechtlich wie sicherheitstechnisch problematisch sind.

Unternehmenskritische Anwendungen wie Salesforce.com werden beschleunigt, indem ihnen ausreichend Bandbreite zur Verfügung gestellt wird. Unerwünschte, produktivitätsverringernde Anwendungen hingegen werden eingeschränkt oder blockiert (zum Beispiel Facebook-Spiele, P2P-Webseiten wie Bittorrent, YouTube-Streaming).

Wireless Security

Wireless Security verhindert den unautorisierten Zugriff auf bzw. die Schädigung von Computern in einem WLAN-Netzwerk.

Die gängigsten Formen von Wireless Security sind Wired Equivalent Privacy (WEP) und Wi-Fi Protected Access (WPA). WEP ist weniger sicher als WPA.

Sicherheits-tipps

So schützen Sie sich vor Viren, Trojanern, Würmern und Spyware

Installieren Sie Virenschutz- oder Endpoint-Sicherheitssoftware.

Installieren Sie auf allen Desktop-PCs und Servern eine Virenschutz- oder Endpoint-Sicherheitssoftware. Stellen Sie sicher, dass diese stets aktuell ist. Neue Malware kann sich extrem schnell verbreiten: Setzen Sie daher auf eine Infrastruktur, mit der Sie alle Computer in Ihrem Unternehmen kurzfristig, regelmäßig und einheitlich updaten können.

Setzen Sie an Ihrem E-Mail-Gateway eine E-Mail-Filterlösung ein, um Ihr Unternehmen vor Bedrohungen durch Viren, Spam und Spyware in E-Mails zu schützen.

Denken Sie beim Schutz auch an Laptops und Desktop-PCs von Mitarbeitern, die von zu Hause aus arbeiten. Viren, Würmer und Spyware können sich auch über diese Geräte leicht Zugang zu Ihrem Unternehmen verschaffen.

Blockieren Sie Dateiformate, die oft Malware enthalten.

Blockieren Sie ausführbare Dateien, denn es ist äußerst unwahrscheinlich, dass Ihr Unternehmen solche Dateitypen von extern zugeschickt bekommt.

Abonnieren Sie einen E-Mail-Benachrichtigungsservice.

Fügen Sie auf Ihrer Webseite oder in Ihrem Intranet gegebenenfalls einen Info-Feed über neue Malware hinzu. Benutzer wissen dann besser über aktuelle Bedrohungen Bescheid. Zuverlässige, aktuelle Informationen dazu finden Sie zum Beispiel im Blog Naked Security unter http://nakedsecurity.sophos.com.

Schützen Sie alle Computer mit einer Firewall.

Installieren Sie Firewalls, um die Computer eines Netzwerks auch voreinander zu schützen. Viele Würmer dringen über USB-Laufwerke, CDs und Mobilgeräte selbst in geschlossene Netzwerke ein. Schützen Sie zudem Laptops und Computer von Mitarbeitern, die von zu Hause aus arbeiten, durch eine Firewall.

Halten Sie Ihre Software-Patches immer auf dem neuesten Stand.

Spielen Sie vor allem bei Windows-Computern stets die automatischen Aktualisierungen (Updates, Patch-Aktualisierungen) ein. Sie schließen sehr häufig Sicherheitslücken, die Ihren Computer für Malware anfällig machen.

Sichern Sie Ihre Daten regelmäßig.

Erstellen Sie regelmäßig Sicherungskopien wichtiger Arbeitsdokumente und Daten. Prüfen Sie regelmäßig, ob deren Wiederherstellung einwandfrei funktioniert. Lagern Sie die Sicherungskopien an einem sicheren Ort, am besten außerhalb des Firmengeländes, damit sie auch bei einem Brand geschützt sind. Wenn Ihr Computer je mit einem Virus infiziert sein sollte, können Sie auf diese Weise verlorene Programme und Daten wiederherstellen. Die Sicherungskopien Ihrer vertraulichen Daten sollten verschlüsselt und zudem physisch geschützt werden.

Implementieren Sie Device Control.

Unterbinden Sie die Möglichkeit, nicht autorisierte Geräte an Ihre Computer anzuschließen. Geräte wie USB-Laufwerke, Musik-Player und Mobiltelefone können Malware enthalten, die bereits beim Anschließen den Computer infiziert.

Deaktivieren Sie die AutoRun-Funktion.

Im Februar 2011 hat Microsoft die automatische AutoRun-Funktion deaktiviert, damit sich Malware von Geräten wie USB-Laufwerken nicht auf Host-Computer und gemeinsam genutzte Netzlaufwerke kopieren kann.

So schützen Sie sich vor Hoaxes

Legen Sie eine Unternehmensrichtlinie für Virenwarnungen fest.

Erstellen Sie eine Unternehmensrichtlinie für Virenwarnungen. Solch eine Richtlinie könnte folgendermaßen aussehen:

> „Leiten Sie Virenwarnungen bitte nur an den Virenschutz-Verantwortlichen weiter. Es ist dabei unerheblich, ob die Virenwarnungen von einem Antiviren-Hersteller, von einem großen IT-Unternehmen oder von Ihrem besten Freund kommen. Virenwarnungen sollten ausschließlich an [Name des Verantwortlichen] gesendet werden. Es ist seine Aufgabe, Virenwarnungen an alle zu versenden. Ignorieren Sie bitte Virenwarnungen aus anderen Quellen."

Informieren Sie sich über Hoaxes.

Halten Sie sich stets über Hoaxes auf dem Laufenden. Informationen dazu finden Sie auf unserer Webseite unter www.sophos.com/security/hoaxes/.

Leiten Sie keine Kettenbriefe weiter.

Leiten Sie Kettenbriefe nicht an andere weiter, auch wenn Gewinne und Belohnungen winken oder die Informationen im Brief nützlich und wichtig erscheinen.

So sichern Sie Ihre Daten

Verschlüsseln Sie E-Mails, Computer und andere Geräte.

Die Verschlüsselung Ihrer Daten stellt sicher, dass nur autorisierte Benutzer mit dem passenden Schlüssel oder Passwort auf die gesicherten Informationen zugreifen können. Verschlüsseln Sie daher stets Ihre Daten. So sind sie immer geschützt – auch dann, wenn Laptops, CDs oder Geräte, auf denen Daten gespeichert sind, verloren gehen oder gestohlen werden oder wenn eine E-Mail mit wichtigen Daten abgefangen wird.

Setzen Sie Device und Application Control ein.

Verhindern Sie, dass Nutzer auf Tauschbörsen und USB-Laufwerke zugreifen. Auf diesen Wegen kommt es häufig zu Datenverlusten.

Erlauben Sie nur Computern Zugriff auf Ihr Netzwerk, die Ihre Sicherheitsrichtlinien erfüllen. Dazu können Anforderungen im Bereich Verschlüsselung oder Device und Application Control gehören.

Blockieren Sie den Mitarbeiterzugriff auf cloudbasierte Speicherdienste.

Richten Sie Kontrollmechanismen ein, mit denen Sie die Nutzung cloudbasierter Speicherdienste wie Dropbox überwachen oder blockieren. Diese Kontrollmechanismen sollten webbasierte URL-Filterung, Application Control und Datenverschlüsselung beinhalten. Indem Sie den Zugriff sperren, verhindern Sie die Übertragung von vertraulichen Daten auf weitgehend ungesicherte cloudbasierte Speicherdienste.

Implementieren Sie Inhaltskontrollen für ausgehende Daten.

Identifizieren Sie vertrauliche Daten, die Sie kontrollieren möchten, zum Beispiel alle Dateien, die den Begriff „vertraulich“ oder eine Kreditkartennummer enthalten. Entscheiden Sie dann, was passieren soll, wenn diese Daten auftauchen. Sie können zum Beispiel eine Warnung vor eventuellem Datenverlust einblenden oder die Weitergabe der Daten per E-Mail, in Blogs oder Foren blockieren.

Mit einer Verschlüsselungslösung können Benutzer sogar beliebige Online-Speicher-Dienste nutzen. Die Daten liegen dann außerhalb des Unternehmens nur verschlüsselt vor, die Schlüssel bleiben im Haus, der Client chiffriert die Daten vor der Synchronisierung. So behalten Sie die vollständige Kontrolle über die Sicherheit Ihrer Daten und müssen sich über Sicherheitslecks beim Anbieter des Online-Speichers keine Gedanken mehr machen.

Viele Endpoint-Sicherheitsprodukte sowie Email und Web Appliances bieten Inhaltsfilterung als Teil ihrer Lösung an.

So schützen Sie sich vor Spam

Statten Sie Ihr E-Mail-Gateway mit Software zur E-Mail-Filterung aus.

Setzen Sie an Ihrem E-Mail-Gateway Software zum Filtern von E-Mails ein. Sie schützt Ihr Unternehmen nicht nur vor Spam, sondern auch vor Spyware, Viren und Würmern, die sich per E-Mail verbreiten.

Kaufen Sie nie aufgrund einer unaufgefordert zugesandten E-Mail.

Jeder Kauf finanziert künftige Spam-Nachrichten. Außerdem besteht die reelle Gefahr, dass Ihre E-Mail-Adresse durch den Kauf auf spezielle Listen wandert und man sie an andere Spammer verkauft. Die Folge sind weitere Spam-Nachrichten. Sie könnten beim Kauf außerdem Opfer eines Betrugs werden.

Löschen Sie unaufgefordert zugesandte E-Mails, wenn Sie den Absender nicht kennen.

Die meisten Spam-Mails stören nur. Einige können jedoch auch Malware enthalten, die den Computer beim Öffnen der E-Mail schädigt oder manipuliert.

Verzichten Sie in Ihrer E-Mail-Anzeige auf die Vorschau-Funktion.

Viele Spammer können feststellen, wenn eine Nachricht angezeigt wird – auch dann, wenn Sie die E-Mail nicht anklicken. Denn schon die Vorschau öffnet die E-Mail und zeigt den Spammern dadurch an, dass die Nachricht zugestellt wurde. Versuchen Sie daher beim Abrufen Ihrer E-Mails schon anhand der Betreffzeile zu entscheiden, ob es sich um Spam handelt.

Geben Sie Ihre E-Mail-Adresse nicht zu bereitwillig heraus.

Wie oft Ihre E-Mail-Adresse im Internet auftaucht, bestimmt zu einem großen Teil darüber, wie viel Spam Sie erhalten. Auf folgende Arten machen Sie es Spammern leicht, an Ihre E-Mail-Adresse zu kommen:

- Nennung Ihrer E-Mail-Adresse im Fließtext auf Webseiten
- Gleiches gilt für Mailing-Listen, die online archiviert sind
- Bekanntgabe Ihrer E-Mail-Adresse an Online-Dienste mit fragwürdigen Datenschutzbestimmungen
- Veröffentlichung Ihrer E-Mail-Adresse in sozialen Netzwerken (zum Beispiel Facebook, LinkedIn)
- Übermäßige Verteilung von Visitenkarten
- Verwendung einer leicht zu erratenden E-Mail-Adresse aus Vorname, Nachname und Unternehmen
- Keine Trennung zwischen geschäftlicher und privater E-Mail-Adresse

Verwenden Sie das Feld BCC, wenn Sie an mehrere Personen gleichzeitig schreiben.

Das Feld BCC (Blindkopie) verbirgt die Liste der Empfänger vor anderen Benutzern. Wenn Sie die Adressen im Feld „An“ eingeben, können Spammer diese kopieren und sie zu ihren Mailing-Listen hinzufügen.

Veröffentlichen Sie Ihre E-Mail-Adresse niemals im Internet.

Geben Sie Ihre E-Mail-Adresse nicht auf Webseiten, in Newsgroups oder anderen öffentlichen Online-Foren an. Spammer besitzen spezielle Programme, um das Internet an solchen Stellen nach Adressen zu durchsuchen.

Geben Sie Ihre Hauptadresse nur an Personen weiter, denen Sie vertrauen.

Geben Sie die für Sie wichtigste E-Mail-Adresse ausschließlich Freunden und Kollegen.

Richten Sie ein oder zwei sekundäre E-Mail-Adressen ein.

Auf Web-Formularen im Internet, von denen Sie keine weiteren Informationen wünschen (zum Beispiel bei Umfragen), geben Sie die sekundäre E-Mail-Adresse ein. So schützen Sie Ihre Hauptadresse vor Spam.

Widersprechen Sie dem Erhalt weiterer Informationen oder Angebote.

Suchen Sie beim Ausfüllen von Formularen im Internet immer die Option zum Widerspruch gegen weitere Informationen oder Angebote. Aktivieren oder deaktivieren Sie diese Option entsprechend.

So schützen Sie sich vor Phishing

Antworten Sie niemals auf E-Mails, in denen Sie nach persönlichen Finanzdaten gefragt werden.

Seien Sie auf der Hut vor E-Mails, die nach Ihrem Passwort oder Ihren Kontodaten fragen oder entsprechende Links enthalten. Banken oder E-Commerce-Unternehmen versenden solche E-Mails normalerweise nicht.

Suchen Sie nach Anzeichen dafür, dass es sich um eine Phishing-E-Mail handelt.

Phishing-E-Mails sprechen ihre Empfänger ganz allgemein mit „Sehr geehrter Kunde" an, da es sich bei ihnen um Spam handelt und der Phisher Ihren Namen nicht kennt. Oft sind Behauptungen enthalten, die Sie erschrecken sollen, zum Beispiel dass Ihre Kontonummer verloren gegangen oder gestohlen worden sei. In den E-Mails tauchen oft falsche Schreibweisen auf und manche Buchstaben werden durch Zeichen ersetzt (z.B. „1nformati0n"). Das soll Spamschutzsoftware täuschen.

Geben Sie die Adresse von Webseiten von Banken immer manuell in die Adresszeile ein.

Klicken Sie nicht auf Links in E-Mails, die Sie nicht angefordert haben. Phisher wollen Sie damit zu einer gefälschten Webseite weiterleiten. Geben Sie stattdessen die komplette Adresse in die Adresszeile Ihres Browsers ein.

Prüfen Sie Ihre Konten regelmäßig.

Melden Sie sich regelmäßig bei Ihren Online-Bankkonten an und überprüfen Sie Ihre Kontoauszüge. Wenn Sie darauf verdächtige Transaktionen feststellen, melden Sie diese umgehend Ihrer Bank oder Ihrem Kreditkartenunternehmen.

Prüfen Sie, ob die besuchte Webseite sicher ist.

Prüfen Sie die Webadresse in der Adresszeile. Wenn sich die besuchte Webseite auf einem sicheren Server befindet, sollte die Adresse mit https:// („s" für Sicherheit) anstelle von http://

beginnen. Suchen Sie außerdem in der Statuszeile des Browsers nach einem Schloss-Symbol. Diese Anzeichen weisen darauf hin, dass die Webseite verschlüsselt ist.

Das heißt jedoch nicht zwangsläufig, dass die Webseite sicher ist, denn auch Hacker können verschlüsselte Webseiten erstellen, die jedoch zum Diebstahl persönlicher Daten ausgelegt sind.

Seien Sie vorsichtig im Umgang mit E-Mails und persönlichen Daten.

Führen Sie Transaktionen immer sicher durch. Teilen Sie niemandem Ihre PINs oder Passwörter mit, schreiben Sie diese nicht auf, und benutzen Sie auf keinen Fall ein und dasselbe Passwort für mehrere Online-Konten. Öffnen Sie keine Spam-Mails, und antworten Sie nicht darauf, da der Absender dadurch erfährt, dass Ihre E-Mail-Adresse gültig ist und sich für zukünftige Betrügereien eignet.

Schützen Sie Ihren Computer.

Spamschutzsoftware fängt zahlreiche Phishing-E-Mails ab; auf diese Weise erreichen diese erst gar nicht Ihren Posteingang. Auch eine Firewall trägt zum Schutz Ihrer persönlichen Daten bei und blockiert unerlaubte Kommunikation. Installieren Sie außerdem eine Virenschutzsoftware, um schädliche Programme zu erkennen und zu deaktivieren, beispielsweise Spyware oder Backdoor-Trojaner, die in Phishing-E-Mails enthalten sein können. Schützen Sie Ihren Browser stets mit den neuesten Sicherheits-Updates.

Melden Sie immer verdächtige Aktivitäten.

Wenn Sie eine E-Mail erhalten, die Sie für gefälscht halten, leiten Sie sie an das Unternehmen weiter, von dem sie angeblich kommt. Viele Unternehmen haben eine spezielle E-Mail-Adresse, an die solche Missbrauchsfälle gemeldet werden können.

So bewegen Sie sich sicher im Internet

In diesem Abschnitt erhalten Sie allgemeine Tipps zur sicheren Verwendung von Internet und E-Mails. Lesen Sie auch unsere Tipps in den Abschnitten „So schützen Sie sich vor Phishing“ und „So schützen Sie sich vor Viren, Trojanern, Würmern und Spyware“

Halten Sie Ihre Sicherheits-Updates immer auf dem neuesten Stand.

Um Computer zu infizieren, machen Hacker sich Sicherheitslücken in Betriebssystemen und Programmen zunutze. Informieren Sie sich über Sicherheits-Updates und Patches für Betriebssysteme, Browser, Plug-ins und andere Software, die das Ziel von Hackerangriffen sein könnte. Stellen Sie Ihren Computer möglichst so ein, dass er Sicherheits-Updates automatisch herunterlädt.

Schützen Sie sich mit Firewalls.

Eine in Ihrem Unternehmensnetzwerk installierte Netzwerk-Firewall lässt nur autorisierte Arten des Datenverkehrs zu. Eine Client-Firewall wird auf jedem Computer in Ihrem Netzwerk installiert und lässt ebenfalls nur autorisierten Datenverkehr zu. Das wehrt Hacker und Internetwürmer ab und verhindert, dass der Computer über nicht autorisierte Programme mit dem Internet kommuniziert.

Klicken Sie nicht auf Links in unerwarteten E-Mails.

Links in unerwarteten E-Mails leiten oft auf gefälschte Webseiten weiter. Dort werden die von Ihnen eingegebenen vertraulichen Informationen – etwa Kontonummern und Passwörter – unter Umständen gestohlen und missbraucht.

Darüber hinaus versuchen Hacker oft, Sie mit solchen Links direkt auf schädliche Webseiten zu leiten.

Nutzen Sie für jede Webseite ein anderes Passwort.

Verwenden Sie für jede Webseite, für die Sie ein Benutzerkonto haben, ein anderes Passwort. Wird ein Passwort entschlüsselt, so ist in diesem Fall nur ein einzelnes Konto betroffen. Stellen Sie darüber hinaus sicher, dass Ihre Passwörter schwer zu erraten sind. Nehmen Sie als Passwort niemals ein Wort, das in einem Nachschlagewerk zu finden ist.

Blockieren Sie gegebenenfalls den Zugriff auf bestimmte Webseiten oder Arten von Webinhalten.

In einer Unternehmensumgebung kann es sinnvoll sein, den Zugriff auf einige Webseiten zu blockieren. Das gilt für Seiten, die am Arbeitsplatz unangemessen oder anstößig sind oder die eine Sicherheitsbedrohung darstellen (zum Beispiel Spyware auf Computern installieren). Zu diesem Zweck gibt es Software-Webfilter und Hardware-Appliances. Auch wenn Nutzer befugt sind, Webseiten zu besuchen, sollten Sie sicherstellen, dass alle besuchten Webseiten auf Sicherheitsbedrohungen gescannt werden.

Prüfen Sie E-Mails auf Malware und Spam.

Virenschutzprogramme können unerwünschte E-Mails erkennen und daran hindern, in den Posteingang des Benutzers zu gelangen. Außerdem durchsuchen sie E-Mails nach darin enthaltener Malware.

Klicken Sie nicht auf Pop-up-Meldungen.

Treffen Sie auf Pop-up-Warnungen, wonach Ihr Computer infiziert sei und mit einer kostenlosen Virenentfernung gesäubert werden könne, dann klicken Sie keinesfalls auf Links oder Schaltflächen zum Herunterladen dieser Software. Es könnte dazu führen, dass Sie schädlichen Code herunterladen, beispielsweise gefälschte Virenschutzsoftware.

Gehen Sie per Router ins Internet.

Ein Router kann die Verbindungen zwischen dem Internet und bestimmten Computern begrenzen. Viele Router enthalten auch eine Netzwerk-Firewall.

So wählen Sie sichere Passwörter

Passwörter schützen Sie vor Betrug und dem Verlust vertraulicher Daten. Doch die wenigsten Benutzer wählen Passwörter, die wirklich sicher sind.

Wählen Sie möglichst lange Passwörter.

Je länger das Passwort ist, desto schwieriger lässt es sich erraten oder durch einen Brute-Force-Angriff entschlüsseln, der einfach alle möglichen Kombinationen durchprobiert. Passwörter mit mindestens 14 Zeichen lassen sich besonders schwer knacken.

Nutzen Sie verschiedene Zeichen.

Nutzen Sie die Möglichkeit, das Passwort mit Zahlen, Satzzeichen, Symbole und Buchstaben in Groß- und Kleinschreibung komplizierter zu machen. Auf Mobilgeräten, bei denen die Eingabe von Sonderzeichen nicht so einfach ist, bieten sich stattdessen längere Passwörter an.

Meiden Sie Wörter, die in einem Nachschlagewerk zu finden sind.

Verzichten Sie auf Wörter, Namen oder Ortsnamen, die in Nachschlagewerken zu finden sind. Hacker könnten mit einem Wörterbuchangriff versuchen, diese Passwörter automatisch zu knacken. Ein Wörterbuchangriff testet dazu einfach alle Wörter eines Nachschlagewerkes.

Beziehen Sie keine persönlichen Daten mit ein.

Ihr Geburtsdatum, der Namen Ihres Partners oder Kindes oder Ihre Telefonnummer sollten nicht im Passwort vorkommen. Alle Mitmenschen, denen diese Informationen bekannt sind, könnten so Ihr Passwort erraten.

Nutzen Sie nicht Ihren Benutzernamen.

Benutzernamen oder Kontonummern sind als Passwort ungeeignet.

Suchen Sie Passwörter, die bei der Eingabe schwer nachzuvollziehen sind.

Wiederholen Sie im Passwort nicht einfach mehrere Zeichen. Tabu sind auch Tastenfolgen oder Tasten, die auf der Tastatur nahe beieinander liegen.

Ziehen Sie eine Passphrase in Betracht.

Eine Passphrase ist eine Kombination aus mehreren Wörtern. Eine ungewöhnliche Aneinanderreihung von Wörtern ist schwer zu erraten.

Merken Sie sich Ihre Passwörter.

Merken Sie sich Ihr Passwort, schreiben Sie es nicht auf. Wählen Sie eine Zeichenfolge, die für Sie eine Bedeutung hat, oder denken Sie sich Eselsbrücken aus, um sich Ihr Passwort zu merken.

Kostenlose Programme unterstützen Sie bei der Verwaltung Ihrer Passwörter. Sie können Ihnen bei der Auswahl einzigartiger Passwörter helfen, die Passwörter verschlüsseln und sicher auf Ihrem Computer speichern. Beispiele dafür sind KeePass, RoboForm und 1Password.

Wenn Sie Ihre Passwörter aufschreiben, verwahren Sie sie an einem sicheren Ort.

Bewahren Sie Passwörter nicht in der Nähe Ihres Computers oder an einem einfach zugänglichen Ort auf.

Schützen Sie jedes Konto mit einem anderen Passwort.

Wenn ein Hacker eines Ihrer Passwörter knackt, betrifft dies dann wenigstens nur eines Ihrer Konten.

Geben Sie Passwörter nicht an andere weiter.

Gelegentlich erhalten Sie die Aufforderung, Ihr Passwort zu bestätigen. Folgen Sie solchen Anweisungen unter keinen Umständen, auch wenn sie scheinbar von einer vertrauenswürdigen Institution oder von jemandem aus Ihrem eigenen Unternehmen stammen (siehe Phishing).

Geben Sie Passwörter nie auf öffentlichen Computern ein.

Geben Sie Passwörter niemals auf einem öffentlich zugänglichen Computer ein, zum Beispiel in einem Hotel oder einem Internetcafé. Solche Computer sind nicht geschützt und es könnten Keylogger darauf installiert sein.

Ändern Sie Ihre Passwörter regelmäßig.

Je einfacher oder kürzer Ihr Passwort ist, desto öfter sollten Sie es ändern.

So verwenden Sie Wechseldatenträger sicher

Schulen Sie die Benutzer.

Nur wenige Benutzer kennen alle Gefahren, die von Wechseldatenträgern oder USB-Geräten und CDs ausgehen. Dazu gehören beispielsweise die Verbreitung von Malware oder mögliche Datenverluste. Eine Schulung kann das Bewusstsein für diese Gefahren stärken und die Risiken senken.

Identifizieren Sie Gerätetypen.

Computer kommunizieren mit immer mehr Wechseldatenträgern. Dazu gehören USB-Laufwerke und MP3-Player ebenso wie Smartphones. Legen Sie für diese Geräte geeignete Beschränkungen und Genehmigungen fest. Verschaffen Sie sich hierfür zunächst einen Überblick über die vorhandenen Wechseldatenträger und ihre Verbindungen zum Netzwerk.

Implementieren Sie Device Control.

Kontrollieren Sie, welche Wechseldatenträgertypen zulässig sind und welche Daten ausgetauscht werden dürfen. Das erhöht die Netzwerksicherheit. Wählen Sie ein Produkt, mit dem Sie Genehmigungen (und Beschränkungen) für einzelne Geräte bzw. ganze Geräteklassen festlegen können.

Verschlüsseln Sie Ihre Daten.

Datenverschlüsselung schützt vor Datenverlust. Dies gilt insbesondere für Wechseldatenträger, die man leicht verlieren kann und die gerne mal gestohlen werden. Dank Verschlüsselung können unautorisierte Dritte die Daten weder lesen noch kopieren.

So tätigen Sie sichere Online-Käufe

Können Sie Ihrem gesunden Menschenverstand und Ihrer Intuition vertrauen?

Leider ist es Benutzern in der Regel nicht möglich, mit bloßem Auge zu erkennen, ob eine Webseite sicher ist oder nicht.

Was Online-Kunden nicht sehen können: Webseiten, die sich nicht ausreichend gegen Manipulation geschützt haben, werden nicht selten von Hackern manipuliert. Nur weil es sich um ein großes, etabliertes Unternehmen handelt, bedeutet das also noch lange nicht, dass die Unternehmenswebseite sicher ist.

Führen Sie Online-Einkäufe nur auf sicheren Computern bzw. Geräten durch. Wenn neueste Virenschutzsoftware, Firewalls und Sicherheits-Updates installiert sind, sinkt die Gefahr, Opfer eines Hackers zu werden.

Klicken Sie nicht auf Links in Online-Nachrichten, die Sie unaufgefordert per E-Mail, Twitter oder Facebook erhalten. Spammer und Hacker nutzen hier Social-Engineering-Methoden, um Ihre Opfer auf betrügerische oder infizierte Webseiten zu locken.

Geben Sie vertrauliche Informationen wie persönliche Daten oder Finanzdaten nur weiter, wenn Sie von der Legitimität des Unternehmens vollständig überzeugt sind.

Kaufen Sie nur auf Webseiten mit sicherer Verbindung ein.

URLs, die mit https:// statt mit http:// beginnen (das „s“ steht für sicher), verschlüsseln Daten bei der Übertragung. Auch Webseiten, bei denen im Internetbrowser ein kleines Schloss-Symbol angezeigt wird, arbeiten mit Verschlüsselung.

Beides garantiert aber nicht, dass diese Webseiten wirklich sicher sind. Denn auch Hacker können Webseiten erstellen, die zwar eine sichere Verbindung aufbauen, aber dennoch nur den Diebstahl Ihrer persönlichen Daten zum Zweck haben.

Geben Sie möglichst wenig persönliche Daten weiter.

Füllen Sie optionale Felder wie zum Beispiel zweiter Vorname, Geburtsdatum, Handynummer, Hobbys und so weiter nicht aus. Viele Webseitenbetreiber fragen neben den für die Durchführung der Geschäftstransaktion nötigen Daten auch optionale Informationen ab. Pflichtfelder werden meist mit einem Sternchen gekennzeichnet.

Geben Sie niemals Passwörter weiter.

Auch wenn jemand anderes den Kauf für Sie tätigt, sollten Sie das Passwort immer selbst eingeben und nie an Dritte weitergeben. Wenn Sie den Computer nicht allein nutzen, verzichten Sie auf die Funktion zum Speichern des Passworts. So verhindern Sie, dass andere Benutzer ohne Ihre Zustimmung oder Ihr Wissen auf Ihr Benutzerkonto zugreifen.

Kaufen Sie möglichst im Inland.

Befindet sich ein Verkäufer im Ausland, ist es meist schwieriger und teurer, Probleme zu lösen oder Ihre Rechte als Käufer durchzusetzen.

Überprüfen Sie Ihre Kontoauszüge.

Überprüfen Sie regelmäßig Ihre Kontobewegungen, insbesondere, wenn Sie etwas über das Internet gekauft haben. Prüfen Sie, ob alle Zahlungen rechtmäßig sind. Wenn Sie Zahlungen entdecken, die Sie nicht zuordnen können, informieren Sie umgehend Ihre Bank.

Bewahren Sie Bestellbestätigungen und Rechnungen auf.

Bewahren Sie wichtige Unterlagen zu einem Kauf immer in gedruckter oder elektronischer Form auf. Sie können Ihnen später helfen, Probleme in Verbindung mit dem Kauf zu lösen.

So sorgen Sie für Sicherheit unterwegs

Klären Sie Ihre Benutzer auf.

Unterschätzen Sie die Risiken des Datenverlusts von ungeschützten Laptops oder Wechseldatenträgern nicht. Legen Sie als Unternehmen klare Richtlinien für die Nutzung von Mobilgeräten fest.

Nutzen Sie sichere Passwörter.

Passwörter sind die erste Barriere zum Schutz Ihrer Daten und sollten immer so stark wie möglich sein. (Lesen Sie hierzu auch den Abschnitt **So wählen Sie sichere Passwörter**)

Implementieren Sie zusätzliche Sicherheitsüberprüfungen.

Smartcards oder Tokens fordern für den Zugriff auf den Computer zusätzliche Informationen an, zum Beispiel Token-Codes in Verbindung mit Passwörtern. Bei biometrischen Lesegeräten müssen Sie Ihre Identität beim Starten oder Einloggen mit Ihrem Fingerabdruck bestätigen.

Verschlüsseln Sie alle wichtigen Daten.

Wenn Sie Ihre Daten stets verschlüsseln, sind diese auch auf Reisen sicher. Das gilt sogar dann, wenn Ihr Laptop oder Wechseldatenträger verloren geht oder gestohlen wird. Wenn Sie nicht Ihre gesamte Festplatte verschlüsseln möchten, erstellen Sie eine virtuelle Festplatte und speichern Sie Ihre vertraulichen Daten dort.

Schränken Sie Plug-and-play ein.

Im selben Augenblick, in dem Sie USB-Laufwerke, MP3-Player oder externe Festplatten an Laptops anschließen, sorgt die Plug-and-play-Funktion automatisch für eine Verbindung und erleichtert so das Kopieren von Daten. Sperren Sie stattdessen den Computer, so dass nur noch autorisierte Geräte eine Verbindung herstellen dürfen.

So sichern Sie Ihre mobilen Mitarbeiter ab

PDAs und Smartphones sind heute aus dem Geschäftsleben nicht mehr wegzudenken. Ihre Mitarbeiter speichern darauf vertrauliche Unternehmensdaten und verschicken E-Mails von unterwegs. Das macht sie für Angriffe von Malware-Autoren anfällig, denn diese suchen nach immer neuen Wegen, Benutzer zu betrügen und vertrauliche Unternehmensdaten zu stehlen.

Im Vergleich zur Malware-Flut auf Windows-Computern sind Viren und Spyware auf Mobilgeräten heute noch ein relativ kleines Problem. Dennoch wachsen die Risiken für die Kommunikation, Reputation und Handlungsfähigkeit einer Firma. Zu diesen Risiken zählt neben Datendiebstahl, dem Ausfall der Mobilfunkverbindungen und dem Mobilgeräte-Hijacking auch der heimliche Versand von SMS-Nachrichten an kostenpflichtige Mehrwertdienste. Die SophosLabs™ haben bereits über 30.000 Beispiele von schädlichem Code auf Mobilgeräten identifiziert.

Mobilgeräte können auf verschiedene Weise infiziert werden, zum Beispiel über E-Mails, MMS, externe Speicherkarten, PC-Synchronisation und sogar über Bluetooth.

Ihre Sicherheitsrichtlinien sollten unbedingt auch eine Strategie für Mobilgeräte bereithalten, die folgende Punkte berücksichtigt:

- Threat Management – Identifikation und Entfernung von Viren, Spyware und Spam
- Zugriffskontrolle und Verwaltung für Geräte – Durchsetzung einer Passwortrichtlinie sowie Application Management
- Datenschutz – Verschlüsselung vertraulicher Daten auf mobilen Geräten sowie Datenlöschung aus der Ferne
- Network Access Control – Kontrolle von VPN-Verbindungen in öffentlichen Netzwerken, Prüfung von Geräten, die sich mit dem Unternehmensnetzwerk verbinden

Sophos Mobile Control schützt kritische Unternehmensdaten und gewährleistet gleichzeitig die Produktivität der Benutzer. Mit dieser Software können IT-Administratoren ganz einfach einheitliche unternehmensweite Sicherheitsrichtlinien für mobile Geräte einführen und durchsetzen.

Die Geschichte der Malware

Wann wurden Viren, Trojaner und Würmer zur Bedrohung?

Für viele markiert der Brain-Virus von 1986 den Beginn der Virengeschichte, doch er war nur der erste Virus für einen Microsoft-PC. Schon deutlich vor ihm gab es Programme, die alle Merkmale von Viren aufweisen. Nachfolgend finden Sie einen Überblick über die Schlüsselmomente in der Geschichte der Viren.

1949 – Selbstreproduzierender „zellulärer Automat“

John von Neumann, der Begründer der Kybernetik, vertritt in einer Veröffentlichung die Ansicht, dass sich ein Computerprogramm selbst reproduzieren kann.

1959 – Core Wars

M. Douglas McIlroy, Victor Vysottsky und Robert P. Morris von den Bell Labs entwickeln ein Computerspiel mit dem Titel „Core Wars“. Programme, die Organismen genannt werden, wetteifern darin um die Rechenzeit des Computers.

1960 – Rabbit-Programme

Programmierer schreiben Platzhalter-Programme für Großrechner: Befindet sich kein Auftrag in der Warteschlange, fügen diese Programme am Ende der Schlange eine Kopie von sich selbst hinzu. Sie erhalten den Spitznamen „Rabbits“, da sie sich rasant vermehren und dabei Systemressourcen verbrauchen.

1971 – Der erste Wurm

Bob Thomas, einer der Entwickler des Internet-Vorläufers ARPANET, schreibt ein Programm namens „Creeper“. Es verbreitet sich sich von einem Computer auf den nächsten und zeigt eine Meldung an.

1975 – Replizierender Code

A. K. Dewdney schreibt die Subroutine „Pervade“ für ein Spiel, das auf Computern mit UNIVAC 1100 läuft. Sobald ein Benutzer das Spiel spielt, kopiert Pervade die aktuelle Version von sich selbst unbemerkt in jedes zugängliche Verzeichnis, einschließlich freigegebener Verzeichnisse. Es verbreitet sich somit im gesamten Netzwerk.

1978 – Der Vampire-Wurm

John Shoch und Jon Hupp von Xerox PARC experimentieren mit Würmern, die hilfreiche Aufgaben ausführen sollen. Der Vampire-Wurm ist am Tage inaktiv; nachts weist er nicht ausgelasteten Computern neue Aufgaben zu.

1981 – Der Apple-Virus

Joe Dellinger, ein Student der Texas A&M University, verändert das Betriebssystem auf Apple-II-Disketten so, dass es sich wie ein Virus verhält. Da der Virus unbeabsichtigte Nebenwirkungen hat, wird er nie veröffentlicht, allerdings geraten andere Versionen des Virus in Umlauf.

1982 – Der Apple-Virus mit Nebenwirkungen

Der 15-jährige Rich Skrenta schreibt den Virus „Elk Cloner“ für das Betriebssystem Apple II. Elk Cloner wird ausgeführt, wenn ein Computer von einer infizierten Diskette aus gestartet wird. Er infiziert alle Disketten, die danach in das Diskettenlaufwerk des betroffenen Computers eingelegt werden. Der Virus zeigt nach jedem 50. Start des Computers eine Meldung an.

1985 – E-Mail-Trojaner

Der Trojaner EGABTR wird über Posteingänge verbreitet und gibt sich als Programm zur verbesserten Grafikanzeige aus. Nachdem das Programm gestartet wird, löscht der Trojaner alle Dateien auf der Festplatte und zeigt eine Meldung an.

1986 – Der erste PC-Virus

Zwei Brüder in Pakistan schreiben „Brain“, den ersten Virus für IBM-PCs, weil sie bemerken, dass ihre Kunden ihre Software kopieren. Der Virus fügt sämtlichen Kopien, die Kunden auf Disketten erstellen, eine Kopie von sich selbst sowie eine Copyright-Meldung hinzu.

1987 – Der „Christmas Tree“-Wurm

Dabei handelt es sich um eine elektronische Weihnachtskarte mit Programmcode. Wenn der Benutzer sie öffnet, zeichnet dieser Code, wie versprochen, einen Weihnachtsbaum. Die Nachricht verschickt sich aber automatisch auch an alle Adressen im Adressbuch des Benutzers. Der daraus resultierende Datenfluss legt das weltweite IBM-Netz lahm.

1988 – Der Internet-Wurm

Der 23-jährige Student Robert Morris infiziert das US-DARPA-Internet mit einem Wurm. Aufgrund eines Programmierfehlers verbreitet er sich auf Tausenden von Computern und infiziert sie mehrfach, so dass sie abstürzen.

1989 – Trojaner verlangt Lösegeld

Der „AIDS"-Trojaner verbreitet sich über Disketten mit Informationen über AIDS und HIV und verschlüsselt die Festplatte des Computers. Im Namen seiner Hintermänner fordert er als Gegenleistung für das Passwort ein Lösegeld.

1991 – Der erste polymorphe Virus

„Tequila" ist der erste polymorphe Virus, der sich weit verbreitet. Virenscanner können polymorphe Viren nur schwer erkennen, da diese ihr Erscheinungsbild mit jeder neuen Infektion verändern.

1992 – Die Michelangelo-Panik

Der „Michelangelo"-Virus sollte jedes Jahr am 6. März (dem Geburtstag von Michelangelo) die Festplatten von Computern löschen. Nachdem zwei Unternehmen versehentlich infizierte Disketten und PCs in Umlauf bringen, bricht weltweit Panik aus. Nur wenige Computer sind wirklich infiziert.

1994 – Der erste E-Mail-Hoax

Der erste E-Mail-Hoax warnt vor einem Virus, der angeblich die komplette Festplatte löscht, wenn eine E-Mail mit dem Betreff „Good Times" geöffnet wird.

1995 – Der erste Dokument-Virus

„Concept" taucht auf – der erste Dokumenten- oder Makro-Virus. Er verbreitet sich, indem er sich die Makrofunktion in Microsoft Word zunutze macht.

1998 – Der erste Virus, der Hardware schädigt

„CIH" oder „Chernobyl" ist der erste Virus, der Computer-Hardware beschädigt. Der Virus manipuliert das BIOS, das für den Start des Computers wichtig ist.

1999 – E-Mail-Viren

„Melissa" verbreitet sich weltweit: ein Wurm, der sich selbst per E-Mail weiterleitet.

„Bubbleboy" ist der erste Virus, der einen Computer allein durch das Anzeigen einer E-Mail infiziert.

2000 – Denial-of-Service-Angriffe

Verteilte Denial-of-Service-Angriffe von Hackern führen dazu, dass bekannte Webseiten stundenlang offline sind, unter anderem Yahoo, eBay und Amazon.

„Love Bug" ist dabei der bisher erfolgreichste E-Mail-Virus.

2000 – Der Palm-Virus

Der erste Virus für das Palm-Betriebssystem wird gemeldet, er infiziert jedoch keine Geräte.

2001 – Viren verbreiten sich über Webseiten oder Netzwerkfreigaben

Schadprogramme nutzen Sicherheitslücken in Software aus, um sich dadurch ganz ohne Zutun des Benutzers verbreiten zu können. „Nimda" infiziert Computer von Benutzern bereits beim Zugriff auf eine Webseite. „Sircam" verbreitet sich über sein eigenes E-Mail-Programm sowie über Netzwerkfreigaben.

2004 – IRC Bots

Schädliche Bots nutzen das Chat-System IRC (Internet Relay Chat). Trojaner legen den Bot auf einem Computer ab, er verbindet sich danach ohne Wissen des Benutzers mit einem IRC-Kanal. Über diesen steuern Hacker den Computer des Opfers aus der Ferne.

2003 – Zombies und Phishing

Mithilfe des Wurms „Sobig" übernehmen Hacker die Kontrolle über Computer. Diese werden zu Zombies und lassen sich zum Versenden von Spam missbrauchen.

Der „Mimail"-Wurm gibt sich als E-Mail von PayPal aus und fordert Benutzer auf, ihre Kreditkartendaten zu bestätigen.

2005 – Rootkits

Durch den auf Musik-CDs von Sony enthaltenen DRM-Kopierschutz installiert sich ein Rootkit auf den Computern der Benutzer. Es verbirgt Dateien, damit diese nicht dupliziert werden können. Hacker entwickeln Trojaner, die das Rootkit ausnutzen und so eine versteckte „Hintertür" installieren.

2006 – Aktien-Betrügereien

Spam-Mails richten die Aufmerksamkeit der Empfänger auf Billig-Aktien kleiner Unternehmen (Pump-and-Dump-Spam), um deren Wert in die Höhe zu treiben.

2006 – Ransomware

Die Trojaner „Zippo" und „Archiveus" verschlüsseln Dateien des Benutzers, Cyberkriminelle erpressen mit ihrer Hilfe ein Lösegeld für das Passwort. Es sind erste Beispiele für Ransomware.

2006 – Der erste Advanced Persistent Threat (APT) wird identifiziert

Der Begriff wurde 2006 von der US Air Force geprägt und 2008 vom Sicherheitsunternehmen Mandiant in Alexandria (Virginia, USA) genauer definiert. APTs sind eine Gruppe raffinierter, entschlossener und koordinierter Angreifer. Sie haben sowohl die Fähigkeit als auch die Absicht, eine bestimmte Einrichtung dauerhaft und effektiv anzugreifen. Bekannte Angriffswege sind infizierte Medien, manipulierte Lieferketten und Social Engineering.

2008 – Gefälschte Virenschutzsoftware

Die Taktik einer höchst geschickten Verunsicherung bringt arglose Computerbenutzer dazu, gefälschte Virenschutzsoftware wie „AntiVirus 2008“ mit Kreditkarte zu bezahlen.

2008 – Erste iPhone-Malware

Das US Computer Emergency Response Team (US-CERT) gibt eine Warnung heraus: Ein gefälschtes iPhone-Upgrade namens „iPhone firmware 1.1.3 prep“ kursiert im Internet, Benutzer sollen es auf keinen Fall installieren. Wird der Trojaner installiert, werden andere Anwendungskomponenten abgeändert. Bei der Deinstallation des Trojaners werden die betroffenen Anwendungen unter Umständen auch entfernt.

2009 – Conficker macht Schlagzeilen

Der Wurm „Conficker“ infiziert Computer ohne Patches und sorgt weltweit für Medienrummel.

2009 – Polymorphe Viren treten erneut auf

Komplexe Viren treten wieder verstärkt auf, zum Beispiel „Scribble“, ein Virus, der sein Erscheinungsbild bei jeder Infizierung ändert und mehrere Angriffswege nutzt.

2009 – Erste Android-Malware

Der Trojaner „Android FakePlayerAndroid/FakePlayer.A“ sendet SMS-Nachrichten an Mehrwertdienste. Um Smartphones mit Android-Betriebssystem zu infizieren, tarnt er sich als herkömmliche Anwendung. Die Benutzer werden aufgefordert, eine etwa 13 KB große Datei mit der Standarderweiterung „.APK“ für die Anwendung zu installieren. Nach der Installation der App sendet der im Paket enthaltene Trojaner SMS an kostspielige Mehrwertdienste. Die Mehrwertdienste werden von Kriminellen betrieben, die ganz einfach die ungerechtfertigt erhobenen Gebühren ihrer Opfer kassieren.

2010 – Stuxnet

Der im Juni 2010 entdeckte Wurm „Stuxnet“ verbreitet sich zunächst willkürlich, enthält jedoch eine hoch spezialisierte Malware, die einzig auf SCADA-Systeme (Siemens Supervisory Control and Data Acquisition) ausgerichtet ist. SCADA-Systeme überwachen und steuern industrielle Prozesse. Experten vermuten, dass Uran-Anreicherungsanlagen im Iran eines der Hauptziele von Stuxnet sind.

2012 – Erste Drive-by-Android-Malware

Die erste Drive-by-Malware für Android wird entdeckt: Der Trojaner „NotCompatible“ gibt sich als Systemupdate aus, fungiert jedoch als Proxyserver-Umleitung. Die Webseite überprüft den User-Agent-String im Browser des Opfers, um zu bestätigen, dass es sich um ein Android-Gerät handelt, und installiert dann automatisch den Trojaner. Ein mit NotCompatible infiziertes Gerät könnte theoretisch auch auf geschützte Informationen oder Systeme von Unternehmen oder Regierungsorganisationen zugreifen.

Boston (USA) I Oxford (Großbritannien) | **www.sophos.de**

0000.de.08.12

SOPHOS