A bis Z

der Computersicherheit

SOPHOS

AbisZ

der Computersicherheit

Egal, ob Sie Netzwerkadministrator sind, im Büro am Computer arbeiten oder einfach nur E-Mails lesen - dieses Buch ist wie für Sie gemacht! Hier erfahren Sie alles Wissenswerte über Viren, Würmer, Spyware, Spam und vieles mehr – verständlich erklärt.

Sophos ist einer der weltweit führenden Anbieter von Integrated Threat Management-Lösungen für Unternehmen, das Bildungswesen und Behörden und schützt vor bekannter und unbekannter Malware, Spyware, Hackern, potentiell unerwünschten Anwendungen, Spam und Richtlinien-Missbrauch. Die verlässlichen und benutzerfreundlichen Produkte von Sophos schützen über 35 Millionen Anwender in mehr als 150 Ländern. Dank 20-jähriger Erfahrung und einem globalen Netz aus Bedrohungsanalysecentern reagiert Sophos rasch auf entstehende Bedrohungen, egal, wie komplex sie auch sein mögen und erreicht die größte Kundenzufriedenheit in der Branche.

ISBN 0-9553212-0-4
ISBN 978-0-9553212-0-7

Inhalt

Einleitung

Jeder weiß über Computerviren Bescheid, oder denkt jedenfalls, Bescheid zu wissen...

Vor mehr als 20 Jahren wurde der erste Computervirus geschrieben. Dieser gab vor, Software auf Disketten vor Bootleggers zu schützen. Seitdem wurden Hunderttausende von Viren und andere Malware geschrieben, darunter E-Mail-Viren, Trojaner, Internetwürmer und Viren zum Speichern von Tastenfolgen. Einige verbreiten sich weltweit und sorgen für Schlagzeilen. Die meisten Anwender haben bereits von Viren gehört, die willkürliche Meldungen auf dem Bildschirm anzeigen oder Dateien löschen. Die Meinung, dass Malware eine Art Streich oder Sabotage ist, ist ebenfalls weit verbreitet. In den 90ern sorgte der Virus **Michelangelo** weltweit für Panik, ist heutzutage jedoch längst vergessen. Im jetzigen Jahrzehnt wurden Millionen von Computern mit dem Virus **SoBig-F** infiziert und luden zu festgesetzten Zeiten unbekannte Programme aus dem Internet herunter. Antiviren-Anbieter versuchten, Internet Service Provider davon zu überzeugen, Server herunterzufahren, um absolutes Chaos wie am Tag des jüngsten Gerichts zu vermeiden. Spielfilme wie *Independence Day* und *Das Netz* verstärken diese Vorstellung noch, in denen sich Virenattacken durch blinkende Bildschirme und Alarme auszeichnen.

Die Wahrheit sieht jedoch ganz anders aus. Die Anzahl der Bedrohungen ist angestiegen, doch die Bedrohungen werden gut getarnt, gezielt eingesetzt und haben nicht das Ziel, Chaos zu verbreiten, sondern ihren Schöpfern schnell zu Geld zu verhelfen.

Heutzutage ist es äußerst unwahrscheinlich, dass Malware Ihre Festplatte löscht, Tabellen beschädigt oder Meldungen anzeigt. Diese Art des Internet-Vandalismus wurde durch gezielte Angriffe abgelöst, die unschuldigen Anwendern das Geld aus der Tasche ziehen. Ein heutiger Virus verschlüsselt beispielsweise Ihre Dateien und verlangt ein Lösegeld, um sie freizugeben. Oder ein Hacker erpresst ein großes Unternehmen, indem er mit einer Denial-of-Service-Attacke droht, die den Zugriff von Kunden auf die Unternehmens-Website verhindert.

Im Allgemeinen verursachen Viren jedoch keine sichtbaren Schäden und verschleiern ihre Präsenz. Stattdessen installiert ein Virus z.B. heimlich einen Key-Logger zum Speichern von Tastenfolgen, der wartet, bis der Anwender auf eine Online Banking-Website zugreift, dann Kennwort und Benutzernamen speichert und diese über das Internet an den Hacker weiterleitet. Der Hacker kann diese Daten dann verwenden, um Kreditkarten zu fälschen oder Bankkonten zu plündern. Das Opfer ist sich dabei gar nicht darüber bewusst, dass sein Computer infiziert wurde. Sobald der Virus Schaden auf dem infizierten Computer angerichtet hat, löscht er sich mitunter, um nicht entdeckt zu werden.

Eine andere Entwicklung im Bereich der Viren sind so genannte gemischte Bedrohungen, die verschiedene Arten von Malware und Hacking-Methoden vereinen. Ein Virenschreiber nutzt beispielsweise die Adressenliste eines Spammers, um einen Trojaner zu versenden. Dadurch stellt er sicher, dass ihn zahlreiche E-Mail-Benutzer innerhalb kurzer Zeit erhalten und das schädliche Programm aktivieren. Diese Methode hilft auch den Spammern. Viren und Trojaner können Computer in ferngesteuerte Zombies verwandeln, die die Spammer dann für die Verbreitung ihrer Spam-Mails verwenden, die das Ziel haben, Anwendern das Geld aus der Tasche zu ziehen.

Hacker greifen nicht einmal mehr zahlreiche Opfer auf einmal an. Der Grund dafür ist, dass solche groß angelegte Angriffe für unerwünschte Aufmerksamkeit sorgen und Antiviren-Hersteller rasch Schutz vor weit verbreiteter Malware erstellen können. Zudem erhalten Hacker durch groß angelegte Angriffe mehr gestohlene Daten, als sie nutzen können. Deshalb werden Bedrohungen nunmehr gezielter ausgeführt.

Spear Pishing ist ein Beispiel dafür. Ursprünglich verstand man unter "Phishing" die Versendung von Massenmails, die angeblich von Banken kamen und Kunden aufforderten, ihre vertraulichen Daten erneut zu registrieren. Diese Daten wurden dann gestohlen. Spear-Phishing dagegen beschränkt sich auf eine kleine Gruppe von Anwendern, normalerweise innerhalb eines Unternehmens. Die E-Mail gibt vor, von Kollegen aus anderen Abteilungen zu kommen, die nach Kennwörtern fragen. Das PrinzDialerist dasselbe, doch der Angriff ist ehr von Erfolg gekrönt, da die Opfer denken, dass es sich um eine interne E-Mail handelt und deshalb unvorsichtig handeln.

Getarnt, klein und zielgerichtet: Der Trend heutiger Sicherheitsbedrohungen.

Doch was wird die Zukunft bringen? Es ist beinahe unmöglich, die Entwicklung von Sicherheitsbedrohungen vorherzusagen. Einige Experten schätzten, dass es nie mehr als ein paar Hundert Viren geben würde und Bill Gates von Microsoft sagte, dass Spam 2006 kein Problem mehr darstellen würde. Wir wissen nicht, welche Bedrohungen uns in Zukunft erwarten oder wie ernst sie zu nehmen sein werden. Fest steht jedoch, dass Hacker und andere Cyber-Kriminelle weiterhin versuchen werden, unbefugten Zugriff auf Computer zu erlangen und Daten zu missbrauchen, solange sie sich einen finanziellen Nutzen daraus versprechen.


A-Z

Adware

Adware ist Software, die Werbung auf Ihrem Computer anzeigt.

Adware oder Advertising-supported Software zeigt Werbebanner oder Popup-Werbung auf Ihrem Computer an, sobald Sie die Anwendung benutzen. Dies ist nicht unbedingt schlecht. Solche Arten der Werbung können die Entwicklung nützlicher Software finanzieren, die dann kostenlos verteilt wird (z.B. der Webbrowser Opera).

Adware wird jedoch zu einem Problem, wenn sie:

- sich ohne Ihre Einwilligung auf Ihrem Computer installiert
- sich in anderen Anwendungen, als denen, in die sie integriert ist, installiert und Werbung anzeigt, sobald Sie diese Anwendungen benutzen
- die Steuerung über Ihren Browser übernimmt, um mehr Werbung anzuzeigen (siehe **Browser Hijacker**)
- unbefugt Daten sammelt, während Sie das Internet verwenden und sie über das Internet versendet (siehe **Spyware**)
- so ausgelegt ist, dass ihre Deinstallation schwierig ist.

Adware kann die Leistungsfähigkeit Ihres Computers einschränken. Sie kann auch Ihre Internetverbindung verlangsamen, indem sie Werbung herunterlädt. Aufgrund von Programmierungsfehlern in der Adware kann Ihr System instabil werden.

Popup-Werbung lenkt Sie ab und verschwendet Ihre Zeit, da Sie die Werbung oft erst schließen müssen, bevor Sie Ihren Computer weiter benutzen.

Einige Antiviren-Programme erkennen Adware und melden sie als potentiell unerwünschte Anwendungen. Sie können die Adware dann entweder erlauben oder von Ihrem Computer entfernen. Es gibt auch Programme speziell zur Erkennung von Adware.

Aktien-Scams

Spammer versenden Kauftipps, um den Preis für Aktien anzukurbeln, so dass sie gewinnbringend verkauft werden können.

Bei Aktien-Scams, auch bekannt als "Pump-and-Dump" Scams, werden Tipps über leistungsstarke Unternehmen per Massmailing versendet. Die Opfer werden ermutigt, die Aktien eines Unternehmens zu kaufen, so dass der Preis künstlich in die Höhe getrieben wird. Die Scammer verkaufen ihre Anteile dann gewinnbringend, bevor der Preis wieder sinkt.

Pump-and-Dump-Mails weisen die Merkmale von Spam auf. Es handelt sich um unerwünschte, kommerzielle E-Mails, die normalerweise von einem Zombie-Computer aus versendet werden, der von Hackern gesteuert wird. Diese E-Mails verwenden Verschleierungsmethoden, um nicht von Antispam-Software erkannt zu werden (die Betreffzeile lautet beispielsweise "Akt1e" anstatt "Aktie"). Diese E-Mails enthalten falsche Aussagen, können aber auch echte Informationen über das vorgestellte Unternehmen enthalten, um plausibler zu erscheinen.

Diese Scams schaden sowohl Investoren als auch kleinen Unternehmen. Sobald die Aktienpreise fallen, verlieren Investoren ihr Geld. Dieser Preisabfall kann für Unternehmen mit begrenzten Ressourcen verheerend sein.

Hier gilt dasselbe wie für andere Arten von Spam: Nicht kaufen, nicht ausprobieren, nicht antworten.

Backdoor-Trojaner

Ein Backdoor-Trojaner ist ein Programm, das einem Dritten über das Internet die Steuerung über den betroffenen Computer ermöglicht.

Ein Backdoor-Trojaner kann sich als legitime Software tarnen, wie andere Trojaner-Programme auch, so dass der Anwender ihn ahnungslos startet. Oft ist es auch der Fall, dass der Trojaner sich hinter einem Link in einer Spam-Mail versteckt und heruntergeladen wird, sobald der Anwender auf den Link klickt.

Sobald der Trojaner gestartet wird, fügt er sich zur Autostart-Routine des Computers hinzu. Er kann dann den Computer überwachen, bis der Anwender mit dem Internet verbunden ist. Sobald der Computer online ist, kann der Sender des Trojaners auf dem infizierten Computer Programme starten, auf persönliche Dateien zugreifen, Dateien verändern und hochladen, die von dem Anwender gedrückten Tasten nachverfolgen oder Spam-Mails versenden.

Zu bekannten Trojanern gehören **Subseven**, **BackOrifice** und der kürzlich aufgetretene **Graybird**, der als Patch für den berüchtigten **Blaster**-Wurm getarnt war.

Um Backdoor-Trojaner zu vermeiden, sollten Sie Ihren Computer durch die neuesten Patches schützen (um Betriebssystem-Schwachstellen zu schließen) und Antispam- und Antiviren-Software verwenden. Sie sollten zudem eine Firewall verwenden, die einen Trojaner davon abhält, auf das Internet zuzugreifen, um Kontakt mit dem Hacker aufzunehmen.

Bluejacking

Bluejacking bezeichnet das Versenden anonymer unerwünschter Nachrichten über Bluetooth-Mobiltelefone oder -Laptops an andere Anwender.

Bluejacking basiert auf der Fähigkeit von Bluetooth-Mobiltelefonen, in der Umgebung befindliche andere Bluetooth-Geräte zu kontaktieren. Der Bluejacker verwendet eine Funktion, die zum Austausch von Kontaktdaten und elektronischen Visitenkarten gedacht ist. Dabei fügt man einen neuen Eintrag in das Adressbuch des Mobiltelefons ein, schreibt eine Nachricht und versendet sie über Bluetooth. Das Mobiltelefon sucht dann nach anderen Bluetooth-Mobiltelefonen und versendet die Nachricht, sobald es ein anderes Bluetooth-Gerät findet.

Trotz seines alarmierenden Namens ist das Bluejacking im Wesentlichen harmlos. Der Bluejacker stiehlt keine vertraulichen Daten und übernimmt auch nicht die Steuerung über andere Mobiltelefone.

Bluejacking stellt erst dann ein Problem dar, wenn es zum Versenden von Werbung, obszönen Nachrichten oder Drohungen verwendet wird. Wenn Sie solche Nachrichten vermeiden möchten, können Sie Bluetooth deaktivieren oder die Einstellung "Unauffindbar" aktivieren.

Bluetooth-Geräte sind zudem dem Risiko des Bluesnarfing ausgesetzt.

Bluesnarfing

Mit Bluesnarfing wird der Diebstahl von Daten eines Bluetooth-Mobiltelefons bezeichnet.

Genau wie Bluejacking hängt Bluesnarfing von der Fähigkeit von Bluetooth-Geräten ab, andere Bluetooth-Geräte in der Umgebung zu erkennen und zu kontaktieren.

Theoretisch kann ein Bluetooth-Anwender, der auf seinem Laptop die entsprechende Software verwendet, Ihr Mobiltelefon in der näheren Umgebung erkennen, sich ohne Ihre Einwilligung damit verbinden und Ihr Adressbuch, Bilder Ihrer Kontakte und Ihren Kalender herunterladen.

Zudem kann die Seriennummer Ihres Mobiltelefons heruntergeladen und somit eine gefälschte Version Ihres Mobiltelefons erstellt werden.

Deaktivieren Sie Bluetooth oder wählen Sie die Einstellung "Unauffindbar". Dank dieser Einstellung können Sie Bluetoot-Geräte, wie Headsets, weiterhin verwenden, Ihr Mobiltelefon ist jedoch für andere Anwender nicht sichtbar.

Bootsektor-Viren

Bootsektor-Viren verbreiten sich, indem Sie das Programm verändern, das für den Start Ihres Computers verantwortlich ist.

Sobald Sie einen Computer anschalten, sucht die Hardware nach dem Bootsektor-Programm, das sich normalerweise auf der Festplatte befindet, aber mitunter auch auf einer Diskette oder CD zu finden ist, und führt es aus. Dieses Programm lädt dann das übrige Betriebssystem in den Speicher.

Ein Bootsektor-Virus ersetzt den originalen Bootsektor mit seiner eigenen, veränderten Version (und versteckt die Originalversion irgendwo auf der Festplatte). Wenn Sie Ihren Computer das nächste Mal starten, wird der infizierte Bootsektor verwendet und der Virus wird aktiv.

Ihr Computer kann nur infiziert werden, wenn Sie ihn von einer infizierten Diskette, z.B. einer Diskette mit infiziertem Bootsektor, starten.

Bootsektor-Viren sind der erste Virentyp, der auftrat und die meisten von ihnen sind inzwischen recht alt. Sie treten heutzutage nur noch selten auf.

Browser Hijacker

Browser Hijacker ändern die standardmäßige Homepage und Suchseite Ihres Internetbrowsers.

Einige Websites führen ein Skript aus, das die Einstellungen Ihres Browsers ohne Ihre Einwilligung verändert. Der Hijacker kann Shortcuts zu Ihren Favoriten hinzufügen oder sogar die erste Seite, die beim Start des Browsers geöffnet wird, verändern.

Es kommt mitunter vor, dass Sie die Startseite Ihres Browsers nicht mehr auf die von Ihnen eingestellte ändern können. Einige Hijacker verändern die Windows-Registry, so dass die von ihnen vorgenommenen Einstellungen jedes Mal wieder hergestellt werden, wenn Sie den Computer neu starten. Andere Hijacker entfernen Optionen von dem Menü 'Extras' Ihres Browsers, so dass Sie die von Ihnen gewählte Startseite nicht mehr einstellen können.

In jedem Fall wird damit ein und dieselbe Absicht verfolgt: Sie sollen eine bestimmte Website besuchen. Dadurch, dass die Website dann viele Besucher hat, erscheint sie bei Suchmaschinen vorne, so dass sie für Werbung interessant wird, wodurch ihre Macher Geld verdienen.

Browser Hijacker können äußerst resistent sein. Einige können durch Sicherheits-Software automatisch entfernt werden. Andere müssen manuell entfernt werden. Mitunter ist es sogar einfacher, einen früheren Status des Computers wiederherzustellen oder das Betriebssystem neu zu installieren.

Cookies

Cookies sind Dateien auf Ihrem Computer, die das Speichern Ihrer Daten auf Websites ermöglichen.

Wenn Sie eine Website besuchen, kann ein kleines Datenpaket, das Cookie genannt wird, auf Ihrem Computer abgelegt werden. Die Website kann dadurch Ihre Daten speichern und registrieren, wie oft Sie die Website besuchen. Cookies können Ihre Privatsphäre gefährden, stellen aber keine Gefahr für Ihre Daten dar.

Cookies wurden entwickelt, um den Internetgebrauch einfacher zu gestalten. Wenn Sie beispielsweise Ihren Benutzernamen auf einer Website eingeben, kann ein Cookie diesen speichern, so dass Sie ihn das nächste Mal nicht erneut eingeben müssen. Cookies sind auch für Webmaster hilfreich, da sie anzeigen, welche Websites gut besucht werden und somit hilfreiche Informationen für eine eventuell geplante Umgestaltung der Website bieten.

Bei Cookies handelt es sich um kleine Textdateien, die Ihre Daten nicht beschädigen. Allerdings gefährden sie Ihre Privatsphäre. Cookies können ohne Ihre Einwilligung oder Ihr Wissen auf Ihrem Computer gespeichert werden und enthalten Informationen über den jeweiligen Anwender, auf die Sie nicht unbedingt problemlos zugreifen können. Wenn Sie dieselbe Website erneut aufrufen, werden diese Daten ohne Ihre Einwilligung erneut an den Webserver gesendet.

Websites erstellen nach und nach ein Profil Ihrer Internetnutzung und Interessen. Diese Informationen können anderen Websites mitgeteilt oder an sie verkauft werden, so dass Werbung, die Ihren Interessen entspricht, auf verschiedenen, von Ihnen besuchten Websites angezeigt werden kann. Zudem wird erfasst, wie oft Sie eine bestimmte Werbung gesehen haben.

Wenn Sie lieber anonym bleiben möchten, können Sie Cookies über die Sicherheitseinstellungen Ihres Browsers deaktivieren.

Denial-of-Service-Attacke

Eine Denial-of-Service-Attacke (DoS) verhindert den Zugriff auf einen Computer oder eine Website.

Bei einer DoS-Attacke versucht ein Hacker, einen Computer zu überlasten oder herunterzufahren, so dass legitime Anwender keinen Zugriff mehr auf ihn haben. Normalerweise richten sich DoS-Attacken gegen Webserver und versuchen, den Zugriff auf Websites zu verhindern. Es werden keine Daten gestohlen oder beschädigt, doch solch eine Unterbrechung von Diensten kann ein Unternehmen teuer zu stehen kommen.

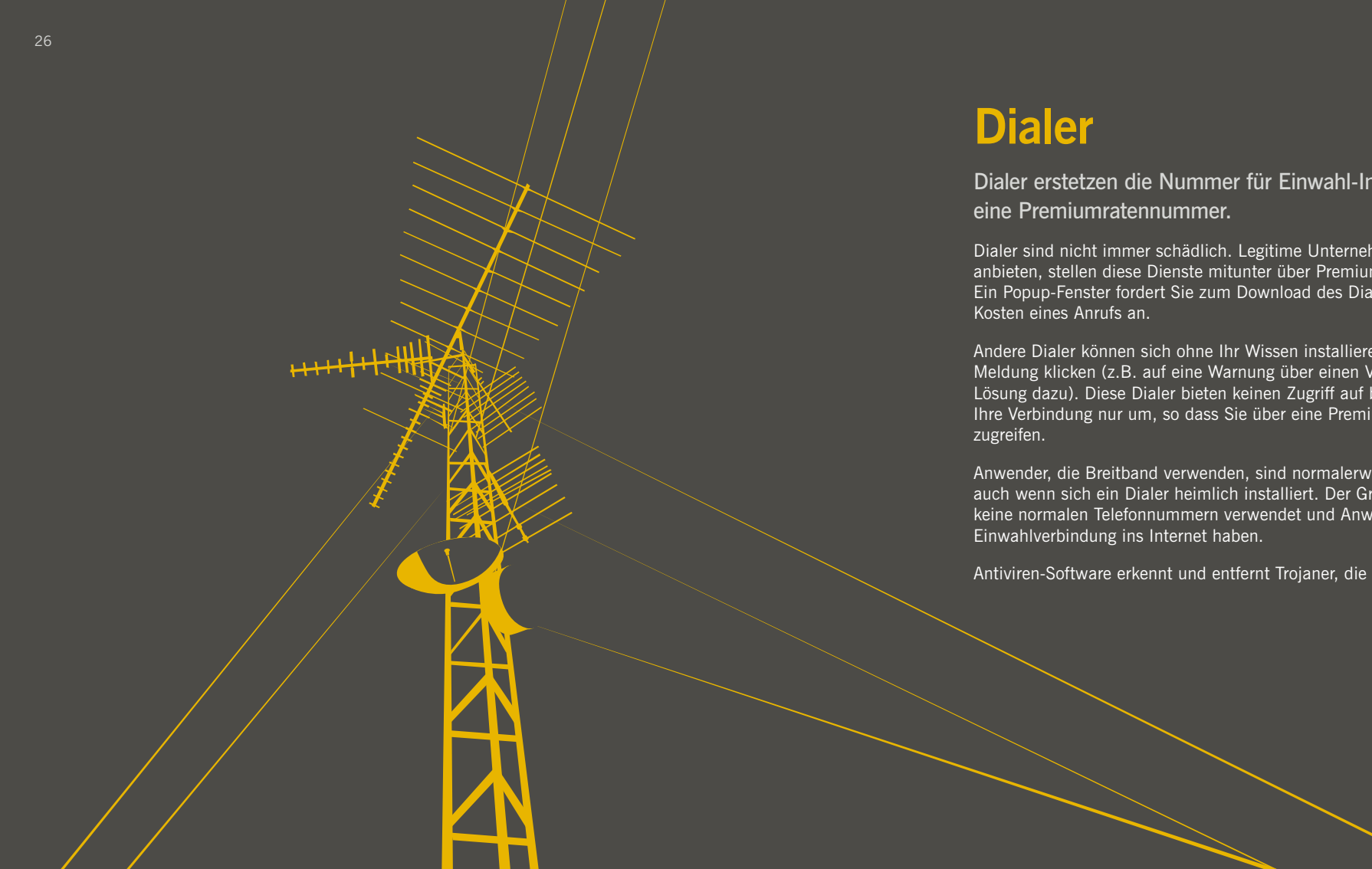
Eine häufig verwendete Art von DoS-Attacken ist die Überschwemmung eines Computers mit Daten, so dass er überlastet wird. Dies wird beispielsweise durch die Versendung übergroßer Datenpakete oder E-Mail-Attachments mit Dateinamen erreicht, die länger sind, als von E-Mail-Programmen erlaubt.

Eine Attacke kann auch die Art und Weise ausnutzen, auf die eine Kommunikationseinheit hergestellt wird, wenn der Anwender den Computer zum ersten Mal kontaktiert. Wenn der Hacker nacheinander zahlreiche Kommunikationsanfragen sendet und dann nicht auf die Antworten eingeht, werden diese Anforderungen eine zeitlang im Zwischenspeicher gelagert. Wirkliche Anfragen der Anwender können somit nicht bearbeitet werden und eine Kontaktaufnahme mit dem Computer ist nicht möglich.

Eine andere Methode besteht in der Versendung einer IP-ping-Nachricht (solch eine Nachricht erfordert eine Antwort von anderen Computern), die von dem Computer des Opfers zu kommen scheint. Die Nachricht wird an zahlreiche Computer versendet, die alle versuchen, zu antworten. Das Opfer wird mit Antworten überflutet, der Computer wird überlastet und ist nicht mehr in der Lage, mit echtem Datenfluss umzugehen.

Bei einer **Distributed-Denial-of-Service-Attacke** wird der Angriff von mehreren Computern aus gestartet. Normalerweise verwenden Hacker einen Virus oder Trojaner, um eine so genannte Backdoor auf fremden Computern zu öffnen, so dass sie die Steuerung über diese übernehmen können. Diese Zombie-Computer können zur Durchführung einer koordinierten Denial-of-Service-Attacke verwendet werden.

Siehe **Backdoor-Trojaner, Zombies.**



Dialer

Dialer erstetzen die Nummer für Einwahl-Internetverbindungen durch eine Premiumratennummer.

Dialer sind nicht immer schädlich. Legitime Unternehmen, die Downloads oder Spiele anbieten, stellen diese Dienste mitunter über Premiumratennummern zur Verfügung. Ein Popup-Fenster fordert Sie zum Download des Dialers auf und zeigt Ihnen die Kosten eines Anrufs an.

Andere Dialer können sich ohne Ihr Wissen installieren, sobald Sie auf eine Popup-Meldung klicken (z.B. auf eine Warnung über einen Virus auf Ihrem Computer und eine Lösung dazu). Diese Dialer bieten keinen Zugriff auf bestimmte Dienste, sondern leiten Ihre Verbindung nur um, so dass Sie über eine Premiumratennummer auf das Internet zugreifen.

Anwender, die Breitband verwenden, sind normalerweise vor Dialern geschützt, auch wenn sich ein Dialer heimlich installiert. Der Grund dafür ist, dass Breitband keine normalen Telefonnummern verwendet und Anwender kein Modem für die Einwahlverbindung ins Internet haben.

Antiviren-Software erkennt und entfernt Trojaner, die Dialer installieren.

E-Mail-Viren

Die meisten der gefährlichsten Viren verbreiten sich automatisch per E-Mail.

Typischerweise muss der Anwender bei E-Mail-fähigen Viren auf ein angehängtes Dokument klicken. Dadurch wird der schädliche Code ausgeführt, der sich dann von dem Computer aus an andere E-Mail-Empfänger versendet. Der Virus **Netsky** durchsucht Computer beispielsweise nach Dateien, die E-Mail-Adressen enthalten und versendet sich über den E-Mail-Client dieses Computers an diese Adressen. Einige Viren, wie **Sobig-F**, benötigen Ihren E-Mail-Client noch nicht einmal, da sie ihre eigene "SMTP Engine" für die Versendung von E-Mails enthalten.

Jeder Anhang, den Sie per E-Mail erhalten, könnte einen Virus in sich tragen. Wird der Anhang aufgerufen, kann Ihr Computer infiziert werden.

Auch ein Attachment mit einem scheinbar sicheren Dateityp, z.B. eine Datei mit einer .txt-Erweiterung, kann gefährlich sein. Bei dieser Datei kann es sich nämlich um ein schädliches VBS-Skript handeln, bei dem der tatsächliche Dateityp (.vbs) versteckt ist.

Einige Viren, wie **Kakworm** und **Bubbleboy**, infizieren Computer, sobald E-Mails gelesen werden, indem sie eine Schwachstelle des Betriebssystems oder E-Mail-Programms ausnutzen. Sie sehen aus wie jede andere E-Mail, enthalten aber ein verstecktes Skript, das startet, sobald Sie die E-Mail öffnen oder sie über eine Vorschau-Funktion ansehen (bei Outlook mit der entsprechenden Version des Internet Explorers). Dieses Skript kann Systemeinstellungen ändern und den Virus per E-Mail an andere Anwender senden.

E-Mail-Viren können die Sicherheit Ihres Computers beeinträchtigen oder Daten stehlen. Am häufigsten erzeugen sie jedoch eine Unmenge an E-Mail-Verkehr und verursachen Server-Abstürze.

Zum Schutz vor E-Mail-Viren sollten Sie Antiviren-Software verwenden und nicht auf unerwartete Attachments klicken. Installieren Sie zudem von Software-Herstellern zur Verfügung gestellte Patches, da diese Schwachstellen, die von E-Mail-basierten Viren ausgenutzt werden, zumeist schließen.

Internetwürmer

Würmer sind Programme, die sich kopieren und über Internetverbindungen verbreiten.

Würmer unterscheiden sich von Computerviren, da sie sich selbst verbreiten und kein Trägerprogramm oder -dateien erfordern. Sie erstellen exakte Kopien ihrer selbst und verbreiten sich über die Kommunikationenskanäle zwischen Computern.

Internetwürmer bewegen sich zwischen verbundenen Computern, indem sie Sicherheitslücken im Betriebssystem ausnutzen. Der **Blaster**-Wurm nutzt beispielsweise eine Schwachstelle in dem Dienst "Remote Procedure Call" auf Windows NT-, 2000- und XP-Computern aus, die nicht durch ein Patch geschützt sind und sendet eine Kopie von sich an einen anderen Computer.

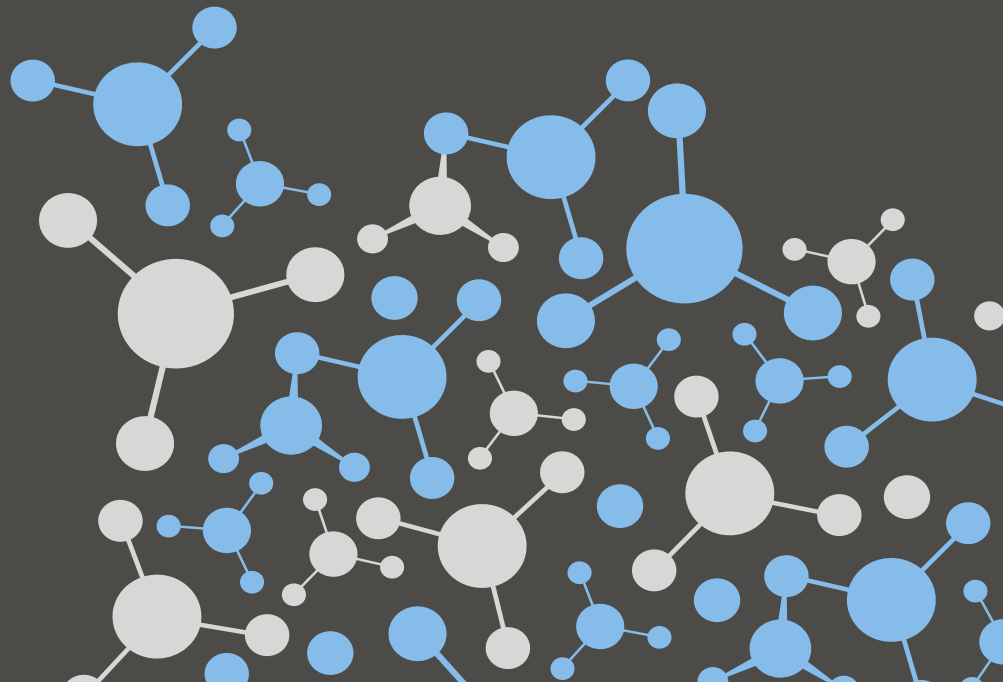
Würmer, wie z.B. **MyDoom** oder **Bagle**, gehören heute zu den häufigsten Schadprogrammen und leiten sich fast ausschließlich per E-Mail weiter.

Ein Wurm kann Schaden anrichten. Er kann beispielsweise infizierte Computer verwenden, um Websites mit Daten oder Anfragen zu überfluten, so dass sie abstürzen (Denial-of-Service-Attacke). Ein Wurm kann auch die Dateien eines Anwenders verschlüsseln, so dass er sie nicht mehr verwenden kann. Durch solche Aktionen können Unternehmen erpresst werden.

Viele Würmer öffnen eine Backdoor auf Computern, so dass Hacker die Steuerung über diese Computer übernehmen können. Diese Computer können dann zum Versenden von Spam verwendet werden (siehe **Zombie**).

Abgesehen von solchen Auswirkungen verlangsamt der Netzwerkverkehr, der von einem sich schnell verbreitenden Wurm verursacht wird, die Kommunikation enorm. Der **Blaster**-Wurm verursacht einen großen Datenfluss im Internet, sobald er sich verbreitet – das führt zu langsamen Verbindungen oder sogar zum Absturz von Computern. Später verwendet er den betroffenen Computer, um eine Microsoft-Website mit Daten zu überfluten, so dass der Zugriff auf diese Website nicht länger möglich ist.

Microsoft (und andere Betriebssystem-Hersteller) stellen Patches zur Verfügung, die Sicherheitslücken in ihrer Software schließen. Um Ihren Computer zu aktualisieren, sollten Sie regelmäßig die Website des Herstellers besuchen.



Kettenbriefe

Ein elektronischer Kettenbrief ist eine E-Mail, in der Sie aufgefordert werden, Kopien dieser E-Mail an andere Anwender weiterzuleiten.

Kettenbriefe, wie Viren-Hoaxes, verlassen sich auf den Anwender anstatt auf Computercode, um verbreitet zu werden. Zu den Hauptarten gehören:

- Hoaxes über Terrorangriffe, Scams zum Wählen von 0190-Nummern, Diebstähle von Geldautomaten usw.
- Gefälschte Angebote von Unternehmen zu kostenlosen Flügen, Mobiltelefonen oder Geldpreisen bei Weiterleitung der E-Mail.
- E-Mails, die vorgeben, von CIA und FBI zu kommen und über Schwerkriminelle in Ihrer Gegend warnen.
- Petitionen. Auch wenn sie echt sind, bleiben sie noch lange im Umlauf, wenn sie schon gar nicht mehr aktuell sind.
- Scherze und Streiche, beispielsweise die Ankündigung, dass das Internet am 1. April aufgrund von Wartungsarbeiten nicht zur Verfügung steht.

Kettenbriefe stellen keine Sicherheitsbedrohung dar, verschwenden jedoch die Zeit des Anwenders, verbreiten falsche Informationen und lenken die Anwender von wichtigen E-Mails ab.

Sie können unnötigen E-Mail-Verkehr erzeugen und E-Mail-Server verlangsamen. Manchmal fordern Kettenbriefe den Leser auf, E-Mails an bestimmte Adressen zu senden, so dass diese mit unerwünschten E-Mails überflutet werden.

Dem Problem durch Kettenbriefe kann man einfach entgegenwirken: Leiten Sie keine Kettenbriefe weiter.

Makroviren

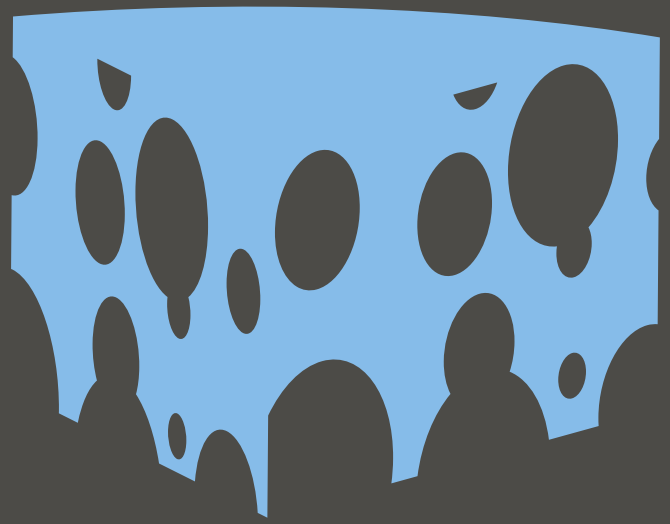
Makroviren nutzen Makros aus, d.h. Befehle, die in Dateien eingebettet sind und automatisch ausgeführt werden.

Zahlreiche Anwendungen, darunter Textverarbeitungs- und Tabellenkalkulationsprogramme verwenden Makros. Ein Makrovirus ist ein Makroprogramm, das sich kopieren und von einer Datei auf die andere verbreiten kann. Wenn Sie eine Datei öffnen, die einen Makrovirus enthält, kopiert sich der Virus in die Startdateien der Anwendung. Der Computer ist somit infiziert.

Wenn Sie das nächste Mal eine Datei mit derselben Anwendung öffnen, infiziert der Virus auch diese Datei. Befindet sich Ihr Computer in einem Netzwerk, kann sich die Infektion rasch verbreiten. Wenn Sie eine infizierte Datei an jemanden senden, kann der Computer dieses Anwenders ebenfalls infiziert werden. Ein schädliches Makro kann Änderungen an Ihren Dokumenten oder Einstellungen vornehmen.

Makroviren infizieren Dateien, die in den meisten Büros verwendet werden. Einige können verschiedene Dateitypen infizieren, beispielsweise Word- und Excel-Dateien. Sie verbreiten sich auf verschiedene Plattformen, je nachdem, auf welcher Plattform die Host-Anwendung ausgeführt wird.

Makroviren traten zum ersten Mal Mitte der 90er Jahre auf und wurden rasch zu den gefährlichsten Viren dieser Zeit. Mittlerweile treten diese Viren nur noch sehr selten auf.



Mousetrapping

Durch Mousetrapping werden Anwender am Verlassen einer Website gehindert.

Wenn Sie auf eine gefälschte Website umgeleitet werden, lässt sie sich möglicherweise nicht über die Zurück- oder Schließen-Schaltfläche schließen. In einigen Fällen ist es nicht einmal möglich, die Website durch Eingabe einer neuen Webadresse zu verlassen.

Wenn Sie durch Mousetrapping am Verlassen einer Website gehindert werden, können Sie entweder auf keine andere Website gehen oder es öffnet sich ein Fenster mit derselben Website. In manchen Fällen von Mousetrappings können Sie die Website nach einigen Versuchen verlassen, doch oft ist dies nicht möglich.

Um solch eine Website zu verlassen, verwenden Sie ein Lesezeichen oder Favoriten oder öffnen Sie die Liste kürzlich besuchter Websites und wählen Sie die vorletzte aus. Sie können auch die Tastenkombination Strg+Alt+Entf drücken und den Task-Manager verwenden, um den Browser zu schließen oder, falls dies auch nicht funktioniert, den Computer neu starten.

Um das Risiko durch Mousetrapping zu verringern, können Sie Java-Skript in Ihrem Browser deaktivieren. Somit können Sie durch Mousetrapping nicht auf Websites festgehalten werden, die dieses Skript verwenden, doch die Anzeige von Websites wird ebenfalls beeinträchtigt.

Page-Jacking

Page-Jacking bezeichnet die Nutzung von Kopien namhafter Websites, mit denen Anwender auf andere Websites umgeleitet werden sollen.

Scammer kopieren Seiten einer renommierten Website und stellen sie auf eine neue Website, die damit als legitim erscheint. Sie registrieren dann diese neue Website bei gängigen Suchmaschinen, so dass Anwender, die eine Suche starten, diese Website finden und auf den entsprechenden Link klicken. Wenn die Anwender dann auf die Website gelangen, werden sie automatisch auf eine andere Website umgeleitet, die Werbung anzeigt oder andere Dienstleistungen anbietet. Manchmal ist es nur durch einen Neustart des Computers möglich, diese Website zu verlassen (siehe **Mousetrapping**).

Scammer verwenden Page-Jacking, um den Zugriff auf eine Website zu erhöhen. Dadurch werden die Einnahmen aus Werbung für diese Website gesteigert und sie ist wertvoller, wenn sich die Scammer zu ihrem Verkauf entschließen. Scammer können Anwender auch auf eine andere Website umleiten und dafür eine Gebühr erheben.

Page-Jacking ist lästig und kann Anwender mit anstößigem Content konfrontieren. Außerdem wird so der Erfolg legitimer Websites reduziert, und Suchmaschinen sind weniger nützlich.

Manchmal wird Page-Jacking im Rahmen von **Phishing**-Attacken verwendet.

Um Page-Jacking zu vermeiden, können Sie ein Lesezeichen oder Favoriten verwenden (Sie müssen jedoch sicher sein, dass der Favorit auf keine Website verweist, bei der Page-Jacking angewandt wurde) oder geben Sie die gewünschte Adresse (URL) direkt ein.

Parasitäre Viren

Parasitäre Viren, oder Dateiviren verbreiten sich, indem sie sich an Programme anhängen.

Wenn Sie ein Programm starten, das mit einem parasitären Virus infiziert ist, wird schädlicher Code ausgeführt. Um sich zu tarnen, gibt der Virus die Steuerung dann wieder an das originale Programm ab.

Ihr Betriebssystem sieht den Virus als Teil des Programms an, das Sie ausführen wollten und gibt ihm dieselben Rechte. Dank dieser Rechte kann sich der Virus kopieren, im Speicher installieren oder Änderungen an Ihrem Computer vornehmen.

Parasitäre Viren traten zu Beginn des Aufkommens von Viren auf, können jedoch immer noch eine Bedrohung darstellen.

Pharming

Pharming leitet Sie von einer legitimen Website zu einer gefälschten Kopie um, so dass Kriminelle die von Ihnen eingegebenen Informationen stehlen können.

Pharming nutzt die Art und Weise der Zusammenstellung von Website-Adressen aus.

Jeder Computer im Internet hat eine numerische IP-Adresse, z.B. 127.0.0.1. Da diese Adressen jedoch nicht einfach zu merken sind, haben sie auch einen Domänennamen, beispielsweise sophos.com. Jedes Mal, wenn Sie eine Adresse eingeben, muss der Domänenname in die IP-Adresse umgewandelt werden. Dies geschieht über einen Domain Name Server (DNS-Server) im Internet, sofern die lokale Host-Datei auf Ihrem Computer die Umwandlung nicht bereits vorgenommen hat.

Hacker können diesen Prozess auf zweierlei Weisen untergraben. Sie können einen Trojaner versenden, der die lokale Host-Datei auf Ihrem Computer überschreibt, so dass der Domänenname mit der gefälschten Website in Verbindung gebracht wird. Sie werden dann auf die gefälschte Website geleitet, auch wenn Sie die korrekte Adresse eingegeben haben. Hacker können auch das DNS-Verzeichnis verändern, so dass jeder Anwender, der versucht, auf die Adresse zuzugreifen, auf die gefälschte Website umgeleitet wird.

Um zu vermeiden, Pharming zum Opfer zu fallen, verwenden Sie sichere Internetverbindungen, wenn Sie auf Websites zugreifen, die sensible Daten enthalten. Achten Sie darauf, dass die Webadresse mit https:// beginnt. Versucht ein Hacker, vorzugeben, dass Sie sich auf einer sicheren Website befinden, werden Sie durch eine Meldung gewarnt, dass das Zertifikat der Website nicht mit der besuchten Adresse übereinstimmt.

Erscheint eine Warnung, dass das Zertifikat der Website nicht gültig ist oder nicht von einer vertrauenswürdigen Stelle ausgestellt wurde, sollten Sie die Website nicht öffnen.

Dafür gibt es auch Software-Lösungen. Manche Software zeigt eine Warnung an, wenn Sie als Antwort auf eine unbekannte E-Mail-Adresse persönliche Daten eingeben. Es gibt zudem Dienstprogramme, die überprüfen, ob Websites oder IP-Adressen sich auf der Blacklist befinden.

Phishing

Beim Phishing werden Anwender mit gefälschten E-Mails und Websites dazu gebracht, vertrauliche und persönliche Daten preiszugeben.

Typischerweise erhalten Sie eine E-Mail, die scheinbar von einem renommierten Unternehmen stammt, wie z.B. einer Bank. In der E-Mail ist ein Link enthalten, der scheinbar auf die Website des Unternehmens führt. Wenn Sie dem Link jedoch folgen, werden Sie mit der Replik der Website verbunden. Alle Daten, die Sie dann eingeben, wie z.B. Kontonummern, PINs oder Kennwörter, können von den Hackern, die die gefälschte Website erstellt haben, gestohlen und benutzt werden.

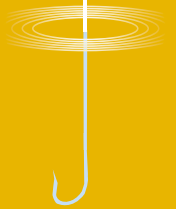
Manchmal führt der Link zu der wirklichen Website, zeigt jedoch ein gefälschtes Popup-Fenster an. Sie können die Adresse der wirklichen Website im Hintergrund sehen, doch Daten, die Sie in dem Popup-Fenster eingeben, können gestohlen werden.

Mitunter verwenden Hacker auch eine Methode namens "Cross-Site Scripting": Der Link führt zwar zur wirklichen Website, untergräbt sie aber, indem fremder Inhalt hinzugefügt wird. Auch hier wird der Bereich, in dem Sie Informationen eingeben, von den Hackern gesteuert.

Phishing begann in den 90ern und Scammer verwendeten diese Methode zum Stehlen von AOL-Kontendetails zum kostenlosen Internetzugriff. Diese Daten werden als "Phish" bezeichnet, da Sie gestohlen werden, indem der Scammer nach Anwendern "fischt". Durch die Verwendung des "ph" wird die Schreibweise "Phreaker" nachempfunden. Dieser Ausdruck bezeichnet Hacker, die sich Zugang zum Telefonnetz schaffen.

Seien Sie bei E-Mails bei allgemeinen Anreden, wie z.B. "Sehr geehrte Kunden" sowie bei in der E-Mail enthaltenen Links stets vorsichtig. Geben Sie stattdessen die Adresse der Website manuell ein oder verwenden Sie ein Lesezeichen/einen Favoriten. Auch wenn Sie die Adresse manuell eingeben, besteht das Risiko, dass Sie auf die gefälschte Website umgeleitet werden (siehe **Pharming**), so dass Sie stets Vorsicht walten lassen sollten.

Antispam-Software kann viele Phishing-E-Mails blockieren. Es gibt Software, die Phishing-Inhalte auf Websites oder in E-Mails erkennt und sie stellt eine Toolbar zur Verfügung, die die wirkliche Domäne der Website anzeigt, deren Link Sie folgen.



Potentiell unerwünschte Anwendungen (PUAs)

Potentiell unerwünschte Anwendungen sind Programme, die nicht zwangsläufig schädlich sind, für Unternehmensnetzwerke jedoch als ungeeignet angesehen werden.

Einige Anwendungen sind nicht schädlich und unter bestimmten Umständen sogar nützlich, jedoch nicht für Unternehmensnetzwerke. Beispiele dafür sind Adware, Dialer, nicht-schädliche Spyware, Tools für die Remote-Verwaltung von PCs und Hacking-Tools.

Manche Antiviren-Programme erkennen solche Anwendungen auf Computern und melden sie. Der Administrator kann diese Anwendungen dann entweder erlauben oder entfernen.

Ransomware

Bei Ransomware handelt es sich um Software, die Ihnen den Zugriff auf Ihre Dateien untersagt, bis Sie Lösegeld bezahlen.

In der Vergangenheit wurden Daten von Schadprogrammen z.B. beschädigt oder gelöscht, heute werden Daten jedoch meistens verschlüsselt und nicht mehr freigegeben. Der Trojaner **Archiveus** kopiert den Inhalt von "Eigene Dateien" beispielsweise in eine Kennwort-geschützte Datei und löscht die Originaldateien. Sie erhalten eine Meldung, dass Sie ein 30-stelliges Kennwort benötigen, um Zugriff auf den Ordner zu erhalten und dass Ihnen das Kennwort zugesandt wird, sobald Sie etwas von einer Online-Apotheke kaufen.

In diesem Fall, wie auch in der Mehrzahl der Fälle von Ransomware, befindet sich das Kennwort oder der Schlüssel im Code des Trojaners und kann von Virenanalysten ermittelt werden. In Zukunft kann es jedoch sein, dass Hacker die asymmetrische oder Public Key-Verschlüsselung verwenden, um Daten zu verschlüsseln, jedoch eine andere Entschlüsselung, so dass das Kennwort nicht auf Ihrem Computer gespeichert wird.

In einigen Fällen ist die Drohung der Zugriffsverweigerung bereits ausreichend. Der Trojaner **Ransom-A** droht beispielsweise damit, alle 30 Minuten eine Datei zu löschen, bis Sie über Western Union für einen Entschlüsselungscode bezahlen. Der Trojaner warnt davor, dass der Computer nach drei Tagen abstürzt, wenn Sie einen falschen Entschlüsslungscode eingeben. Diese Drohung ist jedoch ein Bluff, da **Ransom-A** nicht in der Lage ist, seine Drohung umzusetzen.

Rootkit

Ein Rootkit ist Software, die Programme oder Prozesse auf einem Computer versteckt. Rootkits werden oft verwendet, um den Missbrauch des Computers zu schädlichen Zwecken oder Datendiebstahl zu verschleiern.

Wenn schädliche Software, beispielsweise ein Internetwurm, Zugriff auf Ihren Computer erhält, wird mitunter ein Rootkit installiert. Damit wird die Präsenz von Dienstprogrammen verborgen, die einem Hacker das Öffnen einer Backdoor ermöglichen, über die der Zugriff auf den Computer möglich ist. Diese verborgenen Dienstprogramme können dem Hacker auch Rechte zur Ausführung von Funktionen geben, für die normalerweise Sonderrechte erforderlich sind. (Auf UNIX- und Linux-Computern werden solche Anwender "Root" genannt, daher die Bezeichnung "Rootkit").

Ein Rootkit kann Trojaner zum Speichern von Tastenfolgen oder Kennwort-Sniffern verbergen, die vertrauliche Daten stehen und über das Internet an Hacker senden. Zudem ermöglicht ein Rootkit einem Hacker, den Computer für illegale Zwecke zu verwenden, z.B. für Denial-of-Service-Attacken auf andere Computer oder zum Versenden von Spam, ohne Wissen des Benutzers.

Auch wenn ein Rootkit nicht mit schädlicher Absicht installiert wird (wie im Falle des Digital Rights Management von Sony, das Rootkits zur Vermeidung von Musik-Piraterie installierte), kann ein Computer dadurch anfällig für Hacker werden.

Es ist schwierig, Rootkits zu entdecken. Sobald ein Rootkit auf einem Computer ausgeführt wird, können Sie weder alle laufenden Prozesse noch alle Dateien in einem Verzeichnis auf diesem Computer erkennen. Aus diesem Grund erkennt traditionelle Antiviren-Software Rootkits nicht immer. Rootkits können ihre Aktivitäten auch einstellen, bis die Antiviren-Software die Überprüfung des Computers abgeschlossen hat. Um das Rootkit auch wirklich zu finden, müssen Sie Ihren Computer herunterfahren, von einer Notfall-CD aus starten und ihn dann mithilfe von Antiviren-Software überprüfen. Da das Rootkit nicht ausgeführt wird, kann es sich auch nicht verbergen.

Antiviren-Programme können die Trojaner oder Würmer erkennen, die normalerweise Rootkits installieren, und einige Programme erkennen auch das Rootkit selbst, während es ausgeführt wird.

Spam

Spam sind nicht angeforderte kommerzielle E-Mails, das elektronische Äquivalent zur Werbepost in Ihrem Briefkasten.

Die meisten Spam-Mails bieten Folgendes an:

- verschreibungspflichtige Medikamente, Medikamente zum Vergrößern oder Verschönern von Körperteilen, Kräutermittel oder Medikamente zur Gewichtsabnahme
- Möglichkeiten, schnell an viel Geld zu gelangen
- Finanzdienstleistungen, z.B. Hypotheken oder Schuldenabbau
- Qualifikationen, z.B. Universitätsabschlüsse oder Berufsbezeichnungen gegen Bezahlung
- Online-Glücksspiele
- reduzierte Software oder Raubkopien

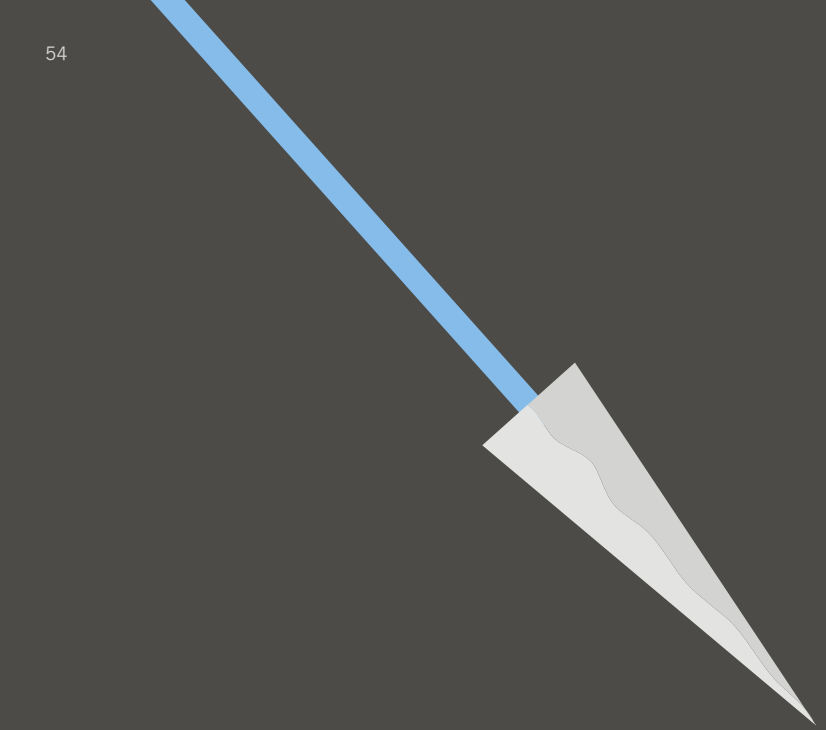
Spam kann sich tarnen, beispielsweise mit einer Betreffzeile, die wie eine persönliche E-Mail klingt, z.B. "Sorry about yesterday", wie eine Geschäfts-E-Mail, z.B. "Your account renewal now due" oder eine Nicht-Zustellbar-Nachricht.

Spammer tarnen ihre E-Mails oft, um Antispam-Software zu täuschen (siehe **Verschleierte Spam-Mails**).

Spam wird versendet, weil es sich lohnt. Spammer senden Millionen E-Mails im Rahmen einer einzigen Kampagne zu geringen Kosten (und wenn sie die Computer Dritter zum Versenden von E-Mails missbrauchen, sinken die Kosten noch mehr). Wenn auch nur ein Empfänger von Tausend eine Bestellung aufgibt, verzeichnet der Spammer einen Gewinn.

Ist Spam gefährlich?

- Spam vergeudet die Zeit der Mitarbeiter. Anwender ohne Spamschutz müssen prüfen, welche E-Mails Spam sind und diese dann löschen.
- Nutzer können schnell wichtige E-Mails übersehen oder sogar löschen, weil sie sie mit Spam verwechseln.
- Spam, Hoaxes und E-Mail-Viren, verschwendet Bandbreite und verstopft Datenbanken.
- Manche Spam-Mails sind anstößig. Arbeitgeber können zur Verantwortung gezogen werden, da sie für eine sichere Arbeitsumgebung Sorge tragen.
- Spammer verwenden zum Versenden von Spam oft Computer Dritter (siehe **Zombies**).



Spear-Phishing

Mit Spear-Phishing wird die Verwendung von gefälschten, internen E-Mails bezeichnet, um Mitarbeiter eines Unternehmens zur Angabe ihrer Benutzernamen und Kennwörter zu veranlassen.

Im Gegensatz zum **Phishing**, das auf Massen-E-Mails beruht, richtet sich Spear-Phishing gezielt auf eine kleine Benutzergruppe. Ein Spear Phisher versendet E-Mails an Benutzer eines einzigen Unternehmens. Die E-Mails scheinen von einem anderen Mitarbeiter desselben Unternehmens zu stammen und bitten die Empfänger, ihren Benutzernamen und ihr Kennwort zu bestätigen. Normalerweise geben solche E-Mails vor, von einer vertrauenswürdigen Abteilung zu stammen, bei der man sich vorstellen kann, dass sie solche Informationen benötigt, beispielsweise IT oder die Personalabteilung. Manchmal werden Mitarbeiter auf eine gefälschte Website des Unternehmens oder eine gefälschte Intranet-Seite umgeleitet. Antworten Sie auf eine solche E-Mail, erhält der Phisher ihre vertraulichen Daten und kann sie für schädliche Zwecke verwenden.

Der Spear Phisher kann die Adressen der Opfer anhand von Spammer-Software erstellen, die beispielsweise Vor- und Nachnamen miteinander kombiniert. Da die E-Mails alle an dieselbe Domäne gesendet werden, ist die Chance gering, dass sie als Spam erkannt werden.

Spoofing

Spoofing bezeichnet das Versenden von E-Mails, die von einem bestimmten Sender zu kommen scheinen, jedoch in Wirklichkeit von einem anderen gesendet werden.

Erlaubt der E-Mail-Server Verbindungen zu einem SMTP-Port, so kann sich jeder mit diesem Port verbinden und E-Mails versenden, die von diesem Server zu kommen scheinen. Bei der Adresse kann es sich entweder um eine wirkliche oder um eine fiktive Adresse handeln. Dies wird als "Spoofing" bezeichnet.

Spoofing kann für verschiedene schädliche Zwecke verwendet werden.

Phisher, also Kriminelle die versuchen, Anwender zur Angabe vertraulicher Informationen zu bringen, verwenden gefälschte (Spoof) Sender-Adressen, so dass E-Mails von einer vertrauenswürdigen Quelle zu kommen scheinen, beispielsweise von Ihrer Bank. Die E-Mail kann einen Link enthalten, der Sie zu einer gefälschten Website führt (z.B. der imitierten Website einer Bank), von der Ihre Daten und Ihre Kennwörter gestohlen werden können.

Phisher können auch E-Mails versenden, bei denen es sich scheinbar um interne E-Mails Ihres Unternehmens handelt, z.B. eine E-Mail von einem Systemadministrator, der Sie bittet, Ihr Kennwort zu ändern oder Ihre Daten zu bestätigen.

Kriminelle, die E-Mails für Scams oder Betrügereien verwenden, können gefälschte Adressen verwenden, um ihre Spuren zu verwischen und die Entdeckung zu vermeiden.

Spammer können eine gefälschte Sender-Adresse verwenden, so dass der Anschein erweckt wird, dass ein unschuldiger Anwender oder ein Unternehmen Spam versendet. Der Vorteil ist, dass die Spammer dann nicht mit Benachrichtigungen überhäuft werden, dass die E-Mail nicht zustellbar ist.

Sie können sich auf zweierlei Arten vor Spoofing schützen.

Konfigurieren Sie Ihr E-Mail-System so, dass sich niemand mit Ihrem SMTP-Port verbinden kann.

Verschlüsseln Sie authentifizierte E-Mails. Dadurch wird sichergestellt, dass E-Mails auch wirklich von dem angegebenen Sender kommen und nicht verändert wurden.

Stellen Sie sicher, dass Ihr E-Mail-System die Erstellung von Protokollen zulässt und dazu konfiguriert ist, ausreichend Informationen in den Protokollen zu speichern, so dass Sie diese bei der Suche des Senders gefälschter E-Mails verwenden können.

Es ist sinnvoll, einen einzigen Eintrittspunkt für E-Mails in Ihr System zu haben. Dazu müssen Sie Ihre Firewall so konfigurieren, dass SMTP-Verbindungen von außerhalb durch ein zentrales E-Mail-Hub geleitet werden. Dadurch werden zentrale Protokolle erstellt, die bei der Suche des Senders gefälschter E-Mails hilfreich sein können.

Spyware

Spyware ist Software, die es Werbemachern oder Hackern ermöglicht, ohne Ihre Einwilligung Informationen zu sammeln.

Spyware-Programme sind keine Viren (sie können sich nicht auf andere Computer verbreiten). Sie können aber unerwünschte Auswirkungen haben.

Spyware kann auf Ihren Computer gelangen, wenn Sie bestimmte Websites besuchen. In einem Pop-Up-Fenster wird Ihnen mitgeteilt, dass Sie eine erforderliche Software herunterladen müssen oder sie wird einfach ohne Ihr Wissen heruntergeladen.

Die Spyware läuft dann auf dem Computer, protokolliert Ihre Aktivitäten (z.B. Besuche auf Websites) und meldet die Ergebnisse an Dritte, z B. an Werbe-Unternehmen. Sie kann auch die Startseite ändern, die angezeigt wird, wenn Sie Ihren Internetbrowser starten. Über ein Einwahlmodem kann Spyware außerdem Premiumratennummern wählen. Spyware verbraucht auch Speicher- und Prozessor-Kapazität und kann den Computer verlangsamen und zum Absturz bringen.

Gute Antiviren-Programme entdecken und entfernen Spyware, die oft genau wie Trojaner behandelt wird.

Trojaner

Trojaner sind Programme, die vorgeben, legitime Software zu sein. In Wahrheit verfügen sie jedoch über versteckte Schadensfunktionen.

Ein Trojaner gibt vor, nur eine einzige Funktion zu haben (und scheint sie auch auszuführen), doch in Wirklichkeit führt er im Hintergrund ohne Ihr Wissen eine ganz andere Funktion aus. **DLoader-L** wird beispielsweise als E-Mail-Attachment versendet und täuscht vor, ein wichtiges Update von Microsoft für Windows XP zu sein. Wenn man den Trojaner startet, lädt er ein Programm herunter, das sich über Ihren Computer mit bestimmten Websites verbindet, um sie zu überlasten (dies wird Denial-of-Service-Attacke genannt).

Trojaner können sich nicht so schnell verbreiten wie Viren, da sie keine Kopien von sich erstellen. Sie treten jedoch immer häufiger in Kombination mit Viren auf. Viren können Trojaner herunterladen, die Tastenfolgen speichern oder Informationen stehlen. Einige Trojaner werden auch dazu verwendet, um einen Computer mit einem Virus zu infizieren.

Siehe **Backdoor-Trojaner**.

Verschleierte Spam-Mails

Als verschleierter Spam werden E-Mails bezeichnet, die getarnt wurden, um Antispam-Software zu täuschen.

Spammer suchen stets nach neuen Arten der Veränderung oder Verschleierung von Spam, so dass er von Antispam-Software nicht als zusammenhängende Sinneinheit erkannt werden kann, von dem Empfänger jedoch schon.

Die einfachste Methode der Verschleierung besteht im Einfügen von Leerzeichen zwischen den Buchstaben eines Wortes, beispielsweise:

V i a g r a

Eine andere gängige Methode ist eine falsche Rechtschreibung oder die Einfügung von nicht standardmäßigen Zeichen, beispielsweise:

V!agra

Diese Tricks können einfach aufgedeckt werden.

Ausgefeiltere Methoden nutzen die Verwendung von HTML-Code (wird normalerweise zur Erstellung von Websites verwendet) in E-Mails aus. Dadurch können Spammer Spam erstellen, den Antispam-Software anders wahrnimmt als der Empfänger.

Wörter können beispielsweise mithilfe von numerischem HTML-Code geschrieben werden, wobei jeder Buchstabe durch einen anderen Code dargestellt wird. Das Wort "Viagra" kann dann folgendermaßen aussehen:

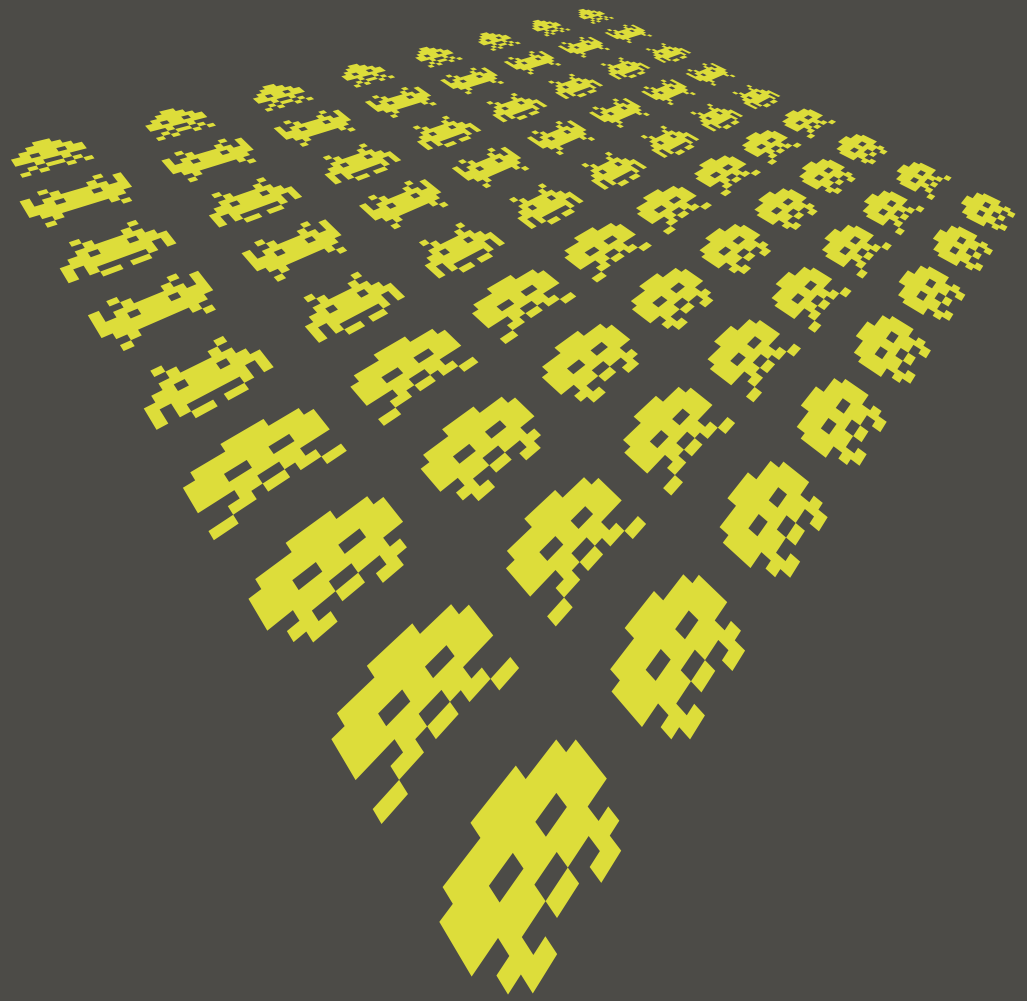
Viagr&#97

Manchmal möchten Spammer, dass das Antispam-Programm eine harmlosere Nachricht liest als der Empfänger. Die Farbe der harmloseren Nachricht entspricht der Hintergrundfarbe.

<body bgcolor=white> Viagra

Hi, Johnny! It was nice to have dinner with you. </body>

Spammer fügen oft versteckten Text ein, der aus Online-Referenzquellen ausgeschnitten wurde, um Antispam-Software zu täuschen, die E-Mails aufgrund der Häufigkeit bestimmter Schlüsselwörter kategorisieren.



Viren

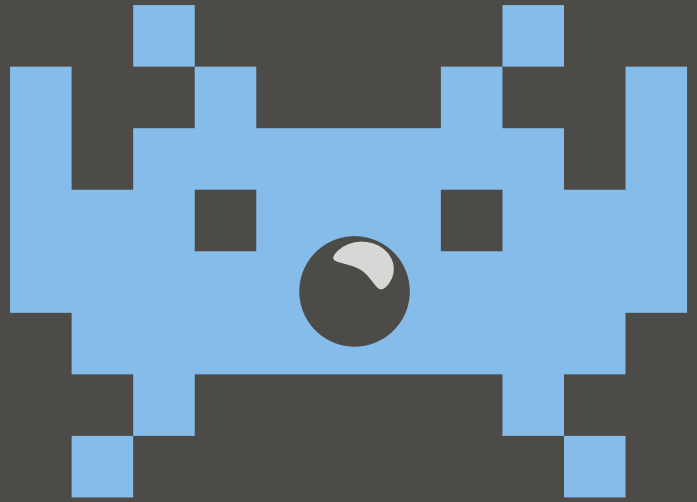
Viren sind Computerprogramme, die sich verbreiten, indem sie Kopien ihrer selbst erstellen.

Computerviren verbreiten sich von einem Computer auf den anderen und von einem Netzwerk auf das andere, indem sie sich kopieren, normalerweise ohne Wissen des Anwenders.

Viren können verschiedene Schäden anrichten, von der Anzeige lästiger Meldungen bis hin zum Stehlen von Daten oder der Übergabe der Steuerung Ihres Computers an Hacker.

Ein Virus kann Ihren Computer nur infizieren, wenn der Virus gestartet wurde. Viren haben ihre Methoden, um dafür zu sorgen, dass dies geschieht. Sie können sich an andere Programme anhängen oder ihren Code so verstecken, dass er automatisch startet, wenn Sie bestimmte Dateitypen öffnen. Viren können auch Sicherheitslücken im Betriebssystem Ihres Computers ausnutzen, um automatisch zu starten und sich zu verbreiten.

Sie können auf verschiedene Arten eine infizierte Datei erhalten, beispielsweise als E-Mail-Attachment, als Download aus dem Internet oder auf einer Diskette. Sobald die Datei aufgerufen wird, startet auch der Virencode. Der Virus kann sich dann in andere Dateien oder auf Datenträger kopieren und Änderungen auf Ihrem Computer vornehmen.



Viren-Hoaxes

Viren-Hoaxes sind Meldungen über nicht existierende Viren.

Hoaxes verbreiten sich normalerweise als E-Mail und können z.B. folgende Inhalte haben:

- Sie warnen vor einem extrem zerstörerischen neuen Virus, der nicht erkannt werden kann.
- Sie werden aufgefordert, keine E-Mails mit einer bestimmten Betreffzeile zu öffnen, beispielsweise "Budweiser Frogs".
- Sie behaupten, dass die Warnung von einer großen Software-Firma, einem Internet Provider oder einer Behörde, wie z.B. IBM, Microsoft, AOL oder FCC, herausgegeben wurde.
- Sie behaupten, dass ein neuer Virus Schäden verursacht, die relativ unwahrscheinlich sind, z.B. behauptet der Hoax **"A moment of silence**", dass "neue Computer infiziert werden, auch wenn keine Programme ausgetauscht werden".
- Sie verwenden eine hochtechnische Sprache. So behauptet **"Good Times",** dass der Virus den PC-Prozessor "in einen unendlichen Binärring mit endlicher Komplexität" bringt.
- Sie fordern dazu auf, die Warnung an andere Anwender weiterzuleiten.

Wenn Anwender eine Hoax-Warnung an sämtliche Freunde und Kollegen weiterleiten, kommt es zu einer regelrechten Flut an E-Mails. E-Mail-Server werden überlastet und stürzen im schlimmsten Fall ab. Dies hat dann denselben Effekt, den auch der echte **Sobig**-Virus hervorgerufen hat, allerdings muss der Verfasser eines Hoax dazu noch nicht einmal einen Computer-Code schreiben.

Es sind aber nicht nur die Anwender, die gerne überreagieren. Auch Unternehmen, die

Viren für Mobiltelefone

Mobiltelefone können durch Viren infiziert werden, die sich über das Mobilfunknetz verbreiten.

2004 wurde der erste Mobiltelefon-Wurm geschrieben. Der **Cabir-A** Wurm, der das Symbian-Betriebssystem ausnutzt, wird als Telefonspieldatei (eine SIS-Datei) übertragen. Wenn Sie die Datei starten, erscheint eine Meldung auf dem Bildschirm und der Wurm startet dann jedes Mal, wenn Sie Ihr Telefon einschalten. **Cabir-A** sucht nach anderen Mobiltelefonen in der Nähe, die Bluetooth im Einsatz haben, und sendet sich an das erste entsprechende Telefon.

Es gibt auch konventionelle Viren, die Nachrichten an Mobiltelefone senden. **Timo-A** beispielsweise benutzt Computermodems, um Textnachrichten (SMS) an ausgewählte Mobiltelefon-Nummern zu senden. In solchen Fällen kann der Virus jedoch das Mobiltelefon nicht infizieren oder beschädigen.

Bis heute sind die Gefahren für Mobiltelefone sehr gering. Der Grund dafür liegt wahrscheinlich darin, dass sie viele verschiedene Betriebssysteme verwenden oder auch dass sich die Eigenschaften der Software und Geräte so schnell ändern.

Viren für PDAs

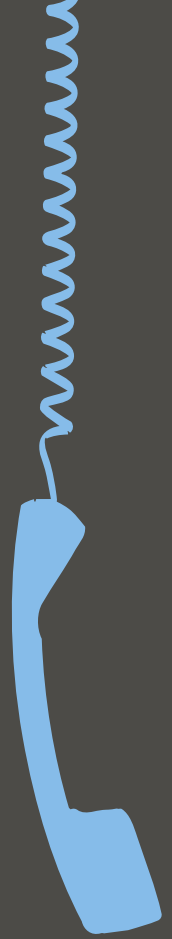
PDAs oder Palmtops bieten neue Möglichkeiten für Viren, allerdings haben Virenschreiber bisher wenig Interesse diesbezüglich gezeigt.

PDAs oder Palmtops laufen mit speziellen Betriebssystemen – wie Palm und Microsoft PocketPC. Diese sind zwar für schädlichen Code anfällig, aber bisher scheinen die Risiken gering zu sein.

Zurzeit gibt es nur wenige bekannte Malware für PDAs.

Virenschreiber zielen lieber auf Desktop-Systeme, da sie weiter verbreitet sind und sich Viren auf ihnen per E-Mail und über das Internet schneller verbreiten können.

Die wirkliche Gefahr zur Zeit ist eher, dass Ihr PDA als Überträger fungiert. Wenn Sie sich mit Ihrem PC zu Hause oder im Büro für die Datensynchronisation verbinden, kann sich ein auf dem PDA harmloser Virus auf den PC übertragen und dort durchaus Schäden anrichten. Um dieses Risiko zu vermeiden, folgen Sie unseren Hinweisen in: **Schutz vor Viren, Trojanern, Würmern und Spyware** und verwenden Sie auf Ihren Desktop-Computern stets Antiviren-Software.



Voice Phishing

Voice Phishing bezeichnet die Verwendung gefälschter Telefonnummern, um Anwender dazu zu bringen, vertrauliche Informationen preiszugeben.

Phishing umfasst ursprünglich das Versenden von E-Mails, die Links auf gefälschte Websites enthalten, wobei Anwender gebeten werden, Kontendaten oder andere vertrauliche Informationen einzugeben. Bei Voice Phishing (oder auch Vishing, V-Phishing oder Phone Phishing) werden Opfer aufgefordert, eine Telefonnummer anzurufen, anstatt eine Website zu besuchen, doch die Absicht ist dieselbe: Diebstahl vertraulicher Daten, um Geld zu scheffeln.

Ein Beispiel dafür ist die **PayPal** Voice Phishing E-Mail. Die E-Mail scheint von dem elektronischen Zahlungsdienst PayPal zu kommen und gibt vor, dass das Konto des Anwenders für betrügerische Aktivitäten verwendet worden sein könnte. Die E-Mail warnt davor, dass das Konto gesperrt wird, wenn der Anwender nicht eine Telefonnummer anruft, um seine Daten zu bestätigen. Sobald der Anwender diese Nummer anruft, fragt eine automatische Stimme nach seiner Kartennummer. Kriminelle können sich dann dank der Kartennummer bereichern.

Anwender sind mitunter vorsichtig und folgen Links in unerwarteten E-Mails nicht und sie können sicherstellen, die korrekte Webadresse ihres Online Banking-Dienstes zu verwenden, wenn sie sie manuell eingeben. Es ist jedoch unwahrscheinlich, dass sie die Telefonnummer solch eines Dienstes kennen.

Sie können sich durch Antispam-Software vor Voice Phishing schützen, da diese Phishing-Mails erkennt, Zudem sollten Sie vorsichtig mit unerwünschten Werbemails umgehen.

Zombies

Ein Zombie ist ein Computer, der remote gesteuert und für schädliche Zwecke verwendet wird, ohne dass der Besitzer darüber Bescheid weiß.

Ein Virus oder Trojaner kann einen Computer infizieren und eine Backdoor öffnen, die Dritten Zugriff auf den Computer ermöglicht. Sobald das geschehen ist, sendet der Virus eine E-Mail an den Virenschreiber, der den Computer jetzt remote über das Internet steuern kann. Jetzt ist der Computer ein Zombie, der von anderen gesteuert wird, ohne das sein legitimer Anwender dies ahnt. Ein Zusammenschluss solcher Zombie-Computer wird als Botnet bezeichnet.

Der Virenschreiber kann den Zugriff auf seine Liste von Zombie-Computern mit anderen Hackern teilen oder an sie verkaufen, so dass sie die Computer ebenfalls für schädliche Zwecke verwenden können.

Ein Spammer kann beispielsweise Zombie-Computer verwenden, um Spam zu versenden. Bis zu 80% aller Spam-Mails werden auf diese Weise verbreitet. Dadurch vermeiden die Spammer, erkannt zu werden und umgehen Blocklists für ihre eigenen Server. Sie senken dadurch auch eigene Ausgaben, da der Besitzer des Computers für die Internetverbindung bezahlt.

Hacker können Zombie-Computer auch für eine Denial-of-Service-Attacke verwenden. Sie sorgen dafür, dass Tausende Computer gleichzeitig auf dieselbe Website zugreifen,

Sicherheits-Software

Antiviren-Software

Antiviren-Software schützt Sie vor Viren, Trojanern, Würmern und – abhängig von Ihrem Produkt – auch vor Spyware und anderer Malware.

Antiviren-Software verwendet einen Scanner, um Programme zu identifizieren, die schädlich sind oder sein könnten. Scanner können Folgendes erkennen:

- **Bekannte Viren** – Der Scanner gleicht Dateien auf Ihrem Computer mit einer Library mit bekannten Virenkennungen ab. Findet er eine Übereinstimmung, gibt er eine Warnung aus und blockiert den Zugriff auf diese Datei.
- **Unbekannte Viren** – Der Scanner untersucht das mögliche Verhalten eines Programms. Weist das Programm die Merkmale eines Virus auf, wird der Zugriff verhindert, auch wenn die Datei nicht mit bekannten Viren übereinstimmt.
- **Verdächtige Dateien** – Der Scanner untersucht das mögliche Verhalten eines Programms. Erscheint das Verhalten unerwünscht, warnt der Scanner vor dem potentiellen Vorhandensein eines Virus.

Die zuverlässige Erkennung von bekannten Viren hängt davon ab, wie oft das Antiviren-Programm mit den neuesten Virenkennungen aktualisiert wird.

Es gibt On-Access- und On-Demand-Scanner. Die meisten Antiviren-Programme umfassen beide Arten von Scannern.

On-Access-Scanner sind auf Ihrem Computer aktiv, solange Sie ihn benutzen. Sie überprüfen Dateien automatisch, wenn Sie sie öffnen oder starten, und verhindern, dass infizierte Dateien benutzt werden.

Mit einem **On-Demand-Scanner** können Sie eine Überprüfung bestimmter Dateien oder Laufwerke starten oder einen Zeitplan für Überprüfungen festlegen.

Antispam-Software

Antispam-Programme können unerwünschte E-Mails erkennen und verhindern, dass sie in den Posteingang der Anwender gelangen.

Diese Programme verwenden eine Kombination mehrerer Methoden, um festzustellen, ob es sich bei einer E-Mail um Spam handelt. Diese Programme haben folgende Funktionen:

- Blockieren von E-Mails, die von Computern stammen, die sich auf einer Blocklist befinden. Dies kann eine kommerziell verfügbare Liste oder eine eigene Liste mit Adressen sein, von denen Ihr Unternehmen zuvor schon Spam erhalten hat.
- Blockieren von E-Mails, die bestimmte Webadressen umfassen.
- Prüfen, ob E-Mails von einer existierenden Domäne oder Internet-Adresse stammen. Denn Spammer verwenden oft gefälschte Adressen, um Antispam-Programme zu umgehen.
- Suche nach Stichwörtern oder typischen Wendungen in Spam (z.B. "Kreditkarte", "Gewichtsabnahme").
- Nach Mustern suchen, mit denen ein Sender den Text zu verbergen versucht (z.B. bei "hardc*re p0rn").
- Suche nach unnötigem HTML-Code (Code zum Schreiben von Websites) in E-Mails, da Spammer damit ihre E-Mails tarnen und Antispam-Programme verwirren möchten.

Das Programm kombiniert alle gefundenen Informationen und berechnet eine Wahrscheinlichkeit dafür, dass die E-Mail Spam ist. Ist die Wahrscheinlichkeit hoch genug, kann die E-Mail abgeblockt oder gelöscht werden, je nach den von Ihnen gewählten Einstellungen.

Antispam-Software muss häufig mit neuen Regeln aktualisiert werden, um die neuesten, von Spammern verwendeten Methoden zu erkennen.

Wie schützt Software E-Mails, die Sie erhalten MÖCHTEN?

Viele Anwender befürchten, dass Antispam-Software wichtige E-Mails löscht. Ihre E-Mails sind sicher und Sie können sich auch ausgewählte Spam-Mails ansehen.

Antispam-Programme sind sehr genau. Typischerweise wird von zehntausend oder hunderttausend E-Mails nur eine erwünschte E-Mail abgeblockt.

Auch wenn das Programm fälschlicherweise eine E-Mail als Spam identifiziert, kann es so konfiguriert werden, dass diese E-Mail in einem "Quarantäne"-Bereich abgelegt wird, anstatt gelöscht zu werden. Ein Administrator kann entscheiden, ob die E-Mail zugestellt oder gelöscht wird. Einige Programme geben jedem Anwender die Möglichkeit, E-Mails aus der Quarantäne anzufordern.

Wie passt sich Software Ihren Anforderungen an?

Einige Antispam-Software ist adaptiv: Sie lernt, welche E-Mails Sie akzeptabel finden und welche nicht.

Angenommen, ein Pharma-Unternehmen installiert eine Antispam-Software. Zunächst versucht die Software, Spam ausfindig zu machen, indem sie nach Wörtern sucht, etwa nach: Kredit, kostenlos, Schulden, Hypothek, Medikamente, Rezept, Arzneimittel, Arzt. Die Software blockt E-Mails mit zu vielen dieser Stichwörter ab, gibt allerdings einzelnen Anwendern die Möglichkeit, die E-Mails zu erhalten, die sie lesen möchten.

Einige Mitarbeiter in der Forschungsabteilung stellen fest, dass erwünschte E-Mails über neue Medikamente abgeblockt wurden, und bitten um Freigabe dieser E-Mails. Die Software lernt, dass der Anwender häufig E-Mails über Medikamente erhält – und gibt Stichwörtern in Bezug auf Medikamente weniger Gewichtung, wenn nach Spam gesucht wird.

In der Finanzabteilung fordern Anwender E-Mails mit Finanzbegriffen an. Die Software lernt so, dass diese Wörter eine geringere Gewichtung haben sollten – blockt aber für diese Anwender trotzdem E-Mails über Medikamente ab.

Firewall

Eine Firewall verhindert unbefugten Zugriff auf einen Computer oder ein Netzwerk.

Wie der Name bereits sagt, ist die Firewall eine Art Trennwand zwischen Netzwerken oder Teilen eines Netzwerks und blockiert schädlichen Datenfluss und Hacker.

Eine **Netzwerk-Firewall** befindet sich zwischen zwei Netzwerken. Normalerweise zwischen dem Internet und einem Unternehmensnetzwerk. Es kann sich dabei um eine separate Hardware-Lösung oder um Software handeln, die auf einem Computer ausgeführt wird, der als Gateway im Unternehmensnetzwerk dient.

Eine **Client Firewall** ist Software, die auf dem Computer eines Endbenutzers ausgeführt wird und nur diesen einen Computer schützt.

Die Firewall prüft den gesamten eingehenden und ausgehenden Datenfluss, um festzustellen, ob er bestimmten Merkmalen entspricht. Ist dies der Fall, so wird der Datenfluss erlaubt; ist dies nicht der Fall, so wird er von der Firewall blockiert. Firewalls können Datenfluss entsprechend folgender Einstellungen filtern:

- Quell- und Zieladressen sowie Port-Nummern (Adressfilterung)
- Art des Netzwerkverkehrs, z.B. HTTP oder FTP (Protokoll-Filterung)
- Attribute oder Status der gesendeten Informationspakete

Eine Client Firewall kann den Benutzer auch jedes Mal warnen, wenn ein Programm versucht, eine Verbindung herzustellen und ihn fragen, ob diese Verbindung erlaubt oder blockiert werden soll. Sie lernt mit der Zeit aus den Antworten des Anwenders, so dass sie weiß, welche Arten des Datenflusses der Anwender erlaubt.

Resource Shielding

Resource Shielding verhindert, dass auf anfällige Bereiche Ihres Computers zugegriffen wird.

Resource Shielding analysiert das Verhalten aller Programme, die bereits auf Ihrem Computer ausgeführt werden und blockiert alle Vorgänge, die schädlich erscheinen. Zum Beispiel überprüft Resource Shielding alle Änderungen, die an der Windows-Registrierung vorgenommen werden und die auf eine Installation von Malware hinweisen können, die sich selbst ausführt, sobald der Computer neu gestartet wird.

Resource Shielding-Produkte ermöglichen Ihnen die Erstellung eigener Regeln, so dass Sie entscheiden können, welche Ressourcen geschützt werden sollen.

Tipps zum sicheren Umgang mit Computern

Wie schütze ich meine Computer vor Viren, Trojanern, Würmern und Spyware?

Verwenden Sie Antiviren-Software

Installieren Sie auf allen Desktops und Servern Antiviren-Software und stellen Sie sicher, dass diese stets aktuell ist. Neue Viren können sich sehr schnell verbreiten. Deshalb ist es wichtig, eine Update-Infrastruktur zu haben, die alle Unternehmenscomputer nahtlos, regelmäßig und kurzfristig aktualisiert.

Verwenden Sie zusätzlich Software zum Filtern von E-Mails an Ihrem E-Mail-Gateway, um Ihr Unternehmen vor E-Mail-basierten Viren, Spam und Spyware zu schützen.

Denken Sie auch daran, Laptops sowie Desktops zu schützen, die von Ihren Mitarbeitern genutzt werden, die von zu Hause arbeiten. Viren, Würmer und Spyware können sich über diese Geräte leicht in Ihr Unternehmensnetzwerk einschleichen.

Blockieren Sie Dateitypen, die oft Viren enthalten

Dazu gehören Dateien mit den Erweiterungen EXE, COM, PIF, SCR, VBS, SHS, CHM und BAT. Unternehmen erhalten normalerweise keine Dateien mit diesen Erweiterungen von außerhalb.

Blockieren Sie Dateien mit mehr als einer Dateierweiterung

Einige Viren verschleiern die Tatsache, dass sie Programme sind, indem sie nach ihrem Dateinamen eine doppelte Erweiterung benutzen, z.B. .TXT.VBS. Auf den ersten Blick sieht eine Datei namens LOVE-LETTER-FOR-YOU.TXT.VBS wie eine harmlose Textdatei oder Grafik aus. Sie sollten alle Dateien mit doppelter Erweiterung am E-Mail-Gateway abblocken.

Stellen Sie sicher, dass alle Programme von Ihrer IT-Abteilung überprüft werden

Sorgen Sie dafür, dass alle Programme, die von außerhalb gesendet werden, direkt zu Ihrer IT-Abteilung, oder bei kleinen Unternehmen, zu dem IT-Verantwortlichen gelangen, um überprüft und freigegeben zu werden. Die IT-Abteilung sollte überprüfen, dass diese Programme für das Unternehmen geeignet, virenfrei, lizenziert und mit bestehender Software kompatibel sind.

E-Mail-Benachrichtigungsservice

Ein Benachrichtigungsservice kann Sie vor den neuesten Viren warnen und Virenkennungen zur Verfügung stellen, mit denen Ihre Antiviren-Software neue Viren erkennt. Sophos bietet einen kostenlosen Benachrichtigungsservice an. Nähere Informationen finden Sie auf www.sophos.de/virusinfo/notifications. Fügen Sie ein ein Live–Information-Feed zu Viren auf Ihrer Website oder im Intranet hinzu, damit Ihre Anwender stets über die neuesten Viren auf dem Laufenden sind.

Verwenden Sie eine Firewall auf Computern mit Internetanschluss

Schützen Sie Computer, die mit dem Internet verbunden sind, durch eine Firewall. Laptops und Computer von Mitarbeitern, die von zu Hause arbeiten, müssen ebenfalls durch eine Firewall geschützt werden.

Mit Software-Patches immer auf dem neuesten Stand

Informieren Sie sich über Sicherheits-News und laden Sie Patches herunter. Diese schließen oft Sicherheitslücken, die Ihren Computer für Viren oder Internetwürmer anfällig machen. IT-Manager sollten die Mailing-Listen von Software-Herstellern abonnieren, wie z.B. die unter www.microsoft.com/technet/security/bulletin/notify.asp. Heimanwender mit Windows-PCs können windowsupdate.microsoft.com besuchen und dort ihren PC auf Sicherheitslücken prüfen und Patches installieren lassen.

Erstellen Sie regelmäßig Sicherungskopien Ihrer Daten

Erstellen Sie regelmäßig Sicherungskopien wichtiger Dokumente und Daten und prüfen Sie, dass diese Sicherungskopien einwandfrei funktionieren. Es ist wichtig, Ihre Sicherungskopien an einem geschützten Ort zu lagern, vielleicht sogar außerhalb des Firmengeländes, um das Risiko der Zerstörung durch Feuer auszuschließen. Wenn Ihr Computer mit einem Virus infiziert ist, können Sie verlorene Programme und Daten durch Backups wiederherstellen.

Deaktivieren Sie den Start des Computers von Disketten

Bootsektor-Viren treten heutzutage äußerst selten auf, doch es ist durchaus sinnvoll, sich trotzdem vor Ihnen zu schützen. Ändern Sie die Startsequenz auf Ihren Computern, so dass Sie zuerst von der Festplatte aus starten, anstatt über das Diskettenlaufwerk (Laufwerk A:). Wenn eine infizierte Diskette versehentlich im Computer gelassen wird, kann der Rechner nicht mit einem Bootsektorvirus infiziert werden. Sollte ein Start von einer Diskette aus erforderlich sein, kann diese Einstellung problemlos wieder geändert werden.

Setzen Sie eine Antiviren-Richtlinie um

Erstellen Sie eine Richtlinie zum sicheren Arbeiten mit Computern und geben Sie sie im gesamten Unternehmen bekannt. Die Richtlinie sollte Folgendes umfassen:

- Laden Sie keine ausführbaren Dateien oder Dokumente direkt aus dem Internet herunter.
- Öffnen Sie keine unerwünschten Programme, Dokumente oder Tabellen.
- Verwenden Sie nur Computerspiele und Bildschirmschoner, die im Betriebssystem enthalten sind.
- Leiten Sie E-Mail-Attachments zur Überprüfung an Ihre IT-Abteilung weiter.
- Speichern Sie alle Word-Dokumente als RTF (Rich Text Format), da sich in DOC-Dateien Makroviren befinden können.
- Gehen Sie vorsichtig mit unerwarteten E-Mails um.
- Leiten Sie Viren- oder Hoaxes-Warnungen direkt an Ihre IT-Abteilung weiter (und niemanden sonst), um festzustellen, ob diese Warnungen echt sind.
- Informieren Sie Ihre IT-Abteilung umgehend darüber, wenn Sie vermuten, dass Ihr Computer von einem Virus infiziert wurde.

Wie schütze ich meine Computer vor Hoaxes?

Unternehmensrichtlinie für Virenwarnungen

Erstellen Sie eine Unternehmensrichtlinie für Virenwarnungen. Solch eine Richtlinie könnte folgendermaßen aussehen:
Leiten Sie Virenwarnungen nur an den Antiviren-Verantwortlichen weiter. Es ist völlig egal, ob die Virenwarnungen von einem Antiviren-Hersteller oder Ihrem besten Freund kommen oder ob sie von einem großen Computerunternehmen bestätigt wurden. ALLE Virenwarnungen sollten nur an [Name des Verantwortlichen] gesendet werden. Es ist seine Aufgabe, Virenwarnungen zu versenden. Virenwarnungen aus anderen Quellen werden ignoriert.

Informieren Sie sich über Hoaxes

Seien Sie stets über Hoaxes auf dem Laufenden. Informationen über Hoaxes finden Sie auf unserer Website unter:
www.sophos.de/security/hoaxes/

Leiten Sie keine Kettenbriefe weiter

Leiten Sie keine Kettenbriefe weiter, auch wenn Ihnen Belohnungen dafür versprochen werden oder so angeblich nützliche Infos verbreitet werden.

Wie schütze ich meine Computer vor Spam?

Verwenden Sie am E-Mail-Gateway Software zum Filtern von E-Mails

Verwenden Sie zusätzlich Software zum Filtern von E-Mails an Ihrem E-Mail-Gateway, um Ihr Unternehmen vor E-Mail-basierten Viren, Spam und Spyware zu schützen.

Geben Sie nie eine Bestellung über unerwünschte E-Mails auf

Mit Ihrer Bestellung sorgen Sie für noch mehr Spam. Ihre E-Mail-Adresse kann zu Listen hinzugefügt werden, die an andere Spammer verkauft werden, so dass Sie noch mehr unnütze E-Mails erhalten. Im schlimmeren Fall können Sie Betrügern zum Opfer fallen.

Kennen Sie den Sender einer unerwünschten E-Mail nicht, löschen Sie sie

Die meisten Spam-Mails sind einfach nur lästig, aber sie können manchmal auch Viren enthalten, die den Computer schädigen, sobald die E-Mail geöffnet wird.

Antworten Sie nie auf Spam-Mails und klicken Sie nie auf darin enthaltene Links

Wenn Sie auf Spam antworten – auch wenn Sie sich nur von einer Mailing-Liste abmelden – bestätigen Sie, dass Ihre E-Mail-Adresse gültig ist, und sorgen damit nur für noch mehr Spam.

Verwenden Sie den Vorschau-Modus Ihres E-Mail-Programms nicht

Viele Spammer können nachverfolgen, wenn eine E-Mail angesehen wird, ohne dass Sie auf die E-Mail geklickt haben. Die Vorschau öffnet die E-Mail und Spammer wissen dann, dass Sie ihre E-Mails erhalten haben. Versuchen Sie allein über die Betreffzeile zu entscheiden, ob es sich bei E-Mails um Spam handelt oder nicht.

Bei E-Mails an mehrere Personen "bcc"-Feld verwenden

Im "bcc"- oder "Blindkopie"-Feld ist die Empfängerliste für andere Anwender unsichtbar. Wenn Sie alle Adressen in das "An"-Feld einfügen, können Spammer diese Adressen aufspüren und sie zu einer Mailingliste hinzufügen.

E-Mail-Adresse niemals im Internet angeben

Erwähnen Sie Ihre E-Mail-Adresse nie im Internet, in Newsgroups oder anderen öffentlichen Foren im Internet. Spammer können mit Programmen an solchen Stellen im Internet nach Adressen suchen.

E-Mail-Adresse nur an vertrauenswürdige Personen geben

Geben Sie Ihre E-Mail-Adresse nur Freunden und Bekannten.

Verwenden Sie sekundäre E-Mail-Adressen

Wenn Sie Formulare im Internet ausfüllen, von denen Sie keine weiteren Informationen wünschen, nutzen Sie eine sekundäre E-Mail-Adresse. Sie schützen somit Ihre Hauptadresse vor Spam.

Keine weiteren Informationen oder Angebote

Wählen Sie beim Ausfüllen von Formularen im Internet nie die Option, weitere Informationen oder Angebote zu erhalten. Aktivieren oder deaktivieren Sie diese Option entsprechend.

Wie schütze ich meine Computer vor Phishing?

Antworten Sie nie auf E-Mails, die nach vertraulichen Finanzdaten fragen

Seien Sie auf der Hut vor E-Mails, die nach Ihrem Kennwort oder Kontendetails fragen oder entsprechende Links enthalten. Banken oder e-Commerce-Unternehmen versenden solche E-Mails nicht.

Suchen Sie nach Merkmalen einer Phishing-Attacke

Phishing-Mails verwenden normalerweise eine generische Anrede, beispielsweise "Sehr geehrte Kunden", da es sich bei der E-Mail um Spam handelt und der Phisher Ihren Namen nicht kennt. Die meisten Phishing-Mails enthalten alarmierende Behauptungen, wie z.B. den Diebstahl oder Verlust Ihrer Kontendetails. Die E-Mails enthalten oft falsche Schreibweisen und manche Buchstaben werden durch Zeichen ersetzt, z.B. "1nformati0n". Somit versuchen sie der Entdeckung durch Antispam-Software zu entgehen.

Gehen Sie zu den Websites von Banken, indem Sie die Adresse jedes Mal neu eingeben

Folgen Sie keinen Links in unerwünschten E-Mails. Phisher verwenden diese Links oft, um Sie zu einer gefälschten Website zu leiten. Geben Sie stattdessen die komplette Adresse in Ihren Browser ein.

Überprüfen Sie Ihre Konten regelmäßig

Melden Sie sich regelmäßig bei Ihren Online-Konten an und überprüfen Sie Ihre Kontoauszüge. Stoßen Sie auf verdächtige Transaktionen, melden Sie diese Ihrer Bank oder Ihrem Kreditkarten-Unternehmen.

Prüfen Sie, ob die von Ihnen besuchte Website sicher ist

Überprüfen Sie die Adresseingabe. Befindet sich die Website auf einem sicheren Server, sollte Sie mit "https://" beginnen ("s" steht für sicher), anstatt mit "http://". Achten Sie auch auf das Schloss-Symbol in der Statusleiste des Browsers. Dieses Symbol weist darauf hin, dass die Website Verschlüsselung verwendet, was aber nicht unbedingt heißt, dass die Website legitim ist.

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

Lesen Sie die Hinweise Ihrer Bank zum sicheren Online Banking. Teilen Sie niemandem Ihre PINs oder Kennwörter mit, schreiben Sie sie nicht auf und verwenden Sie niemals ein und dasselbe Kennwort für mehrere Online-Konten. Öffnen oder antworten Sie nicht auf Spam-Mails, da der Sender dadurch erfährt, dass Ihre E-Mail-Adresse gültig ist und sie für zukünftige Scams verwenden kann.

Schützen Sie Ihren Computer

Durch Antispam-Software werden zahlreiche Phishing-E-Mails abgefangen und erreichen Ihren Posteingang erst gar nicht. Eine Firewall schützt Ihre persönlichen Daten und blockiert unbefugten Dateiaustausch. Verwenden Sie Antiviren-Software, um schädliche Programme zu erkennen, wie beispielsweise Spyware oder Backdoor-Trojaner, die in Phishing-E-Mails enthalten sein können. Schützen Sie Ihren Browser stets durch die neuesten Sicherheits-Patches.

Melden Sie verdächtige Aktivitäten umgehend

Wenn Sie eine E-Mail enthalten, die Sie für gefälscht halten, leiten Sie sie an das Unternehmen weiter, von dem sie zu kommen scheint. (Viele Unternehmen haben eine E-Mail-Adresse, an die solche Fälle des Missbrauchs gemeldet werden können.)

Wie schütze ich meine Computer im Internet?

Dieser Abschnitt gibt allgemeine Tipps zur sicheren Verwendung von Internet und E-Mails. Lesen Sie auch unsere Hinweise zur **Vermeidung, Opfer einer Phishing-Kampagne zu werden**.

Klicken Sie nicht auf Popup-Meldungen

Erscheint eine unerwünschte Popup-Warnung, dass Ihr Computer infiziert ist und wird Software zur Entfernung des Virus angeboten, folgen Sie angegebenen Links nicht und laden Sie auch keine Software herunter, da diese schädlich sein kann.

Klicken Sie nicht auf Links in unerwarteten E-Mails

Solche Links verweisen oft auf gefälschte Websites, auf denen von Ihnen eingegebene vertrauliche Informationen, wie Kontendetails oder Kennwörter, gestohlen und missbraucht werden können. Geben Sie die Adresse der gewünschten Website stets in dem Adressfeld Ihres Browsers ein.

Verwenden Sie für jede Website verschiedene Kennwörter

Verwenden Sie für alle Websites, für die Sie ein Benutzerkonto haben, ein anderes Kennwort. Wird ein Kennwort entschlüsselt, so betrifft dies nur ein Konto.

Sicherheit im Internetbrowser

Deaktivieren Sie Java- oder ActiveX-Applets, Cookies usw. oder stellen Sie ein, dass Sie gewarnt werden, bevor solcher Code gestartet wird. Gehen Sie beispielsweise im Microsoft Internet Explorer auf Extras | Internetoptionen | Sicherheit | Stufe anpassen und wählen Sie die gewünschten Sicherheitseinstellungen.

Blockieren Sie den Zugriff auf bestimmte Websites oder Arten von Webinhalten

In einem Unternehmensnetzwerk ist es sinnvoll, den Zugriff auf Websites zu blockieren, deren Inhalt anstößig ist, die für die Arbeit unangemessen sind oder eine Sicherheitsbedrohung darstellen (die z.B. Spyware auf Computern installieren). Dafür gibt es Software zum Filtern von Webinhalten oder Hardware-Appliances.

Verwenden Sie Reputation Filtering

Reputation Filtering-Software gleicht die Senderadressen in E-Mails mit einer Datenbank ab, die prüft, wie oft die von dem Sender gesendeten E-Mails Spam sind oder Viren, Würmer usw. enthalten. Die Software weist der E-Mail dann eine Reputation-Quote zu, die entscheidet, ob die E-Mail blockiert oder ihre Versendung verzögert wird (E-Mails mit besserer Reputation-Quote werden vorrangig weitergeleitet).

Nutzen Sie Firewalls

Schützen Sie Ihr Unternehmen durch eine Netzwerk-Firewall: sie lässt nur erlaubte Arten des Datenflusses zu. Zudem sollte sich eine Client Firewall auf jedem Computer im Netzwerk befinden, die nur erlaubten Datenfluss zulässt, wodurch Hacker und Internetwürmer blockiert werden. Zudem verhindert sie, dass der Computer über unbefugte Programme mit dem Internet kommuniziert.

Verwenden Sie Router

Sie können einen Router verwenden, um die Verbindung zwischen dem Internet und bestimmten Computern zu begrenzen. Viele Router enthalten eine Netzwerk-Firewall.

Wie wähle ich sichere Kennwörter?

Kennwörter schützen Sie vor Betrug und dem Verlust vertraulicher Informationen, doch die wenigsten Anwender wählen Kennwörter, die wirklich sicher sind.

Wählen Sie ein möglichst langes Kennwort

Je länger das Kennwort, desto schwieriger ist es zu erraten oder alle möglichen Kombinationen zu seiner Entschlüsselung durchzugehen (Brute-Force-Attacke). Verwenden Sie mindestens acht Zeichen.

Verwenden Sie verschiedene Zeichen

Verwenden Sie Zahlen, Satzzeichen sowie Groß- und Kleinschreibung.

Verwenden Sie keine Wörter, die in Nachschlagewerken zu finden sind

Verwenden Sie keine Wörter, Namen oder Ortsnamen, die in Nachschlagewerken zu finden sind. Hacker versuchen, solche Kennwörter mithilfe einer so genannten "Dictionary-Attacke" zu entschlüsseln (es werden z.B. alle Wörter des Nachschlagewerks automatisch durchgegangen).

Verwenden Sie keine persönlichen Informationen

Verwenden Sie nicht Ihr Geburtsdatum, den Namen Ihres Partners oder Kindes oder Ihre Telefonnummer, da anderen diese Informationen bekannt sind und sie Ihr Kennwort somit erraten können.

Verwenden Sie nicht Ihren Benutzernamen

Verwenden Sie nicht Ihren Benutzernamen oder Ihre Kontonummer als Kennwort.

Verwenden Sie Kennwörter, die nur schwer nachzuvollziehen sind, während Sie sie eingeben

Achten Sie darauf, nicht wiederholt Zeichen oder Tasten zu verwenden, die sich auf der Tastatur nahe beieinander befinden.

Verwenden Sie ein Passphrase

Unter Passphrase versteht man die Kombination von mehreren Wörtern. Eine außergewöhnliche Aneinanderreihung von Wörtern ist schwer zu erraten.

Merken Sie sich Ihr Kennwort

Merken Sie sich Ihr Kennwort und schreiben Sie es nicht auf. Wählen Sie eine Zeichenfolge, die für Sie eine Bedeutung hat oder verwenden Sie Gedächtnisstützen, um sich Ihr Kennwort zu merken.

Speichern Sie Ihre Kennwörter nicht auf Ihrem Computer oder Online

Hacker könnten sich Zugriff auf Ihren Computer verschaffen und die Kennwörter finden.

Wenn Sie Ihr Kennwort aufschreiben, verwahren Sie es an einem sicheren Ort

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

Verwenden Sie für jedes Konto ein anderes Kennwort

Wenn ein Hacker eines Ihrer Kennwörter herausfindet, betrifft dies wenigstens nur eines Ihrer Konten.

Geben Sie Ihr Kennwort nicht an Andere weiter

Erhalten Sie eine E-Mail, in der Sie darum gebeten werden, Ihr Kennwort zu bestätigen, folgen Sie dieser Aufforderung unter keinen Umständen, auch wenn die E-Mail von einer vertrauenswürdigen Quelle oder einem Ihrer Mitarbeiter zu kommen scheint. (Siehe **Phishing**).

Verwenden Sie Ihr Kennwort nie auf einem öffentlichen Computer

Geben Sie Ihr Kennwort nicht auf einem öffentlich zugänglichen Computer ein, z.B. in einem Hotel oder einem Internetcafé. Solche Computer sind eventuell nicht geschützt und es können Programme zum Speichern von Tastenfolgen installiert sein.

Ändern Sie Ihr Kennwort regelmäßig

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

Geschichte der Viren

Wann wurden Viren, Trojaner und Würmer zu Bedrohungen? Die Bedrohung durch Viren begann mit dem Brain-Virus 1986. Dies war allerdings nur der erste Virus für Microsoft-Computer. Programme, die Merkmale von Viren aufweisen, traten bereits sehr viel früher auf. Nachfolgend finden Sie einen Überblick über die wichtigsten Viren im Zeitverlauf.

1949 Sich selbst replizierende Programme oder "Cellular Automata"

John von Neumann, der Vater der Kybernetik, vertritt in einer Veröffentlichung die Meinung, dass ein Computerprogramm sich selbst replizieren kann.

1959 Core Wars

H. Douglas McIlroy, Victor Vysottsky und Robert P. Morris von Bell Labs entwickeln ein Computerspiel namens Core Wars, bei dem Programme, die Organismen genannt werden, um die Bearbeitungszeit des Computers im Wettstreit liegen.

1960 Rabbit-Programme

Programmierer beginnen mit der Erstellung von Platzhaltern für Großrechner. Befinden sich keine Jobs in der Warteschleife, fügen diese Programme eine Kopie ihrer selbst am Ende der Warteschleife ein. Diese Programme erhalten den Spitznamen "Rabbit", da sie sich so schnell wie Hasen "fortpflanzen" und Systemressourcen verbrauchen.

1971 Der erste Wurm

Bob Thomas, einer der Entwickler von ARPANET, ein Vorläufer des Internets, erstellt ein Programm mit dem Namen **Creeper**, das sich von einem Computer auf den nächsten verbreitet und eine Meldung anzeigt.

1975 Replizierung von Code

A. K. Dewdney schreibt den Code **Pervade** als Subroutine für Spiele, die auf Computern ausgeführt werden, die das UNIVAC 1100-System verwenden. Sobald ein Anwender das Spiel spielt, kopiert Pervade die aktuellste Version seiner selbst heimlich in jedes zugängliche Verzeichnis, einschließlich in freigegebene Verzeichnisse und verbreitet sich somit im gesamten Netzwerk.

1978 Der Vampire-Wurm

John Shoch und Jon Hupp von Xerox PARC experimentieren mit Würmern, die hilfreiche Tasks ausführen sollen. Der **Vampire**-Wurm verhält sich tagsüber ruhig, weist aber nachts nicht ausgelasteten Computern Tasks zu.

1981 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, wurde er nie veröffentlicht, doch es werden weitere Versionen des Virus geschrieben und in Umlauf gebracht.

1982 Apple-Virus mit Nebenwirkung

Der 15-jährige Rich Skrenta schreibt den Virus **Elk Cloner** für das Betriebssystem Apple II. **Elk Cloner** wird ausgeführt, sobald ein Computer von einer infizierten Diskette aus gestartet wird und infiziert alle Disketten, die in das Diskettenlaufwerk des betroffenen Computers gelegt werden. Der Virus zeigt jedes 50. Mal nach Start des Computers eine Meldung an.

1985 E-Mail-Trojaner

Der Trojaner **EGABTR** verteilt sich über Posteingänge und gibt sich als Programm zur verbesserten Anzeige von Grafiken aus. Sobald er jedoch ausgeführt wird, löscht er alle Dateien auf der Festplatte und zeigt eine Meldung an.

1986 Der erste Virus für PCs

Brain, der erste Virus für IBM PCs, wurde angeblich von zwei Brüdern in Pakistan geschrieben, als sie bemerkten, dass Anwender ihre Software kopierten. Der Virus fügt eine Kopie seiner selbst sowie eine Copyright-Meldung auf sämtliche Kopien, die Kunden auf Disketten erstellen.

1987 **Der Christmas Tree-Wurm**

Dabei handelt es sich um eine elektronische Weihnachtskarte, die Programmcode enthält. Sobald der Anwender sie öffnet, zeichnet er, wie versprochen, einen Weihnachtsbaum, doch leitet sich auch an alle Adressen in dem Adressbuch des Anwenders weiter. Der daraus resultierende Datenfluss legt das weltweite IBM-Netz lahm.

1988 **Der Internetwurm**

Der 23-jährige Student Robert Morris infiziert das US DARPA-Internet mit einem Wurm. Er verbreitet sich auf Tausende Computer und infiziert sie aufgrund eines Programmierungsfehlers wiederholt, so dass sie abstürzen.

1989 **Trojaner verlangt Lösegeld**

Der AIDS-Trojaner verbreitet sich über Disketten und gibt vor, Informationen über AIDS und HIV zu enthalten. Der Trojaner verschlüsselt die Festplatte des Computers und fordert als Gegenleistung für das Kennwort Lösegeld.

1991 **Der erste polymorphe Virus**

Tequila ist der erste, weit verbreitete polymorphe Virus. Die Entdeckung von polymorphen Viren ist für Virenscanner schwierig, da sie ihr Erscheinungsbild mit jeder neuen Infektion verändern.

1992 **Die Michelangelo-Panik**

Der Michelangelo-Virus zielt darauf ab, jedes Jahr am 6. März (dem Geburtstag von Michelangelo) die Festplatten von Computern zu löschen. Nachdem zwei Unternehmen versehentlich infizierte Disketten und PCs verteilten, brach weltweit Panik aus, doch nur wenige Computer wurden tatsächlich infiziert.

1994 **Der erste E-Mail-Hoax**

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

1995 **Der erste Dokumentenvirus**

Concept, der erste Dokumenten- oder Makrovirus, tritt auf. Er verbreitet sich, indem er Makros in Microsoft Word ausnutzt.

1998 **Der erste Virus, der Hardware infiziert**

CIH oder Chernobyl ist der erste Virus, der Computer-Hardware beschädigt. Der Virus infiziert das BIOS, das für den Start des Computers erforderlich ist.

1999 **E-Mail-Viren**

Melissa, ein Wurn, der sich selbst per E-Mail weiterleitet, verbreitet sich weltweit.

Bubbleboy, der erste Wurm, der einen Computer allein durch das Lesen einer E-Mail infiziert, erscheint.

2000 **Palm-Virus**

Der erste Virus für das Palm-Betriebssystem tritt auf, allerdings werden keine Anwender infiziert.

2000 **Denial-of-Service-Attacken**

Durch Hacker verursachte Distributed Denial-of-Service-Attacken sorgen dafür, dass bekannte Websites, beispielsweise von Yahoo, eBay und Amazon stundenlang offline sind.

Der **Loveletter-Virus** ist der bisher "erfolgreichste" Virus.

2001 **Viren verbreiten sich über Websites oder Netzwerkfreigaben**

Schädliche Programme nutzen Schwachstellen in Software aus, so dass sie sich ohne Eingreifen des Anwenders verbreiten können. Nimda infiziert Computer von Anwendern, die einfach nur auf eine Website zugreifen. Sircam verbreitet sich über sein eigenes E-Mail-Programm sowie über Netzwerkfreigaben.

2003 **Zombie, Phishing**

Mithilfe des Sobig-Wurms übernehmen Hacker die Steuerung über Computer, so dass diese zu Zombies werden und zum Versenden von Spam missbraucht werden können.

Der Mimail-Wurm gibt sich als E-Mail von Paypal aus und fordert Anwender auf, ihre Kreditkartendetails zu bestätigen.

2004 IRC Bots

Schädliche IRC (Internet Relay Chat) Bots werden entwickelt. Trojaner legen das Bot auf einem Computer ab, es verbindet sich ohne Wissen des Anwenders mit einem IRC-Kanal und Hacker übernehmen die Steuerung über den Computer.

2005 Rootkits

DRM, ein Kopierschutz für Sony Musik-CDs, installiert ein Rootkit auf den Computern von Anwendern. Dieses modifiziert das Betriebssystem, damit Musik-CDs nicht mehr erkannt und kopiert werden können. Hacker entwickelten Trojaner, die diese Schwachstelle ausnutzen und eine versteckte Backdoor installieren.

2006 Aktien-Scams

Spam-Mails, die Aktien kleiner Unternehmen anbieten (Pump-and-Dump-Spam) ist stark verbreitet.

2006 Ransomware

Die Trojaner **Zippo** und **Archiveus**sind erste Beispiele für Ransomware. Die Trojaner verschlüsseln Dateien, als Gegenleistung für das Kennwort zur Entschlüsselung wir ein Lösegeld verlangt.

Egal, ob Sie Netzwerkadministrator sind, im Büro am Computer arbeiten oder einfach nur E-Mails lesen – dieses Buch ist wie für Sie gemacht! Hier werden aktuelle Sicherheitsbedrohungen und praktische Maßnahmen zum Schutz Ihrer Computer beschrieben.

5,00 £ / 7,50 $ / 7,60 €

ISBN 0-9553212-0-4

SOPHOS
secured.