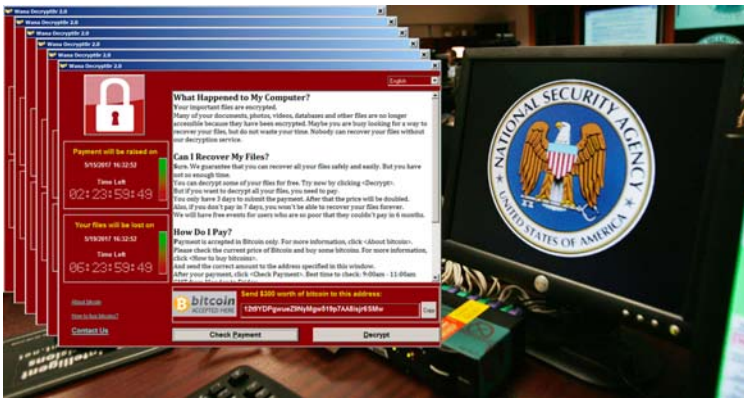
ARTEN VON MALWARE

Irgendwann sind wir alle einmal auf Malware gestoßen. Mittlerweile wurden Abertausende von Programmen entwickelt, um auf Ihr System, Ihre Dateien und Ihren Geldbeutel zuzugreifen. Während sie alle unterschiedliche Spuren hinterlassen, sie haben ihre Wurzeln in den simplen Anfängen. Die moderne Welt sieht sich sowohl kriminellen, wie auch staatlichen Hackern gegenüber, welche die Lebensweise aller bedrohen können. Aber die Anfänge von Malware waren frei von echter Malware. Zu dieser Zeit gab es lediglich die Absicht zu erkunden, was mit Computern tatsächlich möglich ist und nicht, um Schaden anzurichten, zu stehlen oder zu manipulieren.

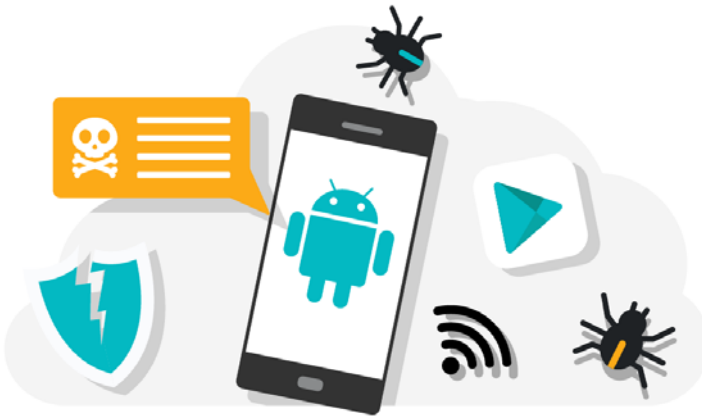


ADWARE

Adware ist zwar selten bösartig, kann jedoch sehr ärgerlich sein, da Ihr Computer gezwungen ist, Anzeigen herunterzuladen oder anzuzeigen, die Sie nicht sehen möchten. Diese Art von Malware stiehlt normalerweise keine Daten, wird jedoch in einigen Fällen zu einem echten Ärgernis, wenn beispielsweise Popups-Fenster nicht geschlossen werden können. Adware kann - vom Benutzer unerkannt - mit anderen Anwendungen installiert werden.

ANDROID MALWARE

Da die meisten Smartphones und Mobilgeräte mit Android laufen und das Google-Ökosystem offen ist, konzentrieren sich die meisten Malware-Angriffe auf Android. Im üblichen Szenario täuschen Cyberkriminelle dem Benutzer vor, sie würden reguläre Apps von Drittanbietern herunterladen oder auf den Google Play Store zugreifen, um angeblich nützliche Tools oder Spiele anzubieten.



„HINTERTÜR"

Hintertüren, sog. Backdoors, auch als geheime Passagen in ein System bezeichnet, sind weit verbreitet. Hersteller können diese entweder für die beabsichtigte Verwendung durch das eigene Personal oder für Strafverfolgungsbehörden einrichten oder unbeabsichtigt mit einer nachlässigen Codierung. Viren und andere Malware können ebenfalls solche Hintertüren erzeugen.

BOTS UND BOTNETS

Ein Bot ist eine Software, die zur Ausführung automatisierter Aufgaben entwickelt wurde. Bots können hilfreich sein, z. B. bei der Seitenindexierung für Suchmaschinen oder wenn Unternehmen sie zur Beantwortung von Kundenfragen verwenden. In Bezug auf IT-Sicherheit ist ein Bot jedoch ein mit Malware infiziertes Gerät, das die schädigenden Aufgaben ohne Kenntnis des Besitzers ausführt. In diesem Sinne ist ein Botnet ein Netzwerk solcher Geräte, mit denen Hacker häufig Spam- oder Phishing-Kampagnen oder andere bösartige Tätigkeiten ausführen. Schlaue Geräte für das Internet der Dinge wurden kürzlich das Ziel von solchen Botnet-Angriffen.

BROWSER HIJACKER

Einige Arten von Malware „übernehmen" Ihren Browser und ändern sein Verhalten. Infolgedessen kann der Browser eine neue Homepage, mehrere Symbolleisten, eine neue Suchmaschine oder eine Unzahl von Werbung anzeigen. Um den Schaden zu vergrößern, werden Sie möglicherweise sogar zu Webseiten weitergeleitet, die noch mehr Malware auf Ihr System herunterladen.

PROGRAMMFEHLER

Solche Programmfehler sind Fehler in einem Teil des Software-Codes. Sie existieren in allen Computerprogrammen, aber die meisten sind nur lästig. Wenn es sich jedoch um Sicherheitslücken handelt, können diese Ihr gesamtes System gefährden.

CRIMEWARE

Malware, die zur Begehung von Straftaten verwendet wird, um finanzielle Gewinne zu erzielen, wird als „Crimeware" bezeichnet. Sie umfasst verschiedene Arten von Schadsoftware.

KRYPTOWÄHRUNG MINER-MALWARE

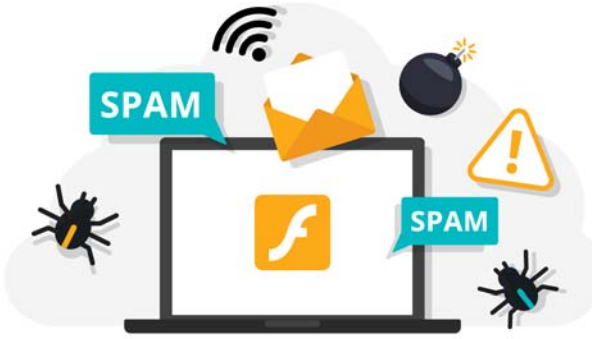
Mit der zunehmenden Popularität von Kryptowährungen entscheiden sich viele Nutzer, per Computer oder Webserver mit Kryptowährungen zusätzliches Geld zu verdienen. Wenn es um Geld geht, folgt jedoch bald Malware. Viele Hacker, die bestrebt sind, so viel Währung wie möglich „abzubauen", erobern in Botnetzen die PC-Leistung anderer für ihre eigenen Zwecke. Oft macht diese Art von Diebstahl den Computer für seinen Besitzer unbrauchbar, und das Opfer weiß nicht, warum es an Rechenleistung verliert. Geräte für das Internet der Dinge wurden auch für diese illegale Bereicherung ins Visier genommen.

GEFÄLSCHTE ODER BÖSARTIGE SICHERHEITS-SOFTWARE

In der letzten Dekade gab es unzählige Fälle mit gefälschter Sicherheitssoftware, getarnt als legale Anti-Malware- und Anti-Virenprogramme. Wenn Sie ein solches Tool installieren, fügen Sie sich selbst schweren Schaden zu und erlauben Cyberkriminellen, Ihr System zu infizieren, Ihre persönlichen Daten zu stehlen und dürfen anschließend noch für die Datenbereinigung zahlen, die Sie eigentlich nicht benötigen.

DATEILOSE MALWARE

Es gibt eine Art von Malware, die nicht dateiabhängig ist. Diese befindet sich nämlich im Arbeitsspeicher eines Computers und nicht auf der Festplatte, daher der Name. Dateilose Malware ist schwieriger zu erkennen, da sie keine Dateien enthält und beim Neustart verschwindet.



INTERNET DER DINGE – MALWARE

Intelligente Geräte, wie Router und Sicherheitskameras, können leicht mit Malware infiziert werden - und der Schaden ist in der Regel erheblich, weil die Sicherheitsvorkehrungen oft nicht ausreichen, um Malware-Angriffe abzuwehren. Solche IoT-Geräte, die wir zu Hause anschließen und wieder vergessen, gewähren Angreifern Zugriff auf unseren persönlichen Bereich und unsere persönlichen Informationen.

KEYLOGGER

Software, die alle vom Benutzer gedrückten Tasten erfasst, wird als Keylogger bezeichnet. Cyberkriminelle verwenden solche Keylogger, um Zugriff auf Konto-Informationen zu erhalten. Einige Unternehmen verwenden sie jedoch, um Mitarbeiteraktivitäten auf kriminelles oder illegales Verhalten hin zu verfolgen.

MALVERTISING

Malvertising ist nicht dasselbe wie Adware, da es über echte Anzeigen und Werbenetzwerke betrieben wird. Wenn Sie jedoch auf eine solche Anzeige klicken oder in einigen Fällen sogar nur darüber scrollen, wird Malware auf Ihren Computer heruntergeladen oder Sie werden auf eine schädliche Webseite weitergeleitet. Einige Cyberkriminelle nutzen seriöse Werbenetzwerke, wie große Nachrichtenportale, Video- und Audiodatenbanken oder sogar die Londoner Börse, um potentielle Opfer anzusprechen. Natürlich ist Geld die treibende Kraft jeder Kampagne von Cyberkriminellen, und Malvertising ist nicht anders. Fakt ist, Malvertising-Kampagnen können mit ihrer großen Reichweite Tausende von Computer infizieren, Kryptowährungs-Mining-Skripte, Ransomware, Trojaner und andere Viren verbreiten.

MOBILE MALWARE

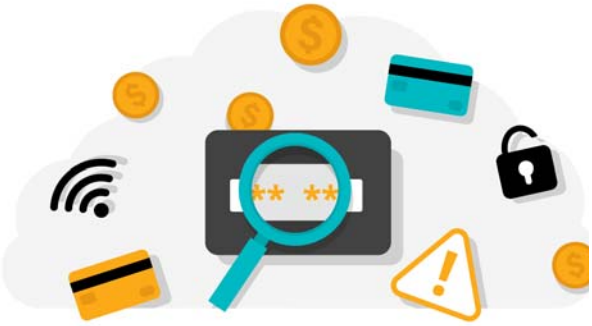
Mobile Geräte wie Smartphones und Tablets haben für Cyberkriminelle ein enormes Potenzial eröffnet. Diese Geräte werden täglich für Gespräche, zum Speichern von Fotos und Daten, usw. verwendet und enthalten Informationen über jeden Einzelnen von uns. Kein Wunder, dass Hacker daran arbeiten, verschiedene Schadprogramme speziell für Smartphones zu entwickeln. Wenn Ihr Gerät infiziert ist, können Cyberkriminelle Sie damit orten, Ihr persönliches Leben ausspionieren oder Sie gar erpressen. Phishing- und Social Engineering-Hacker bevorzugen E-Mail-Angriffe wie Phishing, um Benutzer dazu zu verleiten, ihre Konto-Informationen preiszugeben, bösartige Dateianhänge herunterzuladen oder Webseiten zu besuchen, von welchen automatisch Malware auf ihr System installiert wird. Spear Phishing funktioniert auf die gleiche Weise, mit dem einzigen Unterschied, dass es auf einen bestimmten Benutzer oder eine bestimmte Organisation abzielt.

PHISHING UND SOCIAL ENGINEERING

Hacker bevorzugen E-Mail-Angriffe wie Phishing, um Benutzer dazu zu verleiten, ihre Konto-Informationen preiszugeben, bösartige Dateianhänge herunterzuladen oder Webseiten zu besuchen, von welchen automatisch Malware auf ihr System installiert wird. Spear Phishing funktioniert auf die gleiche Weise, mit dem einzigen Unterschied, dass es auf einen bestimmten Benutzer oder eine bestimmte Organisation abzielt.

RAM SCRAPER

Malware, die Daten aus dem Arbeitsspeicher sammelt, wird als RAM-Scraper bezeichnet. Dieses Tool wird häufig verwendet, um POS-Terminals zu infizieren und Kreditkarteninformationen vor der Verschlüsselung zu stehlen. Es hat viele Fälle gegeben, die bekanntesten sind die Angriffe gegen die beiden großen US-Firmen Target und Home Depot.



RANSOMWARE

Cyberkriminelle setzen heutzutage häufig Ransomware ein und in knapp einem Jahr haben sich die Vorfälle fast verdreifacht. Im Grunde sperrt dieses bösartige Tool Ihr System und gibt Ihnen erst dann wieder Zugriff, wenn Lösegeld gezahlt wurde. Meist wird damit gedroht, dass bei Nicht-Erfüllung der Forderung peinliche oder persönliche Daten auf Social Media oder in anderen Portalen gestellt werden. Nachdem niemand seine „hässliche Seite" offen zeigen will, haben Cyberkriminelle auf diese Weise bereits ein Vermögen verdient.

Beispiel aus dem wirklichen Leben

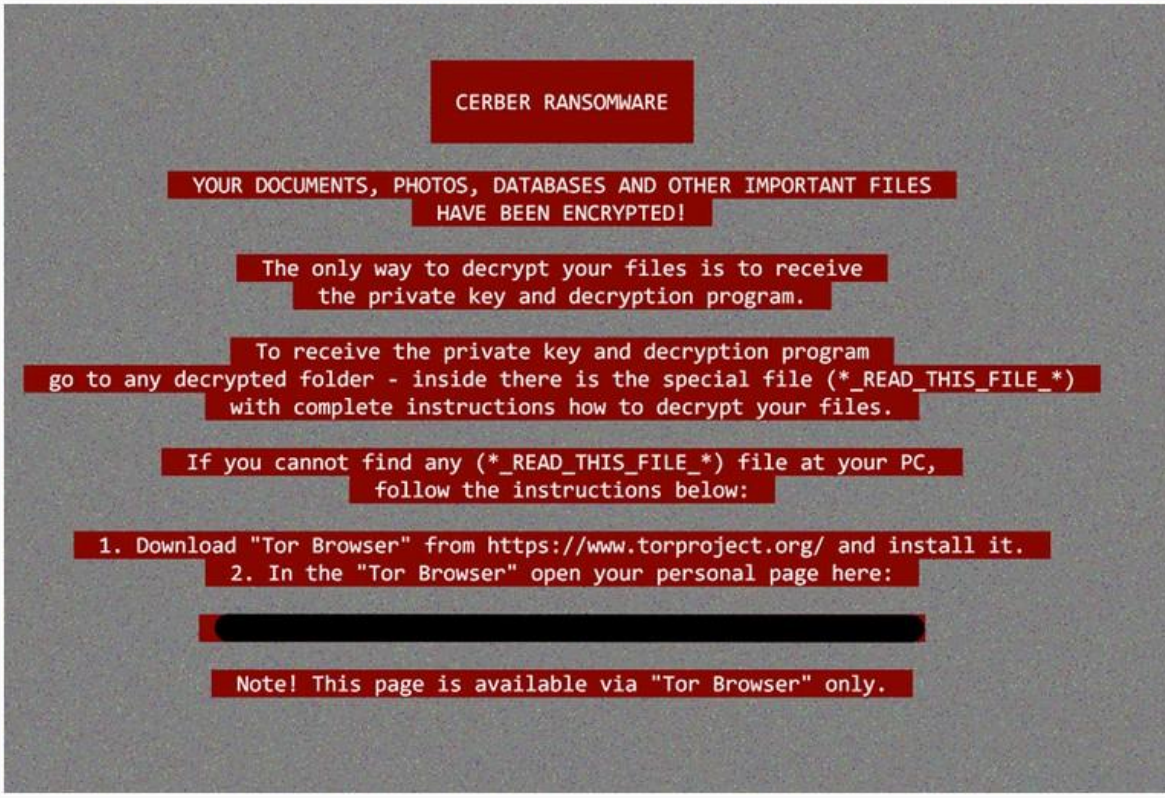


Bild: Malwarebytes „Ransomware verlangt eine Zahlung als Gegenleistung für das Entschlüsseln der verschlüsselten Dateien."

ROOTKIT

Rootkits sind Hacker-Tools, die den Administratorzugriff auf Ihr System ermöglichen. Das führt natürlich dazu, alles zu tun, ohne Ihr Wissen oder ohne Ihre Erlaubnis, inklusive Änderung Ihrer Einstellungen, Aufzeichnen Ihrer Aktivitäten, Zielen auf andere Systeme, usw. Beispiele hierfür sind Stuxnet und Flame.

SPAM

Spam bezieht sich auf die Junk-Mail, die Sie nicht in Ihrem Posteingang sehen möchten. Spam besteht normalerweise aus unerwünschter Werbung, kann jedoch auch schädlich sein, da Angreifer es für Betrug oder zum Senden infizierter Links oder Anhänge verwenden können.

SPYWARE

Software, die zum Sammeln von Informationen über eine Person oder eine Organisation ohne deren Erlaubnis verwendet wird, wird als Spyware bezeichnet. Dies kann von böswilligem Diebstahl von Informationen über gängige Webseiten-Tracking-Cookies bis hin zum offiziellen Ausspähen von Straftatverdächtigen oder ausländischen Regierungen reichen.

TROJANER

Diese Art von Malware, nach dem mythologischen Trojanischen Pferd in hellenistischer Zeit benannt, gelangt unter einem falschen Vorwand in Ihr System. Einmal an Bord, kann es Ihre Festplatte zerstören, Ihre Daten stehlen, Hintertüren für andere schädliche Malware öffnen, usw.

Trojaner werden per E-Mail oder beim Besuch infizierter Webseiten verteilt. Sie müssen jedoch heruntergeladen und ausgeführt werden, um schädlich zu werden und Cyberkriminelle erreichen dies nur allzuoft mit einem Trick. Die häufigste Art, einen Trojaner einzufangen, ist das gefälschte Antivirenprogramm, das vorgibt, dass Ihr Computer infiziert wäre und Sie ein Programm ausführen müssen, um den Virus loszuwerden.

Häufige Beispiele für Trojaner sind:

- Remotezugriffs-Trojaner: Tools, die einem Hacker den Remotezugriff auf Ihr System ermöglichen.
- Daten sendende Trojaner: Sie sammeln Daten von Ihrem Computer und senden sie an den Angreifer.
- Zerstörerische Trojaner: Beseitigt Ihre Dateien und Dienste.
- Trojaner zur Deaktivierung der Sicherheitssoftware: Deaktiviert alle Systemkomponenten, um Ihr Gerät vollständig für schädliche Software anfällig zu machen.

VIREN

Ein Virus ist eine Art von Malware, für die jedoch eine Aktion durch den Nutzer erforderlich ist, damit sie ausgeführt und auf andere Programme und Systeme übertragen werden kann. Es ist mitunter möglich, dass Ihr System in einem Botnet verborgen operiert, um Spam zu versenden, Kontodaten oder Kreditkarten-Informationen zu stehlen oder Ihr System vollständig zu sperren. Computerviren infizieren, sobald sie im System sind, andere Dateien und Programme und erschweren deren Bereinigung. Antivirenprogramme können den Schaden selten rückgängig machen, weshalb sie normalerweise die infizierte Datei unter Quarantäne stellen oder einfach löschen.

Die häufigsten Arten von Viren sind:

- Dateiviren: Sie infizieren ausführbare Dateien, die den Schaden beim Ausführen auf andere Dateien übertragen.
- Makroviren: In der Regel in Excel-Makros enthalten, werden diese Viren bei Ausführung eines Makros aktiviert und verbreiten sich dann, un andere Dateien zu infizieren.
- Master-Boot-Record-Viren: Mit diesen Viren verlieren Sie Ihre Boot-Records und Ihr System wird unbrauchbar.
- Polymorphe Viren: Um der Erkennung zu entgehen, werden viele Viren so codiert, dass sie ihre Form ändern.
- Stealth-Viren: Kaum zu finden, da sie unter legitimen Dateien oder Diensten verborgen sind.
- Multipartite-Viren: Hybride, die Programmdateien infizieren und sich bei der Ausführung in den Startdatensatz einmischen. Beim erneuten Laden des Systems kontaminiert der Virus den Speicher und breitet sich auf Ihrem gesamten System aus.

WIPER-MALWARE

Malware, die nur zum Zweck der irreversiblen Zersetzung oder Löschung aller Daten eines angepeilten Computers oder Netzwerks erstellt wurde, wird als Wiper-Malware bezeichnet. Manchmal werden Daten erst gelöscht, nachdem sie vom Ziel-PC heimlich abgerufen wurden. In anderen Fällen werden vor dem Angriff keine Informationen gespeichert. Die sog. Petya-Ransomware ist ein Beispiel aus den letzten Jahren. Diese wurde ursprünglich als eine Art Ransomware angesehen, jedoch stellten Benutzer und Forscher bald fest, dass auch die Zahlung von Lösegeld ihre Daten vor der Zerstörung durch Petya nicht retten würde.

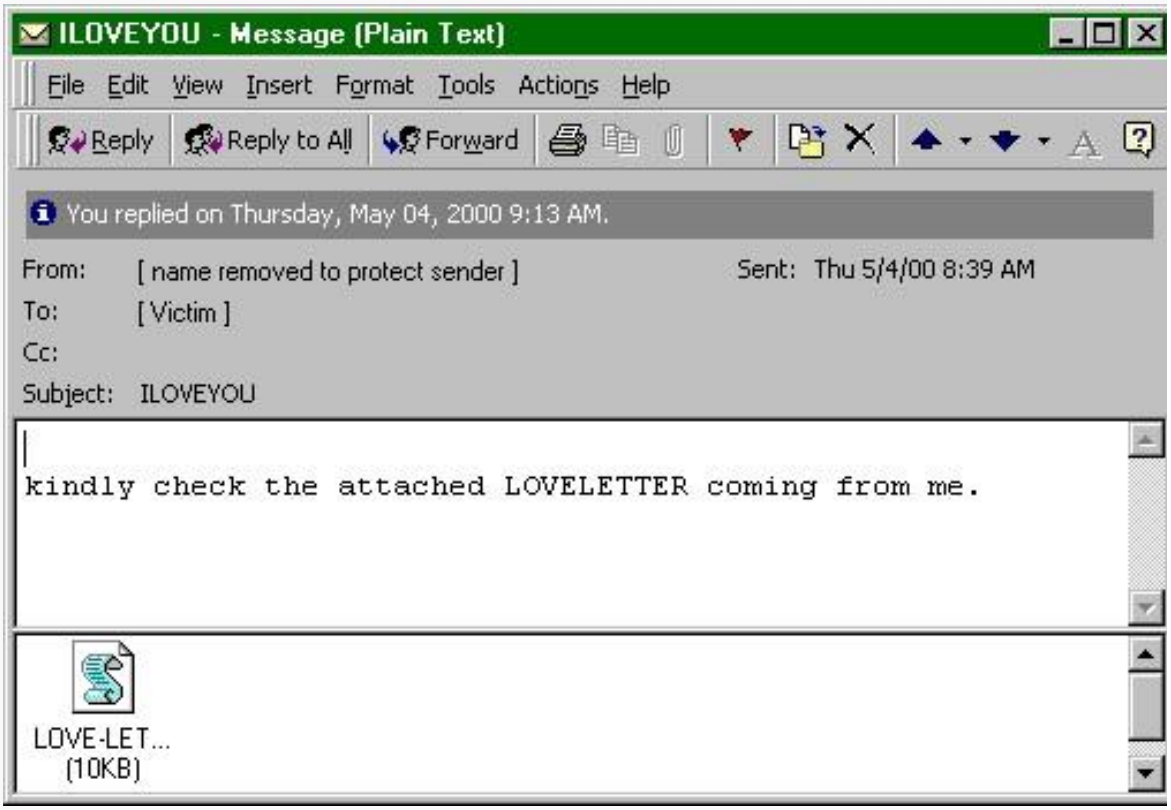
WURM

Ein Wurm benötigt keine Eingriffe von außen, um sich zu verbreiten, da er für den Start andere Programme ausnutzt. Obwohl andere Dateien oder Programme nicht wie bei Viren infiziert werden, ist diese eigenständige Malware berüchtigt, wenn es darum geht, sich von einem System oder Netzwerk auf ein anderes zu verbreiten, was dort zu Chaos führt, wenn sie übertragen wurde.

Mit dem Aufkommen der E-Mail-Kommunikation Ende des 20. Jahrhunderts traten Würmer immer häufiger auf. Die übliche Form der Zustellung waren verschlüsselte E-Mail-Anhänge, die sich nach dem Öffnen durch einfache Selbstreplikation problemlos über das gesamte Unternehmen verteilen konnten.

Ein Beispiel dafür war der ILoveYou-Wurm, der den gesamten Globus betraf und das Fernseh- und Telefonnetz und sogar den Alltag der Menschen beeinträchtigte.

Beispiel aus dem wirklichen Leben



Ein anderer Wurm, der SQL-Slammer, hat eine Microsoft SQL-Sicherheitslücke ausgenutzt, die zwar durch einen Patch abgedeckt war. Dieser Wurm war jedoch in der Lage, jeden nicht gepatchten SQL-Server im Internet in nur 10 Minuten zu infizieren.