Bundesamt
für Sicherheit in der
Informationstechnik

BSI-Leitfaden

Bedrohung der Informationssicherheit durch den gezielten Einsatz von Schadprogrammen

Teil 1: Gefährdungen und Maßnahmen im Überblick

Änderungshistorie

Datum	Änderung
22.01.2007	Version 1
03.04.2007	Version 1.1: Aktualisierung der Literaturhinweise

Ansprechpartner

Referat 113 - VS- und IT-Sicherheitsberatung

E-Mail: Referat113@bsi.bund.de

Tel.: +49 (0) 22899-9582-5220

Referat 125 - IT-Penetrationszentrum, Abwehr von Internetangriffen

E-Mail: Referat125@bsi.bund.de

Tel.: +49 (0) 22899-9582-5304

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Internet: http://www.bsi.bund.de

Thema und Zielgruppe

Die Bedrohung von schützenswerten Informationen hat durch die Weiterentwicklung von Schadsoftware eine neue Dimension erreicht. Dieser Leitfaden beschäftigt sich in erster Linie mit Schadprogrammen, die individuell für ein bestimmtes Opfer geschrieben werden und maßgeschneiderte Funktionen bieten. Sie sind besonders gefährlich, da sie von klassischen Viren-Schutzprogrammen und Firewalls nicht mehr zuverlässig erkannt werden können.

Der Leitfaden besteht aus drei Teilen:

1. Der erste Teil erläutert die Wirkungsweise moderner Schadprogramme, stellt das Gefahrenpotential dar und gibt einen Überblick über mögliche Sicherheitsmaßnahmen. Er richtet sich an **Führungskräfte** mit Zuständigkeit für Informationstechnik und Informationssicherheit, **IT-Sicherheitsbeauftragte** und interessierte **IT-Anwender.** Zum Verständnis ist allgemeines IT-Wissen von Vorteil.

2. Der zweite Teil beschreibt konkrete Maßnahmen und richtet sich an **IT-Sicherheitsbeauftragte** und **IT-Personal** mit guten technischen Kenntnissen. An vielen Stellen werden weitere Informationsquellen wie Studien, Best-Practice-Ratgeber oder Standards angegeben, die bei der praktischen Umsetzung der Maßnahmen hilfreich sind.

   Es gibt zurzeit *kein einzelnes* Sicherheitsprodukt, das einen ausreichenden Schutz gegen individuell angepasste Schadprogramme bietet. Es wird auch jeder Versuch scheitern, *die wichtigste* Maßnahme zu benennen. Einem Angreifer stehen vielfältige Techniken und Informationen zur Verfügung, um in fremde Rechner einzudringen. Ihm genügt eine einzige Schwachstelle im Programmcode einer Anwendung, in Konfigurationsdateien oder im Design einer IT-Landschaft. Sicherheitsmaßnahmen müssen daher ein breites Spektrum abdecken - vom Schutz einzelner Rechner über organisatorische Maßnahmen, die Ausbildung der Mitarbeiter bis zur Netzsicherheit. Dieser Leitfaden hilft bei der Auswahl wirksamer Sicherheitsmaßnahmen und gibt Hinweise, wo Standardmaßnahmen durch höherwertige ergänzt werden müssen.

3. Den dritten Teil bildet ein Kurztest zur Einschätzung der eigenen Bedrohungslage durch gezielte Angriffe mit Schadprogrammen. Das Ergebnis gibt **Führungskräften** einen ersten Anhaltspunkt, wie gut vertrauliche Informationen geschützt sind und wie wahrscheinlich es ist, durch Spionage oder Sabotage Schaden zu nehmen.

Redaktionelle Leerseite

Inhaltsverzeichnis

1 Managementzusammenfassung

Organisierte Kriminalität und Spionage mit Schadprogrammen

Wurden Schadprogramme in der Vergangenheit von experimentierfreudigen Cracker ohne finanzielle Interessen geschrieben und verbreitet, werden sie heute für kriminelle Handlungen und zur Spionage eingesetzt.

„Phishingangriffe“ auf Internetnutzer sind inzwischen hinlänglich bekannt: Privatpersonen werden beim Onlinebanking belauscht, Passwörter für Bezahlsysteme oder Internet-Auktionshäuser werden gestohlen und Kreditkartendaten ausgeforscht. Die Angriffe erfolgen wahllos über das Internet, ohne die Opfer im Vorhinein gezielt auszusuchen.

In der Öffentlichkeit weniger bekannt sind gezielte Angriffe auf ausgewählte Opfer mit Spionage- oder Sabotageprogrammen. Besonders gefährdet sind Behörden, Unternehmen und Universitäten, die auf die Vertraulichkeit ihrer Daten angewiesen sind. Die möglichen Schäden sind vielschichtig: wirtschaftliche Verluste, Bedrohung der inneren Sicherheit, Preisgabe von Verhandlungspositionen, Kompromittierung von einzelnen Personen oder Institutionen. Mit Schadprogrammen lassen sich auch gezielte Angriffe auf die Verfügbarkeit von Systemen oder die Integrität von Daten durchführen.

Warum sind moderne Schadprogramme so gefährlich?

Viren-Schutzprogramme und Firewalls werden überlistet

Lange Zeit boten Viren-Schutzprogramme, Firewalls und regelmäßige Softwareupdates einen zuverlässigen Schutz vor Schadsoftware. Die Sicherheitslage hat sich jedoch grundlegend geändert. Die neue Generation von Schadsoftware ist so gefährlich, da sie von Viren-Schutzprogrammen und Firewalls nicht mehr zuverlässig entdeckt oder aufgehalten werden kann.

Die Anzahl bekannter Schadprogramme steigt

Die Anzahl bekannter Schadprogramme steigt seit Jahren dramatisch an. Zum einen werden immer mehr Schwachstellen bekannt, die von Schadprogrammen genutzt werden können, um beliebigen Programmcode auf einem Opfersystem auszuführen. Zum anderen gibt es immer bessere Tools, mit denen sich Schadprogramme relativ einfach programmieren, verändern und an spezielle Rahmenbedingungen anpassen lassen. Im Internet finden sich vielfältige Anleitungen und sogar Toolkits zu Eigenbau von Schadsoftware.

Alle Dateien können gefährlich sein, nicht nur ausführbare

Galten früher nur wenige Dateitypen als potentiell gefährlich (z. B. ausführbare Dateien in E-Mail-Anhängen oder Makros), muss die Liste der entsprechenden Dateien ständig erweitert werden. Auch in Officedateien, Bildern, Videos oder PDF-Dateien lässt sich Schadcode transportieren. Gezielte Angriffe lassen sich zudem gegen alle Betriebssysteme durchführen - nicht nur gegen Windows-Rechner.

Schwachstellen werden immer schneller ausgenutzt

Wird eine Schwachstelle in einer IT-Anwendung bekannt, dauert es kaum mehr eine Woche, bis ein passendes Schadprogramm veröffentlicht wird. Bis zum Einspielen eines Sicherheitsupdates ist ein betroffenes System gefährdet. Diese Zeitspanne kann in Einzelfällen mehrere Monate dauern.

Moderne Schadprogramme sind multifunktional

Die Funktionen von Schadprogrammen werden immer vielfältiger: Sie können fremde Rechner vollständig kontrollieren, Daten ausspionieren oder IT-Systeme sabotieren. Zusätzlich besitzen sie hoch entwickelte Tarnfunktionen, laden Updates über das Internet und funktionieren auf verschiedenen Betriebssystemen.

Wie erfolgen Angriffe?

Früher mussten Spione und Datendiebe erhebliche Anstrengungen unternehmen, um an die gewünschten Informationen zu gelangen und diese abzutransportieren. Das Anbringen von Wanzen, das Abhören von Leitungen oder Einbrüche in geschützte Objekte waren zudem immer mit Gefahren verbunden.

Heute kann ein Angreifer über das Internet auf fremde Rechner zugreifen. Hat er einen Arbeitsplatz-Rechner unter seine Kontrolle gebracht, kann er riesige Datenmengen automatisiert nach Stichworten durchsuchen und danach spurlos kopieren und anonym weltweit verschicken - und das bequem und sicher von jedem beliebigen Büro, Hotelzimmer oder WLAN-Hotspot aus.

Am häufigsten werden E-Mail-Anhänge oder präparierte Webseiten verwendet, um Schadprogramme auf einem fremden Rechner zu platzieren. Auch über externe Datenträger (Werbe-CDs, Konferenzunterlagen, Produktbeschreibungen, Gesprächsprotokolle uvm.) werden Spionageprogramme verbreitet.

In den meisten Fällen hat der Angreifer im Vorfeld sorgfältig recherchiert und das Angriffsmedium (das „Trojanische Pferd“) so sorgfältig vorbereitet, dass das Opfer kaum eine Chance hat, die Falle zu erkennen.

BEISPIEL: ANGRIFF MIT PRÄPARIERTEN WMF-BILDERN

Am Beispiel der „WMF-Schwachstelle“ lassen sich sehr gut die geschilderten Gefahren und Angriffsmethoden darstellen:

- *Bilder gelten allgemein als „harmloses“ Datenformat. Mitte Dezember 2005 wurden allerdings Informationen über eine bislang unbekannte Windows-Schwachstelle bei der Anzeige von Bildern des Typs WMF im Internet für 4000 $ zum Kauf angeboten.*
- *Am 27. Dezember wurde die Schwachstelle erstmalig öffentlich beschrieben. Besonders tückisch war, dass bereits der Besuch einer präparierten Webseite zur Infektion ausreichte - ohne weitere Aktionen des Anwenders. Bei WMF-Dateien in einem E-Mail-Anhang führte bereits die Anzeige im Vorschaufenster zur Ausführung des Schadcodes.*
- *Innerhalb einer Woche wurden mehrere hundert Internetseiten mit infizierten Bildern registriert. Darunter befanden sich auch Trojanische Pferde, die Zugangsdaten fürs Onlinebanking ausspionierten. Viren-Schutzprogramme konn-*

ten die infizierten Dateien nur teilweise erkennen, da diese immer wieder in neuen Varianten auftauchten.

- *Am 2. Januar erhielten nach britischen Medienberichten einige Mitglieder des englischen Parlaments E-Mails mit präparierten WMF-Dateien im Anhang. Es wurde vermutet, dass die Empfänger gezielt ausspioniert werden sollten.*
- *Am 5. Januar wurde von Microsoft ein Sicherheitspatch veröffentlicht.*
- *Auch Wochen später wurden noch Angriffe mit WMF-Dateien registriert.*

2 Täter und Gefahren

Die Programmierer von Schadprogrammen waren in der Vergangenheit zumeist Saboteure oder experimentierfreudige Cracker ohne finanzielle Interessen. Sie strebten nach Ruhm, Selbstbestätigung oder Rache und verursachten spektakuläre Störungen des IT-Betriebs. Ein Angriff blieb daher selten unbemerkt. Während diese klassischen Angriffe stetig zurückgehen, arbeiten die meisten Schadprogramme heute im Verborgenen, kontrollieren ihre Opfer und spähen vertrauliche Informationen aus. Die Angreifer haben handfeste materielle oder ideologische Ziele und bewegen sich im Umfeld von organisierter Kriminalität oder Spionage. Es gibt zwei grundlegend unterschiedliche Vorgehensweisen, um Schadprogramme gewinnbringend einzusetzen:

1. Ein Angreifer möchte möglichst viele Rechner infizieren und verbreitet ungezielt massenhaft Schadsoftware über das Internet.
2. Ein Opfer wird gezielt ausgewählt und mit individuell erstellten Programmen angegriffen. Eine massenhafte Verbreitung der Angriffsprogramme über das Internet wird bewusst vermieden, damit die Hersteller von Schutzsoftware keine Muster erhalten. Ohne Muster ist eine Erkennung mit Schutzprogrammen kaum möglich.

In den nächsten Abschnitten werden die zwei Angriffsvarianten näher beschrieben - Behörden und Unternehmen können durch beide geschädigt werden. Die Darstellung beruht auf Erkenntnissen aus der Praxis und lässt sich durch ein Studium der in Kapitel 7 zusammengestellten Publikationen über bekannt gewordene Angriffe vertiefen.

Angriffe mit Massen-E-Mails und Botnetzen

Ein bekanntes Beispiel für diese Angriffvariante ist das Ausspionieren von Zugangsdaten für Online-Konten, Auktionshäuser oder Bezahlsysteme. Die Angreifer verschicken E-Mails wahllos an möglichst viele Personen und versuchen, die Empfänger zum Öffnen eines angehängten Schadprogramms oder zum Besuch einer mit Schadsoftware präparierten Webseite zu verleiten. Die Schadprogramme spionieren dann den IT-Anwender aus oder setzen Sicherheitsfunktionen (z. B. SSL beim Online-Banking) außer Funktion.

Schadprogramme, die massenhaft im Internet kursieren, werden in der Regel den Herstellern von Schutzsoftware gemeldet und lassen sich durch Viren-Schutzsoftware abwehren. Es dauert allerdings wenige Stunden bis Tage, bis Erkennungsmuster für die Schutzprogramme bereit gestellt werden. In dieser Zeit sind IT-Anwender ungeschützt.

Weniger bekannt sind Schadprogramme (sogenannte Bots), die einem Angreifer die Fernsteuerung eines fremden Rechners erlauben. Es ist nicht selten, dass ein einzelner Angreifer die Kontrolle über mehrere tausend Rechner gleichzeitig - ein „Botnetz“ - besitzt. Diese gebündelte Rechenleistung kann von Kriminellen für verschiedene Angriffe auf Behörden und Unternehmen genutzt werden:

AUS DER PRAXIS: BOTNETZ MIT 100.000 RECHNERN

Ein gigantisches Botnetz wurde im Oktober 2005 von der Polizei in den Niederlanden enttarnt. Drei festgenommene junge Männer sollen mindestens 100.000 Rechner unter ihrer Kontrolle gehabt haben. Sie haben auf diesen Rechnern Zugangsdaten von Kreditkarten, Paypal-Konten und eBay-Accounts ausgespäht und weiterverkauft. Weiterhin wurde berichtet, dass Unternehmen mit Denial-of-Service-Attacken erpresst wurden. In mindestens einem Fall wurde der angedrohte Angriff auch tatsächlich durchgeführt. Andere Unternehmen wurden mit Provisionsbetrug (siehe unten) geschädigt. (Quelle: www.heise.de/newsticker/meldung/64742)

Koordinierte Angriffe auf Behörden und Unternehmen

Botnetze können sehr preiswert (ca. 1 Cent pro Rechner und Tag) auch gut ausgebaute E-Mail-Server und Internet-Anbindungen in Behörden und Unternehmen für mehrere Tage oder sogar Wochen lahm legen. Hängen Geschäftstätigkeit oder Image von der Verfügbarkeit der Internet-Dienste ab, können die Folgen beträchtlich sein.

Am häufigsten werden Botnetze jedoch zum Spam-Versand eingesetzt. Die Kosten für das Löschen unerwünschter E-Mails sind ärgerlich, bedrohen aber nicht die Existenz. Massive Schäden können dagegen durch eine indirekte Folge von Spam entstehen. Wenn ein Spam-Versender den Namen einer Behörde oder eines bekannten, seriösen Unternehmens als Absender für seine Spam-Mails verwendet, werden im schlimmsten Fall automatisiert Millionen Antwort-E-Mails an den vermeintlichen Absender gesendet (z. B. „E-Mail konnte nicht zugestellt werden."). Die meisten E-Mail-Server sind nicht für derartige Belastungen ausgelegt, so dass die E-Mail-Kommunikation zusammenbricht.

Darüber hinaus gab es gezielte Denial-of-Service-Attacken auf einzelne Unternehmen oder Behörden. Beispielsweise wurden Verbraucherschutzseiten, die über Spam und betrügerische Dialer aufklären, mehrfach durch gebündelte Denial-of-Service-Angriffe überlastet. Denial-of-Service-Angriffe werden auch häufig nur angedroht, um von den Opfern Schutzgeld zu erpressen. Werden tatsächlich Angriffe durchgeführt, sind in den meisten Fällen Konkurrenten oder ideologisch motivierte Gruppen die Auftraggeber.

Provisionsbetrug

Viele Betreiber von kommerziellen Webseiten zahlen Provisionen an registrierte Vertriebspartner, wenn Internetsurfer auf ihre Webseite weitergeleitet werden oder wenn die Partner Werbe-Popup-Software auf den Rechnern potentieller Kunden installieren. Ein Botnetz-Betreiber (oder „-Mieter") kann sich daher als Partner registrieren lassen und mit einer Botnetz-Armee hohe Provisionen erwirtschaften - ohne dass der Betreiber der Webseite einen einzigen Kunden gewinnen würde.

Gezielte Angriffe mit maßgeschneiderten Schadprogrammen

Die zweite Angriffsvariante ist der gezielte Angriff auf ausgewählte Opfer mit maßgeschneiderten Programmen (z. B. Trojanischen Pferden). Diese werden speziell an bestimmte Einsatzumgebungen angepasst, so dass sie von Viren-Schutzprogrammen nicht erkannt werden.

Zugriff auf vertrauliche Daten: Spionage, Erpressung, Kompromittierung

Behörden, Unternehmen und Universitäten, die auf die Vertraulichkeit ihrer Daten angewiesen sind, sind durch Angriffe mit Spionageprogrammen besonders gefährdet. Die möglichen Schäden sind vielschichtig: wirtschaftliche Verluste, Bedrohung der inneren Sicherheit, Preisgabe von Verhandlungspositionen, Kompromittierung von einzelnen Personen oder Institutionen. Auch Erpressungsfälle sind aktenkundig: Die Täter drohen damit, gestohlene Informationen an die Konkurrenz zu verkaufen oder zu veröffentlichen. Andere verschlüsseln im Zuge ihres Angriffs wichtige Daten auf Systemen des Opfers und verlangen „Lösegeld" für ein Passwort zur Entschlüsselung.

Die Techniken, um vertrauliche Informationen auf fremden Rechnern zu sammeln, sind ausgereift und werden nachweislich auch angewendet. Die gesammelten Informationen werden dann unentdeckt über das Internet an den Angreifer gesendet. Eine Firewall kann aber nur die Kommunikation unterbinden, die den Regeln widerspricht. E-Mail und Surfen werden jedoch fast überall zugelassen und reichen aus, um Informationen zu verschicken. Spionageprogramme können so viele Monate oder sogar dauerhaft unentdeckt arbeiten.

AUS DER PRAXIS: WIRTSCHAFTSSPIONAGE IN ISRAEL

Ein umfangreicher Fall von Industriespionage wurde im Mai 2005 in Israel bekannt. Mit Hilfe von Spionageprogrammen wurden bis zu 60 Unternehmen und Einzelpersonen über Monate durch ihre Konkurrenz ausspioniert. In allen Fällen konnten die eingesetzten Viren-Schutzprogramme die Spionageprogramme nicht erkennen. Beim Einschleusen der Schadsoftware wurde immer die Gutgläubigkeit der Opfer ausgenutzt. Neben Werbemedien und unverdächtigen E-Mails wurden auch CDs mit Informationen und Datensammlungen verwendet, die den Opfern sogar zum Kauf angeboten wurden.

Der entstandene Schaden durch die Spionage kann nur schwer beziffert werden. Die Börse reagierte mit spürbaren Kursverlusten bei betroffenen Unternehmen. Überführt wurde der Täter nur durch Zufall, als er ein Schadprogramm in seinem privaten Umfeld einsetzte.

Früher mussten Spione und Datendiebe erhebliche Anstrengungen unternehmen, um an die gewünschten Informationen zu gelangen: Das Anbringen von Wanzen, das Abhören von Leitungen oder Einbrüche in geschützte Objekte waren immer mit Gefahren verbunden. Zudem waren bestimmte Informationen nur sehr schwer zu finden. Hatte man es dennoch geschafft, mussten diese unentdeckt abtransportiert oder mühsam von Hand kopiert werden. In jedem Fall war ein beträchtlicher Zeitaufwand notwendig. Der Anschluss eines Netzes an das Internet erfüllt somit den Wunschtraum aller Angreifer. Riesige Datenmengen können automatisiert nach Stichworten durchsucht und danach spurlos kopiert und anonym weltweit verschickt werden - und das bequem und sicher von jedem beliebigen Büro, Hotelzimmer oder WLAN-Hotspot aus.

AUS DER PRAXIS: SPIONAGE BEI ERICSSON

Im April 2005 wurde in Schweden ein Mann wegen Spionage zu einer mehrjährigen Haftstrafe verurteilt. Im März 2002 verschaffte er sich mit Schadprogrammen Zugang zum weltweiten Unternehmensnetz von Ericsson. Bis zu seiner Festnahme im Oktober 2004 forschte er mehrere Tochterfirmen aus und kopierte eine große Anzahl geheimer Daten, darunter den Quellcode zu den Mobiltelefonen aus dem Hause Sony Ericsson sowie Militärgeheimnisse der schwedischen Streitkräfte. Der schwedische Geheimdienst wurde auf den Spion aufmerksam, als dieser unvorsichtig wurde und geheime Daten im Internet zum Kauf anbot.

Sabotage

Wichtige Aufgaben in kritischen Bereichen wie Transport und Verkehr, Energie, Telekommunikation oder Verwaltung können nur dann uneingeschränkt erfüllt werden, wenn die Informationstechnik ohne größere Beeinträchtigungen verfügbar ist. Mangelhafte Notfallplanung (Business Continuity) und IT-Probleme waren beispielsweise wesentliche Ursachen für den größten Stromausfall der amerikanischen Geschichte im August 2003. Bösartige Software mit Sabotagefunktionen oder zur Kontrolle fremder Rechner kann daher unabsehbaren Schaden verursachen.

3 Schadprogramme: Wie sie funktionieren

3.1 Mit welchen „Schadprogrammen“ beschäftigt sich dieser Leitfaden?

Das BSI möchte mit diesem Leitfaden in erster Linie auf Gefahren durch Schadsoftware, die individuell für ein bestimmtes Opfer geschrieben wird, aufmerksam machen. Diese ist so konstruiert, dass sie maßgeschneiderte Funktionen bietet und in der Regel von den klassischen Viren-Schutzprogrammen nicht erkannt wird.

Die Medien berichten regelmäßig über derartige Angriffe und sprechen von „Trojanischen Pferden“. Gemeint sind damit Programme, die auf einem Rechner ohne Wissen und ohne Einwilligung des Besitzers aktiv sind und heimlich eine Schadfunktion ausführen. In diesem Leitfaden werden allgemeinere Begriffe wie „Schadprogramm“ oder „Schadsoftware“ bevorzugt. Die Einteilung von Schadprogrammen in verschiedene Klassen (Viren, Würmer, Spyware, Trojanische Pferde ...) hat unbestritten ihre akademische Berechtigung - für den Praktiker ist sie aber verwirrend und nicht notwendig. Im Zuge eines Angriffs kommen in der Regel verschiedene, modular aufgebaute Programme nacheinander oder zeitgleich zum Einsatz. Technisch interessierte Leser finden eine ausführliche Typologie von Schadprogrammen in [MID].) Aus historischen Gründen wird weiterhin von „Viren-Schutzprogrammen“ gesprochen, obwohl diese Programme auch andere Schadsoftware erkennen können.

3.2 Wozu werden Schadprogramme eingesetzt?

Frühere Schadprogramme waren unflexibel und hatten häufig nur eine einzige Aufgabe. Moderne Schadprogramme haben nichts mehr gemeinsam mit ihnen, sie bieten dem Angreifer umfangreiche Kommunikations- und Steuerungsmöglichkeiten und besitzen eine Vielzahl von Funktionen. Diese lassen sich beliebig kombinieren sowie über das Internet nachrüsten und aktualisieren. Im Folgenden eine kurze Zusammenfassung der Möglichkeiten moderner Schadsoftware:

- **System fernsteuern**

  Programme zur Fernsteuerung geben dem Angreifer eine ähnliche Kontrolle über das angegriffene System, wie sie der Benutzer selbst hat, und erlauben vollen Zugriff auf alle Systemressourcen. Der Angreifer kann so z. B. das Dateisystem durchsuchen, Sicherheitsmechanismen abschalten, weitere Schadprogramme installieren oder den Rechner zum Versand von E-Mails nutzen.

- **Passwörter ausforschen**

  Auf privat genutzten Rechnern haben es die Angreifer in der Regel auf Zugangsdaten zum Online-Banking, zu Internet-Bezahlsystemen oder Auktionshäusern abgesehen. In Behörden und Unternehmen sind Zugangsdaten für Benutzerkonten, IT-Anwendungen oder Netzdienste von Interesse.

- **Daten sammeln**

  Es wird gezielt nach Dateien mit bestimmten Schlüsselwörtern gesucht. Diese werden dann komprimiert, häufig verschlüsselt und über das Internet an den Angreifer verschickt.

- **Tastatureingaben und Bildschirmausgabe aufzeichnen**

  Ein „Keylogger“ zeichnet alle Tastatureingaben des angegriffenen Systems auf und sendet die Daten (meist verschlüsselt) über das Internet an den Angreifer. Während im Jahr 2000 ca. 300 Keylogger bekannt waren, gab es im Jahr 2005 bereits über 6000 verschiedene (Quelle: NISCC Monthly Bulletin November 2005).

- **Vandalismus und Sabotage**

  Daten auf dem angegriffenen System können verändert oder gelöscht werden. Oftmals werden diese Programme erst beim Eintreten eines bestimmten Ereignisses aktiv (z. B. ein bestimmtes Datum).

- **Angriffe auf Dritte anonym durchführen**

  Mit einem infizierten Rechner unter seiner Kontrolle kann ein Angreifer bei Angriffen auf Dritte seine eigene Identität verschleiern. Wird der Angriff zurückverfolgt, lässt sich lediglich der gekaperte Rechner, aber nicht das System des eigentlichen Angreifers ermitteln.

- **Schutzsoftware deaktivieren**

  Um ihre Aufgabe ungestört verrichten zu können, suchen professionelle Schadprogramme nach bekannter Schutzsoftware und deaktivieren sie. Die Folge ist ein ungeschütztes System, welches nun für den Angreifer komplett geöffnet ist.

- **Tarnung**

  Schadprogramme können so versteckt werden, dass infizierte Dateien, Datensammlungen oder Prozesse von Standardtools nicht angezeigt werden (z. B. Speicherung in ungenutzten Bereichen einer Festplatte, Processinjection, Kernelmanipulationen, Flashupdate des BIOS).

- **Manipulation der Bildschirmanzeige**

  Die typischen SSL-Sicherheitsmerkmale (Schlosssymbol und „https:// ...“ in der Adresszeile des Browsers) können beispielsweise gefälscht oder durch Bilder überblendet werden.

- **Manipulation von Internetverbindungen**

  Schadprogramme können Internetverbindungen manipulieren. Ein IT-Anwender gibt beispielsweise die Adresse „www.Meine-Bank.de“ in seinen Browser ein und wird unbemerkt auf eine vom Angreifer betriebene Seite umgeleitet. Die Update-Funktion von Viren-Schutzprogrammen wird nutzlos, wenn ein Schadprogramm die Adressen des Update-Servers fälscht.

3.3 Warum ist moderne Schadsoftware so gefährlich?

Schadprogramme gibt es schon lange. Warum die Gefährdung zunimmt und die bekannten Sicherheitsmaßnahmen zunehmend ihre Schutzwirkung verlieren, steht in diesem Kapitel.

Die Anzahl bekannter Schadprogramme steigt.

Warum steigt die Anzahl von Schadprogrammen? Zum einen werden immer mehr Schwachstellen bekannt, die von Schadprogrammen genutzt werden können. Zum anderen gibt es immer bessere Tools, mit denen sich Schadprogramme relativ einfach programmieren, verändern und an spezielle Rahmenbedingungen anpassen lassen.

STATISTIK: IMMER MEHR SCHADPROGRAMME

Ende 2005 waren ca. 150.000 Schadprogramme für Windows-Systeme bekannt. Im ersten Quartal 2003 wurden 994 neue Viren und Würmer gefunden, 2004 waren es im gleichen Zeitraum 4496 und 2005 bereits 10866. Quelle: Symantec

Am Beispiel von „Zotob“ wird deutlich, wie schnell die Verfasser bösartiger Software arbeiten: Am 14.08.2005 wurde Zotob erstmals beschrieben. Nach zwei Tagen gab es fünf, zwei Wochen später bereits mehr als 100 Varianten.

Wenig qualifizierte Programmierer konnten früher keinen eigenen Schadcode entwickeln. Heute sind sie dazu problemlos in der Lage, da im Internet vielfältige Anleitungen, Beispielcode und Toolkits zu finden sind. Auf Bestellung werden Schadprogramme auch von Experten maßgefertigt.

Viren-Schutzprogramme bieten keinen ausreichenden Schutz gegen gezielte Angriffe.

Viren-Schutzprogramme erkennen Schadprogramme an typischen Codesequenzen („Signaturen“). Die Hersteller beobachten die Szene und erstellen möglichst schnell, nachdem ein neues Schadprogramm aufgetaucht ist, eine Signatur aus typischen Codezeilen. Während die Hersteller von Schutzsoftware ein Schadprogramm noch analysieren, kann dieses nicht entdeckt werden. Sogenannte heuristische Viren-Schutzprogramme versprechen, auch unbekannte Schadsoftware zu entdecken. In Praxistests stellt sich aber immer wieder heraus, dass die heuristischen Funktionen noch nicht zuverlässig arbeiten und die Nachweiswahrscheinlichkeit für Schadprogramme nicht wesentlich erhöhen.

Ein Angreifer hat gute Erfolgsaussichten, wenn er bekannte Schadsoftware leicht verändert. Wenn er ein angepasstes - oder sogar völlig neues - Schadprogramm nur bei sehr wenigen Opfern einsetzt, ist es nahezu ausgeschlossen, dass dieses Programm den Herstellern von Schutzsoftware überhaupt bekannt wird. Eine Erkennung durch signaturbasierte Standard-Schutzsoftware ist daher fast unmöglich.

Selbst wenn ein technisch unkundiger Angreifer nur auf bekannte Schadprogramme zurückgreift, hat er durchaus Chancen - er muss nur ein möglichst seltenes Exemplar auswählen. Kein Viren-Schutzprogramm erkennt alle Schadprogramme.

PRAXISTEST: WIRKSAMKEIT VON VIREN-SCHUTZPROGRAMMEN

Die Dramatik der Situation verdeutlicht folgende Untersuchungen des BSI (Ende 2005):

Selbst wenn fünf gängige Viren-Schutzprogramme gleichzeitig betrieben würden, würden mindestens 1500 bekannte Trojanische Pferde nicht erkannt.

Firewalls lassen sich umgehen.

Firewalls können keine eingehenden Schadprogramme erkennen, die über erlaubte Kommunikationswege wie E-Mail, HTTP oder über Datenträger eingeschleust werden. Auch die Kommunikation zwischen Schadsoftware und Angreifer lässt sich kaum unterbinden, wenn Dienste und Programme verwendet werden, die auch im geschäftlichen Alltag genutzt werden. Erschwerend kommt hinzu, dass auch viele normale Programme einen Tunnel durch die Firewall aufbauen - was von den Herstellern gerne als „Feature“ verkauft wird.

Die Anzahl bekannter Schwachstellen in IT-Anwendungen, die für Angriffe ausgenutzt werden können, steigt.

Blieben früher die meisten Schwachstellen unentdeckt, werden sie heute in großer Zahl im Internet publiziert. Potentielle Angreifer können so auf umfangreiche Informationen zurückgreifen und diese dann zum Eindringen in fremde Rechner missbrauchen. Die zunehmende Komplexität von IT-Anwendungen und Betriebssystemen ist sicherlich eine Ursache für die Zunahme von bekannten Schwachstellen. Während Windows 3.1 im Jahr 1990 mit 2,5 Mio. Programmzeilen auskam, benötigte Windows XP im Jahr 2002 schon 40 Mio. Zeilen. Ein weiterer Grund liegt darin, dass immer leistungsfähigere Tools zur Analyse von Programmcode zur Verfügung stehen. Der Weg von einer

Schwachstelle zum funktionierenden Schadprogramm wird durch diese neuen Methoden immer kürzer und einfacher. Gerade die Analyse von Updates und Patches wird dazu genutzt, Schwachstellen und Sicherheitslücken von Programmen zu identifizieren.

STATISTIK: ANZAHL DER BEKANNTEN SCHWACHSTELLEN STEIGT

Die Anzahl veröffentlichter Schwachstellen in weit verbreiteten Anwendungen steigt exponentiell. Laut CERT/CC wurden im Jahr 1995 171 Vulnerabilites gefunden, 2005 dagegen schon 5990. Man muss davon ausgehen, dass nur ein Bruchteil aller Schwachstellen überhaupt veröffentlicht wird. (Quelle: www.cert.org/stats/cert_stats.html)

Alle Dateien können gefährlich sein, nicht nur ausführbare.

Galten früher nur wenige Dateitypen als potentiell gefährlich (z. B. ausführbare Dateien in E-Mail-Anhängen), muss die Liste der entsprechenden Dateien ständig erweitert werden. Beispielsweise wurden PDF-Dateien oder JPEG-Bilder lange Zeit als unbedenklich angesehen. Inzwischen wurden Schwachstellen bekannt, die unter bestimmten Bedingungen dazu führen, dass beim Öffnen der Dateien beliebiger Code ausgeführt werden kann. Durch zeitnahes Einspielen von Updates und Patches und die Verwendung aktueller Viren-Schutzprogramme lässt sich das Risiko nur reduzieren, aber nicht völlig beseitigen.

BEISPIEL: SCHWACHSTELLE BEI DER ANZEIGE VON JPEG-BILDERN

Microsoft beschreibt im Security Bulletin MS04-028 eine kritische Schwachstelle bei der Verarbeitung von JPEG-Bildern. Speziell präparierte Bilder bringen Microsoft-Anwendungen bei der Darstellung zum Absturz und ermöglichen das Ausführen beliebigen Codes.

Alle IT-Systeme sind betroffen - nicht nur Windows-Rechner.

Es werden überwiegend Rechner mit Windows-Betriebssystemen angegriffen. Das liegt aber nicht daran, dass Windows prinzipiell unsicherer oder fehlerhafter wäre als andere Betriebssysteme. Der Hauptgrund liegt in der weiten Verbreitung von Microsoft-Produkten und der einfachen Verfügbarkeit von Tools zum Generieren von Schadsoftware. Das Verhältnis von Aufwand und Nutzen ist viel günstiger als z. B. bei Linux- oder Macintosh-Systemen.

Anwender in einer Nicht-Microsoft-Umgebung dürfen sich keineswegs in Sicherheit wiegen und Sicherheitsmaßnahmen vernachlässigen. Gezielte Angriffe mit individuellen Schadprogrammen sind auf jedes IT-System möglich. Das SANS Institute (www.sans.org) z. B. warnt davor, dass inzwischen mehr Schwachstellen in plattformübergreifenden Anwendungen gefunden und ausgenutzt werden als in Windows-Betriebssystemen. Betroffen sind u. a. Viren-Schutzprogramme, Backup-Programme, verschiedene Media Player, PHP-basierte Anwendungen, File-Sharing-Applikationen oder Datenbanken.

Veröffentlichte Schwachstellen werden innerhalb weniger Tage von Schadprogrammen ausgenutzt.

Wird eine Schwachstelle in einer IT-Anwendung bekannt, dauert es kaum mehr eine Woche, bis ein passendes Schadprogramm veröffentlicht wird. Jedes Sicherheitsupdate wird inzwischen als Anleitung zum Programmieren von Schadprogrammen missbraucht. Administratoren bleibt kaum Zeit, um Up-

dates zu testen und einzuspielen. Dabei reicht es nicht mehr aus, nur Schwachstellen im Betriebssystem, E-Mail-Programm oder in Browsern regelmäßig zu beheben. Auch alle anderen IT-Anwendungen sind betroffen und können für Angriffe missbraucht werden.

BEISPIEL: DER KURZE WEG VOM SICHERHEITSUPDATE ZUM SCHADPROGRAMM

Am 09.08.2005 stellte Microsoft ein umfangreiches Windows-Update zur Verfügung. Dieses Update beseitigt u. a. eine kritische Plug-and-play-Schwachstelle, die einem Angreifer das Ausführen beliebigen Codes ermöglicht. Zwei Tage später wurde das Konzept eines Schadprogramms im Internet veröffentlicht. Nach weiteren drei Tagen nutzte mit dem Zotob-Wurm das erste Schadprogramm diese Schwachstelle aus.

Schadprogramme sind multifunktional.

Hatten Schadprogramme früher eine einzige Aufgabe (z. B. Löschen aller Textdateien), sind sie inzwischen multifunktional und lassen sich über das Internet aktualisieren und mit neuen Funktionen nachrüsten. Im Kasten „Phatbot - der Superwurm“ wird als Beispiel der Funktionsreichtum eines älteren Wurms aus dem Jahr 2004 beschrieben.

AUS DER PRAXIS: PHATBOT - DER SUPERWURM

Phatbot tauchte 2004 auf und ermöglicht die vollständige Kontrolle des befallenen Rechners. Sein Funktionsumfang ist fast grenzenlos, hier nur eine kurze Auswahl:

Phatbot läuft unter Windows und Linux. Um in möglichst viele Rechner eindringen zu können, sind verschiedene Methoden implementiert. Es werden z. B. gleich mehrere bekannte Windows-Sicherheitslücken genutzt, die eine Infektion ohne Zutun des Anwenders ermöglichen. Zusätzlich untersucht Phatbot, ob Hintertüren von diversen Mail-Würmern vorhanden sind.

Phatbot enthält weiterhin ein Update-Modul zum automatischen Nachladen neuer Exploits und Schadfunktionen.

Zum Eigenschutz verfügt der Wurm über Tarnfunktionen und verbirgt seinen Prozess vor dem Windows Task-Manager. Weiterhin kann er andere aktive Schadprogramme sowie Viren-Schutzprogramme deaktivieren. Um seine Analyse im Virenlabor zu erschweren, sucht er typische Test- und Analyseprogramme und ändert sein Verhalten.

Um den Wurm zu verbreiten, hat der Autor den Quellcode im Internet veröffentlicht und liefert gleich noch ein grafisches Konfigurationstool mit.

4 Infektionswege: Wie gelangt Schadsoftware auf ein IT-System?

Das Internet ist für einen Angreifer die wichtigste Schnittstelle, um auf fremde Rechner zuzugreifen und gesammelte Informationen abzutransportieren. Während mit klassischen Hacking-Techniken in der Regel über das Internet direkt ein Server angegriffen wird, ist das erste Angriffsziel von Schadprogrammen der Arbeitsplatz-PC („Client“) eines einzelnen IT-Anwenders. Über diesen Umweg ist dann auch in vielen Fällen ein Zugriff auf zentrale Server einer Organisation möglich. Besonders in Umgebungen mit gut gesicherten Servern ist ein Angriff über einzelne Arbeitsplatz-Rechner Erfolg versprechender als ein Hacking-Angriff auf zentrale Server. Im Gegensatz zu Servern lassen sich nämlich unbedarfte oder leichtsinnige Computernutzer täuschen und zur unfreiwilligen Kooperation mit dem Angreifer verleiten. Jeder kennt eine vergleichbare Situation aus dem realen Leben: Wer ohne Erlaubnis unauffällig in ein Bürogebäude eindringen möchte, wählt am besten die Mittagszeit, wenn die hungrige Belegschaft zahlreich zwischen Büro und Kantine pendelt. Der freundliche Herr im dunklen Anzug hat gute Chancen, dass ihm ein Mitarbeiter bereitwillig die Eingangstür aufhält - auch wenn kein Dienstausweis zu sehen ist.

Ein externer Angreifer hat verschiedene Möglichkeiten, Schadprogramme auf einem fremden Rechner zu platzieren (siehe Abbildung 1): Er kann das Internet nutzen (E-Mail oder andere Protokolle), Mitarbeiter zur Ausführung von Software verleiten oder sich selbst Zugang zu IT-Systemen verschaffen. Innentäter haben es einfacher - sie haben direkten Zugriff auf Daten und Systeme.

Ein typischer Angriff über das Internet verläuft meist so, dass ein sehr kleines Schadprogramm auf den Rechner des Opfers gebracht wird. Dieses sorgt dafür, dass ein weiteres, größeres Schadprogramm nachgeladen wird. Ist die Tür einmal geöffnet, können jederzeit beliebige Programme für Spezialaufgaben platziert werden.

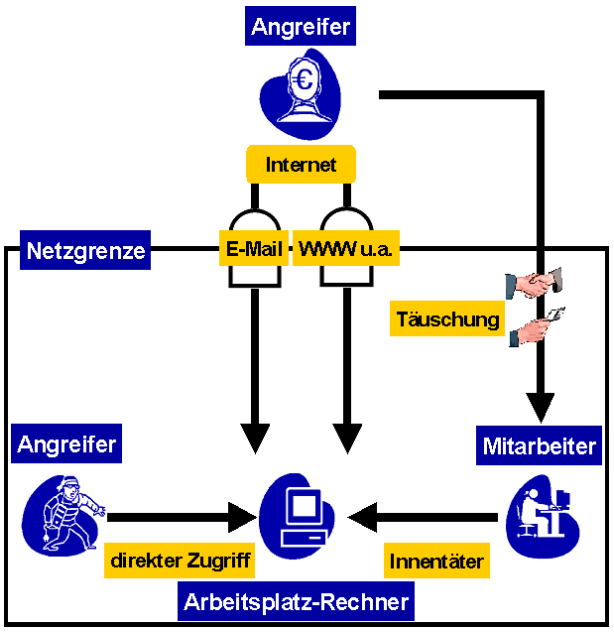

Abbildung 1: Angriffe mit Schadprogrammen

Im Folgenden verdeutlichen einige Beispiele die Schwachstellen, die von Angreifern besonders häufig ausgenutzt werden:

Anschluss von hoch schutzbedürftigen Systemen ans Internet

Infektionswege ohne Mithilfe des IT-Anwenders

Es gibt inzwischen viele Schadprogramme, die sich über das Internet verbreiten und keine aktive Mitwirkung eines IT-Anwenders erfordern (z. B. Sasser oder Zotob). Sie nutzen beispielsweise Schwachstellen des Betriebssystems oder fehlerhafte Konfigurationen aus. Untersuchungen zeigen, dass ein ungeschützter Rechner bereits wenige Minuten nach Etablierung einer Internet-Verbindung infiziert wird. Das Öffnen von Browser oder E-Mail-Programm ist dazu **nicht** notwendig.

Infektion mit aktiver Mitwirkung des IT-Anwenders

Bei jeder Internetnutzung werden mit fremden Systemen viele Dateien ausgetauscht, die dann auf dem eigenen Rechner angezeigt oder verarbeitet werden. Der Besuch unbekannter oder sogar dubioser Seiten birgt daher große Gefahren, wenn das genutzte IT-System auch zum Verarbeiten vertraulicher Dokumente verwendet wird (siehe unten „Schwachstellen in Anwendungsprogrammen“).

Unvorsichtiger Umgang mit E-Mails

Obwohl eine E-Mail kaum sicherer als eine Postkarte ist, wird ihr landläufig sehr viel mehr Vertrauen entgegengebracht. (Eine Postkarte hat gegenüber einer E-Mail dabei den Vorteil, dass sie - vom Inhalt abgesehen - keinen weiteren Schaden beim Empfänger anrichten kann.) Dass ausführbare Anhänge gefährlich sein können, ist zwar inzwischen hinlänglich bekannt, aber auch in harmlos aussehenden Dateien können bösartige Programme verborgen sein, die sich nach dem Öffnen unbemerkt installieren. Es gibt verschiedene Möglichkeiten, einen Anhang zu tarnen. Die Vergabe von Doppelendungen für Dateien (z. B. Brief.pdf.exe) ist ein sehr plumper, aber immer noch wirksamer Trick. Ausführbarer Code lässt sich auch über Makros unauffällig in Office-Dateien verankern.

Auch von E-Mails ohne Dateianhang kann unmittelbar Gefahr ausgehen, wenn sie im HTML-Format verfasst sind und eingebettete Skripte enthalten. Besonders gefährlich sind in diesem Zusammenhang so genannte Komforteinstellungen in E-Mail-Programmen, die Anhänge bzw. HTML-Code ungefragt ausführen.

Absenderangaben in E-Mails sind nicht vertrauenswürdig. Besonders gefährlich ist es, wenn das E-Mail-Programm des Empfängers nicht die vollständige E-Mail-Adresse des Absenders, sondern nur einen Namen anzeigt. Absendernamen oder Replyadressen lassen sich sehr einfach fälschen.

Selbst wenn die Absenderangaben korrekt sind und der Absender vertrauenswürdig ist, kann nicht davon ausgegangen werden, dass dieser wissentlich die E-Mail geschickt hat. Ein Schadprogramm auf seinem Rechner kann sich des Adressbuches bemächtigt und voll automatisch E-Mails generiert haben.

Angreifer, die eine Webseite mit Schadprogrammen präpariert haben, locken ihre Opfer häufig mit E-Mails in diese Falle. Während bei üblichen Spam-Mails der Empfänger schnell durchschaut, dass der Absender keine guten Absichten hat, werden gezielte Angriffe sehr gut und professionell vorbereitet. Das Opfer erhält eine E-Mail mit für ihn relevantem Inhalt. Beispielsweise werden Arbeitskreise vorgestellt oder gemeinsame Konferenzbesuche erwähnt.

Zulassung von Aktiven Inhalten beim Surfen im Internet

Das BSI warnt eindringlich vor dem Gefahrenpotential von Aktiven Inhalten beim Surfen und bei E-Mails im HTML-Format. Es sind inzwischen unzählige Schadprogramme bekannt, die sich beispielsweise über Javascript oder ActiveX installieren. Diese Techniken werden von Angreifern besonders häufig für Angriffe genutzt, weil das Aufrufen einer präparierten Webseite bereits ausreicht, um Schadcode unbemerkt auszuführen.

TECHNISCHER EXKURS: AKTIVE INHALTE

Für eine bessere interaktive Informationsdarstellung können Browser kleinere Programme und Skripte, so genannte „Aktive Inhalte", direkt beim Anwender ausführen. Zu den Aktiven Inhalten zählen insbesondere JavaScript bzw. JScript, VBScript, Java-Applets sowie ActiveX-Controls. Besonders gefährlich sind ActiveX-Controls, da sie nach der Installation, die je nach Einstellung des Browsers unbemerkt geschieht, mit allen Rechten des angemeldeten IT-Anwenders ausgestattet sind.

Durch die Zulassung Aktiver Inhalte erhöht sich das Risiko, dass Schwachstellen im Betriebssystem oder Browser ausgenutzt werden können. Eine Auswertung der Microsoft Security Bulletins ergab, dass viele Schwachstellen nur gefährlich waren, wenn die Ausführung Aktiver Inhalte aktiviert war. Wer Aktive Inhalte grundsätzlich nicht zugelassen hatte, überstand daher die Zeitspanne zwischen Veröffentlichung einer Schwachstelle und Einspielen des Patches unbeschadet. Die Gefahr steigt weiter, wenn Browser-Plugins zur Funktionserweiterung installiert werden, die Aktive Inhalte nutzen (z. B. Macromedia Flash).

BEISPIEL: KRITISCHE LÜCKE IN FLASH-PLAYER

Am 14.03.2006 wurde vor einer kritischen Lücke im Flash-Player gewarnt. Diese kann dazu führen, dass ein Angreifer die Kontrolle über ein System erlangt. Dazu muss ein Anwender lediglich eine Web-Seite mit einer eingebetteten Flash-Animation in einem Browser mit Flash-Plugin öffnen. Updates wurden für Windows und Linux bereitgestellt.

Schwachstellen in Anwendungsprogrammen

Da erfahrungsgemäß jede komplexe Software Fehler hat, finden Angreifer immer wieder Schwachstellen, die sich zum Angriff ausnutzen lassen. Technisch interessierte Leser können in [FL] nachlesen, wie sich Schwachstellen in Anwendungsprogrammen dazu ausnutzen lassen, beliebigen Code auszuführen.

BEISPIEL: PRÄPARIERTE HTML-DOKUMENTE

Im Dezember 2004 haben Unbekannte Werbung bei Google platziert, um Internetnutzer auf ihre Webseite zu locken. Die verlinkten Seiten wurden präpariert, um einen Fehler im Internet Explorer auszunutzen.

Die Schadsoftware (Trojan.Vundo) wird im System-Verzeichnis gespeichert und sorgt mit einigen Registry-Einträgen dafür, dass sie zukünftig zusammen mit dem System gestartet wird. Danach lädt sie über das Internet ein weiteres Modul nach.

Von besonderer Brisanz sind Schwachstellen beim Anzeigen von Bilddateien. Die bekanntesten Schwachstellen betreffen JPEG- und WMF-Dateien. Hier kann der bloße Besuch einer Webseite - auch wenn Aktive Inhalte nicht zugelassen sind - bereits zu einer Infektion führen.

Externe Datenträger und ungeprüfte Software

Datenträger von Externen (Kunden, Auftraggeber, Berater, Vertriebsmaterial, Werbung etc.) sind ein gerne gewählter Weg, um Spionagesoftware unauffällig zu platzieren. Ein Beispiel ist unter der Überschrift „Aus der Praxis: Wirtschaftsspionage in Israel“ auf Seite 11 beschrieben. Wer mit Wirtschaftsspionage rechnen muss, sollte daher grundsätzlich in Bereichen mit vertraulichen Informationen jeder CD oder DVD misstrauen, auch wenn sie von namhaften Herstellern oder Geschäftspartnern erworben wurde.

Fehlende Klassifizierung von Informationen

Informationen können nur entwendet werden, wenn sie für den Angreifer zugänglich sind und Möglichkeiten zum Abtransport bestehen. Oftmals scheitert der Schutz vertraulicher Informationen schon daran, dass den Mitarbeitern die Bedeutung von bestimmten Daten nicht bekannt ist oder diese nicht als vertraulich gekennzeichnet wurden.

Die Einstufung von Daten geschieht oftmals ohne konkretes Konzept und ohne einheitliche Vorgaben. So kann es sein, dass unkritische IT-Anwendungen ohne dienstliche oder geschäftliche Relevanz durch ein Passwort geschützt sind, vertrauliche Dokumente hingegen völlig ungesichert abgespeichert werden und einem großen Teil der Belegschaft offen stehen. Verwirrende, unlogische, fehlende oder nicht kommunizierte Vorgaben sind daher ein guter Nährboden für Sicherheitsprobleme.

Social Engineering: Arglose Mitarbeiter als unfreiwillige Komplizen

Kevin Mitnick, einer der bekanntesten Hacker, hat vor amerikanischen Politikern berichtet, wie er nahezu spielend in fremde Netze eindringen konnte. Sein psychologisches Einfühlungsvermögen war mindestens so ausgeprägt wie sein technisches Know-how. Er überredete immer wieder arglose Mitarbeiter zur Preisgabe wichtiger Informationen, zum Deaktivieren von Sicherheitsmechanismen oder zur Installation von Software.

Ein gängiger Trick ist die Vorspiegelung einer falschen Identität. Angreifer geben sich als Administrator, neuer Kollege, wichtiger Kunde, Servicetechniker oder sogar Vorgesetzter aus und verleiten Mitarbeiter, ihnen zu helfen oder zumindest zu vertrauen. Ein Angreifer verschafft sich häufig auch selbst Zugang zu Rechnern oder IT-Infrastruktur. So können beispielsweise bei Wartungs- oder Reparaturarbeiten heimlich IT-Systeme verändert oder Programme installiert werden.

Innentäter

Ein Angreifer muss nicht von außerhalb kommen. Innentäter sind aufgrund ihres Wissens und der technischen Möglichkeiten unter Umständen sehr viel gefährlicher. Wer sich nur auf den Schutz der Außengrenzen seines Netzes verlässt, geht daher ein hohes Risiko ein.

5 Abwehr von Schadprogrammen

Die Frage nach *der* wichtigsten Maßnahme gegen speziell angepasste Schadprogramme lässt sich nicht beantworten. Professionelle Angreifer besitzen tiefgehende technische Kenntnisse über Betriebssysteme und Softwareprogrammierung. Sie zeichnen sich zudem durch eine hohe Motivation, ausreichende Ressourcen und viel Geduld aus. Eine einzige Schwachstelle kann ihnen daher ausreichen, um in einen Rechner einzudringen.

Standard-Sicherheitsmaßnahmen wie IT-Grundschutz vom BSI sind daher das Fundament für eine sichere Informationsverarbeitung. Sie sind nicht nur die Grundvoraussetzung für den erfolgreichen Schutz vor *bekannten* Schadprogrammen, sie können auch das Risiko durch Angriffe mit *individuell angepasster* Schadsoftware deutlich verringern. Entscheidend ist, dass die Maßnahmen konsequent und vollständig umgesetzt und punktuell durch höherwertige Maßnahmen ergänzt werden.

Zum besseren Verständnis der nachfolgend beschriebenen Sicherheitsziele werden in Abbildung 2 die gängigen Funktionen von Schadsoftware zusammengefasst: Ein Schadprogramm kann Spionage- oder Sabotagefunktionen ausführen (symbolisiert durch Auge und Bombe) und dabei lokal auf dem befallenen Rechner wirken oder über das Netz auf weitere Daten zugreifen. Der mögliche Schaden hängt entscheidend davon ab, auf welche Netzbereiche bzw. Dateien der betroffene IT-Anwender zugreifen darf. Über das Internet werden ausspionierte Daten abtransportiert bzw. der infizierte Rechner ferngesteuert.

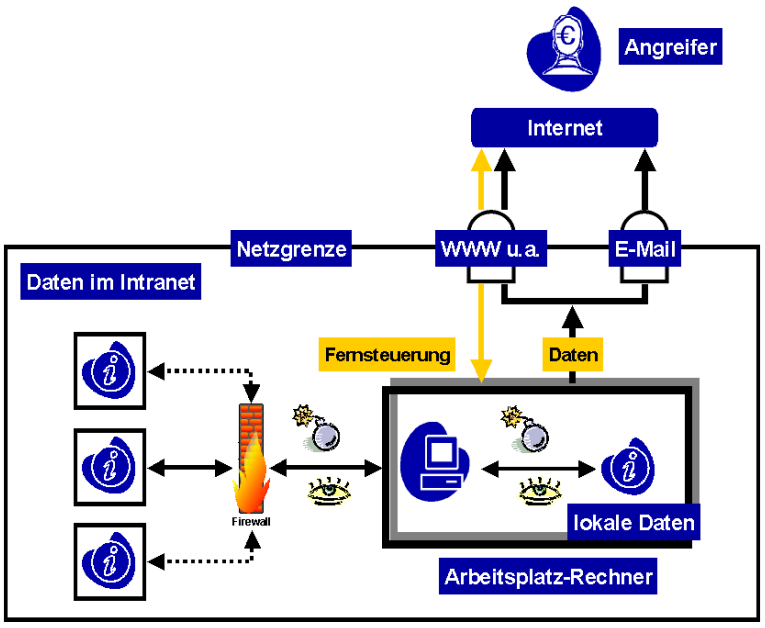

Abbildung 2: Schadfunktionen

5.1 Ziele von Schutzmaßnahmen

Da sich individuell erstellte Schadprogramme nicht zuverlässig durch Viren-Schutzsoftware detektieren lassen, müssen Sicherheitsmaßnahmen vor allem auf folgende Ziele ausgerichtet sein:

1. **Einfallstore schließen**

   Die Kommunikation über E-Mail, Internet und Datenträger sollte je nach Schutzbedarf der Daten abgesichert, eingeschränkt oder bei hohem Risiko ganz vermieden werden. Mitarbeiter müssen gefährliche Situationen erkennen und richtig handeln.

2. **Schadfunktion behindern**

   a) Start und dauerhafte Installation eines unerkannt eingedrungenen Schadprogramms müssen verhindert werden.

   b) Ein Schadprogramm darf nicht auf schützenswerte Daten zugreifen können.

   c) Eine Kommunikation zwischen Schadprogramm und Angreifer über das Internet muss verhindert werden.

Auch Schadprogramme, die vom Standard-Virenschutz nicht gefunden werden können, hinterlassen Spuren und verraten dadurch ihre Anwesenheit. Daher muss bei hohen Sicherheitsanforderungen ein weiteres Ziel angestrebt werden:

3. **Systemveränderungen und Kommunikationsversuche detektieren**

   Schadprogramme lassen sich auf Arbeitsplatz-Rechnern mit forensischen Methoden und Spezialprogrammen entdecken (z. B. durch Veränderungen an Systemdateien, unbekannte Programme oder Prozessanalyse). Auch wenn sie Daten über das Internet verschicken oder Rechner von außen fernsteuern, hinterlassen sie Spuren. Die Netzkommunikation sollte daher so protokolliert werden, dass sich Auffälligkeiten bei der Auswertung der Logdaten erkennen lassen. Diese Maßnahmen sind aufwendig, bieten aber häufig die einzige Chance, individuell angepasste Schadprogramme aufzuspüren.

5.2 Die wichtigsten Sicherheitsmaßnahmen

Die Empfehlungen in diesem Kapitel lassen sich in der Praxis nicht immer problemlos umsetzen, da ein typischer Interessenskonflikt vorliegt: Es gibt keine technischen Sicherheitsmaßnahmen, die gleichzeitig einen zuverlässigen Schutz bieten und dabei benutzerfreundlich und leicht administrierbar sind. Bei hohen Sicherheitsanforderungen sollten jedoch Komfort- oder Funktionsanforderungen zugunsten der Sicherheit zurückgestellt werden und Standard-Sicherheitsmaßnahmen durch aufwendigere Verfahren ergänzt werden. Aus diesem Grund empfiehlt es sich, sehr präzise die Bereiche mit hohen Sicherheitsanforderungen zu identifizieren. Gelingt eine sinnvolle Abgrenzung, können aufwendige und teure Maßnahmen auf wenige Anwendungen bzw. einzelne Mitarbeiter beschränkt werden.

Die wichtigsten Maßnahmen werden in Abbildung 3 im Überblick dargestellt und im weiteren Text kurz beschrieben. Im zweiten Teil des Leitfadens finden sich dann umfangreichere Informationen für IT-Sicherheitsbeauftragte.

Abbildung 3: Übersicht über die wichtigsten IT-Sicherheitsmaßnahmen

Daten und Informationen: den Zugriff schützen

Angreifer sind den Verteidigern meistens eine Techniklänge voraus: Viren-Schutzprogramme und Firewalls bieten keinen 100 Prozent zuverlässigen Schutz. Anwendungsprogramme werden immer Schwachstellen haben, die sich zur Ausführung von Schadcode ausnutzen lassen. Aus diesen Tatsachen ergibt sich zwangsläufig, dass zunächst der Zugriff auf die Daten geschützt werden muss. Wie können aber Daten und Informationen geschützt werden, selbst wenn ein Arbeitsplatz-Rechner mit einem Schadprogramm infiziert ist?

Die Hauptziele beim Schutz wichtiger Daten sind:

1. Schützenswerte Daten und Informationen müssen identifiziert werden.
2. Der Zugriff auf schützenswerte Informationen muss erschwert und auf möglichst wenige Personen (und IT-Systeme) eingeschränkt werden. (Schützenswert können z. B. Dateien, IT-Anwendungen, Funktionen des Betriebssystems, Konfigurationseinstellungen und Passwörter sein.)
3. Kann ein Schadprogramm vertrauliche Daten kopieren, sollten diese Kopien nach Möglichkeit für den Angreifer nutzlos sein.
4. Unberechtigte Zugriffe und Veränderungen müssen erkannt werden.

Beispiele:

- Werden hoch vertrauliche Daten nur auf Stand-alone-Systemen ohne Internetzugang verarbeitet, wird der Zugriff für einen Spion deutlich erschwert. Er ist dann auf klassische Methoden wie Abhören, Einbruch, Erpressung oder Bestechung angewiesen.

- Sicher verschlüsselte Dateien haben für den Angreifer keinen Nutzen.

- Eine restriktive Rechtevergabe erhöht den Aufwand für einen Angreifer enorm. Jedes Programm, das der rechtmäßige IT-Anwender nicht verwenden darf, steht auch einem Angreifer nicht zur Verfügung, wenn er den Rechner übernommen hat. Dateien, auf die ein Anwender nicht zugreifen darf, sind auch dem Angreifer nicht zugänglich.

Mitarbeiter: ausbilden und die Aufmerksamkeit wach halten

In allen Empfehlungen zur IT-Sicherheit wird die Ausbildung der Mitarbeiter immer an vorderer Stelle genannt. In der Praxis wird die Schulung der Mitarbeiter jedoch häufig vernachlässigt. Sensibilisierung findet noch seltener statt. Untersuchungen aus dem Jahr 2005 zeigen jedoch, dass gerade die eigenen Mitarbeiter gravierende Sicherheitsverstöße begehen. Zum einen gibt es Mitarbeiter, die die Gefahr unterschätzen. Sie geben ihrer Neugier nach, weil sie der Sicherheitstechnik am Arbeitsplatz blind vertrauen. Anderen sind die Konsequenzen ihres leichtsinnigen Verhaltens egal, da sich „schon jemand um den Schaden kümmern“ wird.

Eine gute Ausbildung *aller* Mitarbeiter ist eine Grundvoraussetzung für IT-Sicherheit und darf sich nicht auf die Fachabteilungen oder den IT-Betrieb beschränken. Ein erfahrener Social Engineer wählt zunächst jemanden aus, der nicht unmittelbar im Zielbereich arbeitet. Er hofft so, schlechter ausgebildete oder weniger sensible Personen anzutreffen. Beliebtes Angriffsziel ist beispielsweise Empfangs- oder Bibliothekspersonal, über dessen Rechner auf das interne Netz zugegriffen werden kann. Auch unerfahrene Mitarbeiter sind besonders gefährdet.

UMFRAGE: DER FEIND IN DEN EIGENEN REIHEN

Eine Umfrage über das Verhalten von Mitarbeitern am Arbeitsplatz im Auftrag von McAfee in Europa ergab folgende Antworten [McA]:

- *Mehr als 50 % schließen auch private Geräte an den Dienst-PC an - ein Viertel davon jeden Tag.*
- *60 % speichern private Dateien auf dem Dienst-PC.*
- *10 % laden absichtlich Dateien aus dem Internet, obwohl sie wissen, dass ihr Arbeitgeber entsprechende Inhalte auf seinen Rechnern verboten hat.*
- *62 % schätzen ihr Wissen um IT-Sicherheit als gering ein.*
- *5 % gaben zu, sich im Intranet Zugang zu für sie verbotene Bereiche zu verschaffen (z. B. Personaldaten).*

Verantwortliche und Führungskräfte in Wirtschaft und Verwaltung sollten sich regelmäßig über Sicherheitsaspekte von IT-Technik und neue Angriffsmethoden informieren, um bei Planung und Organisation keine falschen - weil unsicheren - Vorgaben zu machen.

Theorie alleine ist nicht ausreichend. Sensibilisierung und Kontrollen gehören dazu, um praktische Erfahrungen zu sammeln, das Gelernte im Alltag zu verinnerlichen und Verhalten dauerhaft zu verändern. Im Idealfall sollten regelmäßig durch externe Experten Social Engineering-Angriffe simuliert werden.

UMFRAGE: RISKANTES ONLINE-VERHALTEN AM ARBEITSPLATZ

Trend Micro belegte mit einer Umfrage, dass viele IT-Anwender in Großunternehmen am Arbeitsplatz ein wesentlich riskanteres Online-Verhalten an den Tag legen als zu Hause [TrM].

- *39 % aller Befragten glauben, dass ihre IT-Abteilung sie davor bewahrt, Opfer von Spyware- oder Phishing-Bedrohungen zu werden.*
- *In Deutschland gaben 76 % zu, dass sie verdächtige E-Mails oder Internetlinks eher am Arbeitsplatz als zu Hause öffnen, da Sicherheitssoftware auf ihrem Rechner installiert sei.*
- *29 % der deutschen Mitarbeiter gaben an, dass sie deswegen verdächtige Inhalte am Arbeitsplatz öffnen, da es sich bei der Computer-Ausstattung nicht um ihr Eigentum handelt.*

Arbeitsplatz-Systeme: absichern und härten

Die Sicherheitsmaßnahmen für die Arbeitsplatz-Rechner verfolgen drei Ziele:

1. Das Schadprogramm sollte keine Kommunikationsverbindungen zum Angreifer öffnen können.
   Eine Desktop-Firewall sollte daher zusätzlich zum Virenschutz auf jedem Rechner installiert werden. Die aktuellen Desktop-Firewalls sind keine reinen Paketfilter mehr, sondern beinhalten auch Funktionen wie Registry- oder Prozess-Monitoring.

2. Im Idealfall sollte ein Schadprogramm auf dem infizierten System gar nicht funktionieren. Eine Reihe von Maßnahmen bietet sich an:
   - Nur die nötigsten Programme dürfen installiert sein.
   - Alle Anwendungen müssen regelmäßig aktualisiert werden - nicht nur Betriebssystem und Browser.
   - Die Benutzerrechte müssen stark eingeschränkt sein. Dazu gehört auch, dass möglichst nur solche Anwendungen betrieben werden, für die keine Administratorrechte benötigt werden.

3. Der Arbeitsplatz-Rechner muss so überwacht werden, dass unbekannte Programme bzw. Prozesse, Systemveränderungen oder ungewöhnliche Netzzugriffe auffallen.
   Ein Administrator muss dazu jeden Rechner genau kennen: Welche Programme sind installiert, welche Dateien sind vorhanden? Wurden System- oder Programmdateien verändert? Sind wirklich nur erlaubte Prozesse aktiv?

Vernetzung: Konzept für internes Netz und Internetnutzung erstellen und Netzgrenzen sichern

Die meisten Schadprogramme kommen über E-Mail und Web und nutzen das Internet zur Kontaktaufnahme mit dem Angreifer. Wer mit größtmöglichem Komfort und uneingeschränkter Funktionalität das Internet nutzen möchte, muss bei der Sicherheit Abstriche machen. Dieser Leitfaden stellt im zweiten Teil technische Möglichkeiten vor, die Komfort und Sicherheit unterschiedlich gewichten, damit jeder eine für ihn angemessene Lösung finden kann.

Die Absicherung des Netzes darf sich nicht auf die Außengrenzen beschränken. Zum Schutz vertraulicher Daten müssen auch intern sichere Teilnetze gebildet werden, die möglichst gut gegen andere Netzbereiche abgeschottet sind. Eine kluge Netzsegmentierung mit ausreichendem Schutz an den internen Netzgrenzen schränkt die Möglichkeiten von Außen- wie Innentätern ein. In Abbildung 2 ist dargestellt, dass ein Angreifer durch eine konsequente interne Netzsegmentierung durch Firewalls am unbegrenzten Zugriff auf Daten gehindert werden kann.

Netzzugriffe und Kommunikationsverbindungen müssen protokolliert werden, um Auffälligkeiten zu entdecken oder im Nachhinein einen Sicherheitsvorfall nachvollziehen zu können.

Gewichtung der Sicherheitsmaßnahmen

Abwehr von Schadsoftware

Die folgende Abbildung 4 veranschaulicht die Wirksamkeit von Sicherheitsmaßnahmen bei der *Abwehr* von individuell angepassten Schadprogrammen.

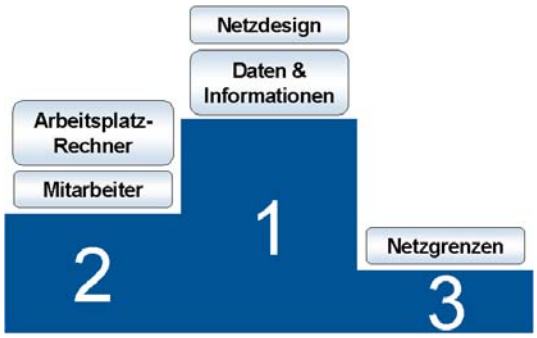

Abbildung 4: Einordnung der Wirksamkeit von IT-Sicherheitsmaßnahmen zur Abwehr von Schadprogrammen

Rang 3: Am wenigsten sollte man sich auf die Verfahren zum Schutz der Netzgrenzen (Sicherheitsgateway, Virenschutz) verlassen. Jeder Sicherheitsverantwortliche sollte einkalkulieren, dass ein individuell angepasstes Schadprogramm den äußeren Wall überwinden und auf einen Arbeitsplatz-Rechner gelangen kann.

Rang 2: Schulung und Sensibilisierung aller Mitarbeiter sollten stets eine hohe Priorität haben. Auf einem Arbeitsplatz-Rechner müssen sowohl die Funktionsfähigkeit als auch das Kommunikationsverhalten des Schadprogramms gestört werden. Je mehr Rechte ein IT-Anwender hat, desto höher die Wahrscheinlichkeit, dass ein Schadprogramm fehlerfrei funktioniert und sich fest im System einnisten kann.

Rang 1: Fällt auch der Verteidigungswall am Arbeitsplatz-Rechner, hängt alles davon ab, ob ein Angreifer auf vertrauliche Daten zugreifen kann oder nicht. Der Schutz von Daten und Informationen ist daher fundamental, da er auch dann noch greift, wenn Schadsoftware einen Arbeitsplatz-Rechner in Besitz genommen hat. Da die Sicherheit von Daten entscheidend vom Speicherort und den Zugriffsmöglichkeiten abhängt, hat das sichere Netzdesign ebenfalls höchste Priorität.

Detektion von Schadsoftware

Wenn die Abwehr nicht gelungen ist und sich eine Schadsoftware aktivieren konnte, sollte sie möglichst schnell anhand ihres Verhaltens entdeckt werden. Die größten Chancen bestehen durch eine genaue Beobachtung des Netzes. Die Protokollierung der Netzaktivitäten und des E-Mail-Verkehrs sind daher sehr wichtig.

Die Beobachtung von Arbeitsplatz-Rechnern ist ebenfalls sehr effektiv. Die regelmäßige Integritätsprüfung aller Dateien ist eine große Hilfe - in großen IT-Landschaften aber leider sehr aufwendig. Ein großer Fortschritt bei der Überwachung von Dateien und Prozessen auf Windows-Rechnern ist durch die Weiterentwicklung von Desktop-Firewalls gelungen, die immer effektiver werden. Da auch ihre Anwendung einfacher und komfortabler geworden ist, sollten sie zur Grundausstattung jedes Arbeitsplatz-PCs gehören.

6 Ausblick

Die bisherige Sicherheitsstrategie basiert im Wesentlichen auf den Säulen Firewall und Viren-Schutzprogramm. Durch die Fortentwicklung der Angriffstechnik bietet sie keinen zuverlässigen Schutz mehr. Individuell angepasste, multifunktionale Schadprogramme lassen sich nicht mehr erkennen und kommunizieren über erlaubte Wege wie E-Mail oder HTTP über das Internet mit dem Angreifer. Der entscheidende Grund für die größer werdende Gefährdung durch Schadprogramme liegt in der Entwicklung von Werkzeugen, mit denen Schwachstellen gefunden und ausgenutzt werden können.

Ein sicherheitsbewusstes Design der IT-Landschaft und ein umfassendes Sicherheitskonzept basierend auf den Empfehlungen dieses Leitfadens bieten jedoch immer noch einen sehr guten Schutz. Fehler im Konzept, Lücken in der Umsetzung und der Anschluss von hoch schutzbedürftigen IT-Systemen an das Internet bedeuten aber ein ungleich größeres Risiko als in den vergangenen Jahren. Gewohnte Komfort- und Funktionalitätsansprüche lassen sich nur mit gesteigerten Anstrengungen und aufwendigeren Sicherheitsmaßnahmen aufrecht erhalten.

Was bringt die Zukunft? Sind gegenwärtig die Angreifer leicht im Vorteil, kann sich die Situation in den nächsten Jahren wieder zugunsten der Verteidiger verändern. Aktuelle Hard- und Software beruht zu großen Teilen noch auf Architekturprinzipien aus Zeiten, in denen IT-Sicherheit kein zentrales Thema für die Gesellschaft war. Auch die Internetprotokolle wurden entworfen, als die heutige Bedeutung des Internets noch nicht gesehen wurde. Qualitätssicherung in der Softwareentwicklung, Vermeidung von Pufferüberläufen, Kontrolle von Prozessen, E-Mail-Authentisierung sowie die Verbesserung des DNS-Protokolls sind nur einige Themen, an denen gearbeitet wird. Hersteller und Standardisierungsorganisationen sind bestrebt, Hard- und Software sowie Protokolle grundlegend zu verbessern oder sogar zu erneuern. Die Zukunft gehört IT-Systemen, die auch ohne Viren-Schutzprogramm sicher sind, da sie nur die vom Anwender zugelassenen Anwendungen und Prozesse ausführen. Dieses Ziel lässt sich entweder durch zusätzliche Hardware-Komponenten („Trusted Platform Module“) oder durch Software-Lösungen („Whitelist-Programme“) erreichen. Das BSI beteiligt sich aktiv an beiden Entwicklungsrichtungen und wird sich weiterhin für sichere und praxistaugliche Informations- und Kommunikationstechnik einsetzen.

7 Literatur und Quellenverzeichnis

Im Text referenzierte Bücher und Links

[McA] http://www.theregister.co.uk/2005/12/15/mcafee_internal_security_survey/

[MID] M. G. Swimmer, Malware Intrusion Detection, Books on Demand GmbH, ISBN 3-8334-3436-8, Norderstedt 2005

[FL] Felix Lindner, Ein Haufen Risiko - Pufferüberläufe auf dem Heap und wie man sie ausnutzt, http://www.heise.de/security/artikel/72101

[TrM] http://de.trendmicro-europe.com/enterprise/about_us/spresse.php?id=183

Weitere Informationsquellen und Berichte über Vorfälle

- Informationsbroschüren des Bundesamtes für Verfassungsschutz zu den Themen „Spionageabwehr und Geheimschutz“ (z. B. „Wirtschaftsspionage: Information und Prävention“):
  Startseite: http://www.verfassungsschutz.de/de/publikationen/spionageabwehr_geheimschutz/
- Melde- und Analysestelle Informationssicherung MELANI (Schweiz): Siehe unter „Lageberichte“ http://www.melani.admin.ch/
- WMF-Exploit ging für 4000 US-Dollar über den Tisch:
  http://www.heise.de/newsticker/meldung/69207
- Schwachstelle im Microsoft Betriebssystem Windows Grafikformat "Windows Metafile" (WMF):
  http://www.bsi.bund.de/av/texte/windowswmf.htm
- Angriff auf Behörden über WMF-Schwachstelle:
  http://news.com.com/British+parliament+attacked+using+WMF+exploit/2100-7349_3-6029691.html
- Angriffe auf britische Behörden mit Trojanischen Pferden: NISCC Briefing 08/2005 - Targeted Trojan Email Attacks: http://www.cpni.gov.uk/docs/ttea.pdf
- Spionage in Schweden bei Ericsson: http://www.heise.de/newsticker/meldung/58281
- Wirtschaftsspionage in England: http://business.guardian.co.uk/story/0,,1639928,00.html
- Diebstahl von 40 Millionen Kreditkarten-Daten in den USA:
  http://www.heise.de/newsticker/meldung/60810
- Wirtschaftsspionage in Israel:
  - http://www.msnbc.msn.com/id/8145520/
  - http://www.viruslist.com/de/news?id=164526200
  - http://www.viruslist.com/de/viruses/news?id=164559078
- Botnetz-Betreiber erpressten Adware-Verteiler: http://www.heise.de/newsticker/meldung/65749
- Angriff auf Verbraucherschutz-Sites abgewehrt: http://www.heise.de/newsticker/meldung/67907

- Gezielte Viren-Attacken auf Firmen: http://www.heise.de/newsticker/meldung/61221
- Angreifer verschlüsseln Dateien, um ein „Lösegeld“ zu erpressen:
  - http://www.sophos.com/pressoffice/news/articles/2006/04/ransom.html
  - http://www.sophos.com/virusinfo/analyses/trojzippoa.html
- Botnetzbetreiber zu hoher Haftstrafe verurteilt: http://www.heise.de/newsticker/meldung/72907