REPORT

Gefahren aus dem Netz

[20.07.2009] Unverändert ernst ist die Bedrohung der IT-Sicherheit durch Schad-Software. Im Bericht des Bundesamts für Sicherheit in der Informationstechnik zur Lage der IT-Sicherheit in Deutschland heißt es, das Bewusstsein für IT-Sicherheit in der öffentlichen Verwaltung müsse erhöht werden. Behörden und Ämter investieren zu wenig in die IT-Sicherheit und es fehlt an qualifiziertem Personal.

Die gute Nachricht zuerst: Die Wirtschaftskrise lähmt offenbar auch die Versender von Werbe-Mails. Das geht aus dem aktuellen Spam-Bericht des IT-Security-Spezialisten Kaspersky Lab hervor. Die Virenanalysten erwarten einen etwas ruhigeren Verlauf der Spam-Angriffe aus dem Netz und vermuten, dass einige Auftraggeber für unerwünschte Werbe-Mails Pleite gegangen sind. Das wäre wenigsten eine gute Nachricht in der Krise.

Lage der IT-Sicherheit

Weniger positiv klingt der Bericht zur Lage der IT-Sicherheit in Deutschland, den das Bundesamt für Sicherheit in der Informationstechnik (BSI) Anfang März 2009 vorgelegt hat. Danach ist die Bedrohungslage unverändert ernst. Tag für Tag überschwemmen Tausende neuer Schadprogramme das Internet. Und beinahe täglich werden neue Sicherheitslücken in IT-Systemen entdeckt. Wie das BSI herausfand, eigneten sich rund die Hälfte der im Jahr 2008 entdeckten Schwachstellen, Benutzer- oder sogar Administratorrechte zu erlangen. Über drei Viertel der Lecks können von einem entfernten Angreifer ausgenutzt werden. Und: Für etwa die Hälfte der Schwachstellen wurde von den Software-Herstellern kein Update zur Behebung des Sicherheitsproblems bereitgestellt. Zudem stellt das BSI einen deutlichen Anstieg so genannter Zero-Day-Angriffe fest. Dabei wird eine Sicherheitslücke noch vor oder am gleichen Tag der öffentlichen Bekanntmachung ausgenutzt. Da die meisten Anwender inzwischen die Betriebssysteme auf dem neuesten Stand halten, gehen die Angreifer dazu über, Schwachstellen in weit verbreiteter Software auszunutzen. Auch hier stellen viele Entwickler Updates nicht rechtzeitig zur Verfügung.

Neue Infektionswege

Das BSI diagnostiziert auch, dass sich die Infektionswege geändert haben. Während die meisten Schadprogramme noch vor zwei Jahren per E-Mail verschickt wurden, erfolgt die Verbreitung inzwischen meist über präparierte Websites (Drive-by-Download). Durchschnittlich 15.000 Websites werden pro Tag infiziert. Angreifer manipulieren dabei vermehrt auch seriöse Websites, um vom Nutzer unbemerkt Schadcode auf den Rechner zu schleusen. Ausgenutzt werden hierzu Sicherheitslücken im Browser oder in installierten Zusatzkomponenten (Plug-Ins). Die meisten Schwachstellen bei Browsern gibt es in den ActiveX-Steuerelementen, die zur Darstellung von aktiven Inhalten verwendet werden. Was die Schadprogramme selbst betrifft, wird es laut BSI immer schwieriger, diese in Kategorien wie Viren, Würmer, Trojanische Pferde oder Bots einzuteilen. Die meisten Schadprogramme sind modular aufgebaut und verfügen über mehrere Funktionen. Ein Trojanisches Pferd kann etwa Backdoor- und Spyware-Funktionen enthalten, einen Keylogger verwenden und den befallenen Rechner zusätzlich an ein Bot-Netz anschließen.

Werkzeuge der Hacker

Trojanische Pferde sind die wichtigsten Werkzeuge, um Passwörter zu stehlen oder ein Opfer gezielt auszuspionieren. Nach Angaben des IT-Security-Unternehmens Trend Micro wuchs der Anteil trojanischer Programme an Schad-Software für Datendiebstahl von 52 Prozent im Jahr 2007 auf 87 Prozent im folgenden Jahr; im ersten Quartal 2009 lag der Anteil sogar bei 93 Prozent. Während früher hauptsächlich zentrale Server einer Behörde oder eines Unternehmens angegriffen wurden, haben sich die kriminellen Hacker darauf verlegt, einzelne Arbeitsplatzrechner einer Organisation zu infizieren. Die IT-Anwender werden dazu gebracht, eine präparierte E-Mail oder Website zu öffnen oder einen manipulierten Datenträger, etwa einen USB-Stick, anzuschließen. Für Identitätsdiebstähle werden Spyware-Programme benutzt, die heimlich Anmeldenamen, Benutzernamen oder Passwörter mitprotokollieren. Eine besondere Gefahr geht von so genannten Bot-Netzen aus. Bots (abgeleitet vom Begriff robot) sind kleine Programme, die weitgehend autonom bestimmte Aufgaben verrichten. Web-Crawler von Suchmaschinen sind Beispiele für gutartige Bots. Bösartige Bots sammeln E-Mail-Adressen für Spam-Zwecke, kopieren Inhalte von Webseiten oder spionieren Software-Lücken auf Servern aus, um diese anzugreifen. Ein Bot-Netz besteht aus zahlreichen infizierten Rechnern, die von einem Angreifer kontrolliert werden, etwa um Spam-Mails zu versenden oder eine Denial-of-Service-Attacke zu starten.

Droht der Cyber-Krieg?

Koordinierte Denial-of-Service-Angriffe (DDoS – Distributed Denial of Service) werden inzwischen als eine Form des Cyber-Kriegs verstanden. Den schwersten Angriff dieser Art erlebte Estland im Jahr 2007. Nach einem Streit mit Russland über den Abriss eines sowjetischen Kriegsdenkmals griffen Hacker in mehreren Wellen die Server von Regierung und Unternehmen an. Zeitweilige brachen die IT-Systeme des baltischen Staates zusammen. Auch ein Treffen des französischen Präsidenten Nicolas Sarkozy mit dem tibetischen Oberhaupt Dalai Lama war offenbar Auslöser für eine Cyber-Attacke: Die Website der französischen Botschaft in Peking war für mehrere Tage nicht erreichbar. Wie hoch die Gefahren eingeschätzt werden, zeigen Pläne der amerikanischen Regierung. Nach Medienberichten hat US-Verteidigungsminister Robert Gates die Einrichtung eines Cyber-Kommandos angeordnet, das die militärischen Netzwerke gegen Hacker-Angriffe abschirmen soll. Doch auch zivile Behörden sind gefährdet. Allein in den USA hat sich nach den Angaben des Ministeriums für Heimatschutz (Department of Homeland Security) die Zahl der bekannten erfolgreichen Angriffe auf Regierungscomputer zwischen 2006 und 2008 verdoppelt. Ende Mai kündigte Präsident Barack Obama an, eine spezielle Behörde zu schaffen, die sich mit kriminellen Machenschaften im Internet befasst. Obama ist selbst ein gebranntes Kind: Während des Präsidentschaftswahlkampfes sind die Computer-Systeme seiner Wahlkampf-Organisation geknackt worden, gab Obama zu. Die Eindringlinge seien an E-Mails und eine ganze Reihe von Wahlkampf-Daten gekommen, darunter Positionspapiere und Reisepläne.

Neue IT-Sicherheitskonzepte

Um solche Angriffe zu verhindern und die sensiblen Daten von Bürgern, Unternehmen und Behörden zu schützen, arbeiten die Antiviren-Software-Hersteller an neuen Erkennungsmethoden. Denn: Die bisher verwendete signaturbasierte Technik erkennt nur bereits bekannte Schadprogramme. Nun sollen verhaltensbasierte Verfahren besseren Schutz bieten. Allerdings führen diese Erkennungsverfahren zu einer deutlich höheren Anzahl an Fehlalarmen (false positives). Auch die Cyper-Kriminellen verfeinern beständig ihre Methoden. Künftig ist mit Schadprogrammen zu rechnen, die das Betriebssystem in eine virtuelle Umgebung verschieben. Das heißt, die Malware installiert sich zwischen Hardware und Betriebssystem und kann von herkömmlichen Schutzprogrammen nicht mehr erkannt werden.

Nach Auffassung der Hersteller von Anti-Viren-Software haben traditionelle Sicherheitskonzepte ausgedient. Über viele Jahre stand die Absicherung von Arbeitsplatzrechnern im Zentrum der Sicherheitskonzepte. Angesichts der immer komplexer werdenden Bedrohungslage ist jedoch eine neue Strategie notwendig. Trend Micro beispielsweise verfolgt einen präventiven Ansatz, der gegen Bedrohungen auf verschiedenen Ebenen reagiert. Schad-Software soll bereits im Internet blockiert werden, noch bevor sie in ein Netzwerk eindringen kann. Smart Protection Network nennt das Unternehmen dieses Konzept. Unter Nutzung von Korrelationstechnologien und Verhaltensanalysen werden dabei Aktivitäten im Internet auf ihr Gefahrenpotenzial hin untersucht. Durch die Analyse von E-Mails, eingebetteten Links, Dateianhängen und im Web gehosteten Dateien lassen sich infizierte Websites oder Dateien identifizieren und sofort den Reputationsdatenbanken von Trend Micro hinzufügen, um neue Bedrohungen schnell zu blockieren.
Umfassenden Netzwerkschutz verspricht auch das Unternehmen Cisco Systems. Security-Hardware wie die IronPort-Serie soll verhindern, dass Angreifer eindringen können. Die Web Security Appliance kombiniert mehrere Sicherheitstechnologien. Zudem betreibt Cisco das weltweit größte Netzwerk zur Überwachung von E-Mail- und Web-Verkehr. Nach Angaben des Konzerns werden mehr als 25 Prozent des weltweiten Internet-Verkehrs überwacht und auf mögliche Bedrohungen hin analysiert. Dies ermögliche einen Blick auf die globalen Sicherheitsbedrohungen in Echtzeit. Kunden von Cisco, die eine IronPort-Appliance einsetzen, können so seriöse Absender einer E-Mail von Spammern und anderen Angreifern unterscheiden.

Gefahren ernst nehmen

Das ist auch dringend nötig. Fast 87 Prozent des weltweiten E-Mail-Verkehrs besteht aus unerwünschten Nachrichten. Auch Behörden werden überschwemmt mit Spam-Mails. Allein am Netzübergang der Bundesbehörden sind nach Erhebungen des BSI von 100 empfangenen E-Mails im Durchschnitt gerade einmal 1,5 legitim. Auch die kommunalen Verwaltungen bleiben von Spam nicht verschont. Beispielsweise beträgt das Mail-Aufkommen des Landratsamts Schwandorf über eine Million Nachrichten pro Woche, der Spam-Anteil liegt bei 98 Prozent. Der Kreisverwaltung hat deshalb den unerwünschten Nachrichten den Kampf angesagt und das Cisco-Produkt IronPort C150 beschafft.
Nicht jede Behörde nimmt jedoch die Gefahren aus dem Internet so ernst wie das Landratsamt Schwandorf. Im BSI-Bericht zur Lage der IT-Sicherheit in Deutschland heißt es kritisch, das Bewusstsein für IT-Sicherheit müsse bei den Entscheidungsträgern in der öffentlichen Verwaltung erhöht werden. Noch werde zu wenig in die IT-Sicherheit investiert und es fehle an qualifiziertem Personal. Das kann man von der Gegenseite nicht behaupten. Die Zeiten der Script-Kiddies sind längst vorbei. Cyber-Kriminalität ist inzwischen Teil einer professionell und international aufgestellten Schattenwirtschaft. Die organisierte Kriminalität nutzt das Internet und Informationstechnik zunehmend für eigene Zwecke. Deren Hauptmotiv ist die finanzielle Bereicherung. Aber auch Wirtschaftsspionage, politische und terroristische Motive spielen bei der IT-Sicherheit eine Rolle.
BSI-Präsident Udo Helmbrecht mahnte deshalb kürzlich, viele IT-Verantwortliche seien sich der Gefahren nicht bewusst, weil die Angriffe nahezu unsichtbar verlaufen. Verwaltungen, Unternehmen und Bürger müssten daher weiter dafür sensibilisiert werden, sich und ihre IT-Systeme gegen Angriffe zu schützen. Das heißt: Nur durch den konsequenten Einsatz traditioneller Sicherheitskonzepte wie Virenschutz-Software, Firewalls, regelmäßige Updates des Betriebssystems und dessen Anwendungen kann das Risiko einer Infizierung oder eines Angriffs gesenkt werden. Vor allem aber müssen die Nutzer große Sorgfalt im Online-Verhalten walten lassen. Es ist eine Binsenweisheit: Das größte Sicherheitsrisiko für Computer-Netze sitzt vor dem Monitor.

(al)

Stichwörter: IT-Sicherheit, IT-Sicherheit, Bundesamt für Informationssicherheit in der Informationstechnik (BSI), Cisco Systems, Trend Micro, Kaspersky Lab