SECURITY
FACHARTIKEL

Profitgier treibt die Hacker an

Durch die Vernetzung eröffnen sich auch für illegale Aktivitäten scheinbar unbegrenzte Möglichkeiten. Die Umtriebe finden ihren Niederschlag etwa in ausgefeilten Phishing-Methoden, die Anwendern sensible Daten wie Kontoinformationen entlocken.

von Jürg Buob

«Das Internet zieht nun einmal auch Menschen an, die nicht davor zurückschrecken, Gesetze zu übertreten und die Schädigung anderer in Kauf nehmen, solange sie selbst einen Gewinn daraus ziehen.» Mit diesen Worten beschreibt Symantec-Sicherheitsexperte Olaf Lindner einen Trend zu Diebstahl, Betrug und Erpressung im Internet, der im vergangenen Jahr zu beobachten war und bei dem Experten davon ausgehen, dass er sich auch im kommenden Jahr fortsetzen wird.

Vor allem in den USA, wo der Handel über das Internet weit verbreitet ist, boomt der Diebstahl im Internet. Doch auch in Europa häufen sich die Vorkommnisse. Je mehr Transaktionen per Kreditkarte abgewickelt werden, desto öfter kommen Online-Betrüger an Kreditkartennummern und andere persönliche Informationen von E-Commerce-Kunden heran.

Die Bekämpfung computergestützter Straftaten bereitet Entwicklern und Betreibern von Computersystemen seit langem Sorge. Tausende Internetanwender fallen jährlich solchen Straftaten zum Opfer. Mit Hilfe ergaunerter Daten eröffnen die Betrüger neue Konten, beschaffen sich Kreditkarten und gehen in grossem Stil auf Einkaufstour. Häufig dauert es Monate oder gar Jahre, bis die vom Datenmissbrauch Betroffenen die Banken, Kreditgeber und Geschäfte davon überzeugen können, dass sie Opfer von Identitätsklau waren und die Käufe nicht selbst getätigt haben.

Olaf Lindner

«Auch bei Open Source Browsern nimmt die **Zahl der Schwachstellen zu.»**

Olaf Lindner, Symantec

Phisher fischen im Trüben

Vor allem «Phishing», eine besonders raffinierte Form des Trickbetruges, bei der «Phisher» ihren Opfern offiziell wirkende Schreiben, meist E-Mails, schicken, die sie verleiten sollen, personenbezogene oder vertrauliche Informationen preiszugeben, hat enorm zugenommen. Zwar können moderne Betriebssysteme Daten zum Schutz vor Hackern verschlüsselt übertragen, doch sind die User mit dieser Funktion oft überfordert. Ohne darauf zu achten, ob die Verbindung verschlüsselt ist, übermitteln sie im Internet arglos Kreditkartennummern oder Passwörter.

Vor einer «Secured Phishing-Technik», die Besucher von Websites zur Offenlegung vertraulicher Informationen verleiten soll, warnte kürzlich etwa der Sicherheitsspezialist Surfcontrol. Mit Hilfe dieser Methode versuchen die Betrüger die Internetnutzer in den Glauben zu versetzen, dass sie sich auf gesicherten Internetsites befindet. Die bei Online-Transaktionen übliche verschlüsselte Verbindung ist daran zu erkennen, dass sich im Browser die URL-Adresse von http:// auf https:// ändert. Das «s» steht in diesem Zusammenhang für SSL, was eine verschlüsselte Verbindung zum Zielserver bedeutet. Zudem erscheint ein eingeblendetes Schloss in der Statusleiste des Browsers.

Doch nicht einmal dann kann man ganz sicher sein. Manchmal wird diese Sicherheit dem Opfer nur vorgegaukelt. «Die Seiten sehen derart echt aus, dass ahnungslose Anwender den Betrügern in die Falle gehen», sagt Gernot Huber, Marketing-Chef des Sicherheitsanbieters Surfcontrol. «Erst recht, wenn sie durch das Verschlüsselungs-Symbol im Glauben sind, sich in einem gesicherten Bereich zu bewegen.» Mit der neuen Technik versuchen die Phisher soviel Realitätsnähe wie möglich zu erzielen. Viele Anwender, mit dem Inhalt der Warnung in der Pop-up-Dialogbox nicht vertraut, drücken dann gewohnheitsmässig auf Ja, um auf der Site zu bleiben.

Eindeutiges Erkennungsmerkmal für den Anwender ist, wenn das Windows-System vor dem Öffnen der Seite per Dialogfeld auf Probleme mit der Gültigkeit des digitalen SSL-Zertifikats hinweist. Der Security-Spezialist rät allen Nutzern Warnungen, die das Zertifikat betreffen, ernst zu nehmen und natürlich niemals auf E-Mails zu reagieren, in denen persönliche Informationen abgefragt werden.

Hacker-Angriffe aus Profitgier

Laut dem halbjährlich erscheinenden Symantec Security Report wehrte das Unternehmen im vergangenen Halbjahr 1,04 Milliarden Phishing-Attacken ab – das sind doppelt so viele wie im Halbjahr zuvor. Täglich wird demnach weltweit mehr als fünf Millionen Mal versucht, ein Opfer mit falschen Angaben aufs Glatteis zu führen.

Um diesem Missbrauch vorzubeugen, stellt Microsoft seit kurzem ein kostenloses Hilfsprogramm zur Verfügung. Das Add-in benutzt dieselbe Technik, die auch im Internet Explorer 7 zum Einsatz kommen wird. Vor dem Aufruf einer unbekannten Site schlägt der Phishing-Filter erst in einer lokalen Whitelist nach. Ist diese dort nicht verzeichnet, sendet er die Adresse an einen Anti-Phishing-Server weiter, der sie in Echtzeit untersucht. Erregt die Site Verdacht, warnt der Browser.

Da die finanziellen Gewinnmöglichkeiten durch Cyberverbrechen immer verlockender werden, werden Angreifer künftig wohl noch ausgefeiltere Methoden entwickeln – auch solche mit Tarnmechanismen, die darauf abzielen, Virenschutz, Firewalls und andere Sicherheitseinrichtungen ausser Kraft zu setzen. Der Sicherheitsspezialist McAfee warnt, dass auch weiterhin mit einer grossen Zahl von Hackern zu rechnen ist, die mit zunehmend trickreicheren Virenvarianten Unternehmensnetze und Privatbenutzer attackieren. Dabei tritt laut McAfee der Hacker-Typus «Techie», den nur das Interesse am Eindringen in abgesicherte Bereiche treibt, in den Hintergrund. Seine Stelle nehmen statt dessen Kriminelle mit handfesten materielle Interessen ein.

Um missliebige Konkurrenten auszuschalten oder um Schutzgelder zu fordern, wird etwa fremde Rechenleistung gekapert, zu Botnets zusammengeschaltet und kombiniert für die massenhafte Verbreitung von Spam oder Viren eingesetzt. Zuweilen sind es Tausende von Rechnern, die

VIRENSCHUTZ OHNE VIRENSOFTWARE

Forscher am IBM Almaden Lab haben einen Weg gefunden den Computer vor Viren zu schützen, ohne Antivirus-Software installiert zu haben, wie das britische Portal Techworld berichtet. Die Idee dahinter kommt von IBM-Forscher Amit Singh. Die Methode arbeitet, im Gegensatz zu herkömmlichen Methoden, statt mit Blacklists mit Whitelists. Im Kernel werden hier nur zuvor autorisierte Codes verarbeitet.

Im Rahmen des Projektes Assured Execution Enviroment (AXE) arbeiten Forscher seit zwei Jahren an der Entwicklung von Software, die die Nutzung von PCs vereinfachen soll. Beim Booten des Computers lädt AXE mit Hilfe einer patentierten IBM-Technik spezielle Runtime-Software in den Betriebssystem-Kernel. Diese Software überprüft fortan jedes Programm, das auf dem Computer läuft, und stellt sicher, dass nur Anwendungen mit zuvor autorisiertem Code zur Ausführung kommen. Dabei blockiert AXE, im Gegensatz zu Antivirensoftware, nicht von vornherein alle bösartigen Programme, sondern verhindert nur die Ausführung von Codes, die nicht zuvor für AXE autorisiert wurden. Laut Singh arbeitet die Software sowohl unter Windows als auch unter Mac OS.

Bei der Konzeption der Software setzten die Forscher auf maximale Flexibilität: Die PCs sollen sich so konfigurieren lassen, dass unbekannte Software nur nach vorheriger Zustimmung des Users ausgeführt werden kann. Nach Einschätzung von Experten werden auch Anbieter von Sicherheitssoftware in Zukunft mit Whitelists arbeiten. Die derzeit übliche Technik, Malware zu blockieren, sei auf lange Sicht zu aufwendig. Die Kehrseite sei jedoch, dass IT-Administratoren bei jedem Update aktiv werden müssen und der Software erneut erlauben müssen zu arbeiten. Die interessante Frage sei nicht, ob die Software funktioniere, sondern wie leicht sie zu handhaben ist, so ein Experte. *(pte)*

durch spezielle Schadprogramme, so genannte Bots, von Hackern ferngesteuert werden – ohne Wissen der PC-Besitzer. Ein solches Netz von ferngesteuerten Rechnern gibt Angreifern eine schlagkräftige Waffe mit hoher Rechnerleistung an die Hand. Mit einer Flut von Anfragen können damit Server so sehr überlastet werden, dass diese zusammenbrechen und dadurch beispielsweise Websites nicht mehr erreichbar sind.

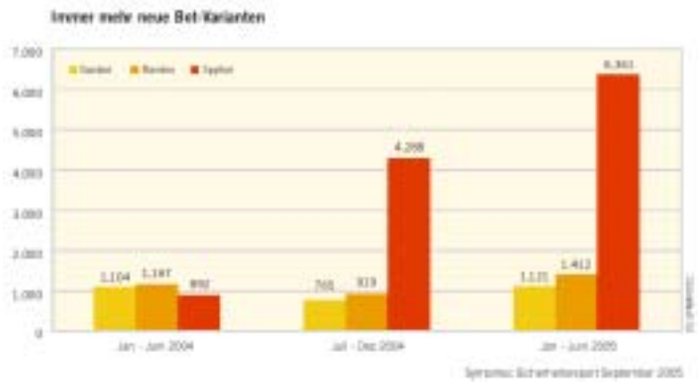
Aufgeklärte Anwender

Neu ist, dass zunehmend kleine und mittlere Unternehmen ins Visier der Angreifer geraten. «Wir konnten generell eine Abkehr von spektakulären Offensiven gegen grosse Netzwerke feststellen und einen Schwenk hin zu kleineren Angriffszielen», so Olaf Lindner von Symantec. Eine Besorgnis erregende Entwicklung, zumal Online-Shopping und Internetbanking immer beliebter werden. In der ersten Jahreshälfte 2005 machten Schadprogramme, die vertrauliche Informationen abschöpften, bereits 74 Prozent der 50 am häufigsten gemeldeten Cyberschädlinge aus. Zudem verschwinden die Unterschiede zwischen den verschiedenen Bedrohungsformen immer mehr. Die existierenden Techniken werden gezielt miteinander kombiniert, um so neue Angriffsformen zu entwickeln, die sich in ihrer Wirkung potenzieren. Oft handelt es sich um Würmer oder wurmähnliche Viren, die sich über infizierte E-Mail-Anhänge und Netzwerklaufwerke ausbreiten.

«Mittelständische Unternehmen haben genau dieselben Sicherheitsanforderungen wie die Grossindustrie, aber ihre Infrastruktur ist personell eingeschränkt,» sagt Ralph Kreter, Business Unit Manager beim Sicherheits-Spezialisten Trend Micro. Weil es zumeist keine eigene IT-Abteilung oder direkten IT-Verantwortlichen gibt, muss Kreter zufolge bei der Entwicklung von Sicherheitslösungen für KMU vor allem darauf geachtet werden, dass Wartung und Administration einfach und auf ein Minimum beschränkt sind. Um ein Netzwerk abzusichern, ist ein mehrschichtiges Sicherheitssystem nötig, das insbesondere die exponierten Eintrittspunkte am Gateway, Mailserver und Client sichert.

Eine weitere Schwierigkeit ergibt sich laut einer aktuellen Trend-Micro-Studie daraus, dass viele Anwender am Arbeitsplatz ein wesentlich riskanteres Online-Verhalten an den Tag legen als zuhause. Der Untersuchung zufolge besteht ein direkter Zusammenhang zwischen dem Vorhandensein einer IT-Abteilung und der Erwartungshaltung der Anwender beim Schutz vor Viren, Würmern und Spy-

Im 1. Halbjahr 2005 wurde ein Anstieg von 48% an neuen Viren-/Wurm-Varianten verzeichnet. Dies belegt einen Trend weg von weit verbreiteten Schadprogrammen wie E-Mail-Würmern hin zu modular aufgebauten und modifizierbaren Bedrohungen.



Die Anzahl neuer Bot-Varianten hat seit Anfang 2004 stark zugenommen. Grund: Der Quellcode einiger Bots ist im Internet frei verfügbar. Bots ermöglichen den Zugriff Dritter auf infizierte Rechner über Internet-Relay-Chat-(IRC)-Kanäle.

E-MAIL-FILTER ALS MANAGED SERVICE

Die E-Mail-Sicherheit im Unternehmen aufrechtzuerhalten, ist heute eine Zeit raubende Aufgabe. Entlasten lassen sich die IT-Abteilungen, indem besonders kritische Komponenten, wie das Filtern von Viren und Spam, ausgelagert werden. Führende Anbieter in diesem Bereich bieten diese Option innerhalb ihres Portfolios ebenso an wie verschiedene andere Lösungen, die den Administrator bei der Verwaltung der einzelnen Sicherheitsmassnahmen unterstützen. Hierzu zählen auch selbstständig arbeitende Appliances, die den Datenverkehr am Gateway überwachen.

Unternehmen, die sich für eine so genannte Managed-Service-Lösung entscheiden, müssen eine eigene E-Mail-Domain mit einer statischen IP-Adresse sowie einen dedizierten E-Mail-Server besitzen, entweder im Haus oder von einem Internet-Service-Provider betrieben. Diese Lösung bietet den Vorteil, dass für die täglichen Sicherheitsabläufe keine zusätzlichen Ressourcen in Form von Hardware, Software oder Personal vorgehalten werden müssen. Dadurch lassen sich die Gesamtkosten für die E-Mail-Sicherheit senken. Diese Lösung ist interessant für Unternehmen, die nicht über die nötigen Personalressourcen verfügen oder sich aus Kostengründen für das Outsourcing des IT-Aufgabenbereichs E-Mail-Sicherheit entscheiden.

Unternehmen, die eine lokal installierte Lösung bevorzugen, aber keine zusätzlichen Hardware-Kapazitäten für Sicherheitsszwecke zur Verfügung haben, sind mit einer Appliance-Lösung gut beraten. Der Vorteil dieses Konzepts: Es wird eine komplette Sicherheitslösung mit Hardware und Software gestellt, die sich nach der Installation automatisch verwaltet und die erforderlichen Aktualisierungen über das Internet einholt. Die Systeme, die am Internet-Gateway zum Einsatz kommen, überwachen den ein- und ausgehenden Datenverkehr unter den Protokollen SMTP (E-Mail-Verkehr), HTTP (Web-Datenverkehr beim Surfen), FTP (Downloads) und POP3 (Zugriff auf E-Mail-Konten). Appliances eignen sich grundsätzlich für Unternehmen jeder Grösse als zuverlässige Lösung zur Erkennung und Beseitigung von Viren sowie zum Schutz vor unerwünschten Inhalten. *(Quelle: McAfee)*

«Mit **Secured Phishing** wird dem Opfer Sicherheit nur vorgegaukelt.»

Gernot Huber, Surfcontrol

ware. So gab beinahe die Hälfte der Befragten an, dass sie glauben, die IT-Abteilung bewahre sie davor, Opfer von Spyware- oder Phishing-Bedrohungen zu werden. «Dieser Glaube verführt die Anwender oft zu einem leichtsinnigeren und riskanten Online-Verhalten», so Kreter weiter.

Diese Haltung erschwert die Aufgabe der IT, Geschäftsprozesse vor der steigenden Zahl unvorhersehbarer Bedrohungen zu schützen. Für die Unternehmen bedeutet dies letztlich, dass mehr als nur die Verfügbarkeit der Netzwerke und die Integrität der Informationen auf dem Spiel stehen. Das Wissen um das Mitarbeiterverhalten und der damit verbundene Schutz der Unternehmensinteressen können den erfolgreichen Geschäftsbetrieb massgeblich beeinflussen. Wichtige Massnahmen in diesem Zusammenhang sind laut Kreter die konsequente Aufklärung der Anwender über aktuelle Bedrohungslagen, mehrschichtige Sicherheits-Infrastrukturen sowie zeitnahe Updates zum Schutz der Netzwerke.

«Die existierenden Techniken werden gezielt miteinander kombiniert, um so **neue Angriffsformen zu entwickeln,** die sich in ihrer Wirkung potenzieren.» Ralph Kreter, Trend Micro

Ausblick auf das Jahr 2006

Die Sicherheitsanbieter gehen davon aus, dass sich die Entwicklung von hoch entwickeltem Schadcode, der mit Tarnfunktionen ausgestattet ist und Virenschutz, Firewalls und andere Sicherheitsmassnahmen zu umgehen sucht, weiter beschleunigen wird. Da sich Security-Anbieter gegen diese Art von komplexen Bedrohungen gewappnet haben, werden Virenschreiber auf raffiniertere Methoden ausweichen. Hierzu gehört etwa der modulare Aufbau von Schadprogrammen, die zunächst über limitierte Funktionen verfügen und eher harmlos erscheinen, jedoch weitere Module mit schadensträchtigen Funktionalitäten herunterladen, sobald sie einen Computer infiziert haben.

Laut Symantecs Security Report bleiben Botnets ein Thema, nicht nur im Zusammenhang mit steigenden Denial of Service-(DoS)-Angriffszahlen, sondern auch als Grundlage für Spamverteilung und internetbasierte Erpressung. Im kommenden Jahr werden vermutlich besser koordinierte Botnets entstehen, die punktgenaue Attacken ausführen können. Diese weiterentwickelten «Virenschleudern» könnten zudem mit Methoden zur Verschlüsselung und zur Tarnung ausgestattet sein.

Auch die Akzeptanz von Telefonie über das Internetprotokoll (Voice over IP; VoIP) nimmt stetig zu und mit ihr die Wahrscheinlichkeit für Schadprogramme. Da bei der Internettelefonie Sprache in Daten umgewandelt und über dieselbe Netzwerkverbindung wie herkömmliche Daten transportiert wird, ist mit einer ähnlich gelagerten Sicherheitsproblematik zu rechnen. Daneben wird es Vertraulichkeitsverluste durch Anrufumleitungen, Lauschangriffe oder Voice Phishing geben, bei dem Anwender durch automatisierte Anrufe zur Angabe sensibler Finanzinformationen aufgefordert werden.

Voraussagen auf kommende Entwicklungen zu machen ist naturgemäss schwierig, doch eines ist sicher – die Zunahme der bekannten Gefährdungen lässt sich anhand statistischer Aussagen präzise prognostizieren. McAfees so genannter «Malware Count» (Viren, Würmer, Bots etc.) hat sich gegenüber dem Vorjahreszeitraum nahezu verdoppelt – eine Stagnation der Attacken auf IT-Systeme ist daher sehr unwahrscheinlich. Neben der zu erwartenden quantitativen Zunahme für das kommende Jahr, geben auch immer perfidere Angriffsmethoden Anlass zur Sorge. Den eigentlichen Wendepunkt in Sachen Internetbedrohungen markiert aber der Trend weg von Aufmerksamkeit heischenden Aktionen hin zu Attacken, die eindeutig auf finanziellen Profit ausgerichtet sind. ■

+ + + NEWSTICKER + + + NEWSTICKER + + + NEWSTICKER + + +

KAMPF GEGEN PHISHING ZEIGT ERFOLGE

Obwohl die weltweite Anzahl an Phishing-Websites im August dieses Jahres mit über 5200 Seiten einen neuen Höchststand erreicht hat, zeigen sich die Protagonisten im Kampf gegen die Betrugs-Seiten zuversichtlich. Laut Anti Phishing Working Group (APWG) sinkt die Anzahl der Spam-Mail-Kampagnen, die User auf Phishing-Sites locken sollen, kontinuierlich. Im August dieses Jahres wurden weltweit rund 13 700 Aktionen registriert.

MESSAGELABS: INSTANT MESSAGING IM VISIER

Der E-Mail-Sicherheitsdienstleister MessageLabs hat mit Omnipod einen Anbieter von Instant Messaging-Services für Geschäftskunden übernommen. Mit der Übernahme baut MessageLabs sein Portfolio in Richtung des populären Instant Messaging aus.

E-COMMERCE: ANGST VOR DATENDIEBSTAHL

Der Handel im Internet befindet sich sowohl in den USA als auch in Europa im Aufwärtstrend. Die Angst vor Datendiebstahl und anderen Onlinegefahren trübt jedoch zunehmend das Vertrauen in dieses Medium, hat eine Studie des Sicherheitsspezialisten RSA Security ergeben. Demnach geben die User in den untersuchten Märkten insgesamt zwar mehr aus als noch vor einem Jahr. Ein mittlerweile erheblicher Anteil von ihnen hat dagegen seine Ausgaben bereits wieder zurückgefahren.

IT-SICHERHEIT LÄSST ZU WÜNSCHEN ÜBRIG

Unternehmen sind immer mehr auf die Sicherheit ihrer Informationstechnologien angewiesen, doch weltweit häufen sich die Probleme. PricewaterhouseCoopers (PwC) befragte 8200 IT-Verantwortliche aus 63 Ländern zum Thema Sicherheit. Wie die Umfrage zeigt, kletterte die Zahl der sicherheitsbezogenen Vorfälle von rund 700 im letzten Jahr auf rund 860 im Jahr 2005, wobei Hacker der Hauptgrund für IT-Ausfälle waren. *(pte/ICT)*