G DATA

Whitepaper 2008

Die neuen Formen des Datendiebstahls

Ralf Benzmüller, Leiter G DATA Security Labs

Geschützt. **Geschützter. G DATA.**

Das Geschäft mit Cyber-Attacken ist längst zu einem ernst zu nehmenden Problem herangewachsen, das weltweit Bundespolizei und Geheimdienste beschäftigt. Die heutigen, differenzierten Attacken, die sich über das Internet erstrecken, haben primär kriminelle Hintergründe und werden von international agierenden Organisationen durchgeführt. Online-Kriminalität verursacht jährlich Schäden in Milliardenhöhe. Phishing mit E-Mails, die auf gefälschte Webseiten verweisen, ist dabei nur eine Spielart. Immer häufiger werden Daten mit Trojanischen Pferden gestohlen. Dabei geht es mittlerweile um weit mehr, als PIN und TAN Nummern. Anwender verlieren ihre gesamte Online-Identität!

Phishing

Phishing ist der Versuch, vertrauliche Daten des Anwenders durch gezielte Täuschungsmanöver zu stehlen. Seit den ersten Betrugsversuchen dieser Art Mitte der 1990er Jahre ist die Anzahl der Phishing-Attacken dramatisch gestiegen. Die Wachstumsphase scheint nach Einschätzung der G DATA Security Labs abgeschlossen zu sein. Seit etwa einem Jahr stagniert die Zahl der neuen Phishing-Mails und der dazugehörigen Webseiten. Die anfänglichen Probleme mit Zeichensätzen und Sprache sind überwunden. Durch flexible und einfach zu bedienende Tools, wie beispielsweise RockPhish, ist es den Tätern möglich unterschiedliche Phishingseiten auf einer Website zu hosten.

Die häufigste Zielgruppe sind nach wie vor Kunden von Onlinebanken - insbesondere in Ländern, wo PIN und eine einfache TAN die einzige Barriere zwischen Dieb und Konto darstellt – wie beispielsweise in Großbritannien und den USA.

Neue „Märkte“

Gefälschte eBay-Webseiten und deren Bezahldienst Paypal nehmen ebenfalls Spitzenplätze ein. Die Suche nach neuen Opfern ist weiterhin in vollem Gange, so nehmen Webseiten von Online-Shops mittlerweile in der Rangliste der Betrugsseiten immer höhere Plätze ein. Auch für Loginseiten von Social-Networking Plattformen, Jobbörsen und Online-Spielen wurde bereits Fälschungen bekannt. Die Accounts werden für Online-Kriminelle immer wertvoller. Ein gestohlener eBay-Account kann dazu genutzt werden, das per Phishing verdiente Geld zu waschen. In Social Networking Plattformen finden Datendiebe Informationen, die sie akkumulieren und dann verkaufen können. Gekaperte Accounts werden auch dazu genutzt Foren-Spam zu verbreiten.

Ein Schutz gegen Phishing ist der Spamfilter. Er erkennt Phishingmails und stellt diese im Idealfall erst gar nicht zu. Für einen wirkungsvollen Schutzmechanismus muss dieser jedoch alle Formen von Spam inhaltsunabhängig erkennen und blockieren. Mit der OutbreakShield-Technologie setzt G DATA den effektivsten Spam-Filter ein, der in Echtzeit inhaltsubabhängig jegliche Form von Spam- und Phishing-Mails wirkungsvoll abwehrt.

Veränderte Taktik

Die immer wirkungsvolleren Schutzmechanismen von Spam-Filtern zwang Online-Kriminelle ihre Taktik zu ändern. Der Zugang zu Phishingseiten erfolgt daher seit längerem nicht mehr ausschließlich über Spam – Gefahren lauern beim Chat, in Spielen oder in Foren.

Abwehr

AntiPhishing-Toolbars in Browsern warnen vor Phishingseiten oder verbieten den Zugang komplett. IE7, FF2 und viele Internet Security Lösungen enthalten sie von Hause aus. Alle anderen können sie z.B. von Phishtank, Google, Netcraft &Co. herunterladen und installieren. Diese Toolbars setzen einerseits auf heuristische Verfahren zur Erkennung schlechter URLs. Da hier immer die Gefahr eines False Positives besteht, sind die Regelsätze eher konservativ.

Viele Anbieter setzen zusätzlich auf die Kraft der Community. Wer eine gefälschte Webseite findet, meldet sie dem Response Team, das diese dann verifiziert und ggf. in die Blockliste aufnimmt.

Diese Listen haben jedoch einen entscheidenden Nachteil: Für die Verifizierung der Seite vergeht immens viel Zeit. Bei Phishtank im Jahresdurchschnitt knapp 2 Tage, bei kommerziellen Anbietern wenige Stunden. In diesem Zeitfenster können die Datendiebe ungestört agieren.

Anwender in der Pflicht

Technische Lösungen gegen Phishing sind also nicht unfehlbar. Die Sensibilisierung des Anwenders ist - wie bei so vielen Betrugsszenarien - das wichtigste Mittel im Kampf gegen Datenverlust. Beim Umgang mit persönlichen Daten im Internet sollten Internetnutzer daher generell Vorsicht walten lassen. Der überprüfende Blick auf die URL (https:// und Domainname von rechts lesen) sollte daher zum Pflichtprogramm gehören.

Pharming

Pharming ist eine Alternative zum klassischen Phishing-Ansatz. Anwender werden bei dieser Form des Betrugs unbemerkt auf gefälschte Webseiten weitergeleitet, obwohl der korrekte Domain-Name eingegeben wurde.

Technik des Pharmings

Basis dieser Betrugsweise ist die Ermittlung der IP-Adresse des Domainnamens. Dazu kann das DNS-System selbst Ziel von Angriffen werden. In Broadcast-Domains, wie z. B. WLANs, ist es sehr einfach die DNS-Anfragen zu fälschen.

Aber auch schlecht gewartete oder konfigurierte DNS-Server bieten Möglichkeiten, dies reicht vom Füllen des Cache der DNS Server mit falschen Informationen (DNS Cache Poisoning) bis hin zum Cracken des DNS-Servers.

Ansatzpunkte zur Aushebelung des DNS-Systems bestehen jedoch auch auf Client-Ebene und werden hauptsächlich von Trojanischen Pferden genutzt. Wie ist einfacher Schutz mögliche? Bereits durch einfache Methoden ist es möglich sich vor lokalen DNS-Angriffen zu schützen – beispielsweise, wenn Anwender den Link zur Online-Bank als IP-Adresse in den Favoriten abspeichern. Anders sieht es bei Angriffen auf die DNS-Infrastruktur aus. Hier muss sich der Internetnutzer auf die Betreiber der DNS-Server verlassen.

Crime-Ware

Trojanische Pferde, Exploits und Schadcode

Ein weiteres Phänomen zum Diebstahl von Identitäten: Trojanische Pferden. Diese bestreiten mittlerweile die überwiegende Mehrheit der Phishing-Angriffe.

Die vielfältigen Schutzmechanismen gegen Phishing und die fortschreitende Aufklärung der Nutzer zeigen Wirkung. Auch die Gegenmaßnahmen der Geldinstitute wie z.B. iTAN, mTAN, Token für zeitlich begrenzte TANs und HBCI tragen dazu bei, dass die gephishten Information nicht mehr verwertet werden können.

Die Cyberkriminellen brauchen - zumindest in den meisten Ländern – neue Mittel, um die Daten abzugreifen und schnellstmöglich in klingende Münze umzuwandeln.

Zu diesem Zweck setzen Online-Kriminelle unterschiedlichste Arten von Crimeware ein:

- **Keylogger** zeichnen Tastaturaktionen auf. Sie können als Treiber realisiert sein oder Informationen an den im Betriebssystem dafür vorgesehen Schnittstellen abrufen (WinAPI SetWindowsHook oder WinAPI GetKeyboardState). Zur Tarnung integrieren sie sich in gängige Systemprozesse (z.B. winlogon.exe, services.exe) oder nutzen Rootkits.
  Oftmals werden diese erst dann aktiv, wenn bestimmte Bedingungen erfüllt sind. Dies ist beispielsweise der Fall, wenn die gerade geöffnete Webseite in einer oft sehr langen Liste von Domainnamen enthalten ist oder wenn Fenster mit bestimmten Titeln geöffnet werden.
- **Screenlogger:** Als Gegenmaßnahme gegen Keylogger wurden Bildschirmtastaturen entwickelt. Die Reaktion der Malware-Autoren sind Screenlogger. Sie schießen entweder in regelmäßigen Abständen Bilder des gesamten Bildschirminhalts (z.B. Rbot) oder erzeugen bei jedem Mausklick eine Grafik des Umfelds der Maus. Manchmal werden die Bildsequenzen gleich in einen AVI-Film umgewandelt.
- **Browsermanipulation:** Einige Schädlinge (z.B. Torpig) verändern das Aussehen des Browsers. Sie sind in der Lage die Adresszeile mit der korrekten Adresse darzustellen, obwohl die Inhalte von einer anderen, gefälschten Domain kommen. Auch das Schloss, das eine verschlüsselte Verbindung symbolisiert, kann ungerechtfertigt eingeblendet werden.
- **Inhalte fälschen:** Manche Schädlinge (z.B. Bancos-Varianten oder Nurech) manipulieren die Inhalte bestimmter Webseiten und fügen entweder weitere Formularfelder oder ganze Webseiten ein. Dabei bleiben bestehende SSL-Zertifikate aktiv. Ohne spezielle Tools ist es nicht möglich, zu erkennen, ob diese Daten gefälscht sind oder nicht. Die so gewonnenen Daten werden sowohl an die Angreifer als auch an die echten Webserver geschickt. Nach dem Datendiebstahl wird die Sitzung normal fortgesetzt, so dass bei den Opfern kein weiterer Verdacht entsteht. Erst der Blick auf die Abrechnung offenbart den Angriff.
- Frühe **Session Hijacker** haben die Verbindung des Opfers unterbrochen, nachdem es seine Daten eingegeben hat. Dadurch wurde der Angriff unmittelbar bemerkt. Seit einiger Zeit werden Sessions so übernommen, dass der Angreifer die Beträge und Kontoangaben zu seinen Gunsten ändert (z.B. Bancos). Dem Opfer werden aber seine Angaben angezeigt. Sogar der Kontostand wird entsprechend gefälscht. Auch hier wird der Betrug erst beim Blick auf die Kontoauszüge ersichtlich.

- **DNS Spoofing:** Wie oben schon erwähnt, werden die lokalen Möglichkeiten einem Domainnamen eine falsche IP-Adresse zuzuweisen immer häufiger ausgenutzt. Ein Angriffspunkt, der von der Malwarefamilie QHosts häufig genutzt wird, ist die Datei Hosts im Verzeichnis C:\windows\system32\drivers\etc. In dieser Datei kann einem Domainnamen eine IP-Adresse zugewiesen werden. Wenn dies gelingt, werden keine weiteren Versuche unternommen die gefundene IP-Adresse zu verifizieren. Eine andere Möglichkeit bieten die Einträge für DNSServer. Sie werden so manipuliert, dass die DNS-Anfragen auf einen Server, der vom Angreifer kontrolliert wird umgeleitet. Für die meisten Seiten werden dann auch korrekte Ergebnisse geliefert -aber für andere eben nicht.
- **Redirector:** Lenken den Datenfluss so um, dass ein Man-in-the-middle Angriff möglich wird. Das kann ein lokaler Proxy sein oder ein Proxy-Server, der unter der Kontrolle des Angreifers steht. Darüber lässt sich die gesamte Netzkommunikation des Opfers belauschen. E-Mails, Chats, besuchte Webseiten, Formulardaten und Dateidownloads können so überwacht werden.
- **Sniffer:** Um den Datenstrom in einem Netzwerk abzufangen werden Sniffer installiert. Mittels ARP-Spoofing funktioniert das auch in ungeswitchten Netzwerken.
- **Spy-Trojans** durchsuchen den gesamten PC nach verwertbaren Informationen. Das können E-Mailadressen sein oder Dateien mit bestimmten Inhalten oder eines bestimmten Dateityps. Diese Daten werden gepackt und an den Angreifer gesendet. Sehr beliebt sind auch auf dem System gespeicherte Login-Informationen, Registrierungsschlüssel und Passwörter (oder deren Hashes). Im Protected Storage Area werden die Passwörter von Webseiten und E-Mail-Accounts gespeichert, sofern ein Nutzer das allzu nützliche Angebot des Browsers oder E-Mailclients annimmt, die Passwörter zu speichern. Es ist also eine gute Idee, auf das automatische Speichern der Passwörter und Anmeldeinformationen zu verzichten. Auch die Passwörter von Spielen, Registrierungsschlüssel des Betriebssystems und beliebter Software sind an bekannten Orten (Registry oder Dateien) auf dem System gespeichert und werden von dort entwendet.
- Auch der unbedachte Klick auf einen Link kann zum Datenverlust führen. Per **Cross Site Scripting** können Daten mitgelesen werden. So wurde beispielsweise der „Bieten"-Button von eBay-Auktionen so manipuliert, dass man auf eine gefälschte Anmeldeseite gelangt.
- **Cookies** sind eigentlich ungefährlich und für viele Webshopseiten unentbehrlich. Sie bieten aber auch wertvolle Informationen darüber welche Seiten jemand gerne besucht. Solche Informationen sind für Werbetreibende sehr wertvoll. Aber auch der Diebstahl eines Cookies kann sich lohnen. Wenn jemand vergessen hat sich in seinem Webshop oder seiner Kontaktbörse abzumelden, kann mit dem Cookie der Zugang zu dieser Webseite mit den Einstellungen des Opfers erfolgen.

Schutzmaßnahmen

Für jede einzelne dieser Bedrohungen sind spezielle Lösungen erforderlich, die sich an der jeweiligen Situation orientieren müssen. Unified Threat Management (UTM)-Systeme bieten aber einen soliden Grundschutz. Sie integrieren unterschiedliche Sicherheitsechnologien, wie zum Beispiel Firewall, Antivirus, Intrusion Detection oder Intrusion Prevention in einer integrierten Lösung und bietet einen Rundumschutz. Anhänger des „Best-of-Breed"-Konzepts kaufen die jeweils besten Einzelkomponenten und nehmen die umständlichere Konfiguration in Kauf. Eine neue Annäherung an das Thema ist „Behaviour Blocking": Die Behaviour Blocking-Technologie stellt ein sogenanntes proaktives Verfahren zur Analyse möglicher Malware dar. Die Technologie analysiert aktive Inhalte (Active Content), die eventuell schädlichen Code enthalten, in Bezug auf ihr Verhalten im Dateisystem, in der Registry und teilweise auch im Arbeitsspeicher des Rechners. Einige Lösungen setzen auch auf Sandboxverfahren, bei denen die Analyse in einem speziellen geschützten Bereich vorgenommen werden.

Schadensbilanz

Der Diebstahl von Daten ist nicht mehr nur die Domäne von Wirtschaftsspionen, Geheimdiensten und Terroristen. Cyberkriminelle Banden haben den Wert von Daten erkannt. Im Oktober 2005 wurde Kunden der schwedischen Bank Nordea ein AntiSpam-Tool zum kostenlosen Download angeboten. Es installierte eine Version des Keyloggers Haxdoor, der eine Fehlermeldung erzeugte und zur erneuten Eingabe der Zugangsdaten aufforderte. Als bemerkt wurde, dass zahlreiche Konten von Nordea-Kunden geplündert wurden, schloss die Bank das Onlinebankingportal.

Insgesamt entstand ein Schaden von etwa 900.000 EUR. Wie hoch der Schaden durch Onlinebankingbetrug ist, lässt sich nur schätzen. Deutsche Banken schweigen sich über die Schadenssummen aus. Der BITKOM geht für 2006 von 3250 Phishingfällen mit einem mittleren Schaden von 4000 EUR aus - zusammen also 13 Mio. EUR. Tendenz steigend [5]. Im Vereinigten Königreich ist die Informationslage etwas besser. Die Organisation APACS beziffert für 2006 die Schäden im Onlinebanking in Großbritannien auf ca. 46,5 Mio. EUR. Die Onlineschäden durch gestohlene Kreditkarteninformationen werden auf 214,6 Mio EUR geschätzt. Die weltweiten Schäden durch Datendiebstahl liegen demnach im Bereich von mehreren Milliarden Euro.

Die Aktivitäten sind aber schon lange nicht mehr auf Onlinebankingdaten begrenzt. Manche Datenspione stehlen auf infizierten Rechnern alle Eingaben in Formulare. Davon sind dann auch Zugangsdaten zu Social Networking Foren, Email-Postfächern, Onlineshops, Jobbörsen, Chaträumen uvm. betroffen. Die so ermittelten Datenmengen liegen deutlich im Terabyte-Bereich und sind nur mit leistungsfähigen Rechner- und Datenbankarchitekturen zu verarbeiten.

Im einfachsten Fall werden die Daten unsortiert auf dem Schwarzmarkt verkauft - 380 MB für 60 EUR. Die Zugangsdaten können aber auch zur Geldwäsche und zum Versand von Foren-Spam genutzt werden.

Trojan-Spy Programme packen alle Dokumente eines Rechners und versenden sie an die Angreifer. Im Falle des Trojaners, der Ende August im Bundeskanzleramt entdeckt wurde, konnte der Versand von 160 GB auf chinesische Webserver verhindert werden. Auch im Bereich der Datenbanken wurden einige große Coups gelandet. Bekannte Beispiele sind die Jobbörse Monster.com und das Studierendenportal StudiVZ.

Viele Fälle kommen aber gar nicht erst ans Licht der Öffentlichkeit, da die betroffenen Personen und Organisationen Rufschädigung befürchten. Diese Zahlen belegen, dass der Diebstahl von Informationen ein florierendes Geschäft ist.

Fazit

Der Diebstahl und der Handel mit gestohlen Daten ist ein weltweites Geschäft. Die Täter agieren länderübergreifend und in Netzwerken mit einem hohen Organisationsgrad. Die „Generation eCrime“ hat in den vergangenen Jahren auf unterschiedlichen Ebenen aufgerüstet – sei es infrastrukturell, taktisch oder ökonomisch - und verfügt im eCrime-Business über langjährige Erfahrung. Die Erschließung neuer Märkte und Crimeware-Konzepte wird 2008 sicherlich weiter voran schreiten.

Der Einsatz leistungsstarker Sicherheits-Lösungen, die AntiViren-, Antiphishing-, Firewall und Spam-Schutz vereinen, sollte auf Anwenderseite obligatorisch sein. Die Ergebnisse der

G DATA Security-Umfrage im Februar 2008 zeigte jedoch, dass Anwender es mit dem Virenschutz immer noch nicht genau nehmen: 47 Prozent der befragten Windows-User surften ungeschützt im Internet – davon nutzen 73 Prozent Online-Banking. Leichtfertigkeit im Umgang mit dem Thema Datensicherheit und der geringe Informationsstand über die Vorgehensweise der Online-Kriminellen erleichtert es der eCrime-Society, ihre dunklen Geschäfte im großen Stil zu realisieren.