



Veröffentlicht am: 18.06.2008

Blue Coat Systems: Martin Walzer

Autor: Martin Walzer, Technical Manager DACH & Osteuropa



Phishing & Pharming

Die Angreifer nutzen zunehmend gezielt Sicherheitslücken in Browsern oder Websites für ihre Angriffe aus

Wieso sind Phisher immer noch so erfolgreich?

"Weil sich die Angriffsart geändert hat: Phishing-Attacken laufen nicht mehr nur über E-Mail-Attachments, sondern die Angreifer nutzen zunehmend gezielt Sicherheitslücken in Browsern oder Websites für ihre Angriffe aus. Auch neue Technologien wie Mashups kommen ihnen dabei zu gute. Denn solche Web-Applikationen vereinen Daten aus unterschiedlichen Quellen in einer Anwendung beziehungsweise auf einer Seite. Gelingt es dann einem Angreifer, eine verbreitete Quelle zu kompromittieren, hat er gleichzeitig alle Seiten infiziert, die aus dieser Quelle Inhalte beziehen. Stellen Sie sich vor, es gelänge, Google Maps zu infizieren..."

Woher kommt Phishing oder Pharming, speziell aus welchen Ländern kommen die IP-Adressen, die verwendet werden?

"Die IP-Adressen der Angreifer ändern sich fortlaufend. Daher ist es schwierig bis unmöglich, die Angriffe auf bestimmte Länder einzugrenzen."

Sind Reputationsfilter basierend auf IP-Adressen wirksam?

"Nein. Denn die IP-Adressen der Angreifer ändern sich ja fortwährend, was eine Klassifizierung schwer bis unmöglich macht. Zudem analysiert ein klassischer Reputationsfilter Websites mit einer guten Reputation gar nicht. Wenn ein Hacker in so einer Website einen Iframe mit Schadcode injiziert, ist der Reputationsfilter schon wirkungslos. Das ist momentan tatsächlich ein großes Problem. Denn diese Art von Attacken zielt natürlich vornehmlich auf Websites mit einer guten Reputation ab. Stellen Sie es sich vor wie ein Pförtner in einem Unternehmen oder Ministerium, der regelmäßig Taschenkontrollen durchführen soll. Wenn der Pförtner nicht wirklich immer alle Taschen jeder Person überprüft, ist seine Arbeit letztlich wirkungslos. Denn wenn er bei Bekannten Ausnahmen macht und keine Kontrollen durchführt, können genau diese Personen einmal unbemerkt etwas ins Unternehmen einschleusen. Ein Reputationsfilter ist daher zwar gut für E-Mails aber nicht für Web-Inhalte, die Trojaner über 'gute Websites' einschleusen können. Hier hilft nur, URL- und Virenfilter für alle Inhalte anzuwenden – egal welcher Art und Herkunft."

Welche Methoden zur Erkennung sind effektiv und Ressourcen schonend?

"Ideal ist eine Kombination aus Virens Scanner und Content-Filter mit Mechanismen für Caching und Beschleunigung. Das ist effektiv, weil der Virens Scanner alle Arten von Webverkehr ausnahmslos überprüft. Der Content-Filter sorgt dafür, dass nur gewünschte Inhalte überhaupt aus dem Internet geladen werden. Und es ist Ressourcen schonend, denn einmal als 'sauber' klassifiziert hält der Cache die Daten eine bestimmte Zeit lokal vor und kann sie dem nächsten Anwender schnell zur Verfügung stellen, ohne sie nochmals analysieren zu müssen. Beschleunigungsmechanismen helfen dabei vor allem Unternehmen mit verteilten Standorten, die viel Datenverkehr über ihr Weitverkehrsnetz hin- und herschicken müssen."

Welche anderen Wege neben E-Mail suchen sich die Angreifer, um ihre Nachrichten zu verbreiten?

"Derzeit vor allem infizierte Websites, Trojaner und Phishing Sites."

Welche Konsequenzen drohen den Betreibern (egal ob ISPs oder Mobilfunkbetreiber)?

"Keine. Denn die Betreiber stellen ja nur den Weg für die Übertragung zur Verfügung. Stellen Sie sich vor, Sie kaufen in einem Baumarkt einen Hammer. Der ist eigentlich zum Nägel einschlagen gedacht. Wenn Sie nun aber auf jemanden losgehen und ihm mit dem Hammer den Kopf einschlagen, können Sie nicht den Baumarkt für den Verkauf des Hammers zur Rechenschaft ziehen."

Wie genau äußert sich der Trend in Richtung Spam im Web 2.0? Was macht diesen Spam so gefährlich?

"Im Gegensatz zu früher werden die Angriffe professioneller. Den Hackern geht es nicht mehr nur darum, eine Website lahmzulegen. Vielmehr wollen sie an vertrauliche Informationen wie etwa Kundendaten gelangen. Darüber hinaus finden die Angriffe nicht mehr wie früher über infizierte E-Mails statt, sondern mehr und mehr durch kompromittierte Websites. Dies erfordert Lösungen, die in Echtzeit Analysen durchführen und somit einen möglichst umfassenden Schutz bieten."

Mit welcher Art von Lösungen lassen sich Angriffe schnellstmöglich erkennen und blockieren?

"Derzeit sind sichere Web-Gateways eine gute Lösung, um den modernen Gefahren Herr zu werden. Denn diese Geräte bieten durch die Kombination von drei Elementen schichtweise Abwehrmechanismen, die Unternehmen größtmöglichen Schutz bieten: Diese umfassen erstens führende Anti-Malware-Engines mit heuristischer Analyse, zweitens URL-Filter, die URLs in Echtzeit überprüfen und auch sogenannte "Call Home"-Versuche erkennen und blockieren können und drittens die Kontrolle von Web-Inhalten, die unter anderem den Typ einer Datei (HTML-Seite, Skript, Flash, Grafik, etc.) berücksichtigen, Skripte und aktive Inhalte filtern, Zertifikate validieren oder auch bestimmte Arten von Verkehr wie Instant Messaging oder FTP berücksichtigen."

Wohin geht der Trend beim Phishing?

"Die Angriffe werden immer professioneller und die Hacker greifen zu immer ausgefeilteren Tricks. Zudem nutzen viele Angreifer gezielt die Schwachstellen und Sicherheitslücken in den modernen Web-2.0-Technologien."

Wie funktioniert ein proaktiver Schutz?

"100-prozentigen Schutz wird es nie geben. Das muss jedem klar sein. Doch bereits heute können Unternehmen sich durch netzwerkbasierendes Virenscreening am Gateway und durch einen Web-Filter mit Echtzeitkontrolle effektiv schützen. Grundsätzlich wird dem URL-Filter in Zukunft eine neue Bedeutung zukommen. Denn Web-2.0-Technologien erfordern einen Echtzeitansatz bei der Überprüfung von URLs. Zudem sollten Unternehmen mehrere Schichten einführen, um sich vor Malware unterschiedlichster Art zu schützen – beispielsweise vor dem Herunterladen von bösartigen Inhalten, die sich auf bekannten oder unbekanntem Sites 'verstecken'. Zudem müssen Unternehmen wissen, welche verschiedenen Arten von Web-Inhalten überhaupt in ihr Unternehmen hineindürfen. Denn unangemessene Inhalte wie beispielsweise Pornographie können auch in vermeintlich harmlosen Seiten versteckt sein oder als unerwünschter Treffer von Suchmaschinen ausgeliefert werden. Zudem ist es ratsam Lösungen einzusetzen, die eine möglichst granulare Abbildung der Unternehmensrichtlinien bieten und URLs beispielsweise mehreren Kategorien zuordnen können."

Martin Walzer, Technical Manager DACH & Osteuropa bei Blue Coat Systems

www.bluecoat.de