



TOP-SICHERHEITSTRENDS 2010

Sicherheit im Internet bleibt auch 2010 einer der wichtigsten Aspekte sowohl für Unternehmen als auch für ihre individuellen Benutzer. Blue Coat hat für Sie eine Übersicht der wichtigsten Trends zusammengestellt, damit Sie wissen, vor welchen Gefahren Sie sich in diesem Jahr besonders schützen sollten:

1. Web-basierte Gefahren

Seit 2007 nutzen Kriminelle hauptsächlich Online-Sicherheitslücken, um vertrauliche Daten und Finanzinformationen zu stehlen sowie infizierte Computer, die sie zu sogenannten Botnetzen zusammen schließen. Bereits in den ersten sechs Monaten des Jahres 2009 entdeckten Viren-Scanner mehr Malware als im gesamten Jahr 2008. Ebenso stieg Phishing in den ersten sechs Monaten 2009 auf 585 Prozent an. Über 300 Firmenmarken wurden Opfer von Phishing-Attacken. Auch 2010 wird dieser Trend unvermindert anhalten. Denn das Geschäftsleben hat sich durch den Einsatz von externen, web-basierten Anwendungen zunehmend ins WorldWideWeb verlagert. Zudem nutzen Mitarbeiter immer öfter Freizeit-Anwendungen auch im Unternehmen. Das Internet tut sein übriges: Es bietet Malware große Chancen auf Profit. Erfolgreich sind dort vor allem solche Attacken, die nur kurze Zeit existieren und nach einigen Stunden verschwinden bevor traditionelle Abwehrmechanismen greifen.

2. Infiltrierte Suchmaschinen

Die Infiltrierung von Suchmaschinen ist ein einfacher Weg um Anwender zu Malware zu locken: Cyberkriminelle nutzen die Algorithmen der Suchmaschinen, die dann gehackte Blogs als höhere Ergebnisse anzeigen. Die Links führen meist zu Schein-Viren-Scannern und verseuchten Raubkopien von Software, Spielen, Musik oder anderen Anwendungen. Ein Beispiel: die Labore von Blue Coat entdeckten vor kurzem einen Hack auf den Suchbegriff „Halloween“. Suchten Nutzer danach, zeigte die Suchmaschine verseuchte Blogs als beste Ergebnisse an. Je leichter Hacker Suchergebnisse durch Blogs beeinflussen können, umso wahrscheinlicher werden Angriffe darauf. Denn Suchmaschinen dienen für nahezu alle Anwender als Zugang zum Internet und das Vertrauen in Relevanz und Sicherheit der Ergebnisse macht die Nutzer zu leichten Opfern von Cyberkriminellen.

3. Linkketten, die zu Schadcode führen

Cyberkriminelle nutzen immer häufiger komplexe Pfade über mehrere miteinander verlinkte Webseiten, um unentdeckt zu bleiben. Solche Linkketten beginnen häufig mit einer Seite aus den Ergebnissen einer Suchmaschine. Von dort aus führen Kriminelle die Besucher über mehrere verlinkte Seiten – zum Beispiel über einen oder mehrere gehackte Blogs – auf eine verseuchte Seite mit Schadcode. Diese Attacken sind besonders schwer zu erkennen, da der Angriff nur dann erfolgt, wenn der Nutzer die vom Angreifer ersonnene Linkreihenfolge einhält. Gelangt er beispielsweise über einen anderen Pfad auf die Seite mit Schadcode oder gibt er die Adresse der verseuchten Seite direkt in seinen Browser ein, liefert die Zielseite keinen Schadcode aus. Derartige Attacken werden auch 2010 weiter zunehmen, da sie es Cyberkriminellen leichter machen, unentdeckt zu bleiben.

4. Menschliches Fehlverhalten

Traditionell galten einfache Passwörter und fahrlässiges Verhalten von Nutzern als Sicherheitsrisiken. Nun kommen neue, Web-basierte Gefahren hinzu, die das menschliche Verhalten auf einer neuen Ebene ausnutzen: Cyberkriminelle infiltrieren gerade die Bereiche, denen Nutzer besonderes Vertrauen schenken. In sozialen Netzwerken wie Twitter und Facebook bilden Anwender Gruppen und Online-Beziehungen zu ihren Freunden. Das Vertrauen in diesen Gruppen nutzen Cyberkriminelle aus, um durch gestohlene Logins an sensible Daten zu gelangen. Zur größten Gefahr für Sicherheitsmanager 2010 wird damit die Kombination aus Angriffen in sozialen Netzwerken, die das Vertrauen der Anwender ausnutzen, und der Infiltrierung von Suchmaschinen, deren Ergebnisse Anwender ohne sie zu hinterfragen anklicken.



Sicherheit in Echtzeit wird wichtiger – Vorteile einer Security Cloud

Die oben genannten Gefahren zeigen, dass Schutz in Echtzeit zunehmend an Bedeutung gewinnt. Denn nur so können Unternehmen sich vor dynamischem, web-basiertem Schadcode und Angriffen effektiv schützen, ohne ständig neue Updates oder Patches herunterladen zu müssen. Angriffe dauern heute oft nur noch knapp zwei Stunden, daher müssen Sicherheitssysteme immer schneller reagieren. Dies ist mit herkömmlichen statischen Antiviren-Programmen, die Client-basiert sind, nicht möglich. Cloud-basierte Technologien bieten hingegen die Möglichkeit, auf Input in Echtzeit mit Output in Echtzeit zu reagieren. Zudem können sie eine große Gruppe und nicht nur Einzelpersonen oder einzelne Unternehmen schützen.

Über Blue Coat Systems

Blue Coat Systems schützt die Internetkommunikation von Unternehmen und beschleunigt unternehmenskritische Anwendungen im Weitverkehrsnetz (WAN). Die Appliances und Client-Lösungen des amerikanischen Herstellers kommen in Niederlassungen und Rechenzentren sowie am Internet Gateway und auf Endpunkten zum Einsatz. Dort ermöglichen sie eine regelbasierte Kontrolle des Datenverkehrs und erlauben es Unternehmen, ihre Sicherheit zu optimieren und die Interaktionen zwischen Anwendungen und Anwendern zu beschleunigen. Blue Coat hat weltweit bereits mehr als 70.000 Appliances verkauft. Zu den Kunden zählen unter anderem Merck, die Süddeutsche Klassenlotterie, die U.S. Air Force, der ZEIT Verlag und andere. Der Hauptsitz von Blue Coat ist in Sunnyvale, Kalifornien (USA), die Deutschlandvertretung in München.