

Ein Mausklick kann Cyberkriminellen Tür und Tor öffnen

Studie zeigt: Dynamische, ausgefeilte Bedrohungen erfordern Web Security mit Echtzeitschutz

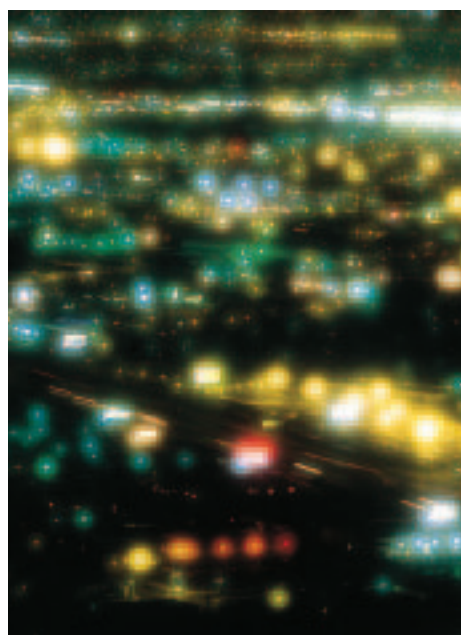
Blue Coat Systems hat den Web Security Report 2011 erarbeitet. Die Studie analysiert die Webnutzung von Anwendern und untersucht die Malware, denen sie am häufigsten ausgesetzt sind. Der Report basiert auf Daten des Blue Coat® WebPulse™-Dienstes, der pro Woche rund drei Milliarden Anfragen nach Webinhalten in Echtzeit bewertet. Damit erhalten die Blue Coat Security Labs umfassenden Einblick in die Veränderungen bei der Nutzung des Internets sowie in neue Angriffsmethoden von Cyberkriminellen.

Die Ergebnisse der 60-seitigen Studie gliedern sich in drei Gruppen: Daten über die veränderte Nutzung des Webs in 2010, neue Angriffsmethoden von Cyberkriminellen sowie deren Folgen für Unternehmen. Zudem gibt der Report konkrete Hinweise, wie Unternehmen ihre Nutzer und Daten besser schützen können. Die Basisdaten der Untersuchung stammen aus den Blue Coat Security Labs sowie aus dem Blue Coat WebPulse-Service. WebPulse analysiert angeforderte Webinhalte von weltweit mehr als 70 Millionen Benutzern in Echtzeit und stellt die Erkenntnisse umgehend seiner Nutzergemeinschaft zur Verfügung.

Veränderungen bei der Nutzung des Webs

Soziale Netze haben sich fest als neue Kommunikationsplattform etabliert. Dabei stehen persönliche Seiten und Blogs, Chat und Instant Messaging sowie E-Mail mittlerweile an zweiter, dritter und vierter Stelle der am meisten nachgefragten Unterkategorien von sozialen Netzen. Webmail hingegen stieg bei den beliebtesten Kategorien des gesamten

Webs in 2010 auf Platz 17 ab – von Platz neun in 2009 und Platz fünf in 2008. Grund dafür ist eine massive Abwanderung der Internetnutzer zu sozialen Netzen als Kommunikationsplattform ihrer Wahl.



Die Bedrohungen im Web sind dynamisch.
Alle Bilder creativ collection

Weiterhin zeigt der Blue Coat Web Security Report 2011, dass die weltweit hohe Arbeitslosigkeit mit ihren finanziellen Herausforderungen zur einer Verschiebung der Webnutzung führte – von der Befriedigung persönlicher Lüste hin zu mehr geschäftsorientierten Inhalten. Blue Coat konnte beispielsweise einen signifikanten Rückgang von Nachfragen nach Inhalten aus den Kategorien «Persönliches/Flirts», «Pornografie» und «Inhalte für Erwachsene» feststellen. Diese Themen standen in 2009 noch an vierter, fünfter und achter Stelle der zehn meistgefragten Kategorien. In 2010 dominierten hier «Audio/Video-Clips», «Nachrichten/Medien» und «Referenz».

Neue Bedrohungen aus dem Web

Bei den webbasierten Bedrohungen werden Angriffe immer ausgefeilter und kombinieren jetzt verschiedene Techniken in mehreren Stufen. Zu den wichtigsten Entwicklungen in 2010 zählen:

Soziale Netze werden Angriffsvektor für Malware: In 2010 konnten Cyberkriminelle erfolgreich die vertrauenswürdigen Beziehungen zwischen Freunden innerhalb sozialer Netze ausnutzen,

um schnell neue Nutzer zu infizieren und deren Benutzerkonten zu kompromittieren. Social Network Phishing und Clickjacking waren entsprechend die zwei verbreitetsten Attacken in sozialen Netzwerken in 2010. Phishing-Attacken verlagern sich zunehmend in Social Networks in der Hoffnung, dort Benutzerdaten für den Zugriff auf Banking-Anwendungen, Finanzdienste und andere Online-Konten abzugreifen, die dasselbe Passwort nutzen.

Seriöse Sites werden Teil der Angriffsinfrastruktur: Eine der auffallendsten Veränderungen der Bedrohungslandschaft in 2010 war die Migration von Angriffsinfrastrukturen von kostenlosen Domains hin zu bekannten Sites mit einer vertrauenswürdigen Reputation und einer entsprechend positiven Einstufung bei der erlaubten Internetnutzung. Durch den Einbruch in vertrauenswürdige Sites können Cyberkriminelle dort Infrastrukturen mit einer positiven Kategorisierung für ihre Angriffe aufbauen.

Malware versteckt sich in erlaubten Webkategorien: In der Vergangenheit hat sich Malware meist in Webseiten versteckt, deren Inhalte normalerweise auf Grund von Richtlinien für die zulässige Nutzung des Internets blockiert wurden. Doch in 2010 wuchs die Zahl der Sites

mit Malware am stärksten in den Kategorien «Online-Speicher» und «offene/vermischte Inhalte», die an zweiter respektive sechster Stelle lagen. Die Zahl der Online-Speicher-Sites mit Malware stieg dabei um 13 Prozent an, während die Zahl der Malware-Sites aus der Kategorie «offene/vermischte Inhalte» um 29 Prozent gewachsen ist. Beide Kategorien fallen in den meisten Unternehmen typischerweise unter die erlaubte Internetnutzung.

Angriffe auf Social Networks

Schlussfolgerungen für den Schutz von Mitarbeitern und Daten

Auf Basis dieser Erkenntnisse gibt der Blue Coat Web Security Report 2011 Ratschläge, wie Organisationen ihre Mitarbeiter und ihre vertraulichen Daten besser schützen können:

Dynamische Abwehr ist der Schlüssel für den Schutz vor Malware: Über dynamische Links können Cyberkriminelle Angriffsinfrastrukturen aufbauen, bei denen sie lediglich den Speicherort ihrer Malware verändern. Um die Auslieferung von Malware sowie Call-Home-Versuche, Betrugsmaschen und Phishing zu blockieren, ist eine Abwehr nötig, die dynamisch reagiert, neue und unbekannte Inhalte bewertet und dynamische Links analysiert. Denn diese sind zunehmend fester Bestandteil von Malware-Attacken.

Bewertungen in Echtzeit sind für erfolgreiche Webabwehr ausschlaggebend:

Wenn Abwehrmechanismen Webanfragen nicht in Echtzeit analysieren und sofort Einstufungen zurückliefern, setzen sie ihre Nutzer Angriffen aus, die oft nur wenige Stunden dauern können.

Weniger auf Reputationsbewertungen verlassen: Um nicht entdeckt zu werden, hacken Cyberkriminelle zunehmend seriöse Websites mit einer guten Reputation und nutzen diese Sites als Ausgangsbasis für ihre Angriffe. Eine Abwehr, die sich nur auf Reputationsbewertungen verlässt, kann seine Nutzer nicht vor diesen Angriffen schützen.

Schutz für entfernte Benutzer: Der Zugang zum Web ist fast überall möglich. Daher muss der Webzugang auch rund um die Uhr und an jedem Ort geschützt werden.

Datenverlust durch Malware: Keine Data Governance und keine automatische Data Loss Prevention werden den Verlust von Daten auf Grund von Malware verhindern. Daher werden Organisationen zukünftig eine dynamische Webabwehr einsetzen müssen, die Command- und Control-Server identifizieren kann und Anfragen dieser Server sowie Sendeversuche von Daten an diese Server blockiert.

Der vollständige Blue Coat Web Security Report 2011 ist kostenlos in Englisch verfügbar unter: www.bluecoat.com/doc/15802



Eine gute Reputation allein schützt nicht mehr vor Cyberkriminellen.

KONTAKT: Blue Coat Switzerland
Route des Arsenaux 3a
1700 Fribourg
Tel. 026 350 52 00
Fax 026 350 52 02
www.bluecoat.com