

Sicherheitsdienste aus der Cloud

Der Schutz der Vielen

Eine Gruppe von Menschen ist gegenüber Einzelpersonen oft im Vorteil. Das wissen nicht nur die Kandidaten von „Wer wird Millionär“, wenn sie mit ihrem Publikumsjoker das „Wissen der Vielen“ anzapfen. Auch Cyberkriminelle nutzen beispielsweise die geballte Masse „der Cloud“, um über Bot-Netze mit Distributed-Denial-of-Service-Attacken gezielt Websites in die Knie zu zwingen. Doch was die Bösen aktiv praktizieren, lässt sich auch zum Guten einsetzen. Denn Security-Services können ebenfalls die Macht der Cloud nutzen und ihre Nutzer – mit deren Hilfe – wirksam vor Angriffen schützen.

Am 4. Mai 2011 jährt sich zum elften Mal der Tag, an dem sich der Skript-Virus „Loveletter“, auch „I-love-you-Virus“ genannt, explosionsartig per E-Mail-Attachment weltweit verbreitete. Ein Grund für den „Erfolg“ des Virus war seinerzeit ein Attachment mit dem Namen „LOVE-LETTER-FOR-YOU.TXT.vbs“, das viele Empfänger zum Klick animierte – und so zu ihrem Verhängnis wurde.

Viren, Würmer und Trojaner sind in den letzten elf Jahren nicht weniger geworden. Doch haben sich ihre Verbreitungswege stark verändert. So gelangten laut einer Untersuchung von Osterman Research in 2009 bereits 90 Prozent der Malware über versteckte Links in vertrauenswürdigen und beliebten Webseiten auf die Rechner ihrer Opfer. Jeden Tag wurden in 2009 dabei rund 15.000 Webseiten mit Malware infiziert.

Statische Filter schützen nicht mehr

Ein Grund für die Verschiebung der Angriffsvektoren ist, dass Cyberkriminelle damit an der aktuell schwächsten Stelle der Malware-Abwehr in Unternehmen ansetzen: bei Webfiltern mit statischen URL-Datenbanken. Anbieter entsprechender Filterlösungen aktualisieren ihre URL-Datenbank zwar regelmäßig. Doch reicht dieser klassische Ansatz bei der Dynamik der heutigen Attacken nicht mehr aus. Denn das Web ist inzwischen einfach zu groß geworden und wächst viel zu schnell, um es nur annähernd in seiner Gesamtheit in statischen Datenbanken abzubilden. So hat beispielsweise allein das soziale Netzwerk Facebook im Jahr 2010 pro Sekunde geschätzt knapp acht neue Nutzer gewonnen – und soll mittlerweile rund 600 Millionen Mitglieder zählen. Jeder Nutzer erhält dabei auf Facebook eine sich ständig ändernde Web-Seite mit Informationen aus seinem Netzwerk. Weiterhin kann jeder Nutzer selber beliebig viele dynamische „Pages“ etwa

für seinen Sportverein oder Lieblingssänger anlegen. Rechnet man dies nur auf alle deutschsprachigen sozialen Netze, Blogs, Nachrichtenseiten etc. hoch, so wird schnell klar, dass statische Filter diesem Wachstum schlicht nicht gewachsen sein können.

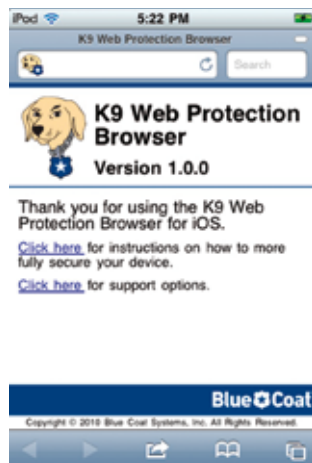
Neue Angriffsarten über dynamische Links

Trieb früher ein Klick auf ein Attachment einen Nutzer in sein Unglück, reicht heute bereits der Besuch einer infizierten Webseite aus. Um potentielle Opfer dorthin zu führen, setzen Angreifer auf verschiedene Verfahren mit dynamischen Links. Ein Trick ist beispielsweise, entsprechende Links in Suchergebnissen eines scheinbar harmlosen Web-Angebots zu verstecken. Früher kam diese Art von Angriffen hauptsächlich in Suchmaschinen zum Einsatz für nicht ganz so harmlose Inhalte wie Raubkopien, illegale Seriennummern oder pornographisches Material. Doch das Bild hat sich komplett gewandelt. Aktuelle Untersuchungen der Blue Coat Labs zeigen beispielsweise, dass die beliebtesten Web-Köder dieser Art heute in Suchergebnissen von Sites auftauchen, die entweder kostenloses Lernmaterial für Kinder oder Rabatt-Coupons für Einkäufe anbieten.

Eine weitere verbreitete Art von Attacken sind so genannte Drive-by-Injections. Cyberkriminelle infizieren hierbei beispielsweise eine legitime Website und verstecken dort einen iFrame mit einem dynamischen Link. Oder sie nutzen ein kompromittiertes Benutzerkonto eines sozialen Netzwerks, um darüber Nachrichten mit dem Titel „Ein Bild von Dir“ und einem dynamischen Link auf eine Malware-Seite zu verschicken. Oft reicht bereits ein Besuch einer so infizierten Seite aus, um Malware ohne weiteres Zutun auf dem Rechner des Besuchers zu installieren.

Um ihre Herkunft noch weiter zu verschleiern, nutzen Angreifer zudem Verkettungen von dynamischen Weiterleitungen. Ein Klick auf einen Link leitet die Anfrage dabei an eine ganz andere URL weiter, hinter der wiederum eine Kette von Weiterleitungen stehen kann. Das wahre Ziel eines Links (oder die Quelle einer iFrames) ist so für Benutzer nicht mehr erkennbar.

Beide Arten von Angriffen sind deshalb so effektiv, da sie meist sehr kurzlebig sind, scheinbar aus vertrauenswürdigen Quellen stammen und ihr Ziel über dynamische Links verschleiern. Der Schlüssel zu einer erfolgreichen Abwehr kann daher nur sein, die dynamischen Linkziele erst zu erkennen, dann das entsprechende Wissen über die darin versteckten Gefahren zu besitzen, diese zu bewerten und dieses Wissen schließlich in Echtzeit an die Stellen auszuliefern, die Benutzer vor Bedrohungen aus dem Web schützen sollen.



Das Web Security Module des Blue Coat Cloud Service nutzt die Macht seiner Community, um seine Nutzer rund um die Uhr vor neuen Gefahren aus dem Web zu schützen.
Quelle: Blue Coat Systems



Auch mobile Nutzer können als Mitglied einer Cloud-Community vom Schutz der Vielen profitieren.
Quelle: Blue Coat Systems

Hoffnung aus der Cloud

Das Web besteht heute aus Abermilliarden von Webseiten, von denen sich viele fast in Echtzeit verändern. Statische Positiv- und Negativlisten, meist von Hand und von Web-Spidern gepflegt, haben keine Chance mehr, mit dem Wachstum und der Dynamik von Webseiten mitzuhalten. Doch wenn man über die Cloud – sprich das Internet – eine möglichst große Zahl von Nutzern zu einer Community zusammenschließt, die Informationen über die von ihnen besuchten Webseiten anonymisiert an eine zentrale Stelle übertragen, so hat man sehr gute Chancen, dabei auch möglichst viele kompromittierte Links und Seiten zu treffen. Diese Community kann so aktiv dazu beitragen, einem Security-Service in der Cloud ein realistisches Bild von den aktuell gefragten Web-Inhalten zu liefern. Und dann haben intelligente Mechanismen innerhalb eines Cloud-Service wiederum die Chance, in den angefragten Seiten dynamische Links zu unerwünschten Inhalten zu entdecken – und die Community davor zu warnen.

Dynamische Linkanalyse

Um zu erkennen, was sich hinter einem Link befindet, müssen die von der Cloud-Community angeforderten Seiten zunächst von dem Security-Service analysiert werden. Dies leisten in der Praxis große Serverfarmen in weltweit verteilten Rechenzentren. Zunächst wird dort bei der Anfrage einer unbekanntenen URL durch einen Benutzer die angeforderte Ressource geladen

und anschließend werden alle dort referenzierten Inhalte – einschließlich potentiell verlinkter Malware oder in iFrames versteckter Inhalte – analysiert. Verlinkte Dateien werden zudem durch mehrere Antiviren-Engines geschickt, um dort versteckte Bösewichte zu entdecken.

Mit einer vielschichtigen dynamischen Linkanalyse lassen sich so beispielsweise bei Blue Coats Cloud Service rund 98 Prozent der von den aktuell 80 Millionen Cloud-Nutzern angefragten Inhalte innerhalb von 300 Millisekunden automatisiert analysieren und kategorisieren. Dabei fließen auch Daten von Dritten wie beispielsweise von Google, der Anti-Phishing Working Group (APWG), PhishTank und weiteren in die Analyse mit ein. Für die restlichen zwei Prozent erfolgen tieferegehende Analysen, an deren Ende auch menschliche Experten in den verteilten Rechenzentren stehen können. Die Ergebnisse der dynamischen Linkanalysen gleicht der Cloud-Service laufend zwischen seinen weltweiten Rechenzentren ab.

Weltweiter Schutz nur aus der Cloud

Ruft dann beispielsweise ein Nutzer des Cloud-Service in Singapur eine Seite mit einem versteckten iFrame auf, der auf Mal-

ware verlinkt, übermittelt ein zwischengeschalteter Proxy die Anfrage zunächst an den Dienst in der Cloud. Ist der Link nicht in der zentralen Datenbank verzeichnet, beginnt die nächstgelegene Serverfarm automatisch mit der Analyse der dort hinterlegten Inhalte. Entdeckt die dynamische Linkanalyse beispielsweise einen Trojaner, kategorisiert sie den Link entsprechend und liefert ihre Einstufung an den anfragenden Proxy zurück. Dieser entscheidet dann anhand von hinterlegten Richtlinien, ob der entsprechende Benutzer auf die Zielseite darf oder nicht. Darauf folgende Anfragen nach dem Link – egal woher sie auf der Welt kommen – werden dann für eine gewisse Zeit automatisch mit der entsprechenden Bewertung beantwortet, bevor eine neue Analyse erfolgt. Zum Vergleich: Ein statischer Filter hätte bestenfalls erst Stunden später beim nächsten Signatur-Update oder Patch eine entsprechende Bewertung geliefert – die dann vielleicht schon längst überholt wäre.

Es gibt viele Möglichkeiten, wie einzelne Nutzer aktives Mitglied einer Security-Cloud werden können, beispielsweise durch einen kostenlosen Internetfilter für zu Hause wie etwa „K9 WebProtection“, über ein sicheres Web-Gateway im Unternehmen mit Verbindung zu einem Cloud-Service oder über eine lokale Desktop-Software für mobile Nutzer und Telearbeiter.

Unabhängig davon, wie die Anbindung letztlich erfolgt, ist eines sicher: Nur gemeinsam und mit Hilfe der Cloud können Nutzer heute mit den schnelllebigen Bedrohungen aus dem Web mithalten. Und je mehr Nutzer sich einer solchen Community anschließen, desto besser ist ihr Schutz. Klassische Webfilter mit statischen Signaturdatenbanken werden Angreifern immer hinterherlaufen. ■

Dietmar Schnabel,
Geschäftsführer DACH & Osteuropa
bei Blue Coat Systems



Für Abonnenten ist dieser Artikel auch digital auf www.datakontext.com verfügbar..



Weitere Artikel/News zum Schwerpunkt unter www.datakontext.com/cloud