SONICWALL

KURZDARSTELLUNG: WIE CYBER-KRIMINELLE IHRE REPUTATIONS-MANAGEMENTLÖSUNG UMGEHEN

Die Entwicklung des Reputationsmanagements für die E-Mail-Sicherheit

Zusammenfassung

Cyberkriminelle nutzen den technologischen Fortschritt, um neue Taktiken und Angriffsvarianten zu entwickeln. 1997 entwickelt, bildet die Real-time Blackhole List (RBL) die Grundlage des heutigen DNS-based Blackhole List(DNSBL)-Formats. Doch Hacker sind mit ihren Angriffen in der Lage, solche IP-Reputationsmanagementsysteme lahmzulegen und zu umgehen. Sicherheitsexperten sollten daher ihre Lösungen ständig weiterentwickeln, um Kriminellen einen Schritt voraus zu sein und diese Angriffe zu stoppen.

Wie Cyberkriminelle IP-basierte Reputationsmanagementlösungen umgehen

Je beliebter IP-Reputation-Systeme werden, desto mehr gerieten sie ins Fadenkreuz von Hackern. Mittlerweile steigen immer mehr Cyberkriminelle von Spam auf Phishing um: Sie geben sich als vertrauenswürdige Partner oder Freunde aus und versuchen über Ihr E-Mail-System und Ihre Mitarbeiter Ihr Unternehmen zu treffen. Ihre Phishingmails zielen darauf ab, legitime E-Mail-Server in großen, bekannten Unternehmen zu kompromittieren oder E-Mail-Konten von ISPs und ASPs wie Yahoo® oder Gmail® zu hacken. Cyberkriminelle können so eine Auflistung in traditionellen IP-Reputation-Systemen vermeiden oder zumindest hinauszögern, indem sie bösartige E-Mails zusammen mit unbedenklichen E-Mails aus den kompromittierten Servern legitimer Unternehmen heraus versenden.

Obwohl sie ihre IP-Adressen manipulieren, verändern sie nicht alle Aspekte einer Phishing- oder Spammail auf gleiche Weise. Wie andere profitorientierte Organisationen verringern Hacker ihre Verwaltungskosten, indem sie die Komplexität reduzieren. Sie tendieren dazu, IP-Adressen sowie Inhalte, Layouts, Hyperlinks

Um sich auf künftige E-Mail-Bedrohungen vorzubereiten, müssen Sie aus bisherigen Erfahrungen lernen.

und Bilder wiederzuverwenden. Diese Tatsache kann man für eine zusätzliche Verteidigungsstufe aus Reputationsidentifizierung und -verwaltung, die über bloße IP-Adressen hinausgeht, nutzen.

Wie alles begann: die Entwicklung des Reputationsmanagements

Das ursprüngliche E-Mail-Reputationsmanagementsystem geht auf die Real-time Blackhole List (RBL) zurück. Die allererste RBL wurde 1997 von Paul Vixie für das Mail Abuse Prevention System (MAPS) entwickelt. Wie eine Netzwerkverbindung, die eingehenden Datenverkehr ablehnt, anstatt ihn weiterzuleiten, beabsichtigte Vixie mit dem „Blackhole“ in diesem Fall, E-Mail-Verkehr von Websites abzulehnen, die Spam direkt versenden oder unterstützen. Die ursprüngliche RBL bestand aus einer Liste verdächtiger Websites, die über das Border Gateway Protocol (BGP) an Systemadministratoren weitergeleitet wurde, die sie abonniert hatten. Abonnenten konnten diese Liste dann anwenden, um TCP-/IP-Verkehr von diesen Websites zu blockieren.

RBL-Reputationen waren zwar ein wichtiger Schritt bei der Bewältigung von Spam, brachten allerdings auch enorme Herausforderungen mit sich. MAPS überprüfte sorgfältig, ob die Websites auch tatsächlich auf die Liste gehören, bevor sie anschließend veröffentlicht wurden. Zwar konnte damit die Anzahl an Falschmeldungen reduziert werden, doch gleichzeitig wurde die Reaktion der Abonnenten auf Angriffe erheblich verlangsamt. Im Laufe der Zeit entwickelte MAPS RBL-Clients, die sich mit E-Mail-Software integrieren ließen. Auf diese Weise konnten Administratoren ihre eigene RBL individuell anpassen, um eingehende E-Mails je nach Server abzulehnen.

Die MAPS-RBL legte den Grundstein für die Entwicklung des DNS-based Blackhole List(DNSBL)-Formats. Der Internetdienst Domain Name System (DNS) übersetzt mithilfe eines DNS-Servers Domain-/Hostnamen in IP-Adressen (Forward-DNS) und IP-Adressen in ihre entsprechenden Domain-/Hostnamen (Reverse-DNS). Die DNSBL war mehr als nur eine einfache Liste: Sie umfasste mehrere Standards, um IP-Adressen dynamisch zur Liste hinzuzufügen oder wieder zu entfernen. DNSBL-Serviceprovider konnten dann mittels eines standardisierten Formats aktualisierte Listen über den Internet Domain Name Service (IDNS) verteilen. Zu Identifizierungs- und Analysezwecken fügten Early Developer von DNSBLs weitere Kriterien hinzu, z. B. ob der sendende Mailserver potenziell unsichere offene Relays oder Proxys nutzt oder ob ein Mailserver Spam an ein „Honeypot“-System sendet, das zum Sammeln und Erfassen von Spam gedacht ist.

Heute gibt es Dutzende DNSBL-Services. Dabei sind die meisten E-Mail-Server in der Lage, diese Dienste abzufragen, um die Reputation der IP-Adressen zu prüfen. Allerdings nutzen diese Services unterschiedliche Standards, um IP-Adressen in ihren Listen hinzuzufügen, zu entfernen oder zu behalten. So kann es vorkommen, dass manche Servicelisten potenziell gefährliche IP-Adressen außer Acht lassen oder fälschlicherweise gültige IP-Adressen führen.

Fazit

E-Mails sind ein kritischer Bedrohungsvektor, den Cyberkriminelle ständig für ihre Angriffe nutzen. Wie sich herausgestellt hat, wurden Phishingmails in der Vergangenheit als wichtige Vehikel für die meisten erfolgreichen Angriffe auf Unternehmensnetzwerke eingesetzt. Mit dem Vormarsch von Spear-Phishing- und Whaling-Attacken wird es immer schwieriger, bösartige Nachrichten von legitimen geschäftlichen E-Mails zu unterscheiden. Daher sollten Sie auf jeden Fall einen Blick auf Ihr Reputationsmanagementsystem werfen und sicherstellen, dass es einen effektiven Schutz vor neuen E-Mail-Bedrohungen bietet.

Erfahren Sie mehr. Lesen Sie unsere Lösungsübersicht Wie Sie mit erweitertem Reputationsmanagement gegen E-Mail-Bedrohungen vorgehen.

Über SonicWall

Seit über 25 Jahren schützt SonicWall kleine, mittlere und große Unternehmen weltweit vor Cyberkriminalität. Mit unseren Produkten und Partnerschaften können wir eine Echtzeit-Cyberabwehrlösung für die individuellen Anforderungen von über 500.000 globalen Organisationen in über 150 Ländern bereitstellen, damit sie sich voll und ganz auf ihr Geschäft konzentrieren können.

Wenn Sie Fragen zur Nutzung dieser Unterlagen haben, wenden Sie sich an:

SonicWall Inc.
5455 Great America Parkway
Santa Clara, Kalifornien 95054, USA

Weitere Informationen finden Sie auf unserer Website.
www.sonicwall.com