

URL-Filter und Internet-Sicherheit (Cascadia Labs)

Ergebnisse vom Sommer 2009

Zusammenfassung

Im Sommer 2009 testete Cascadia Labs die Wirksamkeit fünf marktführender Lösungen für Internet-Gateway-Sicherheit, darunter drei Appliances für den Netzwerkrand von Blue Coat und McAfee, Software von Websense und die Trend Micro InterScan Web Security Virtual Appliance.

Die für die Tests verwendeten URLs wurden von Cascadia Labs unabhängig gesammelt, klassifiziert und verifiziert. Keines der Unternehmen, dessen Produkte getestet wurden, hatte also

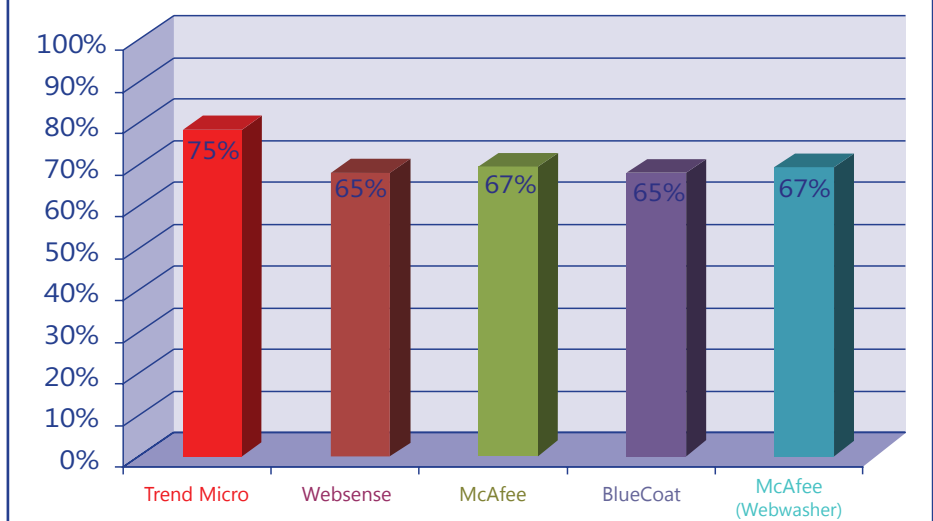
Trend Micro ging als klarer Sieger hervor und baute seine 2008 erzielte Führungsposition weiter aus.

diese URLs bereitgestellt noch waren sie ihnen bekannt. Wir sammelten und verifizierten in den Tagen unmittelbar vor dem Testen Sicherheitslinks, um zu gewährleisten, dass es sich um aktuelle Bedrohungen, einschließlich potenzieller Zero-Day-Angriffe handelte, die zurzeit aktiv im Umlauf waren.

Trend Micro ging aus diesen Tests als eindeutiger Gesamtsieger hervor und baute dadurch seine führende Position, die das Unternehmen in unseren Tests Ende 2008 eingenommen hatte, weiter aus.

Trend Micro zeigte auch gegenüber Sicherheitsbedrohungen einen entscheidenden Vorteil, wozu die Web-Reputation-Services einen wesentlich Beitrag leisteten. In jeder Sicherheitskategorie – Malware, Exploits, Phishing, Proxys und

Tabelle 1: Wirksamkeit der Abwehr insgesamt (gewichteter Durchschnitt)



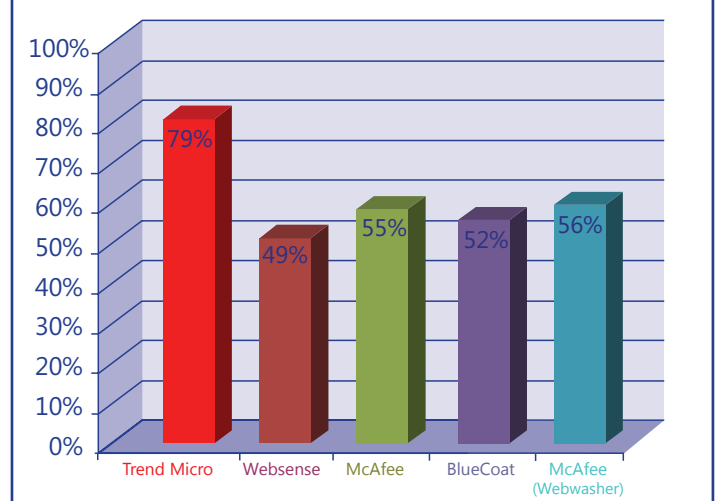
potenziell unerwünschte Anwendungen – erzielte Trend Micro das beste Ergebnis. Die Trend Micro IWSVA Internet-Gateway-Sicherheitslösung wehrt Sicherheitsbedrohungen zu fast 80 Prozent ab. Damit hebt sich diese Lösung deutlich von anderen Produkten ab, die im Schnitt gerade einmal 49 bis 55 Prozent erreichten.

Überblick

Internet-Gateway-Sicherheitslösungen verfügen über zahlreiche Funktionen, um den Zugriff auf Web-Inhalte am Netzwerkrand zu verwalten, zu sperren und zu steuern. Unternehmen verlassen sich auf diese Produkte, um ihre

Mitarbeiter, PCs und Netzwerke vor gefährlichen, unangemessenen und unerwünschten Inhalten im Internet zu schützen. Zusätzlich zur Durchsetzung von Nutzungsrichtlinien für Webseiten mit eindeutig sexuellen, gewaltverherrlichenden oder illegalen Inhalten können diese Produkte auch eine

Tabelle 2: Wirksamkeit der Sicherheitsabwehr insgesamt



entscheidende Rolle beim Schutz von Unternehmensnetzwerken vor Internet-Bedrohungen, einschließlich Drive-by-Downloads, Malware und Phishing-Angriffen, spielen.

Da diese webbasierten Sicherheitsbedrohungen an Häufigkeit, Umfang und Raffinesse zunehmen, sind zusätzliche Schichten einer tiefgreifenden Schutzstrategie selbstverständlich von immer größerem Nutzen. Filter für nicht jugendfreie oder produktivitätsstörende Sites sind schon beinahe Massenware. Es gibt jedoch große Abweichungen darin, wie wirksam Produkte Funktionen wie URL-Datenbanken und Web-Reputation-Services kombinieren, um Sicherheitsbedrohungen zu sperren.

Im Sommer 2009 testete Cascadia Labs fünf marktführende Internet-Gateway-Sicherheitslösungen: Appliances für den Netzwerkrand von Blue Coat und McAfee (darunter ein früheres Webwasher-Produkt), Websense-Software und die virtuelle Appliance von Trend Micro. Trend Micro ging aus dem Test als eindeutiger Gesamtsieger hervor und zeigte eine klare Überlegenheit im Bereich Sicherheitsbedrohungen.

Wie in Tabelle 1 gezeigt, erzielte Trend Micro InterScan Web Security Virtual Appliance (IWSVA) eine gewichtete Gesamtbewertung von 75 Prozent. Die beiden McAfee-Produkte belegten den zweiten Platz und erreichten jeweils 67 Prozent. Zusätzlich zur höchsten Gesamtbewertung war Trend Micro führend beim Sperren von URLs, die zu Sicherheitsbedrohungen führen. IWSVA erzielte hier eine dominierende Bewertung von 79 Prozent, verglichen mit den Ergebnissen anderer Produkte von durchschnittlich 50 Prozent.

Abgesehen von der Sicherheit spielen URL-Filterprodukte auch beim Durchsetzen allgemeinerer Unternehmensrichtlinien zur Internet-Nutzung eine wichtige Rolle. Unsere Tests haben gezeigt, dass sie alle die überwiegende Mehrzahl nicht jugendfreier und produktivitätsstörender URLs sperren.

Außerdem zeigten alle Produkte eine angemessene Leistung, die allerdings hinsichtlich Bandbreitennutzung, Kommunikation und Haftung noch verbesserungsfähig ist.

Getestete Produkte

Cascadia Labs testete im August 2009 die folgenden fünf Produkte:

- **Trend Micro InterScan Web Security Virtual Appliance v5**
- **Websense Security Suite v7.1**
- **McAfee Email and Web Security Appliance 3000**
- **Blue Coat Proxy SG 210A v5.4.1.12**
- **McAfee Web Gateway WW500E (ehemals Webwasher) v6.8**

IronPort verweigerte uns die Zustimmung, seine Software für diesen Test zu erwerben.

Bitte beachten Sie, dass Websense sein Produkt in „Websense Web Security“ umbenannt hat.

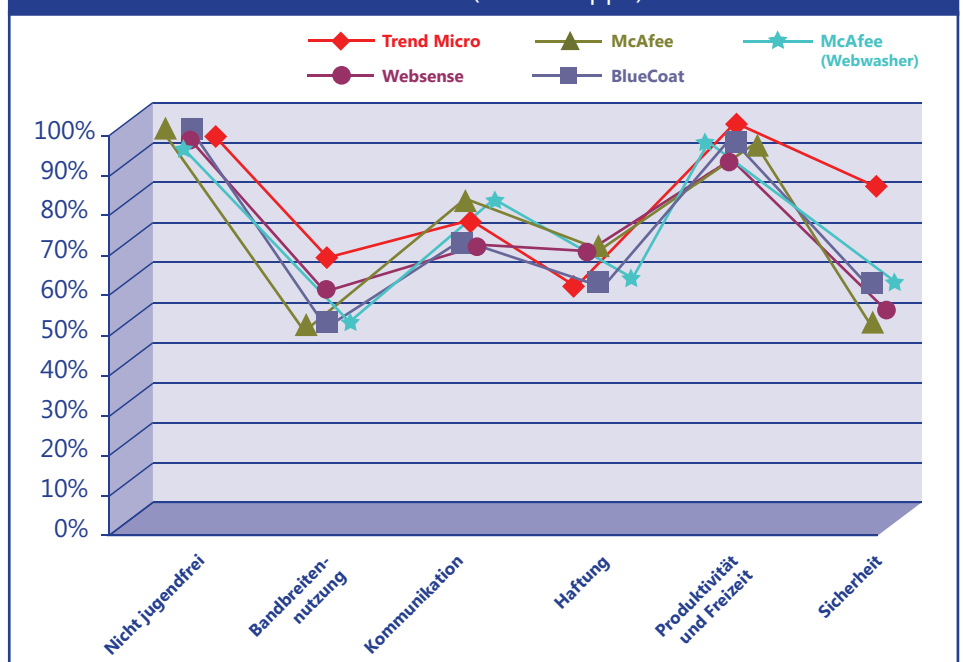
In diesem Bericht konzentriert sich Cascadia Labs ausschließlich auf die Wirksamkeit der Abwehr von URL-Datenbanken und Web-Reputation-Funktionen des Produkts.

Ergebnisse und Analyse

Trend Micro IWSVA, das sowohl Funktionen zur Remote-Bewertung als auch zur Web Reputation umfasst, erzielte konsistent bei jeder Art von Inhalten Spitzenwerte oder lag minimal darunter (Tabelle 3).

Funktionen zur Remote-Bewertung und zur Web Reputation haben in den vergangenen Jahren dazu beigetragen, dass viele Internet-Gateway-Sicherheitsprodukte schneller auf ein komplexes und sich schnell veränderndes Internet reagieren. Anstatt einfach nur eine lokale Kopie einer URL-Datenbank heranzuziehen, können Produkte mit Remote-Bewertungen externe Server abfragen, um sekundengenaue Daten bereitzustellen. Ebenso sind Produkte mit Web-Reputation-Funktionen mittels Heuristiken in der Lage, ungewöhnliche Muster zu entdecken – sowohl im Inhalt der Seite selbst als auch darüber hinaus. Während wir den Beitrag dieser verschiedenen Ansätze analysieren, interessieren sich Kunden ungeachtet der zugrunde liegenden Technologie letztendlich dafür, dass die Produkte unerwünschte URLs sperren können. Daher zeigen unsere veröffentlichten Berichte nur die Ergebnisse bezüglich

Tabelle 3: Wirksamkeit der Abwehr (nach Gruppe)



der Wirksamkeit der Abwehr auf oberster Ebene.

Sicherheitsbedrohungen sind auch weiterhin die große Herausforderung für diese Produkte. Die durchschnittlichen Sperrraten liegen bei 58 Prozent; das ist relativ niedrig im Vergleich zu anderen Kategorien, obwohl sich der Durchschnittswert im vergangenen Jahr verbessert hat. Trend Micro zeigte in diesem Bereich eine deutliche Überlegenheit gegenüber den anderen von uns getesteten Produkten.

In nicht sicherheitsbezogenen Kategorien waren die Effektivitätsabweichungen gering. Die Produkte sperrten durchschnittlich 59 Prozent der gefährlichen URLs, ohne dass ein einzelnes Produkt ein deutlich besseres Ergebnis erzielte. Beim Sperren von Bandbreitennutzung waren alle Produkte mit einem Durchschnittswert von 47 Prozent weniger wirksam. Die Produkte sperrten durchschnittlich 69 Prozent der URLs von Kontaktnetzwerken und Chatrooms, einschließlich der allseits präsenten Kategorie sozialer Medien. Wie auch in den vergangenen Quartalen sperrten alle Produkte wirksam die Gruppen „Nicht jugendfrei“ sowie „Produktivität und Freizeit“. Es gab keine bedeutsamen Unterschiede.

Sicherheit

Trend Micro sperrte im Durchschnitt 79 Prozent der Angriffe in allen Sicherheitskategorien. Dieser Wert positioniert die Appliance unangefochten vor den anderen Produkten, deren Wirksamkeit zwischen 49 und 55 Prozent lag. Die Fähigkeit, sogar mit deaktivierter Suche am Netzwerkrand nicht weniger als vier von fünf Bedrohungen zu sperren, veranschaulicht, dass Internet-Gateway-Sicherheitslösungen einen wertvollen Beitrag zu einer tiefgreifenden Sicherheitsstrategie leisten können.

Malware

Trend Micro sperrte drei Viertel aller Malware-URLs, gefolgt von McAfee 3000 mit 62 Prozent. Die anderen Produkte sperrten zwischen 53 und 55 Prozent. Nach unserer Definition umfasst der Begriff „Malware-URLs“ sowohl URLs, die direkt auf bösartige Binärdateien verweisen (die häufig Social-Engineering-Tricks verwenden, um Benutzer so zu verwirren, dass sie die Dateien unabsichtlich herunterladen und installieren) als auch URLs zu Schadteilen, die durch Drive-by-Downloads heruntergeladen werden.

Das Sperren von Malware-URLs bedeutet geringe Latenzzeiten und ist eine Alternative zur Suche in

Binärdateien am Netzwerkrand. Um sich auf die URL-basierten Sperrfunktionen der Produkte zu konzentrieren, aktivierte Cascadia Labs für diese Tests keine verfügbare Malware-Suche.

Exploits

Trend Micro sperrte fast 80 Prozent der Exploit-URLs. Die anderen Produkte lagen zwischen 48 und 58 Prozent. Exploits, so genannte Drive-by-Downloads, sind heimtückische Bedrohungen, die Schwachstellen in Browsern und Anwendungen von Dritten ausnutzen, wenn Benutzer nichts weiter tun, als einfach eine Webseite zu besuchen. Es ist für Internet-Gateway-Sicherheitslösungen besonders wichtig, diese Bedrohungen zu sperren, da sie unsichtbar sind und sogar von vertrauenswürdigen und stark frequentierten Sites übertragen werden können – in der Regel als Folge eines SQL-Injection-Angriffs oder einer Gefährdung durch benutzererstellte Inhalte.

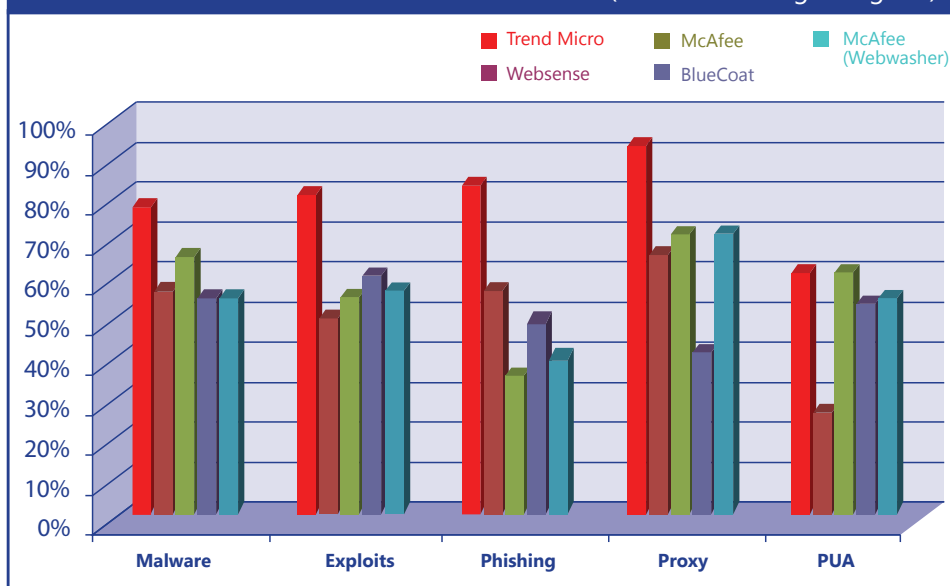
Phishing

Trend Micro sperrte über 80 Prozent der Phishing-URLs. Websense und Blue Coat sperrten jeweils 55 und 47 Prozent und McAfee-Produkte wehrten weniger als 40 Prozent ab. Phishing ist ein bekanntes Problem, und während E-Mail-Sicherheitsprodukte selbst viele der E-Mails entfernen können, bieten Internet-Gateway-Sicherheitsprodukte eine zusätzliche Schutzschicht, indem sie den Link zur gefährlichen Phishing-Site in E-Mails sperren, die nicht anderweitig gefiltert werden, oder auf die Benutzer über einen ungeschützten dritten E-Mail-Provider zugreifen.

Anonymisierende Proxys

Wie auch in den anderen Sicherheitskategorien erzielte Trend Micro das beste Ergebnis: Die Appliance sperrte 91 Prozent der Proxys. Die beiden McAfee-Produkte und Websense belegten die nächsten Plätze, mit einer Sperrrate von über 60 Prozent. Blue Coat nahm mit einer Wirksamkeit von unter 40 Prozent den letzten Platz ein. Anonymisierende Proxys sind selbst nicht gefährlich, können aber Benutzern eine Möglichkeit bieten,

Tabelle 4: Wirksamkeit der Sicherheitsabwehr (nach Bedrohungskategorie)



Nutzungsrichtlinien zu umgehen, um auf anstößige oder potenziell gefährliche Inhalte zuzugreifen. Die von uns in diesem Bericht getesteten Proxy-URLs sind webbasierte Proxys, bei denen Benutzer einen Link in ein Formularfeld eingeben.

Potenziell unerwünschte Anwendungen Trend Micro und McAfee 3000 sperrten 59 Prozent dieser URLs. Auch Blue Coat und das McAfee Webwasher-Produkt wehrten über 50 Prozent ab. Websense sperrte nur 23 Prozent dieser URLs. Nach unserer Definition umfassen „potenziell unerwünschte Anwendungen“ auch Tools, die zwar rechtmäßig verwendet werden können, die aber viele Unternehmen sperren möchten. Dazu zählen bestimmte System-Dienstprogramme, Netzwerksondierungstools und Adware.

Nicht jugendfrei

Wie es für diese Gruppe typisch ist, zeigten alle Produkte eine bessere Leistung als die 90 Prozent Wirksamkeit, die Cascadia Labs erwartet. Die Gruppe „Nicht jugendfrei“ enthält Inhalte, die sexuell eindeutig sind oder sich auf Unterwäsche und Bademoden beziehen und als nicht angemessen für den Arbeitsplatz erachtet werden.

Bandbreitennutzung

Die Gruppe „Bandbreitennutzung“ enthält Downloads, Peer-to-Peer- und Streaming-Media-URLs sowie Torrent-Sites und Video-Inhalte im Internet. SurfControl war der klare Sieger in dieser Kategorie und erzielte 75 Prozent im Gegensatz zum Durchschnitt von 59 Prozent. Auf den nächsten beiden Plätzen kamen IronPort und Trend Micro, die jeweils 62 und 59 Prozent erreichten. Das niedrigste Ergebnis lag bei 47 Prozent. Zu beachten gilt, dass unsere Tests zur Bandbreitennutzung die Fähigkeit von Produkten testen, URLs anhand des Links selbst statt anhand des Protokoll- oder Dateityps zu sperren. Letztere sind ergänzende Ansätze, die Unternehmen auch übernehmen können.

Kommunikation

Das Webwasher-Produkt von McAfee belegte in dieser Gruppe den Spitzenplatz: Es sperrte fast drei Viertel aller URLs. Die restlichen Produkte sperrten zwischen 62 und 69 Prozent. Diese Gruppe umfasst Sites mit sozialen Medien, Blogs sowie private Kommunikation und Foren.

**Sicherheits-URLs stellen
aktuelle Bedrohungen dar
und wurden weder von
den Unternehmen, deren
Produkte wir testeten,
bereitgestellt noch waren sie
ihnen bekannt.**

Haftung

McAfee 3000 erzielte hier mit 63 Prozent das beste Ergebnis, dicht gefolgt von Websense mit 61 Prozent. Andere Produkte sperrten nur knapp über die Hälfte der Inhalte dieser Gruppe, zu denen kriminelle Aktivitäten, Hass und Gewalt, Drogen und anstößige Inhalte zählen. Wie auch bei den Kategorien von „Nicht jugendfrei“ sperren Unternehmen diese Kategorien in der Regel, um eine angenehmere Arbeitsumgebung ohne unangemessene oder rechtlich bedenkliche Inhalte bereitzustellen.

Produktivität und Freizeit

Wie in der Gruppe „Nicht jugendfrei“ gibt es in diesen Kategorien wenig Unterschiede zwischen den Produkten; alle sperrten etwa 90 Prozent der URLs. Diese Kategorien umfassen alles, womit Benutzer möglicherweise Zeit verschwenden, wie z. B. Unterhaltung, Spiele, Nachrichten und Shopping-Sites.

Einstufungen, Datenmaterial und Verfahren

Bewertung und Einstufungen

Unsere Gesamtergebnisse basieren auf der Gewichtung der reinen Sperrergebnisse, die unserer Meinung nach die relativen Prioritäten typischer Enterprise-Kunden darstellen. Cascadia

Labs bewertet diese Gewichtung vierteljährlich neu. In den vergangenen Jahren wurde das Thema Sicherheit immer wichtiger; für diesen Bericht trägt die Gruppe Sicherheit 30 Prozent zu unserer Gesamtbewertung bei. „Nicht jugendfrei“ trägt zu 20 Prozent bei, „Bandbreitennutzung“ zu 15 Prozent, „Haftung“ zu 15 Prozent, „Kommunikation“ zu 10 Prozent sowie „Produktivität und Freizeit“ zu 10 Prozent. Während diese Gewichtung die erhöhte Wichtigkeit von Internet-Gateway-Sicherheit als Komponente einer tiefgreifenden Sicherheitsstrategie widerspiegelt, erkennt sie auch die fortgesetzte Notwendigkeit von Unternehmen an, sichtbare Inhalte, wie z. B. soziale Medien und anstößige Webseiten, zu sperren.

Zu beachten ist, dass diese Einstufungen nicht die Leistung, Skalierbarkeit, Benutzeroberfläche, Funktionen oder Funktionalität berücksichtigen, sondern nur die Wirksamkeit der Abwehr bezüglich unseres Datenmaterials vom Sommer 2009.

Das Datenmaterial

Wir haben unabhängiges Datenmaterial aus URLs erstellt, um den Bedürfnissen des Enterprise-Marktes gerecht zu werden. Besonderes Augenmerk galt hierbei dem Aspekt Sicherheit. Das Datenmaterial enthält 22 einzelne Kategorien, die in sechs Gruppen mit über 1.600.000 URLs aus etwa 100.000 einzelnen Domains organisiert sind. Vorzugsweise wurden hier Domains gewählt, die für englischsprachige Benutzer von Interesse sind.

Unser Datenmaterial umfasst Sicherheitsbedrohungen in fünf verschiedenen Kategorien: Malware, Exploits, Phishing, Proxys und potenziell unerwünschte Anwendungen (PUAs). Wir sammeln und verifizieren in den Tagen unmittelbar vor dem Testen Sicherheits-URLs, um zu gewährleisten, dass sie aktuelle Bedrohungen, einschließlich potenzieller Zero-Day-Angriffe, darstellen, die tatsächlich im Umlauf sind. Diese Zeitnähe ist entscheidend, um die Fähigkeit der

Produkte bezüglich der Bewältigung realistischer, kurzlebiger, webbasierter Bedrohungen zu unterscheiden.

Für diesen Bericht testete Cascadia Labs mit über 2.000 Sicherheits-URLs, darunter etwa 250 Malware-URLs, 1.100 URLs zu Sicherheitslücken, 400 URLs zur Proxy-Umgehung und mehr als 200 URLs zu potenziell unerwünschten Anwendungen.

Die für den Test verwendeten URLs wurden mit Hilfe verschiedener proprietärer Techniken für Entdeckung, Analyse und Verifizierung auf aktiven Websites gesammelt. Sie wurden weder von den Unternehmen, deren Produkte wir testeten, bereitgestellt noch waren sie ihnen bekannt.

Testverfahren

Die Testprodukte wurden als Proxy-Server konfiguriert. Für Websense haben wir die Integration in Microsoft ISA Server verwendet.

Die Produkte konnten alle verfügbaren Remote-Bewertungsfunktionen verwenden und während des Testzeitraums permanent aktualisiert werden.

Da jeder Anbieter eigene Kategorien zur URL-Klassifizierung nutzt, bilden wir unsere Kategorien auf die vom Anbieter ausgewählten Kategorien ab, um sicherzustellen, dass wir für jedes Produkt vergleichbare Sperrkonfigurationen verwenden. Für unsere Testzwecke haben wir jedes Produkt so konfiguriert, dass eine ganze Gruppe (die per Definition ähnliche Kategorien enthält) gesperrt wird. So werden unserer Sperrergebnisse nicht durch geringe Unterschiede beeinflusst, die Anbieter bei der Wahl ihrer Kategorien möglicherweise vornehmen.

Da Web Reputation in erster Linie auf Sicherheits-URLs abzielt, wurde es nur für Tests dieser Gruppe aktiviert.

Um die entscheidenden URL-Filterfunktionen der einzelnen Produkte zu isolieren, hat Cascadia Labs auf keinem der Produkte Protokollfilter oder Malware-Scanner aktiviert. Protokollfilter können eine wirksame zusätzliche Maßnahme beim Sperren von Instant Messaging oder anderen unerwünschten Services sein. Sie eignen sich jedoch angesichts der

Bedeutung des Internets natürlich nicht für HTTP selbst (und die von uns getesteten URLs). Auch das Durchsuchen von Binärdateien am Netzwerkrand bietet eine weitere Schutzschicht, kann aber für Benutzer zu zusätzlichen Verzögerungen führen. Für den vorliegenden Bericht wurde diese Funktion nicht in die Tests miteinbezogen.

Um das Testen von Echtzeit- und Remote-Bewertungsfunktionen zu aktivieren, ohne die laufende Integrität unseres URL-Datenmaterials zu gefährden, verwendete Cascadia Labs eine Sammlung von 1.000 zufällig ausgewählten URLs in jeder Kategorie (und 2.000 für alle Sicherheitskategorien). Wir können daher Sperrergebnisse in den meisten Kategorien mit einer Zuverlässigkeitsabweichung von plus oder minus 3 Prozent angeben (bei einem Zuverlässigkeitsmaß von 95 Prozent). Die URLs werden, mit Ausnahme von URLs für häufig frequentierte Sites, nur einmal verwendet, um keinem Produkt einen Vorteil bei nachfolgenden Tests zu verschaffen. ▲



Independent evaluations of technology products

Ansprechpartner: info@cascadialabs.com
www.cascadialabs.com



Dieser unabhängige Vergleichstest wurde von Cascadia Labs im Sommer 2009 durchgeführt und von Trend Micro gesponsert. Ziel von Cascadia Labs ist die Bereitstellung einer objektiven, unparteiischen Analyse jedes Produkts, die auf Tests vor Ort im eigenen Sicherheitslabor basiert.