Eine Sonderveröffentlichung der Heise Zeitschriften Verlag GmbH & Co. KG

iX extra
Security

Firewalls, IDS/IPS und Virenscanner im Zeitalter von Cloud und Web 2.0

Veranstaltungen

5. – 7. März 2013, Hannover
CeBIT
www.cebit.de

22. – 23. März 2013, Heidelberg
iX-Workshop: Metasploit – Das Penetration-Testing-Framework
www.ix-konferenz.de

23. – 25. April 2013, London
Infosecurity Europe
www.infosec.co.uk

14. – 16. Mai 2013, Bonn
BSI: 13. Deutscher IT-Sicherheitskongress
www.bsi.de

iX extra Security zum Nachschlagen:
www.heise.de/ix/extra/security.shtml

Verknüpfte Systeme

Cloud- und Web-2.0-Security: Klassische Mittel mit Korrelation

Für die Sicherheit von Web-2.0- und Cloud-Anwendungen benötigen Unternehmen nicht unbedingt neuartige Techniken. Bekannte Systeme wie Firewall, Virenschutz, Intrusion Detection und Intrusion Prevention behalten ihre Bedeutung. Sie müssen allerdings in einem übergeordneten Ansatz aufgehen.

Der Trend zu Cloud-Services und Web 2.0 wälze die ganze klassische IT-Organisation um, heißt es in vielen Fachbeiträgen zu diesen Themen, und dies beträfe auch die Informationssicherheit. Zugleich aber preisen die Anbieter heute verfügbarer Sicherheitstechnik ihre Produkte immer wieder als für Cloud-Umgebungen geeignet und notwendig an und mahnen die Anwender, für den sicheren Schritt ins neue Zeitalter fehle es nur an konsequenter Implementierung. Dabei tun sich besonders Anbieter hervor, die ein umfangreiches Portfolio an unterschiedlichen Sicherheitsprodukten bieten oder die Lösungen wie Next Generation Firewalls und Application-Delivery-Produkte für die Cloud-Security miteinander kombinieren.

Bietet aber tatsächlich das bekannte Arsenal an Sicherheitslösungen genau diejenigen Funktionen, die es erlauben, Cloud-Anwendungen und Web 2.0 sicherheitstechnisch zu beherrschen? Die Antwort erfordert zunächst einen eingehenden, aber nüchternen Blick auf die angeblich so revolutionären Phänomene.

Vom „Web 2.0“ redet die Fachwelt schon seit Jahren, der Cloud-Trend ist ein wenig jünger. Web 2.0 bezeichnet den Schritt zur interaktiven Internetnutzung. Dem Anwender, der Internet-Angebote zuvor fast ausschließlich konsumierte, stehen nun Blogs, soziale Medien wie Facebook, Xing, Twitter, Fototauschbörsen und ähnliche Anwendungen zur Verfügung.

Bedeutsam für die Sicherheit ist zum Beispiel, dass die Benutzer sowohl privat wie auch als Unternehmensmitarbeiter Internet-Plattformen mit eigenen Inhalten füllen. Für die Sicherheitsabteilungen der Unternehmen hat dies zur Folge, dass sie den gleichzeitigen privaten und Unternehmenszugriff auf Webressourcen am Arbeitsplatz zu regeln haben. Außerdem verlangt Web 2.0 von den Sicherheitsverantwortlichen, stärker auf den Informationsfluss aus den Organisationen hinaus zu achten, während zuvor der Download unerwünschten Materials und die – natürlich bleibende – Malware-Gefahr im Mittelpunkt des Interesses standen.

Wer von der „Cloud“ spricht, meint die Nutzung von IT-Leistungen über Webverbindungen im Intra- oder Internet. Als Cloud-Dienste sind neben

„dummen“ Services wie denen von File- oder Storage-Servern längst auch komplexe Angebote wie branchenspezifische Berechnungs- und Buchungssysteme verfügbar. „Öffentliche“ Cloud-Dienste („Public Cloud“) lassen sich dabei von Anwendern unterschiedlichster Herkunft nach einfacher, oft sicherheitstechnisch allzu simpler Anmeldung nutzen, „private“ Cloud-Dienste stellt ein interner oder externer Anbieter einer Organisation exklusiv zur Verfügung. Darüber hinaus gibt es „hybride“ Mischformen und Angebote, bei denen Cloud-Services ihrerseits weitere Angebote aus dem Web nutzen.

Faktisch sind Web 2.0 und Cloud zwei Seiten einer Medaille. Wenn externe Mitarbeiter eines Unternehmens beispielsweise ihre Leistungen von immer neuen Einsatzorten aus mithilfe einer für sie programmierten Webanwendung erbringen und über die gleiche Plattform die Unterstützung durch Kollegen in einzelnen Projekten organisieren, arbeiten sie aus ihrer Sicht mit einer Cloud-Anwendung, die ihnen ihr Unternehmen zur Verfügung stellt und die Web-2.0-Funktionen aufweist.

Social-Media-Plattformen wiederum sind nichts anderes als öffentliche Cloud-Dienste zur Kontaktpflege und Kommunikation, die immer häufiger auch Funktionen für die persönliche Zusammenarbeit einerseits und die Kommunikation zwischen Organisationen und ihren Kunden, Partnern und Mitarbeitern andererseits bieten. Dies alles hat sich inzwischen als so nützlich erwiesen, dass große Unternehmen bereits die Ergänzung klassischer E-Mail-Systeme durch interne „soziale Webs“ erproben.

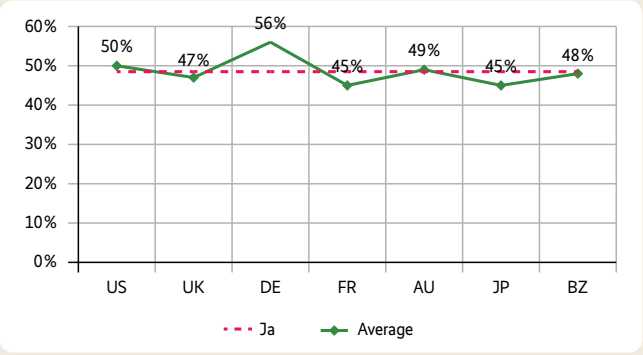
Wer, wie, was

Die unterschiedlichen Security-Aspekte der beschriebenen Konstrukte lassen sich am besten nach dem Muster: „Wer macht was zu welchem Zweck mit welchem Anbieter und mit wessen Daten“ aufschlüsseln. Unternehmen haben es dabei vor allem mit folgenden Interaktionsformen zu tun:

– Anwender und Applikationen im Unternehmen übertragen Informationen zum Verarbeiten oder Speichern auf externe Applikationen oder Server, die ihnen als branchenspezifische Systeme von spezialisierten Dienstleistern übers Internet zur Verfügung gestellt werden. Die externen Dienste können dabei als öffentliche oder als private Dienste konzipiert sein.

– Anwender im Unternehmen nutzen öffentliche, für die Allgemeinheit entwickelte Webapplikationen für Unternehmenszwecke – vom Reisebuchungssystem über eBay als Beschaffungsportal bis hin zu Online-Storage-Angeboten. Das kann die entsprechende Organisation so vorsehen, meist aber entscheiden sich einzelne Nutzer oder Abteilungen aus eigenem Antrieb dafür, weil sie mit diesen Werkzeugen effizienter arbeiten können als mit den Angeboten der Unternehmens-IT. Für die Organisationen entstehen hier neue Risiken, da sich der Schutz der Informationen in diesem Fall nicht nur ihrem direkten Einfluss entzieht, sondern möglicherweise in die Obhut eines Providers übergeht. Außerdem ist es schwierig, zu überwachen, ob Mitarbeiter nur dazu freigegebene Informationen an externe Stellen übertragen.

– Mitarbeiter nutzen vom Arbeitsplatz aus Cloud-Dienste, die in variablen Anteilen sowohl ihren privaten Interessen als auch denen ihres Arbeitgebers zugutekommen. Auch hier liegen Risiken darin, dass Mitarbeiter interne Informationen oder Informationen über ihr Unternehmen unkontrolliert Fremden zugänglich machen.



„Speichert Ihre Organisation bereits vertrauliche Daten in der Cloud?“ In Deutschland sagen besonders viele Unternehmen „Ja“ (Abb. 1).

Quelle: Ponemon-Studie „Encryption in the Cloud“, Juli 2012

Alles über Port 80

Allen Nutzungsformen gemeinsam ist, dass sie technisch-formal fast ausschließlich als legitime Webzugriffe und Webtransaktionen stattfinden. Vor allem bei Interaktionen zwischen internen und externen Applikationen können komplexere Schnittstellen wie solche für den XML-Datenaustausch oder getunnelte Protokolle hinzukommen – aber auch dies funktioniert auf der Basis des normalen Internet-Verkehrs über Port 80. Damit liegen die „neuen“ Risiken außerhalb des Regelungsbereichs klassischer Firewalls.

Ob nämlich ein Zugriff auf eine Webanwendung legitim ist oder nicht, entscheidet sich nicht anhand des Ports, über den er stattfindet, sondern anhand der Person, die sie durchführt, anhand des Inhalts, der transferiert wird, und des Übertragungsziels – um all das zu überwachen, sind die Fähigkeiten von Identitäts- und Berechtigungsmanagement, Content-Filtern und Next-Generation-Firewalls gefragt. Auch Cloud-Umgebungen können aber jederzeit auf längst vertrauten Wegen angegriffen werden. Cloud und Web 2.0 machen deshalb keine jener Sicherheitslösungen überflüssig, die schon in rein LAN-basierten IT-Umgebungen mit internen Servern und Applikationen existierten, auch nicht die Firewalls herkömmlicher Technik.

Sicherheitsspezialisten weisen immer wieder darauf hin, dass die Rechenzentren der Dienstleistungsanbieter ein besonders attraktives Ziel für Datendiebe darstellen. Bei sogenannten kombinierten Angriffen bedienen sich die Angreifer einer ganzen Reihe technischer und nicht technischer Vorgehensweisen, um an vertrauliche Informationen zu gelangen, wobei die Einzelschritte typischerweise kaum auffallen und erst bei einer Korrelation von Security-Events und -Incidents sichtbar werden. Ziel der Angriffe ist in vielen Fällen der Diebstahl einer Identität, die den Zugriff auf Cloud-Anwendungen ermöglicht, und der anschließende Transfer von Daten oder eine Sabotage in Form einer Denial-of-Service-Attacke. Ideal für einen Angreifer ist es, wenn er entweder in die Rolle eines berechtigten Cloud-Anwenders oder gar in die eines Cloud-Administrators schlüpfen kann.

Angriffe auf die Web-Frontends beispielsweise mit Cross-Site Scripting und Spionage mittels untergeschobener trojanischer Pferde, Seitenkanal-Attacken auf die verwendeten Verschlüsselungssysteme und Denial-of-Service-Angriffe sowohl auf einzelne Systeme beim Anbieter als auch auf diejenigen beim Kunden gehören zusammen mit Social-Engineering-Taktiken zum Angreifer-Repertoire.

Damit wird unmittelbar deutlich, welche zentrale Rolle die klassischen Sicherheitssysteme in Cloud- und Web-2.0-Szenarien noch spielen und wie sie eingesetzt werden müssen, um wirksam zu sein. Für die gerade geschilderten Angriffsvektoren auf die Web-Frontends etwa stehen Web Application Firewalls (WAF) zur Verfügung, die unzulässige Eingaben abfangen.

Malware-Schutz bleibt ebenfalls wichtig, und zwar auf allen Ebenen – auf den Hosts der

25YEARS
INNOVATIVE
TOP-RATED
ANTIVIRUS
PROTECTION

ESET ENDPOINT LÖSUNGEN

IT-PROFIS VERTRAUEN AUF ESET.

Erstklassiger Schutz für Ihre Endpoints mit der mehrfach ausgezeichneten Erkennungstechnologie, cloudbasiertem Scan, Webkontrolle und Remote Administration.

ERFAHREN SIE MEHR!

ESET Business Solutions

auf www.eset.de

eset

www.eset.de

Webapplikationen, an den Gateways der Anbieter und Kunden sowie gegebenenfalls auf virtuellen Maschinen und deren Hosts beim Provider. Eine besonders wichtige Rolle spielen die Endgeräte der Nutzer, an denen sich Zugangsinformationen und Kennwörter abfangen lassen und wo die Nutzdaten entschlüsselt werden müssen.

Gut umgehen können sollten diese Produkte auch mit auf Webseiten platzierter Malware, denn die Verteiler trojanischer Pferde verwenden zunehmend ihre Energie darauf, ihre Schadsoftware über grundsätzlich gut beleumundete Social-Media-Plattformen zum Anwender zu bringen. In den sozialen Netzen nämlich können sie die Zielgruppen besser eingrenzen und über die Mechanismen der Kontaktpflege neue Social-Engineering-Techniken nutzen.

Auf Netzwerkebene leisten die bekannten Intrusion-Detection- und -Prevention-Systeme gute Dienste bei der Erkennung übergreifender Angriffsmuster. Wie allerdings soll ein solches System Muster erkennen, deren einzelne Aktionen teils beim Cloud-Kunden, teils beim Anbieter ablaufen?

SIEM korreliert alle Daten

Die verteilten Strukturen, die durch Cloud-Nutzung entstehen, und die Taktik der Angreifer, mittels vieler unauffälliger kleiner Schritte vorzugehen, machen es schwierig, komplexe Angriffe auf Unternehmensinformationen überhaupt zu erkennen. Versucht ein Mitarbeiter des Cloud-Anbieters per Fernzugriff aus dem Gebäude des Kunden in Hamburg heraus Einstellungen vorzunehmen, obwohl er ähnliche Maßnahmen genau fünf Minuten früher noch im Münchner Rechenzentrum des Anbieters in Angriff genommen hat? Ergibt sich aus den Meldungen der Anti-Viren-Software und der IDS-Systeme sowohl im Netz des Kunden als auch in dem des Anbieters einer privaten Cloud, das in beiden Systemen nahezu zeitgleich eine potenzielle Zero-Day-Malware aktiv wird? Legt ein privilegierter Benutzer plötzlich einen Administrator-Account an, von dem aus kurz darauf Sicherheitseinstellungen entgegen den Compliance-Vorgaben eines bestimmten Mandanten verändert werden?

Solche Auffälligkeiten entdeckt kein Einzelsystem beim Kunden oder beim Cloud-Service allein, sondern nur eine Software für das sogenannte Security Information Event Management (SIEM) der neuesten Generation, die aus Sicht der IT-Abteilung des Kunden arbeitet und in Echtzeit die Log-Dateien aller Sicherheitssysteme auswertet, die für den Zugriff auf die internen und die ausgelagerten Ressourcen des Kunden zuständig sind. Die klassischen Sicherheitsprodukte haben in dieser Konstellation die Aufgabe, Teilschritte eines groß angelegten Angriffs oder klassische kleine Bedrohungen selbstständig abzuwehren, zugleich aber als Sensoren für eine übergeordnete Sicherheitsinstanz zu fungieren.

Sicherheitsfunktionen, die in Cloud- und Web-2.0-Umgebungen eine (noch) größere Bedeutung haben als in klassischen Netz- und Anwendungskonstellationen, sind Verschlüsselung und, wie bereits angedeutet, IAM (Identitäts- und Rechtemanagement).

Bei der Verschlüsselung ist nicht nur die notwendige Sicherung des Übertragungswegs zwischen der IT des Kunden und der des Anbieters von Bedeutung, sondern auch der Schutz der beim Anbieter gespeicherten Daten. Wo immer dies funktional möglich ist, sollten Informationen auf den fremden Servern so abgelegt sein, dass die Schlüssel allein in der Gewalt des Kunden verbleiben, der ja schließlich die Verantwortung für seine Datenbestände behält.

Identitätsmanagement- und Berechtigungskonzepte sollten durchgängig implementiert sein und den Zugriff auf die Cloud-Dienste in existierende Rollen- und Gruppenkonzepte einbeziehen. Dabei ist nicht nur auf die menschlichen Benutzer zu achten: Bei der Nutzung von Cloud-Diensten interagieren häufig auch Applikationen, die somit ebenfalls einbezogen werden müssen.

Einige der mit Cloud-Nutzung verbundenen Risiken lassen sich mit Technik auf dem direkten Wege überhaupt nicht beherrschen. Den Sicherheitslevel eines Anbieters beispielsweise kann ein Kunde nur anhand der Einhaltung von Standards für das Sicherheitsmanagement wie BSI Grundschutz oder ISO 27001 einschätzen und darüber hinaus vertraglich einfordern. In einigen Konstellationen ist dies aus Compliance-Gründen notwendig.

Idealerweise sollten die Informationen über Compliance-Vorgaben auch den oben erwähnten SIEM-Systemen zugänglich sein und somit für die Korrelation mit den Echtzeitmeldungen der Sicherheitsprodukte zur Verfügung stehen – solch eine Lösung könnte dann beispielsweise sofort Alarm schlagen, wenn ein Mitarbeiter Informationen in einem Cloud-Storage-System ablegen will, das in einem Land angesiedelt ist, in das genau diese Informationen aus Datenschutzgründen nicht übertragen werden dürfen.

Wie immer: Der Faktor Mensch

Bei der Nutzung von Cloud-Diensten treten eine Reihe menschlicher Faktoren als Risiken in Erscheinung, die in klassischen Umgebungen keine oder eine geringere Bedeutung haben. Eines dieser Risiken, auf das bereits kurz hingewiesen wurde, resultiert aus der Attraktivität und Benutzerfreundlichkeit mancher öffentlicher Webangebote: Ist es mit unternehmensinternen Mitteln schwierig, effizient Informationen auszutauschen oder bestimmte Kommunikationsverbindungen aufzubauen, greifen Mitarbeiter oder Unternehmensabteilungen gern in eigener Regie zu Angeboten wie Dropbox für den Dateiaustausch, Skype für die Fernkommunikation oder frei zugängliche Konferenzsysteme. Anbieter von Sicherheits- und Kommunikationsprodukten, die zum Bespiel mit UTM- oder Next-Generation-Firewall-Systemen granulare Sperren auf der Protokollebene oder mittels Paketanalyse (Deep Packet Inspection) einrichten können, haben dies inzwischen erkannt und bieten entsprechende Blockiermöglichkeiten an.

Das Verbieten oder technische Sperren ohne gleichzeitige Analyse der Gründe für die Flucht der Mitarbeiter zu derartigen Diensten schürt aber nicht nur Unmut, sondern weckt auch die Kreativität der Anwender bei der Suche nach neuen Auswegen. Das Sperren unsicherer Dienste ist deshalb nur sinnvoll und Erfolg versprechend, wenn das Unternehmen seinen Angestellten die Gründe dafür im Rahmen von Awareness-Maßnahmen nahebringt und ihnen sichere Alternativen anbietet.

Die administrativen Mitarbeiter beim Cloud-Anbieter können ebenfalls zum Risiko werden. Angreifer könnten versuchen, sich als Angestellte einzuschleichen oder sich Zugang zu verschaffen, indem sie die Mitarbeiter durch Social-Engineering-Tricks manipulieren.

Für potenzielle Kunden bedeutet dies, bei der Auswahl eines Cloud-Dienstleisters möglichst auch einen Blick auf dessen Standards bei der Personalauswahl und sein Schulungsprogramm zu werfen und zu ermitteln, welche genauen Rechte die IT-Administratoren beim Zugriff auf die verarbeiteten Daten haben. Gibt es ein professionell umgesetztes Berechtigungskonzept und sind die Zugriffs-Logs dem SIEM-System des Kunden zugänglich, sofern sie seinen Informationsbestand betreffen? Viele Dienstleistungen sind vollständig umsetzbar, ohne „privilegierten“ Personen beim Dienstleister jemals Zugang zu unverschlüsselten Nutzdaten zu gewähren.

(ur/sf)

Bettina Weßelmann ist freie Journalistin und Beraterin für Unternehmenskommunikation.

Bei c’t sind Sie der Souverän.

Wir liefern Ihnen neutrales Wissen, Sie treffen Ihre Wahl. In eigenen Testlabors untersuchen wir, was neue IT-Hard- und Software wirklich kann. Als c’t-Leser profitieren Sie von der Erfahrung der über achtzig neutralen Spezialisten in Deutschlands größter IT-Redaktion, die 14-täglich aus der Flut der Informationen genau das Wichtige für Sie auswählt. Gründlich recherchiert, unabhängig analysiert, verständlich geschrieben. Mit dem Know-how aus Ihrer c’t haben Sie immer den Überblick und können stets zu Ihrem Vorteil handeln. Ganz souverän.

Das sind Ihre Vorteile:
- Bequeme Lieferung frei Haus
- 34% Rabatt für Sie
- Ihr Geschenk: das 4-teilige Gepäck-Set mit 3 Universal-Taschen plus Trolley

↳ Weiterlesen, wo andere aufhören.

Ja, ich will c’t lesen und dann souverän entscheiden. Senden Sie mir 6 Mal das aktuelle Heft mit 35 % Ersparnis für nur € 15,20 und das praktische 4-teilige Reisegepäck-Set als exklusives Geschenk.

Vorname, Name

PLZ, Ort

Straße, Haus-Nr.

Telefon + E-Mail (für evtl. Rückfragen) CTP12101

Nach dem Test kann ich c’t für € 3,45 statt € 3,90 pro Heft weiter lesen. Andernfalls sende ich Ihnen nach Erhalt des vierten Hefts eine Nachricht.
Ich bin einverstanden, dass der Heise Zeitschriften Verlag mich aktuell über seine Angebote und Produkte informiert. Diese Infos wünsche ich per: ☐ E-Mail, ☐ Telefon. Eine Weitergabe meiner Daten an Dritte erfolgt nicht. Meine Einwilligung kann ich jederzeit widerrufen; auf Wunsch auch nur für einzelne Kommunikationsmittel. Dazu genügt eine formlose Nachricht an: Heise Zeitschriften Verlag GmbH & Co. KG, Vertrieb & Marketing, Karl-Wiechert-Allee 10, 30625 Hannover, oder datenservice@heise.de (Datenschutzhinweis: www.heise.de/privacy).

Hier ordern: ctvorteil.de

Fax: 040 3007 85 3525
Tel.-Hotline: 040 3007 3525

Neue Schleusen

Next Generation Firewalls erkennen Applikationen

Firewalls zählen neben Virenschutzprogrammen zu den meistverkauften Security-Produkten. Die Next Generation Firewalls kombinieren klassische Firewalls mit IPS-Funktionen, Application-, Content- und Benutzer-Awareness und ermöglichen granulare Regelwerke.

Firewalls der ersten Generation haben nach Herstelleraussagen ausgedient. Nur Modelle der nächsten Generation sollen vor den neuen Bedrohungen schützen. Unterschiedliche technische Ansätze verfolgen dasselbe Ziel: den Kontrollverlust am Gateway durch Application Awareness wieder wettzumachen. Eine Firewall soll auf Netzwerkebene Richtlinien durchsetzen und hat die Aufgabe, anhand von Regeln zu entscheiden, welcher Datenverkehr von einem Netz in ein anderes gelangen darf. Als Entscheidungskriterien stehen den Paketfilter-Firewalls der ersten Generation IP-Adresse(n) der Quelle und des Ziels, Quell- und Ziel-Port(s) nebst Protokoll (TCP, UDP, ICMP, …) sowie bei manchen Modellen auch die betroffene Netzwerkschnittstelle zur Verfügung. Durch Stateful Packet Inspection dürfen Antwortpakete ohne zusätzliche Regeln die Firewall passieren.

Grundsätzlich wird das Regelwerk einer Firewall nach dem Positivmodell konfiguriert. Das bedeutet, dass der Administrator für den erwünschten Datenverkehr entsprechende Regeln erzeugt, alle anderen Verbindungen blockiert die Firewall. Möchte ein Unternehmen beispielsweise den Zugang zu Webservern im Internet über einen Proxy-Server via Port 8080 erlauben, wird dieser als Ziel-Port für den Proxy-Server und für erlaubte Quelladressen geöffnet. Andere Ports des Servers bleiben aus anderen Netzen unerreichbar, sofern sie nicht explizit durch eine Regel freigeschaltet sind.

Im Laufe der Jahre kamen immer mehr Funktionen hinzu: Firewall-Systeme beherrschen Network Address Port Translation, schützen vor IP-Spoofing in internen Netzen und parieren rudimentär auch einzelne Angriffstypen wie sogenannte LAND-Attacken (Local Area Network Denial), eine Sonderform des Denial-of-Service-Angriffs. Sie können als VPN-Gateway für Remote Access oder Site-to-Site-Verbindungen fungieren und enthalten grundlegende Funktionen für Routing und Bandbreitenmanagement.

Die „Von allem ein bisschen“-Könner

Je nach Zielgruppe beherrschen Firewalls die gängigen Hochverfügbarkeitsmodi und können auch virtuell ihre Funktion ausüben. Andere Systeme bringen weitergehende Intrusion-Detection- oder -Prevention-Funktionen (IDS/IPS) mit, die jedoch nicht mit modernen und dedizierten IDS/IPS mithalten können. Einige bieten SSL-VPN für Remote Access, virtuelle Router, WAN Acceleration und andere spezielle Features.

Zurück zum Beispiel mit der Firewall-Regel für den Proxy-Server: Die Richtlinie greift, solange sich alle legitimen Benutzer an sie halten und keine unerwünschten Teilnehmer oder Softwarekomponenten im Spiel sind. Die klassische Firewall versagt hier jedoch bei der Prüfung von getunnelten Datenpaketen und bei SSL-verschlüsselten Verbindungen. Desktop-Sharing-Anwendungen wie Teamviewer verbinden sich problemlos über Port 80 und bauen damit eine Brücke in nicht vertrauenswürdige Netze.

Instant-Messaging-Programme und andere Software werden mit dem Merkmal „Firewall-friendly“ beworben, und das heißt, die typischerweise für den Internetzugang geöffneten Ports 80 und 443 beziehungsweise der Port des dazwischenstehenden Proxy-Servers lassen sich für die Kommunikation nutzen. Für Port 80 werden die Pakete dazu in HTTP-Pakete umverpackt, und bei Port 443 prüfen klassische Firewalls aufgrund der zu erwartenden SSL-Verschlüsselung gar nicht erst, welcher Art Protokoll die passierenden Datenpakete angehören.

Ist ein Durchkommen auf diesen Ports nicht möglich, versuchen insbesondere Instant-Messaging-Programme mittels Port Hopping ein Tor zur Außenwelt zu finden. Ohne Inhaltsfilterung lassen sich auch auf privaten Webservern liegende Proxy-Skripts dazu nutzen, Webfilter wirksam zu umgehen.

Die Möglichkeiten, trotz Firewall Datenbestände selbst größeren Umfangs aus dem gesicherten Netz zu schaffen, ergeben sich durch webbasierte Upload-Skripts oder komfortabel über Cloud-Speicherdienste, per WebDAV auf Online-Festplatten, per E-Mail-Anhang, dank Web-2.0-Technologie auch als Anhang von Nachrichten auf Social-Media-Plattformen und über die File-Sharing-Funktionen der Instant-Messaging-Programme.

Neben dem möglichen Missbrauch des Internetzugangs oder Datenklau durch interne Mitarbeiter haben beim Einsatz klassischer Firewall-Technik gezielte externe Angriffe deutlich höhere Erfolgsquoten. Gut vorbereitete, gezielte Phishing-Attacken ermöglichen durch klassische Firewalls hindurch die Etablierung eines permanenten Brückenkopfs in Unternehmensnetze, von dem aus der Angreifer weiter vordringen und sich auch über lange Zeit im Unternehmensnetz aufhalten kann (Stichwort Advanced Persistent Threats). Selbst breit gestreute Trojaner, die sich Benutzer durch Drive-by-Downloads sogar von harmlosen Webseiten wie wetter.com oder in sozialen Netzwerken durch präparierte Onlinewerbung einfangen können, haben bei der alten Firewall-Generation leichtes Spiel durchzukommen, Daten herauszuschleusen oder sich mit einem Command-and-Control-Server zu verbinden.

Die Schwächen der Firewalls auf Layer 7 sind schon lange bekannt. Daher haben die meisten Firewall-Hersteller bereits seit vielen Jahren die Technik eingeführt, in die Datenpakete hineinzuschauen und das Einhalten von Protokollen zu erzwingen. So lässt sich beispielsweise bei HTTP PUT und GET explizit filtern oder bei SSH die Nutzung auf Version 2 einschränken. Die Art und Weise dieser sogenannten Deep Packet Inspection (DPI) ist jedoch für den Erfolg entscheidend. Werden nur Header oder das erste Paket geprüft, ist der Rechenaufwand geringer, jedoch sind unerlaubte Inhalte weiter hinten im Payload nicht auszumachen. Auch die Nutzung von anderen als den vorgesehenen Standard-Ports macht so manche Firewall blind in Bezug auf die Inhalte. Nicht zuletzt dadurch kamen vor einigen Jahren die Unified-Threat-Management-Systeme (UTM) auf den Markt. Diese sind neben der Firewall mit Anti-Virus/Malware-Modulen, IPS, URL-Filtern und meist noch mit Anti-Spam-Modulen ausgestattet.

Der größte Nachteil der UTM-Systeme ist die fehlende Verzahnung der einzelnen Module. Teile davon sind nicht selten von anderen Herstellern als OEM-Ware zugekauft. Die Pakete durchlaufen in der Regel die Module sequenziell. Sind alle Module aktiviert, brechen die Durchsatzraten gegenüber den im Datenblatt angegebenen Werten dramatisch ein.

Next Generation Firewalls (NGFW) sollen es nun besser

machen. Sie sind „Application Aware“, das heißt, sie erkennen Applikationen unabhängig von Ports und durchleuchten nicht nur die ersten, sondern fortlaufend Datenpakete mit Deep Packet Inspection auf dem ganzen Protokoll-Stack. Die Firewall versieht Applikationen mit eindeutigen ID-Nummern und fasst sie zu Applikationsklassen zusammen. Innerhalb der Applikations-Datenströme werden die Inhalte unterschieden (Content Awareness).

Ganz neu ist die Idee des applikationsbasierten Ansatzes nicht, gab es doch bereits Mitte der 90er-Jahre Proxy- beziehungsweise Application-Layer-Firewalls, die Verbindungen nicht wie Paketfilter weiterleiten, sondern das Applikationsprotokoll verstehen und getrennte Verbindungen vom Quell- und zum Zielsystem halten. Sie unterstützten jedoch nur wenige populäre Protokolle.

Doch NGFW können mehr: Sie verstehen über tausend unterschiedliche Applikationen. Überdies können sie innerhalb von HTTP zwischen verschiedenen Applikationen wie Salesforce oder Facebook unterscheiden. Hinter vielen Verbindungen stehen nicht nur Maschinen, sondern auch Benutzer. Es braucht folglich neben Application und Content Awareness noch User Awareness. Durch Schnittstellen zu Verzeichnisdiensten wie LDAP oder das AD sind benutzer- und gruppenbezogene Firewall-Regeln möglich.

Bei der zunehmenden Dominanz des Hyper Text Transfer Protocol werden immer mehr Anwendungen per SSL verschlüsselt. Firewalls der neuen Generation brechen diese analog zur Technik der Man-in-the-Middle-Attacke auf („SSL-Terminierung“) und ermöglichen damit die Analyse der Inhalte. Auch die Inhalte von SSH-Verbindungen sollen nicht mehr unsichtbar bleiben. Damit können die Systeme beispielsweise Shell-Verbindungen erlauben, Dateitransfers per *scp* oder das Tunneln von Protokollen wie X11 jedoch unterbinden.

Zur Vermeidung von Performance-Problemen gehen einige Hersteller den Weg, die Pakete anders als bei UTM nur noch durch einen Prozess zu prüfen (Single-Pass-Verfahren). Gleichzeitig wird die Prüfung mit hardwaregestützten FPGAs (Field Programmable Gateway Array) optimiert, und die Parallelisierung der Datenströme reduziert die Latenzzeit durch die Prüfung auf ein Minimum.

Als integrierte Netzwerksicherheitsplattform ergänzen Intrusion-Prevention-Funktionen das Positivmodell der NGFW durch Erkennung von Angriffsmustern. Sie können damit selbst Angriffe verhindern, die sich aus Sicht der Firewall-Engine applikationskonform verhalten. Dabei sollten die Funktionen so integriert sein, dass zum Beispiel bei Erkennung von Angriffsmustern auch dynamische IP-Adresssperren im Regelwerk bei den angreifenden Systemen erfolgen können. Überdies sollte die Firewall in der Lage sein, verschleierte Angriffe in Form von sogenannten Advanced Evasion Techniques (AETs) zu erkennen und zu verhindern. NGFWs brauchen sich mit IPS-Funktionen kaum noch hinter dedizierten IPS-Systemen zu verstecken.

Dedizierte Next Generation IPS haben zwar Content Awareness und die Full Stack Visibility mit den NGFW gemein und beherrschen auch SSL-Entschlüsselung, doch fehlen die Firewall-Funktionen und es bleibt beim Negativmodell. Mit einem Merkmal jedoch punkten IPS-Systeme der neuen Generation gegenüber den NGFW: Sie erlauben mit Context Awareness die Einbeziehung von weiteren Datenquellen wie dem Patch-Stand von zu schützenden Systemen, Informationen über Schwachstellen aus Security-Scans, Reputationsdatenbanken, Black- und Whitelisting und anderen Quellen.

Einige NGFW ergänzen die Content-Filter-Funktionen mit URL-Filtern und betreten damit das Terrain der Secure Web Gateways (SWG) oder auch klassischer Web-Proxies, etwa Squid. Abhängig von den Anforderungen können im Perimeter dadurch Firewalls und SWGs konsolidiert werden. Typische Unterschiede bestehen in der Qualität und Tiefe der statischen sowie der Echtzeit-Kategorisierung und der Erkennungsrate von Malware.

Weitere konvergente Tendenzen sind in Richtung Application Delivery Controller (ADCs) beziehungsweise Web Application Firewalls zu beobachten, beherrschen doch NGFW dank SSL-Entschlüsselung, Deep Packet Inspection und IPS deren wesentliche Funktionsmerkmale.

Die Policy einer NGFW droht schon aufgrund der vielen neuen Filtermerkmale komplexer zu werden. Hier müssen die Hersteller in den Managementoberflächen durch echte Integration zeigen, wie sie diese Komplexität auf ein Minimum reduzieren können. Immerhin lassen sich jetzt Verbindungen mit weiten Port-Bereichen und/oder dynamischen Ports wie die für MS Exchange Server, Active Directory Server oder dem Legato Networker vergleichsweise einfach konfigurieren.

Auch wenn die Performance dank Hardwarebeschleunigung und neuer technischer Ansätze im Vergleich zu UTMs besser ist, gehen Inhaltsanalyse und Entschlüsselung zulasten des Datendurchsatzes. Die auf den Datenblättern der Hersteller angegebenen Werte sind in der Realität nicht zu erreichen. Die SSL-Entschlüsselung ist dabei häufig die größte Bremse. Zudem machen sich die verwendeten Algorithmen deutlich in der Performance bemerkbar.

Grenzen von Next Generation Firewalls

Wird statt mit dem schwachen RC4-MD5 mit dem starken AES-256/SHA gearbeitet, gibt die Durchsatzrate nochmals spürbar nach. Hier empfiehlt es sich, bestimmte vertrauenswürdige SSL-Verbindungen von der Entschlüsselung auszunehmen. Je nach Hersteller drücken auch AV-/Malware-Inspection und die IPS-Funktion die Performance. Einige Firewalls schalten implizit die AV-/Malware-Inspection aktiv, wenn SSL-Decryption ins Spiel kommt. Die zunehmende Einführung von IPv6 dürfte die Durchsatzraten bei softwarebasierten Engines noch weiter strapazieren.

ANBIETER VON NEXT GENERATION FIREWALLS & CO.

Hersteller	Produkt	Website
Adyton Systems	Network Protector	www.adytonsystems.com/de
Barracuda	NG Firewall	www.barracuda.com
Check Point	NGFW	www.checkpoint.com
Cisco	ASA-Firewall (SecureX)	www.cisco.com
Dell SonicWALL	E-Class NSA	www.sonicwall.com/de
Hewlett-Packard	TippingPoint	www.hp.com.de
Juniper Networks	AppTrack	www.juniper.com
McAfee	Firewall Enterprise	www.mcafee.com/de
Palo Alto	PA-Series	www.paloaltonetworks.com
Sourcefire	FirePOWER Appliance	www.sourcefire.com
Stonesoft	NGFW	www.stonesoft.de
Watchguard	NGFW	www.watchguard.com
UTM-Firewalls		
Fortinet	FortiGate	www.fortinet.com
gateprotect	NGFW	www.gateprotect.com
Sophos	UTM	www.sophos.com
Next Generation IPS		
Corero Network Security	IPS	www.corero.com
IBM	Security Network Protection XGS 5000	www.ibm.com

Die Übersicht erhebt keinen Anspruch auf Vollständigkeit.

Einschränkungen bei der Inhaltsanalyse ergeben sich bei Applikationen mit proprietärer Verschlüsselung. Auch große Dateien, beispielsweise ISO-Images, kommen aufgrund impliziter Einstellung an der Inhaltskontrolle der Firewall üblicherweise ungeprüft vorbei.

Unbekannte Applikationen werden von den Firewalls blockiert. Das ist so lange unproblematisch, wie alle genutzten legitimen Applikationen der Firewall bekannt sind. Ändert sich etwas am Profil, kann es bis zum nächsten Update des Herstellers zum unerwünschten Blockieren von Datenverbindungen kommen. Abhilfe hier könnte die Möglichkeit für Anwender sein, eigene Applikationsprofile schreiben zu können, um im Notfall selbst Hand anzulegen. Entscheidend bei der Auswahl einer NGFW ist daher die Abdeckung der selbst genutzten Applikationen und nicht die bloße Anzahl unterstützter Applikationen. Die Erkennungsrate von IPS- und AV-/Malware-Engine, aber auch die Wirksamkeit des URL-Filters hängen ebenfalls von der Update-Frequenz ab.

Organisatorische Herausforderungen

Bei der SSL-Entschlüsselung ist zu beachten, dass die Firewall dem Decryption Certificate in den eingesetzten Browsern vertrauen muss. Manche SSL-Verbindungen lassen sich dennoch nicht aufbrechen: Das Windows- oder Firefox-Update prüft nicht nur die Gültigkeit des Zertifikats, sondern auch die ausstellende CA. Die Entschlüsselung ist bei Vorliegen der gesetzlichen Voraussetzungen zwingend mit Personal- und Betriebsrat sowie mit dem betrieblichen Datenschutzbeauftragten abzustimmen. Dies gilt auch für die nun viel detaillierter vorliegenden Firewall-Protokolle, da diese aufgrund des Tiefenblicks mit Deep Packet Inspection mehr personenbezogene Daten enthalten und für Leistungskontrollen missbraucht werden könnten.

Die höhere Komplexität des Regelwerks kann die Fehleranfälligkeit erhöhen. Einige Firewall-Administratoren dürften auch mit den neuen Filtermerkmalen überfordert sein. Bei der Einführung sind daher entsprechende Qualifizierungsmaßnahmen und daraus resultierende Kosten zu berücksichtigen. Sind der Betrieb von Firewalls und Intrusion-Prevention-Systemen heute getrennt, kann die Einführung einer NGFW eine Zusammenlegung der Betriebsbereiche erfordern. Damit lässt sich der höhere Betriebsaufwand wieder kompensieren. Bei benutzerbezogenen Regeln ist eine nahtlose Integration in Identity-Management-Systeme erforderlich.

Das Troubleshooting kann bei einer NGFW schwieriger sein, wenn die Ursache für eine blockierte Verbindung in unterschiedlichen Logs zu finden ist. Einige Modelle zeigen bei Port-Scans alle Ports als offen an, wenn keine Ports als Filterkriterium konfiguriert sind. Das bringt neue Herausforderungen für Penetrationstester, aber vor allem für das Troubleshooting der Firewall-Betreiber. Hier gewinnen Regelsimulationen oder Tests von Regeln an Bedeutung, insbesondere eine Prüfung von Endpunkt zu Endpunkt, unabhängig davon, welche Netzwerkkomponenten sich zwischen den Punkten befinden.

Zu unangenehmen Überraschungen kann es bei der Einführung einer NGFW kommen, wenn Unternehmensbereiche von der IT unbemerkt Cloud-Services nutzen. Eine vorherige Bestandsaufnahme hilft, Unterbrechungen und Frust bei den Kollegen zu vermeiden.

Entscheidend für die Einführung einer NGFW sind die möglichen Einsatzszenarien. Soll die Firewall den zentralen Internetübergang, Systeme in einer demilitarisierten Zone oder internen Sicherheitszone schützen, Geschäftspartnerzugänge kontrollieren oder für Spezialfälle wie nicht patchbare Systeme eingesetzt werden? Daraus leiten sich die Anforderungen an benötigte Merkmale und Durchsatzraten ab.

Fazit

Firewalls gelten als Standard mit nur noch geringem Innovationspotenzial. Verkauft werden sie primär über den Preis und die dafür gebotenen Durchsatzraten. Mit den Merkmalen der NGFW beheben die Hersteller lange bekannte Schwächen. Insofern ist der Schritt konsequent, wenn auch etwas spät erfolgt. Sie kombinieren den klassische Funktionsumfang mit IPS-Funktionen, Application, Content und User Awareness und ermöglichen granulare Regelwerke.

Mehr denn je müssen sich Organisationen damit auseinandersetzen, vor welchen Risikoszenarien sie sich schützen wollen und mit welchen Maßnahmen. Damit liegt die Entscheidung für den Einsatz einer NGFW in der Verantwortung des Geschäftsprozesseigners und Dateneigentümers. Hält dieser aufgrund der Eintrittswahrscheinlichkeit bei Risikoszenarien eine Prüfung der Datenpaketinhalte für verzichtbar, kann die Entscheidung zugunsten einer klassischen Firewall ausfallen. In absehbarer Zeit werden sich Entscheider jedoch keine Gedanken mehr zu pro oder contra NGFW machen müssen, da alle Hersteller ihre Produktentwicklung in Richtung Application Awareness und Content Inspection lenken. (ur/sf)

Martin Holzhofer ist Geschäftsführer der auf Informationssicherheit spezialisierten Holzhofer Consulting GmbH.

In iX extra 02/2013

Networking – Unified Communications als Service

Getrieben durch Mobilität und nutzereigene Endgeräte wird Kommunikation immer vielfältiger: Von Web- und Videokonferenzen über Instant Messaging bis zu Collaboration reicht das Spektrum unter dem Schlagwort Unified Communications (UC). Da die Kommunikation nicht mehr an Unternehmensgrenzen haltmacht, liegt der Gedanke nahe, hierfür die Dienste eines Providers in Anspruch zu nehmen.

Inzwischen richten alle Hersteller ihre Produkte konsequent auf gehostete Lösungen aus und bieten zunehmend selbst solche Dienste neben ihren Produkten an. Auch Systemhäusern und Service-Providern stehen damit Software-Werkzeuge zur Verfügung, um Services für Unified Communications zu entwickeln. iX extra zeigt was die Hoster zu bieten haben.

Erscheinungstermin:
24. Januar 2013

DIE WEITEREN IX EXTRAS:

Ausgabe	Thema	Erscheinungstermin
03/13 Security	Compliance und Sicherheitsmanagement	21. 02. 13
04/13 Drucken, Scannen, Archivieren	Multifunktionsgeräte	28. 03. 13
05/13 Networking	Highspeed Hardware mit 40- und 100-GE	25. 04. 13