Firewalls benötigen ständige Kontrolle.

SICHERHEIT IM NETZ

DIE SCHUTZMAUER MIT DER FIREWALL

von Andreas Wisler

Jedes Unternehmen besitzt heutzutage eine Firewall, um sich vor den Angriffen aus dem Internet zu schützen. Heutige Firewalls können aber nicht nur den Netzwerkverkehr filtern, sondern bieten auch eine Vielzahl von weiteren Möglichkeiten. Doch einfach kaufen, einstecken, den Einrichtungs-Wizard durchführen und dann laufen lassen, genügt bei Weitem nicht. Eine Firewall benötigt regelmässige Beachtung.

Eine Firewall trennt verschiedene Netzwerke voneinander. Klassisch ist dies das Internet und das interne LAN. Bei grösseren Firmen kommt oft noch eine DMZ dazu, in welcher vom Internet her erreichbare E-Mail- oder Web-Server untergebracht sind. Immer beliebter werden zudem Mikroarchitekturen, in welcher für jede Art von Dienst eine eigene Zone definiert wird.

SICHERHEIT VON INNEN NACH AUSSEN

Wird eine Firewall aus dem Karton ausgepackt, sind bei Home- und KMU-Firewalls oft zwei Grundregeln voreingestellt: Jeglicher Verkehr aus dem Internet wird blockiert, jeglicher Verkehr vom internen Netz aus ist erlaubt. Theoretisch reicht dies bereits für den Schutz, jedoch stellt gerade die Regel «Von innen nach aussen ist alles erlaubt» eine grosse Gefahr dar. Zwar läuft auf Anhieb alles, doch auch ein möglicher Schädling kann ungehindert mit seinem Ersteller kommunizieren und weitere Daten nachladen. Daher muss auch der Verkehr Richtung Internet blockiert und nur erwünschte Verbindungen erlaubt werden. Möchte man nun solchen weiteren Verkehr zulassen, müssen entsprechende Regeln dargelegt werden, die definieren, von wo nach wo was fliessen darf. Zum Beispiel darf der E-Mail-Server E-Mails verschicken und empfangen. So werden nach und nach die einzelnen Verbindungen eingerichtet, aber wichtig ist, dies nicht konzeptlos zu tun. Erfahrungen aus einer Vielzahl von Audits zeigen, dass sich im Laufe der Zeit viele Regeln ansammeln. Regelmässig sind darunter auch solche, die gar nicht mehr benötigt werden. Wird ein neuer Server hinzugefügt, der die gleiche IP-Adresse eines ausrangierten Servers erhält, erbt er die veralteten Regeln, und plötzlich sind Dinge erlaubt, die gar nicht sein dürften. Schon manch erfolgreicher Angriff auf ein Unternehmen geschah über solch eine vergessene Regel.

PROZESSE FÜR DIE ERHÖHTE SICHERHEIT

Ein umfassender Firewall-Prozess könnte wie folgt aussehen: Als Erstes wird eine Regel bestellt. Alle notwendigen Angaben wie Quelle (IP und Dienst), Ziel (IP und Dienst), allfällige Einschränkungen (Bandbreite, Zeiten), zuständige Dienste (Intrusion Detection, Web-Filter) und Dauer der Regeln (von–bis) müssen angegeben werden. Zweitens wird der Antrag an den CISO (Chief Information Security Officer) geschickt, der überprüft, ob die Regel so Sinn macht, ob es allenfalls schon eine solche Regel gibt oder ob weitere Einschränkungen möglich sind. Die Regel wird dann zurückgewiesen oder der IT zur Umsetzung gegeben. Drittens wird die Regel entsprechend umgesetzt. Im Kommentarfeld der eingerichteten Regel sollte zwingend die Ticketnummer des Antrags enthalten sein, damit später nachvollzogen werden kann, für wen und warum diese Regel erstellt wurde.

Es empfiehlt sich mindestens jährlich, besser halbjährlich, ein Review der Regeln durchzuführen. Bei einem Ticketing-System erhält der Besteller eine Meldung, ob diese noch benötigt wird (Status-Review). Mit einem Klick auf «Ja» bleibt diese aktiv, bei einem Klick auf «Nein» wird der Auftrag an den Firewall-Verantwortlichen ausgelöst, die Regel zu löschen. Der Prozess sieht vor, dass eine aktive Regel jederzeit gelöscht oder inaktiv gesetzt werden kann. Inaktiv dann, wenn die Regel vermutlich nochmals benötigt und daher nicht gelöscht wird. Nicht mehr benötigte Regeln sind zwar auf der Firewall gelöscht, jedoch als Ticket noch vorhanden. So kann jederzeit nachgewiesen werden, was in der Vergangenheit eingerichtet wurde.

ZUGANG ODER ABGANG

Eine Firewall ist heute nicht mehr nur der Türsteher ins eigene Netzwerk. Die Firewalls können bei Weitem mehr, als Verkehr zu blockieren oder durchzulassen. Je nach Hersteller heissen solche Firewalls UTM (Unified Threat Management) oder NG (Next Generation). Die klassischen Erweiterungen wie Intrusion Detection/Prevention sind dabei. Der Netzwerkverkehr wird auf Anomalien untersucht, und werden Abweichungen festgestellt, wird bei reinen Detection-Systemen ein Alarm ausgelöst. Prevention-Systeme können sogar Gegenmassnahmen starten und beispielsweise die Verbindung unterbrechen. Dies muss natürlich mit grosser Sorgfalt konfiguriert werden, damit nicht der gewünschte Netzwerkverkehr blockiert wird.

ZUGRIFF ODER SPERRUNG DURCH DEN PROXY

Die Verbindung wird dabei auf der Firewall aufgebrochen. Dies ermöglicht eine Vielzahl von weiteren Möglichkeiten, wie zum Beispiel das Untersuchen auf mögliche Viren oder andere Schädlinge. Je nach Konfiguration ist dies auch für verschlüsselte Verbindungen der Fall. Hier empfiehlt es sich, wenn das Unternehmen transparent darüber informiert. Doch nicht jede Verbindung lässt sich aufbrechen, gerade beim Online-Banking reagieren dann die Systeme der Banken und verhindern einen Verbindungsaufbau, da nicht unterschieden werden kann, ob ein Hacker sich in die Verbindung eingeschlichen hat oder «nur» das Unternehmen. Durch den Proxy können auch bestimmte Seiten gesperrt werden, wie zum Beispiel Facebook. Doch der Proxy erkennt nicht nur die Webseite, sondern er kann auch erkennen, ob es sich bei der Anfrage wirklich um eine Abfrage einer Webseite handelt oder ob sich ein Programm so tarnt, um nicht aufzufallen. In diese Kategorie fällt beispielsweise der TeamViewer, der sich als normaler Webseiten-Aufruf tarnt, um geschlossene Ports zu umgehen.

ERWEITERTE FUNKTIONEN

E-Mails können bereits auf der Firewall auf Unerwünschtes untersucht werden. Analog den bekannten Filtern im E-Mail-Programm versucht die Firewall verschiedene Begriffe und Muster zu erkennen und so die E-Mail zurückzubehalten oder in eine Junk-E-Mail-Box zu verschieben. Zudem können VPN-Verbindungen (Virtual Private Network) zwischen Standorten, aber auch von Geräten zum Unternehmen aufgebaut werden. Jeglicher Verkehr zwischen den Endpunkten ist verschlüsselt. So wird ein Arbeiten von zu Hause oder unterwegs wie am Arbeitsplatz gewohnt ermöglicht. Dazu kommt der Bedarf an immer mehr Bandbreite für die Dienste, denn irgendwann reicht die Internetverbindung nicht mehr für alles. Dann kann Ferner kann die Firewall einen bestimmten Verkehr vor anderen bevorzugen, und somit werden beispielsweise für die Telefonie (VoIP) entsprechende Ressourcen reserviert, und andere Verbindungen werden gedrosselt. Wird ein Web-Server hinter der Firewall betrieben, lohnt sich der Einsatz einer WAF (Web Application Firewall), damit alle Anfragen auf den Web-Server untersucht werden. Auf diese Weise sollen Angriffe wie SQL-Injection, XSS und viele weitere direkt geblockt und gar nicht erst weitergeleitet werden.

Wie man erkennen kann, werden Firewalls mit den vielen Zusatzfunktionen immer komplexer, und einfach auspacken und laufen lassen reicht nicht mehr. Es braucht ein klares Konzept. Trotz der vielen Möglichkeiten kommen die eingebauten Prozessoren schnell an den Anschlag, und plötzlich steht das komplette Netzwerk still. Eine Firewall muss überwacht und die Logdaten müssen ausgewertet werden. Gibt es Auffälligkeiten oder Abweichungen? Nur bei regelmässiger Betreuung können genügend schnell Massnahmen eingeleitet werden und nicht erst wenn es bereits zu spät ist. Nur wer die Firewall im Auge behält, regelmässig aktualisiert und mit klaren Regeln betreibt, kann sie vor den immer zahlreicher werdenden Gefahren effektiv schützen.

ANDREAS WISLER

ist Leiter bei goSecurity.

www.goSecurity.ch