MEINUNGEN

NETZWERKSICHERHEIT UND FIREWALL: TOP 6 DER ZU VERMEIDENDEN FEHLER

Simon Dansette
Product Manager,
Stormshield

Eine Firewall zu kaufen ist gut. Sie perfekt bereitzustellen, ist besser. Ein Fehler bei der Umsetzung ist schnell passiert und kann Ihre gesamte Sicherheitsrichtlinie gefährden. Erstellung von Sicherheitsrichtlinien, Benennungsrichtlinien, Aktualisierungen und Regelkonsistenz ... Zurück zu den häufigsten Fehlern und wie man sie vermeidet.

Firewalls sind die Säulen der IT-Sicherheit und stehen im Mittelpunkt der Absicherung von IT-Netzwerken gegen Cyberbedrohungen. Diese Tools müssen jedoch mit Bedacht installiert werden. Wir werfen einen Blick auf die sechs Fehler, die Sie bei ihrem Einsatz vermeiden sollten.

DIE PLANUNG VERGESSEN

„In einem Umfeld, in dem ein IT-Manager eine Vielzahl von Aufgaben zu bewältigen hat, kann selbst der erfahrenste IT-Manager abgelenkt werden und bei der Einrichtung einer Firewall einen Fehler machen“, erklärt **Quentin Tieghem**, Pre-Sales Engineer bei Stormshield, gleich zu Beginn. Der Schlüssel, um damit umzugehen? *„Planen, damit nichts vergessen wird, aber auch die längerfristige Verwaltung der Firewall erleichtern*“. Konkret ist das Abbilden des Netzwerkverkehrs mithilfe einer Datenflussmatrix der Ausgangspunkt, um über zukünftige Firewallregeln nachzudenken. *„Die Datenströme im Netzwerk zu identifizieren ist eine wichtige und notwendige Aufgabe. Dann muss man sich fragen, wie man seine Firewall positionieren soll, welche Elemente man schützen will und welche nicht, man muss sich fragen, wie viel Segmentierung man braucht*.“ Um die Einrichtung der Firewall zu erleichtern, muss man also an die unternehmensspezifische Nutzung denken, z. B. an die Bedürfnisse der Mitarbeiter im Telearbeitsplatz. Sie sollten auch wissen, wer das Netzwerk verwalten soll. *„Die Logik*“, so **Guillaume Boisseau**, Manager Professional Services bei Stormshield, *„besteht darin, zunächst theoretisch zu konfigurieren und dann in der Praxis zu überprüfen, ob die eingerichteten Regeln angemessen sind*.“ Da sich die Regeln einer Firewall zusammen mit dem Netzwerk, das sie schützt, weiterentwickeln werden, rät Quentin Tieghem dazu, die Aktualisierungsverfahren schon vor der Einrichtung der Firewall zu antizipieren. *„Man sollte von Anfang an ein Verfahren schreiben, das erklärt, wie man die Firewall einrichtet, aber auch, wie man sie in einem optimal funktionierenden Zustand hält.*“

DIE STANDARDKONFIGURATION BEIBEHALTEN

„Einer der häufigsten Fehler ist, dass die Firewall nicht sofort nach der Installation vollständig konfiguriert wird“, sagt Guillaume Boisseau. Der unumgängliche Schritt ist, die standardmäßig eingerichteten Dienste zu überprüfen – oder unnötige Dienste zu deaktivieren – und sich für neue Passwörter zu entscheiden, die so sicher wie möglich sind. *„Besondere Aufmerksamkeit sollte den Standard-Administratorkonten gewidmet werden*“, insistiert Quentin Tieghem. Er empfiehlt, sie so zu konfigurieren, dass die Berechtigungen auf die spezifischen Bedürfnisse der einzelnen Benutzer beschränkt werden. Ein weiterer Fehler ist es, eine Regel aktiv zu lassen, weil man denkt, dass man sich später darum kümmern wird – und sie dann doch beiseite legt. *„Das ist üblich und ziemlich logisch in einem Beruf, in dem das Tempo oft sehr hoch ist*“, erklärt der Ingenieur. *Angesichts dieser Situation gibt es zwei Möglichkeiten: sich zu verpflichten, den Prozess sofort zu Ende zu führen, oder bereits bei der Erstellung ein Zeitobjekt mit einem Enddatum auf Regeln mit begrenzter Lebensdauer einzuführen*“. Denken Sie auch daran, das SNMP-Protokoll zu deaktivieren oder entsprechend Ihren Bedürfnissen zu konfigurieren: Es ermöglicht Netzwerkadministratoren, Geräte zu verwalten.

VERNACHLÄSSIGUNG DER BENENNUNGSRICHTLINIEN

Ein weiteres zentrales Element für Guillaume Boisseau ist die Benennung der Netzwerke und Geräte, die an die Firewall angeschlossen sind. *„Das ist eine Problematik, die sehr häufig auftritt. Mein Rat ist immer, sich an bereits bestehende Regeln zu halten. Wenn Sie sich die Arbeit gemacht haben, Ihre Server mit einem DNS-Server zu benennen, verwenden Sie die gleiche Benennung, um Probleme zu vermeiden.“* Man muss auch besonders darauf achten, wie sich die Tätigkeiten innerhalb des Unternehmens entwickeln. *„Ein typisches Beispiel“*, erklärt er, *„ist ein Server, der in einem Unternehmen anders genutzt wird, aber im Netzwerk immer noch mit der gleichen IP-Adresse identifiziert wird. Der Server hat sich also geändert, aber die Firewallregeln haben sich nicht geändert und dieser Server hat nun Rechte, die er nicht haben sollte.“*

VERGESSEN, DASS DAS SCHLIMMSTE PASSIEREN KANN

Selbst die stärkste Infrastruktur kann einen Hardware- oder Stromausfall erleiden. Die Herausforderung besteht dann darin, den Schaden zu begrenzen und die Dienste so gut wie möglich in Betrieb zu halten. *„Die Firewalls sind oft die wichtigsten Knotenpunkte im IT-Netzwerk eines Unternehmens“*, sagt Quentin Tieghem. *„Es ist von entscheidender Bedeutung, dass sie im Rahmen des Plans zur Wiederherstellung der Geschäftstätigkeit (ARP) und des Plans zur Aufrechterhaltung der Geschäftstätigkeit (BCP) integriert werden und dass diese Integration kalibriert wird.“* Das Problem ist natürlich nicht dasselbe, wenn die Firewall einen zentralen Platz in der Unternehmensarchitektur einnimmt oder wenn ihr Absturz dazu führt, dass nur wenige Mitarbeiter auf E-Mails zugreifen können. *„Man muss die Umsetzung von PRAs und PCAs testen und dabei über den reinen Softwareteil hinaus gehen“*, sagt Guillaume Boisseau und fährt fort: *„Wenn man ein hohes Maß an Verfügbarkeit von Geräten hat, geht es darum, sicherzustellen, dass es immer eine Möglichkeit gibt, die Verbindung zu überbrücken. Man muss also regelmäßig Backups machen, aber vor allem das Umschalten zwischen Haupt- und Notfallausrüstung testen“*. Ebenso könnte es Ihnen später viele Enttäuschungen ersparen, wenn Sie von Anfang an eine Protokollsenke einrichten.

DIE ÜBERWACHUNG VON FILTERREGELN VERNACHLÄSSIGEN

Änderungen im Produktionsprozess, Entwicklung von Telearbeit, Einführung einer neuen Aktivität ... Eine Firewall, eine Art lebendes Objekt, muss sich logischerweise mit den Aktivitäten des Unternehmens weiterentwickeln. Die Aufrechterhaltung des sicheren Zustands (Safe Condition Maintenance, SCM) wird wiederum bereits bei der Einrichtung des Systems bedacht. *„Da Firewalls immer häufiger das Herzstück von Netzwerken sind, ist es logisch, dass die Infrastruktur durch das Versäumnis, die Regeln auf dem neuesten Stand zu halten, Malware und Ransomware aber auch den jungen Geek, der einen Gelegenheitsangriff mit einem Rootkit starten wird“*, erinnert Quentin Tieghem. Ein Risiko, angesichts dessen der Ingenieur eine einfache Strategie vorschlägt: *„protokollieren,*

alles protokollieren". *Man muss eine klare Historie der Regeln und der Entwicklung der Infrastruktur haben*", sagt er, „*damit man nicht in die Situation gerät, dass eine große Anzahl von Regeln ohne jeden Kommentar eingesetzt wird und man somit nicht weiß, wozu sie dienen*". Der Einsatz von Auditing-Tools ermöglicht es, die Verwendung von Regeln und Objekten genau zu kennen, zu überprüfen und unnötige Verfahren aufzudecken. „*Man kann durchaus manuell eine Tracking-Datei mit den hinzugefügten Regeln erstellen und eine methodische Historie der Entwicklung der Firewall aufbewahren*", sagt Guillaume Boisseau. Die Regeln auf dem neuesten Stand zu halten und auf die Filterung von IPs und URLs zu achten, wird mit einer solchen Archivierungsarbeit viel einfacher. „*Wenn ein Unternehmen einen Dienstleister beauftragt, ist es sehr wichtig, dass es nachvollziehbare Ergebnisse verlangt*", erklärt er. *Diese Dokumentation, die intern oder von einem externen Unternehmen erstellt wird, erleichtert auch die Weitergabe, da sie verhindert, dass das gesamte Wissen auf ein und demselben Mitarbeiter lastet.*"

DIE INFORMATIONSKANÄLE SCHLECHT ORGANISIEREN

Schließlich bedeutet MCS auch Maintenance in Operational Condition (MCO). „*Man sollte die Signaturen so oft wie möglich aktualisieren, um nicht anfällig für neue Angriffe zu sein, und daran denken, die Geräte selbst zu aktualisieren, damit sie immer auf dem neuesten Stand der Wartungspatches und der neuesten Sicherheitsmerkmale sind*", fasst Quentin Tieghem zusammen. Experten sagen es immer wieder: Vorausschauendes Handeln ist der Schlüssel, um Versäumnisse zu vermeiden und langfristig seine Arbeitsbelastung zu verringern. Guillaume Boisseau sagt: „*Man sollte schon bei der Einrichtung daran denken, RSS-Feeds und andere Informationstools zu den Lösungen zu abonnieren, die man verwendet. Dies ist der beste Weg, um frühzeitig über Schwachstellen informiert zu werden, die in den Software-Bausteinen, aus denen die Firewall besteht, entdeckt werden, und um schnell Fehlerkorrekturen zu installieren und die damit verbundenen Sicherheitslücken zu schließen*".

Ein OCM, das auch mit einer regelmäßigen Wartung der Infrastruktur einhergeht, ein zentrales Thema, das allein schon Gegenstand eines (weiteren) Artikels sein könnte.