WHITEPAPER

MANAGED FIREWALL

Die Brandmauer - die Wand, die vor Feuer schützen soll.

In diesem Whitepaper soll es um die gute Firewall gehen. Die Brandmauer – die Wand, die vor Feuer schützen soll. Wer möchte schon einen Brand im Netzwerk? Das Sicherungssystem reguliert die Kommunikation in ein Netzwerk hinein und aus einem Netzwerk hinaus und existiert bereits seit den 90er Jahren.

Und auch drei Jahrzehnte später hat sie noch eine Daseinsberechtigung – vielleicht ist sie wichtiger als je zuvor, da der Netzwerkverkehr kontinuierlich zunimmt. Die Kernaufgabe einer klassischen Firewall ist die Steuerung von Datenpaketen. Welche Daten dürfen in welche Richtung fließen. Erst mit der Entwicklung von sogenannten Next Generation Firewalls ist der Schutz des Unternehmensnetzwerks stärker in den Fokus gerückt. Mehr Features bedeutet aber auch erhöhten Aufwand in der Administrierung und Konfiguration.

Das Managen dieser Systeme wird zunehmend komplexer und damit auch die Frage: Selbst machen oder auslagern? Denn seit längerem gibt es Modelle wie Firewall as a Service(FWaaS) oder auch Managed Firewall Security Services (teil von MSSP). Ist das für alle die richtige Entscheidung? Wohl kaum. Deshalb sollten grundsätzliche Überlegungen getätigt werden, ob ein Managed Security Service Provider (MSSP) die richtige Lösung sein kann.

EXPERTISE

Zuallererst sollte überlegt werden, ob Firewall-Expertise zur Verfügung steht. Steht diese nicht zur Verfügung, sollte geprüft werden, ob Ressourcen beschafft werden können. Denn die Verwaltung von Firewalls erfordert ein tiefgreifendes Verständnis der Prinzipien von Netzwerken und der Netzwerksicherheit, der Firewall-Konfiguration, der Next-Generation-Features und des Umgangs mit den neuesten Bedrohungen und Schwachstellen. Zudem ist es wichtig, dass Updates und Upgrades kontinuierlich und zeitnah installiert werden, damit z. B. Schwachstellen umgehend geschlossen werden.

Ein aktives Managen der Firewalls ist eine Hauptanforderung an die IT-Sicherheit jedes Unternehmens.

FLEXIBILITÄT UND SKALIERBARKEIT

Wächst Ihr Unternehmen schnell? Eröffnen Sie neue Standorte und erschließen neue Länder? MSSPs bieten oft skalierbare Lösungen an, die sich Ihren Anforderungen anpassen. Wenn Sie mit schnellem Wachstum und häufigen Änderungen der Netzwerkinfrastruktur konfrontiert sind, können MSSPs die nötige Flexibilität bei der Unterstützung der Inhouse-IT bieten.

KOSTEN / NUTZEN

Managed Security Services beinhalten in der Regel planbare Preismodelle, die die Kosten für Wartung, Betrieb, Monitoring und Support beinhalten. Berücksichtigen Sie die Kosteneffizienz eines MSSP im Vergleich zu den Kosten, die mit der eigenständigen Verwaltung von Firewalls verbunden sind.

KONTROLLE UND ANPASSUNG

Wenn Sie die Administration der Firewall auslagern, schränkt das gefühlt Ihre Kontrolle ein. Wenn Ihr Unternehmen eine sehr genaue Kontrolle über Regelwerk und Konfiguration der Firewalls vorschreibt, mag die Eigenverwaltung der richtige Weg sein. Im Managed-Modell hingegen ist es möglich die Anforderungen an Kontrolle und Anpassung mit dem MSSP so zu definieren, wie es für Ihre individuelle Situation erforderlich ist.

NETZWERKARCHITEKTUR

Haben Sie eine Cloud-First-Strategie oder ein eigenes Rechenzentrum? Die Rahmenbedingungen sind mit dafür verantwortlich, welche und wie viele Firewalls benötigt werden. Egal an welchen Standorten – die Sicherheitsrichtlinien der Firewalls sollten nicht stark voneinander abweichen. Das Entscheidende ist gar nicht die große Komplexität, sondern vor allem eine Dokumentation der Architektur. Je besser diese beschrieben ist, desto einfacher ist ein sauberes Handling von einem MSSP.

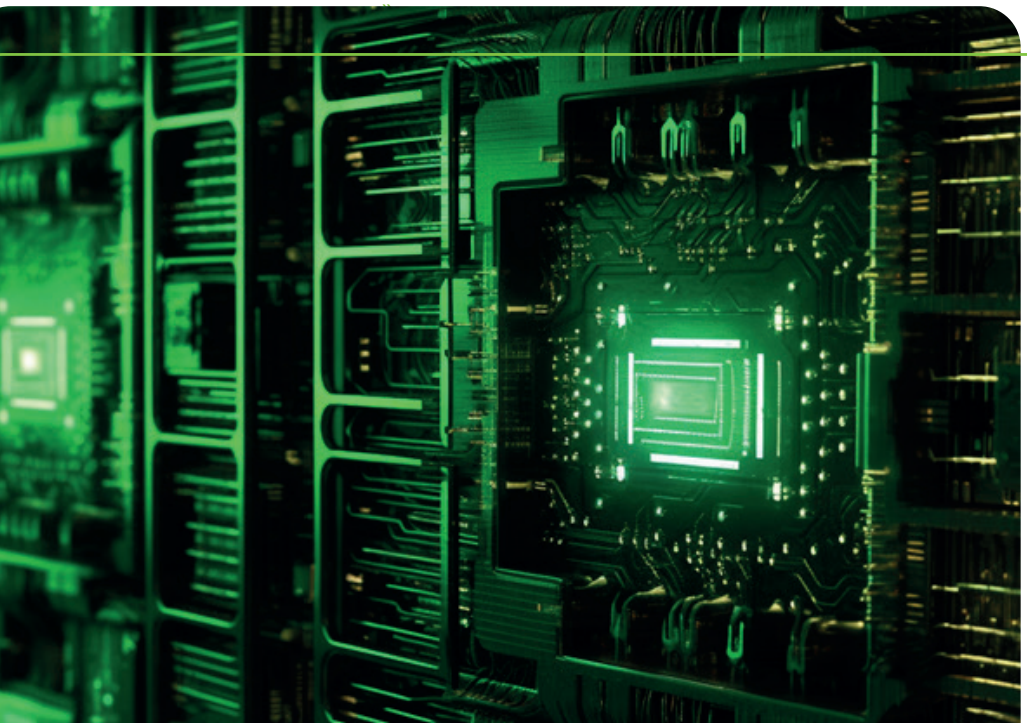
RISIKOBEWERTUNG

Führen Sie eine Risikobewertung für Ihre Organisation durch. Bewerten Sie die potenziellen Risiken, die mit der internen Verwaltung von Firewalls verbunden sind, einschließlich des Risikos von Fehlkonfigurationen, nicht gepatchten Sicherheitslücken, unzureichender Überwachung von Bedrohungen oder begrenzten Ressourcen.

Weitere Risiken können sein:

- Schwachstellen und Exploits
- Unzureichende Regelverwaltung
- Unzureichende Protokollierung und Überwachung
- Fehlende regelmäßige Updates und Patches
- Insider-Bedrohungen
- Einzelner Ausfallpunkt (Single Point of Failure)

Um diese Risiken zu mindern, sollten Unternehmen Best Practices für die Firewall-Verwaltung anwenden, wie z. B. die regelmäßige Überprüfung und Aktualisierung von Firewall-Regeln, die Durchführung gründlicher Sicherheitsbewertungen, die Implementierung starker Authentifizierungs- und Zugriffskontrollen, regelmäßige Patches und Aktualisierungen der Firewall-Firmware, die Implementierung umfassender Protokollierungs- und Überwachungsfunktionen sowie die kontinuierliche Schulung von Firewall-Administratoren.



FAZIT

Letztlich hängt die Entscheidung zwischen FWaaS, Einsetzen eines MSSP und der eigenen Verwaltung von Firewalls von den spezifischen Anforderungen Ihres Unternehmens ab. Machen Sie sich als Team hierzu Gedanken und führen Sie eine Kosten-Nutzen-Analyse durch. Auch können Sie auf IT-Sicherheitsdienstleister zugehen, um ein Beratungsgespräch zu führen.

Wenn Sie sich zusammensetzen – hier die Agenda:

- Schwachstellen und Exploits
- Unzureichende Regelverwaltung
- Unzureichende Protokollierung und Überwachung
- Fehlende regelmäßige Updates und Patches
- Insider-Bedrohungen
- Einzelner Ausfallpunkt (Single Point of Failure)

TIPPS

- » Any-Any-Verbindungen sollte es gar nicht geben
- » Protokollierung ist essenziell
- » Anpassen der Standard-Konfiruration bei Auslieferung (alles schon erlebt...)
- » Testen und ordnen der Regelwerke - regelmäßig!
- » Einzelner Ausfallpunkt (Single Point of Failure)

suresecure GmbH
Dreischeibenhaus 1
40211 Düsseldorf

Telefon: +49 (0) 2156 974 90 60
Telefax: +49 (0) 2156 975 49 78

E-Mail: kontakt@suresecure.de
www.suresecure.de