4 grundlegende Tipps für eine sichere Firewall

Firewalls gehören in Unternehmen zu den wichtigsten Sicherheitskomponenten, um das Netzwerk vor Angriffen zu schützen. Mehr noch, im integrierten und vernetzen Zusammenspiel mit weiteren Security-Lösungen, beispielsweise für die Endpoint-, Mobile- oder Cloud-Security und mit den immer wichtigeren Security-Services durch menschliche Experten, fügt sich die Firewall in ein ganzheitliches Security-Ökosystem ein, das alle IT-Bereiche im Unternehmen bestmöglich vor Angriffen und vor Schäden bewahren kann.
Doch was eigentlich Sicherheit bieten soll, mutiert schnell zum Risiko – nämlich genau dann, wenn die Basics vergessen werden und die Firewall nicht gut genug gepflegt wird. Chris McCormack, Security-Spezialist bei Sophos, gibt vier wichtige Tipps und Best-Practices, mit denen Unternehmen den gewünschten Schutz durch ihre Firewalls sicherstellen.

1. Firmware mit jedem Update aktualisieren
Das vermutlich wichtigste Element für den Erhalt der Schutzwirkung von Firewalls und damit stellvertretend für alle Komponenten in einem Netzwerk, ist das kontinuierliche und schnelle Aktualisieren. Die meisten Firmware-Updates für das Firewall OS enthalten wichtige Sicherheitsverbesserungen. Der beste Weg, um die Firewall-Sicherheit dauerhaft zu gewährleisten, ist immer die neueste Firmware im Einsatz zu haben.

2. Hotfixes automatisieren
Hotfixes heißen so, weil sie Wichtiges schnell korrigieren, etwa neu entdeckte Sicherheitslücken. Und genau deshalb sollten Hotfixes sofort durchgeführt werden, idealerweise automatisch. Es gibt Unternehmen, die diese standardmäßig aktivierte Funktion deaktivieren. Administratoren, die zu dieser Gruppe gehören, sollten diese Funktion unbedingt wieder einschalten, wenn nicht elementare Gründe dagegen sprechen

3. Zugriff auf Firewall-Dienste einschränken
Firewalls bietet eine Reihe von Möglichkeiten, den Zugriff auf Dienste zu beschränken, die nicht benötigt werden – um die Belastung im WAN zu verringern aber auch, um das Risiko im Allgemeinen zu senken. Diese Einstellungen für den Gerätezugriff sollten regelmäßig geprüft werden, um stets den individuell minimalen Zugriff sicherzustellen. Dringend empfohlen ist beispielsweise die Deaktivierung der Remote-Verwaltung über HTTPS und SSH sowie das Captive Portal und das Benutzerportal im WAN. Sollten Fernzugänge unbedingt nötig sein, beispielsweise um die Firewall zu administrieren, sind ein VPN oder noch besser ein Zero Trust Network Access (ZTNA) empfehlenswert.

4. Multi-Faktor-Authentifizierung und rollenbasierte Verwaltung
Wo auch immer möglich, bietet die Multi-Faktor-Authentifizierung (MFA) oder One-Time-Passwörter (OTP) neben sicheren Kennwörtern einen guten Schutz, um Firewalls und damit das Netzwerk vor unberechtigtem Zugriff durch gestohlene Zugangsdaten oder Brute-Force-Hacking-Versuche zu schützen. Moderne Firewalls unterstützen diverse MFA-Authentifizierungsoptionen, einschließlich der neuen Azure AD Single-Sign-On-Authentifizierung für den Webadministrator-Zugang.

Social Media von Sophos für die Presse
Wir haben speziell für Sie als Journalist*in unsere Social-Media-Kanäle angepasst und aufgebaut. Hier tauschen wir uns gerne mit Ihnen aus. Wir bieten Ihnen Statements, Beiträge und Meinungen zu aktuellen Themen und natürlich den direkten Kontakt zu den Sophos Security-Spezialisten.
Folgen Sie uns auf und

LinkedIn: https://www.linkedin.com/groups/9054356/
Twitter: @sophos_info

Pressekontakt:

Sophos
Jörg Schindler, PR-Manager Central & Eastern Europe
joerg.schindler@sophos.com, +49-721-25516-263

TC Communications
Arno Lücht, +49-8081-954619
Thilo Christ, +49-8081-954617
Ulrike Masztalerz, +49-30-55248198
Ariane Wendt +49-172-4536839
sophos@tc-communications.de