BLUE CONSULT.

Firewall Security Assessment für NIS-2

Was haben Firewall-Konfigurationen mit Anforderungen der NIS-2-Richtlinie zu tun?

Die Zeiten, in denen IT-Sicherheit ausschließlich Aufgabe der IT-Abteilung war, sind vorbei. Mit der NIS-2-Richtlinie wird Cybersicherheit zur Verantwortung der gesamten Unternehmensleitung. Geschäftsführung und IT müssen gemeinsam sicherstellen und nachweisen, dass die IT wirksam vor aktuellen Bedrohungen geschützt ist. Denn schon ein erfolgreicher Cyberangriff kann Produktion, Kommunikation und Geschäftsprozesse lahmlegen. Die Firewall bildet dabei die erste Verteidigungslinie Ihres Unternehmens.

Sie steuert den Datenverkehr und schützt Netzwerke vor unbefugten Zugriffen. Doch über Jahre gewachsene Regelwerke, veraltete Firmware und Freigaben oder fehlende Netzwerksegmentierung erhöhen das Sicherheitsrisiko.
Ein Firewall Security Assessment schafft Transparenz über den Sicherheitsstatus Ihrer Firewall. Es deckt Schwachstellen auf, zeigt Optimierungspotenziale und unterstützt Sie dabei, Ihre Cyber-Resilienz zu stärken und die technischen Anforderungen der NIS-2-Richtlinie wirksam zu erfüllen.

Fakten-Check:

- **86 %** der untersuchten Cyberangriffe führten zu Betriebsunterbrechungen oder erheblichen geschäftlichen Auswirkungen.
- Angreifer exfiltrierten **in fast jedem fünften Vorfall** bereits innerhalb der ersten Stunde Daten. Eine wirksame Netzwerksegmentierung und korrekt konfigurierte Firewall-Regeln erschweren Angriffe und laterale Bewegungen.
- **25 %** der Angriffe auf kritische Infrastrukturen beginnen mit der Ausnutzung bekannter Schwachstellen. Regelmäßige Updates und sichere Firewall-Konfigurationen reduzieren dieses Risiko erheblich.
- **70 %** der untersuchten Sicherheitsvorfälle betreffen mehrere Angriffsflächen gleichzeitig. Eine wirksame Firewall mit sauberem Regelwerk und Netzwerksegmentierung bildet dabei eine zentrale Schutzkomponente.

Quellen: Branchenumfragen, Statistiken

Wie ist die Lage bei Ihnen?

- Sind alle Firewall-Regeln dokumentiert, fachlich begründet und werden Änderungen nachvollziehbar protokolliert?
- Werden nicht mehr benötigte Firewall-Regeln regelmäßig überprüft und entfernt?
- Ist Ihre Firewall auf dem aktuellen Firmware- und Patchstand?
- Werden sicherheitsrelevante Ereignisse zentral protokolliert und ausgewertet?
- Sind Administrator-, VPN- und Remote-Zugänge durch Multi-Faktor-Authentifizierung geschützt und werden diese regelmäßig überprüft?
- Ist Ihr Netzwerk sinnvoll segmentiert (z. B. Office, Server, Produktion, IoT und Gäste)?
- Existiert ein getestetes Backup- und Restore-Konzept für Ihre Firewall?
- Kennen Sie den End-of-Life- bzw. End-of-Support-Status Ihrer Firewall?

Angebot BLUE

Mit unserem Firewall Security Assessment prüfen und bewerten wir Ihre Firewall-Infrastruktur herstellerunabhängig auf Sicherheitslücken, Konfigurationsrisiken und Optimierungspotenziale im Kontext der NIS-2-Anforderungen.

Was unsere Experten anbieten:

- Firewall-Hardening und Grundkonfiguration
- Firmware- und Patchmanagement
- Analyse des Firewall-Regelwerks
- Netzwerksegmentierung
- VPN- und Remote-Access-Konfiguration
- Administratorrechte und Multi-Faktor-Authentifizierung
- Logging, Monitoring und Alarmierung
- Intrusion Prevention, Application Control und weitere Security Services
- Backup- und Wiederherstellungskonzepte
- Hochverfügbarkeit und Ausfallsicherheit
- Dokumentation und Änderungsmanagement
- Abgleich mit Best Practices und einer risikobasierten Sicherheitsstrategie gemäß NIS-2
- Management-Bericht mit einer priorisierten Maßnahmenliste und individuellen, konkreten Handlungsempfehlungen

Firewall als wichtiger Baustein für NIS-2:

Die NIS-2-Richtlinie schreibt den Einsatz einer Firewall zwar nicht ausdrücklich vor, sondern verfolgt einen technologieoffenen Ansatz und fordert Unternehmen auf, angemessene technische und organisatorische Maßnahmen zur Beherrschung von Cyberrisiken umzusetzen.

Eine Firewall zählt jedoch zu den wichtigsten technischen Schutzmaßnahmen, um diese Anforderungen wirksam zu unterstützen. Als zentrale Sicherheitskomponente kontrolliert und filtert sie den Netzwerkverkehr, verhindert unbefugte Zugriffe und reduziert die Angriffsfläche für Cyberkriminelle. Gleichzeitig ermöglicht sie eine sichere Netzwerksegmentierung und trägt dazu bei, die Ausbreitung von Schadsoftware innerhalb der IT-Infrastruktur zu verhindern.

Benefits

- Transparenz über den Sicherheitsstatus Ihrer Firewall
- Identifikation kritischer Schwachstellen und Fehlkonfigurationen
- Priorisierte Handlungsempfehlungen nach Risiko und Aufwand
- Verbesserte Netzwerksicherheit und Angriffserkennung
- Unterstützung bei der Umsetzung der NIS-2-Anforderungen
- Dokumentierte Ergebnisse als Grundlage für Audits
- Fundierte Entscheidungsgrundlage für Geschäftsführung und IT-Leitung
- Herstellerunabhängige Bewertung durch erfahrene Security-Spezialisten

Ergänzende Dienstleistungen:

Nach dem Assessment unterstützen wir Sie bei der Umsetzung der empfohlenen Maßnahmen:

- Firewall-Hardening
- Einführung/Optimierung des Firewall-Regelwerks
- Einführung/Optimierung der Netzwerksegmentierung
- Implementierung zusätzlicher Sicherheitsfunktionen
- Firewall-Migrationen und Herstellerwechsel
- Managed Firewall Services
- Security Monitoring und SIEM-Anbindung
- Regelmäßige Firewall Health Checks
- Unterstützung bei weiteren technischen NIS-2-Maßnahmen

Die Wirksamkeit einer Firewall hängt nicht allein von ihrer Anschaffung ab, sondern vor allem von ihrer Konfiguration und kontinuierlichen Pflege. Regelmäßige Assessments helfen dabei, Schwachstellen aufzudecken, Sicherheitslücken zu schließen und das volle Schutzpotenzial der Firewall auszuschöpfen. Damit stärken Sie die Cyber-Resilienz Ihres Unternehmens.

René Angenheister

CTO

rene.angenheister@blue-consult.de
+49 2151 6500 10
www.blue-consult.de