Tipps & Checkliste

HISCOX

CyberSafe! Ihr Wissensboost zu Firewall-Sicherheit

Firewalls und Netzwerksegmentierung zählen zu den wichtigsten Bausteinen moderner IT-Sicherheit – werden im Alltag jedoch häufig unterschätzt. Gerade in komplexen oder gewachsenen Unternehmensnetzen entscheiden klare Strukturen und definierte Regeln darüber, ob Systeme geschützt sind oder unnötige Angriffsflächen entstehen. Wer versteht, wie Zugriffe gesteuert und Netzbereiche sinnvoll getrennt werden, schafft die Grundlage dafür, Cyber-Risiken wirksam zu begrenzen. Machen Sie Firewall-Sicherheit zur festen Routine – für mehr Schutz und Kontrolle im Alltag.

Trainingsvideo: Netzwerksegmentierung & Firewalls

Gemeinsam mit unserem IT-Krisendienstleister geben wir praxisnahe Einblicke, worauf es bei einer sicheren Firewall-Konfiguration wirklich ankommt. Erhalten Sie im Expertenvideo konkrete Tipps, wie Sie mit gezielten Maßnahmen Ihr Netzwerk optimal sichern.

Zum Expertenvideo

Expertentipps zum Nachlesen

Lesen Sie hier die wichtigsten Take-Aways aus dem Expertenvideo:

- **Netzwerksegmentierung umsetzen**
  Trennen Sie sensible Systeme (z. B. Server, Backups, Produktionsumgebungen) vom restlichen Netzwerk, um Schadensausbreitung zu verhindern.
- **Firewall-Regeln klar definieren und dokumentieren**
  Regeln Sie eindeutig, welcher Datenverkehr erlaubt ist – und halten Sie diese Regeln nachvollziehbar fest. Dokumentation sorgt für Transparenz und Sicherheit.
- **Minimalprinzip anwenden („Deny Any“)**
  Erlauben Sie ausschließlich notwendige Zugriffe. Alles andere bleibt standardmäßig gesperrt und reduziert die Angriffsfläche erheblich.
- **Regelmäßige Überprüfung und Freigabeprozesse etablieren**
  Setzen Sie auf Vier Augen Prinzip und wiederkehrende Prüfungen, um veraltete oder unnötige Regeln zu vermeiden.
- **Firewall-Logs aktiv nutzen**
  Überwachen und analysieren Sie Logfiles regelmäßig, um verdächtige Aktivitäten frühzeitig zu erkennen und Vorfälle nachvollziehen zu können.
- **IT-Dienstleister und interne Expertise einbinden**
  Stimmen Sie sich eng mit externen Partnern ab und definieren Sie klare Verantwortlichkeiten für Betrieb und Wartung.
- **Standardpasswörter und Grundeinstellungen prüfen**
  Ersetzen Sie Standardzugänge und optimieren Sie Basiseinstellungen, um einfache Angriffswege zu schließen.

Hier gelangen Sie zur kompletten Videoreihe „CyberSafe! Ihr Wissensboost für mehr IT-Sicherheit“

Weitere Videos entdecken

HISCOX

Ausgezeichneter Schadenservice
4,7 / 5
Kundenzufriedenheit
(Kundenbefragung 2023)

Wissensboost: Firewall-Sicherheit

Firewalls sind kein technisches Detail, sondern essenzieller Bestandteil jeder IT-Sicherheitsstrategie. Wer seine Firewall klar strukturiert konfiguriert und regelmäßig prüft, reduziert Risiken deutlich und schafft eine stabile Grundlage für Cyber-Sicherheit im Unternehmen.

Was versteht man unter Firewall und Netzwerksegmentierung?

Eine Firewall fungiert als digitaler Türsteher des Unternehmensnetzwerks: Sie prüft anhand festgelegter Regeln, welcher Datenverkehr zugelassen wird – und welcher nicht. Dabei kontrolliert sie sowohl eingehende als auch ausgehende Verbindungen und schützt so vor unbefugtem Zugriff.

Die Netzwerksegmentierung ergänzt diesen Schutz, indem das interne Netzwerk in klar getrennte Bereiche aufgeteilt wird, zum Beispiel für Arbeitsplätze, Server oder sensible Systeme. So wird verhindert, dass sich Angriffe oder Schadsoftware ungehindert im gesamten Netzwerk ausbreiten können.

Warum ist Firewall-Sicherheit so wichtig?

Firewalls und Netzwerksegmentierung entfalten ihre Schutzwirkung nur dann, wenn sie konsequent betrieben, regelmäßig überprüft und an veränderte Anforderungen angepasst werden. Erst das Zusammenspiel aus gut gepflegter Firewall und intelligenter Netzwerk-segmentierung sorgt dafür, dass Angriffe frühzeitig abgewehrt, Schäden begrenzt und der laufende Geschäftsbetrieb gesichert werden.

Checkliste: Das sollten Sie prüfen

☐ Ja	Ist das Netzwerk in sichere Segmente unterteilt?
☐ Ja	Gibt es eine Firewall, die den Datenverkehr zwischen internem und externem Netzwerk kontrolliert?
☐ Ja	Gilt das Minimalprinzip und werden nicht explizit freigegebene Verbindungen geblockt(„Deny Any“)?
☐ Ja	Ist das Netzwerk so aufgebaut, dass nicht jeder Bereich frei erreichbar ist?
☐ Ja	Werden Änderungen nach dem Vier-Augen-Prinzip freigegeben?
☐ Ja	Werden Logfiles regelmäßig ausgewertet und ausreichend lange gespeichert?
☐ Ja	Sind Standardpasswörter ersetzt und Grundeinstellungen angepasst?
☐ Ja	Sind interne Verantwortlichkeiten und externe Dienstleister klar eingebunden?
☐ Ja	Sind alle Firewall-Regeln dokumentiert und aktuell?

Cyber-Versicherung: Allround-Schutz bei digitalen Risiken

Die genannten Tipps helfen dabei, die Cyber-Sicherheit zu stärken. Leider lässt sich aber auch mit umfassenden Schutzmaßnahmen ein Cyber-Angriff nicht vollständig ausschließen. Um im Ernstfall handlungsfähig zu bleiben, sollten Sie das Restrisiko zusätzlich absichern. Zum Beispiel mit einer Cyber-Versicherung von Hiscox. Als Experte für Cyber-Gefahren und Pionier am deutschen Versicherungsmarkt hält Hiscox Selbstständigen und Unternehmen den Rücken frei – vorbeugend, mitten in der Krise, bei der Schadenregulierung und bei der nachgelagerten Sicherheitsanalyse.

Hiscox
Bernhard-Wicki-Straße 3, 80636 München

Für Makler
T +49 89 54 58 01 100
E hiscox.info@hiscox.de
W makler.hiscox.de/cyber

Für Endkunden
T +49 89 54 58 01 700
E myhiscox@hiscox.de
W hiscox.de/cyber

Hiscox in Social Media