Tunen Sie Ihr Firewall-Regelwerk - wir unterstützen Sie dabei!

FIREWALL TUNING

Einer unserer Firewall-Spezialisten überprüft remote, ob die Firewall-Regeln entsprechend gewartet sind und die Vergabe der minimal notwendigen Rechte umgesetzt worden ist. Um diese Frage zu beantworten, muss bei jeder Regel anhand der Traffic-Protokolle deren Verwendung analysiert werden.

ÜBERPRÜFUNG DES FIREWALL REGELWERKS
Remote-Überprüfung durch einen unserer zertifizierten Firewall-Experten.

AUSFÜHRLICHE DOKUMENTATION
Umfassender Bericht der Untersuchungsergebnisse inkl. Compliance-Report.

EMPFEHLUNGEN FÜR GEGENMASSNAHMEN
Empfehlungen, wie etwaige Sicherheitslücken behoben werden können.

Konfigurationsänderungen werden im Rahmen des Review NICHT durchgeführt.
Auf Wunsch erstellen wir ein gesondertes Angebot für die Durchführung der empfohlenen Maßnahmen.

ERFAHRUNG UND KNOW-HOW

Bei uns sind Profis am Werk!

- Als **FORTINET PLATINUM PARTNER** mit den meisten und höchsten Zertifizierungen sind wir einer der wichtigsten Implementierungspartner und bieten Expertenwissen auf höchstem Niveau.
- Wir betreuen seit vielen Jahren mehr als **4.000 Fortinet-Geräte** sowohl im Inland als auch an den internationalen Standorten unserer Kunden.
- Wir bieten umfassenden Support sowie ein **hauseigenes höchst-zertifiziertes Fortinet-Team** in unserem Support Center. (Fortinet NSE4 bis NSE8)
- **Managed-Service-Leistungen** rund um die Themen Firewalling, Netzwerk- und Unified Threat Management, Advanced Persistent Threats . 24x7 - seit 2007!

FORTINET PLATINUM PARTNER

FORTINET 8 Network Security Expert

FOLGENDE **ASPEKTE** WERDEN ANALYSIERT

Fortinet Firewall Tuning

+ Basis Review der Firewall (Memory, CPU, Log-Einträge, Software-Stand)
+ Review der Benutzer- und Administratorrechte auf der Firewall und ggf. im Regelwerk
+ Wird Zwei-Faktor-Authentifizierung verwendet?
+ Werden "Trusted Hosts" verwendet?
+ SSL-VPN (wenn im Einsatz) Werden Client-Zertifikate verwendet?
+ IPsec VPN (wenn im Einsatz): Sind die Phase2-Selektoren (Encryption Domains) nur auf die benötigten Sources und Destinations eingeschränkt?
+ Review der Security Profile
+ Gibt es unkommentierte Regeln?
+ Gibt es redundante Regeln, die entfernt werden sollen?
+ Gibt es Regeln, die nicht mehr verwendet werden?
+ Gibt es Dienste in den Regeln, die nicht mehr verwendet werden?
+ Gibt es irgendwelche Gruppen oder Netze in den Regeln, die nicht mehr verwendet werden?

WEITERE **ASPEKTE** DIE ANALYSIERT WERDEN:

+ Gibt es Regeln mit dem Wert „ANY“ in einem der Felder Quelle, Ziel, Service, Protokoll & einer permissiven Aktion?
+ Gibt es übermäßig permissive Regeln? Kann das Regelwerk optimiert werden?
+ Gibt es Möglichkeiten, die Firewall-Performance durch Regelanpassung zu steigern? (zB. IPS, AV, Webfilter Profile)
+ Gibt es Regeln, die riskante Dienste aus dem Internet „Inbound“ ermöglichen? Als Basis dient hier eine Liste dessen, was als „riskant“ für Ihr Unternehmen definiert sein könnte. (z.B. Klartextprotokolle mit Anmeldeinformationen wie Telnet, FTP, POP, IMAP, http, NetBIOS usw.)
+ Gibt es Regeln, die riskante Dienste „Outbound“ mit dem Internet ermöglichen?
+ Gibt es Regeln, die direkte Zugriffe aus dem Internet auf das interne Netzwerk (nicht die DMZ) ermöglichen?
+ Gibt es Regeln, die Datenverkehr vom Internet zu sensiblen Servern, Subnetzten, Geräten oder Datenbanken ermöglichen?

Dokumentation der gefundenen Lücken und Empfehlungen für Gegenmaßnahmen!

Sie erhalten einen Bericht, der das Untersuchungsergebnis entsprechend dokumentiert.

Empfehlungen, wie etwaige Sicherheitslücken behoben werden können.

Dokumentationsbericht inkl. Compliance-Reports (z.B.: PCI DSS, SANS)

ANTARES NETLOGIX

Antares-NetlogiX Netzwerkberatung GmbH
Feldstraße 13, A-3300 Amstetten
T: +43 74 72 / 65 480-0 E: office@netlogix.at

www.netlogix.at