Intrusion Prevention/Detection Systeme (IPS/IDS) - regelmäßige Wartung vom Fachmann

IPS/IDS-Wartung

Um ein funktionelles Intrusion Prevention/Detection System (IPS/IDS) zu betreiben, sind laufend Aktualisierungen und regelmäßige Überprüfungen der Konfiguration unumgänglich. Pattern und Signaturen müssen erneuert werden und die IPS Checks an die aktuelle Sicherheitsumgebung angepasst werden. Dies ist mit einem permanenten Personal- und Zeitaufwand verbunden.

Notwendig bzw. sehr hilfreich hierzu sind langjährige Erfahrungen, um das Wichtige vom Unwichtigen unterscheiden und Sicherheitsrisiken realistisch abschätzen zu können. So wird auch vermieden, dass Ihr Netzwerk durch neue Signaturen beeinträchtigt oder gar blockiert wird.

Bei diesen Aufgaben unterstützen wir Sie gerne als externer Dienstleister mit mehrjähriger Erfahrung in diesem Themenbereich.

Ihre Vorteile

- ✓ Stets aktuelles IPS
- ✓ Profilanpassungen
- ✓ Aktivierung neuer Profile
- ✓ Log Auswertung
- ✓ Dokumentation

Ablauf

Zu Beginn eines Projektes wird uns von Ihnen ein sicherer Remotezugang zu den relevanten Systemen bereitgestellt (VPN Tunnel/GUI Zugriff). Die Klärung weiterer Details und Zugriffsrechte erfolgt in gemeinsamer Absprache.

Danach erfolgt die IPS-Wartung einmal wöchentlich nach Absprache. Hierzu gehören u.a. IPS Updates, Policy Installationen und weitere notwendige Arbeiten auf der Check Point Firewall.

Tätigkeiten

Die IPS-Wartung umfasst folgende Tätigkeiten:

- Aktualisierung des IPS
  (1-mal wöchentlich)
- Nachverfolgung neuer Patterns
  (1 Woche im Modus *Detect*, dann erst Aktivierung nach Kundenvorgabe)
- Aktivierung neuer IPS Checks nach Kundenvorgabe
- Logauswertung auf geloggte IPS Events und Export dieser Logfiles in eine CSV Datei, es erfolgt **keine** Analyse möglicher Angriffe (nur nach Absprache)
- Entfernung offensichtlicher „false Positives“ aus den gewarteten Profiles
  (Definition sog. *Execptions*)
- Dokumentation der Konfiguration des IPS Systems
  (per Export in eine Datei im Excel-Format)

Preise

Preis für diese Dienstleistung auf Anfrage.

Der übliche Wartungszeitraum beträgt 1 Jahr.

Werden mehr als ein einzelnes aktives IPS Profil einer Check Point Firewall oder Clusters verwendet, werden weitere aktiv verwendete Profile rabattiert.

Weitere Fragen beantworten wir Ihnen gern. Sprechen Sie uns an:

Ihre direkten Ansprechpartner:

Dr. Matthias Leu
Telefon: +49 8102 895 190
E-Mail: mleu@aerasec.de

Bernd Ochsmann
Telefon: +49 151 125 999 41
E-Mail: bochsmann@aerasec.de

Marco Remmel
Telefon: +49 173 703 92 44
E-Mail: mremmel@aerasec.de

AERA SEC
www.aerasec.de

Tel.: +49 8102 895190
Fax: +49 8102 895199
Mail: info@aerasec.de