Managed SOC: SIEM Service

DURCHGÄNGIGER SCHUTZ KRITISCHER SYSTEME

Ausgangssituation

- Schutz unternehmenskritischer Systeme inklusive industrieller Steuerungssysteme und eingebetteter Software in Geräten vor Befall von Schadsoftware, Spionage oder missbräuchlicher Nutzung unverzichtbar
- Erkennung und Abwehr von Angriffen anhand definierter Maßnahmen
- Einhaltung eines klar definierten Sicherheitsniveaus muss gewährleistet sein

Lösungsansatz SIEM Service

- Analyse und Definition der Sicherheitsanforderungen und des Netzwerks
- Installation einer vorkonfigurierten Appliance für Eventkorrelation und/oder Netzwerk-Flow-Überwachung im RZ des Kunden
- Betrieb aller notwendigen Appliances über abgesicherten Fernzugriff im IS4IT SOC
- Umsetzung auf Basis vereinbarter SLAs

Leistungsumfang SIEM Service

- Bereitstellung aller Sicherheitsdaten in Echtzeit
- Überwachung und Korrelation der eingegangenen Events und des analysierten Netzwerk-Traffics, Auswertung durch geschulte IT-Security-Experten
- Regelmäßige Aktualisierung der Datenbanken bezüglich schädlicher URLs und IP-Adressen
- Incident Management bis zur Erledigung eines Vorfalls
- Regelmäßige Dokumentationen und Auswertungen
- Kontrollierte Ticketverarbeitung je nach Art der Sicherheitsvorfälle
- Anlassabhängige Vorschläge für Service-Meetings zur Optimierung der Sicherheitslage
- Service-Zeiten je nach Paket von 08:00 bis 17:00 Uhr, 06:00 bis 22:00 Uhr oder rund um die Uhr
- Rufbereitschaft außerhalb der Service-Zeit
- Reaktionszeiten je nach Kritikalität und Service-Level zwischen 30 Minuten und 24 Stunden

Organisatorische Aufgaben mit kundenseitiger Mitwirkung

- Bereitstellung von VMware-Umgebung
- Implementierung der VPN-Verbindungen
- Konfiguration der Firewalls für die Weiterleitung der Events zur Appliance
- Implementierung der Regeln der Event-Weiterleitung
- Umgehende Meldung von Ereignissen, die die Nutzbarkeit oder Sicherheit des Betriebes der Lösung beeinträchtigen
- Archivierung aller Informationen gemäß Aufbewahrungsfristen

Nutzen für den Kunden

- Zeitgleiche Überwachung sämtlicher Unternehmensnetzwerke
- Maximale Sicherheit für unternehmenskritische Systeme
- Ungestörter Produktivbetrieb gewährleistet

IS4IT KRITIS GmbH Kraftwerkstraße 1 74847 Obrigheim telefon +49 6261 31944-0 fax +49 6261 31944-9 info@is4it-kritis.de www.is4it-kritis.de