Hochsicherer unidirektionaler Datentransfer von Sicherheits– und Systemmeldungen

FUNKTIONEN UND EIGENSCHAFTEN

Sichere Netztrennung
- Proprietäres Übertragungs-protokoll (SID-HS)
- Sicherheit durch Hardware
- Sicherheit durch Software

Systemsicherheit
- Gehärtetes Debian Linux
- SSHv2
- HTTPS
- Filesystem-Integrity-Checks
- Security-Baselining
- Lokale Firewall
- Firewall-Integritätsprüfung
- Signierte Software-Pakete

Management
- Setup über SSHv2 und seriell
- Out-of-Band Management bei SID-LAN
- Alert-System (E-Mail, Pager, Syslog, Logfiles)
- Backup/Restore/Recovery
- Watchdog
- Hardware-Monitoring

Installation
- USB Stick oder über OOB

Integration
- Sichere Updates über Internet oder lokal
- NTPv3 Zeitsynchronisation
- E-Mail
- Syslog

Support
- 5x8 per Telefon und E-Mail

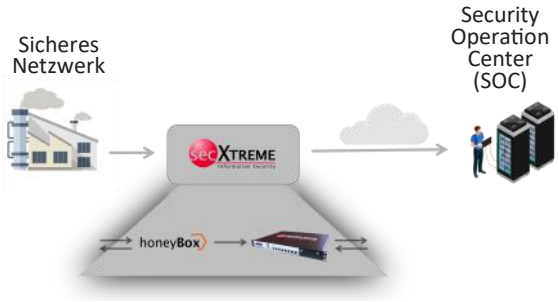
Hardwaretausch
- NBD-Tausch für bis zu 5 Jahre
- Keep-Your-Flash-Disk-Option

Lösung

Die secXtreme Information Diode (SID) ermöglicht Ihnen je nach Kundenwunsch die interne oder externe Übertragung von Sicherheitsmeldungen. Durch ein proprietäres Sicherheitsprotokoll und weiteren Sicherheitsmechanismen wird der bidirektionale Datenfluss zuverlässig verhindert. Dies führt für Sie zu einem hohen Nutzen bezüglich Vertraulichkeit, Verfügbarkeit und Integrität der sicheren Netze und gleichzeitig zeitnaher und zentraler Verfügbarkeit der Sicherheitsmeldungen.

secXtreme Information Diode
LAN Generation 2

Unsere Lösung bietet einen Mix aus Hard- und Software-Sicherheitslösung. Die secXtreme Information Diode hilft Ihnen auch durch ihre umfangreichen Protokollierungsfunktionen Angriffe rechtzeitig zu erkennen, um größere Schäden zu vermeiden.



Die secXtreme Information Diode (SID) kann in Kombination mit einer honeyBox Management-Appliance betrieben werden. Die SID besitzt ein speziell gehärtetes Betriebssystem und eine umfangreiche Selbstüberwachung. Die SID wird in einem unsicheren Netzwerk platziert, während die honeyBox-Appliance in einem sicheren Netzwerk steht. Dabei übernimmt die honeyBox den internen Teil des SID High Security Paars.

Aufgabenstellung

KRITIS-Unternehmen benötigen eine sichere Verbindung, über die sensible Daten in nur eine Richtung von hochsicheren Netzwerken in unsicherere Netzwerke übertragen werden. Während herkömmliche Datendioden häufig für die entgegengesetzte Richtung konzipiert sind, ist durch die secXtreme Information Diode der Zugriff von außen auf die internen Daten der Systeme im sicheren Netzwerk durch Protokollbruch und Hardware-Trennung nahezu unmöglich.

secXtreme Information Diode LAN Standalone

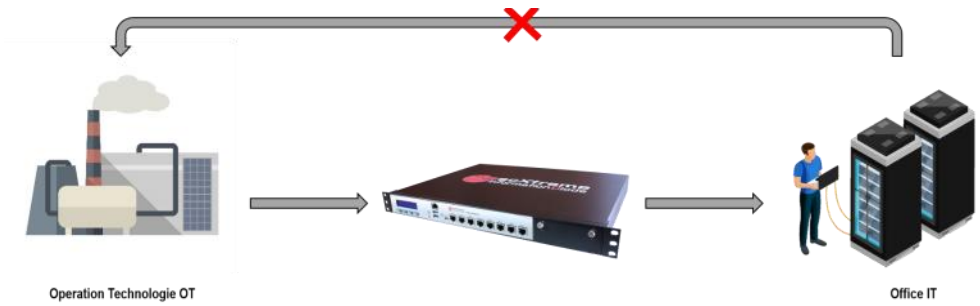
EINSATZSZENARIEN

Managed Service

Situation: Sie besitzen bereits honeyBox-Appliances und wollen deren Meldungen zur Auswertung sicher an einen externen IT-Sicherheitsdienstleister senden.
Umsetzung: Der Einsatz der SID ermöglicht eine rein unidirektionale und hochsichere Kommunikation vom sicheren Unternehmensnetzwerk nach außen zum Security Operation Center (SOC). Somit kann zuverlässig verhindert werden, dass Angreifer Zugriff auf Systeme und Daten des sicheren Netzwerks erhalten.
Ergebnis: Durch eine unverzügliche Datenübertragung und zeitnahe Auswertung kann sich das SOC umgehend mit ausgewählten Mitarbeitern Ihres Unternehmens in Verbindung setzen, sodass der Angriff gemeinsam eingedämmt werden kann, bevor ein größerer Schaden entsteht.

Sichere Datenübertragung ohne Netzwerkverbindung

Situation: Sie besitzen isolierte Hochsicherheitsnetzwerke ohne Verbindung zu anderen Netzwerken und wollen Daten der honeyBox-Appliances an Ihr internes honeyBox-Management weiterleiten.
Umsetzung: Über ein proprietäres Sicherheitsprotokoll verbindet die SID-HS isolierte Netzwerke ohne Netzwerkverbindung mit Ihrem honeyBox-Management, wobei der Fokus erneut auf einer einseitigen Verbindung vom sicheren in den unsicheren Bereich Ihres Unternehmens liegt.
Ergebnis: Zeit- und Kostenersparnis aufgrund zentraler Überwachung



Implementierung

Durch den Einsatz von SID ermöglichen Sie eine hochsichere unidirektionale Kommunikation vom internen sicheren Netzwerk Ihres Unternehmens nach außen zum SOC (Security Operation Center) oder Ihrem eigenen SIEM-System. Somit verhindern Sie den Zugriff auf Ihre Systeme und sensible Daten aus Ihren Netzwerk. Die schnelle Auswertung im SOC ermöglicht Ihnen eine schnelle Reaktion um gemeinsam den Angriff einzudämmen. Einsparung von Zeit und Kosten ist nur durch die zentrale Überwachung von Meldungen mit Hilfe der SID möglich.

CPU	Intel Pentium GT4400TE 2,4 GHz
Arbeitsspeicher	4 GB DDR4
Netzwerk	6 x RJ-45 GbE Ethernet 2 x SFP Ports
USB	2 x USB 3.0
Speichermedium	250 GB 2,5“ SATA SSD
Leistungsaufnahme (typ.)	220 Watt
Spannungsversorgung	90 - 264 VAC 43 - 67 Hz
Betriebstemperatur	0°C bis +40 °C
Luftfeuchte	5 % - 90 %
Gewicht	7,5 Kg
Abmessungen	438 mm x 44 mm x 321 mm (BxHxT)
Zertifizierungen	CE, RoHS, FCC, WEEE

secXtreme Information Diode LAN Generation 2

Über secXtreme: Die secXtreme GmbH hat sich auf die Sicherheit Ihrer Informationen spezialisiert. Dazu gehören die Bereiche Audit, Penetration Testing, Sicherheitsanalysen und Trainings. Neben diesen Bereichen entwickelt secXtreme Lösungen im IT-Sicherheitsumfeld. secXtreme unterstützt seine Kunden bei Incident-Management und Forensik- Aufgaben und bietet in diesen Bereichen Managed Security Services an.

secXtreme GmbH
Alte Landstraße 21
D-85521 Ottobrunn

Tel. +49(0)89-18 90 80 68-0
E-Mail: info@sec-xtreme.com
www.sec-xtreme.com