

## KONTROLLIERTE UND SICHERE NETZWERKE

### Ausgangssituation

- Unkontrollierter Netzwerkverkehr erhöht die Risiken
- Hoher Bedarf an kompetenten Mitarbeitern zur Überwachung
- Keine Ressourcen zur permanenten Überwachung verfügbar
- Tool-Unterstützung oft unzureichend
- Hochleistungsfähige Tools für kleinere Organisationen zu teuer
- Mangelnde Integration in einer unternehmensweiten Sicherheitslösung

### Lösungsansatz Network Security Service

- Einsatz der Advanced-Security-Analysis-Plattform von finally safe
- Analyse des Traffics in festgelegten Bereichen
- Umsetzung von Maßnahmen nach Kritikalität
- Einbindung in SIEM-Service-Plattform

### Leistungsumfang Network Security Service

- Inbetriebnahme des Sensors vor Ort beim Kunden mittels VPN-Verbindung
- Monatliche Reports über die Sicherheitslage sowie Sicherheitsvorfälle
- Reaktionszeit auf Incidents je nach vereinbartem Service-Level und vereinbarter Servicezeit
- Servicezeit je nach Paket von 08:00 bis 17:00 Uhr, 06:00 bis 22:00 Uhr oder rund um die Uhr
- Rufbereitschaft außerhalb der Servicezeit
- Reaktionszeiten je nach Kritikalität zwischen 30 Minuten und 24 Stunden
- Hardware-Austausch vor Ort je nach Kritikalität zwischen vier Stunden und fünf Arbeitstagen

### Technische Sicherheitsmerkmale

- Automatisiertes Aufdecken veralteter OS und Browser
- Automatisiertes Aufdecken fehlender oder schwacher Verschlüsselungen
- Intelligentes Lernen des Netzwerkverhaltens
- Automatisiertes Aufdecken von Anomalien
- Aufdeckung von Systemfreigabe- und Policy-Verstößen
- Meldung bei Aufdecken von versteckten Kommunikationskanälen
- Forensik zu Betriebs- und Sicherheitsvorfällen
- Automatisiertes Aufdecken von Advanced Persistent Threats
- Botnetzerkennung und Aufdeckung versteckter Steuerkanäle
- Erkennung von Manipulationen von Netzwerkverbindungen

### Nutzen für den Kunden

- Automation der Überwachung reduziert Kosten
- Konstante und professionelle Überwachung des Netzwerks minimiert das Risiko erfolgreicher Angriffe
- Ausgereifte und modernste Technologie mit optimiertem Preis-Leistungs-Verhältnis

## MANAGED SERVICES ENTLASTEN IHR TEAM

### Ausgangssituation

- Bedrohungslage nimmt ständig zu und wird immer aggressiver
- Neue Regularien und Gesetze (EU-DSGVO, KRITIS etc.)
- Strafen drohen – Bußgelder bis zu 4 % des Umsatzes bzw. bis zu 20 Mio. Euro
- Kronjuwelen des Unternehmens bewerten und schützen
- Security-Analysten und Forensik-Experten sind teuer

### Lösungsansatz Managed SOC

- Security-Analysten betreuen mehrere Unternehmen parallel
- Optimale Infrastrukturnutzung □ Mandantenfähigkeit und virtuelle Server

### Leistungsumfang Managed SOC

- |                       |                            |
|-----------------------|----------------------------|
| ■ SIEM Service        | ■ E-Mail-Service           |
| ■ SOAR Service        | ■ Vulnerability Management |
| ■ Endpoint Protection | ■ Incident Response        |
| ■ IPsec               | ■ Endpoint Service         |
|                       | ■ Network Security Service |



### Warum Informationssicherheit mit IS4IT?

- Schneller Return on Investment
- Klare Aufgabentrennung zwischen Betrieb und Sicherheit

### Nutzen für den Kunden

- Monatlicher Festpreis, halbjährige Kündigungsfrist,
- Mindestlaufzeit von 12 oder 36 Monaten
- Rechtlich abgesicherte Sicherheitskonzepte und revisionssichere Datenhaltung

