FORTINET

OT-Netzwerke sicher betreiben

Bei industriell eingesetzten Systemen wie SCADA-Servern oder industriellen Kontrollsystemen (ICS) wiegen Cybervorfälle besonders schwer: Aus einer fehlerhaften Steuerung können physische Gefahren resultieren bis hin zum Verlust menschlichen Lebens. Deshalb sollte der Sicherheit in OT-Netzwerken (Operational Technology) höchste Aufmerksamkeit zukommen. Fortinet bietet auf der Basis seiner Security Fabric optimale Visibilität über die gesamte Infrastruktur, ergänzt um eine Datenbank mit Sicherheitsinformationen zu zahlreichen OT-Systemen und -Geräten. Dazu kommen robuste Varianten der Sicherheits-Appliances und spezielle Services für Industrial Security.

- Fortinet Security Fabric: umfassende Sicherheitsarchitektur für IT und OT
- Rugged-Versionen von Firewalls, Switches etc.
- Unterstützung industrieller Protokolle wie Modbus und Profibus
- Spezifischer Schutz für Systeme von ICS-Herstellern wie Siemens, ABB, Rockwell, GE etc.
- Abgestimmte Dienstleistungen für Sicherheit in industriellen Umgebungen

www.boll.ch/de/fortinet

paloalto® NETWORKS

Endpunktschutz auf höchstem Niveau

Konventioneller Endpunktschutz wehrt aktuelle Cyberangriffe nur unzureichend ab. Die Extended-Detection-and-Response-Lösung Cortex XDR von Palo Alto Networks kombiniert Erkennung, Prävention, Analyse und Reaktion auf Cyberangriffe auf einer einzigen Plattform. Dabei setzt Cortex XDR auf künstliche Intelligenz und Verhaltensanalyse und bietet damit ein markant höheres Sicherheitsniveau. Die cloudbasierte Verwaltung erlaubt eine rasche Bereitstellung des schlanken Endpunktschutzes und bietet dabei volle Transparenz über Vorfälle und Geräte – ohne dass dazu vor Ort Server oder Netzwerksensoren installiert werden müssen.

- Konsolidiert Endpunkte-, Netzwerk- und Cloud-Informationen, um «blind spots» zu vermeiden
- Ausgezeichneter Schutz durch Einsatz neuester Technologien
- Verhaltensbasierte Analyse verdächtiger Vorgänge
- Erlaubt Fokussierung des Sicherheitsteams auf wichtige Vorfälle
- Verbessert Erkennung, Forensik und Incident Management

www.boll.ch/info/PAN-XDR

RAPID7

Externe Bedrohungen aus dem Darknet erkennen

Unternehmen, starke Brands, aber auch Behörden müssen ihre Assets und Reputation auch in der digitalen Welt schützen. Heute genügt es nicht mehr, den Blick bezüglich Security nur nach innen zu richten: Gefälschte Domains und Fake-Social-Media-Profile sowie geleakte Unternehmensinformationen können enormen Schaden anrichten. Rapid7 treibt mit der Integration des israelischen Spezialisten IntSights den Kampf gegen solche Bedrohungen voran. External Threat Intelligence von Rapid7 sammelt Daten ausserhalb der Organisation aus dem Clear-, Deep- oder Darknet und liefert, kombiniert mit strategischer Bedrohungsaufdeckung durch Spezialisten von Rapid7, informative Risikoanalysen.

- External Threat Intelligence überwacht Unternehmens-Assets im Cyberspace
- Erlaubt, Gefahren aus dem Netz frühzeitig zu erkennen
- Ermöglicht, proaktiv Gegenmassnahmen zu treffen
- Kombination von automatisierter Analyse und Expertenwissen

www.rapid7.com