RADAR
CYBER SECURITY

Ohne uns könnte Ihre Welt plötzlich Kopf stehen.

Secure your Operational Technology (OT)

- Detection of OT/ICS threats and vulnerabilities
- Converged Cyber Security for OT and IT

IT Security
made in Europe

OT- und IT-Sicherheit

Die Learnings nach Petya & WannaCry

OT (Operational Technology) ist heute hochgradig vernetzt – sowohl innerhalb der OT als auch mit der IT (Information Technology). Eingebettete Systeme kommunizieren selbstständig miteinander, Anlagenführer überwachen und steuern aus der Ferne, Planungssysteme aus der Cloud berechnen Auftragsschritte und Maschinenbelegungen, Wartungspersonal greift weltweit zu und führt Konfigurationsänderungen aus.

Die Bedeutung von Schutzmechanismen für die OT und IT ist heute zumindest gleich hoch den physischen Schutzmaßnahmen einer Fabrik. Über die Netzwerk-Verbindungen können Angreifer in die Systeme eindringen und sie manipulieren. Schadsoftware kann weite Bereiche vollständig lahmlegen und dabei auch immense physische Schäden sowie Gefahren für Leib und Leben verursachen.

Nicht erst seit zahlreichen Produktionsausfällen bei multinationalen Konzernen in 2017 ist klar, dass Fabriken und Anlagen Ziele für Cyber-Angriffe sind.

OT- und IT-Sicherheit in der industriellen Produktion unterliegt besonderen Rahmenbedingungen: So stellt die Steuerung von Produktionsanlagen Echtzeit-Anforderungen, die Veränderungen auf den Systemen schwierig bis unmöglich machen. Das heißt zum Beispiel, dass Software-Patches auf den Systemen, Malware-Scannern und Antivirus-Programmen die Funktionsfähigkeit beeinträchtigen können. Hinzu kommt, dass sich der vergleichsweise lange Nutzungszeitraum von Hard- und Software in der Produktion erheblich von anderen Einsatzgebieten unterscheidet.

Für Produktionsumgebungen müssen daher durchdachte Sicherheitskonzepte gefunden werden, um OT- und IT-Sicherheit - sowohl von neuen Systemen als auch von Altanlagen - in der Praxis umzusetzen.

Aktuelle Vorfälle

Ransomware Petya & NotPetya legen Markenhersteller für Schokolade und Kosmetik, Reederei, weitere multinationale Konzerne und Behörden lahm
Angriffe, die Chaos zum Ziel hatten und dieses Ziel in mehreren multinationalen Konzernen und nationalen Infrastrukturen weltweit erreicht haben: Die Ransomware verbreitete sich schnell in Organisationen und hat viele Bereiche lahmgelegt, indem sie Schwachstellen im Windows-Betriebssystem von Microsoft ausnutzte. Sobald die Rechner infiziert waren, wurden die Nutzer aufgefordert, Lösegeld in Form von Bitcoins zu bezahlen. Durch Petya & NotPetya sind für die betroffenen Unternehmen Schäden in Millionenhöhe entstanden, allem voran teilweise wochenlange Produktionsausfälle oder der Stillstand anderer kritischer Geschäftsprozesse.

Ransomware WannaCry infizierte 230.000 Geräte branchenübergreifend in über 150 Ländern
Eine der bislang größten Ransomware-Attacken setzte zunächst bei älteren Windows-Systemen (Windows XP und Windows Server 2003) an. Die Schadsoftware nutzte offenbar eine Sicherheitslücke im SMB-Protokoll von Microsoft. Die Lücke ist auch unter dem Namen „EternalBlue“ bekannt und wurde von der amerikanischen NSA mehr als fünf Jahre lang für eigene Zwecke ausgenutzt. Seit einem Sicherheitsvorfall bei der NSA erfuhr eine Hackergruppe namens „Shadow Brokers“ von „EternalBlue“ und veröffentlichte die Schwachstelle. Lahmgelegt wurden Organisationen aus allen Branchen, vor allem kritische Infrastrukturen, Automobilhersteller, Logistik- und Telekommunikationskonzerne.

APT-Angriff auf ein Stahlwerk
Mittels Kombination aus Social Engineering und Datendiebstahl per E-Mail (Spear-Phishing) erlangten Angreifer Zugriff auf das Büronetz eines Stahlwerks. Von dort aus arbeiteten sie sich in die Produktionsnetze vor. Steuerungskomponenten und ganze Anlagen fielen aus. Ein Hochofen konnte nicht mehr geregelt herunterfahren werden und befand sich in einem undefinierten Zustand. Die Anlage wurde massiv beschädigt.

Angriff auf Produktionsnetze durch Dragonfly
Dragonfly ist eine Gruppe, die in Deutschland bereits mehrere Dutzend Unternehmen angriff. In einer ihrer Angriffskampagnen griffen sie im ersten Schritt Hersteller von Software für Industriesteuerungssysteme an. Den Installationsdateien auf den Downloadservern wurde das Schadprogramm Havex angehängt. Damit sammelten sie gezielt Informationen im Bereich industrieller Steuerungssysteme, darunter Informationen zu den im Produktionsnetz verwendeten Geräten und Systemen. Das BSI geht davon aus, dass die Täter die gewonnenen Informationen für weitere Angriffe verwenden und verfolgt die Angriffskampagne gemeinsam mit dem Bundeskriminalamt weiter.

Risikoszenarien

Szenario 1
Angreifer schleusen Schadprogramme ein und blockieren die gesamte Produktion und Logistik. Produktions- und Auslastungsdaten werden eingesehen, Anwendungs- und Systemdaten manipuliert. Im schlimmsten Fall richtet eine lahmgelegte oder fehlgesteuerte Maschine physischen Schaden in ihrem Umfeld an.

Szenario 2
Befehle an Industrieroboter werden über eingebettete Systeme gegeben, welche in der Regel an eine speicherprogrammierbare Steuerung angeschlossen sind. Die Steuerungskomponenten sind mit dem Internet verbunden. Ein Angreifer kann so Anwendungs- und Systemdaten auslesen, Datenpakete installieren und in weiterer Folge Fertigungslinien und verbundene Systeme bis hin zur gesamten Unternehmens-IT sabotieren.

Szenario 3
Social Engineering: Angreifer nutzen menschliche Eigenschaften wie Hilfsbereitschaft, Vertrauen, Neugier oder Angst von Mitarbeitern aus, um an Daten zu gelangen, Schutzmaßnahmen zu umgehen oder Schadcode auf deren Computern zu installieren. Sie erreichen so ihr Ziel, sich ungestört im Unternehmensnetzwerk aufzuhalten.

Industrie 4.0 = Sicherheit 4.0?

Industrie 4.0 bezeichnet die vierte industrielle Revolution, die Zukunft der industriellen Produktion unter Einbindung des „Internets der Dinge“. Kennzeichnend ist eine ausgeprägte Individualisierung der Produkte bei gleichzeitiger Berücksichtigung der Bedingungen einer dynamischen (Großserien-) Produktion. Fabriken werden zu Smart Factories. Prozesse werden in Echtzeit über Landes- und Unternehmensgrenzen hinaus gesteuert und koordiniert. Damit das gelingt, ist die Standardisierung und Modularisierung der einzelnen Prozessschritte sowie die Programmierung von virtuell bearbeitbaren Modellen dieser Module notwendig. Die Individualisierung der Produkte wird es Unternehmen in vielen Branchen ermöglichen, zu geringen Kosten eine hohe Zahl an Produktvarianten zu produzieren und so individuelle Kundenwünsche zu bedienen. Unternehmen können flexibel auf Marktentwicklungen, kurzfristig geänderte Produktanforderungen oder schwankende Rohstoffpreise reagieren. Die starke Anpassungsfähigkeit geht mit einer erhöhten Auslastung der Produktionskapazitäten einher und das flexible Ressourcenmanagement verbessert die Effizienz des Gesamtbetriebs. Durch genaue Kalkulationen wird weniger Material benötigt, Lagerhaltungs- und Fertigungskosten sinken.

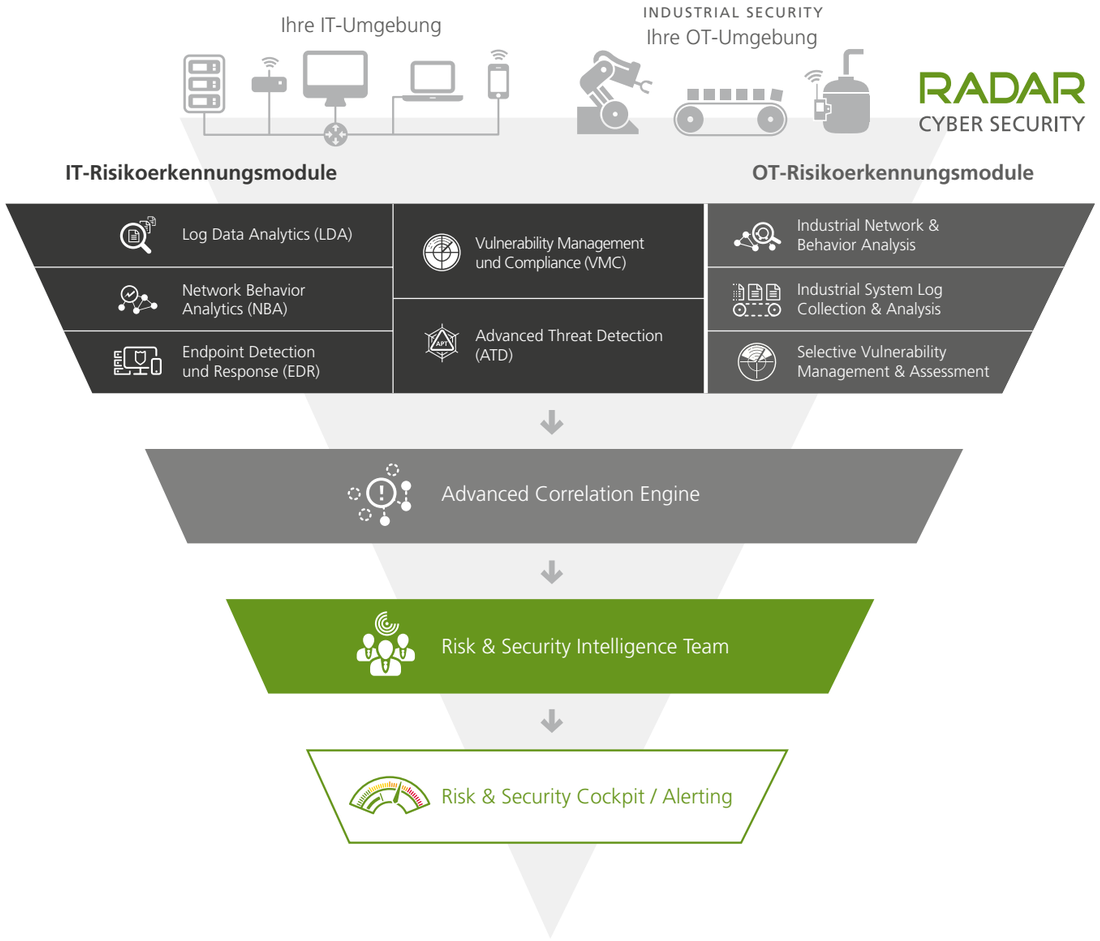
Industrie 4.0 bedeutet Chancen und Herausforderungen. Die Eingliederung des Konzepts in die Organisation bedeutet die Öffnung der betrieblichen OT- und IT-Infrastruktur, macht sie fehleranfällig und angreifbar. Hinzu kommt, dass Angreifer immer wieder neue Wege finden, in Unternehmen einzudringen. Speziell auf industrielle Kontrollsysteme ausgelegte Attacken bedrohen Produktionsanlagen. Befallene Computer können ferngesteuert und ausspioniert werden. Auch angeschlossene oder integrierte Geräte wie Mikrofone, Tastaturen und Bildschirme können ausgewertet werden. Da die Malware unbekannte Sicherheitslücken ausnützt, wird sie auch nicht von Firewalls und Netzwerküberwachungssoftware erkannt.

OT- und IT-Sicherheit heute: Konzeption eines konvergenten Schutzschirms

Für den Schutz ihrer OT und IT müssen produzierende Unternehmen vor allem ein effektives und effizientes Sicherheitsmanagement etablieren. Klassische Abwehrmaßnahmen wie Firewalls, Antivirensoftware und Netzwerküberwachungssoftware decken immer nur ganz bestimmte, kleine Teile der IT-Landschaft und der möglichen Angriffsarten ab. Angreifer hingegen konzentrieren sich darauf, neue und unbekannte Sicherheitslücken aufzuspüren.

Ein ganzheitliches Schutzprinzip wirkt dem entgegen. Die Konzentration liegt auf der zeitnahen Erkennung von IT-Sicherheitsproblemen und Cyberangreifern. Ist ein Unternehmen dazu in der Lage, so erzielt es maximal möglichen Schutz für seine OT und IT und sichert damit eine ständig funktionsfähige OT und IT als Grundlage für die Produktion: Risiken werden schnell erkannt und einer Behebung zugeführt. Auf Knopfdruck ist die Sicherheitslage des Unternehmens tagesaktuell und auf einem Blick erfassbar. Angreifern sind so nahezu alle Einfallstore verschlossen.

Der Schutzschirm setzt sich aus 3 Komponenten zusammen: (1) Erkennungswerkzeuge für eine automatisierte Sammlung und Analyse von sämtlichen potentiell sicherheitsrelevanten Daten aus der gesamten OT- und IT-Landschaft und eine Korrelation dieser Daten zur Erkenntnisgewinnung über ihre Relevanz für ein mögliches Sicherheitsrisiko, (2) die Analyse- und Bewertungstätigkeit von Sicherheitsexperten und (3) die Informationsaufbereitung für eine maßgeschneiderte Weiterverarbeitung zum Beispiel im Rahmen einer Risikobehebung aber zum Beispiel auch als Informationsquelle über den aktuellen Status Quo der OT- und IT-Sicherheit in einer Organisation für verschiedene interne Zielgruppen.



Komponente 1: Exzellente Erkennungswerkzeuge

Die notwendige Software für die kontinuierliche Überprüfung der OT- und IT-Sicherheit setzt sich aus Risikoerkennungsmodulen und einer Advanced Correlation Engine zusammen.

IT-Risikoerkennungsmodule

Für einen umfassenden Schutz der IT-Infrastruktur ist der Einsatz von automatisierten IT-Risikoerkennungsmodulen erforderlich:

» Log Data Analytics (LDA): Die Alarmierung bei Sicherheitsproblemen oder potentiellen Risiken durch die Sammlung, Analyse und Korrelation von Logs aus verschiedenen Quellen.

» Network Behavior Analytics (NBA): Die Erkennung von gefährlicher Malware, Anomalien und anderen Risiken im Netzwerkverkehr auf Basis von signatur- und verhaltensbasierten Detection Engines.

» Vulnerability Management and Compliance (VMC): Ein 360-Grad-Überblick über potenzielle Sicherheitsschwachstellen in Betriebssystemen und Anwendungs-Software und die Überwachung sämtlicher Datenflüsse im Netzwerk auf Anomalien.

» Software Compliance (SOCO): Die automatisierte Überwachung der Befolgung von Compliance Vorschriften und die sofortige Meldung von Verstößen zur Minimierung von Compliance-Risiken.

» Endpoint Detection and Response (EDR): Die Sammlung, Analyse und Korrelation von Server- und Client-Logs sowie die sofortige Alarmierung bei der Erkennung von Angriffen, Missbrauch oder Fehlern. Die Dateiintegrität des lokalen Systems wird geprüft und Rootkits sowie versteckte Angriffe, Trojaner oder Viren durch Systemveränderungen werden identifiziert.

» Avanced Threat Detection for Email & Web (ATD): Der Einsatz von Sandbox-Technologien der nächsten Generation zur Erkennung von "Advanced Malware" in E-Mails und bei Web Downloads.

OT-Risikoerkennungsmodule

Für einen umfassenden Schutz der OT- und IT-Infrastruktur ist der Einsatz von automatisierten OT-Risikoerkennungsmodulen erforderlich:

» Industrial Network & Behaviour Analysis: Die Identifikation von Protokollen und Applikationen im Netzwerkverkehr, die Analyse der extrahierten Daten und die Visualisierung von Anomalien schafft Klarheit über die aktuelle Lage. Die DPI (deep packet inspection) Solution R&S®PACE 2 klassifiziert und dekodiert Datenströme bis hinunter zum Content Layer. So werden auch zulässige Protokolle nach versteckten Attacken untersucht. Sicherheitsprobleme, die von infizierten Maschinen, Fehlkonfiguration oder potentiellen Cyberattacken herstammen, werden erkannt.

» Industrial System Log Collection & Analysis: Die Alarmierung bei Sicherheitsproblemen oder potentiellen Risiken durch die Sammlung, Analyse und Korrelation von Logs aus verschiedenen Quellen im OT-Umfeld.

» Selective Vulnerability Management & Assessment: Schwachstellen-Scans (Vulnerability Management and Assessment, VMC) werden in ausgewählten Bereichen und Umgebungen ausgeführt. Das Scanning verursacht keine Störungen bei der Verfügbarkeit oder Integrität von Daten kommen.

State of the art Advanced Correlation Engine

Die klassischen Abwehrmaßnahmen wie Firewalls oder Antivirensoftware erkennen nur Angriffe, wenn sie ihnen vorher bekannt sind, also ganz bestimmten Mustern folgen.

Aktuelle Angriffsformen sind jedoch oftmals nicht mehr signaturbasierend erkennbar. Sie werden nicht durch Muster sondern durch Anomalien im Verhalten der Systeme aufgespürt. Diese Auffälligkeiten werden sichtbar, wenn sämtliche Sicherheitsereignisse auf zwei Ebenen miteinander korreliert werden: auf der Ebene eines Risikoerkennungsmoduls und auf der Ebene der Cross-Korrelation der Informationen aus verschiedenen Modulen.

Advanced Correlation ist zudem die Voraussetzung zur Erkennung von verdächtigen Verhaltensweisen versteckter oder noch nicht bekannter Angriffsformen.

Für eine erfolgreiche Risikoerkennung und Alarmierung in kritischen Situationen durch die Advanced Correlation Engine müssen Regeln, Policies sowie selbsterlernte Algorithmen und statistische Modelle hinterlegt und regelmäßig erweitert werden.

Komponente 2: Expertenanalyse und -bewertung

Automatisiert gesammelte Sicherheitsinformationen müssen von Experten beurteilt werden. Sie analysieren, bewerten und priorisieren die Ergebnisse und entwickeln die Automatismen anhand neuester Informationen und Erkenntnisse ständig weiter. Dabei sollten alle Resultate als Gesamtbild betrachtet und neben den Vorkommnissen in der eigenen Infrastruktur auch aktuelle Vorkommnisse in der Branche und darüber hinaus erfasst werden.

Expertenteams müssen zudem schnelle und passgenaue Anleitungen zur Problembehebung geben und laufend alle Policies und Regeln innerhalb der Risikoerkennungsmodule und des Advanced Correlation Engines anpassen, um Schwachstellen und neue Angriffsarten schnell zu erkennen und zu eliminieren.

Komponente 3: Informationsaufbereitung

Die Erkenntnisse über die tagesaktuelle Sicherheitslage müssen zentral und in Form von detaillierten und verständlichen Berichten und Statistiken sowohl für die internen Security Teams als auch für die Unternehmensleitung präsentiert werden. Informationen müssen auf die ganz wesentlichen Vorkommnisse konzentriert werden, um die Behebung vollkommen auf das tatsächlich Wichtige zu konzentrieren. In dringenden Fällen müssen Alarmierungen bei den jeweils richtigen Stellen ausgelöst werden.

Das Frühwarnsystem für die OT und IT – selbst managen oder outsourcen?

Die automatisierte Sammlung und Auswertung von sicherheitsrelevanten Daten, die Korrelation aller Informationen, das kontinuierliche Anpassen der Regeln und Modelle sowie die Interpretation aller gewonnenen Informationen erfordert zeitliche, personelle und finanzielle Ressouren. Während sich dieser Aufwand für besonders große Unternehmen rechnen kann, ist ein Outsourcing der Risikoerkennung an externe, spezialisierte Anbieter eine attraktive Variante. Daher lohnt es, das Know-How und die Werkzeuge eines externen Spezialisten zu prüfen.

Radar Cyber Security ist europäischer Marktführer für vorausschauende OT- und IT-Sicherheitsüberprüfung und Risikoerkennung als Managed Services und als Solution. Das Unternehmen stellt seine Technologie „made in Europe“ an seine Kunden zur Verfügung, auf deren Basis dann interne Experten und Prozesse die Risikoerkennungsarbeit durchführen. Bei Managed Security Services gehen die Dienstleistungen von Radar Cyber Security weiter. Hier bietet der Spezialist die Technologie, Experten und Prozesse aus einer Hand an, die ein ganzheitliches Security Monitoring als Outsourcing ermöglichen.

Die Auslagerung von Sicherheitsleistungen bedeutet dabei keine Herausgabe von sicherheitsrelevanten und damit höchst sensiblen Daten. Radar Cyber Security stellt eine Hardware Appliance inklusive aller Module und der Advanced Correlation Engine zur Verfügung. Dort werden alle automatisiert erlangten Informationen gesammelt und analysiert. Betrieben wird diese Hardware Appliance im Unternehmensnetzwerk und stellt somit sicher, dass sicherheitsrelevante Daten physisch niemals das Kundenunternehmen verlassen. Radar Cyber Security konfiguriert und wartet kontinuierlich alle Module. Regeln für die Risikoerkennung und Korrelation werden ständig aktualisiert.

Schlussendlich werden alle wichtigen Informationen, weitgehend frei von false positives und false negatives, im Risk & Security Cockpit präsentiert. Berichte und Statistiken werden in der gewünschten Detailtiefe zur Verfügung gestellt. Alarmierungen werden in dringenden Fällen über das Cockpit, via Email und sogar als Push-Mitteilung auf das Mobiltelefon bereitgestellt. Die Experten stehen jederzeit im Rahmen eines Nachrichten- und Feedback-Systems für die Kommunikation mit den internen Security Teams zur Verfügung. Ein integrierter Business Process Risk View zeigt die von Sicherheitsproblemen gefährdeten Geschäftsprozesse auf und rundet damit das umfassende und gleichzeitig ressourcenschonende Angebot ab.

RADAR CYBER SECURITY | Safeguard your digital journey.

Radar Cyber Security ist Europas führendes Technologieunternehmen im Bereich Detection & Response. Im Mittelpunkt steht die zeitnahe Erkennung von Risiken für die Sicherheit der IT und OT von Unternehmen und Behörden als Solution oder als Managed Service. Basis dafür ist eine hochmoderne, eigenentwickelte Technologieplattform mit der Kunden ihr Cyber Defense Center (CDC) aufbauen können oder die in Kombination mit Security-Analyseexperten, bewährten Prozessen und Best Practices als CDC as a Service zur Verfügung steht. Das Ergebnis: Eine besonders effektive und effiziente Verbesserung von IT-Sicherheit und -Risikomanagement, kontinuierliches IT und OT Security Monitoring und ein auf Knopfdruck verfügbarer Überblick über die sicherheitsrelevanten Informationen in der gesamten IT- und OT-Landschaft einer Organisation.

Radar Cyber Security HQ
Zieglergasse 6
1070 Wien
Österreich

T: +43 (1) 929 12 71-0
F: +43 (1) 929 12 71-710
E: sales@radarcs.com
www.radarcs.com

Radar Cyber Security Deutschland
Taunustor 1
60310 Frankfurt am Main
Deutschland

T: +49 (69) 2443424 655
F: +49 (69) 2443424 150
E: sales_germany@radarcs.com
www.radarcs.com/de