WHITE PAPER

IRMA® - Industrie Risiko Management Automatisierung
08.2019

von Stefan Menge (Achtwerk GmbH, www.acht-werk.de) | Dieter Barelmann (VIDEC GmbH, www.videc.de)

Dem Hacker auf der Spur – nach Empfehlungen des BSI: "Monitoring & Anomalie-erkennung in Produktionsnetzwerken"

Der aktuelle Lagebericht des Bundesamtes für Sicherheit in der Informationstechnik (BSI) stellt neben den bestehenden Angriffen durch Erpressungssoftware (Ransomware wie WannaCry, Petya & Co.) die weiter zunehmende Anzahl an Advanced Persistent Threats (APT) besonders in den Fokus. Voraussichtlich werden diese zielgerichteten Cyber-Angriffe durch fortgeschrittene, gut organisierte und professionell ausgestattete Angreifer die höchste Gefährdung für Unternehmen in naher Zukunft sein.

APTs sind meist sehr komplex und werden in mehreren Phasen durchgeführt. Das Ziel eines APT ist es, über eine längere Zeitdauer vertrauliche Informationen auszuspähen oder zielgerichtet Schaden anzurichten. Diese Art von Cyber-Angriffen hat häufig einen professionellen Hintergrund (z.B. Cyber-Kriminalität oder Wirtschaftsspionage).

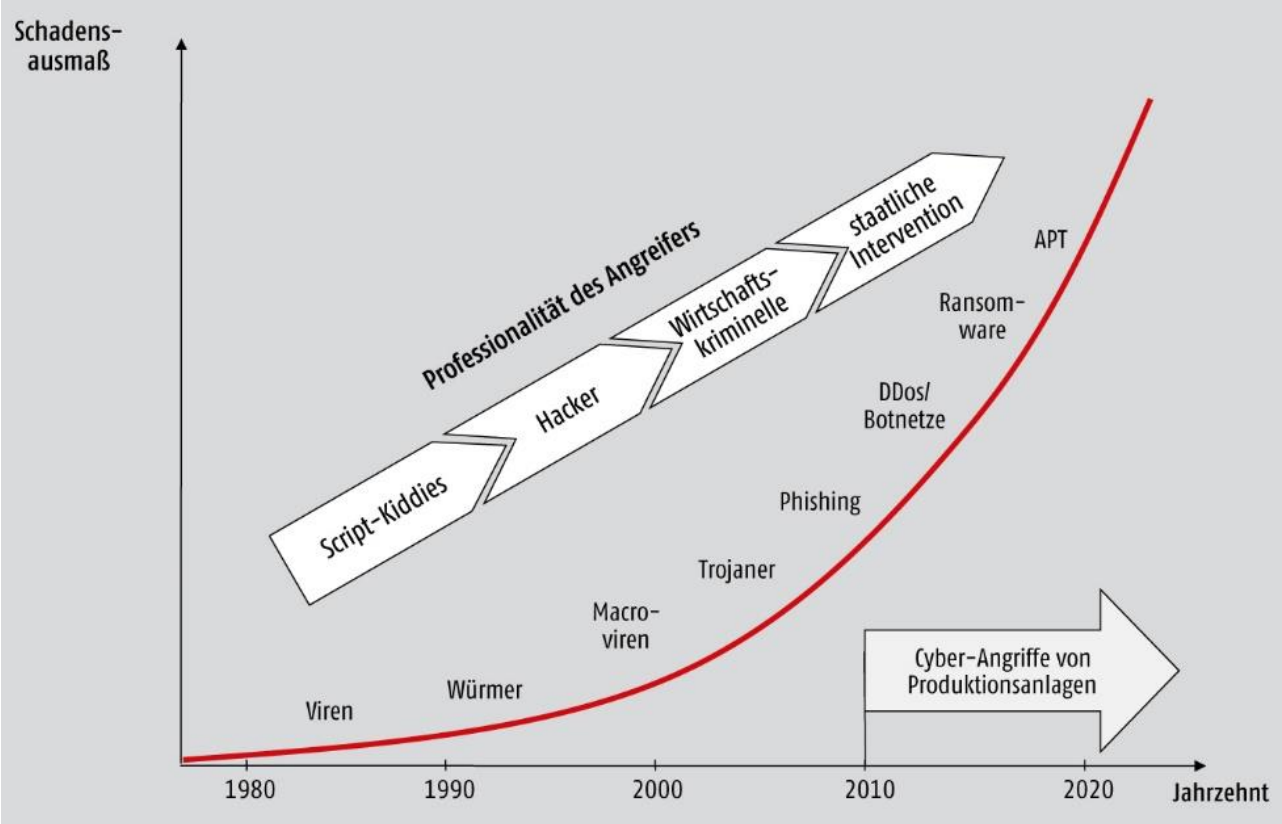

Abb: Entwicklung von Cyberangriffen

Wie stellt sich in Unternehmen und Organisationen mit vernetzten Automatisierungsanlagen der Umgang mit dieser immer weiter steigenden Bedrohungslage dar?

Das Risiko, von einem Cyber-Angriff betroffen zu sein, sowie dessen Auswirkungen werden fast immer erheblich unterschätzt.

Gerne wird vom Betreiber argumentiert, dass das eigene Unternehmen zu unbedeutend ist, um als interessantes Angriffsziel zu gelten. Trotzdem werden auch diese Unternehmen über kurz oder lang Opfer eines Cyber-Angriffs sein, je nachdem, welche Art von Angriffsziel das Unternehmen darstellt:

- Das 'einfache Ziel': Hierzu zählt, ob die Schutzeinrichtung einer Unternehmens-IT ausreichend ist, um einem ersten Angriff standzuhalten. Für Kriminelle, 'Hacktivists' und 'Script Kiddies' sind einfache Ziele lukrativer, da diese Angreifer in der Regel weniger Aufwand für eine Attacke betreiben. Für Staaten und Wettbewerber sind diese Ziele durchaus als Beifang interessant, wobei diese Angreifer meist zielgerichteter arbeiten und dann sehr intensiv attackieren!

- Das 'kollaterale Ziel': Unternehmen können sich als Beifang im Netz von Cyber-Angreifern verfangen. Die Chance besteht insbesondere, wenn Unternehmen engen Kontakt mit Kunden halten, deren Staaten oder Branchen häufig Ziel von Angreifern sind.

Es gibt also Kriminelle, 'Hacktivists' und 'Script-Kiddies' sowie Staaten oder Wettbewerber. Allen gemeinsam ist, dass sie Zeit haben – Zeit zur Vorbereitung, Zeit um Informationen zu sammeln, Zeit zum Auffinden der richtigen Werkzeuge. Dabei ist den wenigsten Angreifern der unmittelbare Schaden, den sie anrichten, bewusst. Sie probieren zunächst nur aus und erkennen erst später die Potenziale ihres Angriffs.

Mit Stuxnet sind im Jahre 2010 solche intelligenten Cyber-Angriffe in der Industrie angekommen. Die gezielt entwickelte Schadsoftware für vernetzte Automatisierungen und Produktionsanlagen findet fokussiert ihre Ziele. Dies erfolgt so intelligent, dass die eigene Verbreitung versteckt und Schäden erst viel später als Cyber-Angriff erkannt werden.

Seit 2017 ist Industroyer im Fokus von Sicherheitsexperten. Diese missbrauchen keine Lücken in den vernetzten Automatisierungsgerätschaften, sondern sprechen einfach in deren Sprache, indem sie die in Industrieumgebungen gängigen Kommunikationsprotokolle beherrschen. Dabei können Angreifer monatelang im Netzwerk aktiv sein und die notwendigen Informationen zusammentragen. Beispielsweise gehören Löschfunktionen, die sämtliche Spuren des Angriffs verwischen, Konfigurationsdateien löschen und das Betriebssystem des befallenen Windows-PCs in einen nicht startfähigen Zustand versetzen, zum Funktionsumfang.

OT Security – im Blindflug?

Man stelle sich einmal vor, wir würden heute in Produktionsnetzwerken ohne Leit- oder SCADA System Produkte herstellen wollen. Keine Sichtbarkeit, keine Kontrolle über den Prozess. Die Automatisierung läuft, jedoch kann man nichts über den Zustand der Anlage aussagen. Solch ein Zustand wäre heute kaum noch denkbar, im Bereich OT Security ist er allerdings immer noch Stand der Dinge.

Im Zuge der Digitalisierung streben Unternehmen einen immer tieferen Grad der Vernetzung von Automatisierung und damit der zunehmenden Abhängigkeit von deren Verfügbarkeit an. Das bedeutet, mit der Standardisierung der Ethernets erfolgt eine immense Erhöhung der Teilnehmer und entsprechend auch der Kommunikation. Wer jedoch mit wem kommuniziert - berechtigt oder auch nicht - ist kaum jemandem bekannt. Durch die steigende Komplexität im Netzwerk und die Implementierung von nicht immer vollständig IP-standardkonformen Geräten kommt es immer wieder zu Seiteneffekten im Netzwerk, die zunächst nicht bemerkt werden und irgendwann zu einem Störfall werden können. Dies wäre mit einer kontinuierlichen Überwachung des Netzwerkverkehrs aufgefallen und vermeidbar gewesen.

Im Bereich der OT Security gehen die meisten Investitionen allerdings in Netzwerksegmentierungen und Firewalls, der Blick auf die Anlage und die Kontrolle über die Kommunikation bleibt verwehrt. Sicherlich sind die Investitionen im klassischen Sinn der Security notwendig, jedoch in keinem Fall ausreichend. Denn wenn erst einmal ein Netzwerk z.B. über einen infizierten Programmierrechner unbemerkt befallen ist, kann sich der Angreifer weiter austoben. Sogar Schadcode nachzuladen, würde von einer Firewall nicht verhindert werden, da der Verbindungsaufbau ins Internet aus der internen Zone erfolgt. Hier hat das BSI aus Sicht der IT Sicherheit dem Hase-und-Igel-Spiel zwischen dem Angreifer und dem Schützenden einen wichtigen Impuls zugunsten des Betreibers gegeben.

Die Vorteile des passiven Monitorings, neben der Möglichkeit der Angriffserkennung, sind vielschichtig. Hier nur ein kurzer Ausschnitt: Jeder Anlagenbetreiber hat sofort alle Teilnehmer im Blick und externe Dienstleister lassen sich über die Zugänge genau kontrollieren. Zusätzlich erhält die IT wichtige Informationen für die Feinjustierung der Firewall, ein wichtiger Punkt bei der Angriffsabwehr. Bei der Alarmierung in der Angriffserkennung lässt sich der Servicebereich in der Regel optimieren und spart Kosten.

Die unterschiedlichen Ansichten über eine aktive bzw. passive Abfrage der Assets sind aus Sicht der Automatisierung sehr einfach gelöst. Die sensible Struktur der Automatisierungsgeräte mit ihren unterschiedlichen Generationen ist bei einem 24/7 Betrieb keine Spielwiese für aktive Abfragen. Das höchste Gut der OT ist die Verfügbarkeit – diese verträgt lediglich die passive Variante.

Die Kontrolle über den Prozess auf Basis eines Risikomanagements zu behalten, Sichtbarkeit der aktuellen Assets und eine Alarmierung bei Unregelmäßigkeiten in der Kommunikation sind die wichtigen Bausteine

für eine sichere Produktion. Das ist heute schon nicht nur eine Empfehlung des BSI sondern Stand der Technik.

Rechtliche Vorgaben und BSI CS-134

Grundsätzliche Anforderungen zur Erfüllung von Compliance-Vorgaben nach Gesetzen und Verordnungen sowie Branchenstandards ergeben sich u.a. aus

- den Vorgaben des Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetzes) vom 25. Juli 2015
- den einschlägigen Verpflichtungen aus dem Gesellschaftsrecht an ein Überwachungssystem in Unternehmen (KonTraG, GmbH-Gesetz, Aktiengesetz)

Dabei soll u. a. der Einsatz und Betrieb zum kontinuierlichen Erfassen und Überwachen aller informationstechnischen Systeme, Komponenten und der Vorgänge der Informationsverarbeitung in Automatisierungen mit der integrierten Möglichkeit für ein IT-Risikomanagement vorhanden sein.

Cyber-Sicherheit im Allgemeinen sowie Monitoring und Anomalieerkennung im Speziellen in der Fabrikautomatisierung und Prozesssteuerung umzusetzen, ist laut BSI angesichts zunehmender Vorfälle eine dringende Notwendigkeit. Dabei ist Monitoring im industriellen Umfeld und im Kontext dieser Cyber-Sicherheits-Empfehlung BSI-CS 134 nicht auf die bloße Zustandsüberwachung (Condition Monitoring, Process Monitoring, Alarmüberwachung) beschränkt. Es beinhaltet zudem die Beobachtung der Kommunikation zwischen Automatisierungskomponenten, zu Aktoren, Sensoren sowie von und zu Fernwirkkomponenten. Dazu gehört auch das Auslösen von Meldungen und Alarmen bei Erkennen besonderer Ereignisse, d.h. insbesondere von Anomalien. Dazu gehören u. a.

- Anschluss eines neuen Gerätes
- Datenpakete eines bisher unbekannten Gerätes
- Datenverkehr zwischen Geräten, die bisher nicht untereinander kommuniziert haben
- Datenverkehr mit einem bisher nicht verwendeten Protokoll
- Datenverkehr mit einem unüblichen oder nicht vorgesehenen Protokoll
- Verwendung unerwarteter Adressen (öffentliche IP-Adressen etc.)
- Allgemein auffällige Ereignisse wie Adress-Scans oder Port-Scans

- Änderungen der Netzwerkqualität wie z.B. hohe Bandbreitennutzung

Um Anomalien zu erkennen, muss zuvor der "Normalzustand" eines Systems – hier eines Produktionsnetzes – bekannt sein. Dazu werden – lt. BSI idealerweise passive – Sensoren (Netzwerk- oder Wiretaps) im Netzwerk bzw. im Netzwerksegment platziert, mittels derer über einen längeren Zeitraum die Daten im Netz erfasst werden können (Trainingsphase).

Ein Unterschied zwischen Aktiv und Passiv besteht darin, ob Anwendungen zum Monitoring und zur Anomalieerkennung die erforderlichen Daten rückwirkungsfrei erfassen (Passiv) oder selbst Daten im zu überwachenden Netz erzeugen (Aktiv), beispielsweise durch eigene Anfragen im Netzwerk, was natürlich mit einem gewissen Risiko in Bezug auf die Verfügbarkeit verbunden ist.

Die in der Trainingsphase gewonnenen Daten lassen sich nach verschiedensten Kriterien analysieren, kategorisieren und bewerten. Mit dieser Datenbasis als Grundlage werden nun Schwellwerte und Triggerpunkte definiert, um außergewöhnliche Zustände und Vorgänge, die vom bisher gelernten "Normalen" abweichen, zu erkennen. Zweckmäßigerweise wird ein Erkennungssystem als eigenständige und unabhängige Komponente in das zu überwachende Netzwerk integriert.

Weitergehende Informationen erhalten Sie hier:

https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_134.pdf?__blob=publicationFile&v=4

PRODUKTINFORMATION

IRMA - Industrie Risiko Management Automatisierung

Security muss übersichtlich, bedienbar und einfach sein. Dieser Anspruch gilt bei uns in der Entwicklung ebenfalls für den Bereich OT Security - seit über 5 Jahren. Das Resultat ist die komplette Erfüllung der Vorgaben des BSI CS 134 mit folgenden Kernthemen:

- Monitoring – Systematische Überwachung und Beobachtung der Kommunikation
- Anomalieerkennung in der Kommunikation (mit Archivierung, Protokollierung und Analyse)
- Angriffserkennung (Intrusion Detection) mit Alarmierung im Bedarfsfall

außerdem

- Kognitive Anomalieerkennung & sofortige IT-Visualisierung
- Kontinuierliche Überwachung mit passivem Ansatz
- Umgehender Nutzen – einfache Bedienbarkeit – einfach zu erlernen
- Integration des IT-SiG Sicherheitsstandards Wasser / Abwasser (W1060 / M1060)

Vorteile

✔ Optimale IT-Sicherheit
auf dem neuesten Stand der Technik

✔ Unmittelbare Erkennung
von Anomalien im IT-Netz

✔ Passive Überwachungsautomation

✔ Absicherung von nicht patchbaren Systemen
wie z.B. Windows NT/2000/XP, alte SPS, OPC Classic

✔ Absicherung von zertifizierten Produktionsanlagen und Prozessen
ohne Re-Zertifizierung (z.B. Pharma, Chemie, Nahrungsmittel)

✔ Sofortige Einsatzbereitschaft
durch einfache Installation und herstellerübergreifendes Konzept

✔ Vollständige Übersicht und Sicherheit
Ihrer IT-Systeme, Netzwerk- und Datenverbindungen

✔ Integriertes Alarmmanagement
für Cyber-Sicherheitsvorfälle

✔ In Echtzeit
Kontinuierliche Überwachung, Angriffserkennung und Reporting

✔ Methodisches Werkzeug
für eine zielgerichtete Risikoanalyse sowie die Unterstützung bei der Firewall Parametrierung