Cybersicherheit in der OT-Security

Die wichtigsten Gefahren in Industrieumgebungen

Inhaltsverzeichnis

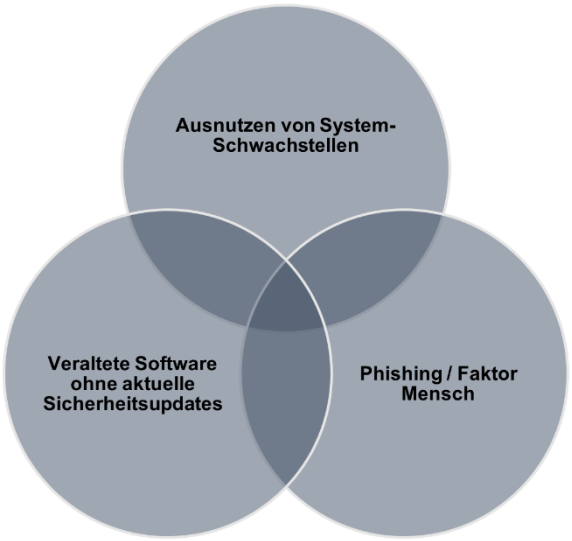
Einleitung

Cyberangriffe sind längst kein Risiko mehr, mit dem sich ausschließlich namhafte Großkonzerne auseinandersetzen sollten, sondern eines, das branchenübergreifend und in allen Betriebsgrößen vorkommt. Diese Gefahr ist den meisten Verantwortlichen inzwischen bewusst und entsprechend steigen die Investitionen in IT-Sicherheitsmaßnahmen. OT-Umgebungen werden jedoch im Bereich Cybersicherheit trotz steigender Vernetzung zum Teil noch vernachlässigt. Dafür ist unter anderem der sehr lange Lebenszyklus der Anlagen von 30 Jahren und mehr verantwortlich. Aufgrund des isolierten Betriebs von Produktionsanlagen waren diese in der Vergangenheit kaum als Angriffsziel interessant. Veraltete Betriebssysteme, welche dem Lebenszyklus der Anlage entsprachen, sowie fehlende Sicherheitsupdates stellten daher kein Problem dar, was sich inzwischen jedoch geändert hat.

Für Unternehmen ist es daher von enormer Wichtigkeit, sich der Gefahren von Cyberangriffen auch im OT-Bereich bewusst zu sein und entsprechende Sicherheitsmaßnahmen zu ergreifen. Denn mithilfe umfassender Vorbereitung und Überwachung können Angriffe erkannt und abgewehrt werden, bevor sie zu ernsthaften Problemen führen. Unserer Beobachtung nach stellen derzeit insbesondere Schwachstellen im System, veraltete Softwarekomponenten sowie Phishing-Angriffe und damit einhergehend der Risikofaktor Mensch große Bedrohungen dar.

Die wichtigsten Gefahren in Industrieumgebungen

Die hier aufgeführten Fälle von Cyberangriffen aus den genannten Risikobereichen zeigen auf, von welch enormer Bedeutung robuste Cybersecurity-Maßnahmen für den Schutz von Produktionsumgebungen sind.



1. Risiko: Ausnutzen von Schwachstellen im System

1.1 Angriff auf DCOM-Schwachstelle in Windows-basiertem OT-System erfolgreich abgewehrt

Vor kurzem meldete unser SOC einen Angriff auf ein OT-System bei einem unserer Kunden, welchen wir Dank der frühzeitigen Detektion erfolgreich abwehren konnten. Der Angreifer nutzte dabei eine Schwachstelle in der DCOM-Kommunikation des Windows-basierten OT-Systems (CVE-2021-26414), um eine Remote-Code-Ausführung zu ermöglichen, das System zu kompromittieren und so auf sensible Daten zuzugreifen.

Schwachstelle im DCOM-Protokoll sollte für Datendiebstahl genutzt werden

Das DCOM-Protokoll (Distributed Component Object Model) ist in vielen Windows-basierten Systemen, einschließlich OT-Systemen, implementiert und wird verwendet, um die Kommunikation zwischen Anwendungen auf verschiedenen Computern zu ermöglichen. Die in diesem Fall ausgenutzte Schwachstelle war eine unzureichende Überprüfung der Zugriffsberechtigungen für DCOM-Objekte. Der Angreifer konnte aufgrund dieser Schwachstelle DCOM-Objekte erstellen und ausführen, ohne dass

eine Authentifizierung oder Autorisierung stattfanden. Nachdem der Angreifer Zugang zum System erlangt hatte, wäre er somit in der Lage gewesen, Daten aus dem OT-System zu extrahieren und wichtige Informationen des Unternehmens zu stehlen. Dank der frühzeitigen Erkennung und Analyse durch unser SOC-Team konnte der Angriff jedoch rechtzeitig abgewehrt werden. Unsere Analysten im SOC haben schnell reagiert, um das Ausmaß des Angriffs zu untersuchen und das betroffene System zu isolieren. Bei einer umfassenden Analyse stellten unsere Experten fest, dass der Angreifer tatsächlich versucht hatte, sensible Daten aus dem OT-System zu extrahieren.

SOC verhindert Verlust sensibler Daten

In Zusammenarbeit mit dem Kunden konnten wir anschließend eine umfassende Sicherheitslösung für das OT-System implementieren. Unser SOC-Team hat Maßnahmen zur Absicherung des Systems ergriffen und empfohlene Sicherheitsprotokolle für zukünftige Angriffe umgesetzt. Der erfolgreiche Einsatz unseres SOC-Teams zeigt, wie wichtig es ist, eine starke Verteidigung gegen Cyberangriffe zu haben. Wir bei der Certified Security Operations Center GmbH bieten unseren Kunden eine ebenso zuverlässige wie effektive OT-Sicherheitslösung an. Fälle wie diese zeigen, dass das frühzeitige Erkennen und Abwehren von Angriffen durch unser SOC-Team, OT-Systeme effektiv schützen kann. Wir bleiben weiterhin wachsam und arbeiten hart daran, unsere Kunden gegen zukünftige Angriffe zu schützen.

1.2. OT-Security-Hack: Schwachstelle in Industrie-Steuerungscomputer (PCL) führt zu Cyberangriff

In einem unserer jüngsten Kundenfälle wurden die OT-Systeme eines deutschen Unternehmens von Hackern angegriffen und kompromittiert. Die Angreifer nutzten dafür eine Schwachstelle in einem industriellen Steuerungscomputer (PLC) aus, um Zugriff auf die OT-Systeme zu erlangen und diese zu manipulieren.

Wir reagierten schnell und instruierten den Kunden, sofort seine Incident-Response-Pläne zu aktivieren. Anschließend stellten wir ihm ein Expertenteam für die genaue Untersuchung des Angriffs zur Verfügung. Dieses konnte die von den Angreifern ausgenutzte Schwachstelle schnell identifizieren abstellen. Zu guter Letzt wurden Maßnahmen ergriffen, um die Manipulationen an den angegriffenen OT-Systemen rückgängig zu machen und die ordnungsgemäße Funktion weiterhin sicherzustellen. Weiterhin arbeitete unser Kunde eng mit Strafverfolgungsbehörden sowie anderen relevanten Organisationen zusammen, um den Vorfall zu melden und die Ursachen zu ermitteln.

Effektive Cybersecurity-Maßnahmen auch für OT-Systeme von großer Bedeutung

Dank der schnellen und effektiven Reaktion des betroffenen Unternehmens konnte Schlimmeres verhindert werden: Nennenswerte Auswirkungen auf die Produktionsprozesse oder die Sicherheit der Mitarbeiter blieben somit aus. Allerdings unterstreicht dieser Vorfall erneut die Bedeutung von robusten Cyber-Security-Maßnahmen für den Schutz von OT-Systemen. Dazu zählt der Einsatz neuester Technologien und Best Practices zur Absicherung der OT-Systeme, einschließlich der Identifizierung und Behebung von Schwachstellen, der Überwachung von Netzwerkaktivitäten sowie der Durchführung regelmäßiger Sicherheitsaudits.

Ganzheitlicher Schutz geht über das eigene Unternehmen hinaus

Darüber hinaus sollten Unternehmen ihre Mitarbeiter schulen und für die Bedeutung der OT-Security sensibilisieren, um sicherzustellen, dass sie sich der Risiken bewusst sind und dazu beitragen können, diese zu minimieren. Doch nicht nur betroffene Unternehmen selbst, sondern auch ihre Lieferanten und Dienstleister sind in der Pflicht, die hohen Standards in Bezug auf OT-Sicherheit erfüllen.

Insgesamt zeigt dieser Vorfall, dass Cyber-Security-Maßnahmen zu einer Priorität werden müssen, um die Verwundbarkeiten zu minimieren und die Widerstandsfähigkeit gegenüber Cyberangriffen zu erhöhen.

2. Risiko: Veraltete Software ohne aktuelle Sicherheitsupdates

2.1. Veraltete Betriebssysteme in 65 Prozent der Produktionsumgebungen

Laut einer kürzlich veröffentlichten Studie, welche das Security-Unternehmen Trend Micro in Auftrag gegeben hat, kommen in 65 Prozent der Produktionsumgebungen veraltete Betriebssysteme zum Einsatz – in Anbetracht des erheblichen Sicherheitsrisikos veralteter Systeme eine alarmierende Zahl. Doch warum werden veraltete Betriebssysteme überhaupt noch eingesetzt? In einigen Produktionsumgebungen machen beispielsweise Kompatibilitätsprobleme mit vorhandener Software oder Hardware einen Umstieg auf eine aktuelle Version extrem schwierig oder sogar unmöglich. Ein weiterer Grund könnte sein, dass es sich für Unternehmen als kosteneffizienter erweist, ein veraltetes System weiterhin zu nutzen, anstatt es zu ersetzen. Dass es für ältere Systeme keine Sicherheitsupdates mehr gibt, wird dabei in Kauf genommen.

Veraltete Betriebssysteme als Einfallstor für Hackerangriffe

Die Verwendung veralteter Betriebssysteme stellt für Produktionsumgebungen jedoch ein hohes Sicherheitsrisiko dar, denn Cyberkriminelle können Schwachstellen in diesen Systemen nutzen, um Zugriff auf sensible Daten oder Netzwerke zu erlangen. Auch können durch das Einschleusen von Schadsoftware Produktionsabläufe gestört oder sogar lahmgelegt werden, was für das betroffene Unternehmen hohe finanzielle Verluste nach sich ziehen kann. Um dieses Risiko zu minimieren, sollten Unternehmen sich bemühen, ihre Produktionsumgebungen auf aktuelle Betriebssysteme umzustellen – auch wenn hierfür zusätzliche Ressourcen für die Anschaffung neuer Software und das Lösen von Kompatibilitätsproblemen mit vorhandener Software oder Hardware bereitgestellt werden müssen. Zudem sollten vorhandene Systeme regelmäßig auf Sicherheitsupdates überprüft und aktualisiert werden.

Alternativlösung: Ein SOC für Produktionsumgebungen nutzen

Ist ein Unternehmen aus verschiedenen Gründen nicht in der Lage, das Betriebssystem seiner Produktionsumgebung auf den neuesten Stand zu bringen, kann die Überwachung durch ein Security Operations Center (SOC) eine Lösung sein. Ein SOC ist ein Team von IT-Sicherheitsexperten, das sich auf die Überwachung und Analyse von Sicherheitsvorfällen spezialisiert hat. Durch den Einsatz spezieller Tools und Technologien können die Experten das Netzwerk eines Unternehmens rund um die Uhr überwachen und zeitnah auf mögliche Bedrohungen reagieren. Wenn Sie sich für eine solche Lösung interessieren, beraten wir Sie gerne hinsichtlich der individuellen Ansprüche Ihrer Produktionsumgebung.

Fazit: Die Verwendung veralteter Betriebssysteme in Produktionsumgebungen stellt ein hohes Sicherheitsrisiko dar. Unternehmen sollten ihre Systeme daher, wenn möglich, auf aktuelle Betriebssysteme umstellen und diese regelmäßig auf

Sicherheitsupdates prüfen. Dies erfordert zwar zusätzliche Ressourcen, ist aber unerlässlich, um die Sicherheit von Daten und Netzwerken zu gewährleisten.

3. Risiko: Phishing / Faktor Mensch

3.1. Sicherheitsvorfall im Bereich OT bei deutschem Hersteller erfolgreich abgewehrt

Bei einem unserer jüngsten Kundenfälle wurde ein führender deutscher Hersteller Opfer einer Spear-Phishing-Kampagne im Bereich der Operational Technology (OT). Dabei gab sich der Angreifer als Lieferant des Unternehmens aus und verschickte eine legitime E-Mail mit bösartigem Anhang. Beim Öffnen des Anhangs führte sich ein PowerShell-Skript selbständig aus. Dies ermöglichte es dem Angreifer Zugang zum System und der PLC zu erlangen. Über die kodierte Meldung „Non interactive PowerShell“ erkannte unser Blue Team die Ausführung dieses Skripts und konnte sie zeitnah melden, um eine Verbreitung der Malware zu verhindern.

Funktionalität des Angriffs

Zu Beginn wartet das Skript zunächst fünf Sekunden, bevor es ausgeführt wird. Es folgt der Aufruf einer Reihe schadhafter URLs, mit dem Versuch, hier Schadcode herunterzuladen. Ist der Download erfolgreich, wird die heruntergeladene Datei ausgeführt. Schlägt der Download fehl, wird das Skript erneut fünf Sekunden lang pausiert und es folgt anschließend der Versuch, die nächste URL in der Liste aufzurufen.

Schützen Sie sich durch umfassende Sicherheitsmaßnahmen

Durch erhöhte Sicherheitsmaßnahmen und Mitarbeiter-Schulungen will das Unternehmen solche Angriffe in Zukunft vermeiden.

Grundsätzlich empfehlen wir allen Herstellern, die OT nutzen, die Implementierung eines mehrschichtigen Sicherheitsansatzes. Dieser sollte die Schulung der Mitarbeiter, die Implementierung von Sicherheitsmaßnahmen wie Firewall- und Antiviren-Software, die Überwachung des Netzwerkverkehrs sowie die regelmäßige Aktualisierung der OT-Systeme beinhalten.

Für Unternehmen, die PLCs und andere OT-Geräte einsetzen, ist es von enormer Wichtigkeit, sich der Gefahren von Cyberangriffen bewusst zu sein und entsprechende Sicherheitsmaßnahmen zu ergreifen. Denn mithilfe richtiger Vorbereitung und Überwachung können Unternehmen Angriffe erkennen und abwehren, bevor sie zu ernsthaften Problemen führen.

Fazit & Empfehlungen

Insgesamt zeigen diese Vorfälle, dass Cybersecurity-Maßnahmen nicht nur in der IT, sondern auch im Produktionsumfeld zu einer Priorität werden müssen, um Verwundbarkeiten zu minimieren und die Widerstandsfähigkeit gegenüber Cyberangriffen zu erhöhen. Sie zeigen aber auch, dass das frühzeitige Erkennen und Abwehren von Angriffen OT-Systeme effektiv schützen kann.

Wir bei der Certified Security Operations Center GmbH bieten unseren Kunden mit unserem SOC eine ebenso zuverlässige wie effektive OT-Sicherheitslösung an. Grundsätzlich empfehlen wir aber allen Produktionsunternehmen die Implementierung eines ganzheitlichen Sicherheitsansatzes. Dieser sollte neben einem System zur Angriffserkennung auch die Schulung der Mitarbeiter, die Implementierung von Sicherheitsmaßnahmen wie Firewall- und Antiviren-Software sowie die regelmäßige Aktualisierung der OT-Systeme beinhalten. Insbesondere die Sensibilisierung von Mitarbeitern für die Bedeutung der OT-Security ist unerlässlich für das Risikobewusstsein aller Beteiligten. Denn nicht nur die Technik, auch der Mensch selbst kann dazu beitragen, das Risiko von erfolgreichen Cyberangriffen zu minimieren.

Wünschen Sie sich mehr Informationen zum Thema Cybersicherheit in OT-Umgebungen oder zu unserem Angebot? Schauen Sie sich gerne auf unserer Webseite um und kontaktieren Sie uns bei weiterführenden Fragen.

Weitere Informationen

Sie haben Fragen zu diesem Report oder möchten mehr über das Thema SOC erfahren? Für weitergehende fachliche Erörterungen der in diesem Report angesprochenen Themen oder zu ergänzenden Aspekten stehen Ihnen gerne die Experten der Certified Security Operations Center GmbH zur Verfügung.

Ihr Ansprechpartner:

Fred Schmidt
Diplom Betriebswirt (FH)
Principal Account Manager

Certified Security Operations Center GmbH
Ein Joint Venture aus TÜV TRUST IT GmbH Unternehmensgruppe TÜV AUSTRIA &
dhpg IT-Services GmbH

Telefon: +49 (0) 151 29149649
E-Mail: fred.schmidt@csoc.de

www.csoc.de

Certified Security Operations Center GmbH
Adenauerallee 45-49
53332 Bornheim