FORTINET

WHITEPAPER

Zerstörerisch und kostspielig: Verschärfte Bedrohungslage gefährdet Betriebstechnologie (OT)

Angriff auf Schwachstellen in OT-Systemen

Zusammenfassung

Network-Operations-Analysten für Betriebstechnologie (OT) sind mit einer verschärften Bedrohungslage konfrontiert. Bekannte Angriffsformen und hochkomplexe Exploits häufen sich, da Cyber-Kriminelle verstärkt industrielle Ziele mit anfälligen Altsystemen attackieren. Verschlimmert wird die Lage durch die Konvergenz von IT und OT, die Betriebstechnologie vermehrten Angriffen aussetzt. Schuld daran ist der Wegfall des Air Gaps – des schützenden „Luftspalts", der bislang OT- und IT-Umgebungen trennte und der zur Absicherung eines Netzwerk-Rands entwickelt wurde, den es in dieser Form nicht mehr gibt. Die Folge ist, dass Malware und andere Cyber-Attacken an Häufigkeit und Stärke zunehmen. Unternehmen sind dadurch nicht nur einem höheren Risiko durch Betriebsunterbrechungen ausgesetzt, sondern haben ein existenzielles Sicherheitsproblem: Gefährdet sind die Systeme, von denen jedes Unternehmen mit Betriebstechnologie abhängig ist.

Bedrohungen wie Port-Scanning, bösartige DNS-Abfragen, anormale Header und ungewöhnlich viele Verbindungen zwischen Geräten wurden an mehr als einem von fünf Standorten beobachtet.[1]

Einleitung: Cyber-Angriffe werden immer ausgefeilter und weitreichender

Trotz Investitionen in Cyber-Security-Technologie und Richtlinien zum Schutz von Steuerungstechnik (ICS) haben Network-Operations-Analysten mit zunehmend ausgefeilterten Angriffen auf Betriebstechnologie (OT) zu kämpfen. Cyber-Kriminelle fahren aggressive Angriffsstrategien mit hochkomplexen Attacken, die in immer kürzerer Zeit entwickelt und ausgeführt werden – schneller als Analysten reagieren können. Erfolgreiche Exploits führen zur Sabotage und Störung industrieller Umgebungen in allen Branchen, von Kraftwerken, Öl- und Gas-Raffinerien bis hin zur Schwerindustrie.

Während bewährte Angriffsmethoden wie Phishing, DDoS (Distributed Denial-of-Service) oder der Diebstahl von Anmeldedaten weiterhin erfolgreich sind und sogar weiterentwickelt werden, kommen unablässig neue Bedrohungen hinzu. Die Angreifer scheinen immer einen Schritt voraus zu sein, strategisch zu denken und mit jedem neuen Angriff eine „Nutzenmaximierung" zu verfolgen. Daher überrascht es kaum, dass fast drei Viertel der OT-Unternehmen im Vorjahr mindestens einen Sicherheitsvorfall meldeten, der zu Datenverlusten, Betriebsstörungen, Ausfällen und Reputationsschäden führte.[2]

Angesichts dieser hochkomplexen Angriffsformen haben Network-Operations-Analysten bei der Entwicklung und Realisierung hochverfügbarer, zuverlässiger und sicherer OT-Systeme allen Grund zur Sorge – zumal viele SCADA/ICS-Systeme und -Geräte jetzt mit IT-Netzwerken verbunden sind. Das Problem verschärft sich noch durch die ständige Einführung neuer Anwendungen und Software-Funktionen im Unternehmen. Denn dadurch steigt die Anzahl der Verbindungen – und damit auch das Gesamtrisiko.

Erst kommt der Späh-Trupp, dann der Angriff: Wie Cyber-Kriminelle neue Angriffsvektoren und Schwachstellen bei Betriebstechnologie ausnutzen

Bei Betriebstechnologie (OT) ist Malware die häufigste Angriffsform (77 %), gefolgt von Phishing (45 %), Spyware (38 %) und Sicherheitsverletzungen bei Mobilgeräten (28 %).[3] Speziell bei Malware setzen Cyber-Kriminelle heutzutage Automatisierungen ein, um bestimmte Schwachstellen zu finden und anzugreifen. Zugleich implementieren sie unterschiedlichste Exploits, die sich jederzeit automatisch aktualisieren lassen. Da in vielen OT-Umgebungen Best Practices bei der Security vernachlässigt werden, lohnt sich für Cyber-Kriminelle das „Malware-Recycling" – eine Wiederverwendung altbekannter Malware –, um OT-Schwachstellen auszunutzen. Im Folgenden werden einige Angriffsmethoden beschrieben, die Cyber-Kriminelle derzeit gegen OT-Umgebungen einsetzen:

Quer durchs Netzwerk: Laterale Schwachstellensuche und Angriffe

Eine Taktik, die ins Netzwerk eingedrungene Angreifer anwenden, ist die Suche nach neuen Schwachstellen. Dies ist besonders effektiv bei frisch vernetzten OT-Systemen. Zuerst testen die Angreifer eine Vielzahl älterer Malware auf wenigen Computern. In der Angriffsphase werden dann sehr viele Rechner im Netzwerk mit Exploits attackiert, die in der „Testphase" gut funktioniert haben.

Per Remote-Access bewegen sich die Cyber-Kriminellen anschließend quer durch das Netzwerk (mit dem Ost-West-Verkehr), wechseln von IT- in OT-Netzwerke und können sich so unentdeckt in der Umgebung ausbreiten.

Remote-Desktop-Protokoll (RDP)

Einer der beliebtesten Ransomware-Exploits ist das RDP. Angreifer gelangen mit Anmeldedaten in das Netzwerk, die sie mit Phishing, Social Engineering, Brute-Force-Angriffen oder durch das simple Abfangen von Klartext-Passwörtern gestohlen haben.[4] Erst letztes Jahr haben Security-Experten ein neues Botnetz entdeckt, über das Millionen mit dem Internet verbundene Windows-Systeme mit einer RDP-Verbindung angegriffen wurden.[5]

2019 verzeichnete ein großes Technologie-Unternehmen einen Anstieg um 200 % bei destruktiver Malware – Cyber-Angriffe, die über das Abgreifen von Informationen hinausgehen und auf physische Schäden abzielen. Rund die Hälfte dieser Angriffe betraf die Industrie.[7]

Schwachstellen in Protokollen

Der gezielte Angriff auf die schwächsten Elemente eines Protokolls gehört ebenfalls zu den – leider oft erfolgreichen – Taktiken von Cyber-Kriminellen. Durch die zunehmende Vernetzung verschärfen sich strukturelle Probleme vieler OT-Umgebungen infolge fehlender Schutzstandards und schlechter Sicherheitspraktiken. Zu lange hatte man sich auf den „Air Gap“ verlassen, der Betriebstechnologie früher vor äußeren Gefahren abschirmte. Beim Datenverkehr ist das mit Abstand am häufigsten angegriffene Protokoll OPC Classic – der Vorgänger von OPC UA, der aber heutzutage weiterverbreitet ist.[6] Dieses Protokoll verwendet Technologien, die größtenteils Ende der 1990er und 2000er Jahre entwickelt wurden. Allein die Verbreitung von OPC-Systemen und ihre entwicklungsbedingte Isolation machen sie zu verlockenden Angriffszielen.

BACnet ist das am zweithäufigsten angegriffene Protokoll, gefolgt von Modbus, einem Kommunikationsprotokoll, mit dem verschiedene OT-Systemkomponenten effektiv interagieren können. Angriffe auf Modbus sind für OT-Teams besonders schwer zu erkennen, zu verfolgen und zu bekämpfen, da es viele Iterationen von unterschiedlichen Anbietern gibt.

Angriffe auf die Industrie nehmen an Häufigkeit und Zerstörungskraft zu

In den letzten Jahren gab es weltweit eine schockierende Anzahl von Angriffen auf kritische Infrastrukturen sowie viele Sicherheitsvorfälle, die nur knapp abgewendet werden konnten. Im Folgenden finden Sie einige ausgewählte Exploits, mit denen Network-Operations-Analysten in heutigen risikobehafteten OT-Umgebungen konfrontiert sind:

Cyber-Angriffe mit ausgefallenen Bezeichnungen

Stuxnet, Havex, Industroyer, TRITON/TRISIS – hinter diesen Bezeichnungen verbergen sich Exploits, die sich speziell gegen Betriebstechnologie (OT) richten. Industroyer und Havex sollen 2016 von russischen Streitkräften als Cyber-Waffen gegen das ukrainische Stromnetz eingesetzt worden sein. Seitdem hat sich die Malware verbreitet und wird immer wieder für Angriffe auf viele andere Netzwerke mit derselben Schneider Electric-Infrastruktur verwendet.[8]

Ausgenutzte Sicherheitslücken in der OT-Infrastruktur

Ende 2019 wurden in Wind River VxWorks – einem vertrauenswürdigen Echtzeit-Betriebssystem (RTOS, Real-Time Operating System) auf über 2 Milliarden Embedded-Geräten – viele Sicherheitslücken entdeckt, die Datendiebstahl, DDoS-Angriffe und andere bösartige Aktionen ermöglichten. Über 200 Millionen Geräte waren betroffen, darunter geschäftskritische SCADA-Systeme und andere Hardware in Industrie-Umgebungen, aber auch Firewalls und Drucker in Unternehmen sowie Medizintechnik im Gesundheitswesen – wie Geräte zur Patientenüberwachung und MRT-Anlagen.[9]

Malware-as-a-Service (MaaS)

Seit kurzem werden zwei bedeutende Ransomware-Familien – Sodinokibi und Nemty – als MaaS angeboten. Sodinokibi ist eine Malware, die sich ständig weiterentwickelt und Systeme über Software-Konsolen für das Remote-Management infizieren kann. Emotet (einer der schlimmsten Trojaner im Bankwesen) ist jetzt ebenfalls „as a Service“ erhältlich: Damit können Angreifer auf Geräte, die mit dem Emotet-Trojaner infiziert sind, weitere Malware wie den Trickbot-Trojaner oder die Ryuk-Ransomware einschleusen.

DDoS-Angriffe

Ein in Utah ansässiges Unternehmen für erneuerbare Energien mit Wind- und Solarkraftwerken in drei US-Bundesstaaten wurde Opfer eines DDoS-Angriffs, der die Kommunikation zu diesen Standorten kurzzeitig unterbrach. Dadurch konnten die Betreiber mehrere Stunden nicht mehr in 5-Minuten-Intervallen mit den Kraftwerken kommunizieren.[10] Dieser Angriff war wahrscheinlich der erste offizielle Cyber-Sicherheitsvorfall, der eine Störung der US-Energiewirtschaft gemäß der Definition des US-Energieministerium verursachte.[11]

Klassischer Schutz versagt bei hochentwickelten Bedrohungen

Cyber-Kriminelle entwickeln und implementieren automatisierte, scriptbasierte Exploits, durch die Angriffe sehr viel schneller und verheerender werden. Möglich wird dies durch die wachsende Anzahl an IoT-Geräten (Internet der Dinge) und die stärkere Einbindung von Betriebstechnologie (OT) in Netzwerk-Infrastrukturen. Aufgrund älterer Technologien und der mangelhaften Sicherheit von OT-Systemen können Network-Operations-Analysten diesen hochkomplexen Bedrohungen nur wenig entgegensetzen. Fakt ist, dass der OT-Bereich heute noch mit Sicherheitsproblemen zu kämpfen hat, die im IT-Sektor längst gelöst sind, und stark unter lateralen Angriffen leidet, die sich quer im Netzwerk mit dem Ost-West-Datenverkehr verbreiten.

Doch damit nicht genug: Auch Cyber-Kriminelle arbeiten zunehmend mit künstlicher Intelligenz (KI), um Netzwerke automatisch abzubilden, Schwachstellen einzuschätzen, Angriffsmethoden auszuwählen und Penetrationstests durchzuführen. Das Ziel sind maßgeschneiderte, automatisierte Angriffe.[12] Und je mehr Netzwerke mit hochkomplexen Technologien wie KI arbeiten, desto schwieriger wird die Abwehr von Angriffen, wenn Cyber-Kriminelle ebenfalls diese Technologien einsetzen.

Auch IoT-Geräte tragen maßgeblich zu den vermehrten Angriffen auf Betriebstechnologie bei. Einer der Hauptgründe sind die unzähligen Sensoren und Geräte, die mit der Steuerungstechnik des Unternehmens verbunden sind. Positiv betrachtet bringen diese neuen Technologien Verbesserungen bei Effizienz, Produktivität, Produktionsflexibilität, Betriebszeit und Transparenz. Zugleich erhöhen aber digitale Innovationen auch die Anzahl der Angriffe erheblich, da Cyber-Kriminelle weitaus mehr IP-basierte Geräte und Schnittstellen infiltrieren können.

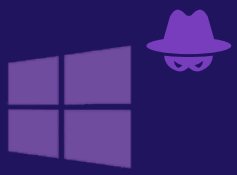
Immer mehr Bedrohungen haben ernste Folgen für Betriebstechnologie

Network-Operations-Analysten für den OT-Bereich müssen zwischen geschäftlichen und gesellschaftlichen Konsequenzen abwägen. Bei IT-Netzwerken zielen viele Angriffe auf Datendiebstahl ab. Doch bei Betriebstechnologie können heutige und künftige Sicherheitsverletzungen die gesamte Steuerungstechnik gefährden, mit der kritische Infrastrukturen betrieben werden.

Erfolgreiche Angriffe auf Kraftwerke, Erdgas-Pipelines oder Kernreaktoren können katastrophale Folgen haben. Längere Stromausfälle, Behinderungen im Verkehrs- und Transportwesen und sogar eine eingeschränkte Frischwasserversorgung sind denkbar. Ohne Strom gibt es kein Internet, keine Bankgeschäfte, keine Kommunikation – sondern nur Chaos und Störfälle.[15] Laut dem US-Geheimdienst stellen Cyber-Bedrohungen ein wachsendes Risiko für die öffentliche Gesundheit, Sicherheit und den Wohlstand dar, das durch die zunehmende Integration von IT-Technologien in kritische Infrastrukturen, wichtige landesweite Netzwerke und Unterhaltungselektronik steigt.[16]

Alarmierend sind auch die weltweiten Angriffe ausländischer Regierungen auf kritische Infrastrukturen wie Kraftwerke und Stromnetze. Russland, China, Nordkorea und Iran verfügen bekanntermaßen über spezielle Cyber-Waffen und zeigen trotz Abmahnungen keinerlei Anzeichen, sich bei Cyber-Aktivitäten zurückzuhalten.[17] Auch IoT-Botnetze – wie Tor-ähnliche Kommunikationsinfrastrukturen – werden zunehmend von staatlichen Gruppen genutzt.[18]

Auch wenn ultraschnelle DDoS-Angriffe mit einer Reflexion/Verstärkung in Terabytes pro Sekunde (TBPS) Schlagzeilen machen, können kleine, scheinbar harmlosere DDoS-Angriffe ein ebenso hohes Risiko darstellen.[13]



2019 wurden mehrere kritische Windows-Sicherheitslücken wie BlueKeep oder DejaBlue entdeckt, mit denen Angreifer wegen Fehlern im RDP die Systeme vollständig kontrollieren können.[14]

Das britische National Security Centre wehrt nach eigenen Angaben pro Woche etwa 10 Cyber-Angriffsversuche aus feindlichen Staaten ab.[19]

Fazit

Nicht nur die Geschäftswelt und die Industrie setzen mit digitalen Technologien auf schnelle Innovationen. Auch Cyber-Kriminelle lernen ständig dazu, eignen sich neue Techniken an, dringen unbemerkt in Systeme ein – und verstecken sich manchmal monate- oder jahrelang in Netzwerken, bevor sie zuschlagen.

Die Bedrohungslage wird immer umfassender, komplexer und ändert sich in rasantem Tempo. Angreifer stellen sich darauf ein und optimieren ihr Vorgehen unablässig, damit Angriffe Unternehmen noch verheerender ins Mark treffen. Multivektor-Angriffe mit

intelligenter Software, DDoS-Angriffe in Terabits pro Sekunde, das Scannen und Ausnutzen von Schwachstellen mit künstlicher Intelligenz und maschinellem Lernen, bevor ein Patching möglich ist – das alles und noch viel mehr ist schon heute Realität.

Da der Air Gap keine schützende Barriere mehr zwischen Angreifern und OT-Umgebungen darstellt, müssen Network-Operations-Analysten diese hochkomplexen Bedrohungen kennen, verstehen und bekämpfen. Das gelingt aber nur, wenn die richtigen Security-Technologien und Best Practices implementiert werden.

[1] „2020 Global IoT/ICS Risk Report". CyberX, 2019.

[2] „Fortinet 2019 Operational Technology Security Trends Report: An Update on the Threat Landscape for ICS and SCADA Systems". Fortinet, 8. Mai 2019.

[3] „Bericht zum Stand der operativen Technologie und der Cyber-Sicherheit". Fortinet, 10. September 2019.

[4] „2020 Global IoT/ICS Risk Report". CyberX, 2019.

[5] Catalin Cimpanu: „A botnet is brute-forcing over 1.5 million RDP servers all over the world". ZDNet, 6. Juni 2019.

[6] „Bericht zum Stand der operativen Technologie und der Cyber-Sicherheit". Fortinet, 10. September 2019.

[7] Peter Maloney: „Cybersecurity focus has shifted to critical infrastructure". American Public Power Association, 25. Oktober 2019.

[8] Lindsey O'Donnell: „Ransomware Behind Norsk Hydro Attack Takes On Wiper-Like Capabilities". Threatpost, 27. März 2019.

[9] „Fortinet Threat Landscape Report Q3 2019". Fortinet, 2019.

[10] Kelly Jackson Higgins: „ICS/SCADA Attackers Up Their Game". Dark Reading, 15. Februar 2019.

[11] Sean Lyngaas: „Utah renewables company was hit by rare cyberattack in March". Cyberscoop, 31. Oktober 2019.

[12] Aamir Lakhani: „The Role of Artificial Intelligence in IoT and OT Security". CSO, 30. Oktober 2018.

[13] Rodney Joffe: „Small DDoS Attacks on the Rise: Why These Supersized Assaults Are Going Tiny". Security Magazine, 21. November 2019.

[14] „2020 Global IoT/ICS Risk Report". CyberX, 2019.

[15] Damiano Bolzoni: „Keeping the Energy Sector Secure Amidst Growing OT Threats". IoT World Today, 18. Juni 2019.

[16] „National Intelligence Strategy of the United States of America". Office of the Director of National Intelligence und United States Intelligence Community, 2019.

[17] Kate O'Flaherty: „Cyber Warfare: The Threat From Nation States". Forbes, 3. Mai 2018.

[18] „2019 Cyber Threat Outlook". Booz Allen Hamilton, 2019.

[19] Beatrice Christofaro: „Cyberattacks are the newest frontier of war and can strike harder than a natural disaster. Here's why the US could struggle to cope if it got hit." Business Insider, 23. Mai 2019.

7. Dezember 2020, 13:21 Uhr

501171-0-1-DE