THREATQUOTIENT™

ThreatQ™ für kritische Infrastrukturen

Hacker greifen unermüdlich kritische Infrastrukturen auf der ganzen Welt an und kompromittieren die industriellen Kontrollsysteme (Industrial Control System, ICS) sowie SCADA-Systeme (Supervisory Control and Data Acquisition), die diese Infrastrukturen steuern. Im Jahr 2010 infiltrierte der Wurm Stuxnet zahlreiche SCADA-Systeme und beschädigte die Atomkraftanlagen im Iran. Fünf Jahre später wurde mit dem BlackEnergy-Hackerangriff auf die ukrainische Stromversorgung der erste Cyberangriff bekannt, der einen Blackout verursachen konnte.

Zu den kritischen Infrastrukturen gehören jedoch nicht nur das Stromnetz, sondern auch Bereiche wie Militär, Fertigung, Gesundheitswesen, Transport, Wasserversorgung und Nahrungsmittelproduktion, um nur einige zu nennen. Im Jahr 2017 zog der Ausbruch der Ransomware WannaCry etliche Gesundheitsunternehmen in Mitleidenschaft. Im Jahr 2018 gab das US-CERT zusammen mit dem britischen National Cyber Security Centre (NCSC) und dem FBI die Warnung heraus, dass die russische Regierung einen Angriff auf kritische Infrastrukturen in verschiedensten Branchen durchgeführt hätte.[1] Und über mehrere Jahre hinweg hielten sich Meldungen über Bedrohungen für Flugbuchungs- und öffentliche Nahverkehrssysteme in den Schlagzeilen. Anfang 2019 begann die Ransomware-Variante LockerGoga, die Produktionsprozesse von Chemiefirmen und Aluminiumherstellern zu infiltrieren und zu stören.

2/3
DER IT-MANAGER AUS DER ÖL- UND GASINDUSTRIE STIMMEN ZU

Mehr als zwei Drittel der von Accenture befragten IT-Manager aus der Öl- und Gasindustrie gaben an, dass sie aufgrund der Digitalisierung (der Bereitstellung digitaler Technologien zur erweiterten Automatisierung) anfälliger für Sicherheitsverletzungen sind.[4]

WICHTIGE HERAUSFORDERUNGEN

RESSOURCEN

Laut einer Untersuchung von (ISC)[2] fehlen weltweit fast 3 Millionen Cybersicherheitsexperten und fast 60 % der 1.452 Umfrageteilnehmer gaben an, dass für ihr Unternehmen ein mittleres bis großen Risiko von Cybersicherheitsangriffen besteht.[2] Die vorhandenen Sicherheitsteams sind kaum in der Lage, die unzähligen Warnmeldungen zu bearbeiten. Zudem sind sie auf oberer Managementebene häufig nicht ausreichend vertreten, um für wichtige Initiativen die nötige Aufmerksamkeit und Unterstützung zu erhalten. So gaben nur 31 % der Befragten aus der Luftfahrtindustrie an, über einen dedizierten CISO zu verfügen.[3] Damit Sicherheitsteams ihre vorhandenen Ressourcen optimal nutzen können, müssen sie die Bedrohungsdaten und Warnmeldungen innerhalb des Kontexts ihres Unternehmens verstehen und priorisieren können. Damit haben die Teams die Chance, relevante Sicherheitsprobleme gegenüber der Unternehmensführung einfach und deutlich zu kommunizieren und für die Verbesserung der Sicherheitsprozesse erforderliche zusätzliche Ressourcen zu begründen.

Unternehmen, die Mitarbeiter für ICS-Sicherheit mit den richtigen Kenntnissen suchen

58 %
STIMMEN ZU

58 % der befragten Unternehmen gaben an, dass die Suche nach Experten für ICS-Cybersicherheit mit den erforderlichen Kenntnissen sich sehr schwierig gestaltet.[6]

BEDROHUNGSLANDSCHAFT

Immer mehr Angriffe nutzen parallel mehrere Vektoren und erschweren die Abwehr. Die oben erwähnte Warnung des US-CERT nannte eine Vielzahl genutzter Taktiken, Techniken und Prozeduren (TTPs), einschließlich Spearphishing-E-Mails, Watering-Hole-Angriffe, Anmeldedaten-Erfassung und spezifische Angriffe auf ICS- und SCADA-Infrastrukturen. Gleichzeitig wächst die Angriffsfläche, da die Betreiber kritischer Infrastrukturen verstärkt in die Cloud wechseln und Mobilgeräte sowie IoT-Geräte einführen. So gaben mehr als zwei Drittel der IT-Manager aus der Öl- und Gasindustrie an, dass sie aufgrund der Digitalisierung (der Bereitstellung digitaler Technologien zur erweiterten Automatisierung) anfälliger für Sicherheitsverletzungen sind.[4] Unternehmen können ihre digitale Landschaft nur dann vor Bedrohungen schützen, wenn sie einen Überblick über die gesamte Infrastruktur sowie die Möglichkeit besitzen, Threat Intelligence kontinuierlich neu auszuwerten und zu priorisieren.

VERALTETE INFRASTRUKTUR

Viele ICS- und SCADA-Systeme sind bereits seit Jahren im Einsatz und verfügen nicht über Sicherheitsfunktionen, die vor aktuellen Bedrohungen schützen können. Die Zahl der gemeldeten Schwachstellen in SCADA-Systemen stieg im Jahr 2018 gegenüber 2017 deutlich an.[5] Diese Systeme werden jedoch selten aktualisiert, da die Betreiber Unterbrechungen befürchten. Trotz der zunehmenden Angriffe auf kritische Infrastrukturen wurde der Schutz nicht erweitert. Vielmehr ist er noch schlechter geworden, da die Geräte und Systeme zunehmend mit dem Internet verbunden werden, ohne die Auswirkungen auf die Sicherheit zu beachten. Obwohl die Verantwortlichen für Informationstechnologie (IT) und operative Technologie (OT) unterschiedliche Ziele, Prozesse, Tools und Konzepte haben, müssen sie zusammenarbeiten, da ihre Umgebungen immer stärker zusammenwachsen.

59 % der befragten Betreiber kritischer Infrastrukturen waren Ziel komplexer Mehrvektor-Angriffe.[7]

VERBESSERTER SCHUTZ FÜR KRITISCHE INFRASTRUKTUREN

Mehr als 75 % der befragten Unternehmen gaben an, dass es sehr wahrscheinlich oder zumindest relativ wahrscheinlich ist, dass sie Opfer eines Cybersicherheitsangriffs auf OT/ICS-Systeme werden. Dennoch halten nur 23 % die brancheneigenen oder gesetzlichen Mindestanforderungen für die Cybersicherheit von ICS-Systemen ein.[6]

Nachrichtenmeldungen über Angriffe auf kritische Infrastrukturen werden schnell als Sensation dargestellt. Es ist häufig schwer, die Fakten hinter der Sensationsmeldung zu finden und zu erfahren, welche Auswirkungen eine groß angelegte Cyberkampagne auf das Unternehmen wirklich hat. Mit der Aktualisierung der ICS- und SCADA-Geräte allein ist es nicht getan. Nur mit einer zuverlässigen Bedrohungsdaten-Plattform können Unternehmen die wirklich relevanten Bedrohungen erkennen und darauf reagieren. Dadurch können sie mit den vorhandenen Ressourcen – Sicherheitsinfrastruktur und Personal – schneller mehr erreichen.

1. CISA (Cybersecurity and Infrastructure Security Agency): „Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors“, 2018, https://www.us-cert.gov/ncas/alerts/TA18-074A
2. (ISC)²: „Cybersecurity Workforce Study“, 2018, https://www.isc2.org/Research/Workforce-Study#
3. SITA: „Air Transport Cybersecurity Insights“, 2018 https://www.sita.aero/resources/type/surveys-reports/air-transport-cybersecurity-insights-2018
4. iDefense: „Managing Malware | Crashoverride/Industroyer Malware Assessment“, 2017, https://www.accenture.com/t20180110T142438Z__w__/us-en/_acnmedia/PDF-69/Accenture-Managing-Malware-Crash-Override.pdf
5. Risk Based Security: „2018 Vulnerability Trends“, 2018, https://pages.riskbasedsecurity.com/hubfs/Reports/2018/Risk%20Based%20Security_2018%20Year%20End%20Vulnerability%20QuickView%20Report.pdf
6. Wolfgang Schwab, Mathieu Poujol: „The State of Industrial Cybersecurity 2018“, 2018, https://ics.kaspersky.com/media/2018-Kaspersky-ICS-Whitepaper.pdf
7. Philippe Alcoy, Steinthor Bjarnason, Paul Bowen, C.F. Chui: „Insights into the Global Threat Landscape“, 2018, https://pages.arbornetworks.com/rs/082-KNA-087/images/13th_Worldwide_Infrastructure_Security_Report.pdf

GEORDNETERE SICHERHEITSABLÄUFE FÜR PROZESSE BEI KRITISCHEN INFRASTRUKTUREN

Die ThreatQ-Plattform liefert Betreibern kritischer Infrastrukturen den Kontext sowie die Sicherheit, die für fundiertere Entscheidungen, schnellere Erkennung und Reaktion sowie für die erweiterte Zusammenarbeit der Teams und Schulungen für fortlaufende Verbesserungen erforderlich sind. Sie müssen keine bestehenden Sicherheitsinfrastrukturen oder Abläufe ändern, da alle Tools und Technologien nahtlos mit der offenen Architektur von ThreatQ zusammenarbeiten.

MIT THREATQ MEHR ERREICHEN:

- **KONSOLIDIERUNG** aller Quellen für externe (z. B. OSINT) und interne (z. B. SIEM) Bedrohungs- und Schwachstellendaten in einem zentralen Repository
- **ERFASSUNG** von Informationen zur Sicherheitslage der gesamten Infrastruktur (lokal, Cloud, IoT, Mobilgeräte und ältere Systeme) durch die Integration der Schwachstellendaten und Threat Intelligence im Kontext aktiver Bedrohungen
- **AUSSORTIERUNG** nicht relevanter Informationen, Vermeidung von Ermüdung aufgrund zu vieler Warnmeldungen und einfache Navigation in enormen Mengen von Bedrohungsdaten zur Konzentration auf wichtige Ressourcen und Schwachstellen
- **PRIORISIERUNG** der Aspekte, die in Ihrer Umgebung am wichtigsten sind, und erneute Priorisierung, wenn neue Daten und Erkenntnisse verfügbar werden
- **PROAKTIVE SUCHE** nach böswilligen Aktivitäten, die schädliches Verhalten, Denial-of-Service-Angriffe sowie andere Störungen und potenzielle Schäden für Kunden, Mitarbeiter und wichtige Komponenten aufzeigen kann
- **KONZENTRATION** auf Aspekte jenseits der Schutzmaßnahmen, um Erkennung, Reaktion und Wiederherstellung zu unterstützen
- **SCHNELLERE ANALYSE** und Reaktion auf Angriffe durch kollaborative Bedrohungsanalyse, damit Erkenntnisse gemeinsam genutzt und Reaktionen koordiniert werden können
- **AUTOMATISCHE** Einbindung relevanter Bedrohungsdaten in Erkennungs- und Reaktionstools

Fordern Sie eine Live-Demo für ThreatQ Platform und ThreatQ Investigations an: threatq.com/demo

ÜBER THREATQUOTIENT™

ThreatQuotient hat sich das Ziel gesetzt, die Effizienz und Effektivität von Sicherheitsabläufen mithilfe einer bedrohungsbasierten Plattform zu verbessern. Durch die Integration der bestehenden Prozesse und Technologien eines Unternehmens in eine zentrale Sicherheitsarchitektur beschleunigt und vereinfacht ThreatQuotient die Untersuchungen sowie die Zusammenarbeit innerhalb von und zwischen Teams und Tools. Dank Automatisierung, Priorisierung und Visualisierung verringern die Lösungen von ThreatQuotient die Menge nicht relevanter Informationen und heben Bedrohungen mit hoher Priorität hervor, damit begrenzte Ressourcen ihren Schwerpunkt auf diese Gefahren legen können und bei Entscheidungen unterstützt werden. ThreatQuotient hat seinen Hauptsitz in Nord-Virginia (USA) sowie internationale Zweigstellen in Europa und im APAC-Raum. Weitere Informationen finden Sie unter https://threatquotient.com.

ThreatQ-for-Critical-Infrastructure_Rev1

THREATQUOTIENT™

11400 Commerce Park Drive, Suite 200, Reston, VA 20191 • ThreatQ.com
Sales@ThreatQ.com • +1 703 574-9885