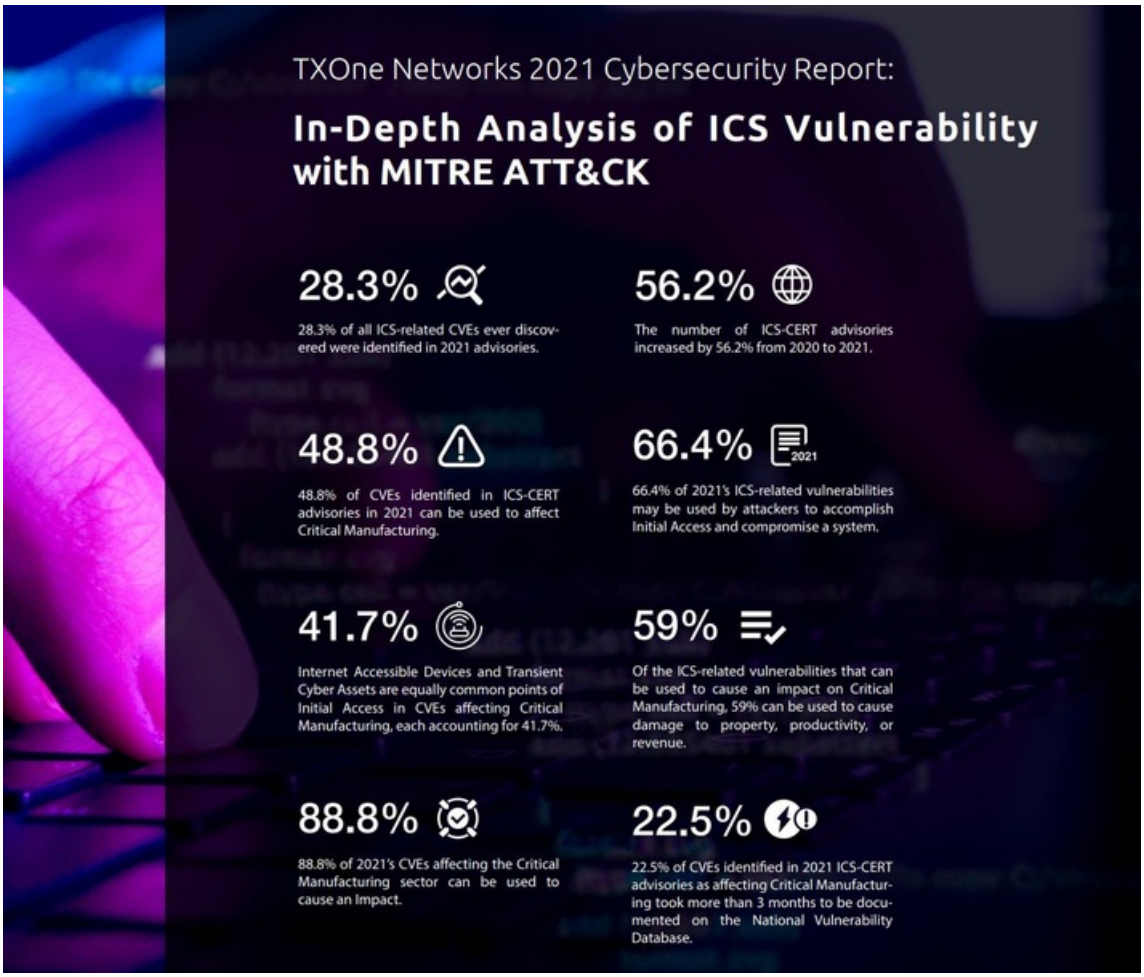
TXOne Networks

01.02.2022 – 14:00 Uhr

Cybersecurity Report 2021: TXOne Networks veröffentlicht detaillierte Analyse von Cyber-Schwachstellen und deren Auswirkungen auf industrielle Kontrollsysteme (ICS)



San Francisco / Taipeh (ots) -

Aktuelle Forschungstrends und Auswirkungen der Cyberbedrohungen vergangener Jahre auf ICS-Umgebungen im Jahr 2022

TXOne Networks, ein weltweit führender Anbieter von Sicherheitslösungen zum Schutz industrieller Kontrollsysteme (ICS) und dem industriellen Internet der Dinge (IIoT), hat seinen jährlichen *Cybersecurity Report 2021* veröffentlicht, der sich auf die Schwachstellen von ICS-Umgebungen konzentriert. Die Sicherheitsexperten von TXOne Networks haben diese Sicherheitslücken von ICS-Umgebungen mit Hilfe der *MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) for ICS*, einer weltweit zugänglichen Wissensdatenbank zu Taktiken und Techniken der Akteure von Cyberangriffen auf industrielle Kontrollsysteme, eingehend analysiert. Anhand der Ergebnisse des Cybersecurity-Berichts kann TXOne Networks aufzeigen, wie sich Cyberbedrohungs- und Forschungstrends aus dem Jahr 2021 und den Vorjahren auf ICS-Umgebungen im Jahr 2022 auswirken werden. Eine wichtige Erkenntnis des Berichts ist, dass Cyberangriffe auf kritische Infrastrukturen mithilfe der sogenannten OT-Zero-Trust-Methode abgewehrt werden können bzw. die Abwehr erheblich erleichtert werden kann. Die Methode umfasst die Überprüfung von Geräten, den Schutz kritischer Anwendungen und Dienste, eine Netzwerksegmentierung und virtuelle Patches.

Der Schwerpunkt des Cybersecurity-Berichts von TXOne Networks liegt insbesondere auf der Analyse der sogenannten *Common Vulnerabilities and Exposures (CVEs)*, also den allgemeinen Schwachstellen und Gefährdungen, die ICS-Umgebungen betreffen können. Diese branchenspezifischen Schwachstellen werden jedes Jahr vom *Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)* identifiziert. Die von TXOne Networks verwendete *MITRE ATT&CK for ICS*-Matrix gibt einen Überblick über die "Taktik" (die Zielsetzungen Cyberkrimineller während eines Angriffs) sowie über die spezifischen "Techniken", die Cyberangreifer einsetzen, um ihre Ziele zu erreichen.

ICS-CERT-Sicherheitshinweise 2021

ICS-CERT-Sicherheitshinweise ("Advisories") werden veröffentlicht, wenn eine ICS-Schwachstelle bekannt wird, die Angreifer ausnutzen könnten, um Schaden anzurichten. Dem Cybersecurity-Bericht zufolge ist die Zahl dieser Sicherheitswarnungen im Jahr

2021 drastisch gestiegen. Es wurden 389 Warnungen veröffentlicht, was, im Vergleich zu den 249 Sicherheitshinweisen im Jahr 2020, den größten jährlichen Zuwachs in der Geschichte des ICS-CERT-Programms darstellt. Die ständig wachsende Zahl von CVEs in Bezug auf ICS-Umgebungen macht deutlich, dass es nahezu unmöglich ist, jede einzelne Schwachstelle umfassend zu berücksichtigen.

Im Jahr 2021 haben sich zudem die Methoden von Cyberkriminellen grundlegend geändert, und es gab mehr ausgefeilte und zerstörerische Angriffe auf Lieferketten als je zuvor. Zu den bekannten Ransomware-Gruppen, die in jüngster Zeit aktiv waren, gehören Maze, Lockbit, REvil und DarkSide, deren Aktivitätsniveau jedoch teilweise variiert.

CVEs beeinträchtigen ICS-Umgebungen

Bei einer sorgfältigen Analyse der Schwachstellen in den ICS-CERT-Sicherheitshinweisen von 2017 bis 2021 (nach betroffenen Sektoren geordnet), fällt ein enormer Zuwachs an Schwachstellen auf, die systemkritische Produktionsbereiche betreffen. So müssen 59,8 Prozent dieser 2021 in Sicherheitswarnungen identifizierten CVEs als kritisch oder hochriskant eingestuft werden.

Während die Fertigungsindustrie offensichtlich an der Spitze der Gefährdungsliste steht, zeigt der TXOne Cybersecurity-Bericht auch einen Anstieg der CVEs, die für Angriffe auf zahlreiche andere Branchen verwendet werden können. Sowohl Angreifer als auch Sicherheitsexperten werden sich in den Jahren 2022 und 2023 verstärkt für diese Art von Schwachstellen interessieren, da Cyberkriminelle ein und dieselbe Schwachstelle in verschiedenen Betriebsumgebungen ("Operational Environments") ausnutzen können.

"Unsere Analyse der 613 im Jahr 2021 identifizierten CVEs die sich voraussichtlich auf kritische Produktionsumgebungen auswirken werden zeigt, dass potenzielle Aggressoren ganze 88,8 Prozent davon ausnutzen könnten, um einen Cyberangriff durchzuführen und ICS-Anlagen sowie ihre Umgebung in wechselndem Maße zu stören", so Dr. Terence Liu, CEO von TXOne Networks. "Für ICS-Umgebungen sind Cyberattacken ein erheblicher Grund zur Besorgnis, da sie Schäden oder Störungen in Bezug auf Finanzen, Sicherheit, Menschenleben, Umwelt und Ausrüstung verursachen."

Sicherheit in der Lieferkette und am Arbeitsplatz

Dem Cybersecurity-Bericht zufolge stellt das ICS-CERT zwar Informationen über CVEs bereit, die unmittelbar nützlich und notwendig sind. Aber es fehlen möglicherweise einige Informationen, die den Prozess zur Behebung dieser Schwachstellen rationalisieren könnten. Ergänzende Informationen, die von der National Vulnerability Database (NVD) bereitgestellt werden, können bei der Erstellung von Software Bills of Materials (SBOMs) und der Verhinderung von Angriffen auf die Lieferkette von entscheidender Bedeutung sein. Aber bei fast 25 Prozent der CVEs dauert es mehr als drei Monate, bis diese Dokumentationsstufe erreicht ist.

Dies unterstreicht einige entscheidende Punkte. Zum einen kann sich in Bezug auf IT/OT-Sicherheit kein Unternehmen auf eine einzige Quelle für Cybersicherheits-Informationen verlassen. Das heißt, die ICS-Cybersicherheit ist eine Gemeinschaftsaufgabe, die ohne den Abgleich mehrerer Informationsquellen nicht effektiv bewältigt werden kann. Zum anderen können sich Unternehmen aufgrund der verlängerten Zeitspanne bis zur Verfügbarkeit von Informationen nicht allein auf Patches der Hersteller oder veröffentlichte Forschungsergebnisse verlassen, um ihren operativen Betrieb zu sichern.

OT Zero Trust

Ein möglicher Weg, diese Herausforderungen und den dringenden Bedarf an Verbesserungen in der Cybersicherheit anzugehen, kann die "Zero Trust Architecture" sein. Die Experten von TXOne Networks empfehlen die sogenannte *OT-Zero-Trust Methode*, eine angepasste Form der Zero-Trust-Architektur, die sowohl für Lieferketten als auch für ICS-Umgebungen einzigartige Verbesserungen der Cybersicherheit bietet.

Ein Kernprinzip von IT-Zero-Trust ist "never trust, always verify". Diese Idee basiert auf der aus dem IT-Bereich kommenden Sichtweise, dass ein Netzwerk für menschliche Anwender oder "Nutzer" konzipiert ist. Da in ICS-Umgebungen die Netzwerke jedoch in erster Linie von Produktionsanlagen und nicht von Personen genutzt werden, muss die dort verwendete Methodik an das *OT Zero Trust-Konzept* angepasst werden, um einen zuverlässigen Schutz zu bieten, der weder die Produktivität noch die Verfügbarkeit der Anlagen beeinträchtigt. "Auf *OT Zero Trust* basierende Verfahren, wie Netzwerksegmentierung, virtuelles Patching, Vertrauenslisten, Asset Hardening und Sicherheitsinspektion, bieten eine überlegene Schutzbasis, indem sie die Sicherheitsstandards für Netzwerke und Produktionsanlagen von Grund auf erhöhen", betont TXOne Networks CEO Dr. Liu.

Der *Cybersecurity Report 2021 von TXOne Networks "In-Depth Analysis of ICS Vulnerability with MITRE ATT&CK"* steht hier zum Download bereit.

Bildmaterial zu dieser Meldung finden Sie unter: https://www.gcpr.de/presseraum/txone-networks/

Folgen Sie TXOne Networks: Blog, Twitter, and LinkedIn

Über TXOne Networks

TXOne Networks bietet praxisbezogene Cybersicherheitslösungen zum Schutz industrieller Steuerungssysteme und sorgt für Zuverlässigkeit und Sicherheit vor Cyberangriffen in der Industrie. Gegründet durch ein Joint Venture von Trend Micro und Moxa, arbeitet der OT-Sicherheitsanbieter mit führenden Anbietern und Betreibern kritischer Infrastrukturen zusammen und entwickelt auf der Grundlage neuester Forschungsergebnisse und Praxiserfahrungen den passenden Sicherheitsansatz für die jeweilige Anwendung. Auf Basis einer Echtzeit-Defense-in-Depth-Methode bietet TXOne Networks sowohl netzwerk- als auch endpunktbasierte Lösungen zur Absicherung von OT-Netzwerken und unternehmenskritischen Produktionsanlagen und Geräten. Weitere Informationen unter www.txone-networks.com

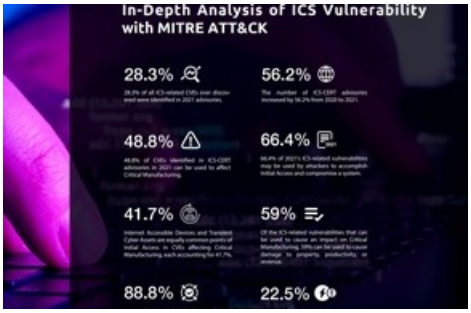
Pressekontakt:

Pressekontakt-TXOne-Networks:
Lynette_lee@trendmicro.com
Tel. +886-2-2378-9666_ext.5133

Pressekontakt-Europa-TXOne-Networks
GlobalCom-PR-Network-GmbH
Martin Uffmann
martin@gcpr.net
Tel.: +49-(0)89-360-363-41

Caroline Hannig-Sachon
GlobalCom-PR-Network-GmbH
caroline@gcpr.net
Tel.: +49-(0)89-360-363-42

Medieninhalte



"TXOne-Networks 2021 Cybersercurity-Report: In-Depth Analysis of ICS Vulnerability with MITRE ATT&CK": - Key Figures Overview / Weiterer Text über ots und www.presseportal.de/nr/155587 / Die Verwendung dieses Bildes ist für redaktionelle Zwecke unter Beachtung ggf. genannter Nutzungsbedingungen honorarfrei. Veröffentlichung bitte mit Bildrechte-Hinweis.