TXOne Networks

28.02.2023 – 10:05 Uhr

TXOne Networks und Frost & Sullivan veröffentlichen Jahresbericht 2022 über aktuelle Cyberbedrohungen im OT-Bereich

Eindhoven (Niederlande)/Taipei (Taiwan) (ots) -

Laut ICS- und Cybersicherheitsexperte TXOne, schärfen Ransomware und Cyberangriffe auf Lieferketten und kritische Infrastrukturen den Fokus auf OT-Sicherheit für 2023

TXOne Networks, ein weltweit führender Anbieter von Cybersicherheitslösungen für das industrielle Internet der Dinge (IIoT), hat heute seinen Jahresbericht 2022 veröffentlicht, in dem das Wachstum von Ransomware und Angriffen auf Lieferketten sowie kritische Infrastrukturen ausführlich beschrieben wird. Der Bericht *Insights Into ICS/OT Cybersecurity 2022*, der kostenlos heruntergeladen werden kann, befasst sich mit den Haupttrends im Bereich der industriellen Kontrollsysteme (ICS), wie z. B. der Konvergenz von Betriebs- und Informationstechnologie (OT – Operational Technology und IT), dem verstärkten Fokus auf Regulierungen, der Zunahme protektionistischer Bestrebungen im globalen Handel und dem gestiegenen Bewusstsein für potenzielle Verluste durch Cyberangriffe auf die OT-Umgebung.

Der in Zusammenarbeit mit dem Beratungsunternehmen Frost & Sullivan erstellte Bericht *Insights Into ICS/OT Cybersecurity 2022* basiert auf einer Umfrage unter 300 leitenden Angestellten (C-Level), Direktoren und anderen Managern in verschiedenen Organisationen/Unternehmen in modernen Produktionsländern weltweit. Der Bericht bietet eine umfassende Analyse der aktuellen Bedrohungen im OT-Bereich und liefert umsetzbare Handlungsempfehlungen, die Unternehmen bei der Entwicklung praktischer, betriebsfreundlicher Ansätze zur OT-Cyberabwehr nutzen können.

Im Bereich der Cybersicherheit schreitet der technologische Fortschritt immer schneller und unvorhersehbarer voran. Das bedeutet, dass Bedrohungen durch Cyberangreifer sehr schnell zur düsteren Realität werden und kaum Vorwarnzeit bleibt. Aus diesem Grund hat TXOne Networks einen detaillierten und vielschichtigen Blick auf die jüngste Entwicklung der OT-Sicherheit im Jahr 2022 geworfen und die Ergebnisse im Cybersicherheits-Jahresbericht veröffentlicht. Die Forscher untersuchten, wie sich die Bedrohungslandschaft im vergangenen Jahr dadurch verändert hat, dass 2022 etwa Ransomware-as-a-Service (RaaS) als Angebot aufkam. So bedrohte beispielsweise „mietbare“ Ransomware wie Black Basta, Pandora und LockBit 3.0 gesamte IT/OT-Umgebungen. Derartige Schadprogramme setzten rücksichtslose Strategien zur mehrfachen Erpressung von Unternehmen ein. Es ist davon auszugehen, dass sich derartige Cyberangriffe vor allem in kritischen Branchen, wie der Fertigung, der Energieversorgung, der Landwirtschaft, dem Gesundheitswesen und der öffentlichen Gesundheit fortsetzen und besonders starke Auswirkungen auf den Automobilsektor haben werden, was den Bedarf an OT-spezifischem Cybersicherheitspersonal und -lösungen weiter erhöht. Der Bericht umfasst auch die von den Regierungen erlassenen Vorschriften, die ins jeweilige Landesrecht integriert werden. So soll die Cybersicherheit gegen die sich abzeichnenden globalen Bedrohungen aufgrund der geopolitischen Spannungen verstärkt werden. Darüber hinaus, erläutert TXOne die Marktkräfte, die die verschiedenen Branchen dazu veranlassen, in OT-spezifische Sicherheit zu investieren, und wie Unternehmen ihre Budgets im Bereich OT-Cybersicherheit ausweiten und sich auf eine breite Einführung derartiger Lösungen und Systeme vorbereiten.

"Bei ICS-/OT-Systemen gibt es viele konstruktionsbedingte Beschränkungen. Die Bewältigung von Cybersicherheitsproblemen unter diesen Umständen erfordert ein individuelles und maßgeschneidertes Portfolio von Lösungen und Methoden. Dies ist mit den standardisierten, wiederverwendeten Lösungsansätzen aus der IT nicht zu leisten“, so Terence Liu, Chief Executive Officer (CEO) von TXOne Networks. „Deshalb sind OT-native Cyber-Defense-Lösungen für ICS/OT-Umgebungen auf dem Weg, Mainstream zu werden. Da sich ICS-/OT-Systeme im Laufe der Zeit weiterentwickeln, werden neue Technologien wie das IIoT, hybride Clouds und 5G-Netzwerke weiter an Bedeutung gewinnen - und visionäre Lösungsanbieter bereiten sich schon jetzt auf diese Zukunft vor."

Einen detaillierten Überblick über die genannten Faktoren und wie sie in ihrer Gesamtheit die OT-Cybersicherheit in der jüngsten Vergangenheit und in naher Zukunft beeinflusst haben, bzw. beeinflussen werden, finden Sie im TXOne Networks' *Insights Into ICS/OT Cybersecurity 2022*.

Folgen Sie TXOne Networks auf dem Blog, bei Twitter und bei LinkedIn.

Über TXOne Networks

TXOne Networks bietet Cybersicherheits-Lösungen, die mithilfe der OT Zero Trust-Methode die Zuverlässigkeit und Sicherheit von industriellen Steuerungssystemen und OT-basierten Produktionsumgebungen gewährleisten. TXOne Networks arbeitet sowohl mit führenden Produktionsunternehmen als auch mit Betreibern kritischer Infrastrukturen zusammen, um praktische, betriebsfreundliche Ansätze für die Cyberabwehr zu entwickeln. TXOne Networks bietet dank seiner Defense-in-Depth-Methode sowohl netzwerk- als auch endpunktbasierte Produkte zur Absicherung von OT-Netzwerken und betriebskritischen Endgeräten in Echtzeit. www.txone.com

Pressekontakt TXOne Networks in Europa:

GlobalCom PR-Network GmbH
Martin Uffmann / Slavena Radeva
martin@gcpr.net / slavena@gcpr.net
Tel.: +49 (0)89 360 363-41 / -50

Medieninhalte

Dr. Terence Liu, CEO TXOne Networks / Weiterer Text über ots und www.presseportal.de/nr/155587 / Die Verwendung dieses Bildes für redaktionelle Zwecke ist unter Beachtung aller mitgeteilten Nutzungsbedingungen zulässig und dann auch honorarfrei. Veröffentlichung ausschließlich mit Bildrechte-Hinweis.

Annual Report "Insights Into ICS/OT Cybersecurity 2022" by TXOne Networks and Frost & Sullivan / Weiterer Text über ots und www.presseportal.de/nr/155587 / Die Verwendung dieses Bildes für redaktionelle Zwecke ist unter Beachtung aller mitgeteilten Nutzungsbedingungen zulässig und dann auch honorarfrei. Veröffentlichung ausschließlich mit Bildrechte-Hinweis.