プレスリリース

2022 年 11 月17日

Nozomi Networks、SANS 2022 OT/ICS サイバーセキュリティレポートの分析結果を発表

OT　環境に対するサイバーセキュリティリスクは依然として高く、企業側のセキュリティ対策も強化されていることが判明

OT/IoT セキュリティのリーダーである Nozomi Networks Inc.は本日、SANS 2022 OT/ICS サイバーセキュリティレポートにおいて、攻撃者が制御システム コンポーネントに狙いを定めることにより、ICS サイバーセキュリティの脅威が依然高いことが判明したことを発表しました。これに対し、組織は昨年からセキュリティ体制を大幅に強化する一方で、3 分の 1 以上（35%）が、自身の組織が侵害を受けたかどうかを把握していない状態となっています。エンジニアリング・ワークステーションへの攻撃は過去 12 ヶ月で倍増しています。

Nozomi Networks の共同創設者で CPO（最高製品責任者）の Andrea Carcano（アンドレア・カルカーノ）は次のように述べています。
「昨年、Nozomi Networks の研究者と ICS サイバーセキュリティコミュニティは、Incontroller のような攻撃が従来の企業ネットワーク上のターゲットから、直接 OT を標的としていることを目の当たりにしました。サイバー攻撃者は ICS のスキルを磨く一方で、強固な防御のための専門的なテクノロジーやフレームワークも利用可能です。今回の調査では、より多くの組織がそれらを積極的に利用していることがわかりました。しかし、まだやるべきことはあります。リスクを最小化し、回復力を最大化するために、今すぐ対策を講じることを推奨します。」

ICS のサイバーセキュリティリスクは依然高いまま

- 回答者の 62%が OT 環境に対するリスクを「高い」または「深刻」と評価しました（2021 年の 69.8%から若干減少）。
- ランサムウェアと金銭目的のサイバー犯罪が脅威のベクトルリストのトップ（39.7%）となり、国家が支援する攻撃（38.8%）がそれに続きました。3 位はランサムウェア以外の犯罪攻撃（32.1%）、4 位はハードウェア／ソフトウェアのサプライチェーンリスク（30.4%）となっています。

- 過去 12 カ月間に情報漏洩を経験したと答えた回答者は 10.5%に減少（2021 年の 15%から減少）しましたが、そのうちの 35%（昨年の 18.4%から倍増）はエンジニアリング・ワークステーションが最初の感染経路であると回答しました。
- 35%（48%から減少）が自分の組織が侵害されたかどうかわからない、24%（前年比 2 倍の改善）がインシデントに遭っていないと確信していました。
- 一般に、IT 侵害が依然として主流なアクセス経路であり（41%）、リムーバブル メディアによる複製がそれに続いています（37%）。

ICS のサイバーセキュリティ体制は確立されつつある

- 66%（昨年の 47%から増加）が過去 2 年間で制御システムのセキュリティ予算が増加したと回答しています。
- 56%（2021 年の 51%から向上）が、インシデント発生から 24 時間以内に侵害を検知するようになったと回答。過半数（69%）が、6～24 時間以内に検知から抑制へと移行していると回答しています。
- 87.5%（昨年の 75.9%から上昇）が過去 1 年間に OT/制御システムまたはネットワークのセキュリティ監査を実施- 現在 3 分の 1（29%）が継続的な評価プログラムを導入しています。
- 大多数（83%）は、自社の OT システムのセキュリティを監視し、そのうち 41%は、専用の OT SOC を使用しています。
- 組織は ICS のトレーニングと認証に投資し、83%の回答者が制御システムの専門的な認証を受ftています。これは、過去 12 ヶ月の 54%から大幅に増加しています。
- 80%近くが ICS の運用を重視した職務を担っており、2021 年の 50%から上昇しています。

OT/ICSサイバーセキュリティの最新動向について

- ダウンロード: ***2022 年以降の OT/ICS サイバーセキュリティのあり方について***

Nozomi Networks について

Nozomi ネットワークスは、世界の重要インフラ、産業、政府機関をサイバー脅威から保護することで、デジタルトランスフォーメーションを加速します。当社のソリューションは、OT/IoT 環境に対して、優れたネットワークと資産の可視性、脅威検出、インサイトを提供します。お客様は、リスクと複雑さを最小限に抑えると共に、運用弾力性を最大限に高めることができます。www.nozominetworks.com

SANS Institute について

SANS Institute は、1989 年に共同研究・教育機関として設立されました。SANS は、世界中の政府や民間機関の専門家にトレーニングと認証を提供しており、最も信頼されている最大手企業です。SANS の著名な講師陣は、200 を超えるライブやオンラインでサイバーセキュリティトレーニングイベントや、50 を超える様々なコースを提供しています。SANS Institute の関連会社である GIAC は、情報セキュリティに関する 30 種類の実践的な技術認定を通じて、従業員の能力を証明しています。SANS Technology Institute は、地域ごとに認定された独立した子会社で、サイバーセキュリティの修士号を提供しています。SANS は、コンセンサスプロジェクト、調査報告書、ニュースレターなど、情報セキュリティコミュニティに対して無数のリソースを無料で提供しているほか、インターネットの早期警戒システムである Internet Storm Center も運営しています。SANS は、企業から大学まで様々なグローバル組織を代表する多くのセキュリティ専門家で構成されており、情報セキュリティコミュニティ全体を支援するために協働しています。www.SANS.org

お問い合わせ先：
担当：清水・神谷
Nozomi Networks広報事務局
e-mail: nozomi@jspin.co.jp