MAY/stock.adobe.com

Jetzt vorbereiten auf NIS2

Mit Umsetzung der EU-Richtlinie NIS2 in nationales Recht müssen sich künftig mehr Unternehmen als bisher mit ihrem Cyber-Risiko-Management beschäftigen. Gefragt sind eine möglichst cyberresiliente Technik und ein hohes Sicherheitsbewusstsein der Mitarbeitenden.

Der Countdown läuft: In wenigen Monaten müssen Unternehmen, die unter die EU-Richtlinie NIS2 fallen, schärfere Vorgaben für mehr Cybersecurity umsetzen. Experten schätzen, dass sich der Kreis der Betroffenen um 30.000 Unternehmen erweitern wird, etwa um kleinere Organisationen wie Stadtwerke sowie um Zulieferer und Dienstleister innerhalb einer Lieferkette. Verantwortliche müssen selbst prüfen, ob NIS2 für sie gilt, und in diesem Fall die Sicherheitsstandards ihrer vernetzten Systeme und Betriebsmittel stärken – auch im eigenen Interesse.

NIS2 steht für Network and Information Security Directive 2. Die zweite Richtlinie für Netzwerk- und Informationssicherheit, die Teil der europäischen Cyber-Sicherheitsstrategie ist, soll bis Oktober dieses Jahres in nationales Recht umgesetzt werden. Für Deutschland liegt der 2. Referentenentwurf des NIS2-Umsetzungs- und Cybersicherheitsstärkungsgesetzes (NIS2UmsuCG) vor. Noch ist nicht alles im Detail festgelegt, aber klar ist jetzt schon: Deutlich mehr Unternehmen als bisher müssen sich künftig stärker mit ihrem Cyber-Risiko-Management beschäftigen. Dazu gehören wirksame technische wie organisatorische Vorkehrungen, um IT und Prozesse gegen Cyber-Angriffe zu schützen sowie Vorgehensweisen zur Bewältigung von Sicherheitsvorfällen, um deren Auswirkungen möglichst gering zu halten.

Die ersten Schritte

Die zentrale Frage für betroffene Unternehmen lautet: Wo fangen wir konkret an, um die aufwendigen Vorgaben umzusetzen? Dreh- und Angelpunkt ist die Sicherheit der vernetzten Systeme und Betriebsmittel. Leider gibt es nicht die perfekte technische Methode oder das per se sichere Produkt. Eine hohe Resilienz gegen Cyber-Kriminalität resultiert aus einem Set an Maßnahmen, die – einmal umgesetzt – auf ihre Wirksamkeit hin beobachtet und stetig weiter verbessert werden müssen. Grundsätzlich ist der erste Schritt eine Analyse des Systemverbunds, die aufzeigt, wie die IT der Organisation sowie ihre

diversen Betriebsmittel, Leitstellen, Überwachungszentralen und vieles mehr vernetzt sind.

Je nach Geschäftsmodell sind zum Beispiel bei Stadtwerken unterschiedliche Netzwerk-Assets im Spiel, die Verteil-, Schalt- und Messeinrichtungen, Kommunikationsanwendungen oder ÖPNV-Betriebsstätten und Haltestellen verbinden. Zum Spektrum gehören selbstbetriebene Übertragungs- und Datennetze mit unterschiedlichen Protokollen, Funkstrecken und -netzen, Routern und Switches ebenso wie von Providern gemietete Verbindungsleitungen oder Vernetzungsdienste. In manchen Fällen übernehmen Stadtwerke darüber hinaus die Rolle eines Providers für Telekommunikations- und Datendienste oder teilen sich mit einem von ihnen zumindest Infrastrukturelemente, wie Kabel und Standorte. Die Bestandsaufnahme ergibt immer ein individuelles, komplexes Bild. Nicht selten zeigt sich dabei, dass viel mehr Technik vorhanden ist, als zunächst gedacht. Dass sich aktuelle Vernetzungstechnologien immer stärker auf den Einsatz softwarebasierter Funktionen abstützen, tut ein Übriges.

Daten sicher verschlüsseln

Verschlüsselungstechnologien werden mit NIS2 – noch mehr als bisher – zum Stand der Technik, den es umzusetzen gilt. Auf der Anwendungsebene ist es mittlerweile selbstverständlich, die Datenübertragung über das Sicherheitsprotokoll TLS (Transport Layer Security) oder klassisch via VPN abzusichern. Für WAN- und LAN-Netzknoten sind standardisierte Verschlüsselungsverfahren für den Link-Layer (MACSec) verfügbar. Um komplette Datenströme Ende-zu-Ende zu verschlüsseln, gibt es leistungsfähige Einzelgeräte oder Lösungen in Kombination mit optischen WDM-Übertragungssystemen, bei Bedarf auch mit einem Zertifikat des Bundesamts für Sicherheit in der Informationstechnik (BSI). Technisch sind also alle Optionen vorhanden. Die Kunst besteht darin, aus dem großen Arsenal die für das jeweilige Unternehmen adäquate Technik auszuwählen.

Angezeigt ist zudem eine Zwei- oder Mehrfach-Authentifizierung – nicht nur für den Zugriff auf die IT-Systeme von außen, sondern auch für die einzelnen Netzwerkkomponenten und ihre Management-Systeme. Sie sind attraktive Ziele für Angreifer und zugleich besonders sensibel. Technische Lösungen für Zugriffsprozeduren und deren Protokollierung gibt es genügend. Ihre Implementierung ist eine gute Gelegenheit, den Umfang administrativer Netzwerkzugriffe durch das eigene Personal oder Dienstleister auf das absolut notwendige Minimum zu beschränken und passende Freigabeprozesse zu entwickeln. Stadtwerke und ähnliche Unternehmen können ihre Betriebstechnik (Operational Technology, OT) leider nicht nur an eigenen und physisch geschützten Standorten unterbringen. Das legt es nahe, nicht nur unerwünschte Zugriffe durch klassische Internet-Angreifer, sondern auch den Zugriff auf schwer schützbare Netzausläufer zu betrachten. Hier hilft das Zero-Trust-Konzept, indem solche Netzabschnitte voneinander separiert und jeweils mit eigenen Zugrifffsregeln beaufschlagt werden.

Nicht zu unterschätzen ist der Aufwand, der mit der Verwendung von Krypto-Algorithmen einhergeht. Er lässt sich durch eine sorgfältige Planung und – wo es möglich ist – die Automatisierung der Schlüsselverwaltungsprozesse beherrschen. In den meisten Fällen ist eine eigene Public-Key-Infrastruktur (PKI) erforderlich, die Sicherheitszertifikate für verschiedene Anwendungen bereitstellt. Eine Aufgabe, die sich schnell zu einem eigenen Projekt entwickelt, da eine PKI über die Lebensdauer einzelner Systeme hinaus langfristig angelegt ist.

Besondere Beachtung bei der Abwehr von Cyber-Kriminellen benötigen drei grundlegende Infrastrukturdienste, welche die zentralen Bausteine für eine hohe Netzverfügbarkeit sind: DHCP (Dynamic Host Configuration Protocol), das Geräten bei der Verbindung mit dem Netzwerk IP-Adressen zuweist, DNS (Domain Name System), das Klarnamen in IP-Adressen auflöst, und das Adress-Management-System IPAM. Nicht selten werden diese in verschiedenen Netzbereichen ▶

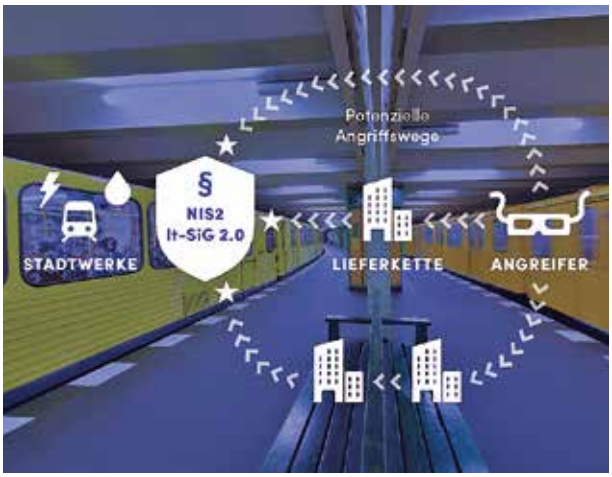
telent GmbH

Der Autor: Dr. Reinhard Wegener

Dr. Reinhard Wegener verantwortet als Leiter technischer Vertrieb und Technologiedirektor der telent GmbH in Backnang seit dem Jahr 2006 Kundenlösungen aus dem kompletten technischen Portfolio.

auch separat verwaltet. Das macht sie schwer überschaubar. Für mehr Transparenz sorgen übergeordnete Systeme, sodass beispielsweise Energieversorger, die beim Aufbau eines Solarparks mit zahlreichen Dienstleistern zusammenarbeiten, den Überblick behalten und somit das Risiko senken, dass sich Unbefugte Zutritt verschaffen.

Netzwerksicherheit geht einher mit einer fortschrittlichen Angriffserkennung und dem Monitoring kritischer Komponenten, wie es das IT-Sicherheitsgesetz 2.0 Betreibern Kritischer Infrastrukturen (KRITIS) bereits seit März 2023 vorschreibt. Für die Systeme der Angriffserkennung ist die Betriebstechnologie im KRITIS-Umfeld allerdings eine ganz andere Situation als die bisherigen Anforderungen der IT-Welt. Priorität hat die hohe Verfügbarkeit der Operational Technology, die eine Angriffserkennung keinesfalls beeinträchtigen darf. Auch hier ist es mit einem System nicht getan, sondern es braucht vielfältige Prozesse, Technologien und Fachleute. Sie spielen am besten in einem Security Operations Center (SOC) zusammen, das der Sicherheit der gesamten IT/OT-Infrastruktur dient und weitere NIS2-Forderungen abdeckt, wie etwa ein Schwachstellen-Management. Ein SOC kann, abhängig von den betrieblichen Kapazitäten, intern oder extern von spezialisierten Dienstleistern betrieben werden.



telent GmbH

Supply-Chain-Angriffe nehmen zu.

Supply-Chain-Angriffe, also Cyber-Angriffe über die Lieferketten, nehmen zu – so erfolgte kürzlich etwa eine Attacke auf den Software-Anbieter PSI, dessen Produkte breit im Markt eingesetzt werden. Im Mittelpunkt des öffentlichen Interesses steht beim Thema Cyber-Kriminalität die Erpressung von Lösegeld und – Stichwort: DSGVO – der Verlust personenbezogener Daten; seltener spricht man über die Netzwerkdokumentation. Doch gerade KRITIS-Betreiber müssen sich vergegenwärtigen, dass sie es mit hochprofessionellen Gegnern bis hin zu staatlichen Akteuren zu tun haben.

Abwarten ist keine Option

Dokumentationsdaten über die betriebenen Infrastrukturen und deren Netzwerke sind hochkritisch. Eine Standortinformation hier, ein Lieferantenkontakt dort, ein Ansprechpartner beim Kunden – werden solche Daten erbeutet, liefern sie die Puzzlesteine für den nächsten, noch wirkungsvolleren Angriff.

Angesichts der Bedrohungslage und der Summe der Maßnahmen, die im Rahmen der NIS2-Umsetzung bedeutsam werden, ist es keine Option, länger abzuwarten. Möglichst cyberresiliente Technik und ein hohes Sicherheitsbewusstsein bei den Mitarbeitenden sind gefragter denn je. Unterstützung leisten dabei spezialisierte Dienstleister, die gleichermaßen mit Cybersecurity und komplexen IT/OT-Strukturen vertraut sind. ■

NIS2-Mindestanforderungen für Cybersecurity

- Konzepte für Risikoanalyse für Informationssysteme und Sicherheit für Informationssysteme,
- Incident Management,
- Krisen-Management und Business Continuity (Back-up Management und Recovery),
- Sicherheit der Lieferkette,
- Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung inklusive Management und Offenlegung von Schwachstellen,
- Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risiko-Management-Maßnahmen,
- grundlegende Verfahren für Cyber-Hygiene (wie Datensicherung, Updatemanagement, Zero-Trust, Netzwerksegmentierung, Identitäts- und Zugriffsmanagement) und Schulungen für Cyber-Sicherheit,
- Konzepte und Verfahren für Kryptografie und Verschlüsselung (Ende zu Ende),
- Sicherheit des Personals, Konzepte für Zugriffskontrolle und Management von Anlagen,
- Multi-Faktor-Authentifizierung oder kontinuierliche Authentifizierung, sichere Kommunikation (Sprache, Video, Text) gesicherte Notfallkommunikationssysteme.

www.openkritis.de