Wirksame Schutzmaßnahmen

Schritt für Schritt zu sicheren IT/OT-Netzen

Der Umbruch in der Energiewirtschaft ist gewaltig. Er führt zur stärkeren Nutzung von Elektroenergie, integriert regenerative Energien und neue Geschäftsmodelle. Zudem steht die Branche im Fokus von Cyberkriminellen, weswegen auch der Gesetzgeber die Vorgaben stetig verschärft. Netzwerke für die Sekundärtechnik – sozusagen die »OT des Energieversorgers« – sicher und hochverfügbar zu halten, ist für Energieunternehmen eine Mammutaufgabe. Sie lässt sich jedoch leichter bewältigen, wird sie in wirksame Einzelschritte aufgeteilt und priorisiert nacheinander umgesetzt.

Die Energiewirtschaft ist sich ihrer Verantwortung als kritische Infrastruktur sehr wohl bewusst. Schon früh hat die Branche allgemein anerkannte Sicherheitsstandards und internationale Normen berücksichtigt, um IT und Steuerungstechnik gegen Cyberangriffe zu wappnen. Wer allerdings hoffte, mit den seit Mai 2023 durch das IT-Sicherheitsgesetz 2.0 geforderten Systemen zur Angriffserkennung sei es getan, der täuscht sich. Denn das NIS2-Umsetzungsgesetz wirft seine Schatten voraus, da die europäische Richtlinie NIS2 bis spätestens Oktober 2024 in nationales Recht überführt werden muss.

Als wären die gesetzlichen Verschärfungen nicht schon herausfordernd genug, stehen die Betreiber bei den Kommunikationsnetzen für die OT (Operational Technology) vor einem Umbauzwang. Ein signifikanter Teil der Stromversorgungsnetze wird derzeit noch mit zeitschlitzbasierten Systemen betrieben, die effektiv Energie- und Steuerungsinformationen in Echtzeit austauschen. Um künftig Erzeugungsanlagen wie Solarparks einzubinden beziehungsweise digitale Geschäftsmodelle abzubilden, reichen weder Topologien noch Kapazitäten aus. Zudem wird es aufgrund der technologischen Entwicklung immer schwieriger, diese langfristig zu supporten. Für eine flexible, dezentrale Energieerzeugung müssen aus Bestandsnetzen IP-Prozessnetze werden, die mit ihrer paketbasierten Infrastruktur vielfältige Anwendungen und eine zukunftssichere Datenübertragung ermöglichen. Nicht zuletzt vor dem Hintergrund personeller Engpässe stellt sich die schwierige Frage: Welche Maßnahmen steigern die Resilienz der Netze gegen digitale Bedrohungen?

SOC als zentrale Sicherheitsstelle

Viele Betreiber beschäftigen sich aktuell mit der Einführung von Funktionen

Quelle: telent GmbH

Je mehr vernetzte Geräte und digitale Lösungen in die IT- und Kommunikationsnetze des Energiesektors einziehen, desto wichtiger wird der Schutz der Infrastruktur gegen Cyberangriffe.

eines Security Operations Center (SOC). Ob als SOC-as-a-Service eines externen Dienstleisters oder intern mit eigenem Team betrieben: Auf lange Sicht wird kaum ein Energieunternehmen ohne SOC auskommen – nicht nur aufgrund der gesetzlichen Regularien, sondern aus ureigenem Interesse. Ein SOC ist die zentrale Stelle, in der speziell geschulte Experten mithilfe klar definierter Prozesse und technischer Tools die Kommunikation in der kompletten IT/OT-Infrastruktur eines Unternehmens überwachen, auswerten, Anomalien erkennen und proaktiv auf Bedrohungen reagieren. Doch selbst ein hochspezialisiertes Team braucht eine gut vorbereitete Netzinfrastruktur. Denn je höher der Reifegrad der Sicherheitsmaßnahmen und je mehr der gängigen Bedrohungen wirksam ausgeschaltet werden, umso mehr können sich die Spezialisten auf die verbliebenen, aber womöglich umso ernsteren Bedrohungen konzentrieren.

Mehr Sicherheit beginnt mit der Transparenz über die vernetzten Geräte und Anlagen. Die Erfahrung zeigt: Asset-Dokumentationen sind oft nicht so vollständig, wie es erforderlich wäre, um komplexe Netzwerke zu analysieren und in klar definierte Bereiche zu gliedern. Früher gab man sich möglicherweise mit wenigen, grob durch Firewalls getrennten Integritätsbereichen zufrieden. Doch die Vielfältigkeit möglicher Angriffsszenarien und lateraler Ausbreitungsmechanismen innerhalb der Netze erfordert heute eine stärkere Separierung bis hin zur Mikrosegmentierung. Mit Next Generation Firewalls, die Einblick in die Anwendungsprotokolle haben, lässt sich der Zero-Trust-Ansatz leichter durchsetzen, damit nur wirklich erwünschte Kommunikation stattfindet.

EDR ersetzt klassischen Virenschutz

Ein weiterer Baustein zur Abwehr von Cyberbedrohungen ist Endpoint Detection and Response (EDR), das den klassischen Virenschutz ersetzt. Die Lösung zeichnet das Verhalten von Endgeräten wie PC oder Servern auf, analysiert die Daten und isoliert automatisch bei verdächtigem Verhalten die Endgeräte. Ein EDR ist zudem eine wichtige Quelle für Protokolldaten. Diese Loggingdaten, die wichtige Informationen über potenzielle Sicherheitsvorfälle enthalten, können an ein SIEM (Security Information and Event Management) oder ein SOC geliefert werden. Ein zusätzliches OT-Monitoring erhöht die Sichtbarkeit der Kommunikation zum Beispiel von Automatisierungssystemen, die in der Energiewirtschaft eingesetzt werden, um physische Prozesse zu überwachen, zu steuern und zu automatisieren. Bei diesen besteht im Gegensatz zu klassischen IT-Geräten nahezu keine Möglichkeit, zusätzliche Software zu installieren. Um Abweichungen zu identifizieren, wird das Netzwerkverhalten mit separaten Sensoren überwacht.

Basisdienste der IP-Netzwerke im Griff

Zunehmend erkennen Betreiber von Datenkommunikationsnetzen auch die Sicherheitsrelevanz der drei grundlegenden Infrastrukturdienste: DHCP (Dynamic Host Configuration Protocol) weist Geräten, die sich mit dem Netzwerk verbinden, IP-Adressen zu, ohne die sie im Netzwerk nicht kommunizieren können. Da es in der Praxis oft komplexe Netzwerke mit verschiedenen DHCP-Quellen gibt, kommt es schnell zum Verlust der Transparenz und in der Folge zu unnötigen Sicherheitsrisiken. Ein übergeordnetes System, das die Adressvergabe zentralisiert und unerlaubte Teilnehmer ausschließt, erhöht die Sicherheit. Dasselbe gilt für DNS (Domain Name System). Die Zuverlässigkeit des Dienstes, der Klarnamen in IP-Adressen auflöst, ist entscheidend für die Verfügbarkeit von Netzwerken, aber auch ein begehrtes Ziel für Angreifer. Zentralisierung schafft auch hier mehr Sicherheit. Auf der Planungsebene kommt IPAM (IP Address Management) hinzu. Das Adress-Management-System organisiert und dokumentiert, welche Adressen existieren und organisiert deren Vergabe. Den Überblick zu behalten, ist für Energieversorger, die zum Beispiel beim Aufbau eines Solarparks mit zahlreichen Dienstleistern zusammenarbeiten, zunehmend herausfordernd. Kommt es zu Duplikaten, ist das ein Anfängerfehler; schleichen sich aber Unbefugte auf diesem Weg ins Netz ein, ist das ein Sicherheitsrisiko.

Standardmaßnahmen im Blick behalten

Auch wenn nach und nach neue Sicherheitsverfahren eingeführt werden, dürfen die Standardmaßnahmen nicht vernachlässigt werden. Bei Fernwartungszugängen ist es entscheidend, nicht nur technische Aspekte zu berücksichtigen, sondern regelmäßig Nutzer, Berechtigungen und mögliche seit Ersteinrichtung hinzugekommene Cyberbedrohungen zu überprüfen. Zu den Standardmaßnahmen kann neben der Verschlüsselung auf Anwendungsebene auch die komplette Leitungsverschlüsselung gehören, die gewährleistet, dass zwischen Netzknoten ausgetauschte Daten, selbst bei Abfangen oder unbefugtem Zugriff, nicht von Dritten gelesen oder manipuliert werden. Die Verschlüsselungstechnik kann nachträglich implementiert werden, ohne bestehende WAN-Infrastrukturen zu verwerfen. Die Umsetzung oder Verbesserung der Zugangskontrolle auf der Netzwerkebene (Network Access Control) ist und bleibt eine weitere wichtige und wirksame Maßnahme.

Cyberkriminelle suchen sich zunehmend potenzielle Schwachstellen in der Lieferkette, indem sie beispielsweise Dienstleister unbemerkt infiltrieren. Diese geben dadurch unwissentlich Schadprogramme und Viren an ihre Kunden weiter, zum Beispiel über Wechseldatenträgern, die bei Wartungsarbeiten eingesetzt werden. Mit einer Datenschleuse, wie die von der Firma telent entwickelte InDEx (Intelligent Data Exchange), wird das leicht unterbunden. InDEx untersucht die zu importierenden Daten, und nur dann, wenn sie keine Bedrohungen findet, erlaubt sie den Zugang ins interne Netzwerk.

Der Schutz vor Cyberkriminalität ist ein kontinuierlicher Prozess, der sich von der vorhandenen Netzinfrastruktur ausgehend auf bestehende ebenso wie neuartige Bedrohungen einstellt. Ein Dienstleister, der sich in den IT- und Kommunikationsnetzen des Energiesektors ebenso auskennt wie im Bereich Cybersecurity verfügt über alle erforderlichen Bausteine bis hin zum SOC-as-a-Service, um Sicherheitsmaßnahmen zu planen und technisch sauber umzusetzen. Er unterstützt Unternehmen auch dabei, Einzelmaßnahmen sinnvoll zu priorisieren, damit sie abhängig vom individuellen Status quo und den vorhandenen Ressourcen die wichtigsten Sicherheitslücken zuerst schließen. So werden Netzwerklösungen schrittweise sicherer und bleiben trotz des technischen Wandels hochverfügbar.

Dr. **Reinhard Wegener**,
Director Technology Center,
telent GmbH, Backnang

>> info.germany@telent.de

>> www.telent.de