www.energiespektrum.de

energie spektrum

01 2020

35. Jahrgang

Nachhaltigkeit

So können Stadtwerke und Industrie ihre Klimabilanz verbessern

Interview

CEO Christoph Ostermann von Sonnen

E-world

15 Seiten News und Messehighlights

Unternehmensführung

CO_2 – Weniger ist mehr. Expertengespräch in München.

DOSSIER

Digitale Energiewende

Wie Filialisten von Verbrauchsmessung in Echtzeit profitieren

Seite 39 ►►►

digitales

CYBERSECURITY – ITSiG 2.0, das zweite Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme, aktuell noch im Entwurf, wird Betreiber von ›KRITIS‹ künftig stärker in die Pflicht nehmen. Aber wie betrachtet man sensible Systeme allumfassend und hält konkrete Vorgaben ein?

Bild: wm-foto.com

SPÜRNASEN IM NETZ

Effektive Cybersecurity für KRITIS-Betreiber stellt vor allem kleine und mittlere Unternehmen vor eine große Herausforderung. In vielen Fällen mangelt es an den nötigen internen Ressourcen und dem Budget. Investiert in die richtigen Technologien, kann aber auch mit einem kleinen Budget, ein effektiver Schutz aufgebaut werden.

Einwandfrei funktionierende kritische Netzwerkinfrastrukturen für die Energie- und Gesundheitsversorgung, Mobilität oder das Finanzwesen sind essenziell in einer modernen Gesellschaft.

Um den Schutz in diesem Bereich noch weiter auszubauen, legte Bundesinnenminister Horst Seehofer im letzten Jahr den Referentenentwurf für das ITSiG 2.0 vor. Es soll nicht nur die Rolle des Bundesamtes für Sicherheit in der Informationstechnik stärken, sondern darüber hinaus auch den Fokus auf allgemein vernetzte Systeme wie Industrial Control Systems oder IoT-Geräte richten.

PRÄVENTIV BIS INS LETZTE GLIED

Vorgesehen ist zum Beispiel, dass die gesamte Zulieferkette im KRITIS-Bereich künftig strengere Sicherheitskriterien und Prozesse einhalten soll. Das heißt im Klartext, Unternehmen und Behörden werden unter anderem Systeme zur Angriffserkennung und -bewältigung, sprich Security Incident & Event Management Systeme, kurz SIEM, betreiben müssen. Für die Architektur solcher Systeme gibt das BSI bestimmte Mindeststandards vor.

Als langjähriger Systemintegrator für kritische Infrastrukturen und Industrie 4.0 hat Telent beispielsweise umfangreiche Erfahrungen mit regulatorischen Verfahren, so das Unternehmen in einer Mitteilung. Von der Schwachstellenanalyse über die Netzplanung mit Notfallkonzept bis zur Umsetzung von Managed-Security-Konzepten (SIEM/SOC) inklusive Echtzeitüberwachung erhalten Kunden eine schlüsselfertige, auf ihre Bedürfnisse angepasste Lösung, heißt es weiter.

HIGHTECH GEGEN HACKER

»Dazu gehören auch moderne Netzwerklösungen mit umfangreichen Funktionen für die Überwachung und Abwehr von Sicherheitsbedrohungen in vernetzten Infrastrukturen«, so Telent. Ein Beispiel sei die Cisco Digital Network Architecture (DNA). Mit dieser softwaregesteuerten Netzwerkarchitektur lassen sich IT-Prozesse vereinfachen, Benutzer, Geräte und vor allen Dingen Bedrohungen transparent abbilden und Betriebsabläufe effizienter gestalten.

Wiederkehrende Aufgaben wie zum Beispiel die Netzwerkkonfiguration werden darüber hinaus automatisiert. Des Weiteren verschaffe die Cisco Identity Services Engine (ISE) konsistente Sicherheit beim Zugriff durch Nutzer anhand eines zentralisierten, einheitlichen Management von Netzwerkrichtlinien, heißt es. Dabei spiele es keine Rolle, ob die Verbindung über ein Kabel-, Wireless- oder ein VPN-Netzwerk erfolge.

WENN SICH DER NORMALZUSTAND ÄNDERT

Auch der Einsatz von sogenannten Anomaly-Detection-Systemen, Lösungen, die Anomalien erkennen, trägt zum Schutz sensibler Infrastrukturen bei. »Egal ob ein Netzwerkgerät plötzlich ein anderes Kommunikationsprotokoll nutzt oder der Netzwerkverkehr ungeplant eine neue Route nimmt, diese Systeme erkennen solche Vorgänge frühzeitig und alarmieren die entsprechenden Stellen«, heißt es aus dem Hause Telent.

Um eine Anomalie, also eine Normabweichung beziehungsweise ein unerwartetes Verhalten überhaupt zu identifizieren, muss zuerst einmal der Normalzustand erfasst werden. Dazu analysiert das System die IT-Architektur und lernt im Hintergrund.

ITK-Systeme kritischer Infrastrukturen benötigen besonderen Schutz. Grundvoraussetzung ist ein ganzheitlicher Ansatz, der die Menschen, Prozesse und Systeme einbezieht, denn nur so lassen sich die richtigen Lösungen finden und etablieren.

Eine durchdachte Strategie für Cybersecurity eröffnet Unternehmen neue Möglichkeiten – sie schaffen dadurch nicht nur Innovation und Wachstum, sondern können sich auch als vertrauenswürdige Geschäftspartner positionieren. ***ls***

E-world Halle 5, Stand 203 | www.telent.de

CHECKLISTE

Der Weg zum sicheren Netz

- Einsatz von Systemen zur Angriffserkennung und Angriffsbewältigung.
- Transparenz von Benutzern, Geräten und Betriebsabläufen.
- Zentralisiertes, einheitliches Management von Netzwerkrichtlinien.
- Analyse der IT-Architektur.
- Frühzeitiges Erkennen von Anomalien mit umgehender Benachrichtigung entsprechender Stellen. ***ls***

Bild: Nikolai Tsvetkov - stock.adobe.com