PMeV NETZWERK SICHERE KOMMUNIKATION
KOMPAKT Nr. 3/2020

Cybersecurity für KRITIS-Betreiber: Bundesregierung erhöht die Anforderungen

Von Nico Werner*

Kritische Infrastrukturen (KRITIS) sind für die Sicherheit von Staat und Gesellschaft essenziell. Daher stehen die Betreiber Kritischer Infrastrukturen in der Pflicht, ihre sensiblen und meist komplexen Systeme optimal und mit oberster Priorität langfristig zu schützen. Diese Intention verfolgt auch der Referentenentwurf für das zweite Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (ITSiG 2.0), den das Bundesministerium des Innern, für Bau und Heimat 2019 vorgelegt hat. Der Referentenentwurf befindet sich derzeit noch in der Ressortabstimmung der beteiligten Bundesministerien.

Wie sehen die Grundzüge des Referentenentwurfs der Bundesregierung aus? Das ITSiG 2.0 würde das Bundesamt für Sicherheit in der Informationstechnik (BSI) mit mehr Autorität ausstatten und beispielsweise Hackeraktivitäten und den Betrieb verbotener Marktplätze im Darknet kriminalisieren. Zudem soll ein neues Kennzeichen die IT-Sicherheit von Produkten sichtbar machen. Der Fokus soll in Zukunft auf allgemein vernetzten Systemen oder IoT-Geräten liegen. KRITIS-Betreiber wie Energieversorger, Verkehrsunternehmen oder Sicherheitsbehörden müssen künftig strengere Sicherheitskriterien und Prozesse einhalten und sogenannte Systeme zur Angriffserkennung und -bewältigung (Security Incident & Event Management Systeme, SIEM) sowie Informationssicherheitsmanagementsysteme (ISMS) wirksam betreiben. Das BSI gibt dafür bestimmte Mindeststandards vor: Es dürfen nur Komponenten von Herstellern verbaut werden, die das Sicherheitskennzeichen tragen. Insbesondere für mittlere und kleine Unternehmen könnten aus den neuen Anforderungen Probleme erwachsen: Denn ihnen fehlen häufig die internen Ressourcen und das Know-how. Die Lösung für sie könnte lauten: Managed Security – der Weg zur sicheren und zukunftsorientierten Infrastruktur.

PMeV - Netzwerk sichere Kommunikation
Professioneller Mobilfunk e. V. • Schönhauser Allee 10-11 • 10119 Berlin
Vorsitzender: Hytera Mobilfunk GmbH • Bernhard Klinger
Redaktion: Jochen Müller • Kommunikation & Public Affairs • Hobsweg 78 • 53125 Bonn
www.pmev.de • mueller@pmev.de

Neu im PMeV:

Pfalzwerke Netz AG

Pfalzwerke Netz
Pfalzwerke Gruppe

Die Pfalzwerke Netz AG (PWN) mit Sitz in Ludwigshafen wurde 2012 gegründet und gehört als 100-prozentige Tochter zur Pfalzwerke AG.

Thomas Stieler

Das Unternehmen betreibt Umspannwerke und ca. 4000 Mittelspannungsanlagen und Ortsnetzstationen auf einer Fläche von etwa 6000 km². Seit 2017 nutzt die PWN für die Krisen- und Notfallkommunikation ein DMR-Funknetz (vorher analoge Gleichwelle) im 4m Bereich, das besonders bei Ausfall von Strom und öffentlicher Kommunikation von Nutzen ist. Neben Betriebsfunk verfügt man über ein Fernwirkfunknetz, um E-Stationen im gesamten Netzgebiet überwachen und fernsteuern zu können.

Die Funkabteilung der PWN agiert als interner Dienstleister für die drahtlose Kommunikation im Unternehmen. Bei den Nutzern des Betriebsfunks handelt es sich größtenteils um die Mitarbeiter im Netzservice, die vorrangig über den Betriebsfunk miteinander und zur Koordinierung mit der Netzleitstelle kommunizieren. Der Fernwirkfunk wird exklusiv von der Netzleitstelle zur Überwachung und Fernsteuerung genutzt.

Thomas.Stieler@pfalzwerke-netz.de
www.pfalzwerke.de/pfalzwerke-gruppe

SIEM as a Service

Die steigende Komplexität von Technologien für Infrastrukturen, Anwendungen, virtuelle Maschinen, Clouds, Endgeräte und das Internet der Dinge (IoT) birgt ein verstärktes Risiko von Hackerangriffen und Ausfällen durch menschliches Versagen. Für IT-/OT-Infrastrukturen ist daher die kontinuierliche Kontrolle aller digitalen Prozesse, Netzkomponenten und eingebundenen Geräte erforderlich. Nur so ist Transparenz in der kompletten Infrastruktur gewährleistet. Bei der herkömmlichen IT stehen Kommunikation und Vertraulichkeit im Mittelpunkt, während in der OT (Operational Technology) besonders Verfügbarkeit und Sicherheit wichtig sind. Gerade für mittlere und kleine Unternehmen bietet es sich an, mit Spezialisten zusammenzuarbeiten, die ihnen mit einem ganzheitlichen Ansatz und solider Erfahrung in den Bereichen Sicherheit, Netze und Prozesse zur Seite stehen.

Spezialisierte Systemintegratoren bieten beispielsweise umfassende Sicherheitslösungen und Dienstleistungen aus einer Hand, die diese Kriterien erfüllen und KRITIS-Kunden mit einem rechtssicheren Gesamtpaket unterstützen. Von der Schwachstellenanalyse über die Netzplanung mit Notfallkonzept bis zur Umsetzung von Managed-Security-Konzepten inklusive Echtzeitüberwachung erhalten Kunden eine jeweils bedarfsorientierte und schlüsselfertige Lösung.

Managed-Security-Lösungen beinhalten sowohl SIEM-Sicherheitstools als auch skalierbare Supportleistungen für den Schutz von IT-/OT-Umgebungen sowie maßgeschneiderte Lösungen für Multi-Vendor-Umgebungen. Hierzu steht fortschrittliche Hard- und Software inklusive maschinelles Lernen und Künstliche Intelligenz (KI) zur Verfügung, um den Datenfluss lückenlos zu überwachen. Umfangreiche Korrelationsinformationen und Algorithmen lösen Alarme aus und weisen auf verdächtige Bedrohungen hin.

Netzwerkplattformen, die solche Analytics-Funktionen bereits in ihrer Architektur implementiert haben, sind z. B. Cisco DNA (Distributed Network Architecture) und Cisco ISE (Cisco Identity Services Engine). Auf der Basis von KI und maschinellem Lernen ermöglicht Cisco DNA eine einfache Verwaltung aller Geräte und Dienste, löst Netzwerkprobleme und sorgt für eine bessere Benutzerfreundlichkeit im gesamten Netzwerk. Mit einer umfangreichen Umbrella-Funktion erlaubt Cisco ISE u. a. die richtliniengesteuerte Zugriffskontrolle in der gesamten Infrastruktur, was für maximale Sicherheit vom Kabel- über das Wireless- bis hin zum VPN-Netzwerk sorgt.

Das zentrale Management verschafft einen transparenten Überblick über Benutzer und Geräte im Netzwerk. Einen integrierten Schutz vor Bedrohungen während und nach einem Angriff bietet Cisco Firepower, die erste vollständig integrierte Next-Generation Firewall (NGFW) mit Unified Management. Firepower-Geräte unterstützen die Integration mit SIEM-Tools von Drittanbietern.

SOC as a Service

Die eingesetzten Lösungen erkennen Bedrohungen und schützen die Infrastruktur. Zusätzlich ist ein sogenanntes Security Operation Center (SOC) erforderlich. Ein SOC verfügt über ein Team von ausgebildeten Experten, welches Netzwerke kontinuierlich überwacht, proaktiv nach Bedrohungen sucht, sie erkennt und neutralisiert. Der Aufbau eines SOC – oder die generelle Schaffung einer solchen Funktion im Unternehmen – ist eine kostspielige und zeitaufwändige Aufgabe, die ständige Anpassungsmaßnahmen erfordert, um effektiv zu sein. Zahlreiche Unternehmen entscheiden sich dafür, kein eigenes SOC aufzubauen. Stattdessen wählen sie andere Optionen zur Sicherheitsüberwachung wie z. B. die Beauftragung eines Managed-Security-Service von spezialisierten Sicherheitsfirmen. Sie sparen somit erhebliche Investitionen.

Ein komplettes Managed-Security-Portfolio eines spezialisierten Sicherheitsunternehmens kann u.a. beinhalteten:

- 24/7-Netzwerküberwachung, Bedrohungserkennung
- Echtzeit-Alarme und schnelle Reaktion
- Integrierter Incident-Management-Workflow
- Behebung von Angriffen und Ausfällen

Fazit

Das noch im Abstimmungsverfahren befindliche ITSiG 2.0 wird die Anforderungen an den besonderen Schutz der ITK-Systeme kritischer Infrastrukturen nochmals erhöhen. Grundvoraussetzung zur Erfüllung der Anforderungen 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.

*Der Autor:
Nico Werner ist Vorsitzender des PMeV-Fachbereichs Cybersecurity und Head of Cybersecurity bei der telent GmbH, einem Mitgliedsunternehmen des PMeV

Nico.Werner@telent.de

Bild S.1: Adobe/telent GmbH