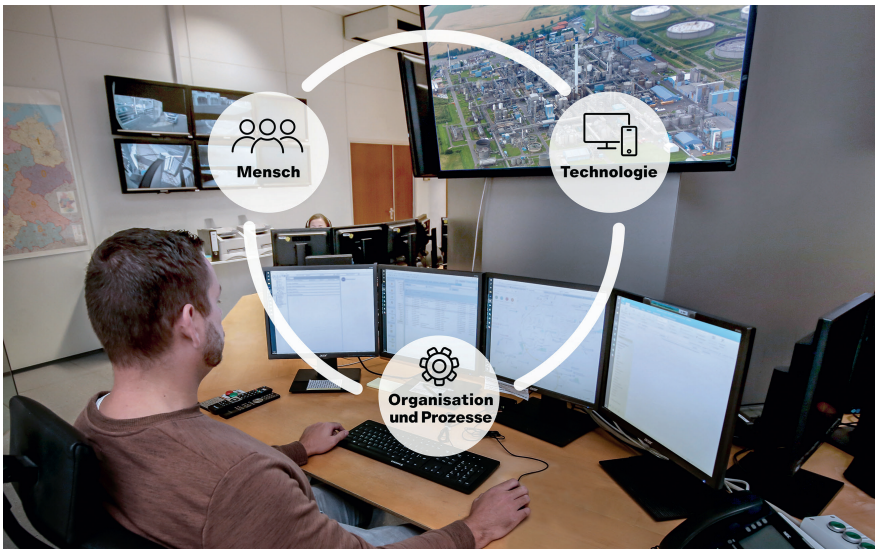
Die Energienetze der Zukunft

Eine permanente Security-Herausforderung

Die Zeiten für Energieversorger und Energienetzbetreiber sind aktuell alles andere als langweilig. Netze müssen für die Zukunft fit gemacht werden, damit die Energiewende reibungslos vollzogen werden kann. Die mit der Digitalisierung einhergehende Transformation umfasst technische und organisatorische Neuaufstellungen, aber auch Veränderungen, die aus neuen Geschäftsmodellen und aus neu entstehenden Produkten und Dienstleistungen heraus eingeleitet und vorangetrieben werden. Und dabei muss die digitalisierte Stromwelt vor allem eines sein: hochverfügbar und sicher.

Zu beneiden ist die Branche wirklich nicht: Sie muss die sich in voller Fahrt befindliche Energiewende meistern. Die ehemals als reine Verbrauchernetze konzipierten Verteilungsnetze müssen nun derart umgestaltet werden, dass dezentral Energie eingespeist und an geeignete Verbraucher verteilt werden kann. Das Verteilnetz muss also zusätzlich die Aufgabe als „Einsammelnetz“ übernehmen. Hand in Hand mit der Energiewende kommt die erwartbar boomende E-Mobilität, die weitere Herausforderungen im Lastmanagement und in Verteilerspitzen mit sich bringt. Ein passendes Lademanagement muss dies abfangen.

Die Veränderungen bei den Energieerzeugern und die wachsenden Anforderungen der Verbraucher machen einen Netzausbau unumgänglich – eine nicht zu unterschätzende Herausforderung, denn es gibt nicht „das eine Energieversorgungsnetz“. Vielmehr ist es ein Verbund aus verschiedenen Teilnetzen, die zu unterschiedlichen Zeiten errichtet wurden und unterschiedliche Hardware und Technologien nutzen. Selbst innerhalb der einzelnen Teilnetze ist keine homogene Technologielandschaft vorzufinden, was die Steuerung und Überwachung schwierig gestaltet.



Der Aufbau organisatorischer Sicherheit gelingt besonders gut, wenn Betreiber und Dienstleister beziehungsweise Netzausrüster eng und interaktiv in allen Projektphasen zusammenarbeiten. *Bild: telent*

Heterogenität im Zusammenspiel

Über die Energieversorgungsnetze erstrecken sich deshalb bereits seit vielen Technologiegenerationen die betrieblichen Kommunikationsnetze der Versorger, um die notwendigen netzübergreifenden Steuer-, Mess-, Überwachungs- und Kommunikationsaufgaben im Rahmen des Netzbetriebes zu ermöglichen. Auch dieses „Netz im Netz“ spiegelt die Heterogenität der im Zusammenspiel erforderlichen Betriebsmittel.

Eine Prämisse steht jedoch über allem: Die Versorgung muss jederzeit sichergestellt sein. Nicht grundlos hat die Bundesregierung den Energiesektor als Kritische Infrastruktur (Kritis) definiert. Die unmittelbaren Auswirkungen auf die Gesellschaft und die Wirtschaft durch einen Ausfall oder bereits durch größere Stö-

rungen wären massiv. Selbst für gestandene Netzintegratoren wie die telent GmbH, die auf eine über 50-jährige Expertise zurückblicken kann, ist dies eine herausfordernde Aufgabe – aber eine, der sie sich stellt.

Spezial-Protokolle treffen auf kurzlebige IT

Als wäre der Wandel im Energietransport und Netzausbau nicht schon genug, treiben smarte Geräte und digitalisierte Dienste und Produkte die Transformation hin zu grüner Energie. Unzählige IoT-Komponenten kommen hier zum Einsatz und werden miteinander vernetzt. Die Energienetze wandeln sich dadurch zu echten „Multifunktionsnetzen“. Hier entsteht jedoch das nächste Problem. Die Produktivumgebung arbeitet mit langlebiger, auf speziellen Kommunikationsprotokollen basierender und nur bedingt veränderbarer IT, sogenannter OT (operational technology); diese trifft nun auf kurzlebige IT-Produkte, die sich anderer Protokolle und Designmethoden bedienen.

Die technologischen Hürden, die etwa durch das Nutzen unterschiedlicher Protokolle entstehen, lassen sich dabei technisch durch entsprechende Schnittstellen und Übergänge lösen. Allerdings sind viele der OT-Protokolle per Design unsicher. Gängige, in der IT selbstverständliche Sicherheitsmaßnahmen, wie etwa Authentifizierung und Verschlüsselung, sind schlichtweg nicht vorhanden. OT-Protokolle wurden entwickelt, um physische Komponenten wie Ventile, Pumpen, Motoren oder Sensoren zu steuern und zu überwachen. Höchste Prämisse ist die Verfügbarkeit. Frühere Hardwaregenerationen brachten oft auch nicht die Rechenleistung auf, die beispielsweise aktuelle Verschlüsselungsalgorithmen als selbstverständlich voraussetzen. Dagegen hat in der IT die Sicherheit einen übergeordneten Stellenwert, die oft nur mit betrieblichen Prozessen, wie regelmäßigem Patchmanagement, erreichbar, in OT-Umgebungen häufig aber nicht praktikabel ist. Mit der Digitalisierung werden die Übergänge zwischen IT und OT unschärfer, beide Technologien verschmelzen. Im Fall der Versorgungsnetze in einem Gesamtsystem, in dem Verfügbarkeit die höchste Priorität hat.

Ein Verbund aus verschiedenen Teilnetzen, die zu unterschiedlichen Zeiten errichtet wurden und unterschiedliche Hardware und Technologien nutzen, ist eine Herausforderung für die IT-Security. *Bild: telent*

Cybersecurity in neuem Rahmen denken

Die Vernetzung wird intensiver und komplexer, die Anzahl von Punkten, über die auf – meistens der OT zuzurechnenden – Komponenten zugegriffen wird, steigt. Und damit auch mögliche Angriffspunkte für Cyberkriminelle und Hacker. Daher verwundert es nicht, dass Energieversorger als lohnendes Angriffsziel identifiziert wurden. Laut Lagebericht 2020 des Bundesamtes für Sicherheit in der Informationstechnik (BSI) wurden im Berichtszeitraum im Energiesektor 73 IT-Sicherheitsvorfälle übermittelt, die nach dem IT-Sicherheitsgesetz seit 2015 zu melden sind. Eine nicht unerhebliche Anzahl dieser Vorfälle zielte dabei explizit auf OT-Steuerungskomponenten ab. Die Behebung – die nur unter Zuhilfenahme externer Dienstleister zu verwirklichen war – dauerte teilweise Monate.

Nur dank der vorhandenen Redundanzen und aufgrund des Designs des Netzes ist kein „Blackout“ eingetreten, wie es Marc Elsberg in seinem gleichnamigen Romanbestseller beschreibt. Die seit Jahren steigende Zahl der meldepflichtigen Vorfälle oder die Angriffe auf das ukrainische Stromnetz in den Jahren 2015 und 2016 zeigen, dass die Gefahr eines kritischen Angriffs, der die Versorgung maßgeblich beeinträchtigt, besteht. In Zukunft werden in den Netzen große Menge Daten von Kunden und Dienstleistern gespeichert sein, die attraktiv für Hackerangriffe und daher besonders schützenswert sind. Dementsprechend wichtig ist es – auch um das Ziel der höchstmöglichen Verfügbarkeit zu garantieren – Maßnahmen zu ergreifen, die die Cybersecurity gewährleisten.

Fortschrittlicher Technologiemix aus Hard- und Software

Das bedeutet natürlich nicht, dass bewährte Securitymaßnahmen, wie etwa Firewalling und die Netzwerksegmentierung, obsolet wären. Im Gegenteil: Sie sind immer noch ein wichtiger Baustein, um ein angemessenes Maß an Security überhaupt gewährleisten zu können.

Dazu kommen ein fortschrittlicher Technologiemix aus Hard- und Software, Maschinelles Lernen (ML) und Künstliche Intelligenz (KI) sowie Anomaly Detection, um den Datenfluss lückenlos zu überwachen. Netzwerkplattformen, die solche Analytics-Funktionen bereits in ihrer Architektur implementiert haben, sind zum Beispiel Cisco DNA (Digital Network Architecture) und Cisco ISE (Identity Services Engine). Auf der Basis von KI und ML ermöglicht Cisco DNA eine einfache Verwaltung aller Geräte und Dienste, priorisiert und löst Netzwerkprobleme. Mit einer umfangreichen Umbrella-Funktion erlaubt Cisco ISE unter anderem richtliniengesteuerte Zugriffskontrolle in der gesamten Infrastruktur, was für maximale Sicherheit vom Kabel- über das Wireless- bis hin zum VPN-Netzwerk sorgt, und damit hilft, eine zentrale Anforderung des Informationssicherheitsmanagements in seiner branchen-

spezifischen Ausprägung, dem BDEW-Whitepaper, zu erfüllen. Das zentrale Management bringt einen transparenten Überblick über Benutzer und Geräte im Netzwerk.

Ein erster, unverzichtbarer Schritt hin zu einer agierenden, vorausschauenden Cybersecurity ist der Einsatz eines Security Information und Event Managements (SIEM). Das System, das die zwei Konzepte Security Information Management (SIM) und Security Event Management (SEM) vereint, ermöglicht einen ganzheitlichen Blick auf die eigene IT-Security. Dazu werden Meldungen, Logfiles und andere Daten aus allen relevanten Teilen der Infrastruktur gesammelt und ausgewertet. Dadurch lassen sich verdächtige Ereignisse, Angriffe und andere Bedrohungen in Echtzeit erkennen und angemessene Gegenmaßnahmen einleiten. Diese technischen Lösungen erkennen Bedrohungen und schützen die Infrastruktur.

Zusätzlich empfiehlt sich aber auch der Einsatz eines Security Operation Centers (SOC). Das ist ein Expertenteam, das Netzwerke kontinuierlich überwacht, nach Bedrohungen sucht und Gegenmaßnahmen vorbereitet. Der Aufbau eines effektiven SOC ist ressourcen- und zeitaufwendig. Daher entscheiden sich zahlreiche Unternehmen, einen erfahrenen Anbieter von Managed Security Services zu Rate zu ziehen, und beauftragen diesen, die SOC-Funktion wahrzunehmen.

Angesichts der neuen Anforderungen ist es ratsam, die vorhandenen Systeme zu erweitern, um eine bestmögliche Überwachung des eigenen Netzwerks und angemessene, zeitnahe Reaktionen auf Bedrohungen zu haben. So können Sicherheit und Verfügbarkeit des gesamten Netzes gewahrt werden.

Security ist mehr als Technik

Technisch ist es heute schon möglich, die Netze von morgen abzusichern. Selten sind es jedoch nur technische Maßnahmen oder spezialisierte „Sicherheitsprodukte“, die im ersten Schritt ausschlaggebend sind. Bewährt und sinnvoll sind zunächst die Definition des individuellen Schutzbedarfes, der Schutzziele und die Identifikation der relevanten Bedrohungen und Risiken. So wird es möglich, die Anforderungen in das richtige Verhältnis zu setzen, bevor eine technische Empfehlung ausgesprochen wird. Als wichtigste Schutzziele gelten in der Regel Verfügbarkeit, Integrität, Vertraulichkeit, Authentizität und Verbindlichkeit.

Zur Erreichung der organisatorischen Sicherheit sind Maßnahmen, wie der Aufbau und der Betrieb eines Informationssicherheitsmanagementsystems (ISMS), unverzichtbar. Dies gelingt besonders gut, wenn Betreiber und Dienstleister beziehungsweise Netzausrüster eng und interaktiv in allen Projektphasen zusammenarbeiten und der Sicherheitsgedanke den gesamten Zyklus „Konzeption – Design – Implementierung – Betrieb“ sowie die Dokumentation durchdringt.

Zu guter Letzt sollten Unternehmen die organisatorische Sicherheit bezüglich des Faktors Mensch erhöhen. Denn im Normalfall sind die Menschen jene Komponente, die am leichtesten zu „hacken“ ist, die in ihrer täglichen Arbeit die definierten Prozesse leben und die (Security-)Technologie kontrollieren müssen. Oder um es mit dem Security-Experten Bruce Schneier zu sagen: „Nur Amateure greifen die Technologie an, Profis nehmen den Menschen ins Visier.“

Die aktuellen Herausforderungen sind offensichtlich vielfältig. Um sie zu lösen, benötigt es einen Partner, der im Aufbau von Netzen und den eingesetzten Technologien Know-how vorweist. IT-Sicherheitsaspekte sind zentraler Bestandteil von Netzen, Systemen und den zugehörigen Betriebsprozessen. Dies führt zu neuen Formen der Zusammenarbeit zwischen Kritis-Betreibern und ihren Integratoren und Dienstleistern für die betriebliche Kommunikationsinfrastruktur. Eine Form der Zusammenarbeit, die nur möglich ist, wenn eine robuste Vertrauensbasis etabliert wird. ■

www.telent.de

Jakob Schmidt

Coordinator Awareness Koramis, Kompetenzzentrum für Cybersecurity bei der telent GmbH

j.schmidt@koramis.de

Bild: telent

Dr. **Reinhard Wegener**

Director Technology Center bei der telent GmbH

reinhard.wegener@telent.de

Bild: telent