IT-SICHERHEIT

Fachmagazin für Informationssicherheit und Datenschutz

Sonderausgabe
2|2017

KRITISCHE INFRASTRUKTUREN

Gewappnet für den Ernstfall

MITHERAUSGEBER:

KASPERSKY

SECUrisk

protekt

DATAKONTEXT

www.itsicherheit-online.com

Vorsicht, Cyberangriff! Spezifischer I -Schutz für kritische und industrielle Infrastrukturen

Die Risiken für Organisationen und Einrichtungen im Bereich kritischer Infrastrukturen sind heute so hoch wie nie zuvor. Cyberangriffe auf Kraftwerke, Anlagen oder Produktionssysteme haben dabei eine Tragweite, die weit über finanzielle Schäden und den geschäftlichen Reputationsverlust hinausgeht. Vielmehr stehen hier ökologische, soziale und makroökonomische Konsequenzen im Vordergrund – eine Herausforderung an die Cybersicherheit.

Kritische Infrastrukturen stehen heute auf einem viel höheren Bedrohungslevel als noch zu Zeiten, in denen Cybersecurity nur eine Frage der physischen Sicherheit war. Der Grund: die wachsende Vernetzung. Während in der Vergangenheit industrielle Kontrollsysteme (Industrial Control Systems, ICS) und kritische Infrastrukturen in physisch isolierten Umgebungen betrieben wurden, ist dies in der Industrie 4.0 nicht immer der Fall. Laut Untersuchungsbericht „Industrial Control Systems Threat Landscape" von Kaspersky Lab sind weltweit 188.019 ICS-Rechner (Hosts) über das Internet erreichbar. Diese Tatsache eröffnet Cyberkriminellen die Möglichkeit zur Fernsteuerung kritischer ICS-Komponenten. Ein solcher Zugriff von extern kann Schäden von Anlagenteilen zur Folge haben und stellt eine potenzielle Gefahr für die gesamte Versorgungskette dar.

Der Bericht zeigt zudem folgenden sicherheitsrelevanten Zusammenhang auf: Je größer die Infrastrukturen industrieller Kontrollsysteme sind, desto größer ist auch das Risiko empfindlicher Sicherheitslücken. Dies ist besonders bedenklich, da insgesamt 13.698 der via Internet erreichbaren ICS-Hosts großen Organisationen aus den Bereichen Energie, Transport, Luft- und Raumfahrt, Industrie, öffentlicher Sektor oder Finanzen zugeschrieben werden können. Darüber hinaus belegt die Untersuchung, dass in den vergangenen fünf Jahren generell die Anzahl gefundener Schwachstellen innerhalb von ICS-Komponenten um das Zehnfache gestiegen ist.

BlackEnergy: Angriff auf Energiesektor

Ein Beispiel für gezielte, hochentwickelte Cyberangriffe auf ICS-Systeme ist BlackEnergy. Im Dezember 2015 gelang Hackern eine koordinierte

Attacke auf mindestens drei Energienetzbetreiber in der Ukraine. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) erläutert in seinem Bericht zur Lage der IT-Sicherheit in Deutschland 2016, dass hinter den Angriffen die Sandworm-Gruppe vermutet wird, die bereits früher mit der Schadsoftware BlackEnergy in Verbindung gebracht wurde. Im Fall der aktuellen Attacke auf den Energiesektor kamen mutmaßlich Spear-Phishing-E-Mails zum Einsatz, die Mitarbeiter zum Öffnen von schädlichen Anhängen bewogen haben. Die Cyberkriminellen spielten dann die Schadsoftware auf Systeme mit veralteten Softwareständen auf, deaktivierten die Stromverteilung und löschten spezielle Software. Parallel dazu führten sie einen DDoS-Angriff auf das Callcenter des Versorgungsunternehmens durch. Mindestens 225.000 Einwohner der Ukraine waren von einem mehrstündigen Ausfall der Stromversorgung betroffen.

Conficker: Ke nkraftwerk im Visier

Grundsätzlich sind KRITIS-Betreiber den gleichen Gefahren ausgesetzt wie andere Unternehmen. Nicht selten sind die in Anlagen eingesetzten PCs mit der gleichen Malware infiziert die auch IT-Systeme in Unternehmen befällt. Darunter bekannte Übeltäter wie Würmer, Trojaner oder Viren. So attackierte der Conficker-Wurm, der nicht speziell auf industrielle Systeme zugeschnitten ist, im April 2016 das Betreiberunternehmen des deutschen Kernkraftwerks Gundremmingen. Er infizierte die Rechner der Brennelemente-Lademaschine in Block B. Glücklicherweise hatte der Wurm keinen Einfluss auf die technologischen Prozesse und das Kraftwerk wurde nicht beschädigt.

Industrielle Cybersicherheit stellt andere Anforderungen

Es mag bei den Bedrohungen einige Überschneidungen geben, die cybersicherheitstechnischen Anforderungen von kritischen beziehungsweise industriellen Infrastrukturen und die von Unternehmen aus anderen Bereichen unterscheiden sich jedoch erheblich. In Unternehmensumgebungen liegt der Schwerpunkt auf dem Schutz vertraulicher Daten. Wenn es um ICS/SCADA-Systeme (Supervisory Control and Data Acquisition Systems) und Einrichtungen in Bereichen wie Energieversorgung, Trinkwassergewinnung oder Datenübertragung geht, zählt jede Minute Ausfall- oder Fehlerzeit. Deshalb haben hier die Verfügbarkeit der IT und ein unterbrechungsfreier Betrieb höchste Priorität.

Cybersicherheitsanbieter müssen also Lösungen bereitstellen, welche die Unterschiede zwischen industriellen Steuerungssystemen und kritischen Infrastrukturen auf der einen sowie betriebswirtschaftlich ausgerichteter Unternehmens-IT auf der anderen Seite berücksichtigen.

Beispiel Automobil-Zulieferer

Kaspersky Lab hat mit Kaspersky Industrial CyberSecurity eine Lösung entwickelt, die speziell auf den Schutz von kritischen Infrastrukturen und komplexen Industrieanlagen ausgerichtet ist. Im Einsatz ist die Software beispielsweise bei der AGC Glass Germany GmbH. Das Unternehmen komplettiert seit 2003 Automobilglas für namhafte Hersteller wie BMW, VW, Mercedes, Volvo oder Opel. Es beschäftigt am Standort Wegberg in der Nähe von Mönchengladbach 150 Mitarbeiter und ist Teil der japanischen Asahi Glass Company, einem weltweit führenden Glashersteller.

Als Zulieferer für die Automobilindustrie ist AGC auf die Kontinuität der betrieblichen Abläufe angewiesen. Jede Produktionslinie wurde deshalb durch die Lösung abgesichert, die sämtliche Aktivitäten scannt und sofort alarmiert, wenn Abweichungen bei der Produktion vorliegen.

Ganzheitlicher Ansatz

Kaspersky Industrial CyberSecurity bietet auf allen Ebenen von Industriesystemen effektive Sicherheit vor Cyberbedrohungen. Damit schützt die Lösung auch zum Beispiel SCADA-Server, HMI-Schnittstellen, Engineering-Workstations, speicherprogrammierbare Steuerungen (SPS) und Netzwerkverbindungen. Ein besonderer Schwerpunkt liegt dabei auf der Aufrechterhaltung der Geschäftskontinuität und der Gewährleistung von unterbrechungsfreien Industrieprozessen. Dank flexibler Konfiguratione kann die Lösung auf die individuellen Sicherheitsbedürfnisse einzelner industrieller Einrichtungen angepasst werden.

Kaspersky Industrial CyberSecurity umfasst folgende Leistungen:

- spezifische Schutztechnologien
- Schulungsangebote
- Expertenservices

For Nodes und for Networks

Kaspersky Industrial CyberSecurity for Nodes kombiniert signaturbasierte und heuristische Malware-Erkennungsmethoden, um Nodes vor Bedrohungen zu schützen. Zu den wichtigsten Funktionen der Lösung zählt außerdem die Kontrolle von Programmstarts. Whitelisting-Mechanismen blockieren hier die Ausführung aller nicht ausdrücklich gestatteten Programme. Zudem können Administratoren mithilfe der Gerätekontrolle festlegen, welche Wechseldatenträger mit geschützten industriellen Hosts verbunden werden dürfen. Über die hostbasierte Firewall lassen sich Richtlinien zur Beschränkung der Netzwerkverbindungen zu Servern, HMIs oder Workstations festlegen und die Funktion Network Attack Blocker überwacht und blockiert verdächtige Aktivitäten auf industriellen Hosts. Ein automatischer Exploit-Schutz, die SPS-Integritätsprüfung und das Vulnerability Assessment, das Software-Schwachstellen und nicht installierte Updates oder Patches erkennt, gehören ebenfalls zum Funktionsumfang. Die Verwaltung aller Vorgänge erfolgt über eine einzige, zentrale Konsole – das Kaspersky Security Center.

Kaspersky Industrial CyberSecurity for Networks, die Sicherheitskomponente auf Netzwerkebene, überwacht den Datenverkehr und kontrolliert die Integrität des industriellen Netzwerks. Sie registriert plötzlich vorhandene, nicht autorisierte Geräte, erkennt neue Netzwerkkommunikation zwischen Nodes und kann Anomalien aufspüren, ohne technologische Prozesse negativ zu beeinflussen Die kontinuierliche Überwachung des Informationsflusses bietet nicht nur Schutz vor externen Bedrohungen, sondern senkt gleichzeitig das Risiko von Insider-Störungen durch Inge-

Die Komponenten für einen ganzheitlichen Sicherheitsansatz

nieure, SCADA-Bediener oder andere Mitarbeiter mit direktem Systemzugriff.

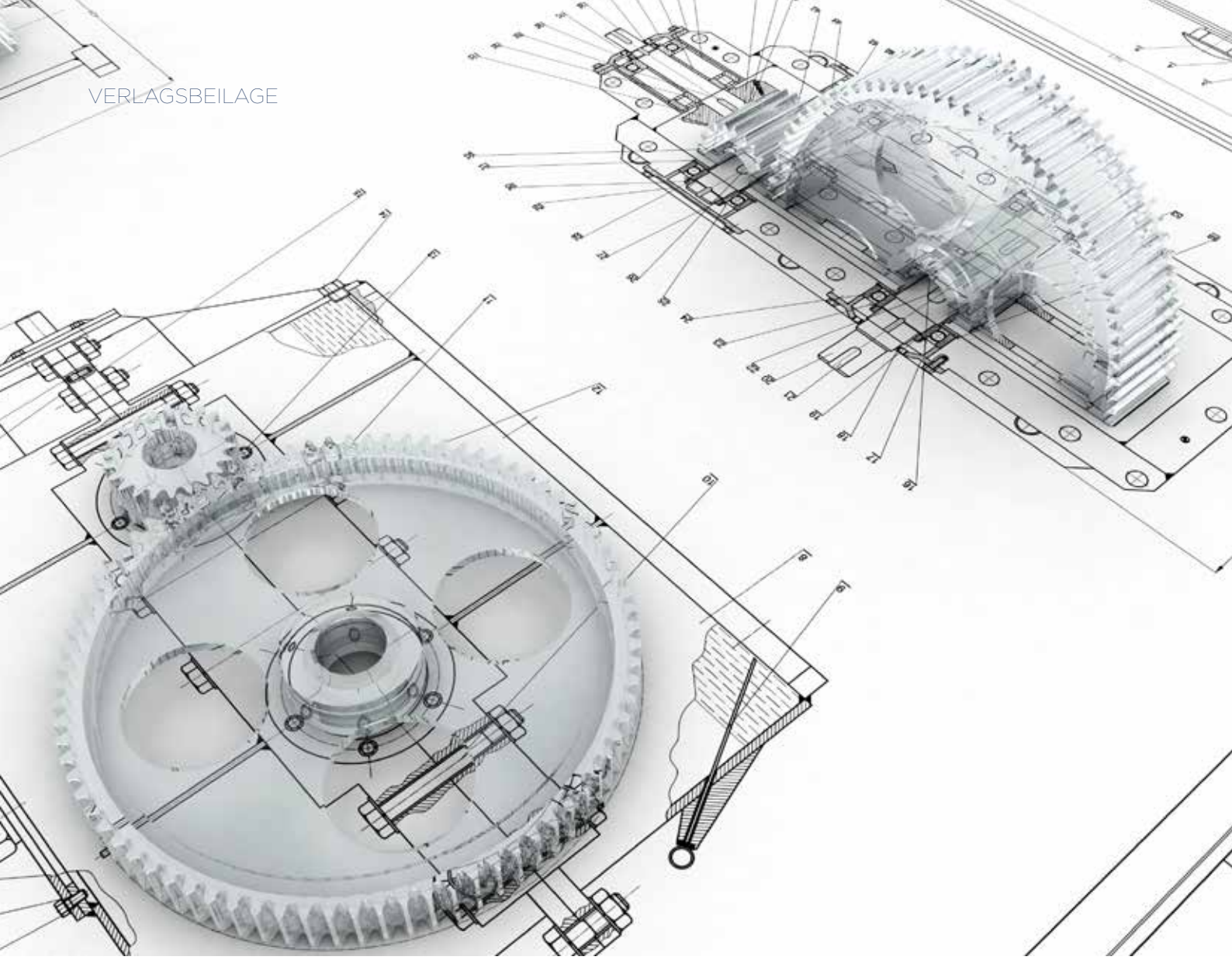
Schulungen und Expertenservices

Eine weitere Säule der industriellen Cybersicherheit bilden die Trainings- und Awareness-Programme von Kaspersky Lab. Sie helfen, Mitarbeiter für Cyberbedrohungen zu sensibilisieren und die Sicherheitskultur zu stärken. Kaspersky Lab bietet spezielle Schulungen für IT-Sicherheitsexperten sowie ICS-Bediener und -Ingenieure an. Außerdem können Industriekunden auf Sicherheitsberichte zurückgreifen, die sie mit aktuellen Informationen zur Bedrohungslage versorgen (Intelligence Reporting). Eine effektive Möglichkeit, auf spielerische Weise das Bewusstsein für Cybersicherheit im Unternehmen zu steigern, sind die interaktiven Kaspersky CyberSafety Games. Beispielsweise werden bei Kaspersky Industrial Protection Simulation (KIPS) echte Cyberattacken auf industrielle Automatisierungssysteme simuliert und die wichtigsten Probleme bei der Bereitstellung industrieller Sicherheit aufgezeigt. Für verschiedene Industriebereiche (Wasseraufbereitung, Energieerzeugung usw.) stehen unterschiedliche Versionen zur Verfügung.

Auch die Expertenservices sind ein wichtiger Teil von Kaspersky Industrial CyberSecurity. Im Rahmen der Cybersecurity-Assessments analysieren Experten das industrielle Netzwerk und helfen dabei, Sicherheitsanforderungen zu bestimmen. Außerdem unterstützt Kaspersky Lab KRITIS-Betreiber und Industrieunternehmen bei der Lösungsintegration und bietet Vorfallsuntersuchungen für Opfer einer Cyberattacke an. Hierzu analysieren Experten die eingesetzte Malware, rekonstruieren den Verlauf des Angriffs, bestimmen mögliche Quellen und Gründe und entwickeln einen Plan zur Problemlösung.

Weitere Informationen zu Kaspersky Industrial CyberSecurity finden Sie im Video unter https://kas.pr/KL_ICS und auf www.kaspersky.de/KICS

KASPERSKY lab



Noch ausbaufähig
Erste praktische Erfahrungen aus der Umsetzung der KRITIS-Verordnung

Das IT-SiG (IT-Sicherheitsgesetz) ist weitestgehend definiert. Am 03. Mai 2016 ist der erste Teil der Verordnung für KRITIS (kritische Infrastrukturen) in Kraft getreten. Betroffen sind Unternehmen aus Energie, Informationstechnik, Telekommunikation, Wasser sowie Ernährung. Der zweite Teil, für die Sektoren Finanzen, Transport, Verkehr und Gesundheit, wird in Kürze erwartet. Mit der Realisierung wurde indes bereits begonnen. Wie die ersten Praxisberichte zeigen, geht das kleinen wie großen Betrieben jedoch nicht allzu leicht von der Hand.

Denn eine zentrale Forderung ist es, ein ISMS (Informationssicherheitsmanagementsystem) umzusetzen und nachzuweisen. Über alle Sicherheitsbereiche hinweg wird dabei eines deutlich: Die Sicherheit in der Gebäudetechnik, also der Teil des Anforderungskatalogs, der sowohl vergleichsweise klein in der ISO 27001 als auch ausgiebig in der EN 50600 behandelt wird, wurde von den meisten RZ-Betreibern unterschätzt. Spätestens bei der Zertifizierung durch den TÜV oder andere Prüfinstitute nimmt dieser Teil dann eine wichtige Rolle ein. Ganz nach dem Motto „die beste Sicherung nützt nichts, wenn die Türe offen steht". Zusätzlich wird die Umsetzung der

ISMS durch eine verbesserungsfähige Kommunikation zwischen Facility-Managern und IT-Managern erschwert. Insgesamt ergeben sich in der Praxis daher Herausforderungen, bei denen Unternehmen auf Unterstützung angewiesen sind.

Die Standzeitkosten sind nur eine grobe Schätzung

So ist für KRITIS die Gesamtrisikoanalyse für Rechenzentren eine ernstzunehmende Aufgabe. Sie gliedert sich in die Ereignisrisikoanalyse und die Geschäftsrisikoanalyse. Erstere deckt Themen wie externe Bedrohungen durch beispielsweise Brand, Flugzeugabsturz, Bombenanschlag oder Einbruch ab und zählt heute eigentlich zum Standard in der Umsetzung. Oft fällt RZ-Betreibern bei der Geschäftsrisikoanalyse allerdings zum ersten Mal auf, dass sie sich zu wenige Gedanken über die wirtschaftlichen Folgen eines IT-Ausfalls gemacht haben. Bei einem Stromausfall schalten auch die Server ab. Hier entsteht im Rahmen der Geschäftsrisikoanalyse die erste Schnittstelle zwischen IT-Hardware, IT-Software, der Gebäudetechnik und dem Umsatz. Schließlich müssen Datacenter-Verantwortliche bei der Zertifizierung nach ISO 27001 auch die Standzeitkosten zumindest ansatzweise definieren können

Relativ einfach ist das, wenn die gesamte IT ausfällt: Dann sind entsprechend alle Geschäftsprozesse nicht mehr verfügbar und Unternehmen können gut abschätzen, wann sie zahlungsunfähig sind beziehungsweise wann es zu ernsthaften Konsequenzen für die Gesellschaft kommt. Für den Ausfall von einzelnen IT-Systemen, beispielsweise wenn die Stromverteilung für nur zehn Server unterbrochen ist, ist diese Analyse dann schon deutlich schwieriger. Aber die Norm fordert genau das: Unternehmen müssen die Standzeitkosten ursachengerecht berechnen. Mit anderen Worten, welcher Schaden entsteht für das Geschäft im Falle eines Einzelausfalls. Diese Kalkulation erweist sich in der Praxis als nahezu unmöglich. In einer virtualisierten Umgebung wissen die Wenigsten, welcher virtuelle IT-Dienst auf welchem physischen Server läuft, geschweige denn, können sie die Standzeitkosten ermitteln. Um die Zertifizierung nach ISO 27001 zu erhalten, wird daher die €-Zahl zum Geschäftsrisiko grob geschätzt.

Seit der EN 50600 existiert eine einheitliche Kategorisierung für die Verfügbarkeits- und Schutzklassen von Datacentern, so gesehen für den Ausfall des RZ respektive dessen Schutz vor externer Bedrohung. Sie regelt damit auch die Gebäudetechnik, inklusive der Stromversorgung. Diese Teile sind gemäß Norm ebenfalls einer Risikoanalyse zu unterziehen. RZ-Betreiber nehmen dies jedoch selten zum Anlass, um die Analyse mit der für die ISO 27001 zusammenzulegen. Zudem sind sie hier nicht selten durch die Schnittstellen zwischen Facility-Technik und IT überfordert. Organisatorisch sind diese beiden Welten seit jeher getrennt. Zu einer Kernaufgabe für die Umsetzung der KRITIS-Verordnung kristallisiert sich daher heraus, „einen Dolmetscher zu finden" Dabei bilden gerade die ISO 27001 aus dem IT-Bereich und die EN 50600 aus dem Gebäudetechnikbereich sehr gute Möglichkeiten, die beiden Organisationseinheiten strukturiert aneinander zu führen.

Zwischen Praxis und Theorie

Allgemein wird in der Praxis die potenzielle Nichtverfügbarkeit von Strom sträflich vernachlässigt. Zwar stellen sich professionelle Betreiber gerade in diesem Bereich überdimensioniert auf. Allerdings sind viele Bestands-RZ mit dem eigentlichen Betrieb der redundanten Stromversorgung überfordert. Zudem sehen sich bestehende Rechenzentren auch mit anderen Herausforderungen konfrontiert. So hadern viele beispiels-

weise bei der Umsetzung des Sicherheitszonenkonzepts, das ebenfalls durch die Norm EN 50600 definiert ist. Während ein neues Rechenzentrum entsprechend geplant werden kann, ist es denkbar schwierig im bestehenden Gebäude eine Wand zu versetzen, oder sie hinsichtlich der Brandschutzwerte aufzurüsten.

Im Besonderen Fall der Pflegeeinrichtungen entstehen dagegen eigene Probleme. So ist auch die Infrastruktur außerhalb des Datacenters, mit allen Knotenpunkten und Verteilern, Teil der KRITIS-Verordnung. Gerade aber diese Netzverteilerpunkte sind in Form von einzelnen kleinen Racks auf nicht selten 40 bis 50 verschiedene, kleine Räume verteilt. Sie sind wichtige Knotenpunkte für viele Endgeräte zum Beispiel auch in OP-Sälen. Allerdings sind sie meist weder gesichert, gekühlt oder mit einer USV-Anlage versehen. Fremdzugriffen sind diese Räume oft schutzlos ausgeliefert. Das öffnet Tür und Tor für Datendiebstahl, Datenmanipulation oder einfach nur Datenbeschädigung.

Die größten Unsicherheiten bestehen jedoch im Notfall- respektive Betriebsmanagement. Vor allem mittelständische Betriebe, die ihre RZ noch selber betreiben, haben selten einen konkreten Plan für Notfälle. Die KRITIS-Verordnung wurde jedoch gerade für den Ausnahmefall geschaffen. Hier suchen Unternehmen derzeit sehr häufig die Hilfe von Beratern. Nicht umsonst werden als Hilfsmittel Notfall-Handbücher für die Gebäudestruktur von Rechenzentren beauftragt. Solche Handbücher sind keine Standards, sondern werden individuell erstellt. Denn: Noch zu selten sind die die Abhängigkeiten der Gerätschaften beziehungsweise der gebäudetechnischen Anlagen im Datacenter dokumentiert. So müssen beispielsweise Alarme definiert Kommunikationswege detailliert aufgeschrieben und konkrete Maßnahmen festgehalten werden. In einem nächsten, großen Schritt folgen Workshops mit den Angestellten, in denen auch herausgefunden werden soll, wer für welche Aufgaben zuständig ist. Neukunden, die ein Rechenzentrum bauen lassen, bestellen dieses Notfall-Handbuch daher oft mit. Sie nutzen die Tatsache, dass die Arbeitsschritte und der Aufbau dem Dienstleister im Detail bekannt sind und die Erstellung der Handbücher entsprechen leichter und schneller geht.

Über den Autor:
Marc Wilkens ist Senior Consultant bei der SECUrisk, einem Unternehmen der DATA CENTER GROUP. Als Auditor für ISMS nach ISO 27001 und Experte im Normungskomitee der EN 50600 hält er Vorträge zu Sicherheit, Verfügbarkeit und Energieeffizienz in Rechenzentren. Zudem berät er Rechenzentrumsbetreiber für einen ganzheitlich optimierten Betrieb von Rechenzentren insbesondere für die Schnittstellen zwischen IT und Gebäudetechnik.

protekt 2017: IT-Sicherheit und physischer Schutz kritischer Infrastrukturen

Mit der stetig wachsenden Vernetzung und Digitalisierung steigt auch die Zahl der Cyber-Angriffe auf kritische Infrastrukturen. Unternehmen und Institutionen der KRITIS-Sektoren müssen deshalb Schutzmaßnahmen ergreifen – nicht nur aus eigenem Interesse, sondern auch aufgrund der rechtlichen Bestimmungen, die sich durch das IT-Sicherheitsgesetz ergeben. Auf der Konferenz und Fachausstellung für den Schutz kritischer Infrastrukturen protekt, die am 21. und 22. Juni in der KONGRESSHALLE am Zoo Leipzig stattfindet, werden die komplexen Bedrohungsszenarien und die Umsetzung des IT-Sicherheitsgesetzes eingehend diskutiert. Namhafte Referenten aus verschiedenen Bereichen vermitteln praktisches Expertenwissen und stellen Lösungsmodelle vor. Neben IT-spezifischen Aspekten werden auch Themen rund um die physische Sicherheit aufgegriffen.

Die Bundesregierung hat sich zum Ziel gesetzt, die Betreiber Kritischer Infrastrukturen durch gesetzliche Vorgaben wie dem IT-Sicherheitsgesetz (IT-SiG) dazu anzuhalten, Widerstandsfähigkeit und Schutzmaßnahmen zu verbessern. Gleichzeitig soll weiterhin auf Kooperation gesetzt werden, damit private Betreiber schon im eigenen Interesse in die Sicherheit ihrer Unternehmen investieren. Nicht zuletzt durch die ständig zunehmende Gefahr von Terror- und Cyberattacken ist jedoch eine neue Lage entstanden. Aktuell erneuert die Bundesregierung daher die Nationale Strategie zum Schutz Kritischer Infrastrukturen. Im Keynote-Vortrag mit dem Titel „Der Schutz Kritischer Infrastrukturen – zwischen Betreiberverantwortung und staatlicher Sicherheitsvorsorge – Zeit für eine neue KRITIS-Strategie?" informiert Ministerialrat Volker Amler, Referatsleiter Kritische Infrastrukturen im Bundesministerium des Innern (BMI) über aktuelle Konzepte und Ziele.

Seit dem Inkrafttreten des IT-SiG hat sich das Bundesamt für Sicherheit in der Informationstechnik (BSI) neu aufgestellt. Der zweite Korb der Verordnung zur Bestimmung Kritischer Infrastrukturen (BSI-KritisV) ist in Arbeit und wird die Sektorenabdeckung des IT-SiG komplettieren. Das BSI arbeitet vor allem im Rahmen des UP KRITIS eng mit den Betreibern zusammen, um eine effiziente und sinnvolle Umsetzung des Meldewesens und des Stands der Technik zu ermöglichen. Für die Bewältigung der kommenden Aufgaben wie der Novellierung des IT-SiG zur Umsetzung der NIS-Richtlinie (Netz- und Informationssicherheit) sieht sich das BSI gut aufgestellt. Benjamin Honisch, Referent für Kritische Infrastrukturen im BSI, berichtet über Erfahrungen und Ausblicke hinsichtlich des IT-SiG.

Umsetzung des IT-SiG für kritische Infrastrukturbetreiber

Konkrete Hinweise für die Umsetzung des IT-SiG in der IT-Branche liefern Christian Semmler (Head of Information Security Management) und Sunita Ute Saxena (Senior Managerin) von Telekom Security. Sie geben Einblick in den geplanten Branchenstandard für Datacenter & Hostingbetreiber und erläutern die aktuellen Entwicklungen des IT-SiG durch das geplante Änderungsgesetz. Weiterhin werden die Auswirkungen der ISO Standards 27001 und ISO 22301 auf die Nachweisfähigkeit eines Information Security Managements und Business Continuity Managements diskutiert. Die Referenten stellen die Herausforderungen im Spannungsfeld des IT-Outsourcings dar und zeigen Handlungsempfehlungen auf.

Ein weiterer Vortrag beschäftigt sich mit den Auswirkungen des IT-SiG speziell auf Krankenhäuser. Viele Krankenhäuser erlebten zuletzt zahlreiche Virenangriffe, teilweise mit fatalen Folgen. Spätestens seitdem genießt das Thema IT-Sicherheit in allen Kliniken besonders hohe Aufmerksamkeit. Zudem definiert das IT-SiG für den Bereich Gesundheit spezielle Sicherheitsanforderungen und führt den Begriff eines einzuhaltenden branchenspezifi chen Sicherheitsstandards ein. Doch wer defi iert diese? Welche Sicherheitsanforderungen müssen Krankenhäuser zukünftig erfüllen? Welche inhaltlichen Vorgaben lassen sich bereits erkennen? Der Vortrag von Thorsten Schütz, Leiter IT und Betriebsorganisation im Klinikum Itzehoe, liefert Antworten.

Cyber-Attacken auf kritische Infrastrukturen – Einzelfälle oder systematische Angriffsziele?

Die zunehmend professionelle und profitorientierte Internetkriminalität basiert auf einer ausgeprägten internationalen Underground-Economy. Dort können nach einem Baukastensystem verschiedene Werkzeuge wie Trojaner, Schadsoftware, IT-Infrastruktur und IT-Know-how sowie spezifische Service-Level für kriminelle Geschäftsideen erworben werden. Für einen effektiven Schutz ist es notwendig, die Methoden der Angreifer und potenzielle Einfallstore zu kennen. Kriminalhauptkommissar Peter Vahrenhorst vom Landeskriminalamt Nordrhein-Westfalen besitzt langjährige Erfahrung als IT-Ermittler. In seinem Vortrag spricht er über verschiedene Ausprägungen von Cybercrime, Präventionsmaßnahmen sowie mögliche Vorgehensweisen im Ernstfall.

Cyber Security Management und Advanced Persistent Threats (APT)

Zu den wichtigsten Präventionsmaßnahmen zählt ein ganzheitliches Konzept für Cyber Security Management. innogy SE als einer der führenden Energieversorger und Verteilnetzbetreiber Europas hat sich auf diese Herausforderung frühzeitig eingestellt. Florian Haacke, Leiter Konzernsicherheit, berichtet zur protekt, wie es gelingt, Digitalisierung mit Sicherheit zu gestalten und Sicherheit als Business Enabler im Unternehmen zu etablieren.

Im Rahmen der aktuellen Diskussionen über gezielte Angriffe bzw. APTs wird deutlich, dass die bisher etablierten Erkennungsmethoden einen professionellen Angreifer, der individuelle Malware verwendet, weder aufhalten noch erkennen können. Auch mit zusätzlicher Unterstützung durch Event-Korrelation oder SIEM-Lösungen kommt man hier kaum weiter. Neue technische Ansätze wie Sandbox-Analyse, C&C-Traffic-Er ennung oder spezialisierte Erkennung von Manipulationen auf Endgeräten sollen heute diese Lücke schließen. Der Vortrag von cirosec-Geschäftsführer Stefan Strobel ordnet die zahlreichen Erkennungstechniken inklusive ergänzender Themen wie SIEM und Threat Intelligence in einen Gesamtkontext ein, bewertet sie und zeigt Perspektiven auf.

Referenzarchitekturmodelle (RAMx): Veranschaulichung von IT-Security-Anforderungen im IoT

Bei den derzeitig stattfindenden Zusammenkünften des maschinenbauorientierten Ingenieurwesens und Informatikern erhofft man die Vorteile beider Welten zu finden denn mit Cloud-Architekturen, COTS und Vollvernetzung sind gänzlich neue Businessmodelle und Services realisierbar. Dabei prallen allerdings Welten aufeinander, die unterschiedlicher nicht sein könnten. Dynamisch agierende Digital Natives treffen auf eine mehr als 100-Jahre alte Ingenieurszunft und der von Hackern besiedelte Cyberspace wird mit Maschinen und Geräten verbunden. Referenzarchitekturmodelle wie RAMI (Industrie 4.0), SGAM (Smart Grid) oder RAMA (Automotive) zeigen Strukturen auf, die das gegenseitige Verständnis von Virtualität mit Maschinenrealität fördern und lassen auch eine bessere Verortung von Security-Anforderungen zu. Markus Bartsch von der TÜV Informationstechnik GmbH stellt die Modelle und deren Potenziale vor.

Intensives Networking in der begleitenden Fachausstellung

In der begleitenden Fachausstellung der protekt präsentieren renommierte Hersteller und Anbieter von Sicherheitslösungen praxiserprobte Produkte, Systeme und Dienstleistungen, die den Anforderungen von KRITIS-Betreibern entsprechen. Dort haben Konferenzteilnehmer die Möglichkeit, sich umfassend über Innovationen rund um den Schutz kritischer Infrastrukturen zu informieren. Als Sponsoren unterstützen die protekt bereits die FAAC GmbH Deutschland, die sich auf Gebäude- und Peripheriesicherheit spezialisiert hat, und die Firma Genetec, einer der führenden Anbieter im Bereich IP-basierter Sicherheitssysteme.

LEIPZIGER MESSE

protekt

21. – 22. juni 2017
leipzig

konferenz und
fachausstellung für
den schutz kritischer
infrastrukturen

ihr schlüssel zur sicherheit

Die **protekt** ist das einzigartige Forum für den Schutz kritischer Infrastrukturen. Dabei werden physischer Schutz und IT-Sicherheit optimal verzahnt.

→ Das hochkarätige Konferenzprogramm mit Vorträgen und Workshops thematisiert die Einhaltung aktueller gesetzlicher Regularien und den effizienten Schutz vor Angriffen und Gefährdungen.
Das komplette Konferenzprogramm finden Sie u ter: www.protekt.de/programm

→ Hersteller und Anbieter von Sicherheitslösungen präsentieren in der begleitenden Fachausstellung Produkte, Systeme und Dienstleistungen der physischen und IT-Sicherheit.

→ Die protekt ist die Plattform für Wissenstransfer und Vernetzung zwischen Betreibern kritischer Infrastrukturen, regulierenden Organisationen und Sicherheitsindustrie über aktuelle Sicherheitstrends.

Vom 21. bis 22. Juni 2017,
in der KONGRESSHALLE am Zoo Leipzig.

Buchen Sie als Leser der IT-Sicherheit Ihren 2-Tages-Konferenzpass vergünstigt!
www.protekt.de/ticket
Promotioncode: protekt_2017_IT Sicherheit_16

www.protekt.de