Informationssicherheit bei Kritischen Infrastrukturen (KRITIS)

Energieversorger & Co. schützen

Kritische Infrastrukturen geraten zunehmend ins Visier von Angreifern. Wegen ihrer Bedeutung gelten für sie strenge Sicherheitsregeln.

→ **VON JÜRGEN MAUERER**

Anschlag auf die Nord-Stream-Pipeline, Sabotage am Kabelnetzwerk der Deutschen Bahn oder Ransomware-Angriffe auf Krankenhäuser, die zum Ausfall der Notfallversorgung führen – die Attacken auf Kritische Infrastrukturen (KRITIS) nehmen zu. Erfolgreiche (Cyber-)Angriffe auf KRITIS-Betreiber können für die Bevölkerung gravierende Folgen haben. Sie reichen von großflächigen Stromausfällen über Störungen der Wasserversorgung bis zum längerfristigen Ausfall des Internets.

Mit Beginn des russischen Angriffskriegs gegen die Ukraine rückte der Schutz Kritischer Infrastrukturen verstärkt in den Fokus der öffentlichen Aufmerksamkeit. Doch bislang war glücklicherweise „eine übergreifende Angriffskampagne gegen deutsche Ziele [...] nicht ersichtlich", heißt es im Bericht „Die Lage der IT-Sicherheit in Deutschland 2022" des Bundesamts für Sicherheit in der Informationstechnik (BSI). Demnach gab es im Zusammenhang mit dem Krieg „nur" kleinere Vorfälle wie den Ausfall der Fernwartung in deutschen Windkraftanlagen nach dem Angriff auf ein Unternehmen der Satellitenkommunikation. Insgesamt verzeichnete das BSI im vergangenen Jahr 452 Meldungen über Angriffe aus dem KRITIS-Bereich, 2019 waren es 252 – Tendenz also steigend. Laut BSI ist die Cyberbedrohung derzeit so hoch wie nie. Angesichts ihrer Bedeutung für die Allgemeinheit verpflichtet der Gesetzgeber Kritische Infrastrukturen zu besonderen Schutzmaßnahmen. Doch wer gehört dazu?

Das BSI definiert Kritische Infrastrukturen als „Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden." Aktuell gibt es zehn KRITIS-Sektoren, darunter Energie, Gesundheit und Wasser (siehe Grafik auf Seite 69), die sich teils noch einmal in verschiedene Branchen untergliedern.

Bild: Shutterstock / LeoWolfert

PROBLEMATISCHE SCHWELLENWERTE

Zentrale Rechtsgrundlage ist das BSI-Gesetz (BSIG), das Gesetz über das Bundesamt für Sicherheit in der Informationstechnik. Die Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSIG (BSI-Kritisverordnung, BSI-KritisV) beschreibt die einzelnen Sektoren näher. Die Schwellenwerte sind darin meist so zugeschnitten, dass eine Untergrenze von 500.000 Einwohnern versorgt wird. Nur Einrichtungen oder Anlagen sind KRITIS, die diese Werte überschreiten (erhebliche Größenordnung). Die Schwellenwerte werden regelmäßig überprüft und angepasst. Zuletzt wurde der Schwellenwert für Stromerzeugung mit installierter Netto-Nennleistung (elektrisch) von 420 Megawatt (MW) auf 104 MW gesenkt. Ein Kraftwerk unter dieser Leistung ist nicht KRITIS.

„Der gesenkte Schwellenwert ist ein guter Schritt, da auch kleinere Kraftwerke für die Stromversorgung der Bevölkerung relevant sind. Wir sind hier grundsätzlich auf einem richtigen Weg, doch die Schwellenwerte reichen bei Weitem nicht aus", sagt Kent Andersson, Geschäftsführer bei Ausecus, einem IT-Sicherheitsdienstleister für Kritische Infrastrukturen und Industrie mit Sitz in Augsburg. Besonders kritisch sieht er die Schwellenwerte für Wasser und Abwasser, die erst ab 500.000 Einwohnern gelten. Denn damit gilt nur etwa 1 Prozent der rund 5500 Wasserwerke als KRITIS-Betreiber mit entsprechend hohen Sicherheitsanforderungen.

NIS 2: ÜBERGEORDNETES EU-RECHT

Für die Zukunft setzt Andersson vor allem auf übergeordnete Rechtsgrundlagen wie die ab 2023 gültige NIS-2-Richtlinie der EU, die binnen 21 Monaten in nationales Recht umgesetzt werden muss. Das wird wohl zu einer neuen BSI-KritisV führen, um die schärferen Schwellenwerte einzuführen. Ziel ist ein gleichmäßig hohes →

DER AUTOR

Jürgen Mauerer
arbeitet als freiberuflicher Fachjournalist in München. Neben seiner redaktionellen Tätigkeit rund um Business-IT und IT-Security entwickelt er Kommunikationsstrategien und konzipiert und moderiert IT-Fachkonferenzen und Kundenveranstaltungen.

452

Meldungen über Angriffe im KRITIS-Bereich verzeichnete das BSI im vergangenen Jahr – Tendenz steigend

Quelle: BSI

Bild: PwC

„Bei KRITIS stehen die Verfügbarkeit und das Business Continuity Management im Mittelpunkt, um die Versorgungssicherheit der Bevölkerung zu gewährleisten."

André Glenzer
Leiter des KRITIS Center of Excellence bei PwC Deutschland

Sicherheitsniveau in Kritischen Infrastrukturen in der gesamten EU. NIS 2 definiert 18 KRITIS-Sektoren in zwei Kategorien (wesentliche und wichtige Einrichtungen) und verzichtet auf Schwellenwerte. Die strengeren Vorgaben treffen dann auch mittlere Firmen ab 50 Mitarbeitern oder einem Jahresumsatz von 10 Millionen Euro. „Einige Betreiber sollen unabhängig von der Größe reguliert werden, etwa Teile der digitalen Infrastruktur und öffentliche Verwaltung. Werden all diese Vorgaben umgesetzt, erhöht sich die Zahl der KRITIS-Betreiber in Deutschland von rund 2000 Unternehmen auf mehr als 10.000", so Kent Anderson. Neben NIS 2 hat die EU auch die „Richtlinie über die Resilienz kritischer Einrichtungen" (CER-Richtlinie) mit Fokus auf physischer Sicherheit verabschiedet. Sie soll die Widerstandsfähigkeit gegen Bedrohungen wie Naturgefahren, Terroranschläge oder Pandemien stärken.

Auch Holger Berens, Vorstandvorsitzender des Bundesverbands für den Schutz Kritischer Infrastrukturen e. V. (BSKI), begrüßt die neue europaweite Gesetzgebung: „Regulatorisch sind wir jetzt auf einem sehr guten Weg. Wenn etwa NIS 2 hierzulande gilt, fallen auch Verwaltungen von Kommunen oder kleinere KRITIS-Betreiber, die derzeit noch unter den Schwellenwerten liegen, unter das KRITIS-Gesetz. Diese Firmen sind sicherheitstechnisch noch nicht gut aufgestellt. Hier gibt es ein großes Delta zu den Anforderungen – und einen Mangel an Budget und Fachpersonal. Das Problem wird also die Umsetzung sein."

Relevante Gesetze für KRITIS-Betreiber

Für KRITIS-Betreiber gelten angesichts ihrer großen Bedeutung für das Allgemeinwohl spezielle Sicherheitsanforderungen. Hier eine Übersicht der wichtigsten Gesetze:

- Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz – BSIG): Nach § 8a haben KRITIS-Betreiber besondere Pflichten für ihre IT-Sicherheit
- Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSIG (BSI-Kritisverordnung, BSI-KritisV): Nähere Beschreibung der einzelnen Sektoren und Schwellenwerte zur KRITIS-Bestimmung
- Die NIS-Richtlinie (Network Information Security). Erste EU-weite Rechtsvorschrift über Cybersicherheit. Ziel ist ein gleichmäßig hohes Sicherheitsniveau von Netz- und Informationssystemen in der gesamten Europäischen Union. Die künftige Version NIS 2 definiert insgesamt 18 KRITIS-Sektoren in zwei Kategorien (wesentliche und wichtige Einrichtungen) und verzichtet auf Anlagen-Schwellenwerte. Die Regulierung mit strengeren Vorgaben an Cybersecurity trifft dann auch mittlere Firmen ab 50 Mitarbeitern oder einem Jahresumsatz von 10 Millionen Euro
- IT-Sicherheitsgesetz (erfüllt viele Vorgaben der NIS-Richtlinie): Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme
- Richtlinie über die Resilienz kritischer Einrichtungen (CER-Richtlinie) mit Fokus auf physischer Sicherheit. Diese neue Vorschrift soll die Widerstandsfähigkeit Kritischer Infrastrukturen gegen Bedrohungen wie Naturgefahren, Terroranschläge oder einer Pandemie stärken

HOHE ANFORDERUNGEN

Die Anforderungen an KRITIS-Betreiber sind alles andere als trivial. „Normale" Unternehmen denken bei der Planung der Sicherheitssysteme primär betriebswirtschaftlich und evaluieren die Eintrittswahrscheinlichkeit eines Bedrohungsszenarios und dessen Auswirkungen für das Unternehmen selbst. „KRITIS-Betreiber hingegen müssen bei der Risikoanalyse die Auswirkungen auf die Versorgung der Bevölkerung einbeziehen. Daraus ergeben sich deutlich höhere Sicherheitsstandards und tiefgreifendere Maßnahmen", betont Holger Berens.

Sie müssen etwa Störungen und Angriffe beim BSI melden, ein Information Security Management System (ISMS) aufbauen und Business Continuity Management umsetzen. Ein ISMS verfolgt einen ganzheitlichen Ansatz zur Informationssicherheit: Neben technischen Aspekten werden auch infrastrukturelle, organisatorische und personelle Themen betrachtet. So werden notwendige Sicherheitsmaßnahmen systematisch identifiziert, die dem Stand der Technik in der jeweiligen Branche entsprechen.

Ab Mai 2023 sind zudem Systeme der Angriffserkennung wie IDS/IPS (Intrusion-Detection-Systeme/Intrusion-Prevention-Systeme) oder SIEM-Lösungen (Security Information and Event Management) verpflichtend. Die getroffenen Maßnahmen müssen zertifiziert, gegenüber dem BSI nachgewiesen und alle zwei Jahre erneuert werden.

„Prüfungsgrundlagen sind beispielsweise die Norm ISO/IEC 27001 mit IT-Grundschutz oder branchenspezifische Sicherheitsstandards. Bei der Umsetzung sollten die KRITIS-Betreiber genau prüfen, welche Standards für sie sinnvoll sind", erläutert André Glenzer, Partner und Leiter des KRITIS Center of Excellence bei PwC Deutschland. „Grundsätzlich stehen bei KRITIS die Verfügbarkeit und das Business Continuity Management im Mittelpunkt, um

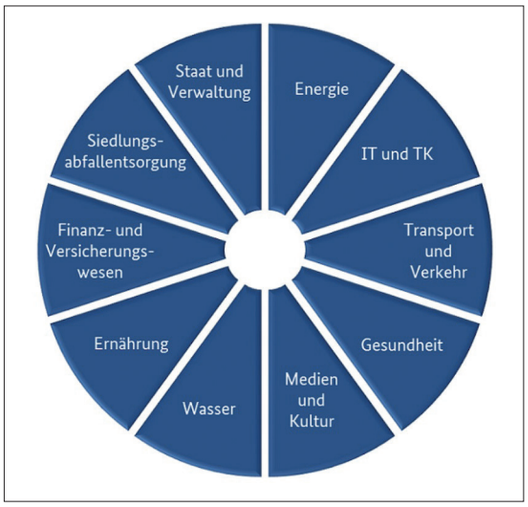

Bild: BSI

Das BSI definiert zehn KRITIS-Sektoren von Energie bis Staat, IT und TK bis Abfallentsorgung.

die Versorgungssicherheit der Bevölkerung zu gewährleisten. Daher müssen Firmen auch Maßnahmen umsetzen, bei denen die Kosten nicht im direkten Verhältnis zum wirtschaftlichen Ertrag stehen, da sie unabdingbar sind, um Menschenleben zu schützen." Als Beispiel nennt er die Notstromaggregate etwa in Krankenhäusern.

SYSTEME ZUR ANGRIFFSERKENNUNG

Hinzu kommen ab Mai 2023 die Anforderungen der Orientierungshilfe zum Einsatz von Systemen zur Angriffserkennung (OHSZA). Dazu André Glenzer: „Firmen müssen ein entsprechendes System installieren und auf einer Reifegradskala von 1 bis 5 mindestens Reifegrad 3 erreichen. Die Einhaltung wird vom BSI geprüft. Die OHSZA fordert auch eine bessere Überwachung von OT-Komponenten etwa in Steuerungsanlagen oder der Leittechnik von Energieversorgern, um den Schutz zu erhöhen. Das haben viele KRITIS-Betreiber bisher nicht auf dem Schirm."

Das Problem: Durch die zunehmende Vernetzung und Digitalisierung der Leit- und Steuerungstechnik (Operational Technology, OT) steigen auch die Sicherheitsherausforderungen. Eine wachsende Anzahl von Verbindungen auf verschiedenen Ebenen stellt für Hacker attraktive Angriffspunkte in die früher so stark abgeschotteten KRITIS-Infrastrukturen dar. „Systeme zur Angriffserkennung lesen Kommunikations- und Systemdaten mit und durchsuchen sie nach Spuren von Cyberangriffen. Wird ein Angriff bemerkt, initiieren sie Gegenmaßnahmen, um den Angriff möglichst schnell und wirkungsvoll zu vereiteln oder zu verhindern, dass er sich weiterverbreitet", erklärt Sascha Jäger, Geschäftsführer von Ausecus.

Ausecus zum Beispiel bietet mit KRITIS Defender eine Angriffserkennung as a Service speziell für kleinere und mittlere Versorgungsunternehmen an. Dazu Sascha Jäger: „Kleine und mittlere Versorger verfügen meistens nicht über ausreichend Fachpersonal, um derartige Systeme zu implementieren und zu betreiben. Sie sind oft schon mit ihrem täglichen Betrieb und den Anforderungen der Digitalisierung stark ausgelastet."

UNTERSCHIEDLICHES SCHUTZNIVEAU

Zu diesen kleineren Versorgern gehören auch die Stadtwerke kleinerer Kommunen. Sie erfüllen mangels Ressourcen die hohen KRITIS-Sicherheitsanforderungen oft nur unzureichend. BSKI-Vorstand Holger Berens rät diesen Kommunen daher, sich – abhängig von der Größe – →

Wozu sind KRITIS-Betreiber verpflichtet?

Nach § 8a des BSI-Gesetzes haben KRITIS-Betreiber besondere Pflichten für ihre IT-Sicherheit. Das BSI-Gesetz wird regelmäßig durch Elemente aus Gesetzen wie Energiewirtschaftsgesetz, Atomgesetz, Telemediengesetz, Telekommunikationsgesetz und IT-Sicherheitsgesetz (Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme) erweitert. Wozu aber sind KRITIS-Betreiber verpflichtet?

Hier eine kurze Übersicht:

- Registrierung beim BSI
- Nennen einer Kontaktstelle, über die sie jederzeit erreichbar sind. An diese Adresse schickt das BSI IT-Sicherheitsinformationen
- Meldung von IT-Störungen oder erheblichen Beeinträchtigungen an das BSI plus Pflicht zur Herausgabe aller zur Bewältigung der Störung notwendigen Informationen
- Erweitertes Risikomanagement und Business Continuity Management (BCM)
- Umsetzen von IT-Sicherheit auf dem „Stand der Technik". Angemessene organisatorische und technische Vorkehrungen zum Schutz ihrer IT-Systeme, Komponenten und Prozesse
- Nachweis zur Umsetzung der Sicherheitsmaßnahmen alle zwei Jahre gegenüber dem BSI durch ein Zertifikat etwa zum Aufbau eines Informationssicherheits-Managementsystems (ISMS) gemäß der Norm ISO 27001 mit BSI-Grundschutz oder branchenspezifischer Sicherheitsstandards (B3S). Bei Nichterfüllung drohen den KRITIS-Betreibern Geldbußen von bis zu 20 Millionen Euro beziehungsweise 4 Prozent des weltweiten Unternehmensumsatzes
- Ab Mai 2023: KRITIS-Betreiber müssen Systeme der Angriffserkennung wie IDS/IPS (Intrusion-Detection-Systeme/Intrusion-Prevention-Systeme) oder Threat Intelligence installieren
- „KRITIS-Kernkomponenten" dürfen nur von vertrauenswürdigen Herstellern stammen

mit anderen kleineren Städten, Gemeinden oder Landkreisen zusammenzuschließen und KRITIS-Cluster zu bilden: „So können sie ihre Ressourcen bündeln, ein einheitliches Sicherheitskonzept für das gesamte Gebiet erstellen und ein gemeinsames IT-Sicherheitszentrum oder zusätzliche Redundanzen aufbauen."

Insgesamt unterscheidet sich das Schutzniveau zwischen den KRITIS-Sektoren und auch innerhalb der Sektoren mitunter stark. Darüber sind sich alle von uns befragten Experten einig. Während die kleineren Versorger eher schlechter aufgestellt sind, gelten große Energieunternehmen mit umfangreichen Ressourcen als Vorreiter. „Da sie Blackout-Szenarien seit 15 Jahren diskutieren und üben, sind Notfall- und Krisenpläne vorhanden. Energie ist sowieso der wichtigste Sektor. Wenn Strom mittel- oder langfristig ausfällt, betrifft das alle anderen Sektoren", so Holger Berens. Auch die Banken sind ihm zufolge sehr gut aufgestellt, da sie durch die Bafin auch in puncto

„Das ist kein strukturierter Katastrophenschutz"

Manuel Atug ist Gründer und Sprecher der unabhängigen AG KRITIS. Im Interview mit com! professional erklärt er, warum der Gesetzgeber beim Schutz Kritischer Infrastrukturen noch nachlegen sollte und wie sich KRITIS-Betreiber angemessen vor Bedrohungen schützen können.

com! professional: Herr Atug, die BSI-Kritisverordnung (BSI-KritisV) beschreibt die einzelnen KRITIS-Sektoren näher und nennt Schwellenwerte, anhand derer bestimmt wird, ob es sich um eine Kritische Infrastruktur handelt. Wie beurteilen Sie diese Schwellenwerte?
Manuel Atug: Die Schwellenwerte sehen dekorativ aus, sind aber nicht zielführend und sollten unserer Meinung nach angepasst werden. Das kann man gut am Beispiel der Wasserwerke aufzeigen. Es sind nur diejenigen als Kritische Infrastruktur definiert, die mehr als 500.000 Menschen versorgen. Von den etwa 5500 Wasserwerken in Deutschland gilt daher nur rund 1 Prozent als KRITIS und muss entsprechend eine hohe IT-Sicherheit gewährleisten. In Städten wie Augsburg oder Bonn würde bei einem Cyberangriff möglicherweise die Wasserversorgung zusammenbrechen, aber diese mussten laut Gesetz keine Cybersicherheitsmaßnahmen umsetzen. Das ist sehr seltsam und kein strukturierter Katastrophenschutz.

com! professional: Das klingt nicht gut. Werden die Schwellenwerte der KritisV regelmäßig überprüft?
Atug: Die KritisV soll grundsätzlich alle zwei Jahre evaluiert werden, auch unter wissenschaftlichen Gesichtspunkten. Das erfolgt allerdings nicht öffentlich. Und es fehlt die Transparenz, da sich nicht nachvollziehen lässt, warum und wie die Schwellenwerte zustande kommen. Auch die Kumulation wurde nicht berücksichtigt, sprich wenn etwa ein Stadtwerk als Wasserwerks- und Kraftwerksbetreiber gleichzeitig auch Internet-Services anbietet. Diesen Punkt haben verschiedene Experten und auch wir bei der Anhörung des Gesetzgebers eingebracht, wurden aber ignoriert. Dabei geht es hier um den Schutz der Öffentlichkeit.

com! professional: Welche Bedeutung haben in diesem Zusammenhang die im IT-Sicherheitsgesetz vorgesehenen „Unternehmen im besonderen öffentlichen Interesse", auch UBI genannt?
Atug: Wir bezeichnen die UBI intern als „KRITIS light". Dazu gehören beispielsweise die Rüstungsindustrie und die in der Störfallverordnung beschriebenen chemischen Anlagen. Die UBI benötigen nur ein IT-Sicherheitskonzept, das jedoch nicht kontrolliert wird. Das ist eine halbherzige Geschichte beziehungsweise ein sehr schlechter Kompromiss – und es zeigt, dass offenbar Lobbyarbeit im Hintergrund erfolgreich funktioniert hat. Auch das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe sieht Chemie ganz klar als Kritische Infrastruktur, doch der Gesetzgeber hat das weichgespült und zu wenig reguliert. Auch dem für Anfang 2023 geplanten KRITIS-Dachgesetz für physische Sicherheit sehen wir nicht positiv entgegen. Es wird sehr schnell ohne Transparenz und Diskussionen oder Beteiligung der Öffentlichkeit durchgepeitscht. Das kann nicht gut sein und zeigt wenig Interesse an einem echten Schutz.

com! professional: Welche Gefahren drohen speziell für KRITIS-Unternehmen?
Atug: Wie „normale" Unternehmen sind auch Kritische Infrastrukturen von Cyberangriffen bedroht, vor allem von Ransomware-Attacken. Zu den Angreifern gehören auch Nachrichten- und Geheimdienste mit dem Ziel, Kritische Infrastrukturen auszukundschaften, sie lahmzulegen und dadurch die Bevölkerung von innen zu destabilisieren. Hinzu kommen mögliche physische Angriffe wie Sabotage an einer Pipeline oder am Stromnetz. Je nachdem, wie der entsprechende KRITIS-Betreiber aufgestellt ist, wird daraus eine Krise oder Katastrophe. Wir müssen geeignete Maßnahmen gegen Ereignisse und Vorfälle anwenden, damit sie nur eine Störung bewirken, aber die Versorgung der Bevölkerung nicht gefährden. Auch beim Hochwasser im Ahrtal wurde Kritische Infrastruktur zerstört. Ich gehe davon aus, dass klimabedingte Katastrophen sowie Ransomware-Angriffe in den nächsten Jahren deutlich zunehmen.

com! professional: Sind die KRITIS-Betreiber Ihrer Meinung nach gut gegen diese Gefahren gerüstet? Unterscheidet sich das Schutzniveau zwischen den KRITIS-Sektoren?
Atug: Das Bild hier ist bunt und vielfältig. Die Bandbreite reicht in allen KRITIS-Sektoren von KRITIS-Betreibern, die nur ein Mindestmaß an IT-Sicherheit umsetzen, bis hin zu KRITIS-Betreibern, die sich sehr gut aufgestellt haben und sich auch gut gegen Ausfälle schützen.

Am höchsten ist das Security-Niveau tendenziell wohl eher bei Banken und Versicherungen wegen der vielen Regulierung seit Jahren und eher niedriger im KRITIS-Sektor Staat und Verwaltung aufgrund der geringeren Bezahlung nach Tarif und der fehlenden Regulierung und Haftung.

Informationssicherheit stark reguliert werden. „Leider fehlt es zwischen den Sektoren wegen unterschiedlicher Aufsichtsbehörden (BSI, Bafin, Bundesnetzagentur) an Koordination, es gibt keine einheitlichen Standards. Die branchenspezifischen Sicherheitsstandards (B3S) unterscheiden sich durchaus in ihrer Qualität“, konstatiert Berens. Ein Beispiel: Die Branchen Strom und Gas orientieren sich an der internationalen Norm ISO/IEC 27001, die Wasserversorger am nationalen BSI-Grundschutz.

VIELE ANGRIFFSPUNKTE

Eine Zertifizierung gemäß den genannten Standards heißt indes nicht, dass schon alles gut ist. Wie andere Unternehmen auch, müssen KRITIS-Betreiber ihre Sicherheitsmaßnahmen kontinuierlich prüfen und verbessern. Denn Hacker entwickeln ihre Methoden ständig weiter, um neue Angriffswege zu finden und Firmen zu infiltrieren. „Wenn ein Krimineller die Angriffsfläche eines Unternehmens bewertet, sucht er nach der passenden Kombination aus ➔

Bild: Manuel Atug

Manuel Atug
Gründer und Sprecher der AG KRITIS

com! professional: Wie ist das eher niedrige Sicherheitsniveau bei Kommunen und Landkreisen zu erklären? Tatsächlich gibt es ja immer wieder Schlagzeilen über Ransomware-Angriffe, die ganze Verwaltungen lahmlegen, etwa im Landkreis Anhalt-Bitterfeld.

Atug: Ja, leider. Das hat mehrere Ursachen. Viele Kommunen und Landkreise nutzen veraltete Lösungen; teils laufen da noch Windows-95-Systeme. Die Digitalisierung wurde bislang nur unzureichend umgesetzt und es fehlt an Fachpersonal mit der notwendigen Digitalkompetenz. Hinzu kommt, dass es für die KRITIS-Sektoren Staat und Verwaltung sowie Medien und Kultur quasi keine gesetzlichen Anforderungen zur IT-Sicherheit gibt. Denn beide Sektoren unterliegen nicht dem IT-Sicherheitsgesetz, das von KRITIS-Betreibern fordert, ein Information Security Management System (ISMS) mit Business Continuity Management (BCM) umzusetzen. Warum ist das so? Medien und Kultur sind schlicht und einfach Ländersache – und die Vorgaben des BSI gelten nicht für Verwaltungen auf Landes- oder Kommunalebene, da das BSI dem Bundesinnenministerium unterstellt und nicht unabhängig ist.

com! professional: Hier wäre Ihrer Meinung nach also der Gesetzgeber gefordert, oder?

Atug: Ja. Grundsätzlich geht die Gesetzgebung in die richtige Richtung, der Einfluss der Lobbyisten und der Wirtschaft ist aber noch zu groß. Der Gesetzgeber sollte Anreize für KRITIS-Betreiber schaffen, sichere Systeme zu betreiben. Stichworte wären hier Security by Design oder Privacy by Design. Es geht um Daten und Datenschutz, weil wir damit den Schutz von Menschen sicherstellen.

Natürlich müssen die umgesetzten Maßnahmen auch überprüft werden. Das Beispiel DSGVO zeigt, dass das Recht nur selten durchgesetzt wird. Es werden nur wenige Firmen, die gegen den Datenschutz verstoßen, ermittelt und bestraft. Insgesamt passiert mir auf gesetzlicher Ebene zu wenig; das ist nicht angemessen im Vergleich zum Risiko und der aktuellen Bedrohungslage. Und schauen Sie auf die Verteilung der Fördergelder: Diese gibt es oft für Hype-Themen wie Blockchain oder KI, nicht aber für Maßnahmen rund um IT-Sicherheit und Menschenschutz. Man könnte aber beispielsweise auch festlegen, dass Unternehmen den Aufwand für den Aufbau und Betrieb eines ISMS mit BCM steuerlich absetzen können.

com! professional: Immerhin bei den Systemen zur Angriffserkennung hat der Gesetzgeber reagiert. Diese sind ab dem 1. Mai 2023 für KRITIS-Betreiber verpflichtend.

Atug: Ja, leider. Denn dieses Gesetz geht an der Praxis vorbei und ist wenig zielführend. Die Lobby verdient sich hier eine goldene Nase. Natürlich sind Angriffserkennungssysteme sinnvoll. Sie bilden aber nicht den ersten Schritt, sondern kommen erst viel weiter hinten in der Sicherheitskette an Stelle x, nicht aber an erster Stelle. Bevor ich als KRITIS-Betreiber ein System zur Angriffserkennung einsetze, sollte ich zunächst die Minimalmaßnahmen eines ISMS mit BCM umsetzen und kontinuierlich verbessern. Das BSI-Gesetz zwingt die KRITIS-Betreiber jetzt zu relativ hohen Investitionen und Aufwand in die Implementierung eines Systems zur Angriffserkennung; es besteht daher die Gefahr, dass andere, wichtigere Security-Maßnahmen auf der Strecke bleiben.

com! professional: Mit welchen Maßnahmen können KRITIS-Betreiber ihre IT-Sicherheit erhöhen?

Atug: Die Lösung ist ein Mix aus verschiedenen Maßnahmen im Rahmen einer ganzheitlichen Cybersicherheitsstrategie, um die Bedrohungen einzudämmen und resilient zu werden. Am Anfang steht die Strategie, erst danach folgen die technischen Maßnahmen. Zentral sind fast langweilige Grundlagen wie Backup und Wiederherstellung von Daten, Backup-Tests oder die Frage, ob Backups auch offline vorliegen. Denn Online-Backups werden meist auch Opfer von Ransomware.

Des Weiteren geht es um die regelmäßige Prüfung von Firewall-Regeln, das schnelle Schließen von Sicherheitslücken durch das Aufspielen von Patches oder die sichere Fernwartung etwa mit Zwei-Faktor-Authentifizierung. Erst danach sollten KRITIS-Betreiber über Systeme zur Angriffserkennung nachdenken müssen.

„Wir sind gesetzlich auf einem richtigen Weg, doch die Schwellenwerte für KRITIS reichen bei Weitem nicht aus."

Kent Andersson
Geschäftsführer Ausecus

Bild: Ausecus

Schwachstellen, Fehlkonfigurationen und Identitätsprivilegien, die ihm am schnellsten den größtmöglichen Zugriff ermöglicht", erläutert Roger Scheer, Regional Vice President Central Europe beim Security-Anbieter Tenable.

Die Einfallstore und Angriffsmethoden sind vielfältig. Das zeigt der aktuelle „Unit 42 Incident Response Report". Phishing-Versuche über Mitarbeiter-E-Mails und soziale Netzwerke (37 Prozent) stehen an erster Stelle vor Software-Schwachstellen (31 Prozent). Es folgen mit großem Abstand Brute-Force-Angriffe auf Zugangsdaten (9 Prozent), bei denen die Hacker versuchen, ein Passwort oder einen Benutzernamen per Trial-and-Error-Methode zu knacken. Weitere Angriffspunkte sind kompromittierte Zugangsdaten, Insiderbedrohungen, Social Engineering oder der Missbrauch vertraulicher Beziehungen/Tools.

Tenable stellte laut Roger Scheer viele Angriffe fest, die auf die IT-Seite des Unternehmens abzielten, durch die enge Vernetzung von OT und IT aber zugleich auf OT-Systeme einwirkten. Besonders effektiv waren demnach Ransomware-Angriffe, in deren Folge zahlreiche Firmen den Betrieb einstellen mussten. „KRITIS-Betreiber sollten zum Schutz ihrer Systeme ihre Ressourcen effizient einsetzen, priorisieren und sich zunächst auf die wichtigsten Assets konzentrieren. Damit meine ich die kritischen Systeme und Dienste, die zum Funktionieren benötigt werden, sensible Daten sowie die Angriffspfade, mit denen Angreifer anfänglichen Zugriff erhalten und sich dann weiter im Netzwerk zum Erlangen von Privilegien bewegen", empfiehlt Roger Scheer.

Bild: Ausecus

Die künftige EU-Norm NIS 2 (Network Information Security) definiert insgesamt 18 KRITIS-Sektoren in zwei Kategorien (wesentliche und wichtige Einrichtungen) und verzichtet auf Anlagen-Schwellenwerte.

BÜNDEL AN SCHUTZMASSNAHMEN

In Bezug auf die Maßnahmen gibt es im Prinzip keinen Unterschied zwischen Kritischen Infrastrukturen und anderen Unternehmen. Die Wirksamkeitsprüfungen sind allerdings strenger. Grundsätzlich entsteht höhere Sicherheit vor Cyberangriffen durch einen Mix aus Maßnahmen im Rahmen einer umfassenden Sicherheitsstrategie. Es geht immer um ein Zusammenspiel von Prozessen, Technologien und Menschen. Sehr wichtig sind Awareness-Schulungen für die Mitarbeiter, um ein Bewusstsein für die zahlreichen Risiken im IT-Security-Umfeld zu schaffen. Auch Business Continuity Management mit Notfallprozessen nach technischen Störungen und Wiederanlaufplänen muss Teil der Gesamtstrategie sein.

Für Brigadegeneral a.D. Daniel Bren, CEO von Otorio, einem Anbieter von OT-Sicherheitslösungen mit Sitz in Israel und Österreich, sind Risikobewertung und Risikomanagement entscheidend: „Jedes Unternehmen sollte mit einer umfassenden Asset-Transparenz beginnen und alle IT- und OT-Systeme komplett erfassen. Mithilfe von Risikomanagement-Tools ist es dann möglich, automatisierte Sicherheitsrisikobewertungen durchzuführen und detaillierte Berichte mit praktischen Empfehlungen und Schritt-für-Schritt-Playbooks zur Risikominderung zu erstellen."

Für KRITIS-Organisationen ist es laut Daniel Bren zudem von entscheidender Bedeutung, Sicherheitswarnungen zu priorisieren und zu kontextualisieren, damit Teams Risiken und Schwachstellen mit hoher Priorität mindern können, die die größten Auswirkungen auf ihren Betrieb haben. Zudem rät er KRITIS-Betreibern, Penetrationstests zu beauftragen, die einen Cyberangriff mit Techniken und Vorgehen echter Angreifer simulieren.

„Penetrationstests sind wie eine lebensrettende Operation, um Cyberschwachstellen in einer industriellen Umgebung zu finden und aufzudecken. So lassen sich kritische Schwachstellen erkennen, die von einem potenziellen Angreifer hätten ausgenutzt werden können, und durch Maßnahmen rechtzeitig abmildern oder schließen", betont Daniel Bren.

Weitere wichtige Schutzmaßnahmen sind die regelmäßige Prüfung von Firewall-Regeln, das schnelle Schließen von Sicherheitslücken durch das Aufspielen von Patches, Zwei-Faktor-Authentifizierung, Systeme zur Angriffserkennung und vor allem regelmäßige Backups auf getrennten, offline genutzten Speichermedien. Damit stellen KRITIS-Betreiber sicher, dass sie auch im Fall einer tatsächlichen Ransomware-Infektion keine Daten verlieren und ihr System einfach wiederherstellen können. •