IS4IT KRITIS

PRESSECLIPPING

Die Welt, Smart IT & Sicherheit 2023, 30.11.2023

Wenns im Supermarkt-Büro piept

Wenn statt nichtzahlender Kundschaft Hacker den Geschäftsbetrieb lahmlegen: Das IT-Sicherheitsgesetz fordert von den Betreibern Kritischer Infrastrukturen, kurz KRITIS, einen umfassenden Schutz gegen Cyberangriffe.

Das im Frühjahr verabschiedete Upgrade des IT-Sicherheitsgesetzes mahnt den Schutz kritischer Infrastrukturen der täglichen Versorgung an. Dazu zählen Energienetzbetreiber und Wasserversorger, der Lebensmittelhandel, Transport- und Verkehrsmittel, das Gesundheitswesen und IT- und Telekommunikationsunternehmen, aber auch Medien und Kultur und öffentliche Verwaltungsbetriebe. Wörtlich hieß es im letztjährigen Entwurf des Bundesministeriums des Innern und für Heimat dazu: »Von der Alarmierung von Rettungskräften über die Stromversorgung bis zum Zahlungsverkehr – Kritische Infrastrukturen (KRITIS) sind für unsere Gesellschaft unverzichtbar. Jede und jeder Einzelne ist im Alltag auf sie angewiesen.« Die KRITIS-Verfügbarkeit sichere die Handlungsfähigkeit staatlicher Institutionen und sei dabei Voraussetzung für wirtschaftliche und gesellschaftliche Aktivitäten. Da die Bandbreite dieser Institutionen groß sei, sei auch die Gefahrenlage vielfältig. Sie reiche »von Naturkatastrophen über Terrorismus und Sabotage bis hin zu menschlichem Versagen«.


Bild: iStockphoto/Roy Eraink

Dass es bei dem Gesetz-Upgrade auch um eine zu vermeidende Panik oder subjektive Ängste geht, verschweigt der Entwurf, auch wenn er explizit die Covid-19-Pandemie und die Sabotageakte bei der Bahn und den Nord-Stream-Pipelines als Gefahrenbeispiele nennt. Es geht bei dem Gesetz eben vor allem darum, Unternehmen im Tagesgeschäft zu mehr Wachsamkeit zu zwingen – und die Angst vor übermächtigen Hackern, die von heute auf morgen gezielt ganze Infrastrukturen lahmlegen oder manipulieren können, klar zu minimieren. Allein die Ankündigung soll zeigen, dass man hinter den Kulissen eben nicht in Ruhe abwartet, sondern sich eindeutig gegen Cyberangriffe positionieren will. In der Neuen Zürcher Zeitung schätzte Lennart Maschmeyer von der ETH Zürich die aktuelle Bedrohung durch kriegerisch zu nennende, flächendeckend wirkende Cyberangriffe ein. Sie sei im Gegensatz zu den gezielten Erpressungsangriffen auf einzelne Unternehmen eher gering. Es gebe die voneinander abhängen: Geschwindigkeit,

> **Uneins ist sich die Ampel-Koalition darüber, ob vorhandene Schwachstellen für Ermittlungen, die Kriminalitätsbekämpfung oder staatliche Spionagetätigkeiten bewusst offenbleiben sollen.**

Intensität und Kontrolle. »Versucht man eine der drei Variablen zu erhöhen, nehmen die anderen zwei ab. Zum Beispiel: Je grösser die Zerstörungskraft sein soll, die man mit einem Angriff erreichen will, desto mehr Zeit braucht er und desto eher gerät er außer Kontrolle. Eine militärisch relevante Cyberoperation kostet tendenziell so viel Vorbereitungszeit, dass sie nicht kurzfristig durchgeführt werden kann.«

Die Kunst der Verknüpfung ist die Kunst der Resilienz

Das IT-Sicherheitsgesetz will aber die Abhängigkeit von Daten mit der Abhängigkeit eines funktionierenden Staates und Alltagslebens kreuzen – und so mehr Resilienz erzeugen, die bis zum einzelnen Bürger wirkt. Auch psychologisch. Wörtlich heißt es im IT-Sicherheitsgesetz: »Die eingesetzten Systeme zur Angriffserkennung müssen geeignete Parameter und Merkmale aus dem laufenden Betrieb kontinuierlich und automatisch erfassen und auswerten. Sie sollten dazu in der Lage sein, fortwährend Bedrohungen zu identifizieren und zu vermeiden sowie für eingetretene Störungen geeignete Beseitigungsmaßnahmen vorzusehen.« Hier kommt das Security Incident Event Management, kurz SIEM, ins Spiel, das sämtliche sicherheitsrelevanten Daten der jeweiligen IT-Infrastruktur nicht nur sammelt, sondern sie auch miteinander verknüpft und auf Muster und Auffälligkeiten untersucht.

Sollen Sicherheitslücken offenbleiben?

Uneins ist sich die Ampel-Koalition darüber, ob vorhandene Schwachstellen für Ermittlungen, die Kriminalitätsbekämpfung oder staatliche Spionagetätigkeiten bewusst offenbleiben sollen. Während SPD und Grüne ein solches staatliches Hacken teilweise befürworten, will die FDP ein komplett lückenfreies und geschlossenes System. Manuel Höferlin, innenpolitischer Sprecher der FDP-Fraktion, gegenüber Netzpolitik.org: »Die Pläne von Bundesinnenministerin Faeser für ein einheitliches Schutzniveau kritischer Infrastruktur gehen in die richtige Richtung, sie vergisst aber einen wesentlichen Aspekt des Schutzes digitaler Infrastruktur. Um die Cybersicherheit zu stärken, müssen wir die IT-Sicherheitslücken konsequent schließen, statt diese für Überwachungszwecke offenzulassen und externe Überprüfungen auf Schwachstellen einführen.«

Im nächsten Schritt sollen die Kritischen Infrastrukturen durch ein KRITIS-Dachgesetz, das ab 2025 in Kraft treten soll, auch physisch geschützt werden. Dazu sollen in Unternehmen Pläne für den Objektschutz intensiviert und Meldepflichten für Störfälle umgesetzt werden. Auch Maßnahmen zur Schulung der Mitarbeitenden und zu konkreten Zugangskontrollen und einer Priorisierung von Verantwortlichen sollen getroffen werden. »Bei Wahrung der verfassungsrechtlichen Zuständigkeiten der Aufsichtsbehörden auf Bundes – und Landesebene in den einzelnen Sektoren« werde das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe »eine koordinierende Rolle erhalten, damit erstmalig ein sektorenübergreifender Überblick über das Gesamtsystem der kritischen Anlagen als einen wesentlichen Teilbereich der Kritischen Infrastrukturen geschaffen wird«. Ob es für diesen Überblick einer Datenschutz- oder sonstigen Lücke bedarf, könnte Gegenstand neuer Diskussionen werden. Eines ist jedoch sicher: Alles hängt mit allem zusammen.

Text: **Rüdiger Schmidt-Sodingen**

Alexander Werkmann

»Zeit ist der Schlüssel – und das Zusammenspiel von Menschen, Prozessen und Technologie«

Das Über von Cybersicherheitsanwendungsfällen ist ein proaktiver Ansatz, um die Sicherheit zu stärken und die Reaktionsfähigkeit auf Cyberangriffe zu erhöhen.

– Alexander Werkmann, Director IBM Technology Security DACH

CISO AS A SERVICE
SECURITY OPERATIONS CENTER
SECURITY-INFRASTRUKTUR
DIE CYBERSECURITY-EXPERTEN STELLEN SICH VOR
INCIDENT RESPONSE
INFORMATIONS-SICHERHEIT
GOVERNANCE, RISK MANAGEMENT & COMPLIANCE