IT-Sicherheit

KRITIS-Regeln verschärft

[12.04.2023] Das IT-Sicherheitsgesetz 2.0 hat die Regelungen für Betreiber Kritischer Infrastrukturen verschärft. Zudem fallen nun deutlich mehr Versorgungsunternehmen unter die KRITIS-Verordnung und müssen entsprechende Maßnahmen umsetzen.

Mit dem im Mai 2021 in Kraft getretenen IT-Sicherheitsgesetz 2.0 und der daraufhin aktualisierten KRITIS-Verordnung sehen sich zahlreiche Unternehmen der Tatsache gegenüber, dass ihre Anlagen nun als Kritische Infrastrukturen gelten – und sie damit verschärften Regulierungen unterliegen. Mit dem IT-Sicherheitsgesetz 2.0 verfolgt der Gesetzgeber einen ganzheitlichen Ansatz mit einem Fokus auf vernetzten Systemen. IT-Sicherheit wird nicht mehr als Angelegenheit eines Einzelnen betrachtet, sondern als Gemeinschaftsaufgabe. Zu den bereits bestehenden rund 1.600 KRITIS-Betreibern kommen geschätzt 270 neue hinzu.
Das IT-Sicherheitsgesetz 2.0 beinhaltet vier wesentliche Neuerungen, so etwa die Verpflichtung, bis zum 1. Mai 2023 ein Angriffserkennungssystem (Instrusion Detection System, IDS) einzuführen, das kontinuierlich den Netzwerkverkehr analysieren und Bedrohungen anhand von Mustern erkennen kann. Damit wird es möglich, automatisiert und in Echtzeit über potenzielle Sicherheitsvorfälle informiert zu werden.

BSI erhält offensive Möglichkeiten

Zudem ist der Einsatz kritischer Komponenten für KRITIS-Betreiber nun meldepflichtig. Zusätzlich müssen die Hersteller der Komponenten eine Garantieerklärung hinsichtlich der Vertrauenswürdigkeit entlang der gesamten Lieferkette abgeben. Bei berechtigten Zweifeln darf das Bundesministerium des Innern und für Heimat (BMI) den Einsatz einer kritischen Komponente untersagen.
Des Weiteren werden die Befugnisse des Bundesamts für Sicherheit in der Informationstechnik (BSI) erweitert. Agierte dieses bislang eher defensiv, erhält es mit dem IT-Sicherheitsgesetz 2.0 eine Vielzahl offensiver Möglichkeiten. So reicht zukünftig bereits der Verdachtsfall auf ein nicht ausreichend geschütztes, öffentlich erreichbares IT-System bei einem KRITIS-Betreiber aus, damit das BSI ohne vorherige Bekanntgabe eigene Maßnahmen wie Portscans oder eine aktive Schwachstellensuche durchführen darf, um mögliche Sicherheitslücken zu detektieren. Zu guter Letzt werden mit dem IT-Sicherheitsgesetz 2.0 die Bußgelder – analog zur Datenschutz-Grundverordnung (DSGVO) – verschärft.

UBI als neue Kategorie

Die Liste der KRITIS-Sektoren wird darüber hinaus um den Sektor „Siedlungsabfallentsorgung“ erweitert. Außerdem wird mit den „Unternehmen im besonderen öffentlichen Interesse (UBI)“ eine neue Kategorie neben den KRITIS-Betreibern geschaffen. In einigen KRITIS-Sektoren werden zudem die Schwellenwerte angepasst. Das hat insbesondere für den Sektor Energie große Auswirkungen. Lag der Schwellenwert für die Einstufung als Kritische Infrastruktur für Stromerzeugungsanlagen zuvor bei 420 Megawatt (MW) Nettonennleistung, wurde er jetzt auf 104 MW abgesenkt. Ist die Anlage für die Erbringung von Primärregelleistung zuständig, gilt sogar ein Schwellenwert von nur 36 MW – wobei schwarzstartfähige Anlagen immer als Kritische Infrastruktur gelten. Waren zuvor also selbst große Windparks an Land außen vor, fallen nun geschätzt fast 170 neue Betreiber allein im Energiesektor in den KRITIS-Bereich.

Notwendige Maßnahmen

Im ersten Schritt ist für Unternehmen, die bislang nicht unter die KRITIS-Verordnung gefallen sind, zu prüfen, ob sie aufgrund der neuen Regelungen nun als Betreiber Kritischer Infrastrukturen gelten. Sollte dies der Fall sein, sind strenge Maßnahmen umzusetzen: Zuallererst gilt es, ein Information Security Management System (ISMS) nach ISO 27001 einzuführen, mehr Informationen zu dokumentieren, in den meisten Fällen die internen Prozesse anzupassen, einen Ansprechpartner für das BSI zu benennen und bei einer IT-Störung der entsprechenden Meldepflicht nachzukommen. Als registrierter KRITIS-Betreiber durchläuft man hierfür eine Zertifizierung, die regelmäßig überprüft wird.

Verschärfung der Regelungen

Auch für diejenigen, die schon vorher KRITIS-Betreiber waren, verschärft das IT-Sicherheitsgesetz 2.0 wie oben erwähnt die Regelungen. Eine Herausforderung besteht in der fehlenden Konkretisierung. So ist für das künftig vorgeschriebene Angriffserkennungssystem etwa dessen Funktionsweise definiert, es gibt aber keine Vorgabe, welche konkreten Systeme den Regelungen entsprechen. Ähnlich gelagert ist die Anforderung, nur validierte kritische Komponenten in KRITIS-Anlagen einzusetzen. Aktuell finden Erzeuger in der Energie- und Wasserversorgung weder spezifische Regelungen noch Whitelists, welche Technologien verbaut werden dürfen. Eine zusätzliche Hürde ist der Umstand, dass vielen Mitarbeitenden derzeit noch das notwendige Hintergrundwissen fehlt, um mit den neuen Anforderungen umgehen zu können.
Mit der nächsten Version des IT-Sicherheitsgesetzes und der Umsetzung der Richtlinie EU NIS 2 ist zudem mit einer weiteren Verschärfung der Sicherheitsanforderungen zu rechnen, aus dem sich zunehmend auch ein Handlungsbedarf für kleinere Stadtwerke ergibt. Ist aktuell etwa der Einsatz eines Angriffserkennungssystems erforderlich, könnte der nächste Schritt eine umfassendere Betrachtung der eigenen Sicherheitslage mittels eines Security Information and Event Management (SIEM) sein, bei dem zusätzlich eine Vielzahl an Log-Nachrichten und Statusmeldungen ausgewertet wird.

Ausweitung des Fokus

In Zukunft werden zudem sektorübergreifende Abhängigkeiten und bislang nicht erfasste Infrastrukturen im Fokus stehen. Nach der Richtlinie EU NIS 2 sollen Kritische Infrastrukturen zukünftig zum Beispiel nur noch nach Unternehmensgröße (Mitarbeiter und Umsatz) eingestuft werden, wodurch sich die Anzahl der KRITIS-Anlagen signifikant erhöhen könnte.
Die Energiebranche ist aufgrund ihrer hohen Bedeutung für Wirtschaft und Gesellschaft ein beliebtes Angriffsziel für Cyber-Kriminelle. Angriffe auf Infrastrukturen der Energie führen aufgrund der Vernetzungen und Abhängigkeiten zwischen den KRITIS-Sektoren nicht selten zu einem Domino- oder sogar Kaskadeneffekt. Wurden früher Opfer noch gezielt ausgewählt, sind heute breit angelegte Angriffswellen üblich. Es ist also nur eine Frage der Zeit, bis eine Anlage attackiert wird. Umso wichtiger ist die Vorbereitung darauf – im gesamten Unternehmen.

()

Dieser Beitrag ist im Schwerpunkt IT-Sicherheit der Ausgabe März/April 2023 von stadt+werk erschienen. Hier können Sie ein Exemplar bestellen oder die Zeitschrift abonnieren.

Stichwörter: Informationstechnik, Fraunhofer IOSB, IT-Sicherheitsgesetz 2.0, KRITIS