IT-Sicherheit
Immer Bescheid wissen

[2.5.2022] Durch das neue IT-Sicherheitsgesetz und die KRITIS-Verordnung zählen mehr Unternehmen zu Betreibern Kritischer Infrastruktur. Sie müssen nun ihre IT-Sicherheitssysteme überprüfen und oft auch modernisieren.

Kritische Infrastrukturen (KRITIS) – wie die Energieversorgung – und staatliche Einrichtungen werden für Hacker immer interessanter. Schon seit Jahren warnen Regierungsbehörden auf der ganzen Welt vor Angriffen von Cyber-Kriminellen, die Daten verschlüsseln, um Lösegeld zu erpressen, oder beispielsweise durch provozierte Versorgungsengpässe versuchen, eine Gesellschaft zu destabilisieren.
Angesichts der zunehmenden Komplexität von Cyber-Bedrohungen lautet die Frage längst nicht mehr, ob eine Behörde, Organisation oder ein Unternehmen attackiert wird, sondern wann – und wie sie weiterhin in der Lage bleiben, ihre Aktivitäten unbeschadet fortzusetzen. Daher hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) nachjustiert – mit einem zweiten Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 2.0, abgekürzt als SiG 2.0) und einer dazugehörigen Verordnung.
Mit der Einführung des SiG 2.0 und der BSI-KRITIS-Verordnung (BSI-KritisV) zählen seit Januar 2022 mehr Unternehmen zu den KRITIS-Einrichtungen, insbesondere aus dem Energiesektor. Für sie und alle anderen Betreiber Kritischer Infrastrukturen bedeutet die neue Verordnung zudem, dass sie ihre IT-Sicherheitssysteme überprüfen und oft auch modernisieren müssen. Der Handlungsbedarf ist groß, da die Bußgelder bei Verstößen auf bis zu 20 Millionen Euro drastisch erhöht wurden. Darüber hinaus werden den IT-Verantwortlichen weitere und vielfältigere Aufgaben übertragen: Sie müssen Systeme überwachen, potenzielle und tatsächliche Risiken frühzeitig erkennen, externe wie interne Risiken und Events analysieren und bewerten sowie geeignete technische und organisatorische Maßnahmen ableiten und umsetzen. Doch welche Neuerungen und Änderungen bringt das IT-Sicherheitsgesetz 2.0 genau mit sich? Und wie können KRITIS-Einrichtungen und Unternehmen im öffentlichen Interesse den neuen Anforderungen bestmöglich gerecht werden?

Mehr KRITIS-Betreiber

Das IT-SiG 2.0 erweitert den Wirkungskreis mit der zusätzlichen Kategorie "Unternehmen im besonderen öffentlichen Interesse"

(UBI) erheblich, wozu Rüstungshersteller und Chemieunternehmen zählen, sowie dem neuen Sektor der Siedlungsabfallentsorgung als Kritische Infrastruktur. Zu beachten ist grundsätzlich, dass privatwirtschaftliche Unternehmen ebenso betroffen sein können wie Verwaltungsdienststellen, Stadtwerke oder andere öffentliche Einrichtungen.
Ein Beispiel hier ist der öffentliche Personennahverkehr, der ebenfalls als Kritische Infrastruktur gilt. Eine große Herausforderung ist sicherlich, dass betroffene Einrichtungen selbst herausfinden müssen, ob sie nach den neuen Vorgaben Betreiber Kritischer Infrastrukturen sind. Schon ab dem ersten Werktag, an dem sie die Schwellenwerte der BIS-KritisV 2.0 erreichen, müssen sie die Anforderungen des IT-SiG 2.0 erfüllen.
Das neue Gesetz sieht für all diese Organisationen umfangreiche Sicherheitsmaßnahmen vor. Für KRITIS-Betreiber besteht die Pflicht, ihre IT-Sicherheit beispielsweise durch vorgegebene Systeme zur Angriffserkennung auf dem neuesten Stand der Technik zu halten, Störungen zu melden, eine dauerhaft erreichbare Kontaktstelle einzurichten und einen jährlichen Lagebericht zu erstellen.
Diese Systeme zur Angriffserkennung müssen laut Gesetz "geeignete Parameter und Merkmale aus dem laufenden Betrieb kontinuierlich und automatisch erfassen und auswerten" (§ 8a Abs. 1a BSIG). Dabei soll der Stand der Technik eingehalten werden. Diesen Anspruch erfüllt beispielsweise ein "Security Information and Event Management"-System (SIEM). Dabei handelt es sich um ein softwarebasiertes Technologiekonzept, mit dem ein ganzheitlicher Blick auf die IT-Sicherheit möglich wird.

Komponenten mit Garantie

Außerdem dürfen KRITIS-Betreiber nur noch kritische Komponenten verbauen, für die der Hersteller eine Garantieerklärung abgegeben hat. Produkte, die vom Bundesministerium des Innern als nicht vertrauenswürdig eingestuft werden, dürfen von KRITIS-Betreibern dann nicht mehr eingesetzt werden. Somit sind nun auch explizit Zulieferer von KRITIS-Betreibern von dem Gesetz betroffen.
Darüber hinaus erhält das BSI mehr Befugnisse beim Aufdecken und Abwehren von Cyber-Angriffen. So darf das Bundesamt zur Erhöhung der Sicherheit in den Mobilfunknetzen künftig Portscans durchführen, um Sicherheitslücken an den Schnittstellen von IT-Systemen zu öffentlichen Telekommunikationsnetzen aufzudecken. Mit knapp 800 neuen Planstellen ist hierfür ein massiver Ausbau des Personals geplant. Die umfangreiche Aufstockung von Kompetenzen und Personal im BSI sowie die

Ausweitung des KRITIS-Geltungsbereichs stellt den öffentlichen Sektor von gesetzlicher Seite vor teils große Herausforderungen. Eine praktikable Lösung bietet eine umfangreiche SIEM-Plattform. Das Security-Management-System von Splunk beispielsweise ermöglicht es, große Datenmengen unabhängig von Format und Quelle nahezu in Echtzeit zu überwachen, zu untersuchen und zu analysieren. Das Monitoring von Schwachstellen, Auffälligkeiten und Abweichungen unterstützt bei der schnellen Identifizierung der Angreifer. Um eine wirksame IT-Sicherheit aufzubauen, können bereits vorhandene eigene Daten als Handlungsgrundlage dienen. Ebenso kann das SIEM bei der Etablierung und Modernisierung eines dedizierten IT-Sicherheitsbetriebs enorme Dienste leisten. Eine SIEM-Lösung bietet den IT-Sicherheitsverantwortlichen Transparenz und handfeste Ergebnisse auf einer zentralen Plattform, die alle wichtigen Kernfunktionen für einen sicheren Betrieb abdeckt: Monitoring, Bedrohungserkennung, Analyse und Reaktion.

Frühzeitige Angriffserkennung

Cyber-Attacken gehören beinahe schon zum Alltag. Das haben zuletzt vor allem die sich häufenden Ransomware-Angriffe deutlich gemacht, die weder vor Versorgungsunternehmen noch vor Kliniken Halt machen. Systeme zur frühzeitigen Angriffserkennung sind in der Abwehr solcher Bedrohungen ein zentraler Baustein – einer, den KRITIS-Betreiber nun verpflichtend vorweisen müssen. Sie müssen sehr viel genauer darüber Bescheid wissen, was in sämtlichen ihrer Systeme, Netze und Endpunkte vorgeht.

Matthias Maier

Der Autor, Matthias Maier
Matthias Maier ist Sicherheitsexperte beim Datenplattform-Anbieter und SIEM-Spezialisten Splunk. Er arbeitet eng mit Betreibern Kritischer Infrastrukturen zusammen, darunter der Flughafen München sowie die Würzburger Versorgungs- und Verkehrs-GmbH.

https://www.splunk.com/de_de
Dieser Beitrag ist in der Ausgabe März/April 2022 von stadt+werk erschienen. Hier können Sie ein Exemplar bestellen oder die Zeitschrift abonnieren. (Deep Link)

Stichwörter: Informationstechnik, KRITIS, BSI, SiG 2.0

Bildquelle: vectorfusionart/stock.adobe.com

Quelle: www.stadt-und-werk.de