Stresstest für IT-Systeme

IT-Sicherheit: Expertenmeinungen zum Schutz Kritischer Infrastruktur (Kritis) sind kontrovers und entsprechen nicht immer den Ansichten aus der Politik.

Von Uwe Sievers

Angriffe und Anschläge auf kritische Infrastruktur (Kritis) führen zu politischen Forderungen nach höherem Schutz der kritischen Infrastruktur (s. Seite 12). Experten sehen Forderungen aus der Politik kritisch, wie eine Recherche während der Security-Fachmesse IT-SA deutlich zeigte. Sie beurteilen nicht nur die Situation differenziert, sondern warten mit unterschiedlichen Lösungsansätzen auf.

Kritis-Unternehmen sind teils überfordert: „Die klassischen IT-Schutzmechanismen greifen einfach zu kurz, weil die Angriffsformen komplexer geworden sind“, erklärt dazu Sahab Ölmez, der beim Anbieter für Hochsicherheitslösungen Rohde & Schwarz Cybersecurity (R&S) für den Vertrieb im Kritis-Segment zuständig ist. Er warnt davor, die Angreifer zu unterschätzen: „Professionelle Angreifer verfügen über umfassendes Fachwissen, die sind nicht naiv.“ Ölmez empfiehlt: „Man muss sich immer überlegen, was ein Tag Betriebs- oder Produktionsausfall kostet.“

Kritis-Unternehmen sehen sich diesen Herausforderungen oft nicht gewachsen. Ölmez beschreibt die Situation so: „Viele Unternehmen wissen, dass sie etwas machen müssen, aber sie wissen nicht was.“ Er fügt hinzu: „Es existieren zwar viele Sicherheitslösungen, aber Unternehmen sind häufig überfordert, die Spreu vom Weizen zu trennen.“

Manchmal wurden zwar sinnvolle Sicherheitsvorkehrungen getroffen, doch sie reichen heute nicht mehr aus. So finden sich im Bahnverkehr an sensiblen Stellen unverschlüsselte Kommunikationsverbindungen: „Zum Beispiel könnte sich jemand bei Weichenstellungen dazwischenschalten und ein Signal oder den Befehl an eine Weiche manipulieren“, erläutert Ölmez. Katastrophale Unfälle könnten die Folge sein.

Die Problemlage sei nicht bei allen Kritis-Betreibern identisch, betont Stefan Strobel, Geschäftsführer und Gründer des IT-Sicherheitsspezialisten Cirosec. „Besonders sensible Infrastruktur wie Kernkraftwerke sind seit Jahrzehnten sehr gut abgesichert“, hebt er hervor. „Dort ist beispielsweise die IT-Architektur in verschiedene Ringe unterteilt aufgebaut, die voneinander abgeschottet sind.“

Anders sieht es bei kleineren Betreibern kritischer Infrastruktur aus. Hier verlasse man sich oft nur auf klassische IT-Sicherheitselemente wie Firewall und Malware-Schutz. Es fehle aber die Möglichkeit, Angriffe oder gar Eindringlinge zu erkennen. Dadurch könnten Gegenmaßnahmen nicht oder nur verzögert eingeleitet werden. Strobel kritisiert die gegenwärtige Regulierung durch das BSI: Die Behörde habe eine „Orientierungshilfe zum Einsatz von Systemen zur Angriffserkennung“ erstellt. „Darin fordert das Amt im Prinzip so etwas wie ein SIEM oder etwas, das regelbasiert Logfiles auswertet“, so Strobel.

Mit einem SIEM, einem Security Information and Event Management, können sicherheitsrelevante Meldungen aus Protokolldateien und anderen Quellen ausgewertet werden. Des Weiteren werde gefordert, dass an Netzwerkübergängen, also an Gateways, eine Erkennung für Eindringungsversuche – Network Intrusion Dection (IDS) – installiert sein muss. Strobel mahnt: „Beides, sowohl SIEM als auch IDS, sind im Prinzip Techniken von vor 20 Jahren, man könnte das stattdessen mit modernen Mitteln machen.“ Doch Betreiber seien verpflichtet, die antiquierten Vorgaben bis zum Frühjahr 2023 umzusetzen.

Foto: PantherMedia / TTstudio

Kritische Infrastrukturen, wie hier eine Raffinerie der Öl- und Gasindustrie, stehen immer im Blickpunkt von Cyberkriminellen. Hier ist besonderer Schutz gefragt.

Resilienz als Lösung: Mirko Ross, Geschäftsführer und Gründer von Asvin, einem Spezialisten für das Internet der Dinge (IoT), betrachtet die Problematik aus einem anderen Blickwinkel. „Kritische Infrastruktur lässt sich nur bedingt schützen. Wenn ich zum Beispiel weiß, wo Transformatorenhäuser stehen, kann ich immer irgendwie einen Stromausfall verursachen.“ Er rät: „Resilienz ist hier das Schlüsselwort.“ Darunter wird die Fähigkeit verstanden, mit Störungen so umzugehen, dass es nicht zu gravierenden Folgen oder Ausfällen kommt.

Digitalisierung in IoT-Bereichen wie im Energiesektor steht vor besonderen Herausforderungen. Dabei müsse bedacht werden, dass IT-Komponenten schnell veralten und irgendwann dafür keine Updates mehr verfügbar sind. „Das kann dazu führen, dass während der Lebensdauer einer Anlage Steuerungselemente öfter mal ausgetauscht werden müssen, um sie update-fähig zu halten oder weil unsichere Hardware ausgewechselt werden muss“, stellt Ross fest.

Er hat noch einen Tipp, der schon in so mancher Notlage geholfen hat: „Es ist ratsam, nach einer Digitalisierung analoge Geräte nicht gleich wegzuwerfen, dann kann man bei größeren Ausfällen noch darauf zurückgreifen.“