Kritis 2.0: IT-Sicherheit im Fokus

Die neuen Anforderungen an kritische Infrastrukturen im Überblick

Mit 2022 ist die Novelle der Kritis-Verordnung offiziell in Kraft getreten. Neben neuen Sicherheitsmaßnahmen für kritische Infrastrukturen, also Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, erweitert sich auch der Adressatenkreis der Vorschrift: Unternehmen mit hoher inländischer Wertschöpfung oder solche, die mit gefährlichen Stoffen arbeiten, fallen nun in eine eigene Kategorie.

©Blue Planet Studio - stock.adobe.com

Die Absicherung von IT-Umgebungen bleibt 2022 ein Kernthema in der Industrie. Seit Jahren beobachten Experten einen Anstieg an Schadsoftware und Cyberangriffen, der durch die Krise der vergangenen Jahre zusätzlich an Fahrt aufgenommen hat. Hacker und Cyberkriminelle entwickeln laufend neue Methoden, um Netzwerke zu infiltrieren, Daten zu stehlen und den Betrieb zu sabotieren. Für betroffene Firmen bedeutet eine erfolgreiche Attacke meist kostspielige und langwierige Ausfälle. Immer öfter wird dabei auch grundlegende Infrastruktur zum Ziel der Kriminellen. Der Angriff auf die Colonial Pipeline in den USA etwa dürfte vielen im Gedächtnis geblieben sein.

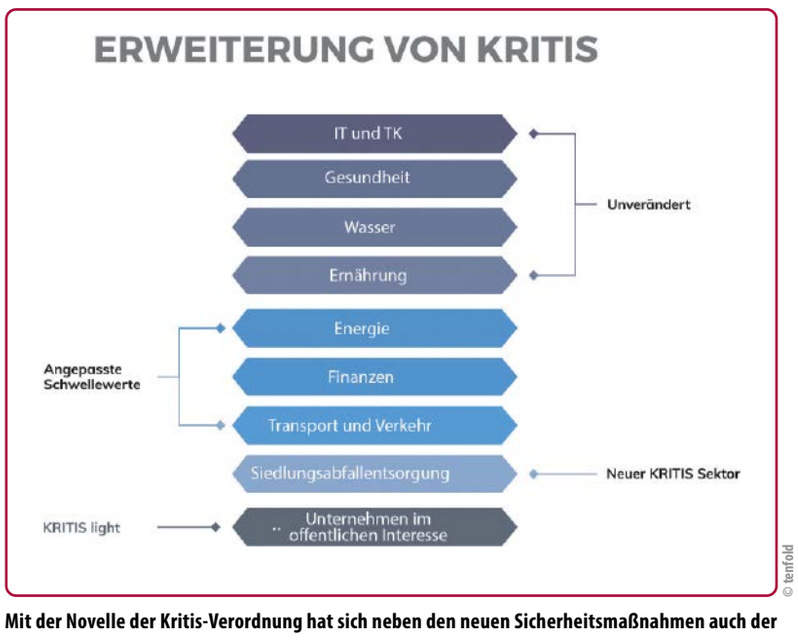
Angesichts immer dreisterer Attacken ist auch das politische Interesse am Thema IT-Sicherheit ungebrochen hoch. Im vergangenen Jahr beschloss der Deutsche Bundestag die Anpassung des bestehenden IT-Sicherheitsgesetzes und der Kritis-Verordnung. Durch die Novellen soll die Grundversorgung der Bevölkerung in Bereichen wie Energie, Gesundheit und Ernährung noch besser gegen digitale Angriffe abgesichert werden.

Schon bisher zählten unter anderem Gasanlagen, Ölraffinerien und die Hersteller von Medikamenten zu jenen Betrieben, die ein angemessenes digitales Schutzniveau nachweisen müssen. Kritis 2.0 ergänzt die bestehenden Sektoren um den Bereich der Abfallentsorgung und etabliert darüber hinaus eine zusätzliche Kategorie: die Unternehmen im besonderen öffentlichen Interesse (UBI). Hier wird zwischen drei Typen unterschieden.

- UBI 1: Unternehmen, die Rüstungsmaterial oder IT-Produkte für staatliche Verschlusssachen herstellen.
- UBI 2: Firmen mit hoher inländischer Wertschöpfung und einer großen Bedeutung für die deutsche Wirtschaft (ein genauer Kriterienkatalog fehlt aktuell noch).
- UBI 3: Betriebe, die mit Gefahrstoffen im Sinne der Störfallverordnung arbeiten und dabei die obere Mengenschwelle überschreiten.

> *Cyberkriminelle entwickeln laufend neue Methoden, um Netzwerke zu infiltrieren.*
>
> Helmut Semmelmayer, Tenfold Software

Während die Betreiber vollwertiger Kritis-Anlagen dazu verpflichtet sind, Schutzmaßnahmen zu treffen und durch eine entsprechende Zertifizierung zu bestätigen, müssen Unternehmen im öffentlichen Interesse bislang kein bestimmtes Sicherheitsniveau nachweisen. Je nach Unterkategorie gilt es aber, einige weitere Auflagen zu erfüllen.



© tenfold

Mit der Novelle der Kritis-Verordnung hat sich neben den neuen Sicherheitsmaßnahmen auch der Adressatenkreis der Vorschriften erweitert.

UBI 1 und 2 müssen sich im Vorfeld beim Bundesamt für Sicherheit in der Informationstechnik (BSI) registrieren, eine Kontaktstelle zu der Behörde einrichten und alle zwei Jahre eine Selbsterklärung zu ihrer IT-Sicherheit abgeben, die über durchlaufene Audits, vorhandene Zertifizierungen und Schutzmaßnahmen für besonders anfällige Komponenten und Prozesse informiert. Betriebe, die in den oberen Bereich der Störfallverordnung fallen, sind hingegen nur zur Meldung von erheblichen Störungen und Ausfällen verpflichtet. Die Registrierung beim BSI ist auf freiwilliger Basis möglich.

Standards für Informationssicherheit

Das übergeordnete Ziel der Kritis-Verordnung ist es, die Informationssicherheit in den operativen Prozessen der Betreiber zu verankern. Neben technischen Schutzmaßnahmen spielen dabei auch die personelle Ausstattung, Organisationsstruktur und physische Absicherung eine wesentliche Rolle. Als Grundlage für die Vorbereitung dienen in der Regel etablierte Standards wie der IT-Grundschutz des BSI oder die internationale Norm ISO 27001. Ein Kernpunkt dieser Modelle ist der Aufbau eines Informationssicherheitsmanagementsystems (ISMS), durch das Ziele, Aufgaben, Planung und Verantwortlichkeiten klar geregelt werden. Neben der Position des IT-Leiters sind dazu etwa die getrennten Rollen des Sicherheitsbeauftragten (CISO, Chief Information Security Officer) und des Verantwortlichen für Sicherheitsvorfälle zu besetzen.

Allgemeine Standards wie ISO 27001 bieten eine Blaupause für die Entwicklung eines IT-Sicherheitskonzepts, gehen aber kaum auf die technischen Besonderheiten von Kritis-Anlagen ein. Leitsysteme, Steueranlagen und ähnliche industrielle Komponenten sind für einen reibungslosen Betrieb von entscheidender Bedeutung und haben einen entsprechend hohen Schutzbedarf im Informationsverbund. Hier ist Eigeninitiative gefragt: Schließlich kennt niemand die eigene Produktionsanlage besser als man selbst. Aus Rücksicht auf die einzigartigen Merkmale der Kritis-Sektoren erlaubt das BSI auch die Einreichung von branchenspezifischen Sicherheitsstandards (B3S). Diese können für die Zertifizierung verwendet werden, müssen es aber nicht.

Die neuen Kritis-Anforderungen

Bei der Abwehr von Cyberangriffen spielen viele Faktoren eine Rolle. Der Katalog an vorgesehenen Sicherheitsmaßnahmen des BSI umfasst etwa den Schutz vor Schadsoftware, die Überwachung von Netzwerkverbindungen, die laufende Analyse von Schwachstellen, regelmäßige und zuverlässige Backups von Daten, die sichere Konfiguration von Systemen, den Einsatz von kryptografischer Verschlüsselung und sichere Anmeldeverfahren für Benutzer. Als Hilfestellung für Unternehmen veröffentlicht die Behörde laufend Informationen zur Umsetzung dieser Maßnahmen, so etwa in dem Sammeldokument „Konkretisierung der Anforderungen gemäß §8a Absatz 1 BSIG“. Durch Kritis 2.0 wird ab 2023 nun zusätzlich der Einsatz von „Systemen zur Angriffserkennung“ explizit vorgeschrieben.

Diese neue Forderung bezieht sich auf die Software-Kategorie des Security Information & Event Management (SIEM), also Anwendungen, die das Firmennetzwerk überwachen und anhand bestimmter Parameter automatisch auf ungewöhnliche Aktivitäten hinweisen, bspw. verdächtigen Datenverkehr oder unberechtigte Zugriffsversuche. Um dabei die Spreu vom Weizen zu trennen und echte Vorfälle von Fehlalarmen zu unterscheiden, muss eine SIEM-Lösung unbedingt durch qualifizierte Fachkräfte betreut werden, die die Daten des Systems auswerten und bei Bedarf Meldung an das BSI erstatten können. Ein durchgehend besetztes Security Operation Center (SOC) kann auch die Funktion als Kontaktstelle zur Behörde übernehmen und Updates zu neuen Bedrohungen empfangen.

Mit Automatisierung zum Erfolg

Die Kombination aus softwaregesteuerter Datensammlung und Auswertung durch geschultes Personal macht deutlich, dass der Schutz digitaler Systeme nur durch die Zusammenarbeit von Mensch und Technik gelingt. Dank automatisierter Lösungen für Sicherheitsupdates, Netzwerküberwachung oder die Vergabe von Zugriffsrechten können Routinetätigkeiten effizient und sicher abgewickelt werden. Dadurch gewinnt das IT-Team Zeit, um sich übergeordneten Themen wie der Analyse von Schwachstellen, Planung von Notfalltests oder der Schulung von Mitarbeitern zu widmen. Richtig eingesetzt bedeuten diese Tools eine ähnliche Erleichterung, wie sie Steuerungssysteme, Automatisierungstechnik und Fertigungsanlagen auf industrieller Ebene mit sich bringen.

© tenfold

Die neuen Sicherheitsstandards sind in den betroffenen Unternehmen schrittweise innerhalb der vorgesehenen Fristen umzusetzen.

Plattformen zur Automatisierung von IT-Aufgaben sind auch deshalb enorm wichtig, da Fachkräfte wie Sicherheitsexperten gerade in Deutschland nach wie vor ein rares Gut sind. Um die Pflichten im Rahmen der Kritis-Verordnung und ähnlicher Zertifizierungen erfüllen zu können, ist es für Betriebe dringend nötig, kleinere Aufgaben so weit wie möglich zu automatisieren. Hier gibt es zahlreiche Ansatzpunkte: Das Einspielen von Sicherheitsupdates, die Erstellung von Backups ebenso wie die Kontrolle von Endgeräten.

Um Arbeitsabläufe zu optimieren und den Schutz sensibler Systeme zu gewährleisten, ist gerade die automatische Benutzerverwaltung eine lohnende Investition. Ohne eine entsprechende Software-Lösung verbringen Admins oft viele Stunden pro Woche allein mit Aufgaben wie der Anpassung von Berechtigungen oder dem Zurücksetzen von Passwörtern. Hier schafft eine Plattform für Identity und Access Management (IAM) dank Self-Service-Funktionen Abhilfe. Gleichzeitig sorgen IAM-Lösungen dafür, dass die Berechtigungen aller Nutzer laufend angepasst werden und diese nur auf notwendige Systeme zugreifen können. Die selbstständige Minimierung von Zugriffsrechten reduziert nicht nur den Arbeitsaufwand, sondern trägt auch dazu bei, das Risiko von Cyberangriffen über Benutzerkonten zu reduzieren. Die zentrale Verwaltung mittels Identity und Access Management bildet somit eine wichtige Grundlage für mehr Informationssicherheit und die Einhaltung der Kritis-Verordnung.

Helmut Semmelmayer, Senior Manager Channel Sales, Mitglied der Geschäftsführung, Tenfold Software, Wien

■ www.tenfold-security.com