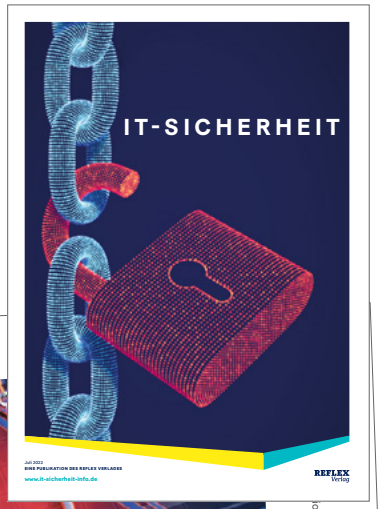
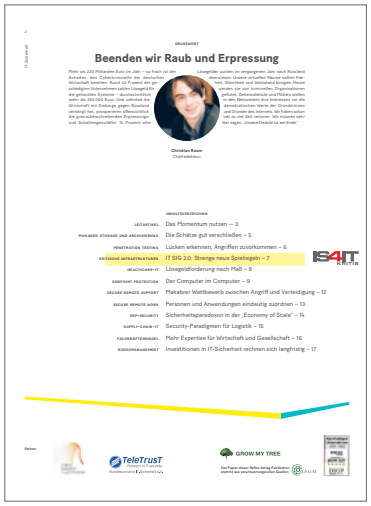
IS4IT KRITIS

PRESSECLIPPING

Sonderbeilage der FAZ vom 21.07.2022





IT-SiG 2.0: Strenge neue Spielregeln

KRITISCHE INFRASTRUKTUREN | VON CHRISTIAN RAUM

Seit Januar 2022 ist das IT-Sicherheitsgesetz 2.0 in Kraft. Damit wurde die Sicherheit von Systemen und Netzwerken zur Pflicht der Betreiber von kritischen Infrastrukturen. Diese sind nur dann gesetzeskonform, wenn sie ihre IT-Security nachweisen können.

Wirtschaft und Gesellschaft haben in den vergangenen Jahren viele Cyberattacken ausgehalten und Hunderte Millionen Euro an kriminelle Banden verloren. Trotz aller Anstrengungen ist weder die Bedrohungslage entspannter, noch ist die Zahl der Angriffe gesunken. Es scheint so, als wären die Angreifer durch das Investieren der Vermögen, die sie geraubt haben, zu weltumspannenden Verbrecherorganisationen mutiert.

Hacker-Industrie kassiert Unternehmen ab

Insider berichten, kriminelle Hacker hätten sich inzwischen zu Cyber-Industrieunternehmen zusammengefunden, die bei der Plünderung arbeitsteilig agieren und in Bitcoins abrechnen. Wissenschaftlerteams brechen in den Laboratorien die neueste Hardware und Software auf, analysieren sie auf Schwachstellen und entwickeln neue Angriffsvektoren und Algorithmen. Damit attackieren deren Kolleginnen und Kollegen dann ihre Opfer. Hier spielen wirtschaftliche Aspekte die wesentliche Rolle – wer am billigsten gehackt werden kann, wird zuerst geknackt, dessen Daten verschlüsselt und die Firmengeheimnisse höchstbietend verkauft. Dann melden sich die Unterhändler, um Geld einzusammeln. Auf Anraten der hackereigenen Rechtsabteilungen erpressen sie ihre Opfer häufig nicht mehr. Stattdessen bieten sie freundlich den Kauf von „Entschlüsselungssoftware" an. So könnten die Kosten buchhalterisch als „Ausgaben für digitale Wirtschaftsgüter" verbucht und bei der Steuer geltend gemacht werden.

Maßnahmen gegen das Plündern und Rauben

Der Staat ist offensichtlich mit seiner Geduld am Ende – sowohl mit der Geduld gegenüber den Angreifern, die Wirtschaft und Gesellschaft Milliarden kosten, als auch mit der Geduld gegenüber den Unternehmen. Hier wiegt das Management oft ab, ob man viel Geld in einen guten Schutz investieren sollte – oder lieber Geld zurücklegt, um im Fall eines staatlichen Audits die Bußgelder zu bezahlen. Mit den Sicherheitsgesetzen 2.0 sollte es diese Option nicht mehr geben: Seit Januar 2022 zwingt der Gesetzgeber mit hohen Strafandrohungen die Unternehmen mit kritischen Infrastrukturen, sich zu schützen. Ab Mai 2023 wird zusätzlich der Einsatz einer Angriffserkennung verpflichtend und muss explizit nachgewiesen werden. ❑

Kriminelle bieten freundlich den Kauf von Entschlüsselungssoftware an, die steuerlich geltend gemacht werden könne.

...tionen unter – www.it-sicherheit-info.de

Silver Business Partner IBM

„Angriff erkennen ist gesetzliche Pflicht"

Fokusinterview

Manuel Noe, Geschäftsführer der IS4IT KRITIS GmbH, erklärt, wie Unternehmen mit einer intelligenten Security-Monitoring-Lösung wie IBM QRadar die Anforderungen aus dem IT-Sicherheitsgesetz 2.0 erfüllen und welche Argumente für das Monitoring durch ein externes Security Operations Center (SOC) sprechen.

Welche Veränderungen hat das IT-Sicherheitsgesetz 2.0 bei der Absicherung der kritischen Infrastrukturen gebracht? Der Gesetzgeber hat die Schwellenwerte angepasst, und die Anzahl der Betreiber von kritischen Infrastrukturen ist somit deutlich gestiegen. Zusätzlich behält sich der Staat vor, Unternehmen mit besonderem öffentlichem Interesse, unabhängig von deren Branche, als kritische Infrastruktur einzustufen. Es gibt keine Schlupflöcher mehr, die Verantwortlichen müssen reagieren und die Anforderungen umsetzen. Der Druck auf das Management ist erhöht, denn eine Änderung im IT-SiG 2.0 ist, dass die Bußgelder für Fehlverhalten um ein Vielfaches höher sind als früher.

Manuel Noe ist Geschäftsführer bei der IS4IT KRITIS GmbH

Welche wichtigen technischen Neuerungen kommen auf die Anwender zu? Da möchte ich insbesondere die Vorsorgepflichten nennen. Ab Mai 2023 müssen Unternehmen aus den kritischen Infrastrukturen Systeme zur Angriffserkennung implementiert haben und diese bei Audits nachweisen.

Welches sind aus der Sicht eines Betreibers von kritischen Infrastrukturen die wichtigsten Kriterien bei der Auswahl einer Angriffserkennung? Der Partner, der die Sicherheitslösung implementiert, muss das Fachwissen besitzen, die Systeme den individuellen Anforderungen der Unternehmen anzupassen. Denn die Lösungen sollten sehr genau in die gesamte IT-Infrastruktur eingefügt werden, nur so kann die geforderte IT-Sicherheit erreicht werden. Für diese Anforderung ist das Tuning der Lösung wichtig.

Zweitens ist die Erstellung eines umfassenden Regelwerks notwendig, und – das ist entscheidend – das Herz des Betriebs, das Security Operations Center, muss 24x7 besetzt sein. Wer am nächsten Freitag sein Sicherheitsteam ins Wochenende schickt, steht vielleicht kommende Woche am Montagmorgen buchstäblich vor verschlossenen Türen und verschlüsselten Datenbanken.

Welche Argumente sprechen für die Zusammenarbeit mit einem Managed-Security-Service-Anbieter? Da sind natürlich das Security Operations Center und die für den Betrieb benötigte Mannschaft zu nennen. Es ist ein größeres Team aus Sicherheitsexpertinnen und -experten notwendig, welches bereit sein muss, im Schichtdienst und auch über das Wochenende zu arbeiten. Das ist ein Grund, warum es für Unternehmen von Vorteil ist, sich auf einen spezialisierten Dienstleister für Cybersecurity zu verlassen, der über die notwendige fachliche Kompetenz und auch die personellen Kapazitäten verfügt, um die Sicherheitssituation seiner Kunden rund um die Uhr im Blick zu behalten.

weitere Informationen finden Sie hier!