IT-Sicherheitsgesetz 2.0: Neuer Solution Brief von Sophos für KRITIS-Organisation zur Umsetzung der Bestimmungen

Der Fokus von cyberkriminellen Handlungen liegt auf Unternehmen und öffentlichen Einrichtungen, maßgeblich um den Betrieb lahm zu legen oder um Erpressungsgelder zu erbeuten. Dass die Gefahrenlage angespannt ist, belegen Fakten: Laut BSI wurden 2021 rund 144 Millionen neue Schadprogramme identifiziert. Rund 25 Prozent der betroffenen Unternehmen und Organisationen, sahen in den Angriffen eine schwerwiegende oder existenzbedrohende Gefahr. Dieses Gefahrenpotenzial wiegt umso schwerer, wenn kritische Infrastrukturen das Ziel der Cyberkriminellen sind, etwa im Gesundheitswesen, in den Bereichen der Energie- und Wasserversorgung oder bei der Nahrungsversorgung. Aus diesem Grund sind die Betreiber von kritischen Infrastrukturen (KRITIS) gesetzlich verpflichtet, „angemessene organisatorische und technische Vorkehrungen" zur Verhinderung von Cyber-Attacken zu treffen. Mit der Verabschiedung des „IT- Sicherheitsgesetzes 2.0" im Frühjahr 2021 wurden diese Pflichten noch einmal verschärft. Ab Mai 2023 müssen die Betreiber kritischer Infrastrukturen diese umsetzen und vor allem „Systeme zur Angriffserkennung" vorhalten.

Neue Auflagen aber wenig konkrete Handlungsempfehlung

Wie schon in der Vergangenheit haben die Behörden, welche die Sicherheit bei KRITIS einfordern, auch bei der neuen Auflage der Bestimmungen genaue Vorstellungen, wie Verstöße geahndet und bestraft werden. Allerdings lassen sie den Unternehmen und Organisationen weitestgehend freie Hand bei der Umsetzung der IT-Sicherheit. Die Begründung: Konkrete Handlungsempfehlungen könnten die fortschreitende Innovation auf dem Gebiet der IT-Technik behindern und dazu führen, dass die gesetzlichen Pflichten mit dem Aufkommen neuer Technologien schnell wieder veralten. Dieser Ansatz ist aus Sicht der Kontrollorgane nachvollziehbar, hilft den Unternehmen jedoch wenig bei der konkreten Umsetzung.

Security-Lösungsansatz für KRITIS

Sophos hat als offiziell vom BSI qualifizierter APT-Response-Dienstleister (Advanced Persistent Threat) für KRITIS einen Solution Brief erstellt, der Unternehmen und Organisationen hilft, ihre Security-Maßnahmen gemäß den neuen Anforderungen rechtzeitig anzupassen. Zur näheren Bestimmung der notwendigen Maßnahmen können sich KRITIS-Unternehmen und -Organisationen an zwei Anhaltspunkte orientieren: den „branchenspezifischen Sicherheitsstandards", die von den einzelnen Branchenverbänden der betroffenen Sektoren entwickelt wurden, und an der aktuellen Handreichung des BSI. Während die branchenspezifischen Sicherheitsstandards ausschließlich für den jeweiligen Sektor anwendbar sind, bietet die Handreichung des BSI allgemeine Anforderungen, die auf alle Sektoren und Branchen anwendbar sind. In diesem Anforderungskatalog legt das BSI 100 relevante Themen fest und erläutert die jeweiligen Sicherheitsvorkehrungen.

Im Solution Brief beschreibt Sophos, welche Themen aus dem Anforderungskatalog des BSI mit welchen Komponenten der Security adressiert werden können, um die geforderten Sicherheitsvorkehrungen umzusetzen – insbesondere im Zusammenhang mit dem neuen IT-Sicherheitsgesetz 2.0. Ein Schwerpunkt der neuen Gesetze liegt auf der Angriffserkennung. KRITIS-Unternehmen und -Organisationen müssen in der Lage sein, in der IT verarbeitete Daten laufend mit Informationen und technischen Mustern abzugleichen, um potenzielle Angriffe zu identifizieren. Dazu müssen Parameter und Merkmale im Betrieb kontinuierlich und

automatisch erfasst und vor allem ausgewertet werden. Die Raffinesse und schnelle Entwicklung der Cyberkriminellen erfordert eine Kombination aus automatisierter und mit Künstlicher Intelligenz angereicherter Security, sowie menschlicher Expertise. Sowohl technisch als auch menschlich betriebene Security sollte sich in einem Ökosystem zusammenfinden, um Bedrohungen zu vermeiden und vor allem eingetretene Störungen so schnell wie möglich zu beseitigen.

Zum Sophos Solution Brief für das IT-Sicherheitsgesetz 2.0 für KRITIS-Unternehmen und -Organisationen geht es hier.

Social Media von Sophos für die Presse
Wir haben speziell für Sie als Journalist*in unsere Social-Media-Kanäle angepasst und aufgebaut. Hier tauschen wir uns gerne mit Ihnen aus. Wir bieten Ihnen Statements, Beiträge und Meinungen zu aktuellen Themen und natürlich den direkten Kontakt zu den Sophos Security-Spezialisten.
Folgen Sie uns auf und

LinkedIn: https://www.linkedin.com/groups/9054356/
Twitter: @sophos_info

Pressekontakt:

Sophos
Jörg Schindler, PR-Manager Central & Eastern Europe
joerg.schindler@sophos.com, +49-721-25516-263

TC Communications
Arno Lücht, +49-8081-954619
Thilo Christ, +49-8081-954617
Ulrike Masztalerz, +49-30-55248198
Ariane Wendt +49-172-4536839
sophos@tc-communications.de