Cyber Risiko Self-Check

Welche dringenden Handlungsfelder JETZT unbedingt im Umfeld des Gesundheitswesens aufgrund der steigenden Bedrohungslage bewertet werden müssen.

Digitale Transformation im Gesundheitswesen und die gesetzlichen Anforderungen in Deutschland sowie die zunehmende Bedrohungslage im Cyber-Raum beeinflussen die notwendigen Sicherheitsmaßnahmen für alle im Gesundheitswesen befindlichen Organisationen maßgeblich.

Nicht umsonst erhöht auch das BSI auf Basis des IT-Sicherheitsgesetzes 2.0 für alle KRITIS-Betreiber die Anforderungen, die sich mit der Umsetzung der europäischen NIS2-Richtlinie in nationales Recht bis zum Herbst 2024 nochmals erhöhen. So werden die Anforderungen praktisch alle Einrichtungen des deutschen Gesundheitswesens betreffen, da sich die Schwellenwerte auf 50 Mitarbeiter und einen Jahresumsatz von 10 Millionen Euro ändern.

Neben der Einführung von Systemen zur Angriffserkennung und -vermeidung bis zum Mai 2023 sind im B3S für das Gesundheitswesen nach IT SIG2.0 neue Anforderungen für das Logging von IT und Medizintechnik, branchenspezifischer Technik, Datensicherung /-Wiederherstellung und Archivierung sowie an die Leitlinie Informationssicherheit formuliert. Ergänzt wurde das Kontinuitätsmanagement sowie die Priorisierung.

Förderprogramme, wie das KHZG, unterstreichen durch die zwingende Berücksichtigung der IT-Sicherheit in Digitalisierungsprojekten die Notwendigkeit der IT-Sicherheit in medizinischen Einrichtungen. Langfristige Sicherheitskonzepte sollten auch über den Förderzeitraum hinaus betrachtet werden, wobei dem Betrieb wie auch der Compliance ein besonderes Augenmerk zu schenken ist.

Zusätzlich zu diesen langfristig umzusetzenden Maßnahmen auf Grund gesetzlicher Vorgaben verschärft sich zunehmend die Bedrohungslage im Cyber-Raum. Neben einem ausgeklügelten Geschäftsmodell mit Milliardenpotential eignen sich Cyber-Angriffe auch, um politische Ziele durchzusetzen.

Die Cyberangriffe nutzen gezielt Schwachstellen, z.B. in eingesetzter Software von Krankenhäusern, aus. Die Größe und Art der medizinischen Einrichtung ist für die Wahrscheinlichkeit eines Angriffs völlig irrelevant. Gerade kleinere und mittlere Einrichtungen geraten derzeit in den Fokus der Cyber-Kriminellen. Die Meinung, dass es Andere aber mich nicht trifft, ist eine fatale Fehleinschätzung! Wirtschaftliche Schäden und im schlimmsten Falle Gefahr für Gesundheit und Leben sind mögliche Folgen eines Cyber-Angriffes.

Daher unsere dringende Empfehlung an jeden IT-/ Sicherheitsbeauftragen einer medizinischen Einrichtung:
Stellen Sie sich die umseitigen 7 Fragen zum Schutz Ihres Unternehmens!

Beugen Sie jetzt vor – stellen Sie sich die folgenden 7 Fragen

1. Würden Sie eine Kompromittierung Ihrer **privilegierten Admin-Accounts** frühzeitig bemerken und adäquat verhindern können?

2. Sind Ihre **VPN Zugänge des Unternehmens** durch eine starke Authentifizierung und Autorisierung geschützt? Wie prüfen Sie, ob die Einwahl nur von **vertrauenswürdigen Geräten und Nutzern** geschieht?

3. Wie erkennen und analysieren Sie die **externen- und interne Schwachstellen** Ihrer IT-Infrastruktur und die daraus resultierende Gefahr von potenziellen Bedrohungen kontinuierlich?

4. Senken Sie Ihr Risiko bereits durch einen **DNS-Schutzschirm zum Internet**, um Aufrufe von maliziösen Webseiten bereits vor Zustandekommen der Verbindung zu unterbinden?

5. Wurde für Ihr internes **Netzwerk eine Anomalien-Erkennung** eingerichtet?
Stichwort: Das Netzwerk sieht alles.

6. Haben Sie Ihr **Notfall- und Wiederherstellungskonzept erprobt**? Stehen für den Eintritt eines IT-Sicherheits-vorfalls **Incident & Response Spezialisten** zur Verfügung?

7. Ist Ihr **Backup-System selbst gegen Kompromittierung geschützt** und wird es mit einer festen Routine aktualisiert? Wie prüfen Sie, ob sich das Backup **bei Bedarf problemlos einspielen** lässt?

Sie haben eine oder mehrere Punkte (noch) nicht umgesetzt? Sprechen Sie uns an!

Zahlreiche Gespräche mit betroffenen Unternehmen zeigen uns, dass diese monatelang und in Einzelfällen sogar jahrelang mit den Auswirkungen eines Ransomeware-/DDOS-Angriffs zu tun haben. Wir sind überzeugt: mit der richtigen Sicherheitsstrategie kann sich jeder schützen. Gemeinsam mit Ihnen finden wir die für Ihre Fragestellung und Ihre Geschäftsumgebung passende Cyber-Security-Lösung. Sprechen sie uns an.

Kontakt

Gehen Sie einfach auf Ihren bekannten Cisco-Ansprechpartner zu, oder nehmen Sie mit uns Kontakt auf via Email an:
it.sicherheit@cisco.com

Cisco-Secure-Portfolio

Cisco bietet als Marktführer von Cybersecurity-Lösungen ein durchgängiges Portfolio für Ihre Security-Resilienz an. Das Cisco-Secure-Portfolio erstreckt sich von der Netzwerksicherheit über Anwendungen, Server, Benutzer, Endpunkte bis in die Cloud. Die Extended Detection- and-Response Plattform (XDR) SecureX hilft Ihnen, Meldungen von Cisco Sicherheits-produkten sowie Drittanbieterlösungen auf einen Blick angezeigt zu bekommen und Ihre Analysen zu vereinfachen und zu beschleunigen.

Weitere Informationen unter: https://www.cisco.com/site/de/de/products/security/index.html