Cyber Risiko Self-Check

Welche dringenden Handlungsfelder JETZT unbedingt aufgrund der stetig steigenden Bedrohungslage bewertet werden sollten.

Digitale Transformation und veränderte Anforderungen an Wirtschaftsunternehmen und Behörden beeinflussen die Sicherheitslage erheblich. Die Bedrohungslage im Cyber-Raum war noch nie so hoch wie jetzt. Eine valide Sicherheitsstrategie ist daher nicht mehr „nice to have", sondern essentiell. Die letzten Jahre haben es deutlich gezeigt: Hacken ist ein ausgeklügeltes Geschäftsmodell mit Milliardenpotential, und längst nicht mehr ein Freizeitsport von IT-Nerds.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) stuft Ransomware-/DDOS-Angriffe in der Wirtschaft derzeit auf Platz 2 der Top 3 IT-Bedrohungen ein. 2022 markiert dabei mit fast 15 Millionen Meldungen zu Schadinfektionen, und dem ersten digitalen Katastrophenfall in Deutschland, einen vorläufigen und traurigen Rekord. Die Cyberangriffe nutzen gezielt Schwachstellen in der eingesetzten Software von Unternehmen und Behörden aus. Immer beliebter wird dabei die Verschlüsselung unternehmenskritischer/infrastruktureller Daten, zum Zwecke der Erpressung erheblicher finanzieller Mittel. Die Größe und Art von Unternehmen und Behörden ist für die Wahrscheinlichkeit eines Angriffs völlig irrelevant. Gerade kleinere und mittlere Unternehmen geraten derzeit in den Fokus von Cyber-Kriminiellen, da oft noch die Meinung vorherrscht: wenn, dann trifft es Andere, aber mich nicht! Eine fatale Fehleinschätzung, die im schlimmsten Fall sogar das unternehmerische Aus bedeuten kann.

Daher unsere dringende Empfehlung an jeden IT-/Sicherheitsbeauftragten:
Stellen Sie sich die umseitigen 7 Fragen zum Schutz ihres Unternehmens!

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

1. Sind **privilegierte Admin-Accounts** vor unberechtigtem Missbrauch durch eine starke Authentifizierung und Autorisierung (Multi-Faktor Authentification inkl. Context Awareness und Posture Check) geschützt?

2. Sind alle **VPN Zugänge** in das Netzwerk durch eine starke Authentifizierung und Autorisierung geschützt?

3. Sind **potentielle externe und interne Schwachstellen** der IT-Infrastruktur analysierbar, bekannt und wurde die Gefahr einer Bedrohungslage eingeschätzt und dokumentiert?

4. Wurde ein **DNS-Schutzschirm** zum Internet etabliert, um auffällige und fragwürdige Kommunikation vom oder zum Internet frühzeitig zu erkennen und zu blocken?

5. Wurde für das eigene, interne Netzwerk eine **Netzwerk-Anomalien-Erkennung** etabliert? Stichwort: Das Netzwerk sieht alles.

6. Ist ein Notfall- und Wiederherstellungskonzept etabliert und ist für den Eintritt eines Vorfalls die Verfügbarkeit von **Incident & Response Spezialisten** im Sinne eines Notarztes vorhanden, den ich jederzeit anrufen kann?

7. Ist das **Backup-System** selbst gegen Angriffe ausreichend geschützt und wird es mit einer festen Routine aktualisiert?

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