Cybersecurity Notfallplan

CAIRO

secure • digital • IT-infrastructures

Cybersecurity Notfallplan

Erfolgreiche Cyber-Attacken sind in aller Munde und das Geschäft mit Cyber-Versicherungen blüht. Je nach Art der Attacke (Malware, Phishing, Ransomware) ist der eintretende Schaden erheblich bis zu existenzgefährdend. Bisher haben viele Firmen das Thema „Sicherheit“ bzw. „Systemausfall“ aus der klassischen Perspektive betrachtet und Vorkehrungen bzw. Wiederanlaufpläne im Sinne Business Continuity, Disaster Recovery, Redundanzen, Ersatzteile geschaffen. Dies reicht heutzutage nicht mehr aus!

Vielmehr ist ein Cybersecurity Notfallplan - auch nach NIS2 oder Anforderungskatalogen von Versicherern - erforderlich, der von der Vermeidung bis zur Schadenseindämmung alle Maßnahmen in Form von verbindlichen Prozessen beschreibt. Eine erfolgreiche Attacke ist immer eine große Sondersituation für alle Beteiligten und nur ein solider Plan garantiert, dass keine weiteren Schäden passieren und die Cyber-Versicherung nicht für den Schaden eintritt.

Inhalte eines Cybersecurity Notfallplans

Für die Inhalte eines Notfallplans gibt es keine detaillierten, normativen oder formalen Vorgaben. Essentiell sind wichtige Verhaltensweisen, Melde- und Entscheider-Wege, Kontaktinformationen, Verantwortlichkeiten, Sofort-Maßnahmen zur Schadenseindämmung oder forensische Analysen.

Rollen wie der Informationssicherheitsbeauftragter (ISB) oder Datenschutzmanager (DSM) müssen klar beschrieben und einzelnen Personen zugewiesen werden. Sie sind zusammen mit dem IT-Leiter und der Geschäftsführung die Hauptverantwortlichen und wichtige Personen auf der Meldekette bevor ein Security Dienstleister, ein IRS, das BSI oder die Polizei informiert wird.

Alle kritischen Systeme müssen im Detail beschrieben werden bzgl. Benutzer, Benutzerberechtigung, MFA, Change und AuditLogs, Backup Zyklen, Schutzklassen-Kategorien, System-spezifische Notfallmaßnahmen und vieles mehr! Ein reiner „Netzwerk oder Endgerät“ zentrierter Notfallplan ist nicht ausreichend. DSGVO relevante Informationen gehören mit in diesen Plan, da ein Angriff oft eine meldepflichtige Datenschutzverletzung in Folge auslöst.

Die Notfallpläne gehören in eine separate Ablage in die Cloud und nicht auf die bestehende On-Prem Landschaft, da diese bereits verschlüsselt sein könnte.

CAIRO als IT Compliance & Security Beratungsfirma hat ihre langjährige Erfahrung in einen fertigen Plan und Poster einfliessen lassen, der nach einer kurzen individuellen Anpassung sofort verwendet werden kann. Sprechen Sie uns an…

Anforderungen einer Cyber-Versicherung

In den Fragebögen und Checklisten zur Preiskalkulation findet man die üblichen statistischen Fragen zu Branche, Firmengröße, Territorien aber genauso viele Fragen zu den vorhandenen Schutzmaßnahmen wie MFA oder der Existenz von Notfallplänen oder Mitarbeiter-Security-Schulungen. Diese Kriterien sind ein vitales (Subset) der Anforderungen nach „State of the Art" für IT-Sicherheit. Besser wäre ein umfangreiches ISMS (Information Security Management System)– aufgebaut nach Normen wie ISO 27000 oder VdS 10000 – inkl. Risikoanalyse aller Systeme. Minimum ist ein Notfallplan der zumindest diese Normen und wichtige praktische Dinge wie „Kritische Systeme" und „Verantwortlichkeiten" wie ISB oder DSM festlegt und assoziiert.

Informationen für Mitarbeiter

IT-Mitarbeiter und Benutzer (alle Mitarbeiter) sollten per Aushang/Poster Informationen erhalten, wie man sich im Fall einer Attacke zu verhalten hat. Eine Papierversion ist unabdingbar, da ja ev. das digitale System nicht mehr zur Verfügung steht. Hier gelten die gleichen Vorkehrungen wie bei medizinischen Notfällen mit z.B. Ersthelfer-Informationen.

Der Benutzer ist typischerweise der erste Angegriffene und darf z.B. nicht durch Panik-Notausschaltung gewisse Spuren verwischen, die für eine forensische Untersuchung unabdingbar sind. Auch diese Informationen sind Teil der Pläne und der Poster.

Der CAIRO Cybersecurity Notfallplan ist Teil unseres Security & Compliance Portfolios von normgerechten Security-Prüfungen, über das Schwachstellen-Management bis zum sicheren IT-Betrieb mit modernen Lösungen oder CAIRO Security Managed Services.

CAIRO ist VdS 10000 zertifiziert für ein Informationssicherheits-Management System (ISMS).

CAIRO
secure · digital · IT-infrastructures

Tel.: +49 (0)621 86 75 10 Mail: info@cairo.ag Web: www.cairo.ag