UIMCommunic@tion
praxisnah.gut.informiert.

10/2023

Ausgabe für Deutschland

Cyberattacke – Was tun? – Lohnt ein Versicherungsschutz?

Das richtige Verhalten beim Cyberangriff

Wie bei einer Gebäudeschutzversicherung gibt es auch Angebote für Versicherungsschutz gegen finanzielle Schäden aus einem Cyberangriff. Oftmals wird neben der finanziellen Deckung des Schadens auch der Rechtsbeistand abgedeckt. „Vor dem Abschluss einer Cyberversicherung ist eine ausführliche Betrachtung von eigenen Sicherheitswünschen und dem Versicherungsangebot erforderlich. Auch das Kleingedruckte sollte aufmerksam gelesen werden. Der Grundsatz ‚Gründlichkeit vor Schnelligkeit' gilt auch hier", erklärt Dr. Jörn Voßbein. Und was ist zu tun, wenn das eigene Unternehmen einem Cyberangriff ausgesetzt ist? Die UIMC geht in einer fünfteiligen Reihe auf verschiedene Themen der Informationssicherheit ein [siehe www.uimc.de/news].

Ob eine Cyberversicherung sinnvoll ist oder nicht, muss in einem Abwägungsprozess festgestellt werden, dem eine Kosten-Nutzen-Analyse zugrunde liegt. Dabei ist von entscheidender Bedeutung, wie hoch das eigene Risiko, Opfer einer Cyberattacke zu werden, eingeschätzt wird. Einige Faktoren für den Abschluss einer Versicherung sind Wahrscheinlichkeit des Schadenseintritts, Geschäftsfeld/Gewerbe (Abhängigkeit von der IT), Höhe des zu erwartenden Schadens oder Unternehmensgröße.

Auch die Art der Absicherung muss gewählt werden, da hier gravierende Unterschiede in den Versicherungsbeiträgen bestehen. Beispiele für Versicherungsarten sind: Garantien gegen Betriebsausfälle, Identitätsdiebstahl oder die vollständige Wiederherstellung des Informationssystems nach einem Cyber-Angriff. In jedem Fall sollten die Risiken, die für den Fortbestand eines Unternehmens elementar sind, tatsächlich abgesichert werden. „Eine Versicherung ist sicher einer der letzten Schritte bei der IT-Sicherheit des eigenen Unternehmens. Zunächst sollte gut und wirkungsvoll investiert werden, denn die Versicherungsunternehmen verlangen bereits einen Katalog an Mindestanforderungen. Dazu gehören unter anderem ein Backup, das gut gegen Manipulation abgesichert ist, Patch-Management zur raschen Schließung von Sicherheitslücken, Firewalls, E-Mail-Security, Schutz privilegierter Konten und Multi-Faktor-Authentifizierung", berichtet Dr. Voßbein.

Wichtiger ist noch die Frage: Was aber ist zu tun, wenn das eigene Unternehmen Opfer einer Cyber-Attacke ist? Hierzu sind Meldewege zu definieren, alle betroffenen Personen zu informieren und Kontaktdaten auch offline bzw. analog verfügbar zu halten, schließlich kann eine digitale Kontaktliste ebenfalls vom Cyber-Angriff betroffen sein. „Was trivial klingt, wird oftmals versäumt", so Dr. Voßbein und verweist darauf, dass bei Attacken insbesondere schnelles Handeln elementar ist.

Bei einem IT-Sicherheitsvorfall sollten die Geräte und das IT-System des Unternehmens vom Internet getrennt werden. Folge: Der Angreifende wird daran gehindert, seinen Angriff zu steuern. Eine mögliche Datenexfiltration wird verhindert. Vom Angriff betroffene Geräte und Computer sollten nach Möglichkeit nicht abgeschaltet werden, um die Arbeit von Ermittlern nicht zu behindern. Für das Unternehmen ist es in einem solchen Angriffsfall von hoher Bedeutung, ob zu normalen Zeiten regelmäßig passgenaue Backups erstellt wurden. Wenn dies so ist, kann der Geschäftsbetrieb zeitnah wieder anlaufen. „Lösegeld sollte auch nicht voreilig gezahlt werden, schließlich weiß man nie, ob die Systeme wieder ‚freigegeben' werden und man nicht beim nächsten Mal gezielt angegriffen wird."

Freikarten: DIGITAL FUTUREcongress, Bochum, 08.11.2023

Am 8. November 2023 findet der Kongress rund um IT-Sicherheit, Digitale Transformation, Strategien, und Datenmanagement in Bochum statt. Die UIMC ist mit Ihrem Vortrag „Compliance in KMU pragmatisch umsetzen" und gemeinsam mit dem networkern.NRW mit einem Stand vertreten. **Wir haben Freikarten.** Melden Sie sich einfach unter communication@uimc.de.

UIMC Dr. Vossbein GmbH & Co KG, Otto-Hausmann-Ring 113, 42115 Wuppertal
Tel.: +49-202-946 7726 200, Fax: - 19, E-Mail: consultants@uimc.de, Internet: www.UIMC.de

UIMCert kündigt Zusammenarbeit mit der DAkkS auf

Ganz nach dem Motto „Tue Gutes und rede darüber" ist eine Zertifizierung eine Bestätigung durch eine „dritte Stelle", dass Anforderungen von Normen erfüllt werden. Die Zertifizierung basiert auf einer Konformitätsbewertung, in der die Erfüllung der Anforderungen geprüft wird. Die UIMCert ist eine führende Stelle, die Zertifizierungen gemäß dem internationalen Informationssicherheits-Standard ISO 27001 vornimmt, und war ***eines der beiden ersten Unternehmen in Deutschland****, das für die Zertifizierung von ISMS gem. ISO 27001 (damals noch die britische Norm BS 7799) von der TGA (Vorläufer der DAkkS) akkreditiert wurde. Sie hat nun das Angebot der akkreditierten Zertifizierung eingestellt.*

Die UIMCert wurde im Jahre 2001 akkreditiert und blickt damit auf eine 20-jährige erfolgreiche Arbeit bei der Erteilung von hochwertigen Zertifikaten für Informationssicherheits-Managementsysteme zurück. In dieser Zeit hat sie in diversen Branchen ihre Kunden dahingehend überprüft, ob sie den zu der jeweiligen Zeit aktuellen Anforderungen an ein Informationssicherheits-Managementsystem (ISMS) genügten und bei positivem Ergebnis ein entsprechendes Zertifikat ausgestellt.

Die immer stärker werdenden formalen Anforderungen der Akkreditierungsstelle mit teilweise sehr fragwürdigen Interpretationen der Akkreditierungsnorm haben nun dazu geführt, dass die Aufrechterhaltung des Angebotes akkreditierter Zertifizierung wirtschaftlich nicht mehr vertretbar ist. So wurden Kompetenzen der Auditoren über viele Jahre akzeptiert, doch plötzlich – trotz hoher Expertise und Erfahrung – ohne vorherige Ankündigung nicht mehr zugelassen. Damit kann das in Deutschland einzigartige Modell der Zertifizierung mit ausschließlich langjährig bewährten, überwiegend fest angestellten Auditoren, das insb. auch aus Sicht der Kunden zu einer fachlich besonders hochwertigen Auditierung geführt hat, nicht mehr weiter betrieben werden.

„Wir bedauern diese Entwicklung, die aus unserer Sicht zu einer Reduzierung der Qualität der Zertifizierungsdienstleistung und zu einem geringeren Wettbewerb führt, sehen aber keine Möglichkeit, die bisherige Vorgehensweise weiter aufrechtzuerhalten," bedauert Rechtsanwältin und Geschäftsführerin der UIMCert GmbH, Arlette Schilde-Stenzel, diesen Schritt.

„Da wir glauben, dass qualitativ hochwertige Zertifizierungsdienstleistungen im Bereich des Informationssicherheits-Managements immer noch wichtig sind, **werden wir auch in Zukunft unsere Dienstleistung in Form von ‚nicht-akkreditierten' Zertifikaten anbieten** und unseren Kunden die Beibehaltung des gewohnt hohen Qualitätsstandards zusichern," so Dr. Jörn Voßbein, Gesellschafter und Auditor der 1. Stunde.

Spruch des Monats: November

Der Urspung dieser Redewendung ist unbekannt. Was sie uns sagen will, ich aber klar: Wenn etwas Unbekanntes im Dunklen liegt, neigen viele Menschen dazu, andere Personen vorgehen zu lassen. Das Ziel ist von den Fehlern und Erfahrungen der Anderen zu profitieren.

Was diese Redewendung übertragen auf den Datenschutz und die Informationssicherheit heißt und welches „**Goodie**" wir diesen Monat für Sie vorbereitet haben, finden Sie wie immer unter

www.uimc.de/kalendersprueche

Aktuelles im Online-Formular-Center

Um über Neuerungen zeitnah informiert zu werden, können Sie unser News-Forum abonnieren und erhalten daraufhin eine E-Mail, sofern Sie einen personalisierten Account haben.

www.uimcollege.de