Cyber-Risiken - nur ein paar Fragen bis zur Absicherung

„Insgesamt zeigte sich im aktuellen Berichtszeitraum eine angespannte bis kritische Lage. Die Bedrohung im Cyberraum ist damit so hoch wie nie zuvor. Wie schon in den vergangenen Jahren wurde eine hohe Bedrohung durch Cyberkriminalität beobachtet."

(Bundesamt für Sicherheit in der Informationstechnik, Die Lage der IT-Sicherheit in Deutschland 2023)

Angespannt bis kritische Lage! Bedrohung so hoch wie nie zuvor! Und dennoch: Trotz der mahnenden Worte des Bundesamts verfügen lediglich 27% der von Statista befragten Unternehmen (https://de.statista.com/statistik/daten/studie/1038935/umfrage/bestehen-einer-cyber-versicherung-in-unternehmen-in-deutschland/) über eine Cyber- Risk-Versicherung.

Trotz klar erkennbarer Schäden für betroffene Unternehmen:

Auswirkung	**in% der betroffenen Unternehmen**
Finanzieller Schaden, z.B. für Schadensbehebung, Lösegeld	(42%)
Minderung der Arbeitsproduktivität unserer Mitarbeiter:innen	(42%)
Dienste für unsere Mitarbeitenden ausgefallen	(38%)
Schaden für die Reputation unseres Unternehmens	(15%)
Produktion zeitweise ausgefallen	(13%)

https://www.tuev-verband.de/?tx_epxelo_file[id]=925194&cHash=11772152e3b993dd496a49e3e533076f

Auch Handwerksbetriebe sind immer mehr Ziel der Cyber-Angriffe, das Handwerksblatt berichtet in einem Online Themen Special ausführlich darüber (https://www.handwerksblatt.de/themen-specials/cyber-attacken-auf-handwerksbetriebe/wenn-datendiebe-zuschlagen).

Warum also eine Minderheit an abgesicherten Unternehmen - auch im Handwerk?

Am komplizierten Antragsprozess liegt es sicher nicht. Es sind in der Regel nicht viele Risikofragen, die für einen Antrag beantwortet werden müssen. Neben der Branche und dem Jahresumsatz spielen beispielsweise beim Assekuradeur der Helmsauer Gruppe folgende Risikofragen eine Rolle:

1. Bearbeiten, speichern oder übermitteln Sie weniger als 20.000 Kreditkartendaten pro Jahr?
2. Werden vom Hersteller bereitgestellte Updates (z.B. Sicherheitspatches) unverzüglich eingespielt?
3. Setzen Sie Malwareschutz (z.B. in Form eines Antivirenprogramms) ein und wird dieser automatisch auf dem aktuellen Stand gehalten?
4. Sind alle Zugänge zum Internet durch Firewalls gesichert?

5. Erfolgt eine mindestens wöchentliche Datensicherung auf separaten Systemen oder Datensicherungsmedien?
6. Besitzt jeder Mitarbeiter nur die für die eigene Tätigkeit notwendigen Berechtigungen und passwortgeschützten individuellen Zugänge?
7. Haben Sie alle vom Hersteller voreingestellten Passwörter auf allen Geräten in Ihrem Netzwerk (z.B. Telefonanlagen, Anrufbeantwortern, Drucker, Router, IoT-Geräte) geändert?
8. Erfolgt der Zugriff auf die interne IT-Infrastruktur über öffentliche oder drahtlose Netze ausschließlich verschlüsselt?
9. Es werden keine automatisierten Produktionssysteme (ICS) genutzt?

Kleiner Tipp am Rand

Sollten Sie eine der Fragen 2 bis 8 mit "**nein**" beantwortet haben, bietet sich ein unverzügliches Gespräch mit ihrem IT-Verantwortlichen an.

Was bleibt, ist dann noch die richtige Wahl der Versicherungssumme, der Selbstbeteiligung und die Auswahl der möglichen Zusatzbausteine wie etwa

- Cyber-Spionage
- Minderung des Reputationsschadens bei Spionage von Betriebs- und Geschäftsgeheimnissen
- Betriebsunterbrechung durch Cloudausfall
- Internet-Diebstahl

Also - nur wenige Fragen und Klärungspunkte bis zur optimalen Absicherung!

Zu guter Letzt

Schieben Sie eine dringend notwendige Absicherung nicht auf die lange Bank und glauben Sie nicht, Sie und Ihr Unternehmen sind zu klein, um Opfer eines Cyber-Angriffs zu werden. Heute setzt sich niemand mehr gezielt an den Rechner und geht das Branchenbuch auf der Suche nach einem neuen Opfer durch - Automatisierung und Frequenz sind längst auch in diesem Metier angekommen!
Gehen Sie also mit Ihrem Versicherungsmakler ins Gespräch, klären Sie Risikofragen und benötigte Versicherungssumme. Übrigens: Ausgewählte Versicherer ersetzen hier übrigens die Risikofragen durch einen kurzen Security Check, der gerade auch dem Unternehmen die aktuelle Aufstellung der eigenen IT widerspiegelt.
Gestalten Sie im Anschluss dann gemeinsam eine optimale Absicherung gegen Cyberschäden.

Jens Christian Ammermann