Cybererpressung – Vorfallreaktionsplan

Gemäss verschiedenen namhaften Sicherheits-Organisationen ist die Cybererpressung (Ransomware) die grösste Bedrohung im Jahr 2022. Nicht nur die Anzahl der Angriffe steigen, sondern auch die Angriffe werden immer ausgefeilter. Lösegeld wird nicht nur für die Entschlüsselung von Daten gefordert, auch mit der Veröffentlichung von vertraulichen Informationen wird gedroht. Die Bedrohung ist real und kann jedes Unternehmen treffen. Es sind nicht nur grosse internationale Firmen ein Ziel, sondern auch KMU, öffentliche Verwaltungen, NGO, etc.

Als Berater für KMU bin ich erstaunt, dass die Verantwortlichen, z.B. für den Brandschutz, präventive Massnahmen mit Notfallplan und sogar regelmässigen Übungen vorsehen. Im Vergleich dazu aber die Unternehmensführung die neue Cyber-Bedrohung zu wenig ernst nehmen.

Neben der Prävention ist ein Vorfallreaktionsplan (Incident-Response-Plan), ähnlich wie beim Brandschutz, essenziell. Man sollte sich vorgängig Gedanken über die wichtigsten Abläufe, d.h vor, während und nach einem Ransomware Angriff machen. Wie beim Brandschutz muss dieser Vorfallreaktionsplan auch durch das KMU regelmässig getestet werden. Dabei wird auch die Effektivität der eingesetzten IT-Security Tools überprüft.

Die Verantwortung für die präventiven Massnahmen und den wichtigen Vorfallreaktionsplan kann nicht delegiert werden, da IT-Sicherheit Chefsache ist!

Erfahrungsgemäss sind die Kosten für die Prävention, den Vorfallreaktionsplan und die Tests um ein Vielfaches tiefer als die Kosten eines Angriffsschadens.

Ich empfehle aus diesem Grund, gemeinsam mit der KMU-Führung das Erarbeiten für den Vorfallreaktionsplan zeitnah zu initiieren. Wie bereits angesprochen, IT-Sicherheit ist Chefsache, erfolgreich ist man nur mit der vollumfänglichen Unterstützung der KMU-Verantwortlichen (Stichwort - Management Commitment).

Meine 7 Punkte für das Erarbeiten eines Ransomware – Vorfallreaktionsplans

1. **Auftrag** zur Erarbeitung des Vorfallreaktionsplans **durch die KMU-Führung**
2. Aufnahme, Überprüfung und ggf. Anpassung der bestehenden **präventiven Massnahmen**
3. Identifikation der **Anspruchsgruppen** (Stakeholders) – relevanten Parteien
4. Wichtigsten Abläufe **vor** einem Angriff identifizieren und im Plan festhalten
5. Wichtigsten Abläufe **während** eines Angriffs identifizieren und im Plan festhalten
6. Wichtigsten Abläufe **nach** einem Angriff identifizieren und im Plan festhalten
7. Vorfallreaktionsplan regelmässig **überprüfen, testen und kontinuierlich verbessern**

(Charles Rüedi, **rüedi -business & ict consulting**, www.rueedi-consulting.ch)