Der „digitale“ Einbruch

Ausgangslage, Problemfelder, DSGVO und Lösung

Ausgangslage

Der „digitale“ Einbruch, also ein Cyber Sicherheitsvorfall, ist zwar nicht mehr eine neue Art eines Verbrechens aber eine stark steigende. Die Anzahl von Cyberattacken nimmt zu, seit der Corona Pandemie kam es zu einem sprunghaften Anstieg. Betroffen sind nicht nur die medial bekannten Großkonzerne oder öffentliche Institutionen, sondern auch KMUs und Selbstständige.

Zugang erlangt der Hacker oft über Phishing Mails und Installation von Trojanern (Schadsoftware). Sobald der Hacker den Zugang zum Computersystem und den Daten hergestellt hat, ergeben sich für diesen im Wesentlichen drei Möglichkeiten zu deren Nutzung:

1. Verschlüsselung der Daten und Erpressung von Lösegeld zum Erhalt des Entschlüsselungscodes
2. Erpressung des Cyberopfers z. B. durch Androhung der Veröffentlichung der Daten
3. Verkauf der gestohlenen Datensätze an andere Hacker im Darknet

Für das betroffene Cyberopfer bedeutet dies im Regelfall viel Arbeit, hohe Kosten, Stillstand im Betrieb / in der Ordination und die Möglichkeit bei Bekanntwerden des Datendiebstahls einen Reputationsschaden zu erleiden. Mit Letzterem spekulieren viele Hacker und erhoffen sich dadurch die rasche Zahlung von Lösegeldern, welche häufig in Form von digitalen Währungen (Bitcoins) erfolgen.

Problemfeld 1 – Sicherheit der eigenen IT

Investitionen in die eigene IT-Sicherheit sind das Gebot der Stunde. Ein Blick eines EDV-Profis in die vorhandene EDV-Infrastruktur bringt hier Klarheit. Besonders wichtig sind vor allem eine auf tagesaktuellen Stand gehaltene Virensoftware, eine gute Firewall und regelmäßige (wöchentlich/täglich) Datensicherungen. Vom Anwender unterschätzt jedoch umso wichtiger sind ebenfalls in regelmäßigem Abstand (jährlich/halbjährlich) durchgeführte Passwortänderungen. Einen Leitfaden hierfür und für sichere Passwörter geben entsprechende Passwortrichtlinien.

Problemfeld 2 – die eigene Sensibilisierung

Die eigene Sensibilisierung und jene der Mitarbeiter zum Thema Cybersicherheit zählt als eine der Schlüsselfaktoren zur erfolgreichen Abwehr von Cyberattacken.

Die kritische Betrachtung fremder oder verdächtiger E-Mails und die bereits angesprochene sichere Vergabe von unterschiedlichen Passwörtern und deren regelmäßiger Änderung helfen dabei bereits enorm. Cyber-Präventionsschulungen durch Experten mit einem Praxistest zeigen Schwachstellen in der IT-Sicherheit und im eigenen Verhalten auf.

DSGVO – Meldeverpflichtung an die Datenschutzbehörde (DSB)

Gemäß Artikel 33 der DSGVO besteht eine gesetzliche Meldeverpflichtung an die zuständige Datenschutzbehörde (DSB), wenn der Schutz personenbezogener Daten verletzt wurde. Eine Nichtmeldung, eine zu späte Meldung (Frist 72h) oder die Setzung falscher Maßnahmen können empfindliche Geldstrafen nach sich ziehen. Die vom Datenmissbrauch betroffenen Kunden/Patienten sind zudem über den Hackerangriff zu informieren. Eine professionelle Beratung und Durchführung der notwendigen Schritte durch Spezialisten ist anzuraten.

Versicherungslösung

Durch Einhaltung der bereits beschriebenen Maßnahmen reduziert sich das Risiko einer erfolgreichen Cyberattacke merklich. Auch ein Cyberversicherer setzt eine regelmäßige Datensicherung, aktuelle Virensoftware und Firewalls für den Versicherungsschutz voraus. Das verbleibende Restrisiko sollte im Rahmen einer Versicherungslösung abgesichert werden.

Der „analoge“ Einbruch in die Ordination ist in der Regel in jeder Ordinationsbündelversicherung gut abgedeckt. Cyberversicherungen zur Absicherung des „digitalen“ Einbruch sind modern, häufig in Polizzenordnern zu finden sind sie jedoch noch nicht.

Cyberversicherungen sind komplexe Produkte und sollten deshalb auch bei spezialisierten Anbietern abgeschlossen werden. Der Leistungsumfang ist höher und die im Schadenfall besonders wichtige Assistance, damit ist der Zugang zu speziellen IT- Forensikern gemeint, ist gesichert und inkludiert. Diese IT-Forensiker arbeiten im Schadenfall sofort mit den vom Klienten beauftragten lokalen EDV-Betreuer zusammen und bringen das notwendige Know-How mit, um die Cyberattacke zu stoppen und den Schaden für den versicherten Klienten möglichst gering zu halten.

Die jährliche Prämie von guten Cyberversicherungslösungen beginnt bereits bei ca. € 500,00 (abhängig vom Umsatz und gewählter Versicherungssumme). Das Kostenrisiko im Falle einer erfolgreichen Cyberattacke ist unverhältnismäßig höher, weshalb eine entsprechende Absicherung empfehlenswert ist. Für die Auswahl des Versicherungsunternehmens und des passenden Leistungsumfangs sollte die Wahl auf einen unabhängigen, und auf Cyberversicherungslösungen speziell geschulten, Berater fallen.

Marco Willinger

Akademischer Versicherungsmakler und Geschäftsführender Gesellschafter bei SWZ Versicherungsmakler GmbH
www.swzvers.at