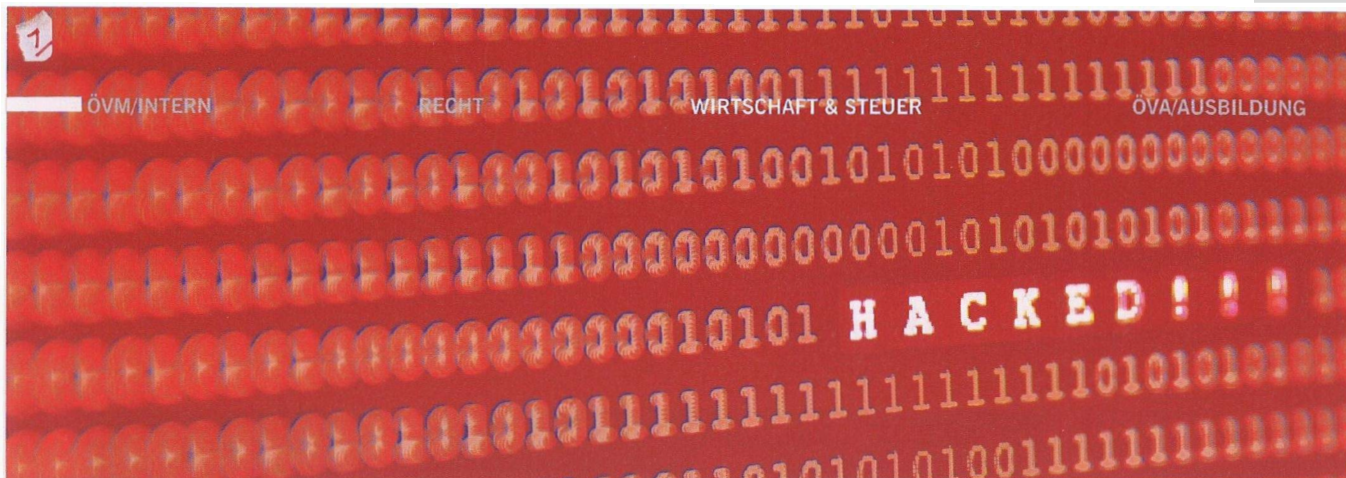




DI René FORSTHUBER

Leiter International
Development

RISK EXPERTS

Cyber Versicherung – 2.0

Im Jahr 2018 fragten wir in einem Artikel unter ähnlicher Unterschrift: „Immer noch ein Hype oder schon angekommen in der Versicherungslandschaft?“ Und damals antworteten wir bereits auf unsere eigene Frage: „Ja, Cyber Risiken sind definitiv in der Versicherungslandschaft angekommen.“

Zum heutigen Zeitpunkt müssten wir vielleicht fragen, warum aber sind sie noch immer nicht beim Versicherungsnehmer angekommen? Darauf haben wir einige Fragen und Antworten zusammengestellt.

Im Vertrieb von Cyber Versicherungen verirrt man sich mit potentiellen Kunden zwangsläufig in komplexen Themenbereichen wie Stand der Technik/Obliegenheiten, zählt die Versicherung überhaupt wenn es zum Crash kommt, welches ist das beste Produkt am Markt, welche Summe ist die richtige, wie soll ich einzelne Klauseln auslegen, bin ich gut genug, kann mir überhaupt was passieren, wann ist der richtige Moment für den Abschluss etc. Und obwohl wir uns diesen Fragen später zuwenden wollen, können wir bereits sagen, dass eine mögliche korrekte Summe zwischen 100.000 und 2.000.000 EUR zu beziffern sein könnte und somit das wichtigste abgedeckt werden kann – und das nahezu unabhängig vom Anbieter des Versicherungsproduktes.

1) WISSEN VERSICHERUNGSNEHMER WURUM'S GEHT? DIE VERSICHERUNG ALS FIRST LINE DEFENSE SUPPORT

Wie kommen wir darauf? In unseren eigenen Erfahrungen mit Schäden bzw. in diversen Statistiken zeigt sich, dass das Summen sind, die durchaus eine adäquate Incident Response bewerkstelligen können, also Krisenmanagement oder auch Betriebsfortführung nach einem Vorfall um schlim-

meres abzuwenden. Ob also die Haftpflichtklauseln „halten“ oder die Betriebsunterbrechungsversicherung auch den erlittenen Schaden deckt kann als sekundär betrachtet werden, da mit der Incident Response oftmals schlimmeres abgewendet werden kann. Somit also die „first line of defense“. Es zeigt sich auch: wird die Incident response adäquat durchgeführt können auch Schäden die dem Kunden und Dateninhaber zustoßen können abgewendet werden – somit hat man auch bereits einen Schutz gegen DSGVO-Schadenszahlungen – indirekt, da diese in Österreich nicht versicherbar sind. Übrigens ist das Auslagern von Daten kein wirklicher Schutz, die Verantwortung für deren Schutz bleibt bei Ihnen, somit auch die Tätigkeit des Benachrichtigten etc. Für den Versicherungsnehmer sind nun nur mehr wenige Faktoren wichtig:

- 100.000 oder doch 2.000.000 EUR? Das ist von meinem Schutzbedürfnis abhängig, außerdem von meiner Menge an sensiblen Daten, Komplexität meiner IT-Infrastruktur, der Wahl meiner IT Sicherheitspartner etc. Generell wird man als KMU mit geringeren Mengen eher das Auslangen finden.
- Passt die Incident response zu mir? Diese wird vom Versicherer unterstützend angeboten, unterschiedliche Unternehmen bieten 24/7 Dienstleistungen an, entsprechende Partner für Datenschutz, PR, IT Security uvm. Als Versicherungsnehmer muss ich prüfen, ob diese Partner mit meinen bereits bestehenden Partnern kompatibel sind. Hier lassen sämtliche Versicherer Gestaltungsspielraum zu um ein passendes Konzept für ihre Bedürfnisse maßzuschneidern. 24/7 ist natürlich ein Muss.

2) WARUM NICHT JETZT VERSICHERN? DAS WISSEN VOM RICHTIGEN ZEITPUNKT.

Hier eine kurze Übersicht, warum Sie als Ver-



sicherungsnehmer bereits sehr passende Zeitpunkte des Kaufs versäumt haben:

- 29.08.1997: Skynet wird selbstbewusst und gliedert menschliche Entscheidung aus strategischen Überlegungen aus (aus Terminator 2: Judgement Day) - > ca. zeitgleich (in einem anderen „Universum“): Entwicklung erster Internet Security Liability Policies – Beginn der Cyber Versicherung.
- 01.01.2000: Y2k Problem, möglicherweise kollabieren die Systeme (in dieser Zeit waren Werbekampagnen von Cyber Versicherern eher unauffällig).
- 21.12.2012: Weltuntergang nach dem Maya Kalender (wir wussten ja damals nicht ob ein virtueller Angriff dahinterstehen könnte)
- 25.05.2018: von manchen als „der kleine Weltuntergang“ bezeichnet (Einführung der DSGVO)
- 16.03.2020: Beginn des Corona Lockdowns in Österreich

Im Nachhinein betrachtet kann man nur schwer sagen, ob die Unterzeichnung eines Cyber Versicherungsvertrags zum damaligen Zeitpunkt richtig gewesen wäre, zumindest ist dies schwer mit den oben dargestellten Szenarien vereinbar. Ist aber jetzt der Moment richtig?

Eines ist klar: Telearbeit vergrößert Angriffspotentiale beträchtlich. Durch die Heimarbeit in vielen Unternehmen ergeben sich neue Risiken für diese Unternehmen, da nun VPN-Zugänge in kurzer Zeit zur Verfügung gestellt werden müssen, ohne sich um das Thema Sicherheit zu kümmern, oder Online-Meeting-Plattformen, die zuvor nicht erprobt oder getestet wurden. Zudem können interne Dienste möglicherweise unabsichtlich im Zuge von Umstellungen im Internet ohne entsprechenden Schutz veröffentlicht werden.

Im Zuge der Heimarbeit werden zudem auch möglicherweise Unternehmensdaten auf Firmenrechnern in privaten Netzwerken oder in einigen Fällen auch auf privaten Rechnern der Mitarbeiter verarbeitet. Dies stellt ein erhöhtes Risiko für die Unternehmensdaten dar, da Informationen in einer weniger kontrollierten Umgebung ein einfacheres Angriffsziel darstellen.

Aber hierzu gibt es Lösungen:

- Mit Remote-Arbeits-Sicherheitschecks für Unternehmen können Kernrisiken adressiert werden, indem nach schwachen

Konfigurationen von VPNs Ausschau gehalten wird und andere Formen der Remote-Arbeitsmöglichkeiten, wie RDP (Remote Desktop Protocol), Citrix, VNC, SSH, hinsichtlich deren sicherer Konfiguration bewertet werden.

- Selbst-Checks (z.B. als Script) helfen dabei, Heimarbeitsumgebungen zu analysieren und mögliche Angriffspotentiale herauszufinden.
- Wenden Sie sich an Ihren IT-Partner, Cyber Versicherer oder an uns für Ihre passende Lösung.

3) „UND ZAHLEN DIE DANN?“ AUF DER SUCHE NACH DEM PASSENDEN PRODUKT MIT DEM NÖTIGEN SUPPORT.

Viele Makler, die sich mit dem Thema bereits intensiv auseinandersetzen sind nicht zu beneiden, da manchmal die Frage im Raum steht: „Wer ist der beste Versicherer?“. Bei doch einigen nennenswerten Anbietern am Markt ist dies nicht leicht zu beantworten, in von uns durchgeführten USP Analysen bewerten wir folgende Punkte (hier nur grob erwähnt):

- Betriebsunterbrechnung (Ertragsausfälle & Leistungszeitraum)
- Haftpflicht (Prüfung, Abwehr, Deckung auch für immaterielle Schäden) Personenschäden, Vermögensschäden, Repräsentative;
- Sonstiges (Cyber Diebstahl, Datenschutzverletzungen, Cyber Erpressung oder Lösegeldforderungen, IT Hardware & Wiederherstellung von IT Systemen zeitliche Befristung)
- Versicherungsumfang (Rückwärtsversicherung, Geltungsbereich, Kumulierung, Outsourcing Dienstleister, Rückwirkungen, Summenspannweite etc.)
- Risikoausschlüsse/ Obliegenheiten
- Incident Response (Support, Krisenmanagement, Forensik, Rechtsberatung u. Support)
- Risikoselektion: Fragebogen, Cyber Scans, Unterstützung zur Prävention (siehe weiter unten)
- Kosten: (Prämie, Selbstbehalt, Versicherungssummen, Submits)

Und wie hoch muss die Sicherheit des Versicherungsnehmers sein? 100% Sicherheit gibt es nicht, aber in Gesprächen mit IT Verantwortlichen zeigt sich meist, dass insbesondere die User Fehler machen können, welche die IT Sicherheit gar nicht abfedern kann – Der Mensch also als schwächstes Glied der IT-Sicherheitskette.

ÖVM/INTERN

RECHT

WIRTSCHAFT & STEUER

ÖVA/AUSBILDUNG

Aber neben organisatorischen Angriffspotentialen gibt es auch technische: mit unseren Sicherheitschecks, die wirklich nur an der Oberfläche kratzen aber dennoch Angriffspotentiale offenlegen, konnten wir folgendes festhalten:

- Ca. 25% der Unternehmen haben (völlig) veraltete SSLv3 Verschlüsselungsalgorithmen, (verwendet von 1996 bis 2014; Ein Angriff namens „Poodle“ hat ihm den Todesstoß versetzt). Prüfen Sie ihr System, vielleicht sind Sie bei diesem Viertel dabei. Sollte ein Vorfall vor Gericht landen, ist hier aus unserer Sicht ein Verschulden des IT-Eigentümers nicht auszuschließen.
- Lediglich 10% haben DNSSEC oder DMARC (relativ unkompliziert zu implementierende Sicherheitsmechanismen zur Gewährleistung der Authentizität und Integrität der Daten): mit DNSSEC wird verhindert, dass eine Verbindung mittels gefälschter DNS-Antworten auf einen falschen Server umgeleitet wird.
- Über 50% der Webseiten Büros leiten nicht von unverschlüsselten Webseiten (http) auf verschlüsselte Webseiten (https) weiter. (Anfängerfehler... ?)
- Ca. 50% der Unternehmen offerieren mehr als die üblichen Dienste im Internet und bieten somit eine erhöhte Angriffsfläche (offene und ungenügend gesicherte Internetports – meist unbeabsichtigt).

Spätestens hier klingt die „Stand der Technik Obliegenheits-Glocke“. Wie unterstützt sie der Versicherer dahingehend?

- Fragebogen: nicht beliebt aber (noch) unvermeidbar. Der Fragebogen dient auch einem

offenen Dialog zwischen Versicherungsnehmer und Versicherer, sodass der Versicherer sich bewusst wird, was eventuell als Obliegenheitsverletzung auftauchen kann und somit den Versicherungsschutz kompromittieren kann. Andererseits entscheidet der Versicherer ob trotz Schwächen Versicherungsschutz angeboten wird.

- Sicherheitschecks: Risk Experts bietet rasche, unkomplizierte und ungefährliche Checks an, um die außenwirksamen Risiken auszuloten (siehe oben). Dazu kommen Vorschläge zur Risikoverbesserung was für Versicherungsnehmer meist sehr attraktive (da kostenlose) Möglichkeiten darstellt.
- Risikodialog: aber hat ein Versicherungsnehmer irgendwo (isoliert, galvanisch getrennt) ein System unter Windows 97 laufen, kann man da überhaupt versichern? Wie schauen ihre besonderen Bedürfnisse aus um die passenden Versicherungsmodule zu wählen? Wie sind Auswirkungen einzuschätzen um die passende Versicherungssumme zu wählen. Welche vorvertraglichen Informationen sind wesentlich/erheblich? In einem offenen Dialog können diese Punkte besprochen und für passende Versicherer in einem Risk Report aufbereitet werden.

Mit diesen Risikoselektionsmethoden steht einer kooperativen Zusammenarbeit nichts mehr im Wege, die sowohl vor einem möglichen Störfall (bin ich sicher), während (Incident response nimmt Sie an der Hand) und danach (Versicherungszahlungen) hilfreich zur Seite steht.