Cyber Risks: Ein Update Schweiz

Liebe argenius-Kunden

Im vergangenen Fachartikel «Cyber Risks: Neu die zweigrösste Gefahr für Unternehmen» haben wir die internationale Ebene, die «Spieler», die Schadenvolumina und die rechtliche Seite behandelt. In diesem Fachartikel – wenn man so will die Fortführung des vorangegangenen Artikels #3 – beleuchten wir die Situation in der Schweiz, aber auch die Reaktion der Assekuranz mit neuen Versicherungsprodukten, respektive deren Fallstricke. Zu guter Letzt erhalten Sie am Schluss dieses Fachartikels ein aktives Angebot zur Unterstützung. Ich wünsche Ihnen erneut eine spannende und hochinteressante Lektüre.

Urs Burger
CEO
argenius Risk Experts AG

Nicht nur international bekannte Schadenfälle sind zu vermerken, wir kennen solche Cyber Attacken genauso in der Schweiz. So wurde 2017 die Swisscom gehackt (800'000 Kundendaten) oder die Stadt Uster stand wegen der Malware «Gandcrab» für einige Tage wegen einer geöffneten, infizierten Blindbewerbung still, um nur zwei Beispiele als Einstieg zu nennen.

Die Schweiz hinkt hinterher

Gemäss dem Leiter Cyberrisks der Zürich Versicherungen (Stephan von Watzdorf) sind die Schweizer KMU's beliebte Angriffsziele. Wir sind noch verhältnismässig wenig sensibilisiert in der Aufrüstung von neuster Firewalltechnologie (Durchlässigkeit von Malware, speziell Ransomware) und gleichzeitig ein finanzstarkes Land, das Lösegeld bezahlen kann. Die Psychologie des Schweizers: «Wir sind neutral, wer will uns etwas antun?» mag da einen Einfluss haben. Wir vergessen, dass es sich bei den Angriffen auf die KMU's um organisiertes Verbrechen handelt und nicht um politische Handlungen.

Im Fokus stehen folgende Gefahren:

- Viren- oder Trojanersoftware (Malware) wie z.B. die international bekannt gewordenen «WannaCry» oder «Petya/Notpetya»
- Ransomware (Erpressungs-Schadprogramme) die die Unternehmenssysteme/Daten verschlüsseln und erst gegen die Bezahlung einer Lösegeldsumme wieder freigeben
- Denial-of-Service-Attacken, welche die Systeme durch eine gezielte Massenanfrage zum Stillstand bringen.

Eine grossangelegte Studie des Bundes (Unternehmensbefragung 2016) unter Einbezug von SVV/SQS/ISSS/ISB führte zur Gesamtnote «ungenügend».

36% der Schweizer KMU's waren schon Opfer von eingedrungener Malware (Schadprogramme). 4% waren Opfer von Lösegelderpressungen, was hochgerechnet also 23'000 KMU's schweizweit ausmacht! Rechnet man das durch mit CHF 10'000 Lösegeld pro Fall, erhalten wir eine Schadensumme von CHF 230'000'000.

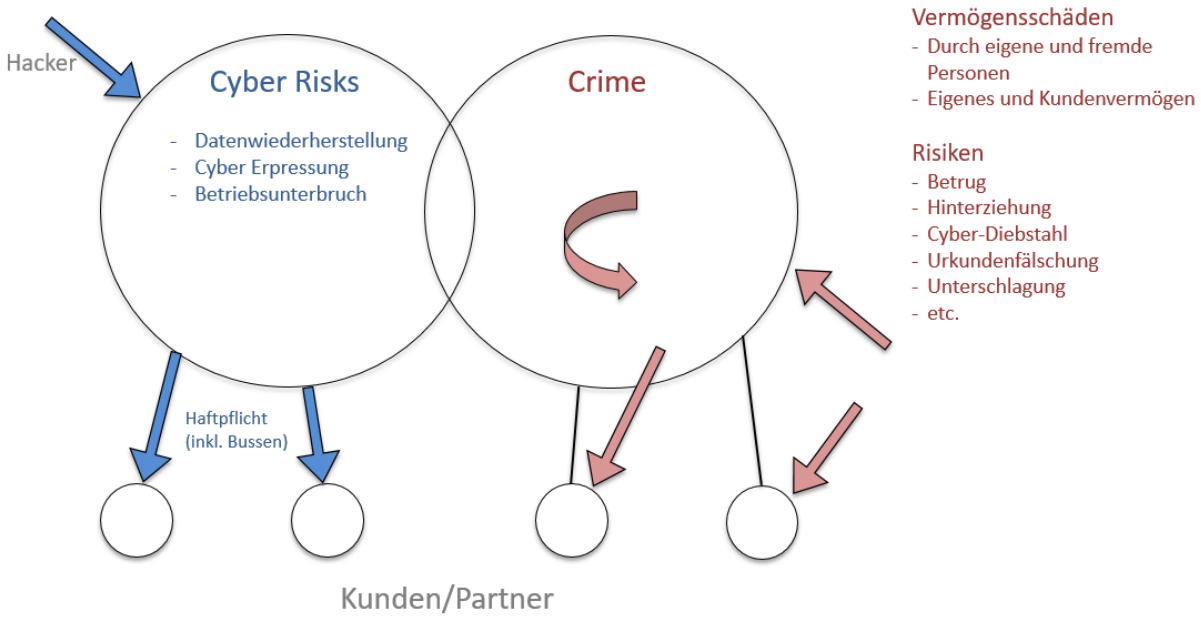
Die Studie analysierte auch die Schutzmassnahmen: Nur 60% sind mit vollständigen Grundschutzmassnahmen ausgerüstet (Firewall, Passwortänderungen, voller Backup); lediglich 20% leisten sich ein System zur Erkennung von Cyber-Vorfällen; lediglich 15% schulen ihre Mitarbeiter zum vorliegenden Thema (Sensibilisierung).

Ausserdem geben 52% der Befragten an, dass Sie einen Cyber-Vorfall aus Imagegründen nicht melden würden. Womit die obgenannten Angriffs-Zahlen also effektiv nochmals deutlich höher ausfallen dürften.

Zwei Versicherungs-Typen involviert

Die Assekuranz hat vor wenigen Jahren mit den Versicherungen «Cyber Risks» und «Crime/Vertrauensschaden» zwei neue Versicherungstypen auf den Markt gebracht, welche sich im Deckungsumfang leicht überschneiden und die sich ausserdem fast monatlich weiterentwickeln. Es braucht definitiv einen professionellen Berater in diesem neuen Segment, um weder Deckungslücken noch Doppelversicherungen und damit Prämienverluste in Kauf nehmen zu müssen. Denn richtig designed schützen die Versicherungen wirkungsvoll vor substanziellen Verlusten. Viele Broker sind hier allerdings noch nicht «sattelfest».

Im Wesentlichen können die beiden Versicherungs-Deckungen wie folgt beschrieben, bzw. unterschieden werden:



Als generelles Abgrenzungsmerkmal kann man sagen, dass es bei der Cyber Risk-Versicherung um Datenverluste/-veränderungen/-löschungen und den daraus resultierenden Kostenfolgen (inklusive Haftungsansprüche) geht. Wie bei einem Auto handelt es sich um eine kombinierte Deckung Haftpflicht-und «Kasko»-Schäden auf Daten samt Kosten.

Bei der Vertrauensschaden/Crime-Deckung stehen Geldflüsse, Geldverschiebungen und –verluste im Vordergrund. Verluste am eigenen oder Kundenvermögen, verursacht durch einen strafrechtlichen Tatbestand (siehe Bild oben). Sogenannte Cyber-Betrugsfälle (auch Social Engineering-Vorfälle genannt, wie u.a. Fake President, Payment Diversion Fraud oder Phishing-Fälle) fallen grundsätzlich also unter die Crime-Versicherung (Betrug/Geldabfluss), obwohl über das Cyber-Netz ausgelöst.

Hingegen sind die Kostenfolgen einer Cyber-Erpressung (Lösegeld-Forderungen/Unterbruch), d.h. wenn jemand droht, Daten zu verändern/löschen/verschlüsseln oder ein System durch Verschlüsselung oder DoS-Attacken etc. lahmzulegen, unter der Cyber-Deckung versichert (obwohl ein Crime-Vorfall).

Versteckte Deckungsunterschiede

Grundsätzlich sind die Deckungen ehrlich und umfassend. Allerdings gibt es verdeckte, relevante Unterschiede im Versicherungsschutz, die nur über ein genaues Studium des «Kleingedruckten» zum Vorschein kommen. Hier einige Beispiele, die zum Teil gedeckt, bei anderen Arbeiten nicht versichert werden:

- Fahrlässige Beschädigung von Daten bei direkter Bearbeitung am System eines Kunden durch eigene Mitarbeitende (Haftpflicht)
- Infizierung von Kundensystemen durch die Weiterleitung von ***privaten*** E-Mails
- Datenwiederaufbringung von Beschädigungen/Verlusten durch eigene Fehlmanipulation, aus Stromausfall oder aus Programmierfehlern (also ohne Hackereinwirkung)
- Deckung ***interner*** Krisenmanagementkosten
- Betriebsunterbruch von ***freiwilligem*** Abschalten der Systeme, um weiteren Schaden abzuwenden

Dies sind nur einige wenige Punkte, damit Sie sich die Details der Deckungsunterschiede vorstellen können. Mit einem Vergleich der Versicherungssumme und des Selbstbehalts ist es also definitiv nicht getan.

Kostenloser Versicherungsvergleich und Firewall-Technologie-Check

Zusammen mit unserer Partnerorganisation im Thema Cyber Risks, Nexus Schweiz AG, haben wir beschlossen, Ihnen zu diesem aktuellen Thema aktiv ein Angebot zu unterbreiten:

- Individuelle Ausschreibung an die fünf in diesem Segment führenden Versicherer, inkl. professionellem, mehrseitigem Offertvergleich (argenius Risk Experts)
- Basischeck der Firewall-Infrastruktur und die Erstellung einer Analyse (Benchmark) mit Angaben über die Gesamtsicherheit (Nexus Schweiz)

Es genügt, wenn Sie uns auf diesen Fachartikel einfach Ihr Interesse mitteilen. Gerne nehmen wir anschliessend mit Ihnen Kontakt auf.

Schlusswort

Cyber Risks und Crime ist eines der grössten Risiken der Gegenwart geworden. Es umfasst längst nicht nur Fremd-Angriffe und Betriebsunterbrüche, sondern genauso die Haftung für die Einhaltung von neuen Gesetzesnormen zum Umgang mit persönlichen Daten oder die Managementkosten im Krisenfall (Forensische Spezialisten, PR-Kosten, Identifikation von Schwachstellen oder Kommunikationsmanagement).

Viele Themen wie die Zweckentfremdung der Computersysteme, beispielsweise für Cryptojacking, haben wir in den vergangenen zwei Fachartikeln noch gar nicht behandelt. Ein Fachartikel soll aufmerksam machen und informieren. Eine Beratung kann er aber nicht ersetzten. Dafür braucht es professionellen Advice. Cyber Risks, aber auch das Thema Vertrauensschäden, werden dieses Jahr bei unseren Kunden schwergewichtig thematisiert.

Zögern Sie nicht, jederzeit auf uns zuzukommen, wenn wir Sie unterstützen können. Insbesondere das oben beschriebene Angebot ist eine gute Gelegenheit, sich ein zuverlässiges Bild der technologischen Infrastruktur zu machen und zu einer professionellen Beratung zu kommen. Wir freuen uns, Ihnen unser Know how weiter zu geben!

Juni 2019

Urs Burger
CEO