Cyber Risks: Neu die zweitgrösste Gefahr für Unternehmen

Liebe argenius-Kunden

Sind Cyber-Angriffe und Cyber-Crime real? Absolut ja! Wir haben uns in diesem Artikel der Analyse dieses Risikos und der Entwicklung der Gefahren gewidmet. Nebst beeindruckenden Zahlen und Schadenbeispielen zeigen wir die Risiko-Einschätzung von internationalen Managern auf. USA, China und Russland beschäftigen Tausende von IT-Spezialisten für die Entwicklung von Spysoftware. Ransomware ist zum internationalen Geschäft geworden, so sind bereits 20'000 Schweizer Unternehmen zu einer Lösegeldzahlung erpresst worden, um die verschlüsselten Unternehmensdaten und Programme wieder frei zu bekommen.

Die Assekuranz hat diesmal schnell reagiert und entsprechende Versicherungslösungen – zu durchaus zahlbaren Prämien – auf den Markt gebracht.

Urs Burger
Geschäftsführer
argenius Risk Experts AG

Beeindruckende Kennzahlen zur Sensibilisierung

9,32 Milliarden Malware-Angriffe (Schadsoftware) wurden 2017 weltweit verzeichnet (37% davon in Europa), was einer Steigerung von 18% gegenüber dem Vorjahr entspricht. Alleine Cyber-Crime (ohne Betriebsunterbrüche) verursachten weltweit Kosten im Umfang von 600 Milliarden US Dollar, was 0,8% des weltweiten BIP entspricht. Zum Vergleich: Die Kosten für Naturkatastrophen, wie beispielsweise Erdbeben, Hurricanes etc. betrugen in den letzten zehn Jahren im Durchschnitt 208 Milliarden US Dollar.

Die den Erdball überwälzende Malware «WannaCry» infizierte 200'000 Server in 150 Länder.

Sicher erinnern Sie sich an die fast täglich eingehenden Schadensmeldungen. Hier nur einige davon: Bei der US-Hotelkette Starwood werden 500 Millionen Gästedaten gestohlen, Yahoo muss 3 Milliarden gehackte User-Konten melden, Facebook ist vom Diebstahl von 50 Millionen Mitgliederinformationen betroffen, Maersk und FedEx melden durch WannaCry einen Betriebsunterbruch in der Höhe von je 300 Mio. US Dollar. Auch die Häfen in San Diego und Barcelona standen still (Schadensumme jeweils über 100 Mio. US Dollar). Generell scheint die Infrastruktur ein beliebtes Ziel zu sein, so standen 2017 u.a. auch viele englische Spitäler still. Politische Hintergründe?

The big Players: Blick hinter die Kulissen

Nur wenige wissen, dass nebst den USA (NSA/US Cyber Command) auch Russland (u.a. Abteilung APT28) und China (Einheit 61'398 – in enger Zusammenarbeit mit der Eliteuniversität Jiaotong) professionelle Spy Hacking Abteilungen betreiben.

Allgemein bekannt ist, dass die USA (zusammen mit Israel) mit dem implementierten Stuxnet-Virus die Rechner des iranischen Atomprogramms lahmlegte. Ebenfalls bekannt ist, dass die Amerikaner sich bei der deutschen Regierung für das Abhören von privaten Gespräche und Mails von höchsten Regierungsbeamten entschuldigen mussten. Weniger bekannt hingegen ist, dass China jährlich über 5 Millionen diplomierte Studenten in die Wirtschaft entlässt. Davon 1 Million IT-Spezialisten, von welchen wiederum 300'000 mit einem Parallel-Abschluss in englischer oder russischer Sprache. Von diesen Studenten kommen jährlich 10% in Staatsbetriebe und davon mehrere der Tausend Besten in die Spionageabwehr, wie zum Beispiel in die «Einheit 61'398». Jährlich wohlgemerkt. Kein Wunder, läuten in den USA die Alarmglocken: Ist doch kürzlich veröffentlicht worden, die Chinesen hätten nicht nur ein Jahr lang in den Servern von Coca Cola und vielen anderen Firmen jeden «Click» mitverfolgt, sondern sich auch über längere Zeit in den Rechnern von kritischen US-Infrastruktur-Staatsbetrieben aufgehalten.

Wer hat wohl vor Kurzem die riesigen Maschinenanlagen der Semiconductor Manufacturing Company Taiwan lahmgelegt (infizierte Steuerungen), welche ein Schlüssellieferant von Apple ist?

Um Russland nicht zu vergessen: APT28 war vermutlich 1 Jahr unbemerkt in den Systemen des deutschen Bundesministeriums der Verteidigung und hackte im Zusammenhang mit den Dopingskandalen während den Olympischen Spielen auch mehrere Schweizer Firmen, die mit Doping-Auswertungen beauftragt waren.

Das Netz generiert das neue organisierte Verbrechen

Malware (Schadsoftware) und Ransomware (Programme, die Unternehmenssysteme verschlüsseln und abschliessen) sind heute die neuen kriminellen Tätigkeitsgebiete. Die Lösegeldforderungen werden oft bezahlt, weil die geforderten Summen (US Dollar 5'000 bis 10'000) im Verhältnis zum längeren Stillstand einfach die viel günstigere Alternative ist.

Die Täterschaft ist international: Vor allem aus der Ukraine, Russland, Indien, Pakistan. Gut ausgebildete Leute ohne Job und mit viel Zeit. Die entwickelten Programme lassen einen Multiplikationseffekt zu und durch die Entschädigung in Kryptowährungen sind die Geldströme nicht zu ihnen rückverfolgbar.

Cyber Risks neu die Unternehmensgefahr Nr. 2

Während der «Regional Risk for doing Business Report» bei einer Umfrage bei 12'000 Unternehmen in 130 Ländern zum Schluss gelangt: «Cyber Angriffe sind neu das grösste Risiko», kommt das «Allianz Risikobarometer 2018» bei einer Umfrage bei 2'400 Risikoexperten (3 Nennungen möglich) zu einem ähnlichen Ergebnis:

Toprisiko:	Betriebsunterbruch (37% Nennungen weltweit / 58% in der Schweiz)
2.	Cybervorfall (37% Nennungen weltweit / 48% in der Schweiz)
3.	Naturkatastrophen (28% Nennungen weltweit / 29% in der Schweiz)
4.	Handelskriege/Zölle/Wirtschaftssanktionen (27% / 29%)
10.	Fachkräftemangel (9% Nennungen weltweit / 15% in der Schweiz)

Als wichtigste Schadenspositionen aus einem Cybervorfall wurden in der Reihenfolge der Nennungen folgende genannt: Betriebsunterbruch (supply chain interruption), Reputationsschaden, Haftpflichtansprüche, Datenwiederherstellung/Systemupdates, Bussen. Interessant ist die Position der Bussen (11% der Gesamtschadensumme), welche unmittelbar auch etwas mit den neuen Gesetzgebungen in den USA und im EU-Raum zu tun haben.

Rechtliche Veränderungen

Die sich seit dem 25. Mai 2018 in Kraft befindliche Europäische Datenschutzgrundverordnung (EU-DSGVO) oder auf Englisch General Data Protection Regulation (GDPR) ermöglicht den Behörden eine direkte Sanktionsmöglichkeit. Die Bussen für ungenügend geschützte persönliche Daten können bis zu 4% des Jahresumsatzes einer Unternehmung (max. Euro 20 Mio.) betragen.

Das heisst, Unternehmen müssen anvertraute Daten (Kreditkarten, Personaldaten, Krankheitsakten, Kontodaten, Lohndaten etc.) gegen Hackerangriffe und Veröffentlichungen konsequent schützen können. Im Falle eines Diebstahls ist eine sofortige Meldung fällig. Je nach Fahrlässigkeit und Kooperationsbereitschaft mit den Behörden fällt die Busse höher oder niedriger aus. Eine solche Gesetzgebung macht aber gleichzeitig auch ein neues Geschäftsfeld für Hacker/Erpressung auf. Damit ergeben nun die Angriffe auf Hotelketten, Handelsbetriebe, Gemeinden, Treuhänder, Anwaltskanzleien, Spitäler, Banken und Versicherungen zusätzlich Sinn.

Das neue Bundesgesetz über den Datenschutz in der Schweiz – mit einer Angleichung an das EU-Recht – ist durch die Vernehmlassung. Wir erwarten die Einführung frühestens per 01.01.2020. Ganz sicher wird das neue Gesetz aber kommen.

Schlussbemerkungen

Um das umfassenden Informationsmaterial für Sie in lesbare Portionen zu teilen, werden wir Ihnen den zweiten Teil dieses Artikels in einem Monat zustellen. In diesem kommenden Teil werden wir die Situation in der Schweiz beleuchten und auf die neuen Versicherungs-Deckungen «Cyber Risks» und «Vertrauensschaden/Crime» eingehen. Bei diesen Deckungen liegt der Teufel in den Details. So tönen einige Deckungen spannend, sind es aber nicht. Wichtig ist hier das Prüfen der wichtigsten Risikopositionen. Nur wenige Broker haben bis jetzt das nötige Knowhow in diesem Bereich. Mehr davon aber in einem Monat.

Ich hoffe es ist uns gelungen, Sie mit diesem ersten Teil für eines der neuen «Big-Risks» sensibilisiert zu haben. Wir freuen uns, Ihnen im in Kürze erscheinenden zweiten Teil auch Lösungen zu präsentieren. Bitte zögern Sie aber nicht, uns bei Fragen oder Bedarfsabklärungen bereits heute anzurufen.

April 2019

Urs Burger
Geschäftsführer
argenius Risk Experts AG

Telefon 044 266 10 70
Email: urs.burger@argenius-experts.ch