INSTITUT FÜR VERSICHERUNGSWIRTSCHAFT
AN DER JOHANNES-KEPLER-UNIVERSITÄT
LINZ/DONAU

Cyberrisken:

Die unterschätzte Bedrohung

Hackerangriffe fordern Unternehmen und die Versicherungswirtschaft

Pressegespräch mit

GD Mag. Othmar Nagl
Vorsitzender des Instituts für Versicherungswirtschaft

Ing. Andreas Klauser
CEO PALFINGER AG

Jürgen Weiss
Geschäftsführer ARES Cyber Intelligence GmbH

Bengt von Toll
Head of Cyber Europe and Latin America Munich Reinsurance Company

Dr. Stefan Korinek
Abteilungsleiter in der FMA, Versicherungs- und Pensionskassenaufsicht

Linz, am 26. April 2022

Die Corona-Lockdowns haben es gezeigt, die Digitalisierung ist wichtig, um auch in Ausnahmesituationen geschäfts- und handlungsfähig zu bleiben. Das hat aber nicht nur gute Seiten. Cyber-Attacken sind rasant angestiegen. Das Bundeskriminalamt verzeichnet von 2019 auf 2020 einen Anstieg von 26 Prozent von angezeigten Hackerangriffen. 2021 kamen weitere 28,6 Prozent dazu, in Zahlen bedeutet das 46.179 Anzeigen. Die Dunkelziffer dürfte aber weit höher liegen. Neben dem finanziellen Schaden verlieren Betriebe bei einem Cyber-Angriff nicht nur den Zugang zu ihren Unternehmensdaten, sie verspielen auch das Vertrauen ihrer Kunden. Und trotz der steigenden Bedrohung wird die Gefahr von vielen noch immer unterschätzt.

Das Institut für Versicherungswirtschaft an der JKU Linz widmet sich in seiner Frühjahrsveranstaltung dieser aktuellen Thematik, die für alle Unternehmen immer mehr zur existenziellen Herausforderung wird. Zu Wort kommen heute neben dem selbst erst jüngst von einer spektakulären Cyber-Attacke betroffenen CEO der Palfinger AG, Andreas Klauser, der Forensiker Jürgen Weiss, Geschäftsführer von Ares Cyber Intelligence sowie Bengt von Toll, Head of Cyber beim weltweit größten Rückversicherer, Munich Re und Stefan Korinek von der Versicherungsaufsicht.

„Der Cyberangriff kam für uns vollkommen unerwartet. Trotzdem hatten wir nach zwölf Tagen wieder vollen Zugriff auf alle unsere Systeme - diesen raschen Erfolg verdanken wir unserem Expertenteam, das mit externen Fachleuten intensiv an der Wiederherstellung arbeitete. Essenziell vor allem gegenüber unseren Kunden und Partnern war, dass wir zeitnah und offen über den Angriff und seine Folgen informiert haben. Leider tabuisieren viele betroffene Unternehmen das Thema und spielen damit den Cyberkriminellen in die Hände“, sagt Andreas Klauser, CEO PALFINGER AG. PALFINGER ist nur eines von vielen Unternehmen, die von solch einer Attacke betroffen waren.

Nach den aktuell veröffentlichten Daten aus der polizeilichen Kriminalstatistik stieg 2021 die Internetkriminalität in Österreich rasant. Rund 46.000 Anzeigen bedeuten einen Zuwachs von 28,6 Prozent im Vergleich zum Vorjahr. Durch die Pandemie bedingte Schließung von Geschäften verlagerte sich nicht nur die Kommunikation, sondern auch der Konsum immer mehr in die digitale Welt. Zudem warnen Experten derzeit vor einem Cyberkrieg Russlands gegen den Westen.

Im sogenannten Darknet, also dem versteckten Teil des Internets, bieten Kriminelle bereits Cybercrime als „Service“ an. Mit vorgefertigten Tools kann praktisch jeder Cyberattacken durchführen. Dieser besorgniserregende Trend beinhaltet eine „doppelte Erpressungstaktik“: Verschlüsselung von Systemen kombiniert mit Datendiebstahl.

Nicht nur Computer, Smartphones, Laptops und ähnliches stellen eine Gefahr dar. Hacker können auch über Geräte Zugang zu Unternehmensdaten erhalten, die nicht an das Internet angeschlossen sind, wie etwa über Brandmelder oder Überwachungskameras. War der Angriff erfolgreich, verlieren Unternehmen oft nicht nur ihre Daten, es stehen auch computergesteuerte Produktionen still.

IT-Spezialisten stoßen an ihre Grenzen

Solch ein Ransomware-Angriff (eine Wortkombination aus "Ransom", Lösegeld, und "Malware", schädliche Software) erfolgt meist vor dem Wochenende. „Freitag, ab 15 Uhr ist oft keiner mehr da, danach arbeiten die Täter ungestört“, erklärt Jürgen Weiss, Geschäftsführer von Ares Cyber Intelligence.

Dann muss schnell gehandelt werden. „Die Verbrecher geben keine Verschnaufpause. Man erhält meist sehr rasch einen Link, um in den Tor-Browser einzusteigen - links steht der geforderte Betrag, in der Mitte läuft der Countdown, rechts ist angegeben, ab wann sich der erpresste Betrag verdoppeln wird. Die Chatfunktion geht auf, und man kann mit den Tätern verhandeln“, so Weiss.

Ist das Management eines Unternehmens nicht vorbereitet, ist man in dieser Situation komplett überfordert. „Ist das Unternehmen bereit, Lösegeld zu zahlen? Wie viel kostet ein Tag Stillstand im Unternehmen? Was ist alles betroffen, ist es möglich, Daten zu retten?", laut Weiss muss gleichzeitig vieles bedacht werden. IT-Experten, die Unternehmen sich zum Installieren von PC´s holen, stoßen bei einer Cyberattacke an ihre Grenzen. Sie sind keine Forensiker, die in solch einem Fall dringend benötigt werden. Und diese haben die meisten Unternehmer nicht bei der Hand.

Die Höhe des Schadens hängt stark vom Unternehmen und den betroffenen Systemen ab. Weiss: „Mit bis zu 100.000 Euro muss man allein für die externen Kosten rechnen, selbst wenn die Daten dank guter Sicherung zu retten sind, kein Lösegeld gezahlt wird und keine Strafe der Datenschutzbehörde oder Kosten für Krisenkommunikation anfallen oder Vertragsstrafen für verspätet abgelieferte Aufträge.“

Chefsache Cyber-Security

Eine Studie der KPMG ergab, dass die meisten Unternehmen in Österreich noch keine ganzheitlichen Perspektive haben, um sich den Herausforderungen der Cyberkriminalität wirksam stellen zu können. Das Thema Cyber-Security muss endlich zur „Chefsache“ erklärt werden. Denn Fachleute sind sich einig: rund 80 Prozent der Schäden

könnten vermieden werden, würden die Unternehmen mehr in die IT-Sicherheit investieren. Drei von vier Unternehmen erfüllen derzeit die Anforderungen an die Cybersicherheit nicht. „Kennen Unternehmen wirklich die Bandbreite dieser Risiken? Ist ihnen klar, dass sie sich gegen Cyber-Risiken absichern können, vielleicht sogar absichern müssen? Und welche Rolle übernehmen dabei Cyberversicherer?“, wirft Bengt von Toll, Head of Cyber beim größten Rückversicherer, Munich Re, einige Fragen auf.

Es interessieren sich laut von Toll zwar immer mehr Unternehmen für Cyberversicherungen, in Verbindung mit technischen Präventionsmaßnahmen und dem begleitenden Service. Gleichzeitig weist er darauf hin, dass angesichts des drohenden Schadenpotentials „darüber hinaus die Versicherer die kritische Linie hinsichtlich der Versicherbarkeit insbesondere bei systemischen Risiken im Blick halten müssen“. Um Sicherheitslücken zu finden, müssen also zuerst mögliche Schwachstellen ausfindig gemacht werden, ähnlich wie bei einem Haus, das vor Einbrechern gesichert werden soll. Der erste Schritt hin zu einer sicheren Cyberabwehr ist also eine Bestandsaufnahme des aktuellen IT-Systems.

Cyber-Polizze ist die Feuerversicherung des 21. Jahrhunderts

Eine Cyber-Versicherung sorgt dank ihrer Assistanceleistungen und dem daran geknüpften Expertennetzwerk dafür, dass bereits im Vorfeld Sicherheitslücken erkannt werden und im Fall eines Angriffs rasch fachkundige Hilfe kommt. Eine gute Cyber-Versicherung kommt zudem für den Eigenschaden auf und haftet auch gegenüber Dritten, wie Kunden oder Lieferanten und übernimmt die Kosten für die datenschutzrechtlich verpflichtende Meldung des Data Breach gegenüber der Datenschutzbehörde.

„Die Cyber-Polizze wird die Feuerversicherung des 21. Jahrhunderts“, bringt Generaldirektor der Oberösterreichischen Versicherung, Othmar Nagl, Vorsitzender des Instituts für Versicherungswirtschaft, die Brisanz dieser Thematik auf den Punkt. „Sensibilisierung und Vorbeugung sind angesichts extrem ansteigender Schäden und immer kreativerer Methoden wichtiger denn je. Niemand ist vor solch einem Angriff sicher. Man kann den Schaden nicht verhindern und nicht ausgleichen, aber jedenfalls die finanziellen Folgen begrenzen. Neben der IT-Sicherheit wird auch die Absicherung gegen Folgeschäden immer wichtiger. Ein IT-Sicherheitspaket ist aus dem Versicherungsschutzschirm jedes Unternehmens nicht mehr wegzudenken“, so Nagl.

Stephan Korinek, Leiter der Abteilung behördliche Aufsicht über Versicherungsunternehmen und Pensionskassen: „Cyberrisiken betreffen einerseits die Versicherungsunternehmen selbst. Dabei ist sowohl die Unternehmens-IT als auch die Unternehmens-Governance gefordert, damit die Risiken ins Risikomanagementsystem einfließen. Das von der FMA entwickelte „Cyber Maturity Level Assessment Tool“ hilft dabei, die Cybersicherheit fundiert beurteilen zu können.

Gleichzeitig sichern Versicherungsunternehmen Cyberrisiken anderer Unternehmen ab. Bei diesen Cyberversicherungen ist für die FMA im Sinne eines effektiven Versichertenschutzes ein guter Produktentwicklungsprozess sowie ein ordnungsgemäßer Vertrieb besonders wichtig. Sollen auch Lösegeldforderungen versichert werden, so unterliegt das zusätzlich besonderen Anforderungen: So müssen Unternehmen ihren Versicherungsschutz geheim halten und externe Sicherheitsberater einsetzen. Im Fall eines Angriffs besteht für versicherte Unternehmen zudem eine Anzeigepflicht an die Polizei.“ Liegen Lösegeldforderungen vor, ist noch immer nicht gesagt, dass wir es hier mit einem „guten“ Erpresser zu tun haben. Es

gibt also keine Garantie, dass der Unternehmer dann tatsächlich seine Daten wieder erhält. Daher sieht die Finanzmarktaufsicht hier ein enormes Gefahrenpotential.

Das Institut für Versicherungswirtschaft

Das Institut für Versicherungswirtschaft an der Johannes Kepler Universität besteht seit 1982 und versteht sich als Schnittstelle zwischen universitärer Forschung und der Versicherungswirtschaft in der Praxis. Die Hauptaufgabe besteht zum einen in der Verbesserung und Versachlichung der Beziehung zwischen der Versicherungswirtschaft und ihrer Umwelt. Im Rahmen von Diskussionsveranstaltungen werden aktuelle Fragestellungen aus der Versicherungswirtschaft aus Sicht der Versicherungsnehmer auf der einen und der Unternehmen auf der anderen Seite erörtert und Lösungsansätze erarbeitet.

Als zweite wichtige Säule hat sich das Institut seit seiner Gründung vor nunmehr 40 Jahren die qualifizierte Aus- und Weiterbildung für Mitarbeiterinnen und Mitarbeiter aus der Versicherungswirtschaft zur Aufgabe gemacht. Ziel ist es, die Beratungsqualität gegenüber dem Kunden nachhaltig zu steigern. Als Beispiel sei hier der Universitätslehrgang für Versicherungswirtschaft angeführt.

Schließlich gilt es die unabhängige Forschung und Lehre auf dem Gebiet des Versicherungswesens zu fördern. Dabei arbeiten renommierte Linzer Professoren, wie etwa Rektor Univ.-Prof. Mag. Dr. Meinhard Lukas, o Univ.-Prof. Dr. Helmut Pernsteiner oder Univ.-Prof. Mag. Dr. Andreas Riedler im Vorstand des Institutes mit. Nähere Informationen unter ivw-jku.at/

Rückfragen an:

Dr. Roland Koppler | Generalsekretär des Instituts für Versicherungswirtschaft an der JKU | tel. 057891-81342 | mail. r.koppler@ooev.at