Cyber-Kriminalität & Cyber-Versicherungen

Die zunehmende Verlagerung des privaten und beruflichen Lebens in das Internet und die geänderten Lebensbedingungen durch die Corona-Pandemie hatten im Jahr 2020 in Österreich einen starken Anstieg der Internetkriminalität (Cyber-Crime) zur Folge. Im Gegensatz dazu sank die Aufklärungsquote. Auch weltweit steht Cyber-Crime an dritter Stelle der Unternehmensrisiken. Der zum Allianz-Konzern gehörende Industrieversicherer Allianz Global Corporate & Speciality (AGCS) hatte für die Erhebung 2.769 Experten aus 92 Ländern zu den wichtigsten Geschäftsrisiken befragt: Allianz-Risk-Barometer-2021.

Was ist unter Internet-Kriminalität zu verstehen?

Das Bundeskriminalamt Österreich versteht unter Cyber-Crime einen umfassenden Begriff, eine allgemein gültige Definition gibt es jedenfalls nicht. Üblicherweise fasst man darunter alle Straftaten, die unter Ausnutzung der Informations- und Kommunikationstechnik (IKT) oder gegen diese begangen werden. Im polizeilichen Bereich wird darüber hinaus zwischen Cyber-Crime im engeren und im weiteren Sinn unterschieden:

- **Cybercrime im *engeren Sinne*** umfasst Straftaten, bei denen Angriffe auf Daten oder Computersysteme unter Ausnutzung der IKT begangen werden. (zB Datenbeschädigung, Hacking, DDoS - Attacken).

- Unter **Cyber-Crime im *weiteren Sinne*** versteht man Straftaten, bei denen die IKT zur Planung, Vorbereitung und Ausführung für herkömmliche Kriminaldelikte eingesetzt wird, wie zB Betrugsdelikte. Diese Straftaten können praktisch jede Form von Kriminalität annehmen.

Status Quo in Österreich

Jährlich erstellt das Bundeskriminalamt einen Lagebericht zur Internet-Kriminalität. Im zuletzt veröffentlichten Cybercrime Report 2020 stieg die Gesamtzahl der angezeigten Fälle gegenüber 2019 um 26,3 % auf 35.915.

Der aktuelle Bericht des Rechnungshofes verweist auf die steigenden Kosten durch Cyber-Angriffe mit Auswirkungen auf die nötigen Personalressourcen zu deren Bekämpfung: Bericht Rechnungshof 2021.

Vor allem die Schließungen des stationären Handels (mit Ausnahme der Grundversorgung) hatten dem Cybercrime Report 2020 zufolge Auswirkungen auf den Internetbetrug. Außerdem würden mangelnde Sicherheitsvorkehrungen Cyberattacken auf Heim- und Arbeitsnetzwerke begünstigen. Der Report fordert deshalb eine ständige Weiterentwicklung des Kriminaldienstes, ein größeres Problembewusstsein und den Ausbau von Präventivmaßnahmen.

Für den Finanzbereich (Banken, Versicherungen, Pensionskassen, Glückspielkonzerne) hatte bereits 2018 die Finanzmarktaufsicht (FMA) auf das wachsende Bedrohungspotenzial aufmerksam gemacht und zur stärkeren Vernetzung (zB mit Institutionen für öffentliche Sicherheit oder mit der Wissenschaft) bei der Prävention aufgerufen. Die FMA veranstaltet zum Thema Fach-Symposien, nimmt an Planspielen teil oder gibt IT-Leitfäden für die ihr aufsichtsrechtlich unterliegenden Unternehmen heraus. In ihrer Publikation Fakten-Trends-Strategien 2021 beleuchtet sie die IT-Verflechtungen im Finanzmarkt und sich daraus ergebende regulatorische Erfordernisse.

Die wichtigsten Fälle 2020 in Österreich

Nach einer Neuregistrierung von mehreren tausend Domains kam es im Zusammenhang mit Covid-19 zu einer starken Zunahme betrügerischer Webseiten zwecks Phishing und Verbreitung von Schadsoftware. Weitere Fälle betrafen Erpressungs-E-Mails, die drohten, Familienmitglieder mit Covid-19 zu infizieren, Mails von vermeintlichen Paketzustelldiensten, die Schadsoftware installierten, oder Betrugshandlungen mit

Desinfektionsmitteln und Atemschutzmasken. Bei den Tätern gab es 2020 einen Trend hin zur Nutzung von Ransomware, RATs (*Trojaner*, die die vollständige Fernsteuerung eines Computers ermöglichen), E-Banking-Trojanern und anderen maßgeschneiderten Crime-as-a-Service-Leistungen.

Prävention

Vorbeugen ist besser als heilen. Hier finden Sie ausgewählte Anregungen zur Steigerung des Problembewusstseins und zur Selbstanalyse:

- Die WKO-Website IT-Sicherheit, Datensicherheit - WKO.at bietet einen Überblick über Themen zur IT-Sicherheit in Unternehmen.

- 10 grundlegende Sicherheitstipps für den richtigen Umgang mit Internet und Computer zur persönlichen IT-Sicherheit zeigt das Informationsblatt „Sicher im Netz“ auf: 10 Tipps wie Sie sich vor Gefahren schützen können.

- Das Informationsblatt 7 Tipps für Unternehmen und öffentliche Einrichtungen widmet sich unternehmensspezifischen Vorbeugungsmaßnahmen.

- Auf it-safe.at finden Sie hilfreiche Informationen für Unternehmen zu Präventionsmaßnahmen, Datenschutz, aktuelle Warnungen, Förderungsmöglichkeiten und Anbieter österreichischer Cloud-Lösungen mit Gütesiegel (Austrian Cloud).

- Die Website IKT-Sicherheitsportal onlinesicherheit.at des BMDW bietet einen Rundumblick zu IT-Sicherheits-Themen.

- Der Fragebogen „Cyber-Sicherheitscheck“ für Unternehmen steht auf der Website des Versicherungsverbandes (VVO) zur Verfügung. Dieser kann neben der Eigenanalyse auch zur Vorbereitung eines Gesprächs zum Abschluss einer Cyber-Versicherung genutzt werden.

- Der KSV 1870 und das Kuratorium Sicheres Österreich (KSÖ) bieten ein Rating für Unternehmen für Cyber-Sicherheit an: CyberRisk Rating by KSV1870, um digitale Risiken in globalen Lieferketten sichtbar zu machen.

- Veranstaltungen und Messen zum Thema Datenschutz und Cyber-Security können wichtige Inputs für die eigene unternehmerische Sicherheitstrategie liefern (zB Prisec 2021; IT-Messen weltweit).

Cyber-Versicherung als Beitrag zur IT-Sicherheit

Im Gegensatz zu klassischen Firmenversicherungen (wie zB Gebäudeversicherungen im Falle von Feuer, Sturm oder Überschwemmung) sind Cyberversicherungen als spezielle Sachversicherungen immer noch vergleichsweise neu für Wirtschaft und Wissenschaft.

Sehr komplex sind die Wechselwirkungen von Cyberangriffen auf globaler und lokaler Ebene. Voneinander unabhängige Firmen können zur gleichen Zeit vom selben Cyberschaden betroffen sein (global). Ein einziger Computer im Betrieb wiederum kann das ganze Unternehmen lahmlegen (lokal). Anbieter von Cyber-Versicherungen und ihre Kunden können von derselben Cyberattacke betroffen sein. Diese Komplexität führt dazu, dass sich der Angebotsmarkt und die vorhandenen Daten ständig an veränderte Situationen anpassen müssen. Daher sind nicht nur Risken auf ihre Versicherbarkeit, sondern bestehende Cyber-Versicherungen auch laufend auf ihre treffsichere Risikoabdeckung hin zu überprüfen.

Die Unabwägbarkeit zukünftig eintretender Schäden, die aktuelle europäische Geldpolitik und der Trend der Versicherungen zur Konsolidierung und zur vorvertraglichen Prüfung von vorhandenen präventiven Abwehrmechanismen der Gewerbekunden werden in den nächsten Jahren mit Sicherheit höhere Versicherungsprämien nach sich ziehen. Unternehmen sollten sich daher möglichst frühzeitig absichern.

In Österreich gibt derzeit etliche **Anbieter von Cyber-Versicherungen**, wie zB: AIG, Allianz, Axa, Berkley Europe, Chubb, CNA/Hardy, Donau, Ergo, Gothaer, HDI, Helvetia, Hiscox, Markel, Tokio Marine, Uniqa, VAV, Wiener Städtische, Zurich, AssProManagerline/Cogitanda/Howden.

Keiner der Anbieter deckt derzeit alle Bausteine in Zusammenhang mit Cyber-Crime ab. Aufgrund der unterschiedlichen Unternehmensgrößen und Risken gibt es außerdem (noch) keine standardisierten Versicherungsangebote (wie zB bei der Haushaltsversicherung) oder Preisgruppen. Der VVO hat 2018 auf seiner Website Allgemeine Bedingungen (Musterbedingungen) für die Cyberrisiko-Versicherung veröffentlicht. Die Bundessparte Information und Consulting (BSIC) in der WKÖ beleuchtet mögliche Bestandteile einer Cyber-Versicherung und beachtenswerte Punkte für den Vertragsschluss: it-safe.

Sprechen Sie Ihren Versicherungsvermittler bei Fragen oder einem Versicherungsbedarf an!
Alle gewerblich registrierten Versicherungsagenten finden Sie hier:
Versicherungsagenten in Österreich

Ich bin Opfer von Cyber-Kriminalität geworden

Wenn Sie (gewerblich oder privat) einen Verdacht auf Internetkriminalität haben oder Hilfe und Informationen benötigen, wenden Sie sich per Email an against-cybercrime@bmi.gv.at, wo Experten des 2012 geschaffenen Cybercrime-Competence-Centers C^4 Auskünfte erteilen. Wurden Sie selbst durch eine Straftat geschädigt oder haben Sie Hinweise auf einen Täter, kann eine **Anzeige bei jeder Polizeidienststelle in Österreich** erstattet werden.

Unternehmen, die Opfer eines Cyber-Angriffes wurden,
erhalten bei der Cyber-Security-Hotline unter 0800 888 133 rund um die Uhr kostenlos Hilfe.

(Stand: 14.09.2021)