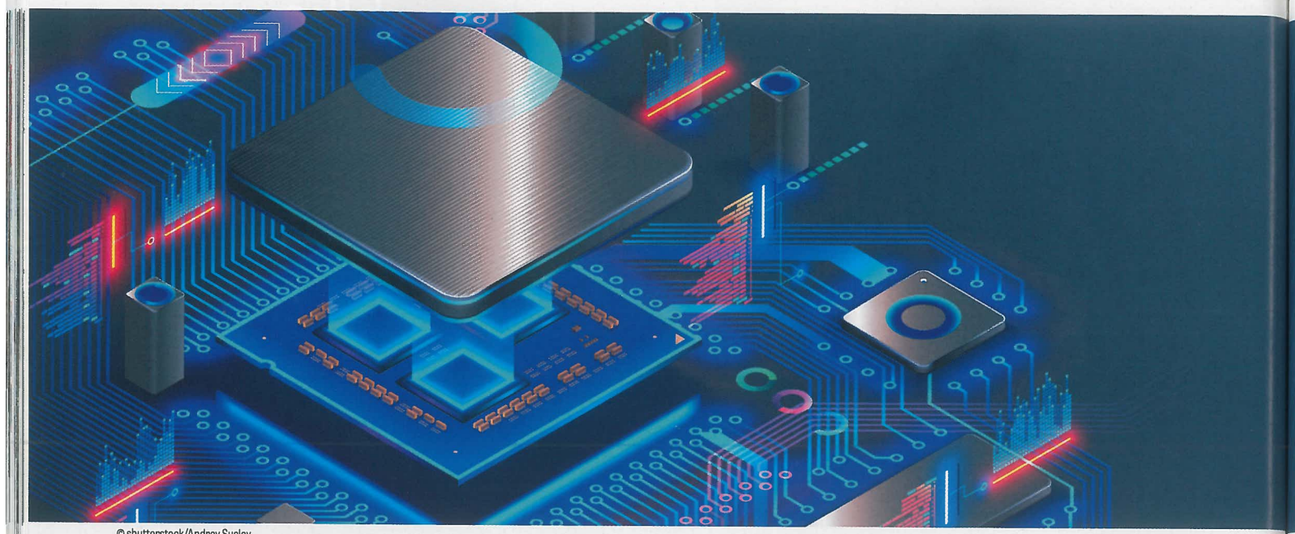


© shutterstock/Andrey Suslov

CYBERSECURITY

2020 hat die Digitalisierung einen großen Schritt nach vorne gemacht. Stefan Albiez und Ivo Rungg, beide Partner bei Binder Grösswang, können mit Expertise praktisch erklären, worauf dabei geachtet werden muss, um Gefahrenquellen zu minimieren.

ALLGEMEIN

In welchen Bereichen beschäftigt Sie das Thema Cybersecurity in Ihrer Arbeit?

Dadurch, dass Geschäftsgeheimnisse in der Regel in digitaler Form verwaltet werden, besteht für Unternehmen immer das Risiko von Angriffen von außen ebenso wie von innen. Das betrifft sowohl Industriespionage als auch ganz allgemeine Betrugsversuche.
Neben den konkreten Schritten zur Wahrung der Rechte unserer Mandanten, ist es uns wichtig, auch bei der internen Aufarbeitung von Datenlecks zu unterstützen und die Verbesserungen der Sicherheitsmaßnahmen im Unternehmen zu begleiten.

Welche Branchen sind davon besonders oft betroffen?

Es können grundsätzlich alle Branchen betroffen sein. Besonders in Branchen und bei Unternehmen mit einer hohen Forschungs-&-Entwicklungs-Quote gibt es aber natürlich eher Geschäftsgeheimnisse, die für Mitbewerber interessant sind. Die meisten Fälle klassischer Industriespionage, mit denen wir zu tun haben, betreffen diese Branchen – etwa den Anlagenbau, die Lebensmittel- und Pharmaindustrie und die Zukunftsindustrien (erneuerbare Energien, Mobilität, etc). Betrugsversuche, die nicht auf den Zugriff auf das Know-how abzielen, können aber alle Unternehmen gleichermaßen treffen. So gibt es gerade auch in Österreich immer wieder Wellen von Fällen, in denen unter Berufung auf real existierende Geschäftsbeziehungen Rechnungen an Unternehmen gesendet wurden, die so gestaltet waren, als stammten sie vom jeweiligen Geschäftspartner, die aber tatsächlich von Dritten erstellt wurden und deren Kontoverbindung im Ausland angaben.

Wie sieht es denn mit der Vertraulichkeit von Geschäftsgeheimnissen aus? Können diese vor Missbrauch geschützt werden?

Geschäftsgeheimnisse liegen rechtlich nur dann vor und sind daher nur dann gegen Missbrauch geschützt, wenn angemessene Geheimhaltungsmaßnahmen getroffen wurden (§ 26b UWG). Diese Maßnahmen können technischer Art (Zugangsbeschränkungen, Passwortschutz etc.) sein, aber auch in Vertraulichkeitsvereinbarungen bestehen. Für den Normalbetrieb eingerichtete Maßnahmen können aber durch die Arbeit im Homeoffice durchlöchert werden. Im eigenen Interesse, zum Schutz des eigenen Know-hows, sollten daher Sicherungsmaßnahmen getroffen werden. Zu bedenken ist auch, dass bestimmte Berufsgruppen besonderen Vertraulichkeitsverpflichtungen unterliegen können, etwa Steuerberater, Rechtsanwälte oder Angehörige medizinischer Berufe. Solche berufsrechtlichen Pflichten können zusätzliche Maßnahmen erfordern.

DATENSCHUTZ

Welche Probleme erleben Sie hier in der Praxis?

In Gerichtsverfahren haben wir immer wieder mit der Frage zu tun, welche Beweismittel verwendet werden dürfen, ohne gleichzeitig gegen datenschutzrechtliche Beschränkungen zu verstoßen. Das betrifft etwa die Frage der Zulässigkeit der Verwendung von Videoaufnahmen von betriebsinternen Überwachungskameras. Zur Verteidigung der eigenen Rechte im Gerichtsverfahren besteht hier ein größerer Spielraum. Unabhängig davon bleibt aber natürlich immer die Frage, ob nicht schon davor Datenschutzregeln verletzt wurden.

Was sollten Unternehmen dahingehend unbedingt beachten?

Unternehmen sind insbesondere verpflichtet, durch technische und organisatorische Maßnahmen ein angemessenes Schutzniveau sicherzustellen (Art. 32 DSGVO). Dabei sind vor allem der Stand der Technik, Implementierungskosten, die Umstände der Datenverarbeitung und der Risikowahrscheinlichkeit zu berücksichtigen. Durch die kurzfristige Umstellung des Bürobetriebs besteht die Gefahr neuer „Leaks". Auch müssen Löschkonzepte auch im Homeoffice eingehalten werden.

©shutterstock/garagestock

▲ Cybersecurity wird von vielen Unternehmen unterschätzt. Remote Work als neuer Standard hat hier neue Fragen an die Oberfläche gebracht.

Würden Sie von der Nutzung von Cloudservices für sensible Daten abraten?

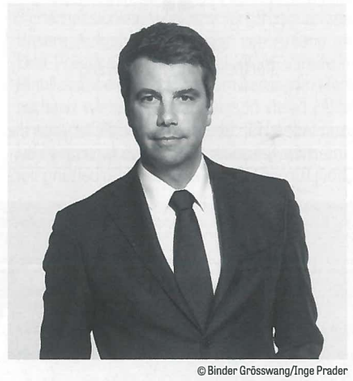
Nein, das würde ich nicht sagen. Das hängt stark vom jeweiligen Anbieter der Cloud-Lösung ab. Werden Cloud-Lösungen eingesetzt, ist sicherzustellen, dass nur Cloud-Anbieter beauftragt werden, die – als Auftragsdatenverarbeiter – Garantien für geeignete technische und organisatorische Maßnahmen bieten. Entscheidend ist vor allem, wo die Rechenzentren der Anbieter stehen, also zum Beispiel innerhalb der Europäischen Union. Das ist auch vor dem Hintergrund bedeutsam, dass z.B. das Privacy-Shield-Abkommen mit den USA vom EuGH im Sommer für ungültig erklärt wurde. Cloud-Anbieter mit hohen Sicherheitsstandards setzten eine Menge an Ressourcen in die Sicherung dieser Rechenzentren ein, die größer ist als das, was viele Unternehmen intern erreichen könnten.

Gibt es eine Frist, wann bekannte Datenschutzverstöße behördlich gemeldet werden müssen?

Die gibt es tatsächlich. Alle Datenschutzverstöße sind unverzüglich und möglichst binnen 72 Stunden der Datenschutzbehörde und bei hohem Risiko den Betroffenen zu melden (Art. 33, 34 DSGVO). Es empfiehlt sich, einen vorhandenen Notfallplan an die neuen Umstände anzupassen.

INDUSTRIESPIONAGE

Welche zivil- und strafrechtlichen Mittel haben Betroffene hier?



© Binder Grösswang/Inge Prader

„Cloud-Anbieter mit hohen Sicherheitsstandards setzten eine Menge an Ressourcen in die Sicherung dieser Rechenzentren ein, die größer ist als das, was viele Unternehmen intern erreichen könnten."

Ivo Rungg
Partner Binder Grösswang

Auf der strafrechtlichen Seite betreuen wir Unternehmen, die Opfer solcher Attacken geworden sind, bei der forensischen Aufarbeitung der Geschehnisse und im Rahmen des Strafverfahrens selbst. Insbesondere vertreten wir auch in Privatanklageverfahren, in denen das Opfer selbst die Rolle der Staatsanwaltschaft übernimmt. Strafrechtliche Verfahren eröffnen für betroffene Unternehmen oft die Möglichkeit, mit Hilfe der Behörden bei der Klärung des Sachverhalts an wichtige Informationen zu gelangen, die dann bei der Durchsetzung der zivilrechtlichen Ansprüche hilfreich sein können. Natürlich betreuen wir unsere Mandanten dann auch im Rahmen solcher zivilrechtlichen Schritte. Es gibt aber selbstverständlich auch Fälle, in denen es sinnvoller ist, nur zivilrechtliche Maßnahmen zu setzen. Das kann z.B. bei Vertraulichkeitsbrüchen ehemaliger oder aktueller Mitarbeiter, die Informationen an Mitbewerber weitergeben, der Fall sein. Hier geht es einerseits um die Durchsetzung finanzieller Ansprüche, viel wichtiger ist es aber oft, Mitbewerber effektiv daran zu hindern, solche Informationen in weiterer Folge zu nutzen. Neben den klassischen, oft langwierigen Zivilverfahren unterstützen wir unsere Mandanten daher auch bei der Erwirkung sofort gültiger einstweiliger Maßnahmen.

Ist das nach Ihrer Erfahrung in Österreich bereits ein relevantes Thema?

Absolut. Wir führen seit vielen Jahren große Verfahren, bei denen straf- und zivilrechtliche Schritte kombiniert werden. Wir haben hier eine stetige Zunahme dieser Fälle bemerkt. Zu juristischen Auseinandersetzungen kommt es insbesondere in zwei Konstellationen. Einerseits dann, wenn Mitarbeiter das Unternehmen verlassen und entweder zu Mitbewerbern wechseln oder ein eigenes Unternehmen gründen. Andererseits dann, wenn mehrere Unternehmen eine Zusammenarbeit – etwa in Form eines Joint Ventures – anstreben, die dann aus bestimmten Gründen nicht umgesetzt wird oder scheitert. Dann kommt es schnell zu Auseinandersetzungen über die weitere Verwendung des jeweiligen Know-hows. ▸

Geht es dabei eher um Sabotage oder Datendiebstahl?

Der Schwerpunkt liegt sicher auf Datendiebstahl. Sabotage unter Mitbewerbern ist in unserer Praxis ein Randphänomen. Anders sieht es mit gezielten kriminellen Angriffen Außenstehender aus, die auf die betrügerische oder erpresserische Veranlassung von Zahlungen gerichtet sind, bei denen sich die Angreifer illegal erlangte Informationen zu Nutze machen.

Welche Fehler machen Unternehmen in der Praxis?

Hier geht es einerseits um technische Versäumnisse. E-Mails werden etwa von vielen Unternehmen immer noch ausnahmslos unverschlüsselt versendet. Andererseits fehlen oft die für diesen Bereich so wichtigen Konkurrenzklauseln in Verträgen mit Mitarbeitern. Ganz allgemein beobachten wir, dass erst langsam eine Sensibilisierung für diese Themen einsetzt. Ein praktisches Zeichen dieser Entwicklung ist es, dass sensible Unterlagen in unserer täglichen Arbeit immer weniger direkt versendet, sondern immer mehr im Wege gesicherter Datenräume geteilt werden.

Wie sollten Unternehmen bei Datenlecks am besten die internen Ermittlungen führen? Braucht es dafür externe Berater?

Das ist zunächst eine Frage des Umfangs und der Sensibilität des Datenlecks, aber auch eine Frage der Unternehmensgröße und -organisation. Da gibt es große Unternehmen, die

© Binder Grösswang/Inge Prader

Die meisten Fälle klassischer Industriespionage, mit denen wir zu tun haben, betreffen die Branchen Anlagenbau, die Lebensmittel- und Pharmaindustrie und die Zukunftsindustrien wie erneuerbare Energien oder auch Mobilität.

Stefan Albiez
Partner Binder Grösswang

zumindest für überschaubare Fälle über die internen Ressourcen und das interne Know-how für eine Sachverhalts-Aufarbeitung verfügen und ohne unmittelbare Mitarbeit externer Berater umfassende Erst-Analysen selbst vornehmen. Aufbauend auf diesen Analysen übernehmen wir dann die weitere Detail-Analyse, zeigen etwaige Lücken auf und bereiten die erhaltenen Informationen bestmöglich für die Durchsetzung der Rechte der Mandantin auf. Gerade im KMU-Bereich fehlen die unternehmensinternen Ressourcen aber in der Regel. Hier macht es oft Sinn, die Aufarbeitung von externen Beratern leiten zu lassen. In allen Fällen geht es jedenfalls darum, möglichst schnell zu handeln. Essenziell ist dabei die möglichst sofortige Zusammenstellung eines Teams zur koordinierten Setzung der erforderlichen nächsten Schritte, wie insbesondere die Sicherung der digitalen Spuren und die Identifikation der in einen Vorfall involvierten internen und externen Personen.

Welche Grenzen setzt das Datenschutzrecht solchen Ermittlungen?

Das Datenschutzrecht kann insbesondere dann zum Hindernis von Ermittlungen werden, wenn es zu einer Vermischung von beruflichen und privaten Daten gekommen ist. Auf private Daten darf man nämlich grundsätzlich bei Untersuchungen durch den Arbeitgeber nicht zugreifen. Es empfiehlt sich daher, dazu genaue Regelungen und Vorgaben im Unternehmen zu treffen. Auch die Löschungsverpflichtung kann Untersuchungen entgegenstehen, wenn die Daten nach der gesetzlichen Löschverpflichtung bereits gelöscht sind, aber für die Ermittlung hilfreich wären – das sind ähnliche Überlegungen wie bei der Vorratsdatenspeicherung.

© Ömelchenko

VERSICHERUNG GEGEN CYBER-RISIKO

Auch in Österreich kann man sich gegen den Schadensfall durch Cyberkriminalität versichern. Die fortschreitende Digitalisierung im Sinne des Auslagerns von Arbeitsprozessen (samt dazugehöriger Software) in den virtuellen Raum, die Bequemlichkeit der Steuerung von Produktionsmaschinen aus der Ferne oder auch die Ablage unternehmenswichtiger Dokumente in digitaler Form (mitunter auf Servern auf anderen Kontinenten) führen zu einer immer größeren Abhängigkeit unserer Computersysteme und deren Vernetzung miteinander. Die Funktionalität, und damit einhergehend die Absicherung dieser Systeme, ist für sehr viele Unternehmen mittlerweile ein existenzbedrohendes Risiko. So sind auch im Allianz Risk Barometer 2020 (www.allianz.at, 2020) erstmals Cyber-Vorfälle global betrachtet das wichtigste Geschäftsrisiko und wurde die klassische Betriebsunterbrechung an erster Stelle abgelöst. Aus der klassischen Risikomanagementlehre heraus kann ein Risiko verhindert, minimiert oder überwälzt werden.

Die gänzliche Verhinderung steht nicht im Einklang mit der Digitalisierung. Mit technischen und organisatorischen Maßnahmen lässt sich das Cyber-Risiko minimieren. Für die Überwälzung des Risikos stehen Versicherungen zur Verfügung. Die seit Jahren in Österreich bestehenden Cyber-Versicherungs-Produkte bieten nicht nur umfassende Kostendeckung für Eigen- und Drittschäden durch Cyber-Vorfälle, sondern stellen auch diverse Servicedienstleistungen zur Verfügung.

©Roland Rudolph

Die Cyberversicherung ist die Feuerversicherung des 21. Jahrhunderts. Eine Betriebsunterbrechung aufgrund einer Cyberattacke ist um ein Vielfaches wahrscheinlicher geworden im Vergleich zu einem Ertragsausfall wegen Brand.

Stefan Kojalek
Aktuell Gruppe

AKTUELL / CORONA / HOMEOFFICE

Sehen Sie aus dem Blickwinkel der Cybersecurity Risiken, die sich aus dem aktuellen Trend zum Homeoffice ergeben? Würden Sie Unternehmen davon abraten, ihre Mitarbeiter zur Verwendung eigener Geräte anzuhalten?

Natürlich gibt es hier zusätzliche Risiken. Aus unserer Sicht kann man jedem Unternehmen nur empfehlen, auch im Homeoffice nur unternehmenseigene IT-Infrastruktur (Laptops/Tablets/Handys) einzusetzen oder – wo das nicht möglich ist – zumindest die privaten Geräte der Mitarbeiter zu prüfen und sichere Zugänge zum internen System zu gewährleisten.

Klar ist, dass für den Normalbetrieb eingerichtete Maßnahmen zur Wahrung von vertraulichen Daten, durch die Arbeit im Homeoffice durchlöchert werden können. Seit Beginn der Corona-Krise wurden verstärkt Phishing-Mails verschickt und Cyberattacken von Kriminellen gestartet, die von der allgemeinen Verunsicherung profitieren wollen. Je nach Ausstattung des Homeoffice und der Kommunikationskultur in dieser Umgebung, könnten bestehende Risiken erhöht werden, zu denken ist dabei etwa an Presidential-E-Mails. Neben technischen Sicherheitsmaßnahmen sind Mitarbeiter besonders bezüglich solcher erhöhten Gefahren zu sensibilisieren.

Wie haben sich hier die Themen und der Beratungsbedarf von Unternehmen in dieser Hinsicht im letzten halben Jahr verändert?

Das Thema Homeoffice hat einen umfassenden Beratungsbedarf nicht nur im Zusammenhang mit Datensicherheit, sondern insbesondere auch im Hinblick auf arbeitsrechtliche Fragen geschaffen.

Je nach Ausstattung des Homeoffice und der Kommunikationskultur in dieser Umgebung, könnten bestehende Risiken erhöht werden. Neben technischen Sicherheitsmaßnahmen sind Mitarbeiter besonders bezüglich solcher erhöhten Gefahren zu sensibilisieren.

Ivo Rungg
Partner Binder Grösswang

Während bei Letzteren die Lösungen unmittelbar erforderlich waren und das Homeoffice in den meisten Fällen auch gut umgesetzt werden konnte, werden sich die Probleme etwaiger Sicherheitslücken wohl erst langfristig zeigen. Unsere Aufgabe war es hier von Anfang an, Best-Practice-Beispiele zu schaffen – gerade im Hinblick auf die so abrupte Umstellung im März rechnen wir aber damit, dass in vielen Fällen erst nachträglich die ratsamen Sicherheitsvorkehrungen nachgezogen werden konnten.

Würden Sie sagen, dass das Homeoffice im Hinblick auf Cybersecurity in Österreich bisher funktioniert? Wo besteht aus Ihrer Sicht Verbesserungsbedarf?

Diese Frage wird man wohl erst kommendes Jahr wirklich beantworten können. Momentan sind uns wenige Problemfälle bekannt – das liegt aber wohl maßgeblich daran, dass diese Themen erst aufschlagen, wenn bekannt wird, dass etwaige Sicherheitslücken auch wirklich ausgenutzt wurden. Wir sehen aber den Trend, dass die Unternehmen nun im Winter besser vorbereitet sind. Es steht eher unternehmenseigene Infrastruktur zur Verfügung, es werden verstärkt sichere Datenräume genutzt. Natürlich ist diese Entwicklung aber noch nicht abgeschlossen.

Welche Problembereiche sehen Sie im Zusammenhang mit Cybercrime?

Da gibt es einige kritische Themenfelder. Die Verwendung von uneinheitlicher/privater Hardware (Computer, Smartphones, Speichermedien und Drucker) oder der Zugang zum Internet und die mögliche Verwendung offener WLAN-Netze sind hier ganz besonders hervorzuheben. Aber auch die Verwendung von Software, die unsicher oder für den professionellen Einsatz ungeeignet ist – wie zur Kommunikation zwischen Mitarbeitern oder das Speichern in einer öffentlichen Cloud – kann häufig zu Problemen führen. Mögliche technische und organisatorische Maßnahmen müssen dann ganz individuell an die Größe und Art des Unternehmens sowie die verarbeiteten Daten angepasst werden und vor allem auch für die Homeoffice-Arbeitsplätze gelten. ■ *MARTIN MÜHL*