makler intern QM
04/2022

Versicherungsleistungen unter der Lupe

Ihre Kund:innen haben ein Elektroauto, aber wer hat die passende Versicherung? Der 1. große Leistungsvergleich.

Ing. Manuel LECHNER, BSc
Risk Consultant

RISK EXPERTS
ENABLING SMART DECISIONS.

Warum guter Objektschutz heutzutage nicht nur Objekte schützt

Objektschutz betrifft uns alle, ob privat oder im Unternehmen. Wer achtet denn nicht auf seine Vermögenswerte? Der Grad von eingesetzten Schutzmaßnahmen korreliert aber oft mit dem subjektiven Sicherheitsempfinden – und dabei gibt es erfahrungsgemäß große Unterschiede.

Mit voranschreitender Digitalisierung und mannigfaltigen Security-Tools wird auch der Objektschutz zu einem immer komplexeren Thema. Die physische Sicherheit von Unternehmen umfasst heute nicht nur Objekte, Gebäude und Assets, sondern zusätzlich Informationssicherheit und Datenschutz. Die „Erhaltung von Verfügbarkeit, Vertraulichkeit und Integrität von Assets durch die Nutzung von ganzheitlichen Maßnahmen“ sind mittlerweile sowohl in der ÖNORM S 2414, 2.36 als auch in der ISO27001 manifestiert.

Mitarbeiter:innen sind ein zentrales Asset

Immer wieder stellen wir bei vorliegenden Schutzkonzepten fest, dass ein zentraler Sicherheitsaspekt oft unzureichend berücksichtigt wird, und zwar jener des Personenschutzes. Gerade bei diesem Thema gibt es für Unternehmen Aufholbedarf, da vor allem die Mitarbeiter:innen in einem Betrieb als zentrales Asset zu sehen sind.

Heutzutage ist die physische Sicherheit eines Unternehmens sehr eng mit Informationssicherheit vernetzt und es entstehen laufend neue Gesetze und Richtlinien für den Umgang mit personenbezogenen Daten. Gerade in den Bereichen Datensicherheit und dem Datenschutz werden wir in den kommenden Monaten und Jahren mit weiteren Auflagen zu rechnen haben.

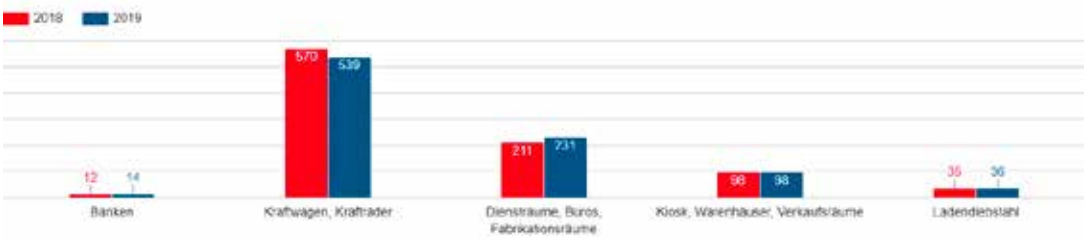
Dieser Artikel erklärt, warum Objektschutz auch für Makler:innen ein wichtiges Thema ist und welche Aspekte Sie dabei wissen sollten.
Die jährliche polizeiliche Kriminalstatistik (PKA, 2021) zeigt zwar einen Rückgang bei Einbruchsdiebstählen, sowohl in privaten Wohnräumen als auch bei Unternehmen, jedoch steigen die Folgeschäden, wie z. B. Haftungen bei Verletzungen im Bereich des Datenschutzes kontinuierlich an.* Allein in Deutschland verursachen Einbrüche Schäden von durchschnittlich 180 Millionen Euro.**

Einbruchschäden bei Unternehmen in Millionenhöhe

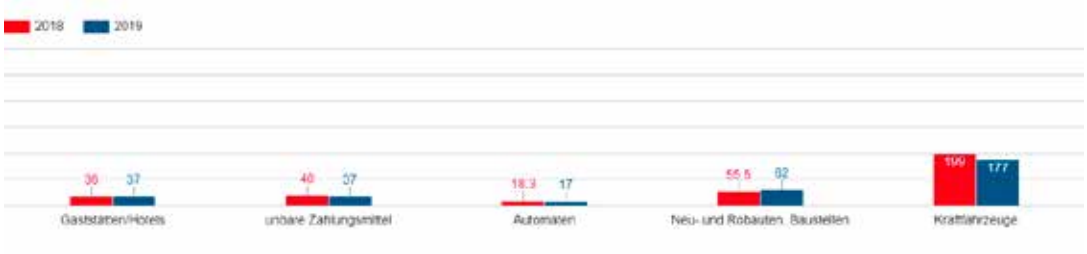
Die Schäden und Folgeschäden aufgrund fehlender Sicherheitskonzepte steigen jährlich an, betroffen sind aber nicht nur die wertvollen Inhalte von Juweliergeschäften oder Bürogebäuden. Wirklich teuer wird es, wenn nach einem Vorfall der Betrieb stillsteht oder Verletzungen bzw. Versäumnisse rund um den Datenschutz festgestellt werden. Kurz gesagt ist kein Unternehmen vor einem Einbruch sicher. Monatlich werden in Österreich mehr als 4.500 Einbruchsdiebstähle gemeldet, wobei des Öfteren Unternehmen in kleineren Städten betroffen sind***.

In vielen Fällen sind sich Unternehmen nicht bewusst, welchen Risiken sie tatsächlich ausgesetzt sind. Die Sicherheit wird bei vielen KMU nur wenig beachtet. Im Management tritt oft die klassische

Schadensumme nach Diebstahlarten (Angaben in Mio.)**



Schadensumme nach Diebstahlarten (Angaben in Mio.)****



Betriebsblindheit zu Tage. Hier haben Sie als Makler:in die Chance als Ritter in glänzender Rüstung aktiv zu werden. Im Sinne des „Best Advice"- Grundsatzes, den das Maklergesetz in §28 beschreibt, sollten Sie erkennbare Mankos direkt ansprechen und so einen zusätzlichen Mehrwert in Ihrer Beratungsleistung schaffen.

Auswirkung von Einbrüchen auf die Informationssicherheit von Unternehmen

Einbrüche führen nicht nur zu Sachschäden oder Wertverlusten, sondern können auch zu Haftungspotenzialen im Rahmen der Informationssicherheit und des Datenschutzes führen. Wie ist das zu verstehen?
Wenn im Zuge eines Einbruchdiebstahls Dokumente, Informationen oder Daten (materiell oder immateriell) gestohlen werden, dann liegt bereits ein Data Breach vor – „Data Breach" bedeutet, dass ein Datenverlust vorliegt, der auch personenbezogene Daten oder beispielsweise Produktionsgeheimnisse beinhalten kann. Ein solcher Vorfall kann auch zu massiven Imageverlusten führen. Wenn zudem gespeicherte Informationen bzw. Assets nicht entsprechend verschlüsselt, versperrt oder gesichert wurden, dann wurden die Grundsätze der DSGVO nicht eingehalten. Vorfälle dieser Art verursachen Haftungspotenziale, die in weiterer Folge wohlmöglich auch empfindliche Strafzahlungen nach sich ziehen. Auch die Gefahr einer länger andauernden Betriebsunterbrechung (BU) kann eine Folge von Einbrüchen sein, wenn relevante Geräte, Ressourcen oder Daten gestohlen bzw. Anlagen/ Server beschädigt werden.

5 Kategorien von Schutzmaßnahmen

Bei der risikoorientierten Beratung von Unternehmen, ist es oft schon ausreichend, die 5 Kategorien von Schutzmaßnahmen anzusprechen. Diese sind unterteilt in:

- Bauliche Schutzmaßnahmen (z.B. Zonentrennungen, Zäune/ Mauern, Wände, etc.)
- Mechanische Schutzmaßnahmen (z.B. Wertschutzbehältnisse, Fenster/ Türen, Schleusen, etc.)
- Elektronische Schutzmaßnahmen (z.B. Überwachungskameras, Zutrittskontrollanlagen, Einbruch-/ Überfallmeldeanlagen, Sensoren, Notstrom, Datenspeicherung, etc.)
- Personelle Schutzmaßnahmen (interner/ externer Wachdienst, Interventionsteam, Ausbildungen/ Know-how, etc.)
- Organisatorische Schutzmaßnahmen (Need-to-Know-Prinzip, Schulungen/Awarness-Trainings, Notfallpläne, Sicherheitsprozesse, etc.)

Viele der Schutzmaßnahmen sind abteilungsübergreifend aufeinander abzustimmen. Jede Abteilung benötigt zudem ausgewiesene Verantwortliche und Stellvertreter:innen, die zu jeder Zeit wissen, was im Notfall zu tun ist.
Während bzw. nach der Implementierung von Maßnahmen oder Prozessen muss unbedingt auch das Personal entsprechend geschult und trainiert werden. Somit entsteht Risikobewusstsein bei allen Mitarbeiter:innen, welches dazu führt, dass die gesetzten Maßnahmen funktionieren. Ein laufender Know-how-Transfer stärkt letztendlich die Widerstandsfestigkeit (Resilienz) eines Unternehmens.

Das Hinzuziehen von externen Expert:innen ist im Bereich Safety und Security grundsätzlich immer zu empfehlen, um der zuvor erwähnten Betriebsblindheit entgegenzuwirken. Auch Sie als Makler:in sind mit dem Thema Risikominimierung vertraut und können bei Versicherungsnehmer:innen für die notwendige Awareness sorgen. Selbst mit dem Verweis auf Fachfirmen, die Risikoanalysen zum Thema „Physische Sicherheit und Informationssicherheit" durchführen, agieren Sie im Sinne des „Best Advice".

Risikoabschätzung erfordert unterschiedliche Sichtweisen

Wie Sie bestimmt wissen, sind Risikoabschätzungen in bestimmten Fällen schwer zu treffen. Gerade im Bereich der physischen Sicherheit in Abhängigkeit von Informationssicherheit und Datenschutz ist es meist eine große Herausforderung, den Überblick zu behalten.

Beim Objektschutz kommt es jedoch nicht nur auf getroffene Schutzmaßnahmen an, sondern auch auf Täterprofile (modi operandi). Darunter versteht man, welche Intention, Motivation, Attraktivität und welches Know-how Tätergruppen aufweisen. Neben dieser „Threat-Analyse" spielt zudem auch die Anbindung und Interventionszeit der Sicherheitskräfte oder der Polizei eine wichtige Rolle.

Wie bewertet man ein Risikopotenzial?

Abschließend möchten wir Ihnen noch einige Punkte an die Hand geben, die es erleichtern, das Risikopotenzial eines Unternehmens (approximativ) zu bewerten: »

Zu Beginn der Analyse sind die Werte (Assets) des Unternehmens zu identifizieren. Daraufhin müssen einzelne Maßnahmen (vorhandene und zu implementierende) evaluiert und den 5 genannten Kategorien zugeordnet werden. Beispiele dafür sind:

1 Sind im Unternehmen die Zugänge zu Bereichen anhand ihrer Kritikalität definiert (öffentlich, intern, vertraulich)?
2 Welche Schutzbarrieren (z.B. Türen/ Schließsysteme, Tresore, etc.) sind vorhanden?
3 Gibt es Bewegungsmelder, Zutrittskontrollen, Überwachungskameras, Sensoren?
4 Sind die Verantwortungen hinsichtlich Unternehmenssicherheit definiert (z.B. interner/ externer Sicherheitsdienst, IT-Security, Objektschutz)?
5 Gibt es Prozesse, wie Besuchermanagement, interne Schulungen, Unterweisungen, Alarm-/ Notfallmanagement?

Bereits mit diesen 5 Fragen sind Sie in der Lage, die Unternehmenssicherheit grob zu analysieren und zu bewerten. Zusätzlich schärfen Sie damit das Bewusstsein bei Ihren Kund:innen.

Unterstützung von Risk Experts

Für die Unterstützung eines ganzheitlichen Schutzes im Bereich Physische- und Cyber-Sicherheit, Risikoanalyse und -reduktion, insbesondere Risk Engineering und Objektschutz (Einbruchsdiebstahl), stehen Ihnen unsere Expert:innen gerne zur Verfügung **(www.riskexperts.at)**.

Folgen Sie uns auch auf LinkedIn!
Weiterführende Links und Wissenswertes:
(*) https://www.bundeskriminalamt.at
(**) https://www.polizei-dein-partner.de
(***) https://www.wirtschaftsforum.de
(****) https://www.protectionone.de

Quellen Grafiken:
Protection One GmbH | Sicherheitsstudie 2021: Wie sicher ist Deutschland | https://www.protectionone.de/webstudie-sicherheit/fakten-quoten/sicherheit-fuer-unternehmen/