COMPUTERKRIMINALITÄT

Die grössten Risiken der heutigen Zeit

Die Computerkriminalität, die sogenannte Cybercrime, gewinnt im heutigen Geschäftsalltag leider zunehmend an Bedeutung. Der Grund ist, dass ein Grossteil der wirtschaftlichen Prozesse heutzutage vernetzt und von der Informationstechnologie abhängig sind. Auch die Metallbaubranche ist davon betroffen. Text: PROMRISK AG / Bild: Redaktion

Die Cyber-Risiken sind nicht zu unterschätzen, insbesondere darum, weil heutige Betriebe immer moderner ausgestattet und mittlerweile auch Maschinen und Anlagen mit dem IT-System verbunden sind. Ebenso speichert ein Metallbaubetrieb wichtige Daten wie z.B. Kundenaufträge, Planungen oder auch Personaldaten. Damit steigt das Risiko für Unternehmen, einen Cyber-Schaden zu erleiden, sei es durch einen beabsichtigten oder unbeabsichtigten technischen Fehler, durch eigene Mitarbeiter, einen Angriff von Cyber-Kriminellen oder sonstige Ursachen. Experten schätzen, dass jährlich über 90% der Unternehmen Cyber-Attacken ausgesetzt sind. In der Schweiz wurden im Jahr 2022 Total 33 345 Angriffe polizeilich registriert, wobei die Dunkelziffer wesentlich höher ausfallen dürfte. Die Aufklärungsrate bei Ransomware-Angriffen z.B. beträgt lediglich 1,3%. Daraus resultierende Datenverluste oder IT-Störungen können zu immensen finanziellen Auswirkungen führen.

Was genau sind Cyber-Risiken?
Das Wort «Cyber» ist heutzutage in aller Munde, doch was bedeutet es eigentlich? Cyber stammt aus dem Englischen und steht für alles, was mit der virtuellen Welt zu tun hat. Kurz zusammengefasst steht Cyber-Risiko für drei Verletzungen im Zusammenhang mit Daten:

- Eigenschäden (Entfernung von Schadsoftware, Wiederherstellungskosten, Betriebsausfall etc.);
- Drittschäden (Datenverlust, Datenschutzverletzung etc.);
- Erpressung/Lösegelder.

Reale Schadenbeispiele von Metallbaubetrieben

Beispiel 1: Fremdschäden
Ausgangslage:
Die Muster Metallbau AG ist eine klassische und mittelgrosse Metallbaufirma mit eigenem Server und wöchentlichem Backup.

Schaden:
Die Muster Metallbau AG wurde von einem Hacker angegriffen. Mittels eines Trojaners wurden sensible Daten von Kunden und Lieferanten gestohlen und vom Hacker unerlaubt veröffentlicht. Einige der Kunden und Lieferanten tragen einen Imageschaden davon und stellen der Muster Metallbau AG einen Schadenersatzanspruch.

Problematik:
Für die Muster Metallbau AG entsteht ein reiner Vermögensschaden gegenüber Dritten. In der klassischen Betriebshaftpflichtversicherung sind reine Vermögensschäden grundsätzlich ausgeschlossen.

Folge:
Die Muster Metallbau AG muss für den entstandenen Schaden selbst aufkommen.

Lösung:
Abschluss einer entsprechenden Cyber-Police mit Einschluss der Fremdschäden.

Beispiel 2: Social Engineering (Fake President)
Ausgangslage:
Die Muster Metallbau AG ist eine klassische, grössere Metallbaufirma mit 30 Mitarbeitenden.

Schaden:
Ein Mitarbeiter aus der Buchhaltung der Muster Metallbau AG bekommt eine sichere E-Mail eines Lieferanten, welcher behauptet, dass eine Eillieferung, die der Chef dringend erwartet, erst versendet werden kann, wenn der offene Betrag in Höhe von CHF 22 500.– sofort überwiesen wird. Eine Stunde nach Erhalt dieser E-Mail erfolgt ein Telefonanruf des «Liefe-

«Die Cyber-Risk-Versicherung deckt sowohl Schäden, die der Versicherte einem Dritten verursacht (Drittschaden), als auch Schäden, die beim Versicherten selbst entstehen (Eigenschaden).»

CRIMINALITÉ INFORMATIQUE

Les plus grands risques de notre époque

La criminalité informatique, ou cybercrime, prend malheureusement de plus en plus d'importance dans le quotidien professionnel d'aujourd'hui. En effet, une grande partie des processus économiques sont aujourd'hui interconnectés et dépendent des technologies de l'information. La branche de la construction métallique est également concernée.

Les cyberrisques ne doivent pas être sous-estimés, notamment parce que les entreprises actuelles possèdent des équipements de plus en plus modernes et que les machines et installations sont désormais reliées à l'infrastructure informatique. De même, une entreprise de construction métallique enregistre des données importantes telles que des commandes de clients, des planifications ou des données personnelles. Pour les entreprises, cela augmente le risque de subir un cyberdommage, qu'il soit provoqué par une erreur technique intentionnelle ou involontaire, des collaborateurs de l'entreprise, une attaque de cybercriminels ou autres. Les experts estiment que plus de 90 % des entreprises sont exposées chaque année à des cyberattaques. En 2022, 33 345 attaques ont été recensées par la police en Suisse. Les chiffres réels pourraient toutefois être beaucoup plus élevés. Le taux d'élucidation des attaques par ransomware p. ex. ne s'élève qu'à 1,3 %.

Im Jahr 2022 wurden in der Schweiz Total 33 345 Angriffe polizeilich registriert. Die Dunkelziffer dürfte jedoch wesentlich höher liegen.
En 2022, 33 345 attaques ont été recensées par la police en Suisse. Les chiffres réels pourraient toutefois être beaucoup plus élevés.

ranten», der nochmals mit Nachdruck auf die Überweisung drängt.

Problematik:
Der Buchhaltungsmitarbeiter ist überfordert, da er über die Knappheit der angeblichen Lieferung (Material) Bescheid weiss und sein Chef als Choleriker bekannt ist. Er möchte nicht, dass die vom Chef vermeintlich bestellte Lieferung seinetwegen nicht rechtzeitig ankommt, und überweist deshalb per Sofortüberweisung den geforderten Betrag.

Folge:
Der bezahlte Betrag von CHF 22 500.– ist verloren.

Lösung:
Abschluss einer entsprechenden Cyber-Police mit der Deckung Social-Engineering.

Was kann dagegen unternommen werden?
Firmen sind lukrative Ziele für Betrüger. Im Vergleich zu Privatpersonen lassen sich in der Regel auf einen Schlag grössere Summen entwenden. Deshalb wenden die Angreifer mehr Zeit auf und die Angriffe erfolgen gezielter und professioneller als bei Privatpersonen. Dabei stehen vor allem die Finanzabteilungen im Fokus. Die Betriebshaftpflichtversicherung deckt Schäden, welche einem Dritten durch Verschulden des Versicherten entstehen. Allerdings werden grundsätzlich ausschliesslich >

Glossar

Fake President
Ist eine Betrugsmasche, bei der Firmen bzw. einzelne Mitarbeiter unter Verwendung falscher Identitäten und Ausnutzung der Autorität zur Überweisung von Geld manipuliert werden.

Social Engineering
Angreifer versuchen, Personen durch Täuschung dazu zu bringen, etwas zu tun, was diese eigentlich nicht wollen. Das dafür gewählte Szenario soll das mögliche Opfer emotional berühren oder sein Interesse wecken. Das Ziel ist es, Nähe aufzubauen und ein vermeintliches Sicherheitsgefühl zu wecken. Die Täterschaft informiert sich im Vorfeld über die Struktur eines Unternehmens oder über persönliche Interessen einer möglichen Zielperson. Dies geschieht oft durch frei verfügbare Informationen (zum Beispiel auf der Website des Unternehmens oder in sozialen Netzwerken wie Linkedin). Daraufhin wird die Zielperson mit einem auf sie zugeschnittenen Szenario konfrontiert.

Ransomware
sind Schadprogramme, die den Computer sperren oder darauf befindliche Daten verschlüsseln. Die Täter erpressen ihre Opfer, indem sie deutlich machen, dass der Bildschirm oder die Daten nur nach einer Lösegeldzahlung wieder freigegeben werden.

Obliegenheiten
Sind Verhaltensvorschriften, die sich aus Ihrem Versicherungsvertrag und den Versicherungsbedingungen ergeben. Als Versicherungsnehmer sind Sie dazu verpflichtet, Ihre spezifischen Obliegenheiten einzuhalten. Andernfalls gefährden Sie Ihren Versicherungsschutz.

Glossaire

Fraude au président
Escroquerie consistant à duper une entreprise ou un collaborateur en utilisant une fausse identité et en abusant de l'autorité en vue d'un transfert d'argent.

Social engineering
Tentative d'escroquerie par laquelle les escrocs essaient d'amener des personnes à réaliser quelque chose qu'elles ne souhaitent pas faire. Le scénario choisi doit toucher la victime potentielle ou susciter son intérêt. L'objectif est de créer de la proximité et de mettre en place un sentiment de sécurité. Les auteurs se renseignent au préalable sur la structure d'une entreprise ou sur les intérêts personnels d'une personne cible potentielle. Pour ce faire, ils consultent souvent des informations librement accessibles (p. ex. sur le site Internet de l'entreprise ou sur les réseaux sociaux tels que LinkedIn). La personne ciblée est alors confrontée à un scénario sur mesure.

Ransomware
Ce sont des programmes malveillants qui bloquent l'ordinateur ou cryptent les données qui s'y trouvent. Les auteurs font chanter leurs victimes en leur annonçant que l'écran ou les données ne seront récupérés qu'après versement d'une rançon.

Obligations
Il s'agit de règles de comportement qui découlent de votre contrat d'assurance et des conditions d'assurance. En tant que preneur d'assurance, vous êtes tenu au respect de vos obligations spécifiques. Dans le cas contraire, vous mettez en péril votre couverture d'assurance.

Les pertes de données ou les dysfonctionnements informatiques qui en résultent peuvent avoir d'énormes conséquences financières.

Que sont exactement les cyberrisques ?
Le mot « cyber » est aujourd'hui sur toutes les lèvres, mais que signifie-t-il au juste ? Cyber vient de l'anglais et désigne tout ce qui a trait au monde virtuel. Pour résumer, le cyberrisque désigne trois atteintes en lien avec des données :

- Dommages propres (suppression de logiciels malveillants, frais de restauration, panne, etc.)
- Dommages à des tiers (perte de données, violation de la protection des données, etc.)
- Extorsion/rançons.

Exemples de dommages réels pour des entreprises de construction métallique

Exemple 1 : dommages causés à des tiers
Situation initiale :
L'entreprise Exemple Construction métallique SA est une entreprise de construction métallique classique de taille moyenne disposant de son propre serveur. Elle effectue une sauvegarde hebdomadaire.

Sinistre :
L'entreprise a été attaquée par un hacker. Des données sensibles de clients et de fournisseurs ont été volées à l'aide d'un cheval de Troie et publiées sans autorisation par le hacker. Certains clients et fournisseurs en subissent une atteinte à l'image et réclament des dommages et intérêts à Exemple Construction métallique SA.

Problème :
Pour Exemple Construction métallique SA, il en résulte un dommage >

> Personen- und Sachschäden sowie die daraus entstehenden Folgeschäden versichert, nicht aber Vermögensschäden, welche üblicherweise im Zusammenhang mit Cyber-Risiken anfallen. Hier greifen die Cyber-Risk-Versicherungslösungen. Die Cyber-Risk-Versicherung deckt sowohl Schäden, die der Versicherte einem Dritten verursacht (Drittschaden), als auch Schäden, die beim Versicherten selbst entstehen (Eigenschaden). Eigenschaden entsteht beispielsweise durch kriminelle Handlungen Dritter, bei denen Daten des Versicherten beschädigt oder vernichtet werden oder die Geschäftsaktivität beeinträchtigt oder gar unterbrochen wird. Erpressungsversuche mit sog. Ramsonware, mittels deren Daten verschlüsselt und für deren Entschlüsselung eine Lösegeldzahlung gefordert wird, kommen ebenfalls vor.

In Schadenfällen decken Cyber-Risk-Versicherungen regelmässig den Ausgleich berechtigter sowie die Abwehr unberechtigter Schadenersatzansprüche Dritter. Die Wiederherstellungskosten des IT-Systems bei durch einen Cyber-Angriff beschädigten, blockierten oder zerstörten Daten, Programmen und Netzwerken werden ebenfalls erstattet. Bei Betriebsunterbruch werden der Ertragsausfall sowie weitere Kosten, welche zur Fortführung der Betriebsaktivitäten erforderlich sind, gedeckt. Erpressungszahlungen können in die Cyber-Police miteingeschlossen werden. Aber nicht nur der Ausgleich des durch den Cyber-Vorfall direkt verursachten Schadens, sondern auch Kosten wie diejenigen für die Beauftragung eines professionellen Krisenmanagements, von externen Computer-Forensik-Analysten, PR-Experten und spezialisierten Anwälten werden regelmässig gedeckt. Abschliessend möchten wir auf den wichtigen Punkt hinweisen, dass die Versicherungsnehmer auch bei einem allfälligen Schadenfall mit ihrem bestehenden IT-Partner zusammenarbeiten können. Diese Versicherung übernimmt dann die Kosten Ihres IT-Partners für sie.

Die PROMRISK AG weiss Rat

Die PROMRISK AG, der offizielle Verbandsbroker des AM Suisse, hat sich seit Aufkommen dieses Themas intensiv mit den Cyber-Risiken auseinandergesetzt. Cyber-Versicherungen sind erst seit wenigen Jahren auf dem Markt, die Produkte unterscheiden sich von Versicherungsgesellschaft zu Versicherungsgesellschaft enorm. Wichtig ist, dass nicht jedes Cyber-Produkt zu jedem Betrieb passt. Es muss individuell je nach Betrieb das Risiko analysiert und dafür ein geeigneter Versicherungspartner gefunden werden. Deshalb erstellen wir jedes Jahr einen neuen und umfangreichen Cyber-Vergleich aller Versicherungsgesellschaften, sodass wir immerzu auf das aktuell beste Produkt je nach Bedarf zurückgreifen können. Hierzu zählen auch die Obliegenheiten im Schadenfall sowie das Ausfüllen des Cyber-Fragebogens.

Wir haben uns auf die Cyber-Risiken der Metallbaubranche spezialisiert und helfen und beraten Sie gerne.
Tel. 044 851 55 66 oder info@promrisk.ch
www.promrisk.ch ■

PROMRISK
Verbandsbroker AM Suisse

> économique pur vis-à-vis de tiers. Les dommages économiques purs sont exclus de l'assurance responsabilité civile d'entreprise classique.
Conséquence :
Exemple Construction métallique SA doit assumer elle-même le dommage subi.
Solution :
Conclure une cyberpolice correspondante incluant les dommages causés à des tiers.

Exemple 2 : Social engineering (fraude au président)

Situation initiale :
Exemple Construction métallique SA est une grande entreprise de construction métallique classique qui emploie 30 collaborateurs.
Sinistre :
Un collaborateur de la comptabilité de l'entreprise reçoit un e-mail sécurisé d'un fournisseur qui prétend qu'une livraison urgente attendue par le chef ne peut être envoyée que si le montant dû de CHF 22 500.– est versé immédiatement. Une heure après la réception de cet e-mail, le « fournisseur » téléphone et insiste pour recevoir le virement.
Problème :
Le collaborateur de la comptabilité est débordé, il sait que la soi-disant livraison porte sur du matériel en pénurie et son chef est connu pour être colérique. Il ne souhaite pas que le matériel prétendument commandé par le chef n'arrive pas à temps à cause de lui et vire donc instantanément le montant exigé.
Conséquence :
Le montant de CHF 22 500.– versé est perdu.
Solution :
Conclure une cyberpolice correspondante couvrant le social engineering.

Que peut-on faire pour se prémunir ?

Les entreprises sont des cibles lucratives pour les escrocs. Par rapport aux particuliers, des sommes importantes peuvent y être détournées d'un seul coup. C'est pourquoi les hackers y consacrent plus de temps et agissent de manière plus ciblée et professionnelle que pour des particuliers. Ce sont surtout les services financiers qui sont ciblés. L'assurance responsabilité civile d'entreprise couvre les dommages causés à un tiers par la faute de l'assuré. Toutefois, seuls les dommages corporels et matériels ainsi que les dommages consécutifs qui en résultent sont assurés, mais pas les dommages économiques qui surviennent habituellement en relation avec les cyberrisques. C'est là que les solutions d'assurance cyberrisques interviennent. L'assurance cyberrisques couvre à la fois les dommages causés à des tiers et les dommages subis par l'assuré lui-même (dommages propres). Les dommages propres peuvent p. ex. découler d'actes criminels de tiers qui endommagent ou détruisent des données de l'assuré ou qui entravent, voire interrompent, l'activité commerciale. Une autre technique employée est celle de la tentative de chantage par ransomware : le hacker crypte des données et exige une rançon pour les décrypter.

En cas de sinistre, les assurances cyberrisques couvrent régulièrement la compensation des prétentions en dommages-intérêts justifiées ainsi que la défense contre les prétentions en dommages-intérêts injustifiées de tiers. Les frais de restauration du système informatique en cas de données, de programmes et de réseaux endommagés, bloqués ou détruits par une cyberattaque sont également remboursés. En cas d'interruption d'exploitation, la perte de gain ainsi que les autres coûts nécessaires à la poursuite de l'exploitation sont couverts. Le paiement du chantage peut être inclus dans la cyberpolice. Outre la compensation des dommages directement causés par le cyberincident, les coûts comme ceux liés au mandat d'une gestion professionnelle de crise, d'analystes de la criminalité informatique, d'experts en RP et d'avocats spécialisés, sont régulièrement couverts. Enfin, il convient de souligner que les preneurs d'assurance peuvent également collaborer avec leur partenaire informatique existant en cas de sinistre. Cette assurance prend alors en charge les coûts de ce partenaire informatique.

Demandez conseil à PROMRISK SA

Depuis toujours, PROMRISK SA, le courtier officiel d'AM Suisse, se consacre intensivement à la problématique des cyberrisques. Les cyberassurances ne sont présentes sur le marché que depuis quelques années et les produits varient énormément d'une compagnie d'assurance à l'autre. Soulignons que tous les cyberproduits ne conviennent pas à toutes les entreprises. Il faut analyser le risque au cas par cas en fonction de l'entreprise et trouver un partenaire d'assurance approprié. C'est pourquoi nous réalisons chaque année un nouveau comparatif complet des cyberassurances de toutes les compagnies, ce qui nous permet d'avoir toujours accès au meilleur produit du moment en fonction des besoins. Cela inclut également les obligations en cas de sinistre ainsi que le remplissage du questionnaire cyber.

Nous sommes spécialisés dans les cyberrisques de la branche de la construction métallique. Nous vous aidons et vous conseillons volontiers.
Tél. 044 851 55 66 ou
info@promrisk.ch
www.promrisk.ch ■