TEAM

Der Berg ruft

Voller Vorfreude traf sich das Intermakler-Team am 26. August frühmorgens zum alljährlichen Teamausflug. Mit dem Zug ging es von Bern nach Zermatt in Richtung Matterhorn, wo unsere Mitarbeitenden einen erinnerungswürdigen Tag verbrachten.

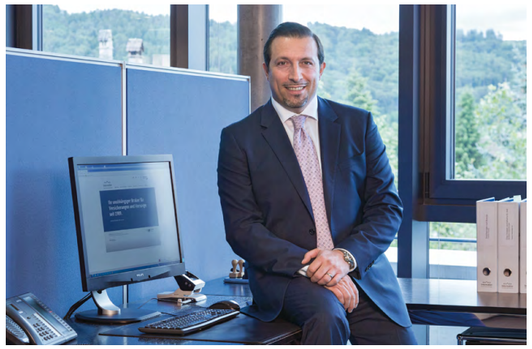
Die Familie Schüpbach in ihrem Element. Zu Fuss ging's durch die prächtige Bergwelt.

Für einmal selbst die Gefahr. Beim Tontaubenschiessen kam so manches (Nicht-)Talent hervor.

Im schönen Hotel Sonne in Zermatt gab's ein sommerliches Raclette.

Zufrieden und entspannt: das Intermakler-Team unisono.

Zwei neue Gesichter bei Intermakler



Gaspare Vescio

Versicherungsfachmann mit eidg. Fachausweis
Mandatsleiter, Mitglied des Kaders

Der Aufgeschlossene. Gaspare geht mit seiner positiven Art in neuen Herausforderungen so richtig auf. Identifikation und Dienstleistungsqualität stehen bei ihm an oberster Stelle. Entspannung findet er am Neuenburgersee, beim Spazieren, Baden und Grillieren – am liebsten an der Seite seiner Familie und Freunde.

Monika Lyner

Versicherungsfachfrau mit eidg. Fähigkeitszeugnis
Büroassistenz Administration

Die Vielseitige. Monika ist an vielen Fronten im Einsatz. Zu Hause hat sie ihre drei Kinder im Griff und bei Intermakler den Büroalltag. Die Wiedereinsteigerin ist jeden Tag topmotiviert und unterstützt mit viel Optimismus und Organisationstalent die Mandatsleiter. Nach Feierabend stehen Sport, Lesen und Konzerte auf ihrem Programm.

Impressum
Herausgeber: Intermakler AG, Worbstrasse 46, 3074 Muri bei Bern | Layout & Grafik: Sarah Hepp Grafikdesign | Konzept & Redaktion: Nik Schwab Communications
Auflage: 1'500 Exemplare | Druck: Vögeli AG, Langnau i.E.

Nr. 2/2016

Intermakler Bulletin 5

Angstmacherei oder echte Gefahr?

Die Schlagzeilen rund um Cyberattacken reissen nicht ab. Aber wie gefährlich sind die Angriffe aus dem Internet für ein «normales» Unternehmen? Was sind die Folgen? Wir beantworten die häufigsten Fragen zu diesem hochaktuellen Thema und zeigen auf, wie Sie sich schützen können.

Die Versicherung ist nur das Auffangnetz

von Gaspare Vescio Seit jeher schützen uns Barrieren, Empfangstheken und Zäune vor unwillkommenen Gästen. Aber die Furcht vor dem Spion in der Fabrik ist in den letzten Jahren der Angst vor dem Hacker auf dem Server gewichen. Die Versicherungsbranche antwortete mit Produkten, welche die finanziellen Folgen von Cyberattacken abdecken. Korrekterweise beginnt der Schutz aber auch in diesem Fall mit Hürden zur Verhinderung von Cyberattacken.

Denn Cyberrisk ist in erster Linie ein IT-Thema. Jedes Unternehmen muss zuerst seine digital mit der Aussenwelt verbundenen Systeme bestmöglich vor Schlupflöchern schützen. Eine Versicherung kommt dann zum Zug, wenn es den Angreifern gelungen ist die Hürden trotzdem zu überwinden. Sie ist das Auffangnetz bei finanziellen Schäden. Und diese sind beträchtlich: Cyberangriffe kosten die Schweizer Wirtschaft pro Jahr 537 Millionen Franken.

Die Cyberrisk-Versicherungen decken:

- den Eigenschaden: interne Kosten wie zum Beispiel für die Schadenbeseitigung oder die Betriebsunterbrechung
- den Drittschaden: die Haftpflichtkomponente

Der Eigenschaden ist in den meisten Fällen grösser und kann sich für KMUs als folgenschwer erweisen. Wann aber rechnet sich die Cyberrisk-Versicherung? Dafür gilt es zu analysieren, welche Angriffspunkte bestehen und was ihre finanziellen Folgen wären. Je nach Branche ist die Gefahrensituation sehr unterschiedlich.

GUT ZU WISSEN

Wann und für wen Cyberattacken weitreichende Folgen haben können:

- Alle Unternehmen, die vertrauliche Personendaten speichern (z.B. Banken, Versicherungen, öffentliche Institutionen wie Gemeinden, Altersheime oder Krankenhäuser) oder über umfangreiche, kundenspezifische Informationen verfügen (z.B. Telekommunikationsbranche, Detailhandel, Hotels/ Reiseveranstalter).
- Wenn der Umsatz davon abhängig ist, dass digitale Kanäle funktionieren, was vor allem bei eCommerce-Unternehmen (Online-Handel) der Fall ist.
- Beratungs- und Forschungsunternehmen, die durch den Verlust digitaler Daten oder geistigen Eigentums finanziellen Schaden erleiden.
- Versorgungsunternehmen wie Kraftwerke, Gas-, Wasser- und Stromversorger, die elektronisch ferngesteuert und überwacht werden.
- Produktionsunternehmen, die zur Auftragsabwicklung auf eine integrierte und funktionsfähige Betriebssteuerung angewiesen sind.

gaspare.vescio@intermakler.ch

Intermakler AG, Worbstrasse 46, CH-3074 Muri bei Bern
T +41 31 350 55 05, F +41 31 350 55 00
info@intermakler.ch, www.intermakler.ch

Intermakler
Versicherungen & Vorsorge

Die häufigsten Fragen zu Cyberrisk

WAS PASSIERT BEI EINEM CYBERANGRIFF?

Das Spektrum ist sehr breit. Schon lange bekannt und verbreitet ist «Phishing», wobei durch gefälschte E-Mails oder Websites versucht wird an vertrauliche Daten wie zum Beispiel Passwörter oder Bankdaten zu gelangen. Dies lässt sich durch richtiges Handeln der Betroffenen verhindern. Bedrohlicher, weil schwieriger abzuwehren, ist «Hacking». Hier nutzen die Täter Sicherheitslücken, um direkt in die Infrastruktur der Firma einzudringen. Dort sammeln, beschädigen oder löschen sie Daten. Immer häufiger werden Erpressungsversuche, wo für gestohlene, sensitive Daten ein Lösegeld verlangt wird. Zuletzt standen auch Ddos-Angriffe (Distributed Denial of Service) in den Schlagzeilen, bei denen der Betrieb durch die Überlastung der Netzwerke von aussen lahmgelegt wurde. Das führt dazu, dass Websites (z.B. Webshops), interne Anwendungen oder ganze Produktionsanlagen nicht mehr funktionieren.

WELCHE SCHÄDEN RICHTET EINE CYBERATTACKE AN?

Bei den finanziellen Folgen gilt es zwischen internen und externen Kosten zu unterscheiden.

Dem Eigenschaden zuzurechnen sind:

- Kosten für die Schadenbeseitigung, Wiederherstellung der Daten sowie des Systems (oftmals nur durch externe Unterstützung möglich)
- Betriebsunterbrechung, die einen Ertragsausfall nach sich zieht (häufig der grösste Schaden)
- Kosten für die Information der Dateninhaber sowie der Behörden
- Lösegeldzahlungen bei Erpressungsversuchen (selten)

Ausserhalb des Unternehmens:

- Schadenersatzforderungen von Drittparteien, die zu Schaden gekommen sind
- Anwaltskosten bei Haftpflichtprozessen

Einige Versicherungen vergüten auch Reputationsschäden.

DECKEN MEINE BESTEHENDEN BETRIEBSVERSICHERUNGEN DIE SCHÄDEN, DIE DURCH HACKER ENTSTEHEN?

GUT ZU WISSEN

Die bestehenden Versicherungen (Haftpflicht-, Sach- und EDV-Versicherungen) sind darauf zu prüfen, ob bereits eine Deckung besteht. In der Regel besteht über diese Verträge aber kein Versicherungsschutz. Jeder Fall ist individuell zu prüfen, vor allem auch hinsichtlich Vermögensschäden, die aufgrund eines Cyberangriffs entstehen.

BIN ICH HAFTBAR, WENN DIE DATEN EINES KUNDEN GESTOHLEN WURDEN?

Das lässt sich nicht allgemein beantworten. Wichtig ist, dass man als Unternehmen nicht fahrlässig handelt. Wenn Sie vertrauliche Daten gespeichert haben, ist es Ihre Pflicht diese gegen unerlaubte Zugriffe zu schützen.

Weitere Fragen und Antworten von unseren Versicherungsexperten finden Sie auf unserem Blog: **blog.intermakler.ch**

So schützen Sie das Unternehmen vor Cyberrisiken

1. Erfassen der Risiken und der Folgekosten
2. Analyse der bestehenden IT-Sicherheit
   Analyse der bestehenden Versicherungsverträge
3. Schliessen von IT-Sicherheitslücken
4. Versicherung für hohe Cyberrisiken

Die IT-Checkliste für KMUs

Diese und weitere Tipps finden Sie im «Merkblatt IT-Sicherheit für KMUs», verfasst von der Melde- und Analysestelle Informationssicherung MELANI der Bundesverwaltung.

Vor allem KMUs verfügen oft nicht über das nötige Fachwissen, um sich vor Cyberrisiken zu schützen. IT-Experte Dominique Merz klärt auf, welche Massnahmen zu ergreifen sind.

- ☑ **Eine Firewall schützt Ihr Unternehmensnetzwerk**
  Die Firewall muss so eingerichtet sein, dass sämtlicher eingehender und ausgehender Datenverkehr unterbunden wird, ausser dem explizit zugelassenen.
- ☑ **Potenziell schädliche E-Mails mit einem Gateway bzw. Spam-Filter blockieren**
  Falls Ihr Unternehmen beispielsweise nur in der Schweiz tätig ist, wäre es eine Option, E-Mails aus bestimmten Ländern (welche z.B. bekannt für ein hohes Spamaufkommen sind) abzuweisen.
- ☑ **Auf jedem Computer ein Virenschutz**
  Stellen Sie sicher, dass sich dieser regelmässig aktualisiert, und lassen Sie ihn regelmässig einen vollständigen Systemscan durchführen (z.B. wöchentlich oder monatlich).
- ☑ **Täglich ein Backup aller Daten durchführen**
  Überprüfen Sie das Backup regelmässig auf seine Funktionsfähigkeit. Bewahren Sie die Backups an einem sicheren Ort und physisch getrennt vom Server auf. Behalten Sie die Vorgängerversionen des Backups über einen bestimmten Zeitraum.
- ☑ **Automatische Updates aktivieren**
  Alle Computer und Server im Netzwerk müssen regelmässig Sicherheitsupdates durchführen und sämtliche installierte Software aktualisieren. Veraltete Software ist ein beliebtes Einfallstor für Schadsoftware.
- ☑ **Definieren Sie eine Passwort-Policy und setzen Sie diese technisch um**
  Die Mitarbeitenden sollten pro Anwendung ein unterschiedliches Passwort benutzen.
- ☑ **Achtung bei Cloud-Diensten**
  Sensible Daten sollten nie in der Cloud abgelegt, sondern nur lokal gespeichert werden.
- ☑ **Kollektiv-E-Banking-Verträge schützen Ihre Bankkonten**
  Bei den meisten E-Banking-Systemen gibt es die Möglichkeit von Kollektiv-E-Banking-Verträgen. Hierbei wird eine Zahlung über einen zweiten E-Banking-Vertrag freigegeben. Sprechen Sie mit Ihrer Bank über entsprechende Möglichkeiten.

NETZWERK

«Bei unbekannten Internetshops ist ein gesundes Misstrauen berechtigt.»

Wie gross ist die Gefahr, wenn wir privat im Internet unterwegs sind? Darüber sprechen wir mit IT-Experte Dominique Merz.

Man liest viel über Viren und trojanische Pferde. Vor welchen Gefahren müssen wir wirklich Angst haben?
Aktuell sind sogenannte CryptoLocker Tools die grösste Bedrohung. Per E-Mail versendete Programme verschlüsseln die Daten der Benutzer und machen diese unbrauchbar. Wenn kein Backup vorliegt, sind die Daten nicht mehr zu retten.

Was sind die häufigsten Sicherheitslücken bei Privatpersonen oder Fehler, die sie begehen?
Viele Benutzer verwenden bei allen Logins das gleiche Passwort, was man unbedingt ändern sollte. Der unvorsichtige Umfang mit E-Mails und eine ungenügende Datensicherung sind zwei weitere häufige Fehler.

Was muss ich tun, wenn ich merke, dass ein Virus meinen PC befallen hat?
Sofort die Daten sichern und den PC herunterfahren. Einzig mit einer Formatierung der Harddisk und einer Neuinstallation des PCs ist man zu 100% sicher, dass der PC virenfrei ist.

Wir bewegen uns jeden Tag im Internet. Welches Produkt empfehlen Sie für den Privatgebrauch?
Grundsätzlich ist die Schutzsoftware den neuen Computerviren immer einen Schritt hinterher und schützt nur gegen bereits existierende Viren. Pro Tag entstehen weltweit schätzungsweise 350'000 neue Varianten von Computerviren.
Privat verwende ich einen Virenschutz von Trend Micro.

Ist es wahr, dass man die Webcam abdecken sollte?
Ich persönlich kenne keinen Fall, bei welchem die Webcam per Remotezugriff missbraucht wurde. Zudem ist die Webcam grösstenteils auf das Gesicht des Benutzers ausgerichtet – der Schaden hält sich also in Grenzen.

Viele Menschen haben Angst, ihre Kreditkarte im Internet anzugeben. Ist die Angst berechtigt?
Bei neuen, unbekannten Internetshops ist ein gesundes Misstrauen berechtigt. In Shops, bei welchen ich bereits Kunde bin, verwende ich die Kreditkarte ohne Bedenken. Den möglichen Schaden kann man mit einer Kreditkarte mit einer kleinen Ausgabelimite begrenzen.

Was machen Sie persönlich, um sich online zu schützen?
Ich surfe bewusst im Internet und gehe vorsichtig mit E-Mails um. Ausserdem verwende ich ein Standard-Virenschutzprogramm, benutze unterschiedliche Passwörter und sichere meine Daten in unterschiedlichen Ablagen.

JPAG Johner + Partner AG www.jpag.ch

Johner + Partner AG berät Unternehmen, unter anderem auch die Intermakler AG, in sämtlichen IT- und Sicherheitsfragen. www.jpag.ch