**Die Presse** 09.02.2017
Erscheinungsland: Österreich | Auflage: 76.360 | Reichweite: 315.000 (4,3) | Artikelumfang: 39.288 mm² Seite: 19 1/2

**Thema:** Anwaltskanzlei PHH Wien
**Autor:** Christine Kary

# Cybercrime: Firmen reagieren oft zu spät

## **Studie.** Europäische Unternehmen bemerken Hackerattacken im Schnitt nach 15 Monaten.

VON CHRISTINE KARY

**Wien.** Vergangenen Sonntag traf es das Parlament, im November zwei Ministerien: Hackerattacken häufen sich, auch in Österreich. In Relation zum BIP gibt es hier sogar überproportional viele Cyberangriffe: Laut einem aktuellen Report über Cyberbedrohungen, den das IT-Sicherheitsunternehmen FireEye und der Risikoberater Marsh & McLennan erstellt haben, werden Finanzbranche, Telekommunikation, herstellende Industrie und öffentliche Stellen besonders oft von Hackern angegriffen – und vier Prozent der Attacken, die 2016 europaweit in diesen Sektoren beobachtet wurden, richteten sich gegen Ziele in Österreich.

„Österreich ist damit mehr als doppelt so stark betroffen wie Deutschland", sagt Christian Berger, Geschäftsführer von Marsh Austria, zur „Presse". Auf Deutschland entfielen laut der Studie 19 Prozent der Attacken, die übliche Österreich-Deutschland-Relation von eins zu zehn trifft hier also nicht zu. Absolut gesehen, sind deutsche Einrichtungen laut dem Report das häufigste Ziel von Cyberkriminellen, gefolgt von belgischen (16 Prozent) und britischen (zwölf Prozent).

### Hacker lesen monatelang mit

Die Firma Marsh berät nicht nur bei der Risikovorsorge. Sie vermittelt zudem Industrieversicherungen, auch gegen Cyberattacken. Versichern lassen könne man sich nicht nur gegen die unmittelbaren Schäden, sondern auch gegen Haftungsrisiken die entstehen, wenn Dritte zu Schaden kommen, sagt Berger. Das Interesse daran nehme zu – noch wichtiger sei den meisten Unternehmen jedoch etwas anderes: „Dass jemand ins Haus kommt und die Sache managt." Also nach einer Cyberattacke die IT wieder zum Laufen bringt. Denn vor Betriebsunterbrechungen fürchten sich viele am meisten – noch viel mehr als etwa vor Datenklau.

Insgesamt steigt laut Berger die Sensibilität für das Thema, Unternehmen tun aber noch zu wenig, um sich zu schützen. Das beginnt damit, dass es Firmen oft viel zu spät bemerken, wenn ihre IT gehackt wurde. Bis ihnen das auffällt, dauert es laut dem Report in Europa im Schnitt 15 Monate – dreimal so lang wie im weltweiten Durchschnitt. Damit erhöht sich das Schadenspotenzial: Kriminelle können zum Beispiel monatelang das Rechnungswesen eines Unternehmens ausloten, um dann unauffällig Buchungen zu ihren Gunsten hineinzuschummeln. Oder sie lesen interne E-Mails mit und stellen sich in aller Ruhe auf den Umgangston ein, der im Konzern herrscht. Den miesen Trick, der dann folgt, kennt man als „Fake CEO Fraud": Der Betrüger schlüpft in die Rolle des Chefs, zieht den Buchhalter scheinbar bei einer heiklen Mission ins Vertrauen und weist ihn unter dem Siegel der Verschwiegenheit an, eine hohe Summe auf ein Konto zu überweisen. So geschehen etwa beim heimischen Flugzeugkomponentenhersteller FACC, der Anfang des Vorjahres auf diese Weise um 50 Millionen Euro erleichtert wurde.

Zahlenmäßig häufiger sind jedoch andere Formen der Cyberkriminalität. Etwa sogenannte DDoS-Attacken – so etwas war es wohl auch, was vergangenen Sonntag die Parlamentshomepage vorübergehend lahmlegte. Dabei werden Webseiten mit Anfragen überschüttet, bis sie ausfallen – meist, um „Schutzgeld" zu erpressen. Auch Ransomware ist stark im Kommen: Endgeräte werden gesperrt und Daten verschlüsselt – und für die Entschlüsselung Geld verlangt (siehe auch Artikel rechts).

Von den Attacken betroffen sind längst nicht mehr nur Großfirmen. Vor allem Cyberbetrug richte sich oft gegen kleinere Unternehmen, sagt Berger. Auch, weil diese oft weniger gut vorbereitet sind und dort leichter Panik ausbricht – was die Erfolgsaussichten der Kriminellen erhöht.

Datendiebstahl betrifft dagegen meist Großfirmen. Mittelständler können dabei jedoch ebenfalls zum Angriffsziel werden: Sind sie Zulieferer, haben sie oft Datenschnittstellen zu großen Unternehmen, das mache sie zum potenziellen „Einfallstor" für Cyberattacken, sagt Berger. Auch in solchen Fällen können ihnen Haftungsfolgen drohen.

# Hackern das Leben schwer machen

## Simple Vorsichtsmaßnahmen genügen oft, sagen Experten.

**Wien.** „Kein Lösegeld für Daten zahlen", rät Mathias Preuschl, Anwalt und Cybercrime-Experte, Opfern von Cyber-Erpressern. Richtig wäre folgende Reaktion: „Die Attacke anzeigen, die Sicherheitslücken schließen. Und sofort alle Betroffenen informieren." Cyberattacken anzuzeigen, wird übrigens bald Pflicht: Bis 2018 muss die EU-Richtlinie zur Netz- und Informationssicherheit umgesetzt werden, und diese sieht eine Meldepflicht vor.

Dass die Realität jedoch oft anders aussieht, ist Preuschl klar: „Viele zahlen, weil es nicht anders geht." Deshalb, „und weil man sich dafür geniert", sei auch die Dunkelziffer bei Cybercrime so hoch. Bei den potenziellen Opfern ortet der Jurist ein „klassisches duales Problembewusstsein": Professionell gemanagte Unternehmen seien meist gut geschützt, bei vielen KMU und Privatpersonen herrsche dagegen die Ansicht vor, man sei für Kriminelle ohnehin uninteressant.

„Das stimmt aber nicht. Etwa beim Identitätsdiebstahl ist jeder gleich viel wert." Cybercrime habe hochgradig professionelle Strukturen: Mit Kreditkartendaten werde schwunghaft gehandelt, samt

**Die Presse** 09.02.2017
Erscheinungsland: Österreich | Auflage: 76.360 | Reichweite: 315.000 (4,3) | Artikelumfang: 39.288 mm² Seite: 19 2/2

**Thema:** Anwaltskanzlei PHH Wien
**Autor:** Christine Kary

regelrechten Abverkäufen kurz vor dem Ablaufdatum der Karten. „Und einen Cyberangriff muss man nicht selber machen, man kann ihn im Darknet bestellen."

### „Hacker sind faul"

Aber wie schützt man sich? Das ist an sich nicht neu: E-Mail-Anhänge im Zweifel nicht öffnen, komplizierte Passwörter verwenden und oft ändern. Und Daten redundant sichern – fehlen Sicherungskopien, wird man erpressbar.

Veraltete Software sei ein weiterer Schwachpunkt, sagte IT-Security-Spezialist Peter Kleissner bei einer Veranstaltung zum Thema in der Anwaltskanzlei PHH. „90 bis 95 Prozent aller Hackerattacken könnten verhindert werden, wenn die Unternehmen ihre Betriebssysteme und Software up to date hielten."

Kleissner war selbst Hacker, heute berät er Unternehmen beim Schließen ihrer Sicherheitslücken. Sein grundsätzlicher Tipp: „Hacker sind faul. Wer es ihnen schwer macht, ins IT-System einzudringen, wehrt schon viel ab. Denn es gibt genug andere potenzielle Opfer." (cka)