Cyberkriminalität

Homeoffice als Risikofaktor

Seit bald einem Jahr befinden sich so viele Menschen im Homeoffice wie nie zuvor. Dadurch wächst für Unternehmen und andere Organisationen auch die Gefahr für Cyberkriminalität. Allerdings können Risiken auch minimiert werden, so IT-Security-Experte Florian Skopik gegenüber ORF.at.

Online seit heute, 6.08 Uhr

Auch wenn es im Bewusstsein vieler noch nicht angekommen ist: Cyberkriminalität ist auch in Österreich ein ernstes Problem. Laut dem Innenministerium gab es im vergangenen Jahr fast 28.500 gemeldete Fälle bzw. rund 78 Anzeigen pro Tag. Dabei trifft es immer wieder auch große Organisationen: zuletzt unter anderem die Palfinger-Group, im Vorjahr auch A1 Telekom Austria und das Außenministerium. Die Dunkelziffer dürfte enorm sein. Eine jüngere Studie von KPMG geht davon aus, dass 57 Prozent aller Firmen binnen der letzten zwölf Monate betroffen waren.

Laut Skopik, Leiter des Forschungsbereichs Cyber Security am Austrian Institute of Technology (AIT) im Center for Digital Safety & Security, können Angriffe auf die IT-Infrastruktur für Unternehmen aller Branchen und Größen gravierende Folgen haben. Finanzielle Schäden durch Betrug seien hier nur der Anfang. Cyberangriffe können in schlimmen Fällen den ganzen Betrieb lahmlegen, es könnten Firmengeheimnisse geleakt und systemrelevante Infrastruktur gefährdet sein. Auch Strafen bei Brüchen der Datenschutz-Grundverordnung (DSGVO) der EU können existenzbedrohend sein.

Reuters/Jason RedmondEin anschauliches Beispiel für die potenziell gravierenden Auswirkungen von Cyberangriffen
auf Firmen stammt aus dem Jahr 2017: Der „NotPetya“-Angriff legte damals Dutzende Firmen, unter anderem den Reedereikonzern Maersk, tagelang lahm

Schrift überdauert

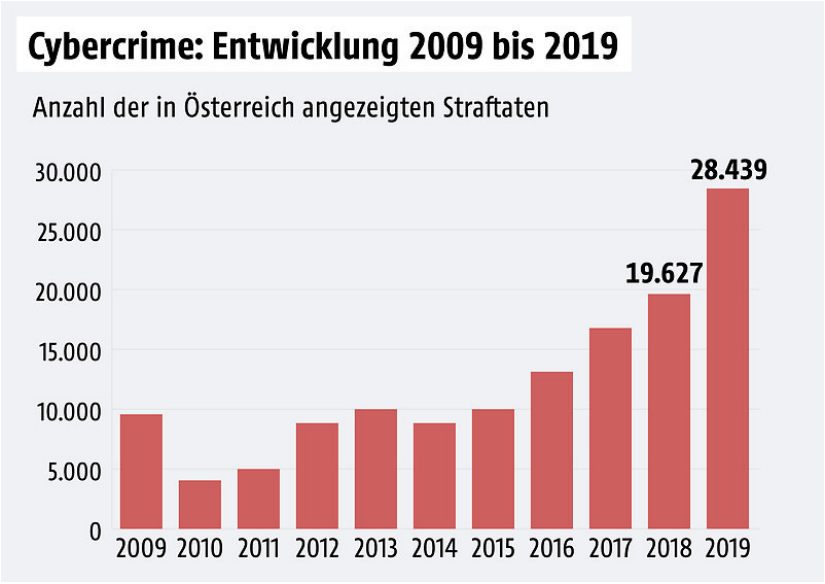
Daher ruft Skopik dazu auf, geeignete Maßnahmen zu ergreifen – gerade auch für das Personal im Homeoffice: „Daten und Informationen in Büros und Firmenräumlichkeiten zu schützen ist schon schwierig genug. In gut

abgesicherten Räumen passiert bereits viel, im Homeoffice ist das Risiko noch größer.“ Entscheidend dabei: „Wenn Personal mit firmensensitiven Informationen arbeitet, erstreckt sich das Büro in das private Arbeitszimmer der Mitarbeiterinnen und Mitarbeiter. Entsprechend müssen Arbeitgeber dort für Sicherheit sorgen.“

Was die aktuelle Ausnahmesituation anbelangt, sieht er mehrere besonders gewichtige Punkte. Einer davon ist, dass mehr denn je schriftlich und asynchron kommuniziert wird. Heikle Gespräche finden nicht mehr in Besprechungsräumen statt, sondern digital. Das sorgt einerseits dafür, dass mehr sensibles, schriftliches Material existiert. Andererseits öffnet es dem Betrug über Phishing-Attacken Tür und Tor.

Wenn die Kaffeeküche fehlt

Phishing-Attacken sind laut Skopik „eines der größten Risiken“ und den meisten bekannt. Dabei wird versucht, mit gefälschten Websites, E-Mails und Kurznachrichten an Daten zu kommen, Menschen z. B. zu falschen Überweisungen zu bewegen oder ihnen andere Infos zu entlocken. Die Klassiker seien falsche Zahlungsanweisungen und angstmachende E-Mails, seit geraumer Zeit auch mit Coronavirus-Fokus. Problematisch ist dabei derzeit, dass im Homeoffice der Gegencheck durch Zuruf mit den Kolleginnen und Kollegen bzw. der IT-Abteilung wegfällt. Wer alleine im Homeoffice sitzt, ignoriert seine Skepsis womöglich eher und tappt in eine Falle.



Grafik: APA/ORF.at; Quelle: onlinesicherheit.gv.at

Das kann durchaus passieren, denn längst sind viele Phishing-Versuche äußerst raffiniert gestaltet und zielen mit Insiderwissen auf bestimmte Firmen ab. Nicht zu vernachlässigen sei auch der menschliche Faktor: „Wir sind alle in einer Ausnahmesituation, viele Kämpfen mit Homeschooling oder Kinderbetreuung, viel Arbeit wird unter Stress und mitunter erst tief in der Nacht erledigt, das alles verbessert die Lage nicht“,

so Skopik. Deswegen gilt: Sollte irgendeine Abweichung misstrauisch machen, lieber einmal zu viel als zu wenig bei der IT nachfragen.

Keine Arbeit auf Privatgeräten

Der zweite zentrale Punkt für ein sicheres Homeoffice ist, dass Arbeitgeber die entsprechenden Gerätschaften und Infrastruktur zur Verfügung stellen müssen. Konkret bedeutet das laut Skopik: entsprechend eingerichtete Firmenlaptops, die nur für die Arbeit verwenden werden, Firmen-Smartphones für das datenschutzkonforme Speichern von Firmenkontakten und eine VPN-Verbindung ins Unternehmensnetzwerk für sicheren Datenaustausch.

HELP
Komfortable Back-up-Lösungen im Test

Auch im Homeoffice sollten regelmäßig Back-ups gemacht werden – bei einem Ransomware-Angriff können diese Gold wert sein. Allerdings sollten Daten nur über Mittel und Wege übertragen werden, die von der Firma zur Verfügung gestellt werden. Von privaten Dropbox-Accounts und ähnlichen Services sollte man absehen. Grundsätzlich gilt es, die Software aufmerksam zu wählen. Insbesondere viele Gratisservices haben einen zweifelhaften Ruf bezüglich der Datenverarbeitung und verwerten potenziell sensible Firmendaten auf unerwünschte Weise.

Arbeit auf Privatgeräten zu erledigen sei tabu, „im schlimmsten Fall teilen sich auch noch mehrere Familienmitglieder ein Gerät“. Bei Privatgeräten ist die Wahrscheinlichkeit wesentlich höher, dass diese nicht ordentlich upgedatet sind (was wiederum ein Sicherheitsrisiko darstellt), ein Gerät bei der Privatnutzung kompromittiert wird oder sowieso schon ist. Dazu kommt: „Teilweise beginnen Leute auch unwissentlich damit, private und professionelle Daten zu vermischen“, so Skopik. Das kann nicht nur riskant sein, sondern auch peinlich enden – z. B. wenn auf einmal Daten aus privaten Cloud-Services durch automatische Synchronisationsvorgänge oder aus Versehen bei der Firma landen.

Passwörter und Misstrauen als Erstmaßnahme

Laut Skopik gibt es auch einige Punkte, mit denen jeder Einzelne aktiv für mehr Sicherheit sorgen kann – etwa indem man sich bei Phishing-Versuchen auf Warnsignale sensibilisiert. Man müsse sich fragen: „Sind alle Namen, Absenderadressen und Daten korrekt? Wenn es irgendwelche Links gibt – wie schauen diese aus und wo führen diese hin? Enthält der Text Grammatikfehler? Werden unrealistische Dinge versprochen? Macht der Text Angst? Ist er drängend oder droht er mit Sanktionen?“ Sollte es Anlass für Zweifel geben, sollten solche E-Mails lieber einmal zu viel als zu wenig in die IT-Abteilung oder mit Vorgesetzten abgeklärt werden.

Ein weiterer wichtiger Punkt seien sichere Passwörter. Diese müssen vor allem lang sein und dürfen keinem Muster entsprechen. Ein guter Trick sei beispielsweise, sich einen Satz zu merken und die Anfangsbuchstaben in Groß- und Kleinschreibung als Passwort zu verwenden. Optimalerweise integriert man in diesen Satz auch Zahlen und Sonderzeichen.

Namen und Geburtsdaten sind tabu, ebenso das Wiederverwenden von Passwörtern bei unterschiedlichen Diensten. Tunlichst vermeiden sollte man jedenfalls, für private und berufliche Anwendungen die gleichen Passwörter zu verwenden. Skopik empfiehlt auch die Verwendung von Passwort-Managern wie KeePass oder, wo möglich, Zwei-Faktor-Authentifizierung.

Eine Art Präventionsparadox

Letzten Endes sei IT-Sicherheit immer ein Geben und Nehmen: Einerseits müssten Arbeitgeber für sichere Rahmenbedingungen, die richtige Ausstattung und geschultes Personal sorgen, andererseits braucht es die Bereitschaft der Beschäftigten, sich mit der Materie zu beschäftigen, diese ernst zu nehmen und in den richtigen Momenten skeptisch zu sein. Aber: „Sicherheit kann nicht ausschließlich auf den Mitarbeiter abgewälzt werden“, so Skopik. Arbeitgeber müssen hier gezielt Schulungen anbieten und Richtlinien festlegen. Gerade bei kleinen Unternehmen würden Trainings mehr bringen als teure technologische Maßnahmen.

Wie bei der Pandemie wird auch bei der Cybersecurity eine Art Präventionsparadox schlagend: Als vorbeugende Maßnahme wirkt sie, aber gerade wenn über längere Zeit kein Schaden eintritt, wird ihr immer weniger Bedeutung beigemessen. Treffend ist auch der Vergleich mit einer Versicherung: Wenn man sie im Schadensfall braucht und sie nicht hat, ist es zu spät. Im Endeffekt sei IT-Sicherheit immer eine Sache der Vorbereitung, so Skopik: „Angst muss man keine haben, die ist ein schlechter Berater. Man muss vor allem seine Hausaufgaben machen.“

® ORF.at, 15.02.2021 Saskia Etschmaier