Risiken im Homeoffice steigen

Sicherheit. Cyberrisiken sind gerade jetzt allgegenwärtig. Vor allem KMU sind im Visier von Cyberkriminellen

Mit dem Shutdown Mitte März wurden viele Mitarbeiter unvorbereitet ins Home-Office geschickt. Laut einer gemeinsamen Umfrage von TQS Research & Consulting und Talk Online Panel unter 1.000 Befragten in der zweiten Aprilhälfte hat ein Viertel der Österreicher seit Beginn der Ausgangsbeschränkungen von zu Hause aus gearbeitet, 40 Prozent von ihnen hatten das davor noch nie getan, weitere 20 Prozent nur selten. 86 Prozent können von daheim aus Job und Familie gut oder sehr gut unter einen Hut bringen, 70 Prozent macht die Arbeit daheim Spaß - und wollen auch nach der Corona-Pandemie diese Möglichkeit verstärkt nutzen.

Gleichzeitig haben die Millionen Menschen im Homeoffice den IT-Experten schlaflose Nächte beschert. Auf das Unternehmensnetzwerk wird via VPN-Tunnel zugegriffen, viele Mitarbeiter nutzen dafür ihr privates Notebook, oftmals ohne Firewall oder ohne aktuelle Anti-Viren-Programme. Das machte es Cyberkriminellen besonders einfach, mit Phishing-Attacken oder Schadsoftware illegal auf Rechner zuzugreifen. Manfred Bartalszky, Vorstand der Wiener Städtischen, zuständig für die Marke s Versicherung: „Gerade in der Coronakrise haben wir ein extrem steigendes Risiko für Unternehmen aufgrund der vermehrten Nutzung von Homeoffice. Warum? Die IT-Sicherheit zu Hause ist meist nicht so stark ausgeprägt, daher ist es umso wichtiger, das Bewusstsein für Cyberrisiko bei unseren Kundinnen und Kunden zu schärfen."

AIMSTOCK/ISTOCKPHOTO.COM

Laut KFV waren rund 80 Prozent der KMU in Österreich in den letzten Jahren Ziel von Cyberangriffen

Cyberattacken steigen

Für Cyber-Kriminelle bietet die aktuelle Situation nahezu ideale Voraussetzungen, um Profit aus der Krise zu schlagen. So schnellte nach Erhebungen von G Data Cyber Defense, einem der führenden Anbieter von Virenschutz-Software in Deutschland, die Zahl der Cyber-Attacken im März diesen Jahres im Vergleich zum Februar um rund 30 Prozent in die Höhe. Dabei handelt es sich nur um die entdeckten Angriffe. Die Gesamtzahl der Angriffe dürfte um ein Vielfaches höher liegen und der damit verbundene Schaden etliche Millionen Euro betragen.

Weltweit ist zudem ein dramatischer Anstieg von Phishing-Webseiten rund um das Thema Corona zu verzeichnen. Von Jänner auf März sind diese Internetseiten um 350 Prozent auf rund 522.000 Phishing-Webseiten angewachsen. Auch Spam-Mails mit Stichwörtern wie „Corona" und „Covid-19" sind massiv im Umlauf und bergen eine immense Gefahr, Opfer einer Cyberattacke zu werden.

Sicherheit ausbaufähig

Bei Österreichs Klein- und Mittelunternehmen ist die IT-Sicherheit noch stark ausbaufähig. Das zeigt auch eine Studie des Kuratoriums für Verkehrssicherheit (KFV) aus dem vergangenen Jahr. Laut KFV waren rund 80 Prozent der KMU in Österreich in den letzten Jahren Ziel von Cyberangriffen. Tatsächlich einen Schaden erlitten 2019 beachtliche 39 Prozent. Der Mehrheit der betroffenen Unternehmen, die in der KFV-Studie auch einen finanziellen Verlust beziffern konnten oder wollten, entstanden jeweils Schäden zwischen 130 Euro und 10.000 Euro, wobei einige der Befragten Gesamtschäden von sogar bis zu

IAN EHM

„Wir müssen das Bewusstsein für Cyberrisiken bei unseren Kundinnen und Kunden schärfen"

Manfred Bartalszky
Vorstand Wiener Städtische

150.000 Euro angaben. Mit zunehmender Unternehmensgröße steigt auch der realisierte Schaden. Gerade Klein- und Mittelunternehmen bemerken häufig nicht, dass sie Opfer von Cybercrime geworden sind, oft werden Schäden auch aus Angst vor Imageverlust nicht mal gemeldet.

Die Erfahrung der Cybercrime-Experten der Wiener Städtischen zeigen, dass viele heimische Unternehmen die Gefahren aus dem Netz noch immer unterschätzen: „Weniger als ein Drittel der Unternehmen, mit denen wir diesbezüglich in Kontakt waren, achten auf die Verschlüsselung von Datenträgern und nur rund 60 Prozent verfügen über einen IT-Sicherheitsverantwortlichen. Dieser ist jedoch gemäß der Vorgaben der DSGVO verpflichtend", so Bartalszky. Und: Erst rund jedes vierte Unternehmen in Österreich hat eine Versicherung gegen Cyberangriffe abgeschlossen.

STEPHAN SCOPPETTA

Sechs Tipps gegen Cyberangriffe

Jeder ist ein Angriffsziel
Machen Sie sich bewusst, dass auch Sie ein potenzielles Ziel für Angriffe sind. Allzu oft sehen sich die Menschen nicht als Ziel für Angreifer und sind deshalb nicht wachsam genug.

Nicht auf Mail-Links klicken
Die einfachste Möglichkeit, Phishing-Betrug zu vermeiden, besteht darin, niemals auf einen Link in einer E-Mail zu klicken, wenn man diese nicht zuordnen kann.

Virenschutz-Software einsetzen
Stellen Sie sicher, dass Sie eine aktuelle Antivirus-Software von einem vertrauenswürdigen Anbieter installieren und verwenden Sie nicht zwei Antivirus-Programme gleichzeitig auf Ihrem Gerät.

Regelmäßige Back-ups machen
Sichern Sie Ihre Daten, indem Sie sie an einen anderen Speicherort kopieren. So verliert man bei einer Cyberattacke nicht alle Daten und kann die Geschäftstätigkeit fortsetzen.

Vorsicht bei öffentlichen WLAN-Netzwerken
Wenn Sie über einen öffentlichen WLAN-Hotspot surfen, dann sollten Sie sicherstellen, dass Sie eine VPN-Verbindung (Virtual Private Network) nutzen. Ohne VPN-Verbindung können Cyberkriminelle sehr leicht Daten von Ihrem Gerät abgreifen.

Daten verschlüsseln
Um sensible Daten wie Bankverbindungen und Passwörter zu schützen, ist eine Verschlüsselung dieser Daten jedenfalls ratsam.

„Mit dem Benutzerkomfort steigt das Risiko "

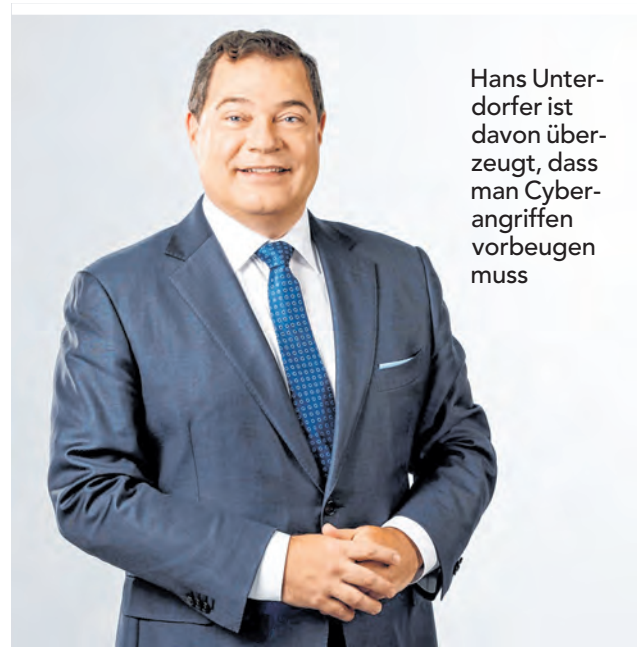
Hans Unterdorfer, CEO der Tiroler Sparkasse, über Internetkriminalität und die Absicherung möglicher Schäden durch Cyberattacken

Wie gefährdet sind heimische Haushalte und Unternehmen, Opfer von Internetkriminalität zu werden?
Hans Unterdorfer: Die aktuelle Statistik des Innenministeriums zeigt eine starke Zunahme der Internetkriminalität. Die gemeldeten Cybercrime-Fälle stiegen im vergangenen Jahr um 45 Prozent. 2019 wurden in diesem Bereich 28.439 Straftaten angezeigt. Die Dunkelziffer liegt laut Experten sogar deutlich höher. In der aktuellen Krise hat das Ausweichen auf arbeiten im Homeoffice mit externen Zugängen zu Firmennetzwerken vielen Unternehmen das Problem noch einmal mehr bewusst gemacht.

Worin liegen Ihrer Meinung nach die Gründe für die Zunahme von Cyberangriffen auf Privatpersonen und Unternehmen?
Leider gehen viele von uns immer noch sehr sorglos mit den neuen Technologien um. Ein gutes Beispiel sind Passwörter, mit denen wir Zugänge auf Handys oder Computer schützen sollten. Das meist genutzte ist immer noch „123456". Nur eine kleine Veränderung, wie das Einbauen eines Buchstabens, würde das Passwort um ein Vielfaches sicherer machen. Diese Schwachstelle nutzen Angreifer.

Mit einer eigenen Versicherung bieten Sie Schutz für Unternehmen zum Thema Cybercrime an. Welche Vorteile bietet diese?
Mit der s Cyber-Protect stellen wir als Sparkassengruppe eine maßgeschneiderte Lösung für Klein- und Mittelunternehmen zur Verfügung. Diese Polizze besteht aus verschiedenen Bausteinen, die sich nach dem Bedarf des jeweiligen Unternehmens richtet. Versichert sind unter anderem: Datenschutzverletzungen, Betriebsunterbrechung, Verletzung der Geheimhaltungspflicht, Cyber-Erpressung, Krisenmanagement, Datenverlust, Datenbeschädigung und Datendiebstahl oder auch Gefährdung der Netzwerksicherheit. Die s Cyber-Protect bietet zudem einen Sofort-Support durch das Cyber Center – 24 Stunden am Tag, sieben Tage die Woche. Und die Kosten sind wirklich überschaubar.

Können Sie die Kosten an einem Beispiel festmachen?
Wenn Sie zu Beispiel einen Metallbaubetrieb mit einem Jahresumsatz von 500.000 Euro hernehmen, dann beträgt die monatliche Prämie lediglich 27 Euro (Basisdeckung) bei einer Versicherungssumme von 100.000 Euro. Im Vergleich zu den finanziellen Folgen eines Cyber-Angriffes zahlt sich diese Investition mit Sicherheit aus.



THOMAS STEINLECHNER

Hans Unterdorfer ist davon überzeugt, dass man Cyberangriffen vorbeugen muss