Cybercrime und Datenschutz

Sicher?

Die Daten in der Cloud, Software im Online-Abo, die Telefonanlage virtuell – einfach zuhause eingeloggt und los. Viele Beschäftigte konnten dank pragmatischer Lösungen mehr oder weniger nahtlos ins Homeoffice wechseln. Höchste Zeit, in Sachen Sicherheit nachzujustieren.

Fehlender Passwortschutz, unverschlüsselte Datenübertragung, veraltete Datenbankstandards, private Geräte ohne ausreichenden Virenschutz – Dennis Schünke und Bernd Dettmers von der Oldenburger CSX-Academy kennen die häufigsten Sicherheitslücken der pandemiebedingten High-Speed-Digitalisierung. Und sind einer Meinung: „Wenn Schnelligkeit vor Sicherheit geht, kann das auf Dauer gefährlich werden. Angriffe durch Ransomware sind das größte Risiko zurzeit." Betrüger schicken massenhaft Mails mit „infizierten" Anhängen. Öffnet man sie, werden alle erreichbaren Daten verschlüsselt – den Code gibt's gegen Lösegeld. Vielleicht. Der Landkreis Anhalt-Bitterfeld rief kürzlich den Katastrophenfall aus, weil ein Schadsoftwarebefall große Teile der Verwaltung lahmgelegt hatte. Kfz-Zulassung, Elterngeldanträge – nichts ging mehr.

„Mit dem Wechsel ins Homeoffice verlassen Mitarbeitende die Sicherheitszone des Unternehmens", erklärt Dettmers; erst recht an privaten Endgeräten. Ein Zugriff per Virtual Private Network (VPN) kann in diesem Fall – korrekt eingerichtet – die Sicherheit erhöhen. „Am besten findet darüber der komplette berufliche Netzwerkverkehr statt. Auch das Abrufen von Mails, Surfen, der Datenzugriff." So profitieren Nutzer automatisch von den Sicherheitssystemen des Unternehmens. Ein solches Setup ist auch für kleine und mittlere Betriebe bezahlbar.

Ebenso wichtig: der Faktor Mensch. Dettmers und Schünke sind darauf spezialisiert, Mitarbeitende in Unternehmen zu sensibilisieren. In „gamifizierten" Online-Trainings und durch Test-Angriffe. „Es reicht, wenn eine Person die falsche Entscheidung trifft, das Makro in einem Worddokument zu laden", betont Schünke. Das passiert schnell, denn die Angriffe werden

Grafik: CSX-Academy GmbH

immer mehr – und raffinierter. Wichtig im Schadensfall: Sofort die Endgeräte vom Netzwerk trennen und die IT informieren. Dafür muss die Unternehmenskultur stimmen. Und das Briefing. Die CSX-Academy hat eigens Infoposter fürs Homeoffice entworfen. Davon profitieren Mitarbeitende auch privat – wer will seine persönlichen Daten schon in Betrügerhand wissen. Zwei-Faktor-Authentifizierung und sichere Passwörter sollten Standard sein.

2020 auch oft vernachlässigt: der Schutz persönlicher Daten. Dennis Schünke, selbst externer Datenschutzbeauftragter, betont, dass die DSGVO-Anforderungen pragmatisch lösbar seien. Wer sich das zertifizieren lasse, gewänne ein wertvolles Marketingargument. Ein Imageschaden durch mangelhafte Datensicherung sei kaum bezahlbar.

Neben der DSGVO sind im Online-Geschäft deutsche und europäische Vorschriften zu beachten – nicht nur Abmahnungen drohen. Orientierung verschafft der kostenlose Online-Check „Ist mein Online-Auftritt rechtssicher?" der Oldenburgischen IHK. „Das Tool wird sehr gut angenommen", freut sich Daniela Haan, bei der IHK zuständig für IT- und Internetrecht. „Ergänzend beraten wir auch persönlich und stellen Mustertexte zur Verfügung." Zudem empfiehlt sie, Regelungen zum Homeoffice in den Arbeitsvertrag aufzunehmen, damit Arbeitnehmer und Arbeitgeber auf der sicheren Seite sind.