Praxistipp Datenschutz 02 | 2021

Wird es in Ihrem Unternehmen 2021 ein Datenleck geben?

Immer mehr Unternehmen werden Opfer von Trojanerangriffen. Trotz zahlreicher bekannter Fälle sind noch immer zu wenige Unternehmen vorbereitet. Dabei drohen Millionenschäden, häufig steht die Existenz auf dem Spiel. Wie stehen die Chancen, dass es in Ihrem Unternehmen 2021 zum Datenleck kommt? Machen Sie den Check.

Tatsache Nr. 1 Was die Corona-Pandemie neben anderem mit sich brachte, sind kurzfristig eingerichtete mobile Arbeitsplätze. Ein viel zu großer Bestand essenzieller Firmendaten befindet sich zum ersten Mal außerhalb der Infrastruktur der Unternehmen.

Tatsache Nr. 2 Für Computerviren sind das perfekte Voraussetzungen für eine rasche Verbreitung. Und daran wird sich in absehbarer Zeit wenig ändern. Denn: Wann die Zahl erforderlicher Impfungen für das Ende des Lockdown-Zeitalters erreicht sein wird, steht in den Sternen. Darum ist jetzt der richtige Zeitpunkt, Wissens- und Sicherheitslücken zu schließen.

Tatsache Nr. 3 Angreifer nutzen die Situation. Immer mehr Angriffe auf mobile Arbeitsplätze sind zu verzeichnen – sofern sie bekannt werden. In zu vielen Fällen dringen Angreifer über schlecht geschützte mobile Arbeitsplätze in Firmennetze ein. Im Verborgenen wird Mailverkehr mitgeschnitten, um über authentisch wirkende Mails weitere Angriffe vorzubereiten. Dateien werden kopiert, um in aller Ruhe deren Schutzmechanismen zu knacken – sofern sie überhaupt geschützt sind. Möglicherweise wird die Verschlüsselung der Unternehmensdateien vorbereitet, um Lösegeld zu fordern. So erging es jüngst nicht nur dem Heise-Verlag und der Funke Mediengruppe.

Tatsache Nr. 4 Wenn Ihr Unternehmen bis heute kein Angriffsopfer geworden ist, haben Sie entweder die richtige Strategie und das Glück des Tüchtigen – oder Sie sind den Angreifern bisher einfach nicht ins Visier geraten.

Tatsache Nr. 5 Wird Ihr Unternehmen angegriffen, ist in aller Regel eine Meldung an die Datenschutz-Aufsichtsbehörde fällig. Zugegeben dürfte das dann eines Ihrer geringeren Probleme sein. Dennoch: Im Ernstfall haben Sie für die Meldung nur 72 Stunden. Besser, wenn Sie vorbereitet sind.

Hand aufs Herz Haben sich Ihre Mitarbeiter 2020 zum ersten Mal ernsthaft mit Themen wie Phishing und sicheren Netzwerken auseinandersetzen müssen? Möglicherweise haben sie bis zum Beginn der Corona-Pandemie nie von zuhause oder unterwegs gearbeitet. Und wenn ja: Wie gelingt es, nach etwa einem Jahr Notstands-Homeoffice-Lösungen endlich das nötige Bewusstsein zu schaffen?

Nur Gefahren, die man kennt, kann man bekämpfen Noch nie gab es so viele Identitätsdiebstähle wie derzeit. Schließlich war es für Angreifer nie so leicht, Identitäten abzugreifen. Umso wichtiger, in angemessener Weise mobil arbeitende Kolleginnen und Kollegen mit diesen Gefährdungen vertraut zu machen. Bevor sie in Unkenntnis Einstellungen vornehmen, die möglicherweise massive Gefahren nach sich ziehen, sollten sie sich unbedingt an die Experten im Unternehmen wenden.

Wie gefährlich sind nicht reglementierte Lösungen für die Unternehmens-IT? Viel zu wenige Unternehmen waren auf mobiles Arbeiten eingestellt. Entsprechend dürftig haben sie Arbeitsplätze auf die strengen Sicherheitsanforderungen der freien IT-Wildbahn eingerichtet. Wie viele unzureichend abgesicherte Cloud-Speicher derzeit wohl im Einsatz sind? Sicher ist: zu viele. Entsprechend viele Angreifer zielen genau darauf ab.

Wie viele Beschäftigte schätzen die Risiken im Homeoffice richtig ein? Oder treffender: wie wenige? Plötzlich müssen Menschen, die sich bisher höchstens geärgert haben, sich zehn- und mehrstellige Passwörter merken zu müssen, Entscheidungen zur Sicherheit ihres Notebooks und der Unternehmensdaten treffen. Wer sorgt dafür, dass eine sichere Anbindung vom mobilen Arbeitsplatz ans Internet erfolgt? Wer entscheidet, ob die Einstellungen am privaten Router sicher sind?

Alles sicher. Bis auf … Nehmen wir einmal an, der mobile Arbeitsplatz ist sicher. Nehmen wir an, das Notebook ist ein Thin Client, hat also keine Daten vor Ort, sondern ist über eine sichere Lösung wie Remote Desktop an die

sichere Unternehmens-IT angebunden. Nehmen wir weiter an, es werden nur sichere Systeme für Video- und Telefonkonferenzen verwendet (von denen gibt es, nebenbei bemerkt, nur sehr wenige). Nehmen wir an, das Drucken funktioniert sicher, Unterlagen werden sicher aufbewahrt und die Vernichtung ist geregelt. Klingt, als sei es die Ausnahme? Ist es. Nehmen wir es dennoch an. Als Nächstes stellt sich nämlich eine Frage.

Wie gut sind die Beschäftigten geschult?

Sind diese auf die mobile Arbeitssituation so vorbereitet, dass sie sich mit Phishing, Social Engineering und Erpressungstrojanern auskennen? Wie ist sichergestellt, dass das Wissen aktuell bleibt? Ist die Authentisierung der Kolleginnen und Kollegen so sicher, dass sich keine Angreifer dazwischenschleichen können? Ehrliche Antworten auf diese Fragen helfen, dem Unternehmen in der Zukunft viel Ärger zu ersparen.

Schnell-Check zum mobilen Arbeiten

Wie steht es um die Sicherheit beim mobilen Arbeiten? Machen Sie den Schnell-Check:

1. Sind die mobilen Arbeitsplätze des Unternehmens sicher im Sinne der Sicherheit der Unternehmens-IT?
2. Gibt es verbindliche Vorgaben, damit die Beschäftigten wissen, was sie im Homeoffice zu beachten haben?
3. Können Vorgaben aus dem Unternehmen am mobilen Arbeitsplatz überhaupt eingehalten werden?
4. Wenn Sie Auftragsverarbeiter sind: Erlauben die Verträge über Auftragsverarbeitung mobiles Arbeiten?
5. Besteht mindestens eine VPN-Anbindung?
6. Ist eine Mehr-Faktor-Authentisierung vorgegeben?
7. Können Sie garantieren, dass die mobil arbeitenden Kolleginnen und Kollegen gegen die verschärften Risiken hinsichtlich Sicherheit und Datenschutz hinreichend gewappnet sind?
8. Sind die eingesetzten Rechner genauso sicher wie im Büro?
9. Unterliegt die Infrastruktur wie Router und Drucker denselben Kriterien wie im Büro?
10. Wurden die Router-Einstellungen hinsichtlich Angriffssicherheit geprüft und für sicher befunden?
11. Sind eingesetzte Videokonferenzsysteme sicher?
12. Sind eingesetzte Telefonielösungen sicher?
13. Sind eingesetzte Telefonkonferenzsysteme sicher?
14. Werden verbindliche Schulungen auch im Homeoffice verlässlich durchgeführt?
15. Finden angemessene und dokumentierte Überprüfungen statt?

Sollten Sie mehr als drei Fragen nicht eindeutig mit Ja beantworten können, sollten Sie sich nicht wundern, wenn es 2021 zu einem (vermeidbaren) Datenleck kommt. Darum: handeln! Schließlich dürfen Vorsätze fürs neue Jahr auch mal gebrochen werden. Besonders, wenn es die von Kriminellen sind.

Rechtsquellen zum Nachlesen

Zu **technischen und organisatorischen Maßnahmen**: Art. 32 DSGVO

Zur **Meldepflicht bei Schutzverletzungen**: Art. 33 DSGVO

Zur **Überwachung des Datenschutzes durch den Datenschutzbeauftragten**: Art. 39 Abs. 1 lit. b DSGVO

Alle Praxistipps gibt es auf team-datenschutz.de

Lösungen zum Thema Sicherheit bei mobilem Arbeiten und zur Überprüfung durch den Datenschutzbeauftragten? Fragen Sie uns.

Persönliche Beratung, passgenaue Umsetzung. Mit *Team* Datenschutz sind Sie in Sachen Datenschutz und Informationssicherheit einen Schritt voraus.

Hier schreibt Eberhard Häcker, Externer Datenschutzbeauftragter, Datenschutzberater, Fachautor und Kongressredner, Geschäftsführer der TDSSG GmbH – Team Datenschutz Services – und der HäckerSoft GmbH (Datenschutz-Software DATSIS und Lernplattform Optilearn.de). Er ist überzeugt, „den spannendsten Beruf der Welt“ zu haben, denn „was man beim Datenschutz erlebt, kann man nicht erfinden – Geschichten, die das Leben schreibt.“ (Eberhard Häcker)