IT-Sicherheit für das Arbeiten zu Hause

Wie sieht ein sicheres Homeoffice aus?



© Julien Eichinger/stock.adobe.com

Ein großer Teil der deutschen Angestellten arbeitet derzeit von zu Hause aus – vom Sachbearbeiter bis zum Geschäftsführer. Das bringt in vielen Fällen neue IT-Sicherheitsrisiken mit sich. Auch Hacker nutzen die aktuelle Unsicherheit verstärkt aus.

1 CHANCEN NUTZEN UND RISIKEN MINIMIEREN

Deutschland ist im Homeoffice-Modus. Das hat viele positive Seiten. Insbesondere beschleunigt sich, wenn zigtausende Arbeitnehmer von zu Hause aus arbeiten, die digitale Transformation von Unternehmen erheblich. Unterlagen werden auf Kollaborationsplattformen geteilt, Teamabsprachen über Chatfunktionen getroffen und Meetings per Video abgehalten. Von dieser für viele neuen Art der Zusammenarbeit werden Unternehmen auch profitieren, wenn die Corona-Pandemie nachlässt. Eine neue Form des Arbeitens könnte dann zur Tagesordnung gehören – und zwar nicht nur in Großkonzernen, sondern auch in kleinen Unternehmen und im Mittelstand. Denn gerade hier herrscht noch Nachholbedarf bei der Digitalisierung von Büroaufgaben.

Dies ist eines der Ergebnisse des Digital Office Index, den der Digitalverband BITKOM 2018 erstellt hat. Auf einer Skala von 0 („überhaupt nicht digitalisiert") bis 100 („vollständig digitalisiert") erreichen große Unternehmen mit mehr als 500 Mitarbeitern demnach einen Indexwert von 63 Punkten, bei den Mittelständlern mit 100 bis 499 Mitarbeitern liegt er bei 58, bei kleineren Unternehmen mit weniger als 100 Mitarbeitern sind es dagegen nur 53 Punkte. Jürgen Biffar, Vorstandsvorsitzender des Kompetenzbereichs ECM im BITKOM, mahnte, der breite Mittelstand müsse nachziehen. Die Corona-Pandemie ebnet dafür einen entscheidenden Weg.

Die neuen digitalen Infrastrukturen eröffnen allerdings auch eine Vielzahl neuer Angriffspunkte für Cyberkriminelle. Die Gefahr ist vor allem deshalb so groß, weil die Anbindung der Heimarbeitsplätze in vielen Unternehmen sehr abrupt erfolgen musste, also ohne die eigentlich erforderlichen Vorbereitungen. Vor allem in kleinen Unternehmen und im Mittelstand waren Improvisation und Pragmatismus gefragt, als Mitarbeiter von einem Tag auf den anderen ins Homeoffice wechseln mussten. Es werden Plattformen genutzt, die eigentlich für die Privatnutzung vorgesehen sind, wie etwa Videokonferenz-Technologien, Cloud-Anwendungen und mobile Endgeräte. Diese erleichtern die Digitalisierung zwar erheblich, sie erhöhen aber auch das Sicherheitsrisiko. Hinzu kommen zigtausende veraltete Computer, ungesicherte

Router und schlecht geschützte WLAN-Verbindungen, die mit einem Mal Zugang zu den sensiblen Daten von Unternehmen bieten. Erschwerend kommt hinzu, dass Hacker die Gunst der Stunde nutzen. Mit einer Flut an Phishing-Mails, neu entwickelter Malware und gefälschten Informationen versuchen sie, aus der Krise Kapital zu schlagen.
Wie aber können Unternehmen unter diesen Bedingungen die Heimarbeitsplätze ihrer Mitarbeiter trotzdem erfolgreich vor Hackerangriffen schützen?

2 VERBINDLICHE REGELN FÜR DEN UMGANG MIT DATEN UND IT

Alle Mitarbeiter, die an das Unternehmensnetzwerk angebunden sind, sollten verbindliche und eindeutige Regelungen für den Schutz der IT und der Daten im Unternehmen erhalten – und zwar schriftlich. Unternehmen können auf diese Weise u. a. festlegen, welche Informationen außerhalb der Institution transportiert und bearbeitet werden dürfen, wer diese mitnehmen darf und welche Schutzvorkehrungen dabei zu treffen sind. Denn wenn Mitarbeiter für die Heimarbeit Unterlagen aus ihrem Büro in Papierform oder per USB-Stick mit nach Hause nehmen, birgt dies ein erhebliches Risiko, dass sensible Informationen ungeschützt sind und in falsche Hände gelangen. Das kann für Unternehmen zu Wettbewerbsnachteilen und finanziellen Schäden führen. Auch Datenschutzvorschriften, wie die DSGVO, müssen selbstverständlich beachtet werden. Andernfalls drohen womöglich hohe Strafen und ein Vertrauensverlust bei den Kunden. Daher sollte auch eine sachgemäße Vernichtung von Unterlagen – Stichwort „Schreddern" – geregelt werden. Vertragsentwürfe oder Bewerbungsunterlagen haben nun einmal nichts im privaten Papiermüll zu suchen.

3 ENDGERÄTE VOR ANGRIFFEN AUS DEM INTERNET SCHÜTZEN

Der aktuelle Informationsbedarf zur Corona-Pandemie wird verstärkt von Hackern ausgenutzt. Sie schleusen Malware über gefälschte Webseiten, E-Mails oder Grafiken auf die Rechner der Arbeitnehmer. Beispielsweise nutzen Hacker die Suche nach Hygieneartikeln und Schutzmasken aus, indem sie entsprechende Angebote per E-Mail versenden und die Empfänger auf mit Malware infizierte Webseiten locken. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat bereits vor der Zunahme solcher Angriffe gewarnt.
Doch bereits vor der Corona-Krise galt: 70 % der Hackerangriffe kommen aus dem Internet. Damit es für Mitarbeiter möglich ist, sicher zu surfen, kann ein sog. virtueller Browser eingesetzt werden. Der Nutzer arbeitet darin mit einer vom Betriebssystem separierten Maschine. Er bewegt sich sozusagen in einer virtuellen „Surfumgebung". Der Vorteil: Anstatt – wie bei Antivirenprogrammen – Schadcodes zu erkennen, werden alle potenziell gefährlichen Aktivitäten in diesem virtuellen Browser isoliert. Jeder Browserstart beseitigt die Schädlinge und versetzt den Browser in seinen Ausgangszustand.

4 DATENSCHUTZ UND PHYSISCHE SICHERHEITSMASSNAHMEN

Vor allem Organisationen mit hohen Sicherheitsanforderungen sollten die Endgeräte ihrer Mitarbeiter mit einer Festplattenverschlüsselung ausstatten. Nur berechtigte Nutzer können dann per Multi-Faktor-Authentifizierung ihre Daten und das Betriebssystem nutzen. Geht das Gerät verloren oder wird es gestohlen, ist es für Dritte nicht möglich, auf die Daten zuzugreifen.

Ein Heimarbeitsplatz ist weniger gut geschützt als die Räume in einem Unternehmen. Besucher, Familienangehörige oder Mitbewohner nutzen die zum Büro umfunktionierten Räume häufig mit. Es ist daher deutlich schwieriger sicherzustellen, dass Unbefugte zu keiner Zeit auf dienstliche IT und Unterlagen zugreifen können. Jeder Mitarbeiter sollte daher angewiesen werden, im Homeoffice einige Maßnahmen zu ergreifen, um sicherzustellen, dass keine sensitiven Informationen frei zugänglich sind. Dazu zählt, dass der Mitarbeiter den Arbeitsplatz in seinen eigenen vier Wänden physisch absichert, wenn er eine Pause macht – bspw. indem er die Tür verschließt und den Bildschirm sperrt. Lässt sich der Raum nicht abschließen oder arbeitet man im Wohnzimmer oder am Küchentisch, sollten ein abschließbarer Schreibtisch, Rollcontainer oder Schrank genutzt werden. Als weitere Schutzmaßnahme empfiehlt es sich, die Webcam am Rechner oder Laptop abzudecken, wenn diese nicht benötigt wird, sowie bei Nichtgebrauch das Mikrofon auszuschalten, um mögliche Spionageattacken ins Leere laufen zu lassen.

5 WLAN, BETRIEBSSYSTEME, WEBANWENDUNGEN UND APPS

Eine WLAN-Verbindung erleichtert die Arbeit im Homeoffice ungemein. Egal ob Küche, Wohn- oder Gästezimmer: Der Arbeitsplatz lässt sich flexibel einrichten – ohne lästige Kabel. Eine WLAN-Verbindung ist allerdings auch ein Sicherheitsrisiko. Denn WLAN-Netzwerke bieten Hackern die Möglichkeit, auf Daten zuzugreifen. Hacker können zudem Computerviren und Trojaner über schlecht oder nicht gesicherte WLANs in ein System einspeisen. Wurde das Administrator-Passwort nicht geändert, haben Hacker ein leichtes Spiel. Denn die Standardpasswörter sind einfach zu knacken. Spätestens wenn die Kollegen von zu Hause aus arbeiten, sollten sie das Standard-WLAN-Passwort durch ein neues, starkes Passwort ersetzen. Weiteren Schutz bietet eine Verschlüsselung. Dabei sollte stets die aktuelle WPA2-Verschlüsselung aktiviert werden, da die älteren WEP- und WPA-Verschlüsselungen nicht mehr genügend Schutz bieten.
Ein wesentlicher Schutz vor Hackern sind Patches und Updates. Alle Mitarbeiter sollten daher regelmäßig Updates ausführen und mit der neuesten Systemversion arbeiten. Updates schließen neu erkannte Sicherheitslücken – also gefährliche Schwachstellen in einem Betriebssystem oder Softwareprogramm. Hacker nutzen solche Schwachstellen aus, indem sie einen Code für eine bestimmte Sicherheitslücke erstellen, der zu einem

Schadprogramm verpackt wird. Diese sog. „Exploits" können Computer infizieren, etwa wenn eine Webseite aufgerufen, eine manipulierte E-Mail geöffnet oder infizierte Medien abgespielt werden. Software-Updates sind daher wichtige Vorsichtsmaßnahme für die Internetsicherheit.

6 VORSICHT VOR BETRÜGERN

Angreifer täuschen und tricksen, um an die begehrten Passwörter, Bankverbindungen oder Zugangsinformationen zu gelangen. Beispielsweise versenden sie täuschend echt wirkende E-Mails, um an vertrauliche Informationen zu gelangen. Oder sie geben sich am Telefon als Mitarbeiter eines IT-Dienstleisters aus und versuchen auf diese Weise Zugangsdaten zu erlangen. Dieses sog. Social Engineering stellt in Zeiten dramatischer Veränderungen eines der größten Risiken im Homeoffice dar. Zum einen, weil die Mitarbeiter verunsichert sind und dies häufig zu Fehlverhalten führt. Zum anderen, weil sich im Homeoffice E-Mails oder Anrufe nicht so leicht zurückverfolgen lassen wie im Büro.
Unternehmen sollten sichere Kommunikationskanäle nutzen, um die Tablets, Smartphones oder PCs der Beschäftigten im Homeoffice an das Unternehmensnetzwerk anzubinden. Werden hierfür unsichere Protokolle verwendet, können Informationen abgehört oder manipuliert werden. Ein sicherer Remote-Zugang ist daher entscheidend für einen sicheren Heimarbeitsplatz. Empfehlenswert sind Virtual Private Networks (VPN). Sie bauen über einen „gesicherten Tunnel" Verbindungen zwischen dem Endgerät und dem Unternehmensnetz auf.

7 STARKE PASSWÖRTER NUTZEN

Passwörter schützen Anwendungen vor unberechtigtem Zugriff – so weit, so bekannt. Je komplexer und eindeutiger Passwörter sind, desto schwerer sind sie zu knacken. Eine Tatsache, die zwar ebenfalls bekannt sein dürfte, aber leider viel zu oft keine Beachtung findet.
Gute Passwörter sind z. B. sog. Passphrasen, wie „Wir verschlüsseln Datenträger!" oder „keine-Zellen-in-Excel-verbinden". Solche Sätze sind leicht zu merken und zu tippen, aber schwierig zu knacken. Ergänzt werden sollten sie um Symbole, Zahlen oder Großbuchstaben. Jede Anwendung sollte mit einem eigenen Passwort geschützt sein. Andernfalls muss ein Angreifer lediglich eine Anwendung erfolgreich kompromittieren, um sich bei weiteren Konten erfolgreich anzumelden.

Ergänzenden Schutz bietet eine Multi-Faktor-Authentifizierung unter Einsatz von PIN, Fingerabdruck oder Passwort. Auf https://haveibeenpwned.com kann man übrigens überprüfen, ob ein Passwort bereits entwendet wurde. Um nicht den Überblick zu verlieren, ist es hilfreich, einen Passwortmanager zu nutzen. Das Programm speichert die Passwörter in einer Art Tresor – im Bedarfsfall kann man sie dort leicht wieder abrufen. Einen Passwortmanager schützt man am besten mit einer starken Passphrase sowie einer zweistufigen Verifizierung.

8 DATEN IN DER CLOUD SCHÜTZEN

Cloud-Anwendungen erleichtern die gemeinsame Arbeit von mehreren Standorten erheblich. Doch Unternehmen geben die Kontrolle über den Schutz ihrer Daten ab. Und das, obwohl die Schutzmechanismen der Cloud-Anbieter den hohen Sicherheitsanforderungen vieler deutscher Unternehmen nicht genügen. Es drohen Datenspionage und Compliance-Verletzungen. Hinzu kommt: Die Mehrzahl der Cloud-Anbieter sitzt im Nicht-EU-Ausland. Dort geltende Regelungen sind oft nicht mit der DSGVO vereinbar. Beispiel Cloud Act: Der „Clarifying Lawful Overseas Use of Data Act" verpflichtet US-amerikanische Cloud-Provider, den US-Behörden Zugriff auch auf nicht in den USA gespeicherte Daten zu gewähren – und macht die DSGVO damit unwirksam. Dies bedroht die Souveränität deutscher Behörden und Unternehmen, weil so Akteure aus Drittstaaten Zugriff auf ihre Daten und Know-how erhalten könnten.

Die Lösung ist ein datenzentrischer Schutz: Anstatt Dateien mit ihren vollständigen Inhalten in die Cloud hochzuladen, wird ein sog. Platzhalter in die Cloud eingestellt. Dieser enthält Metadaten, die z. B. Auskunft darüber geben, wie die Datei heißt und wer sie öffnen darf. Nur autorisierte User können über ein differenziertes Anmeldesystem mit diesem Dummy auf das Original zugreifen. Der Vorteil: Die Originaldatei muss nicht in fremde Hände gelegt werden. Sie kann also auf dem Server des Unternehmens abliegen oder an jedem anderen beliebigen Speicherort. Auf diese Weise kann das Originaldokument verschlüsselt vor Hackern geschützt und trotzdem über die Cloud geteilt werden. Mit einem solchen datenzentrischen Ansatz können Unternehmen und Behörden völlig eigenständig entscheiden, wo ihre Daten gespeichert werden – und auch, dass diese in Deutschland bleiben. Sie entsprechen damit den eigenen Anforderungen an die Datensicherheit und können jede beliebige Cloud gesetzeskonform nutzen.

9 FAZIT

Auch weil Unternehmen den Widerstand ihrer Mitarbeiter befürchteten, zögerten sie die Digitalisierung von Büroabläufen bisher hinaus. Wenn Mitarbeiter den Vorteil der Digitalisierung nicht erkennen, so die Sorge, würden sie den Unternehmen auf dem Weg zum digitalen Büro möglicherweise verloren gehen. Durch die Corona-Pandemie hat sich diese Hürde nahezu aufgelöst. Das ist ein Riesenfortschritt! Die Digitalisierung trägt maßgeblich zum Schutz der Arbeitnehmer bei. Diese ganz konkrete Erfahrung ist überzeugender als jedes Effizienz- oder Nachhaltigkeitsargument des Arbeitgebers. Viele Beschäftigte im Homeoffice haben dadurch quasi nebenbei die Vorteile der digitalen Prozesse erkannt und sich an die Arbeit mit Microsoft Teams und Cloud-Plattformen gewöhnt.
Wenn es gelingt, diesen positiven Digitalisierungsschub mit einem besseren Schutz der IT zu verbinden, kann die Ausnahmesituation eine große Chance für Unternehmen sein.

FEEDBACK

Hat Ihnen der Beitrag gefallen? Sagen Sie uns Ihre Meinung! Alle Infos auf www.auaplus.de

UNSER AUTOR



Dr. Falk Herrmann
CEO von Rohde & Schwarz Cybersecurity, München