Compliance-Pflichten im Homeoffice (Teil 2)

Der Trend zum Arbeitsplatz in den eigenen vier Wänden verstärkt sich und wird die Corona-Pandemie wahrscheinlich überdauern. Technische, organisatorische und personelle Maßnahmen, kurz TOPs, zum Schutz von Daten und IT-Geräten sind auch im Homeoffice unverzichtbar. Konsequent umgesetzt sowie im beruflichen wie privaten Alltag angewendet, schützen sie wirksam von Datenverlusten und Cyber-Attacken. Allerdings, und das ist der Preis den Sie dennoch „bezahlen" müssen, kosten sie mehr oder weniger Bequemlichkeit.

von Andreas Dolezal, Unternehmensberater & Compliance Experte

Sichere Passwörter verwenden

Sichere Passwörter sind eine der einfachsten und gleichzeitig wirksamsten Maßnahmen, um Daten und IT-Geräte für unbefugtem Zugriff zu schützen. Trotzdem sind dummdreiste Passwörter, wie beispielsweise „123456", „passwort" oder „schatzi01", nach wie vor weitverbreitet. Ihr eigenes oder das Geburtsdatum Ihrer Kinder, der Name Ihres Haustieres oder Teile Ihrer Wohnadresse sind keine besseren Passwörter. Gute Passwörter sind kryptisch, das heißt:

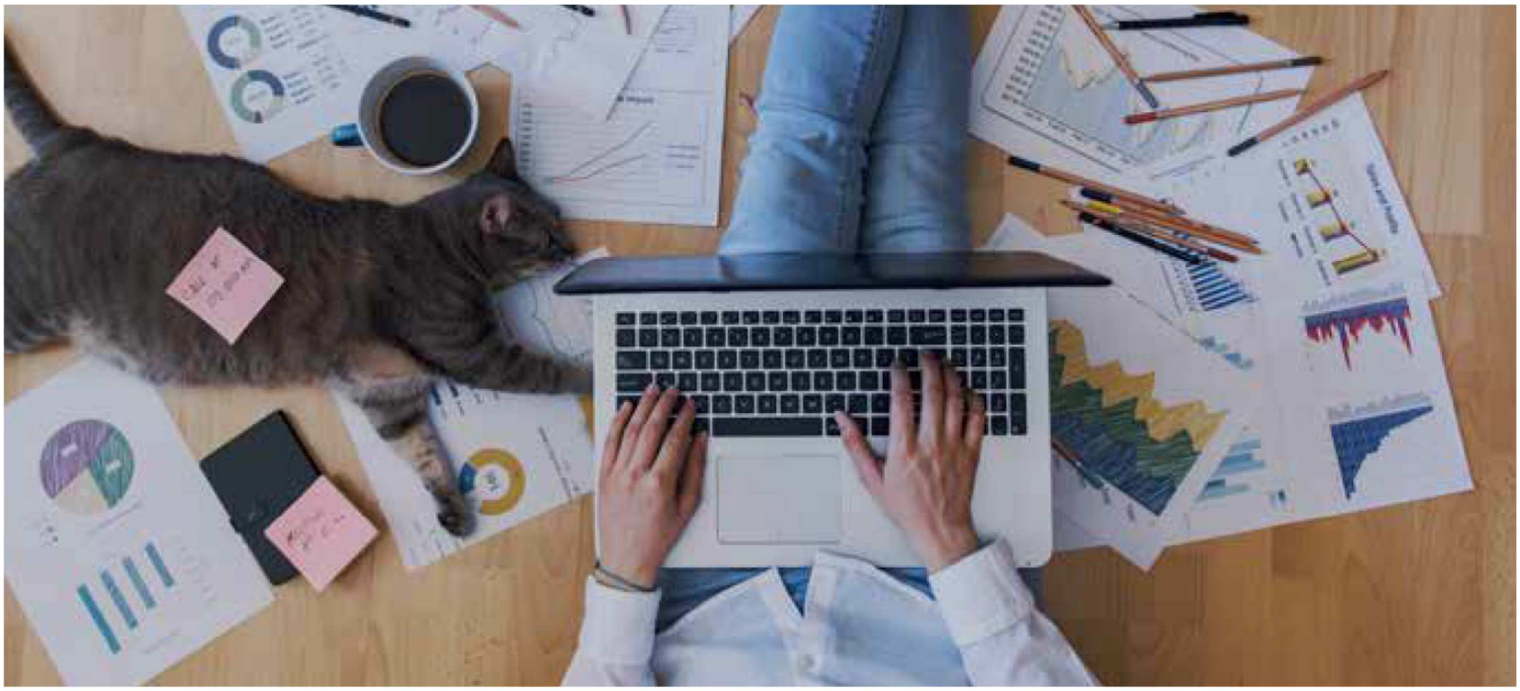
- mindestens acht Zeichen lang: je nachdem wie sensibel oder vertraulich die IT-Systeme, Endgeräte und Daten sind, die geschützt werden, sollen Passwörter bis zu 20 oder mehr Zeichen lang sein,
- zusammengesetzt aus Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen: setzen Sie Groß- und Kleinbuchstaben nicht so wie es den Grammatikregeln entspricht, sondern vermischen Sie Groß- und Kleinbuchstaben willkürlich. Bauen Sie mittendrin Ziffern und Sonderzeichen wie Satzzeichen oder Währungssymbole ein.

Verwenden Sie einen Passwort-Manager, dann schützen Sie diesen mit einem extrem sicheren Passwort, dass Sie – und nur Sie! – auswendig wissen. Insbesondere dieses Passwort darf nirgendwo notiert oder gespeichert sein.
Voreingestellte Standard-Passwörter müssen unverzüglich nach Inbetriebnahme eines IT-Gerätes oder einer Software durch individuelle Passwörter ersetzt werden. Wenn möglich, nutzen Sie die Zwei- oder Mehr-Faktor-Authentifizierung.

Zuerst denken, dann klicken!

Oft reicht schon ein einziger unüberlegter Klick auf einen Dateianhang, ein Banner im Internet, einen Link in einer E-Mail usw., und das Drama nimmt seinen Lauf. Versteckte und bösartige Programmcodes werden – womöglich ohne, dass Sie es bemerken – ausgeführt, nisten sich auf Ihren IT-Geräten ein, laden weitere Schadsoftware nach, stehlen Daten, machen laufende Anwendungen unbrauchbar und Hacker fordern vielleicht Lösegeld für das Wiederfreigeben.

Haben Sie ein wachsames Auge auf alle Benachrichtigungen, Angebote in sozialen Medien oder Banner-Werbungen. Firewall und Virenschutz-Software können Sie nicht vor jeder potentiellen Falle schützen. Nutzen Sie Ihren Hausverstand. Wie lautet die E-Mail-Adresse des Absenders? Passt sie zur eingelangten Nachricht? Aus welchem Grund soll ein Link angeklickt oder eine Datei heruntergeladen beziehungsweise geöffnet werden? Cyber-Kriminelle werden immer



trickreicher, sie erinnern zum Beispiel an eine offene Rechnung oder locken mit einer Gutschrift. Bleiben Sie jedenfalls aufmerksam und skeptisch!

Virenschutz-Programme einsetzen

Schutzprogramme vor Computer-Viren, die im Hintergrund laufend verdächtige Software und Prozesse überwachen und melden, müssen eine Selbstverständlichkeit sein. Denn Schadprogramme können grundsätzlich alle IT-Geräte, IT-Systeme und Betriebssysteme befallen. Betroffen sein können neben klassischen IT-Systemen wie Arbeitsplatzrechnern und Servern auch mobile IT-Geräte wie Laptops, Smartphones und Netzwerk-Komponenten (zum Beispiel Router, Drucker, Kopierer) sowie IoT-Geräte (Internet of Things wie Smarthome-Geräte). Ein Virenschutz-Programm muss daher auf diesen Geräten ebenfalls installiert und richtig konfiguriert sein.

Viele Hersteller solcher Schutzprogramme bieten kostenlose Versionen an. Zwar verfügen diese im Vergleich zu den kostenpflichtigen Versionen oft über einen eingeschränkten Funktionsumfang (oder beinhalten Werbung), grundsätzlich sind aber auch Gratis-Versionen für stationäre Geräte sowie App-Versionen für mobile Geräte geeignet und erhöhen die Sicherheit. Hat Ihr Arbeitgeber bereits eine Wahl getroffen, die zentral installiert ist, dürfen die von der IT-Abteilung vorgenommenen Einstellungen nicht eigenmächtig verändert werden.

Software regelmäßig updaten

Das beste Virenschutz-Programm und die beste (Personal) Firewall können Ihre Daten und IT-Geräte nur dann wirksam schützen, wenn sie stets auf dem aktuellsten Stand sind. Generell sollten alle Anwendungen regelmäßig aktualisiert werden. Updates und (Sicherheits-)Patches werden von den Herstellern in der Regel laufend angeboten und oftmals automatisch installiert. Mit solchen Updates schließen Hersteller unter anderem bekannt gewordene Sicherheitslücken. Es ist daher unerlässlich diese Sicherheits-Updates zeitnahe zu installieren.

Denken Sie dabei aber nicht nur an das Virenschutz-Programm und die Firewall, sondern insbesondere an das Betriebssystem, den Internet-Browser und sämtliche installierte Programme und Anwendungen. Aktivieren Sie den Auto-Update-Mechanismus. Verwenden Sie keine Software, die vom Hersteller nicht mehr mit Updates oder Sicherheits-Patches versorgt wird (wie zum Beispiel Windows 7).

Nur installieren was Sie tatsächlich brauchen

Das Internet ist voll von Freeware, also Anwendungen, die kostenfrei zum Download bereitstehen und genutzt werden dürfen (allerdings nicht immer gewerblich, achten Sie darauf!). Seien Sie sparsam beim Installieren von Anwendungen, denn jede einzelne Anwendung mehr stellt ein zusätzliches Sicherheitsrisiko dar. Beachten Sie, dass Sie möglicherweise von Ihrem Dienstgeber gar nicht die Erlaubnis haben, eigenmächtig Programme zu installieren, oder dies nur nach Rücksprache beziehungsweise nach Freigabe der IT-Verantwortlichen tun dürfen.

Oftmals versuchen Installationsprogramme für Freeware Ihnen zusätzliche Software „unterzujubeln“. So finanzieren sich Hersteller von Freeware teilweise. Klicken Sie sich also nicht unbedacht durch die einzelnen Installationsschritte, sondern schauen Sie genau, wo sich eine vorangekreuzte Checkbox versteckt – und lehnen Sie das Installieren dieser Zusatz-Software ab. Deinstallieren Sie Anwendungen, die Sie nicht mehr benötigen.

Sprachassistenten deaktivieren

Deaktivieren Sie im Homeoffice digitale Sprachassistenten, auch auf Ihrem Smartphone und im Auto, jedenfalls während Sie geschäftlich telefonieren oder an Videokonferenzen teilnehmen. Digitale Sprachassistenten machen uns zwar den Alltag bequemer, aber wie so oft erkaufen wir uns diese Bequemlichkeit mit erhöhten Risiken für den Datenschutz. Lauschen Sprachassistenten im Ruhemodus wirklich nicht? Wohin werden die Informationen übertragen? Und wozu werden sie von den Anbietern noch verwendet? All das sind oft unbeantwortete Fragen.

Bildschirmsperre aktivieren

Die Sperre des Bildschirms lässt sich sowohl manuell aktivieren als auch nach einem vorgegebenen Zeitintervall automatisch. Im Büro ebenso wie im Homeoffice sollte die Bildschirmsperre immer dann aktiviert werden, wenn Sie den Arbeitsplatz verlassen (zum Beispiel für den Weg zur Toilette oder zum Kaffee holen).

Die aktivierte Bildschirmsperre darf sich erst nach Eingabe eines sicheren Passwortes deaktivieren. Lassen Sie sich dabei – zum Beispiel an öffentlichen Orten – nicht beobachten, schon gar nicht filmen.

Vorsicht im Free-/Public-WLAN!

Frei zugängliches WLAN-Netzwerke gibt es heutzutage schon an sehr vielen Orten. Beinahe jedes (Schnell-)Restaurant, Kaffeehaus, Shoppingcenter und Hotel, jeder Bahnhof und Flughafen offerieren Gratis-WLAN. Grundsätzlich sollten öffentliche WLAN-Netze als unsicher eingestuft werden (und im Zweifelsfall gar nicht genutzt werden), denn Sie können niemals sicher sein, wie geschützt übertragene Daten wirklich sind.

Als öffentliches WLAN, dessen Sicherheit Sie nicht kennen, sollten Sie genauso Gäste-WLANs betrachten, die viele Unternehmen Ihren Besuchern zur Verfügung stellen. Dabei sollten gegebenenfalls datenschutzrechtliche Aspekte berücksichtigt werden. Beispielsweise müssen alle Nutzer des Gäste-WLANS darüber informiert werden, welche Daten verarbeitet werden (siehe Informationspflichten gemäß DSGVO), und dass die Verwendung zu illegalen Zwecken untersagt ist.

Keine Messenger-Dienste verwenden

Nicht nur die Datenschutzbehörde spricht die klare Empfehlung aus, keine privaten Kommunikationsmittel, wie beispielsweise WhatsApp, Facebook und Instagram, für das Austauschen beruflichen Informationen zu verwenden.

Ja, ich weiß, wann immer ich Kunden und Geschäftspartner darauf hinweise, dass WhatsApp & Co. in der geschäftlichen Kommunikation nichts zu suchen haben, wird mir erklärt, dass solche Nachrichtendienste heutzutage unverzichtbar sind, auch beruflich. Das mag so sein, es ändert aber nichts daran, dass das Nutzen von WhatsApp & Co. oft datenschutzrechtlich bedenklich ist.

Das liegt weniger daran, dass die übertragenen Informationen nicht sicher sind. Die meisten Messenger übertragen Daten mittlerweile verschlüsselt. Viel mehr sind die möglichen (und in der Regel umfassenden) Zugriffe der Dienstanbieter auf die am Endgerät gespeicherten (personenbezogenen) Daten das Problem. Trotz seitenlanger Nutzungs- und Datenschutzhinweise der Anbieter wissen wir schlichtweg nicht, wie viele und welche Daten aus dem Endgerät ausgelesen werden, wohin diese übertragen und wozu sie verwendet (oder sogar weiterverkauft)

Wirtschaftlicher Schaden einer erfolgreichen Cyber-Attacke

Beispiel Datendiebstahl: Cyber-Kriminelle greifen Ihr IT-System an, verschaffen sich über ein gehacktes Passwort Zugang zu Ihrem IT-System und kopieren bzw. stehlen (Kunden-)Daten. In einer E-Mail an Sie behaupten die Kriminellen, dass sie im Besitz von Daten sind, und belegen dies mit ein paar Beispielen. Die Angreifer drohen, alle gestohlenen Daten zu veröffentlichen, wenn Sie nicht bereit sind, Lösegeld zu bezahlen. Welche wirtschaftlichen Folgen kann das für Sie als Unternehmer haben?

Nach Rücksprache mit der Polizei bezahlen Sie kein Lösegeld. Gemäß den Bestimmungen der DSGVO müssen Sie sowohl die Datenschutzbehörde als auch die betroffenen Personen (Kunden, Interessenten usw.) über den Verlust von - auch sensiblen - Daten informieren. Dazu holen Sie sich sicherheitshalber den Rat eines Rechtsanwaltes ein, der Sie 2.000 Euro kostet. Die Betroffenen sind nach der Information verunsichert und haben intensiven Gesprächsbedarf. Die Zeit, die Sie dafür aufwenden müssen, summiert sich auf den Gegenwert von 2.000 Euro.

Um die offensichtliche Sicherheitslücke zu schließen und die sichere Funktion Ihrer IT-Systeme wiederherzustellen, beauftragen Sie IT-Experten. Diese kosten Sie 4.000 Euro. Bis die Schwachstellen behoben sind und weitere Datendiebstähle verhindert werden, bleibt ihr Betrieb geschlossen. Die Kosten für zwei Tage Betriebsunterbrechung belaufen sich auf 5.000 Euro.

Es kommt wie es kommen muss. Die Hacker veröffentlichen Daten betroffener Personen. Die Betroffenen beauftragen Rechtsanwälte und verlangen Schadenersatz von Ihnen. Es drohen Zahlungen in der Höhe von 20.000 Euro.

Die lokale Presse berichtet über den Datendiebstahl in Ihrem Unternehmen. Zahlreiche Kunden und Interessenten wenden sich von Ihnen ab, Ihr Kundenbestand schrumpft. Für Krisenkommunikation, um zu retten was zu retten ist, investieren Sie 1.000 Euro, die Höhe des Umsatzrückganges wird sich erst in der Zukunft zeigen. Schließlich trifft ein Bußgeldbescheid der Datenschutzbehörde bei Ihnen ein. Weitere 10.000 Euro plus zehn Prozent Verfahrenskosten sind verloren.

Selbst wenn eine Cyber-Versicherung Teile der anfallenden Kosten übernimmt, Umsatzrückgang und Reputationsverlust gehen jedenfalls auf Ihre Rechnung.