Wie Sie virenfrei durch die nächste Zeit kommen

Von Dipl.-Ing. (FH) Harald Müller-Delius, MBA, Datenschutzbeauftragter

Liebe Mandantinnen und Mandanten,
liebe Versicherungsmaklerinnen und Versicherungsmakler,

aktuell ist noch nicht abzusehen, wie weit sich das neuartige Coronavirus noch verbreiten und wie viel Schaden entstehen wird. Tatsache ist, dass auch Einflüsse auf die tägliche Arbeit im Unternehmen die Folge sind. Unabhängig der Auswirkungen in der realen Welt sei hierbei angemerkt, dass die Parallelitäten zwischen Offline- und Online-Welt erschreckend sind: ungeschützte Individuen sind einem hohen Infektionsrisiko ausgesetzt und tragen zur weiteren Verbreitung bei. Je länger die Inkubationszeit, desto schwieriger ist es auch, die Verbreitung einzudämmen.
Allerdings gilt auch für die Daten-Welt: virtuelles Händewaschen kann jeder Einzelne umsetzen. Dabei sind einfache Hygienemaßnahmen wie virtuelles Desinfizieren („Einsatz von Virenscannern“), tragen von Mundschutz („Firewalls“) und vermeiden von Risikogebieten („Einsatz sicherer IT, nutzen seriöser Internetangebote und Software“) beste Ratgeber.

Warum Sicherheit im HomeOffice kein Wunschkonzert ist

Die gesetzlichen Grundlagen der Datenschutzgrundverordnung (DSGVO) sind klar: Unternehmen haben dafür zu sorgen, dass personenbezogene Daten bei der Verarbeitung hinreichend geschützt sind - das betrifft nun grundsätzlich ausnahmslos jedes Unternehmen.
Dafür wurden und werden Sicherheitsvorkehrungen, Konzepte, Richtlinien und Maßnahmen im Unternehmen definiert und eingerichtet, die dafür Sorge tragen, dass die Rechte von Betroffenen eingehalten, unberechtigter und ungewollter Datenabfluss oder -änderung vermieden und Verfügbarkeit garantiert werden.
Im Unternehmen selbst lassen sich deren Installation und Beachtung in der Regel gut umsetzen. Die gleichen Anforderungen gelten allerdings natürlich auch für jede Außenstelle oder externe Verarbeitung, also auch für’s HomeOffice.

Aus aktuellem Anlass hat nun - bei geeigneter Tätigkeit - die Arbeit vom HomeOffice aus überraschend Popularität gewonnen. Beachtet werden hierbei muss sowohl vom Unternehmen als auch vom Mitarbeiter, dass das definierte Datenschutz- und Sicherheitsniveau des Unternehmens auch im HomeOffice nicht unterschritten wird.
Und, aus Praxiserfahrung, dürfte wohl eher vermutet werden, dass dies eher weniger im Alltag vorzufinden sein mag.
Wie so oft bedarf es bei der Umsetzung folgender Maßnahmen der Unterstützung durch professionelle IT-Fachleute, allerdings kann man auch als Laie zumindest notwendige Punkte klären lassen oder besprechen.

Die Umsetzung

Natürlich gibt es einige mögliche Ansätze für konformes Arbeiten im HomeOffice. Richtig bewährt hat sich allerdings das Prinzip der Datenminimierung: was nicht extern gespeichert oder verarbeitet wird, muss auch nicht geschützt werden.
Dafür kommen als alltagstaugliche Lösung zwei Möglichkeiten in Betracht: die Datenverarbeitung per Browser-Anwendung oder sog. Terminal-Server-/Fernzugriff. Bei beiden Möglichkeiten dient der häusliche PC oder das Notebook nur als „Sichtgerät“ auf die Unternehmensanwendung. Damit wird das Unternehmen im Prinzip in’s Haus geholt, die eigentliche Verarbeitung findet nach wie vor auf unternehmenseigenen gesicherten Systemen statt und nach Beendigung der Tätigkeit verbleiben keinerlei Daten physisch zu Hause. Andere Verfahren würden eine Duplizierung oder einen physischen Transport mit den Risiken des Verlustes oder des unberechtigten Zugriffs mit sich bringen.

Die Risiken

Voraussetzung für ein sicheres Arbeiten sind folgende Maßnahmen.

1. *Verschlüsselung*
   Die Browser-Anwendung verlangt eine sichere https-Verbindung, auf den unternehmenseigenen Terminal-Server wählt man sich per VPN ein, in beiden Fällen wird Ihre „private“ Internetanbindung verwendet. Aktuelle Verschlüsselungsverfahren und Zertifikate sind hierbei Voraussetzung. Eine VPN-Verbindung schlägt sozusagen eine sichere Schneise durch den wilden Dschungel des Internets. Und wenn Sie per WLAN von der Couch aus arbeiten, sollte natürlich auch ein sicheres WLAN-Passwort und aktuelle WLAN-Technologie verwendet werden
2. *Technik*
   Kurz gesagt: vom Unternehmens-Server bis zum Verarbeitungsgerät vor Ort sollte „sichere“ IT eingesetzt worden sein. Idealerweise findet auch die häusliche Verarbeitung auf vom Unternehmen gestellter Hardware statt. Wird private IT eingesetzt, besteht immer die Gefahr, veraltete IT zu verwenden für die bekannte Sicherheitslücken existieren, deren Betriebssysteme nicht aktuell oder mit den notwendigen Updates versorgt sind oder durch Installation privater Software auch Schadsoftware mit auf den Rechner gelangt ist. Die Risiken gehen von der Anfertigung regelmäßiger Screenshots des PCs, das Mitschneiden von Tastatureingaben, das Infiltrieren der Unternehmens-IT durch Schadsoftware, Mitschnitte der Kommunikation, Beeinflussung von Kollegen durch Fake-Messages, Löschen oder Zwangsverschlüsselung von Daten bis hin zur Nutzung von Unternehmensressourcen für fremde Zwecke.
3. *Authentifizierung*
   Zwischen der regulären und der unberechtigten Nutzung von Unternehmensdaten steht beim Fernzugriff oft nur das Passwort. Dass dies ausreichend komplex und „sicher“ sein soll, versteht sich von selbst. Merksätze zur Herleitung bewirken hier Wunder, eine regelmäßige Veränderung ist nicht zu empfehlen, da hier in der Regel kein nennenswerter Sicherheitszuwachs zu verzeichnen ist. Moderner und viel sicherer sind die 2-Faktor-Authentifizierung („2FA“), bei der ein zweites Sicherheitsmerkmal wie eine SMS, ein biometrisches Merkmal oder eine Authenticator-App abgefragt wird oder ein Anmeldeverfahren nach FIDO2-Technik, bei der eine sichere Vertrauensstellung zwischen Sender und Empfänger hergestellt wird. Auch die Einschränkung des Zugriffs auf bestimmte Geräte oder IP-Adressen ist hilfreich, allerdings administrativ aufwändiger.
4. *Faktor Mensch*
   Letztlich ist keine Maßnahme sinnvoll oder sicher, wenn sie auf Grund von Komplexität, Performanceproblemen, Ineffizienz oder Inakzeptanz nicht verwendet wird. Schulungsmaßnahmen und Aufklärung der Anwender sind unabdingbar. Jedes Unternehmen tut gut daran, dies anzubieten und jedem Mitarbeiter sei empfohlen, die Angebote anzunehmen und nach entsprechenden Sicherheitsmaßnahmen nachzufragen.

Praxistipps

Was kann man nun als Einzelner konkret tun? Im Folgenden sind einige Anregungen aufgelistet, die Sie selbst prüfen und ggf. durchführen können.

1. Die wichtigste Regel: halten Sie Ihren Impfschutz aktuell. Verwenden Sie nur aktuelle Betriebssysteme (MacOS, iOS, Android, Linux, Windows 10) auf allen Ihren Geräten und insb. installieren Sie regelmäßig die angebotenen Updates. Beachten Sie auch, dass Ihre Netzwerkhardware (bspw. „Fritz!Box“, Drucker, …) regelmäßig Updates wollen und prüfen Sie deren Aktualität.

2. Prüfen Sie verwendete Daten und Dokumente auf Schadsoftware (bspw. mit Virenscannern), nutzen Sie keine Dokumente oder Software aus unbekannten Quellen.

3. Wenn ihr Bauchgefühl sensibel reagiert, fragen Sie bei unplausiblen Mails mit Links oder Anhängen lieber nochmals auf zweitem Weg (bspw. Telefon) um deren Authentizität nach.

4. Prüfen Sie Ihren Passwortschutz. Passwörter sollten in keinem Fall notiert werden (außer bspw. in sicheren Passwort-Safes). Mindestens 8 Buchstaben mit kombinierter Groß-/Kleinschreibung,

Sonderzeichen und Ziffern sind Pflicht. Verwenden Sie für unterschiedlichen Sicherheitsbedarf verschieden komplexe Zugangsdaten.

5. Vermeiden Sie unnötige Kopien und Ausdrucke von Daten. Diese sind meist weniger geschützt und können verloren gehen. Auch das Telefonat auf heimischen Balkon kann mitgehört, im Hausmüll entsorgte Fehldrucke mitgelesen, auf privatem USB-Stick angefertigte Kopien vergessen werden zu löschen.

6. Sichern Sie Ihre Systeme und aktivieren Datenschutzeinstellungen. Jeder Browser, jede Online-Anwendung, jede Software und jedes Betriebssystem werden im Auslieferungszustand nicht mit den datenschutzfreundlichsten Einstellungen ausgeliefert. Googlen Sie nach relevanten Sicherheitseinstellungen von Windows, iOS, Android und MacOS und Ihrer Bürosoftware, aktivieren Sie sicheres Surfen in Ihrem Firefox-, Chrome- und Edge-Browser, nutzen 2-Faktor-Authentifzierung bei Online-Diensten (bspw. „Amazon.de“, „Office365.de“, VPN-Zugang, Web-Mailer, …) wo immer möglich.

7. Sichere Kommunikationskanäle
HomeOffice wird auch Online-Konferenzen und Fernwartung mit sich bringen. Nutzen Sie hierbei nur seriöse Anbieter und schränken Sie den Fernzugriff auf die nur wirklich Berechtigten ein.

Oben stehende Tipps mögen sicherlich nur eine kleine Auswahl von Möglichkeiten zum Schutz darstellen. Wie aber in der Offline-Welt gilt aber auch bei Maßnahmen zur virtuellen Prävention: eine hundertprozentige Sicherheit gibt es nicht, jedes einzelne Detail kann aber das Infektionsrisiko erheblich minimieren. Kommen Sie also gesund und sicher durch die HomeOffice-Zeit!

Bleiben Sie gesund!

Ihr,

Stephan Michaelis LL.M.

Fachanwalt für Versicherungsrecht

Fachanwalt für Handels- und Gesellschaftsrecht