SANOVIS CONSULTING WITH CARE.

CURACON SICHERHEIT GEBEN. LÖSUNGEN BIETEN.

NEWSLETTER DATENSCHUTZ

Liebe Leserin, lieber Leser,

beruflich wie privat ist es den meisten IT-Nutzern wichtig, dass ihre personenbezogenen Daten geschützt sind. Doch der Weg dahin erscheint kompliziert. Hier sorgt Ihr Datenschutz-Newsletter für Abhilfe und informiert über relevante Entwicklungen.
So stellt sich die Frage, wie sich der Datenschutz im Homeoffice besser gewährleisten lässt, da diese Form des Arbeitens auch nach der Pandemie zum Berufsalltag vieler gehören wird. Die Probleme mit der Passwortsicherheit machen zudem biometrische Verfahren wie Fingerabdruck-Scanner interessant. Doch wann ist die Nutzung erlaubt?
Wie sensibel Gesundheitsdaten sind, macht nicht nur die aktuelle Lage deutlich. Deshalb ist es gut zu wissen, wie der Datenschutz bei der Übergabe einer Arztpraxis aussieht. Nicht zuletzt bereiten die Spam-Mails Kummer. Deshalb erfahren Sie, wie Sie Spam-Filter erfolgreicher einsetzen.

Wir wünschen Ihnen interessante Erkenntnisse beim Lesen!

Dr. Uwe Günther
Beratungsfeldleiter Datenschutz, Curacon GmbH
Geschäftsführer, Sanovis GmbH

Stefan Strüwe
Beratungsfeldleiter Datenschutz, Curacon GmbH

August_2021

1 SELBSTDATENSCHUTZ
IM HOMEOFFICE

Beschäftigte im Homeoffice sind in Fragen des Datenschutzes zwar nicht auf sich allein gestellt, aber ihr Anteil an Schutzmaßnahmen ist höher, als viele glauben. Es geht um mehr als die Sicherheit für Notebook und Smartphone.

Selbst sind die Frau und der Mann

In Zeiten der Corona-Pandemie ist die Zahl der Beschäftigten im Homeoffice deutlich gestiegen. Zu Beginn waren viele Maßnahmen noch temporär gedacht, mit heißer Nadel gestrickt und gerade im Bereich der Datensicherheit mehr ein Provisorium als eine Lösung auf Unternehmensniveau.

Inzwischen aber ist in vielen Unternehmen deutlich geworden, dass das Homeoffice nicht mehr komplett verschwinden wird. Im Gegenteil: Viele Firmen wollen das Homeoffice als gleichberechtigten Arbeitsplatz neben dem Büro im Firmengebäude erhalten. Man spricht dann von hybriden Arbeitsplätzen.

Doch wirklich gleichberechtigt sind Homeoffice und Büroschreibtisch in der Firma nicht. Denn der Firmenarbeitsplatz kann von den zentralen Maßnahmen der IT-Sicherheit profitieren. Im Homeoffice sind die Beschäftigten selbst gefragt, für die Sicherheit der personenbezogenen Daten stärker aktiv zu werden.

Betriebliche Notebooks und Smartphones reichen nicht

Wie eine Umfrage des Bundesamts für Sicherheit in der Informationstechnik (BSI) in der deutschen Wirtschaft ergab, verwenden nur 42 Prozent der Unternehmen ausschließlich betriebseigene IT in den Homeoffices. Die Mehrzahl der Unternehmen setzt also darauf, dass die Beschäftigten auch private Geräte betrieblich einsetzen.

Ist dies der Fall, müssen die Beschäftigten die eigenen Geräte wie Notebook und Smartphone genauso stark absichern, wie dies der Arbeitgeber mit den betrieblichen Geräten tut. Insbesondere müssen private und betriebliche Daten und Anwendungen strikt getrennt werden, der Zugriff privater Apps und unbefugter Dritter, wozu auch die eigene Familie der Beschäftigten zählt, auf betriebliche personenbezogene Daten muss ausgeschlossen werden.

Doch selbst die Bereitstellung von Smartphones und Notebooks durch den Arbeitgeber reicht nicht für den Datenschutz im Homeoffice, es ist mehr an Selbstdatenschutz gefragt.

Homeoffice muss sichere Umgebung werden

Tatsächlich nutzen selbst betriebliche Smartphones und Notebooks im Homeoffice auch Geräte, die eben doch private Geräte sind. Dies können die Drucker im Homeoffice sein, das Headset, die Webcam, die Maus, der Bildschirm und insbesondere der Internet-Router, mit dem die Verbindung ins Internet, aber meist auch die Verknüpfung mit dem Firmennetzwerk aufgebaut wird.

Internet-Router sind beliebte Angriffsziele für Hacker, denn sie werden häufig vernachlässigt. Die Sicherheitseinstellungen werden nicht kontrolliert, die Firmware des Routers nicht regelmäßig aktualisiert. Das WLAN-Passwort „kennen“ auch die Smart-Home-Anwendungen, die häufig so reich an Schwachstellen sind, dass ein Angreifer dort das Passwort auslesen kann, um dann den Datenverkehr im Homeoffice zu überwachen.

Nicht nur an die IT denken

Doch nicht nur die komplette private IT, die die Beschäftigten im Homeoffice nutzen, ist Gegenstand des Selbstdatenschutzes, da die IT-Sicherheitsabteilung des Arbeitgebers hier nicht aktiv wird. Auch die Dokumente auf dem heimischen Schreibtisch, die Ausdrucke im privaten Müll und die Telefonate auf dem Balkon oder der Terrasse können zu Datenschutz-Problemen führen.

Wer im Homeoffice arbeitet, muss an den Home-Datenschutz denken. Das umfasst etwa auch das Absperren der heimischen Bürotür, wenn andernfalls unbefugte Zugriffe auf Daten und Dokumente möglich werden könnten.

2 WANN IST DIE ZUGRIFFSKONTROLLE DURCH FINGERABDRUCK O.K.?

Der Scan des Fingerabdrucks schützt Rechner besonders effektiv vor unbefugten Zugriffen. In bestimmten Fällen darf der Arbeitgeber ausdrücklich verlangen, dass Beschäftigte diese Methode nutzen.

Fingerabdrücke sind besonders geschützt

Fingerabdrücke gehören zu den biometrischen Daten. Biometrische Daten sagen unmittelbar etwas über den Körper eines Menschen aus. Deshalb sind sie besonders geschützt.

Ihre Verarbeitung ist nur unter engen Voraussetzungen zulässig. Das ordnet die Datenschutz-Grundverordnung (DSGVO) für biometrische Daten an, wenn sie „zur eindeutigen Identifizierung einer natürlichen Person“ geeignet sind.

Es passt zur Fürsorgepflicht des Arbeitgebers

Das gilt auch im Arbeitsleben. Daran ist nichts Überraschendes. Das Arbeitsrecht kennt die Fürsorge-pflicht des Arbeitgebers. Sie bringt zum Ausdruck, dass die persönlichen Belange von Arbeitnehmerin-nen und Arbeitnehmern im Arbeitsalltag wichtig sind. Sie schafft einen geschützten Rahmen, in dem der Arbeitnehmer seine Arbeitsleistung erbringt.

Die Einzelheiten regelt das BDSG

Manchmal ist eine ordnungsgemäße Arbeitsleistung nur möglich, wenn dabei Daten des Arbeitnehmers verarbeitet werden. Hierzu trifft das Bundesdatenschutzgesetz (BDSG) einige Regelungen. Solche ergänzenden nationalen Vorschriften macht die DSGVO für das Arbeitsleben ausdrücklich möglich.

Zweistufige rechtliche Prüfung bei Fingerabdrücken

Das BDSG sieht eine zweistufige Betrachtung vor. Dies lässt sich am Beispiel von Fingerabdrücken sehr gut zeigen:

- Stufe 1: Zunächst muss feststehen, dass das Scannen von Fingerabdrücken notwendig ist, damit der Arbeitnehmer seine Arbeitsleistung ordnungsgemäß erbringen kann.
- Stufe 2: Anschließend ist zu prüfen, ob im konkreten Einzelfall ausnahmsweise trotzdem schutzwürdige Interessen des Arbeitnehmers den Vorrang haben. Sollte das der Fall sein, wäre das Scannen zwar an sich erforderlich, aber im Ergebnis trotzdem nicht zulässig.

Im Normalfall ist ein Fingerabdruck-Scan übertrieben

Im normalen Büroalltag ist es nicht erforderlich, den Zugriff auf einen Rechner durch das Scannen eines Fingerabdrucks abzusichern. Sofern die „üblichen Bürodaten“ wie etwa Daten von Bestellungen und Lieferungen verarbeitet werden, wäre das schlicht übertrieben. Natürlich brauchen auch solche Daten einen Schutz gegen unbefugte Zugriffe. Dafür genügen aber die üblichen Mittel wie Passwörter und das Sperren des Bildschirms, wenn einige Zeit keine Eingabe mehr erfolgt ist.

Das macht den Büroalltag unbequemer

Für solche Situationen ist das Scannen von Fingerabdrücken nicht erforderlich. Damit fehlt es an den Voraussetzungen der Stufe 1. Der Arbeitgeber darf in diesen Fällen solche Scans nicht vorsehen. Dies gilt auch dann, wenn es den betroffenen Arbeitnehmern eigentlich ganz recht wäre. Denn für sie wäre es oft bequemer, den Daumen auf einen Scanner zu legen, statt

ein Passwort einzugeben, das sie auch noch regelmäßig ändern müssen. Eine Betriebsvereinbarung zu dem Thema könnte weiterhelfen. Eine Einwilligung des Arbeitnehmers sehen die Datenschutzbehörden dagegen mit Skepsis.

In Sonderfällen ist ein Fingerabdruck-Scan geboten

Manchmal ist der Einsatz von Fingerabdruck-Scans erforderlich. Das gilt vor allem für sicherheitssensible Bereiche. Ein Beispiel hierfür ist die Arbeit an technischen Entwicklungen, die später zum Patent angemeldet werden sollen. Ein weiteres Beispiel ist die Durchführung von Aufträgen, die staatlichen Geheimhaltungsvorschriften unterliegen. Dies kommt etwa bei Lieferanten der Bundeswehr vor. Solche Fälle erfüllen die Voraussetzungen der Stufe 1.

Schutzwürdige Interessen stehen fast nie entgegen

Die Prüfung der Stufe 2 ergibt nur ganz selten, dass dennoch schutzwürdige Interessen von Arbeitnehmern als vorrangig anzusehen sind. Denn selbstverständlich wird der Arbeitnehmer schon im eigenen Interesse strikt darauf achten, wer beispielsweise Zugriff auf die Scan-Daten hat. Sonst würde der Schutz, den er mit ihrer Hilfe anstrebt, sofort wieder unterlaufen.

Schutzmaßnahmen brauchen immer ein Gesamtkonzept!

Als einzige Schutzmaßnahme reicht der Einsatz von Fingerabdruck-Scans normalerweise nicht aus. Vor allem das automatische Sperren des Bildschirms, wenn einige Zeit keine Eingabe erfolgt ist, ist zusätzlich notwendig. Und eine ganz banale Absicherung sollte man ebenfalls nie vergessen: Ein PC ist heutzutage so klein, dass er leicht in einer Tasche Platz findet. Es ist deshalb ein Schutz dagegen notwendig, dass ihn ein „Langfinger“ einfach mitnimmt. Jede einzelne Sicherungsmaßnahme taugt eben nur so viel wie das Gesamtkonzept, zu dem sie gehört!

3 DIE PRAXISÜBERNAHME
UND DAS „ZWEI-SCHRANK-MODELL“

Was passiert eigentlich mit Behandlungsunterlagen, wenn eine Nachfolgerin oder ein Nachfolger eine Arztpraxis übernimmt oder wenn eine neue Betriebsärztin auf den bisherigen Betriebsarzt folgt? Das „Zwei-Schrank-Modell“ stellt in solchen Fällen den Datenschutz sicher.

Höchster Schutz für medizinische Daten

Wer sich ärztlich behandeln lässt, erwartet für seine Daten höchsten Schutz. Die ärztliche Schweigepflicht spielt dabei eine zentrale Rolle. Sie muss auch dann gewahrt bleiben, wenn ein Nachfolger eine Arztpraxis übernimmt oder wenn der Betriebsarzt wechselt.

Aufbewahrungspflicht von zehn Jahren

Rein rechtlich ist alles klar: Nach Abschluss einer Behandlung muss ein Arzt die Patientenakte zehn Jahre lang aufbewahren. Das steht so in § 630f Abs. 3 Bürgerliches Gesetzbuch (BGB). Diese Pflicht besteht fort, wenn ein Arzt beispielsweise in den Ruhestand tritt und die Praxis an einen Nachfolger übergibt. Die Patientenunterlagen müssen weiterhin zuverlässig geschützt sein.

Zu schnell steht die Aufbewahrungspflicht nur auf dem Papier

Doch wie lässt sich das in der Praxis sicherstellen? Der bisherige Praxisinhaber will sich im Ruhestand um die Unterlagen nicht mehr kümmern. Und ein Betriebsarzt, der ausgeschieden ist, hat inzwischen auch anderes zu tun. Verständlich, dass er sich mit den vorhandenen Unterlagen am liebsten nicht mehr befassen möchte.

Die Elemente des „Zwei-Schrank-Modells“

Einen Ausweg aus diesem Dilemma bietet das „Zwei-Schrank-Modell“. Die Datenschutzaufsichtsbehörden empfehlen es. Inzwischen ist es allgemein üblich. Für klassische Patientenakten auf Papier funktioniert es in einer Arztpraxis so:

- Man stellt in der Arztpraxis zwei Schränke auf.
- In Schrank 1 kommen die Unterlagen, die bei der Tätigkeit des bisherigen Praxisinhabers entstanden sind. Sie werden eingeschlossen.
- Schrank 2 ist zunächst völlig leer.
- Den Schlüssel für beide Schränke erhält der Praxisnachfolger.
- Der bisherige Inhaber der Praxis und sein Nachfolger schließen einen Vertrag. Darin verpflichtet sich der Nachfolger, die vorhandenen Unterlagen streng gesichert in Schrank 1 aufzubewahren.
- Kommt ein Patient des bisherigen Praxisinhabers zum Nachfolger, fragt dieser den Patienten, ob er den Zugriff auf die vorhandenen Unterlagen erlaubt.
- Meist ist das der Fall. Dann wird Schrank 1 geöffnet und die dort vorhandenen Unterlagen des Patienten kommen in Schrank 2.
- Nach einiger Zeit hat sich Schrank 1 meist ziemlich geleert und Schrank 2 ziemlich gefüllt.
- Die „Restunterlagen“ in Schrank 1 bleiben dort, bis die Aufbewahrungsfrist von zehn Jahren abgelaufen ist. Dann werden diese Unterlagen datenschutzgerecht vernichtet.

Das Modell funktioniert auch bei elektronischen Unterlagen

Das Beispiel der klassischen Patientenakten auf Papier ist besonders leicht nachzuvollziehen. Das Modell funktioniert jedoch auch, wenn die Patientenunterlagen in elektronischer Form vorhanden sind. In wenigen Jahren dürfte das die Regel sein. In diesem Fall wird das „Zwei-Schrank-Modell“ einfach elektronisch nachgebildet.

Der vorhandene Datenbestand wird bei der Übergabe der Praxis gesperrt und besonders gegen Zugriff gesichert. Erst wenn der Patient gegenüber dem Praxisnachfolger zustimmt, schaltet der Praxisnachfolger den Datensatz frei. Das muss er selbstverständlich nicht unbedingt persönlich tun. Auch jemand aus dem Sprechstundenteam, der dafür besonders eingewiesen ist, kann das erledigen.

Besonders datenschutzkonform: die Protokollierung von Zugriffen

Die elektronische Variante ist besonders datenschutzkonform. Bei ihr ist es problemlos möglich, jeden Zugriff zu protokollieren. Wenn die Protokollierung richtig eingerichtet ist, lassen sich die gespeicherten Daten im Nachhinein nicht mehr verändern. Dann lässt sich bei etwaigen Beschwerden leicht feststellen, ob alles ordnungsgemäß abgelaufen ist oder nicht.

Kleine Besonderheiten beim Wechsel des Betriebsarztes möglich

Beim Wechsel des Betriebsarztes lässt sich das Modell an die Strukturen anpassen, die jeweils vorhanden sind. Manche Unternehmen haben die Funktion des Betriebsarztes bei einer externen Praxis angesiedelt, die auch die Patientenunterlagen aufbewahrt. Dann passt alles, was bisher gesagt wurde, 1:1. Bei anderen Unternehmen erfolgt die Aufbewahrung der Patientenunterlagen im Unternehmen selbst. Zugriff hat dabei selbstverständlich nur der Betriebsarzt. In diesem Fall müsste der Schlüssel für die vorhandenen Unterlagen so lange beim bisherigen Betriebsarzt bleiben, bis ein neuer Betriebsarzt bestimmt ist.

4 SCHLUSS MIT SPAM:

SO ARBEITEN SPAM-FILTER MIT MEHR ERFOLG

Unerwünschte Mails, Chat-Nachrichten und Anrufe – Spam hat viele Gesichter. Spam-Filter sollen die Spam-Flut eindämmen. Dazu müssen sie aber richtig eingesetzt werden. Werden sie nicht trainiert, bleiben Spam-Filter erfolglos und dumm, die Spam-Mails weiterhin eine Plage und ein Datenrisiko.

Spam ist mehr als lästig

Zu Beginn des Arbeitstags ruft man seine E-Mails ab, unter den erschreckend vielen Mails, die über Nacht eingetroffen sind, befinden sich zahlreiche Spam-Mails. Ist dies der Fall, sortiert der Mail-Server offensichtlich die Spam-Mails nicht oder nicht gut genug aus. Oder aber der lokale Spam-Filter im E-Mail-Programm verdient wohl seinen Namen nicht.

Wenn man aber viele Spam-Mails im Posteingang hat, ist dies nicht nur ärgerlich. Es kostet Zeit und Nerven, nicht zuletzt kann man versehentlich legitime Mails löschen oder Spam-Mails ungewollt öffnen. Wenn die Spam-Versender dann noch das Öffnen registrieren (über Mail-Tracking), wird die Zahl der Spam-Attacken weiter steigen. Bringt die Spam-Mail Schadsoftware mit, ist schnell der Computer oder das Smartphone verseucht.

Spam-Filter können helfen, wenn man ihnen hilft

Nun stellt sich die Frage, warum die genutzten Spam-Filter diese vielen lästigen und sogar gefährlichen Mails nicht aussortieren. Darauf gibt es mehr als eine Antwort. Zum einen werden die kriminellen Spam-Versender, die Spammer, immer besser. Viele Spam-Mails sind also inzwischen besser getarnt als früher. Dabei hilft den Spammern auch künstliche Intelligenz, die die Spam-Inhalte optimieren, ja sogar auf die Opfer gezielt anpassen kann.

Ein weiteres Problem sind die Spam-Filter selbst, die nicht so eingesetzt werden, wie es eigentlich sein soll. Auch in den Spam-Filtern wird inzwischen zunehmend Maschinelles Lernen eingesetzt. Sie sollen also mit der Zeit immer besser, also immer genauer werden, weniger Spam-Mails übersehen und möglichst keine legitime Mail als Spam einstufen. Dazu müssen die Nutzer aber mit den Spam-Filtern arbeiten.

Das richtige Training für Spam-Filter

Neue Spam-Filter sind relativ dumm. Treffen im Posteingang also viele Spam-Mails ein, sollte man diese nicht einfach löschen, sondern als Spam markieren. Das verschiebt diese Spam-Nachrichten nicht nur in den Spam-Ordner. Man teilt dem Spam-Filter auch mit, dass er einen Fehler gemacht hat.

Umgekehrt sollte man legitime Nachrichten, die in den Spam-Ordner geschoben wurden, von der Spam-Markierung befreien. Das verschiebt sie wieder in den Posteingang und trainiert erneut den Spam-Filter, denn auch hier hat er Fehler gemacht.

Natürlich wird der Spam-Filter nie alles richtigmachen, aber er wird mit der Zeit besser. Je nach Anbieter für den Spam-Filter wird er auch durch externe Updates schlauer gemacht, aber ohne das Training durch Sie als Nutzer geht es nicht. Nur der Mail-Empfänger selbst kann die individuellen Vorgaben machen, die der Spam-Filter kennen muss. Diese Vorgaben macht man durch Markieren als Spam und durch Entfernen der Spam-Markierung.

Dies mag nach Aufwand aussehen, zahlt sich später aber aus. Ein gut trainierter Spam-Filter, der den Datenschutz beachtet, also nichts über

den Nutzer verrät, ist ein wichtiger Teil der E-Mail-Sicherheit.

Haben Sie Spam-Mails im Griff?
Machen Sie den Test!

Übersieht ein Spam-Filter viele Spam-Mails, lohnt sich der Einsatz nicht. Stimmt das?

1. Nein, dann muss man den Spam-Filter besser trainieren, also die übersehenen Spam-Mails mit einer Markierung als Spam versehen.
2. Ja, denn, wenn man selbst die Spam-Mails aussortiert, braucht man keinen zusätzlichen Spam-Filter.

Lösung:

Die Antwort 1 ist richtig. Spam-Filter müssen trainiert werden. Sie sollten schon zu Anfang möglichst viel (offensichtlichen) Spam erkennen und in den Spam-Ordner verschieben. Aber wenn ein Nutzer einen ungewöhnlichen Newsletter abonniert hat, ist eine Einstufung als Spam für Dritte vielleicht richtig, für den Nutzer selbst jedoch nicht. Nur der Nutzer kann die genauen Vorgaben machen.

Markiere ich etwas als Spam, verschiebt dies die Nachricht nur in den Spam-Ordner. Stimmt das?

1. Ja, die Spam-Markierung sorgt für die Sortierung in „Spam“ und „kein Spam“.
2. Nein, das trainiert zusätzlich den Spam-Filter. Die Wahrscheinlichkeit, dass der Filter in Zukunft selbst die Spam-Markierung richtig setzt, steigt.

Lösung:

Die Antwort 2 ist richtig. Wer in seinem Mail-Programm etwas als Spam markiert, hilft dem Spam-Filter und räumt gleichzeitig auf. Wer dagegen Spam-Mails einfach löscht oder anders verschiebt, der teilt dem Spam-Filter nicht mit, dass er etwas übersehen hat. Doch nur mit diesem Training kann der Spam-Filter besser werden und der E-Mail-Sicherheit sowie dem Datenschutz in Zukunft besser helfen.

Spam-Filter gibt es übrigens nicht nur für E-Mail, sondern zum Beispiel auch für SMS und Anrufe auf dem Mobiltelefon sowie für Chat-Nachrichten. Denn auch darüber können Spammer unerwünschte Nachrichten senden.

IMPRESSUM

Redaktion
Dr. Uwe Günther
Sanovis GmbH
Riedenburger Straße 7
81677 München
089 9927579-22
Uwe.Guenther@Sanovis.com

Stefan Strüwe, RA
CURACON GmbH Wirtschaftsprüfungsgesellschaft
Am Mittelhafen 14
48155 Münster
0251 92208-209
Stefan.Struewe@Curacon.de