SANOVIS CONSULTING WITH CARE.

CURACON SICHERHEIT GEBEN. LÖSUNGEN BIETEN.

NEWSLETTER DATENSCHUTZ

Liebe Leserin, lieber Leser,

auch in besonderen Zeiten wie der Corona-Pandemie müssen die Vorgaben des Datenschutzes eingehalten werden. Man kann auch sagen: Gerade in solchen Zeiten. Denn sie sind mit besonderen Risiken verbunden, auf die man mit dem richtigen Datenschutz antworten muss.
Diese Ausgabe betrachtet deshalb, wie Sie am besten auf die erhöhte Gefahr durch Phishing-Mails rund um Corona reagieren und wie sich der Datenschutz auch im Homeoffice gewährleisten lässt. Weitere besondere Situationen liegen vor, wenn der Betriebsarzt Ihre sensiblen Gesundheitsdaten verarbeitet oder wenn Sie auf die Mails eines ausgeschiedenen Kollegen zugreifen wollen. Der Datenschutz hat jeweils eine Antwort, wie Sie richtig reagieren.

Wir wünschen Ihnen interessante Erkenntnisse beim Lesen!

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

Stefan Strüwe
Geschäftsfeldleiter Datenschutz, Curacon GmbH

Juni_2020

1 WENN HOHER INFORMATIONSBEDARF ZUM RISIKO WIRD

Datendiebe nutzen das große Interesse an Informationen zur aktuellen Lage aus, um Zugangsdaten auszuspionieren. Ein Schutz vor Phishing-Mails darf jetzt nicht fehlen.

Vorsicht vor gefälschten Webseiten und Phishing-Mails

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat eine Zunahme von Cyberangriffen mit Bezug zum Coronavirus beobachtet. So werden Unternehmen per E-Mail aufgefordert, persönliche oder unternehmensbezogene Daten auf gefälschten Webseiten preiszugeben. Die Cyberkriminellen geben sich zum Beispiel als vermeintliche Institutionen zur Beantragung von Soforthilfegeldern aus. Die betrügerisch erlangten Daten werden anschließend für kriminelle Aktivitäten missbraucht.

Das erhöhte Informationsbedürfnis im Internet nutzen Cyberkriminelle auch auf anderen Wegen aus. So konnte das BSI eine deutliche Zunahme an Registrierungen von Internetadressen mit Schlagwörtern wie „corona“ oder „covid“ beobachten.
Neben der Nutzung für legitime Informationsangebote werden viele dieser Internetadressen für kriminelle Aktivitäten missbraucht. Nutzer werden auf solchen Webseiten zum Download von Informationen aufgefordert. Tatsächlich infiziert das die Systeme der Nutzer mit Schadprogrammen. Ebenso werden Spam-Mails mit vermeintlichen Informationen in Bezug auf Corona im Dateianhang verschickt, um Schadprogramme zu verbreiten.

Phishing-Attacken nutzen psychologische Tricks

Die Corona-Krise ist dabei nur ein Thema, das Angreifer bei Phishing-Attacken ausnutzen, um die Zugangsdaten der Mail-Empfänger zu erbeuten. Immer wenn sich Menschen für etwas besonders interessieren, besteht für die Angreifer eine größere Chance, für ihre Attacken viele Opfer zu finden.

In einer ernsten Lage werden zudem Vorsichtsmaßnahmen beiseitegelegt, um möglichst schnell an die wichtigen Informationen zu kommen. Wenn man sich um die Gesundheit der Familie oder der Beschäftigten sorgt, scheinen die Bedenken um den Datenschutz nicht nur zweitrangig zu sein, man denkt einfach nicht mehr daran.
Deshalb ist es wichtig, beim Phishing-Schutz auch auf Lösungen zu setzen, die sich nicht mit psychologischen Tricks aushebeln lassen, Lösungen, die automatisiert nach Anzeichen für Mail-Attacken suchen. Deshalb sind jetzt Phishing-Filter wichtig, die lokal im Mail-Programm arbeiten und regelmäßig mit neuen Kennzeichen für Attacken aktualisiert werden.

Phishing-Schutz aus Mensch und Maschine

Jeder Nutzer von digitalen Kommunikationslösungen wie Mail und Chat sollte besonders vorsichtig sein und nicht einfach Links in Mails oder in Suchmaschinen anklicken, sondern die korrekte Internetadresse direkt in den Webbrowser eintippen.
Zusätzlich zu dieser Vorsichtsmaßnahme sollten im Mail-Programm und im Browser die Phishing-Filter aktiviert sein, die Internetadressen gegen bekannte, bösartige Webadressen abgleichen können. Automatisierter Phishing-Schutz und menschliche Awareness sorgen dann gemeinsam für den Datenschutz in Krisenzeiten.

2 ZUGRIFF AUF E-MAILS

AUSGESCHIEDENER MITARBEITER

Der Mail-Account ist noch da, der Mitarbeiter ist aber ausgeschieden. Darf der Arbeitgeber „einfach so“ auf die Mails in dem Account zugreifen? Oder ist das nur zulässig, wenn der Mitarbeiter einwilligt? Mit etwas gesundem Menschenverstand lassen sich diese Fragen leichter lösen, als viele befürchten.

Im Normalfall: keine Probleme

Normalerweise sollte es so laufen: Ein Mitarbeiter scheidet aus dem Unternehmen aus. Der Grund dafür spielt dabei keine Rolle. In jedem Fall sollte er alle wichtigen Mails einem Kollegen übergeben, der sich künftig um darum kümmert.

Unerwartete Hindernisse

Manchmal läuft es freilich anders. Dazu ein Beispiel: Die Übergabe der Mails war für den vorletzten Arbeitstag des Mitarbeiters vorgesehen. Leider war der Kollege, der die Mails entgegennehmen sollte, ab dem Tag aber krank. Nun ist der ausgeschiedene Mitarbeiter weg. Den Zugriff auf den Account bekäme die EDV-Abteilung technisch hin. Aber dann tauchen plötzlich Bedenken auf, ob ein solcher Zugriff erlaubt ist.

Betriebsvereinbarung als Lösung

Falls ein Unternehmen einen Betriebsrat hat, gibt es häufig eine Betriebsvereinbarung zu dem Thema. Aber was, wenn es entweder keinen Betriebsrat gibt oder ausgerechnet dazu keine Betriebsvereinbarung?

Gegenseitige Rücksicht als Maßstab

Die Antwort fällt relativ leicht, wenn man sich zwei Dinge vor Augen hält:

- In keinem Fall ist der dienstliche Mail-Account eines Mitarbeiters seine reine Privatsache. Der Hauptzweck des Accounts besteht darin, damit Aufgaben für das Unternehmen zu erledigen. Beispiele: Es gehen Bestellungen von Kunden ein oder der Mitarbeiter beantwortet Anfragen von Kunden.
- Andererseits muss ein Arbeitgeber Rücksicht auf die persönlichen Interessen des Mitarbeiters nehmen. Das wird dann wichtig, wenn Mails im Account offensichtlich einen privaten Inhalt haben.

Das Gewicht dieser beiden Aspekte hängt davon ab, ob private E-Mails erlaubt sind oder nicht.

Verbot privater Mails durch den Arbeitgeber

Am einfachsten ist es, wenn private E-Mails ausdrücklich verboten sind. Dann gehört der Mail-Account gewissermaßen ganz dem Arbeitgeber. Deshalb kann er nach Belieben darauf zugreifen. Eine Einwilligung des ausgeschiedenen Mitarbeiters ist dafür nicht notwendig.

Doch Vorsicht: Auch in solchen Fällen gibt es Grenzen. Klassisches Beispiel: Schon aus dem Betreff einer Mail lässt sich erkennen, dass sie einen rein privaten Inhalt hat. Die Fairness gebietet es, den ausgeschiedenen Mitarbeiter auf die Mail hinzuweisen und sie ihm zu übermitteln, wenn er das möchte.

Keine „Belohnung eines Regelverstoßes“

Das wirkt auf den ersten Blick etwas merkwürdig. Denn schließlich hat das Unternehmen private Mails doch ausdrücklich verboten. Warum soll es dann Rücksicht nehmen müssen? Nun, kaum jemand kann es völlig verhindern, dass ihm andere Personen private Mails ins Büro schicken. Damit muss ein Arbeitgeber dann in fairer Weise umgehen.

Erlaubnis privater Mails durch den Arbeitgeber

Komplizierter wird es, wenn der Arbeitgeber private Mails ausdrücklich erlaubt hat. Damit hat er bildlich gesprochen seine Herrschaft über den Mail-Account des Mitarbeiters aufgegeben. Der Arbeitgeber muss in solchen Fällen davon

ausgehen, dass ein relevanter Teil der Mails im Account rein privater Natur ist.

Aufforderung zum „Sortieren“

Die Rücksicht auf die persönlichen Interessen des Mitarbeiters muss deshalb hier im Vordergrund stehen. Vom Grundsatz her darf der Arbeitgeber deshalb nicht auf den Mail-Account des Mitarbeiters zugreifen. Er muss vielmehr mit ihm Kontakt aufnehmen und ihn dazu auffordern, die dienstlichen Mails auszusortieren.

Berechtigtes Interesse des Arbeitgebers

Daran hat der Arbeitgeber ein berechtigtes Interesse. Denn diese Mails sind notwendig, um die Aufgaben des Unternehmens zu erfüllen. Deshalb darf der ehemalige Mitarbeiter sich auch nicht „einfach so“ weigern, seinen früheren Arbeitgeber beim Aussortieren zu unterstützen.

Sollte sich der ehemalige Mitarbeiter dennoch querlegen, kann sein ehemaliger Arbeitgeber durchaus rechtliche Schritte beim Arbeitsgericht einleiten. In dringenden Fällen wäre sogar eine einstweilige Verfügung denkbar.

Zwei Lösungsmöglichkeiten

Das sind jedoch Extremsituationen, die in der Praxis kaum vorkommen. Im Normalfall einigen sich der ehemalige Mitarbeiter und sein ehemaliger Arbeitgeber einvernehmlich auf eine von zwei Möglichkeiten:

- Entweder erklärt sich der frühere Mitarbeiter mit dem Zugriff einverstanden. Dann sorgt sein Ex-Arbeitgeber dafür, dass lediglich die dienstlichen Mails anhand des Betreffs aussortiert werden.
- Oder der frühere Mitarbeiter greift nochmals auf den Account zu und übernimmt diese Sortierarbeit selbst.

In beiden Fällen sind die berechtigten Interessen beider Seiten gewahrt.

3 SCHUTZ VON DATEN BEIM BETRIEBSARZT

Ein Betriebsarzt ist in vielen Fällen gesetzlich vorgeschrieben. In jedem Fall liegt seine Tätigkeit auch im Interesse der Arbeitnehmer. Aber wie sieht es bei ihm mit der Verschwiegenheit aus? Können sich Arbeitnehmer auf Geheimhaltung verlassen? Die klare Antwort lautet: Ja! Dennoch gibt es viele interessante Details, die man kennen sollte.

Klassisches Beispiel: Eignungsuntersuchung

Wie ein Betriebsarzt arbeitet, lässt sich gut am Beispiel einer Eignungsuntersuchung erklären. Ein Mitarbeiter soll im Unternehmen eine völlig neue Aufgabe übernehmen. Mit ihr sind körperliche Belastungen verbunden, denen der Mitarbeiter bisher nicht ausgesetzt war. Deshalb beauftragt der Arbeitgeber den Betriebsarzt, eine Eignungsuntersuchung durchzuführen.

Intensive Erhebung von Daten

Bei dieser Untersuchung befragt der Betriebsarzt den Mitarbeiter intensiv zu seinem Gesundheitszustand. Auch die Frage, an welchen

Krankheiten er leidet, spielt dabei eine Rolle. Ferner hält der Betriebsarzt wesentliche körperliche Daten fest wie etwa Gewicht und Blutdruck. Der Betriebsarzt kommt zu dem Ergebnis, dass der Mitarbeiter für die neue Aufgabe gesundheitlich geeignet ist.

Mitteilung lediglich des Ergebnisses an den Arbeitgeber

Dem Arbeitgeber teilt der Betriebsarzt lediglich dieses Ergebnis mit. Die Mitteilung beschränkt sich also auf die Aussage: „geeignet für die neue Aufgabe“. Warum der Betriebsarzt zu diesem Ergebnis gekommen ist, erfährt der Arbeitgeber nicht. Körperliche Daten wie etwa das Gewicht oder Diagnosen wie Bluthochdruck sind für den Arbeitgeber tabu.

Umfassende Mitteilung an den Mitarbeiter

Gegenüber dem Mitarbeiter kann der Betriebsarzt dagegen völlig offen sein. Manchmal hat er sogar die Pflicht, ihm gegenüber deutlich zu werden. Das gilt zum Beispiel dann, wenn er etwas feststellt, das für den Arbeitnehmer gefährlich ist. So mag ein ungewöhnlich hoher Blutdruck zwar kein Hindernis für die neue Aufgabe im Unternehmen sein. Anlass für einen ernsten Hinweis auf mögliche gesundheitliche Folgen ist er aber allemal.

Der Betriebsarzt als Arzt

Das Beispiel der Eignungsuntersuchung zeigt die Rolle eines Betriebsarztes sehr deutlich:
Zunächst einmal ist er ohne Wenn und Aber Arzt. Er unterliegt also derselben Sorgfaltspflicht wie jeder andere Arzt auch.
Selbstverständlich gilt für ihn auch die ärztliche Schweigepflicht. Dies gilt unabhängig davon, ob der Betriebsarzt als Angestellter des Unternehmens intern tätig ist oder ob es sich um einen externen Betriebsarzt handelt. Ein externer Betriebsarzt betreibt eine eigene Praxis und kommt nur im Bedarfsfall in das Unternehmen.

Notwendiges Einverständnis des Arbeitnehmers

Auskünfte über medizinische Sachverhalte darf ein Betriebsarzt dem Arbeitgeber nur geben, wenn der betroffene Arbeitnehmer damit einverstanden ist. Das gilt auch bei einer Eignungsuntersuchung.

Was das bedeutet, wird an einem eher absurden Beispiel besonders deutlich: Die Eignungsuntersuchung fällt zwar positiv aus. Der Mitarbeiter möchte aber dennoch nicht, dass der Betriebsarzt dies dem Arbeitgeber mitteilt. Dann muss der Betriebsarzt diesen Wunsch erfüllen. Allerdings muss der Arbeitnehmer dann auch damit leben, dass er ohne Bestätigung der Eignung den neuen Job nicht bekommen wird.

Erforderlichkeit als Maßstab

In jedem Fall darf der Arbeitgeber nur die medizinischen Informationen erhalten, die für den konkreten Anlass erforderlich sind. Deshalb erfährt er bei einer Eignungsuntersuchung in der Regel nur das Ergebnis „geeignet/nicht geeignet“.
Manchmal genügt dies aber nicht. So ist es etwa denkbar, dass der Mitarbeiter grundsätzlich für die neue Tätigkeit geeignet ist, aber einzelne Einschränkungen zu beachten sind. Klassisches Beispiel: Der Mitarbeiter kann zwar Lasten heben. Sie dürfen aber nicht schwerer als zehn Kilo sein. Dann ist diese Information für den Arbeitgeber notwendig, damit er die Eignung einschätzen kann.

Organisatorische Vorkehrungen

Auch bei einem internen Betriebsarzt steht die ärztliche Schweigepflicht keineswegs nur auf dem Papier. Vor allem sind betriebsärztliche Unterlagen auf keinen Fall Bestandteil der Personalakten. Der Betriebsarzt muss sie vielmehr selbst unter Verschluss halten. Scheidet ein Betriebsarzt aus, darf er die Unterlagen seinem Nachfolger zur Verfügung stellen.

Kein Problem ist es, wenn ein externer Betriebsarzt die erforderlichen Unterlagen im Unternehmen aufbewahrt und nicht in seiner Praxis. Dann ist jedoch beispielsweise ein gesonderter Schrank erforderlich, für den nur der Betriebsarzt den Schlüssel hat.

4 DATENSICHERHEIT IM HOMEOFFICE

Arbeiten im Homeoffice war für viele ein lang gehegter Wunsch. Kommt es aber tatsächlich dazu, ist die Umsetzung gar nicht so einfach. Das gilt auch für die Einhaltung der Datenschutzvorgaben, die am heimischen Schreibtisch genauso wie im Büro gelten.

Homeoffice zwischen Wunsch und Pflicht

Von den Berufstätigen arbeitet mittlerweile fast jeder Zweite (49 Prozent) ganz oder zumindest teilweise im Homeoffice, so eine Umfrage des Digitalverbands Bitkom. Nicht alle Unternehmen und Beschäftigten haben sich aus freien Stücken dafür entschieden.

18 Prozent durften vor der Corona-Pandemie gar nicht im Homeoffice arbeiten und machen das jetzt zeitweise (15 Prozent) oder ganz (drei Prozent). Weitere 31 Prozent konnten bereits vorher im Homeoffice tätig sein und tun das jetzt häufiger (17 Prozent) oder ganz (14 Prozent). Nur 41 Prozent der Beschäftigten sagt, ihre Tätigkeit sei grundsätzlich nicht für Homeoffice geeignet.

Keine Frage: Arbeiten im Homeoffice ist eine Entwicklung, die weiter zunimmt und die auch nach den Krisenzeiten bestehen bleiben wird. Für den Datenschutz bleibt dies aber nicht ohne Folgen.

Viele waren nicht auf Homeoffice vorbereitet

„Für viele Mitarbeiterinnen und Mitarbeiter heißt es gerade: Ab sofort Homeoffice! Viele Unternehmen und Behörden kannten dies bisher gar nicht oder nur in Ausnahmefällen. Deswegen wird vielerorts gerade improvisiert, um den Betrieb am Laufen zu halten und dabei die Bedürfnisse aller Beschäftigten möglichst gut zu erfüllen“, so Marit Hansen, die Landesbeauftragte für Datenschutz Schleswig-Holstein.

Nutzung Doch technische und organisatorische Sicherheitsmaßnahmen sind wichtig für das Arbeiten am Computer, mit Papierdokumenten oder auch beim Telefonieren. Für den Fall, dass doch einmal eine Datenpanne passiert, müssen alle Beschäftigten wissen, wem sie dies melden.

Wie der Bundesverband IT-Sicherheit e.V. (TeleTrusT) ermittelt hat, steht es um die Datensicherheit im Homeoffice nicht gut. So findet man wichtige Sicherheitsmaßnahmen bei Weiten nicht an allen heimischen Schreibtischen:

Nur 65 % haben ihren Rechner passwortgeschützt, 63 % haben das WLAN passwortgeschützt, 61 % haben ein Virenschutzprogramm installiert, 41 % nutzen E-Mail-Verschlüsselung und 37 % eine VPN-Verbindung. 12 % sagen sogar, sie haben keine Datensicherheit im Homeoffice.

Mehr Datensicherheit im Homeoffice

Der Digitalverband Bitkom hat Empfehlungen zusammengestellt, wie das Arbeiten am Schreibtisch daheim sicherer wird, darunter: aktuelle Softwareversionen sowie Antivirensoftware verwenden und regelmäßig Updates installieren

- VPN-Zugang nutzen, falls keine Cloud-basierten Dienste eingesetzt werden
- komplexe Passwörter benutzen, um den Rechner zu entsperren, und für Online-Dienste, die man damit nutzt
- wo immer möglich Zwei-Faktor-Authentifizierung einsetzen
- Festplatten verschlüsseln, insbesondere in Notebooks
- Rechner sperren, wenn man nicht am Schreibtisch sitzt

Ohne eine solche Datensicherheit kann eine datenschutzkonforme Arbeit im Homeoffice nicht gelingen. Aber selbst mit einer dem Risiko angemessenen IT-Sicherheit gibt es Einschränkungen für die Arbeit im Homeoffice: Nicht alle Tätigkeiten dürfen im Homeoffice geleistet werden, beispielsweise schließen dies einige Auftragsverarbeitungsverträge aus. Die Datenschutzvorgaben müssen weiter eingehalten werden, sie bleiben nicht zurück im Büro, sondern kommen mit ins Homeoffice

Achten Sie auf den Datenschutz im Homeoffice? Machen Sie den Test!

Wenn der Arbeitgeber ein sicheres Notebook für das Homeoffice mitgibt, sind die Anforderungen an die Datensicherheit automatisch erfüllt. Stimmt das?

1. Nein, es müssen mehr Maßnahmen erfolgen, um sicheres Arbeiten im Homeoffice zu ermöglichen.
2. Ja, dann ist die Sicherheit die gleiche wie im Unternehmen selbst.

Lösung:

Die Antwort 1. ist richtig. Nur wenn das Firmen-Notebook keine Verbindung zum Internet oder ins Firmennetzwerk aufnimmt und keine Speichermedien oder weiteren Geräte angeschlossen werden, könnte man von einem sicheren Notebook ausgehen. Ansonsten müssen die Datenverbindungen und alle Schnittstellen zusätzlich abgesichert werden.

Im Homeoffice dürfen alle Arbeiten erledigt werden, die man auch sonst im Büro durchführt. Stimmt das?

1. Ja, immerhin nutzt man ja das Firmen-Notebook.
2. Nein, es gibt Einschränkungen. Denn nicht alle Daten dürfen einfach mit ins Homeoffice genommen werden.

Lösung:

Die Antwort 2. ist richtig. Es muss genau festgelegt und geregelt werden, welche personenbezogenen Daten das Unternehmen verlassen und im Homeoffice verarbeitet werden dürfen. Hierzu müssen Verträge und Rechtsgrundlagen überprüft werden. Ebenso muss bedacht werden, dass das Homeoffice mit zusätzlichen Risiken verbunden ist, die ohne entsprechende Gegenmaßnahmen eine Verarbeitung bestimmter Daten nicht möglich machen.

Ein Tipp der Aufsichtsbehörden: Die grundlegende Frage, die Sie sich stellen sollten, ist die, ob Sie überhaupt dringend an Aufgaben mit personenbezogenen Daten arbeiten müssen. Wenn Sie zunächst an Aufgaben ohne Personenbezug und ohne andere sensible Daten arbeiten, können Sie sich an die neue Situation gewöhnen und Erfahrungen sammeln. Dann gewinnen Sie auch Zeit für die Umsetzung der Regeln

IMPRESSUM

Redaktion
Dr. Uwe Günther
Sanovis GmbH
Richard-Strauss-Straße 69
81679 München
089-99 27 579 22
Uwe.Guenther@Sanovis.com

Stefan Strüwe, RA
CURACON GmbH Wirtschaftsprüfungsgesellschaft
Am Mittelhafen 14
48155 Münster
02 51-92 208 209
Stefan.Struewe@Curacon.de