Datenschutz *aktuell - Ausgabe Dezember 2021*

Der Datenschutz-Newsletter aus Nürnberg

Sehr geehrte Damen und Herren,
liebe Leserinnen und Leser,

heute präsentiere ich Ihnen die letzte Ausgabe des Datenschutz-Newsletters aus Nürnberg. Nach wie vor wird auch unser Geschäftsleben von der vorherrschenden Corona Pandemie dominiert.

Seit dem Jahr 2018 wird der Datenschutz von der Datenschutz-Grundverordnung (DSGVO) bestimmt. Regel wurden aufgestellt und diese Regeln müssen umgesetzt und eingehalten werden. Wichtig ist mir hierbei pragmatische Lösungen zu finden und diese im täglichen Geschäftsbetrieb umzusetzen. Hierfür soll dieser regelmäßige Infobrief einen kleinen Beitrag leisten.

Ich wünsche Ihnen zum Ende des Jahres 2021 ein paar geruhsame Tage und einen erfolgreichen Start in ein hoffentlich dann wieder normalisiertes Geschäftsleben.

Wie immer stehe ich für Ihre Fragen immer gerne zur Verfügung.

Mit vielen Grüßen aus Nürnberg

Ihr Peter Brandmann
(Externer Datenschutzbeauftragter)

Aufgepasst bei Online-Videokonferenzen!

Statt persönlicher Besprechungen vor Ort finden vermehrt Videokonferenzen über das Internet statt. Viele dieser Online-Services sind leicht zu bedienen, so scheint es. In Wirklichkeit aber gibt es einiges zu beachten, damit Ihre Privatsphäre geschützt bleibt.

Live aus dem Homeoffice

Unter dem Eindruck der Coronakrise hat sich das Arbeiten in vielen Branchen verändert. 95 Prozent der Unternehmen ersetzen Präsenztreffen durch Videokonferenzen, so eine Umfrage des Digitalverbands Bitkom. Wenn Sie gegenwärtig auch im Homeoffice arbeiten, kennen Sie sicherlich die beliebten Videokonferenz-Dienste wie Zoom oder Teams.

Für die Durchführung von Online-Besprechungen oder die Teilnahme daran ist kaum eine Installation erforderlich. Browser, Webcam, Mikrofon, Lautsprecher und gute Internetverbindung reichen. Entsprechend oft am Tag nimmt man an einem der Online-Meetings teil. Das ist bereits so stark Teil des beruflichen Alltags geworden, dass manche Teilnehmer vergessen, dass die Webcam oder das Mikrofon schon oder noch angeschaltet ist. So werden Bilder und Töne übertragen, die eigentlich nicht für die Öffentlichkeit bestimmt waren. Doch die Privatsphäre ist noch stärker in Gefahr.

Datenschützer und Sicherheitsbehörden geben wichtige Hinweise

Die Aufsichtsbehörden für den Datenschutz haben eine Orientierungshilfe zu Videokonferenzsystemen veröffentlicht und geben darin auch wichtige Hinweise, die die Nutzerinnen und Nutzer betreffen. Daraus ergeben sich Punkte, die Sie bei Online-Videokonferenzen beachten sollten.

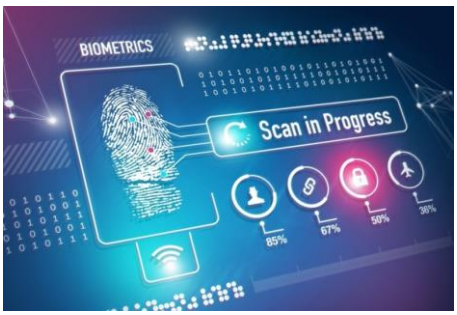
Zum einen ist es wichtig, nur im Unternehmen freigegebene Dienste zu nutzen, auch dann, wenn Sie im Rahmen Ihrer beruflichen Tätigkeit selbst eine Online-Konferenz planen und dazu einladen.

Zum anderen sollten Sie auf bestimmte technische und organisatorische Maßnahmen achten, um Ihre Privatsphäre besser zu schützen, wie das BSI (Bundesamt für Sicherheit in der Informationstechnik) unterstreicht:

- Stellen Sie sicher, dass nur die Personen an Ihrem Online-Treffen teilnehmen, die Sie auch eingeladen haben – das geht beispielsweise mit einer komplexen PIN für Ihren virtuellen Raum.
- Überschreiben Sie die Standardvorgaben der Raumbezeichnung und Ihrer Nutzerkennung durch individuelle Namen. Achten Sie darauf, dass Sie keine trivialen Passwörter, Nutzerkennungen oder PINs vergeben.
- Geben Sie nur die nötigsten Daten ein, wenn Sie sich für den Dienst registrieren müssen.
- Machen Sie sich bewusst, was Sie zeigen, wenn Sie den Bildschirm teilen. Wenn Sie Daten austauschen, können auch Schadprogramme übertragen werden.
- Schließen Sie Sicherheitslücken, indem Sie Updates installieren.
- Achten Sie darauf, dass im genutzten Webbrowser eine aktive Verschlüsselung bestätigt wird, zum Beispiel in der Adresszeile des Browsers durch „https“.
- Schalten Sie Webcam und Mikrofon nur ein, wenn Sie diese wirklich brauchen, und deaktivieren Sie danach diese Funktionen wieder.
- Nutzen Sie für die Webcam am besten eine Abdeckung, die sich vor- und wegschieben lässt.

Beherzigen Sie diese Sicherheitshinweise, um von sich und Ihrem Homeoffice nicht mehr preiszugeben, als Sie wollen.

Gesichtserkennung, Fingerscan & Co.: Bequem, aber nicht ohne Risiko



Passwörter muss man sich merken, seine Fingerabdrücke nicht. Entsprechend beliebt sind biometrische Verfahren bei der Anmeldung für Geräte und Applikationen. Doch der Datenschutz warnt davor, Biometrie vorschnell einzuführen. Warum eigentlich?

Werden Passwörter bald überflüssig?

In einer Umfrage von Cisco unter 500 Anwenderinnen und Anwendern zeigte sich, dass Fingerabdrücke ein beliebter Ersatz für Passwörter sind. Mehr als die Hälfte (55 Prozent) fühlt sich wohl dabei, den Fingerabdruck für den Zugang zu einem Online-Konto zu verwenden. 40 Prozent haben nichts gegen eine Gesichtserkennung einzuwenden.

Tatsächlich ersetzen Unternehmen den Passwortschutz zunehmend durch andere Sicherheitsverfahren. Das gilt vor allem für die Nutzung der Biometrie in Form von Fingerabdrücken und Gesichtserkennung. Smartphones und andere mobile Endgeräte haben Funktionen zur Anmeldung über Fingerabdruck oder Gesichtserkennung gleich an Bord. Entsprechend häufig erfolgt auch die Anmeldung darüber, wenn sich Beschäftigte im Homeoffice befinden oder unterwegs arbeiten.

Laut einer Umfrage der FIDO Alliance unter 1.000 befragten Deutschen gelten biometrische Verfahren nicht nur als bequem, sondern auch als sicherste Art der Identitätsprüfung. Viele Studien gehen deshalb davon aus, dass Passwörter kaum noch eine Zukunft haben, die Biometrie wird sie ersetzen.

Sollte sich der Datenschutz darüber nicht freuen, wo doch so große Probleme mit ausreichend starken Passwörtern bestehen? Ja und nein, lautet die Antwort.

Passwörter kann man tauschen, Fingerabdrücke nicht

Wollen Unternehmen biometrische Lösungen einsetzen, fordert der Datenschutz, die Risiken genau zu prüfen. Dafür gibt es gute Gründe: Biometrische Daten und ihre Analyse eignen sich zwar sehr gut als Identitätsnachweis. Gelangen biometrische Daten aber in die falschen Hände, lassen sie sich für einen Identitätsdiebstahl nutzen.

Haben Angreifer Passwörter gestohlen, kann und muss man sie ersetzen. Bei biometrischen Merkmalen wie den Fingerabdrücken oder dem Gesicht kann man jedoch nicht beliebig neue, eindeutige Kennzeichen wählen. Man hat nur ein Gesicht und eine begrenzte Zahl von Fingerkuppen.

Biometrische Daten lassen sich missbrauchen

Im Gegensatz zu einem Passwort, das sich bekanntlich nicht mit der jeweiligen Person in Verbindung bringen lassen sollte, also zum Beispiel nicht den Namen enthalten soll, haben biometrische Daten sehr wohl mit der Person zu tun. So lässt sich ein Gesichtsausdruck nicht nur nutzen, um eine Person zu identifizieren. Es sind auch weitere Analysen möglich, wie eine Studie des EU-Parlaments warnt. So könnten sich darüber zum Beispiel menschliche Zustände der betroffenen Person leichter identifizieren lassen, wie Angst, Müdigkeit oder Krankheit, so die Studie.

Biometrie erfordert hohe Sicherheit

Wer also den Komfort einer Anmeldung über Gesichtserkennung oder Fingerabdruck nutzen will, muss das Verfahren besonders gut absichern. Das will der Datenschutz sicherstellen, um Missbrauch zu verhindern. Aus diesem Grund fordert der Datenschutz eine Prüfung vor der Einführung von Biometrie – nicht um die Passwort-Probleme zu erhalten, sondern um die Daten der betroffenen Personen zu schützen.

Denken Sie deshalb auch bei privater Nutzung von Fingerscan und Gesichtserkennung daran, nicht einfach jedes Verfahren zu verwenden. Stehlen Angreifer Ihre biometrischen Muster, sind Ihre privaten und beruflichen Zugänge in Gefahr, wenn sie durch Biometrie geschützt werden.

Kennen Sie die Risiken der Biometrie? Machen Sie den Test!

Frage: Die Erkennung von Fingerabdrücken ist sicher, denn einen Fingerabdruck kann niemand fälschen. Stimmt das?

1. Nein, man muss Fingerabdrücke nämlich nicht fälschen, um eine Identität vorzutäuschen. Man kann die Muster der Fingerabdrücke auch stehlen, um sie zu missbrauchen.
2. Ja, Fingerabdrücke sind im Gegensatz zu Passwörtern absolut sicher.

Lösung: Die Antwort 1. ist richtig. Aus den Fingerabdrücken der Nutzerinnen und Nutzer werden bei biometrischen Anmeldeverfahren Muster errechnet und gespeichert. Gelingt es einem Angreifer, diese

errechneten Muster zu stehlen, kann er die biometrische Überprüfung der Identität täuschen und die Identität der Person übernehmen. Biometrische Verfahren müssen deshalb gegen Angriffe abgesichert sein.

Frage: Biometrische Daten lassen sich nicht für andere Zwecke missbrauchen. Stimmt das?

1. Ja, man nutzt die Fingerabdrücke und die Gesichtserkennung nur, um die Identität einer Person zu prüfen.
2. Nein, biometrische Kennzeichen können mehr über eine Person verraten als die zu prüfende Identität.

Lösung: Die Antwort 2. ist richtig. So kann man zum Beispiel aus einem Gesichtsausdruck mittels Analyse versuchen, Rückschlüsse auf Stimmungen, auf das Alter oder auf Anzeichen für Krankheiten zu ziehen. Biometrische Merkmale sind nicht nur ein möglicher Passwortersatz, sie sind Teil des menschlichen Körpers und können deshalb auch mehr über die Person aussagen als ein sinnvoll gewähltes Passwort, das bekanntlich keine personenbezogenen Angaben enthalten sollte.

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.

Impressum
Redaktion: Peter Brandmann (V.i.S.d.P.)
Externer Datenschutzbeauftragter - Zert. Fachkraft DSGVO
Anschrift:
pb beratung & training
Schnepfenreuther Weg 51
90425 Nürnberg

Telefon: 0911/3506118
E-Mail: peter.brandmann@pb-beratung-training.de