Newsletter Datenschutz

Datenschutz *aktuell - Ausgabe 01-2021*

Der Datenschutz-Newsletter aus Nürnberg

Liebe Leserinnen und Leser,

anbei erhalten Sie die neueste Ausgabe des Datenschutz Newsletters.
Gerne können Sie diese Informationen auch weiter verteilen.

Mit den besten Grüßen aus Nürnberg
Ihr Peter Brandmann

Homeoffice – was sollte ich beachten?

Homeoffice von heute auf morgen wegen Corona ist eine Herausforderung. Vieles ist zu organisieren. Der Datenschutz sollte dabei mit im Blick sein. Jede und jeder kann leicht einige einfache Dinge beachten. Das bewirkt oft erstaunlich viel.

Einsatz privater Geräte nur nach Absprache

Homeoffice geht nicht ohne EDV. Wer dafür ein dienstliches Gerät zur Verfügung hat, darf nur dieses Gerät verwenden. Der Einsatz privater Geräte verlangt eine Absprache mit dem Arbeitgeber, zumindest mit dem unmittelbaren Vorgesetzten. Das muss nicht unbedingt schriftlich geschehen. Aber zumindest ein kurzer Mail-Austausch ist sinnvoll. Private Geräte können zusätzliche Risiken für den Datenschutz mit sich bringen, die am gewohnten Arbeitsplatz nicht bestehen würden.

Besonders wichtig: Updates und Virenschutz

Gerade bei privaten Geräten sind die Standardregeln der Datensicherheit zu beachten. Dazu gehören vor allem regelmäßige Updates! Am regulären Arbeitsplatz sorgt dafür oft die EDV-Abteilung, ohne dass man etwas davon merkt. Bei privaten Geräten muss sich jede und jeder selbst darum kümmern. Dasselbe gilt für den Virenschutz.

Bildschirmschoner zum Schutz der Daten

Ein Bildschirmschoner sollte Standard sein. Stellen Sie ihn so ein, dass er nach einigen Minuten ohne Aktivität „anspringt“. Das sorgt dafür, dass Familienangehörige und Besucher möglichst keine Daten sehen können. Besonders wichtig ist das, wenn Sie keinen besonderen Raum für das Homeoffice haben. Manchmal hilft es auch weiter, den Bildschirm etwas zu drehen, damit nicht jeder, der den Raum betritt, gleich alles sieht.

Tücken beim privaten Telefon

Weil der Empfang am Festnetz-Telefon oft besser ist, nutzen erstaunlich viele im Homeoffice nicht das Diensthandy, sondern den privaten Telefonanschluss. Dabei gerät oft in Vergessenheit, dass es in jedem Telefon Anruflisten gibt. Teils lässt sich diese Funktion schlicht ausschalten. Dann ist das Problem gelöst. Wenn das nicht geht oder nicht gewünscht ist, ist ein regelmäßiges Löschen der Listen nötig. Zumindest einmal in der Woche sollte

man dies fest einplanen.

Papierunterlagen sicher aufbewahren!

Ganz ohne Papier geht es meistens auch im Homeoffice nicht. Wer Unterlagen aus dem regulären Büro mit nach Hause nimmt, ist für sie verantwortlich. Ein eigenes Zimmer für das Homeoffice bleibt für viele ein Traum. Aber mit der Aufbewahrung in einem abgeschlossenen Schrank/Rollschrank ist auch schon viel gewonnen.

Altpapier datenschutzkonform beseitigen!

Wo Papier benutzt wird, fällt auch Abfallpapier an. Vielleicht haben Sie ohnehin privat einen kleinen Aktenvernichter im Haus. Egal, ob er nun den Vorgaben für Bürogeräte voll entspricht – es ist besser als nichts. Keinesfalls dürfen Sie Abfallpapier mit personenbezogenen Daten „einfach so“ in die heimische Papiertonne stecken.

Corona als Auslöser von Kreativität?

Vielleicht bietet das Homeoffice aber auch einen guten Anlass dazu, von Abläufen mit Papier auf elektronische Abläufe umzustellen. Das geht erstaunlich oft. Corona kann auch kreativ machen!

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.

Office 365 – ein Datenschutzproblem?

In der Fachpresse, aber auch in den allgemeinen Medien war in letzter Zeit zu lesen, dass Office 365 Schwachstellen beim Datenschutz aufweisen soll. Um was geht es dabei? Muss diese Diskussion den „normalen Nutzer“ überhaupt interessieren? Und wenn ja: Was kann und muss er selbst tun?

Office 365 als Palette von Online-Anwendungen

Office 365, ein Produkt von Microsoft, bietet den Zugriff auf eine ganze Reihe von Webanwendungen, von Outlook über Excel bis OneDrive. Sie stehen dem Anwender online zur Verfügung. Der Marktanteil von Office 365 ist hoch und wächst seit Jahren. Kein Wunder, dass Fragen des Datenschutzes rund um Office 365 große Aufmerksamkeit finden.

Kritik der Datenschutzbehörden

In der letzten Zeit war da und dort verkürzt zu lesen, Office 365 verstoße gegen den Datenschutz und dürfe bald nicht mehr eingesetzt werden. Um es gleich zu sagen: Das ist natürlich nicht richtig. Die Aufsichtsbehörden haben nicht etwa angekündigt, den Einsatz von Office 365 zu verbieten. Vielmehr haben sie mit knapper Mehrheit (also nicht etwa einstimmig) festgestellt, dass derzeit kein datenschutzgerechter Einsatz von Office 365 möglich sei.

Diese Aussage ist eine Art Zwischennachricht. Im Augenblick laufen Verhandlungen zwischen den Aufsichtsbehörden und Microsoft. Dabei werden die aufgetretenen Fragen diskutiert. Das wird mit Sicherheit eine gewisse Zeit brauchen. Von den Ergebnissen wird über kurz oder lang zu hören sein.

Unproblematische Verwendung von Daten

Die Aufsichtsbehörden haben einige Fragen aufgeworfen, die recht interessant sind. Dabei geht es vor allem um den Vertrag zwischen Microsoft und den Unternehmen oder Verwaltungen, die Office 365 einsetzen. Dort ist geregelt, wofür Microsoft die personenbezogenen Daten verwendet, die von den Nutzern übermittelt werden.

Ein Punkt ist dabei völlig unproblematisch: Microsoft verwendet diese Daten, um die vereinbarten Dienste zu erbringen. Wenn etwa Outlook funktionieren soll, dann muss Microsoft die Daten verarbeiten, die dafür notwendig

sind. Das Versenden einer E-Mail klappt beispielsweise nur, wenn die nötige E-Mail-Adresse vorhanden ist und zum Versenden der Mail benutzt wird. Daran gibt es auch keine Kritik.

Verwendung von Daten für „Geschäftstätigkeiten“

Schwieriger wird es, weil Microsoft laut Vertrag Daten auch für „legitime Geschäftstätigkeiten von Microsoft“ verwenden darf. Diese Formulierung ist recht allgemein. Deshalb stellt sich die Frage, ob Unternehmen, die Office 365 nutzen, Microsoft Daten für diesen Zweck zur Verfügung stellen dürfen. In mancherlei Hinsicht lautet die Antwort eindeutig Ja. Das gilt etwa für die Abrechnung von Dienstleistungen, die Microsoft erbringt. Bei anderen Punkten ist dies nicht so eindeutig. So ist die Bekämpfung von Betrug und Cyberkriminalität sicher eine wichtige Angelegenheit. Hier kann man allerdings schon diskutieren, welche Daten dafür konkret erforderlich sind und deshalb an Microsoft übermittelt werden dürfen.

Feld für Fachleute

Diese wenigen Beispiele zeigen, dass es hier um Fragen für Datenschutz-Fachleute geht. Wie exakt müssen vertragliche Bestimmungen sein? Welche technischen Sicherungsmaßnahmen muss Microsoft vorhalten? Das ist alles wichtig. Für den normalen Anwender von Office 365 im Büro lohnt es aber nicht, sich damit zu befassen. Anders wäre das nur, wenn er aus privater Leidenschaft tief in Fragen des Datenschutzes einsteigen will.

Fragen an sich selbst stellen!

Reicht es also, sich ruhig zurückzulehnen und Office 365 einfach zu nutzen, ohne lange zu überlegen? Das wäre auch wieder zu einfach gedacht. Vielmehr sollte gerade der normale Nutzer im Büro einmal kurz nachdenken, was er alles mit Office 365 macht. Das ist im Normalfall erstaunlich viel. Von Mails war schon die Rede. Aber auch einige Gedanken darüber, was so alles in Excel-Tabellen steht, könnten sinnvoll sein.

Vorgaben des Arbeitgebers beachten!

Auf der Basis der Frage „Was tue ich hier eigentlich?“ sollte der Nutzer dann überlegen, ob er sich dabei an die Vorgaben des Unternehmens hält, bei dem er arbeitet. Ist die Excel-Tabelle vielleicht um die eine oder andere Spalte erweitert, weil das so praktisch erschien? Oder hatte das Unternehmen eine solche Spalte vielleicht bewusst nicht vorgesehen?

Eigene Verantwortung sehen!

Das sind Fragen, die nicht Microsoft betreffen. Man sollte nie vergessen, dass auch Office 365 nur ein Werkzeug ist. Solange es nicht benutzt wird, speichert es keinerlei Daten und gibt auch keine weiter. Wenn es Daten speichert und weitergibt, dann hat das der Nutzer ausgelöst. Dafür ist er verantwortlich und nicht Microsoft.

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