Gemeinsam Außergewöhnliches erreichen

ronau-it
Dipl.-Ing. (FH) Roger Naumer

Datenschutz *Now!*

Die Mitarbeiterzeitung zum Datenschutz

Ausgabe 01/2021

Liebe Leserin, lieber Leser,

die eigenen personenbezogenen Daten zu schützen, ist eine immer anspruchsvollere Aufgabe. Die vermehrte Arbeit im Homeoffice und die Nutzung von Online-Videokonferenzen sind Beispiele dafür. Ihre aktuelle Ausgabe gibt Ihnen deshalb wichtige Hinweise, worauf Sie bei Online-Meetings achten sollten. Ebenso erfahren Sie, inwiefern die aktuelle Datenschutz-Diskussion um Office 365 Sie betrifft.

In weiteren Beiträgen lesen Sie, wie Ihnen die sogenannte Cyberfibel sowohl beruflich als auch privat helfen kann, mehr für IT-Sicherheit und Datenschutz zu tun. Nicht wirklich hilfreich sind hingegen viele Datenschutzerklärungen. Deshalb erhalten Sie in dieser Ausgabe Einblicke, was bestimmte Begriffe in den Privacy Policies von Webseiten bedeuten. Nur verständliche Datenschutzrichtlinien machen die Datennutzung transparent.

Ich wünsche Ihnen interessante Informationen!

Roger Naumer - der Datenschutzbeauftragte Ihres Vertrauens

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.

Mehr Sicherheit mit der Cyberfibel

Sind Mails oder Chat-Beiträge wirklich sicher gegen den Zugriff durch Fremde? Beim Online-Banking muss man eine App verwenden. Bringt das echt mehr Sicherheit? Solche und ähnliche Fragen stellen sich immer wieder, egal ob Sie beruflich oder privat im Internet unterwegs sind. Informieren Sie sich mit der Cyberfibel!

Ein Gemeinschaftsprojekt hoch seriöser Akteure

Die Cyberfibel ist ein Gemeinschaftsprojekt von hoch anerkannten Unternehmen und Institutionen. Beteiligt sind unter anderem der Digitalverband Bitkom, Unternehmen wie die DATEV und das Bundesamt für Sicherheit in der Informationstechnik (BSI). Sie haben das gemeinsame Ziel, Verbraucherinnen und Verbrauchern die Kompetenz zu vermitteln, die sie für das Thema „Sicherheit im Internet“ brauchen. Die Schirmherrschaft hat das Bundesinnenministerium übernommen.

Die zwei Säulen der Cyberfibel

Die Cyberfibel umfasst zwei Säulen. Sie stehen gleichberechtigt nebeneinander:

- Der erste Teil „Digitale Lebenswelten“ zeigt alltägliche Anwendungsbereiche digitaler Technologien im privaten und beruflichen Alltag. Dabei geht es unter anderem darum, die eigenen Verhaltensweisen im Internet zu reflektieren.
- Der zweite Teil „Digitale Kompetenzen“ thematisiert Risiken in der Online-Welt und gibt praktische Empfehlungen, wie man sich und seine Geräte vor möglichen Bedrohungen aus dem Netz schützen kann.

Einstieg an jeder Stelle der Cyberfibel möglich

Wichtig und sehr praktisch: Alle „Lebenswelten“ und „Kompetenzen“ lassen sich sowohl nacheinander als auch unabhängig voneinander betrachten. Sie bauen nicht aufeinander auf.

Überblick zu den fünf „Lebenswelten“

Der Einstieg in die Cyberfibel gelingt besonders nah am Alltag über fünf „Lebenswelten“ als Ausgangspunkt:

- Online dabei sein und ins Netz starten
- Online einkaufen und bezahlen
- Online vernetzen und austauschen
- Online Reisen planen und vernetzt mobil sein
- Online sein in Haus und Freizeit

„Online einkaufen und bezahlen“ als Beispiel

In Zeiten von Corona und Lockdown dürfte die Lebenswelt „Online einkaufen und bezahlen“ besonders interessieren. Klickt man sie an, geht es mit diesem Text weiter:

„In der Lebenswelt ‚Online einkaufen und bezahlen‘ lernen Sie:

- was Onlineshopping ist und wie Sie passende Angebote im Internet finden,
- was Profilbildung und personalisierte Werbung ist,
- wie Sie Onlineplattformen sicher nutzen,
- wie Bankgeschäfte (z. B. Überweisungen oder Aktienhandel) über das Internet und andere Bezahlverfahren per App funktionieren.

Die Übungen in den einzelnen Abschnitten ermöglichen es Ihnen auf einfache Weise, Ihr Wissen auch an andere weiterzugeben.“

Erwerb von Kompetenz durch praktische Übungen

Die Übungen führen mitten in die Praxis. So lautet eine Übung zum Online-Banking:

- Recherchieren Sie im Internet nach „Demo-Konto Onlinebanking“.
- Wählen Sie aus der Ergebnisliste einen Treffer aus, der offensichtlich zu einem Test eines Onlinebanking-Zugangs führt.
- Nutzen Sie den Testzugang und verschaffen Sie sich einen Überblick, welche Möglichkeiten das Onlinebanking bietet.
- Finden Sie alle Funktionen, die Sie für Ihre Bankgeschäfte benötigen (zum Beispiel Kontostand, Überweisungen, Daueraufträge).

Linktipps führen weiter

Vor den Übungen stehen jeweils „Linktipps“. Sie führen zu gut gestalteten und seriösen Internetseiten. Beim Online-Banking gibt die Cyberfibel zwei Linktipps:

- Goldene Regeln für die sichere Nutzung des Mobile Banking, herausgegeben vom Bundesamt für Sicherheit in der Informationstechnik
- Phishing-Radar, herausgegeben von der Verbraucherzentrale.

Überblick zu den sieben „Digitalen Kompetenzen“

Neben den fünf Lebenswelten stehen sieben „Digitale Kompetenzen“. Dabei geht es um folgende Themen:

- Sichere Interneteinstellungen
- Geräte und Software sicher einrichten und pflegen
- Sichere Logins nutzen
- Daten schützen und sichern
- Sicher digital kommunizieren
- Sichere Transaktionen
- EXTRA: Risiken verstehen

„Stationen“ als Andockpunkte

Die Themen führen jeweils zu sogenannten „Stationen“. Beim Thema „Sichere Logins nutzen“ stößt man beispielsweise auf die drei Stationen „Einrichtung sicherer Passwörter“, „Einrichtung eines Passwortmanagers“ und „2-Faktor-Authentisierung“.

Zusammen macht es mehr Spaß!

Die Cyberfibel kann man am Bildschirm allein durcharbeiten. Bei den Übungen finden sich aber auch durchgehend Vorschläge für Gruppenarbeiten mit mehreren Personen. Solche Gruppenarbeiten sind sehr gut in Videokonferenzen möglich.

Der Zugang zur Cyberfibel

Der Zugang zur Cyberfibel ist einfach und leicht zu merken: www.cyberfibel.de. Gibt man den Begriff „Cyberfibel“ über eine Suchmaschine wie Google ein, findet man den Zugang als ersten Treffer.

Datenschutzerklärungen besser verstehen

Eine aktuelle Studie zeigt, dass viele Datenschutzerklärungen nicht verständlich genug sind. Entsprechend häufig verzichten Internetnutzer darauf, die sogenannten Privacy Policies zu lesen. Doch darunter kann der persönliche Datenschutz leiden.

Von wegen Erklärung des Datenschutzes

Online-Angebote wie Websites und Webshops müssen eine Datenschutzerklärung besitzen, so verlangt es nicht erst die Datenschutz-Grundverordnung (DSGVO). Trotzdem gibt es immer noch Webseiten, die keine „Privacy Policy“ veröffentlichen.

Andere Online-Dienste haben zwar eine Datenschutzerklärung, doch diese verdient ihren Namen nicht: Sie erklärt nicht den Datenschutz – jedenfalls nicht so, wie es für den normalen Internetnutzer erforderlich wäre.

Umfrage belegt unzureichende Erklärungen

Eine aktuelle Studie hat die Datenschutzrichtlinien führender Social-Media-Plattformen untersucht. Deren Nutzer wurden zudem befragt, um herauszufinden, wie lesbar die Datenschutzerklärungen wirklich sind. Dabei wurden die Altersgruppen berücksichtigt, die die jeweilige Social-Media-Plattform nutzen dürfen.

Hier sind einige der Ergebnisse:

- 87 % der Menschen akzeptieren Datenschutzrichtlinien, ohne sie zu lesen.
- Die Datenschutzrichtlinie von TikTok zum Beispiel erfordert ein Lesealter von 17+ Jahren, trotz der Möglichkeit, sich ab dem Alter von 13 Jahren dafür anzumelden.
- Im Durchschnitt dauert es mehr als 47 Minuten, um die Datenschutzrichtlinien für soziale Medien zu lesen. Die Datenschutzrichtlinien von TikTok, WhatsApp und LinkedIn gehören zu den längsten.
- API (62 %), Cookies (57 %), Drittanbieter (53 %) und IP-Adresse (46 %) stehen ganz oben auf der Liste des Fachjargons für Datenschutzrichtlinien, die die Menschen nicht verstehen.

Offensichtlich vermeiden die meisten Internetnutzer, Datenschutzerklärungen zu prüfen, da sie zu komplex, zu lang und unverständlich sind. Damit entsprechen die Datenschutzerklärungen nicht den Vorgaben der DSGVO. Zudem können die Nutzer von ihren Rechten keinen Gebrauch machen. Denn für sie ist die Datennutzung nicht transparent.

Datenschutz verstehen, um die eigenen Daten schützen zu können

Wenn Sie eine Datenschutzerklärung lesen und etwas nicht verstehen, dann geht es vielen Kolleginnen und Kollegen sicher genauso. Fragen Sie deshalb Ihre Ansprechpartner im Unternehmen für den Datenschutz und bitten Sie um eine Erklärung. Nur so können Sie und die anderen Beschäftigten im Unternehmen wirklich von Ihren Rechten Gebrauch machen und auf die Nutzung eines Online-Dienstes bewusst verzichten, weil Sie mit dem dort praktizierten Datenschutz nicht einverstanden sind.

An dieser Stelle seien die Begriffe erklärt, die für besonders viele Menschen unverständlich sind.

Haben Sie den Durchblick bei Datenschutzerklärungen? Machen Sie den Test!

Können Sie sagen, was sich hinter API, Cookies, Drittanbieter und IP-Adresse verbirgt? Überlegen Sie zuerst und lesen Sie danach die Auflösung!

Frage: Wissen Sie, was „API“ bedeutet?

API steht für Application Programming Interface, also für eine Schnittstelle, über die der genutzte Online-Dienst mit anderen Anwendungen verbunden werden kann. Über solche Schnittstellen lassen sich zum Beispiel die personenbezogenen Daten von der genutzten Webseite an andere Anwendungen übertragen. Dabei stellt sich die Frage, an wen und zu welchem Zweck die Daten übertragen werden sollen.

Frage: Was machen Cookies eigentlich?

Cookies werden von Internet- und Multimedia-Anwendungen genutzt, um Informationen lokal auf dem Computer oder Smartphone des Nutzers zu speichern. Cookies tragen in der Regel eine eindeutige Kennzeichnung (Cookie-ID), um die gespeicherten Informationen einem bestimmten Computer oder Smartphone zuordnen zu können. Über die Identifizierung des Geräts könnte jedoch auch eine Identifizierung des Nutzers möglich werden, wenn sich die Cookie-ID mit weiteren nutzerspezifischen personenbezogenen Daten verknüpfen lässt. Cookies, die nicht aus technischen Gründen nötig sind (zum Beispiel für den Warenkorb in einem Online-Shop), bedürfen der informierten Einwilligung durch den betroffenen Nutzer.

Frage: Was genau sind Drittanbieter?

Drittanbieter sind andere Unternehmen, die Daten des Nutzers vom Betreiber der Webseite erhalten könnten. Bestimmte Produkte bzw. Dienste von Drittanbietern verarbeiten die personenbezogenen Daten der Nutzer, die für die Zwecke des jeweiligen Webseiten-Anbieters erhoben wurden, auch zu ihren eigenen Zwecken. Hier stellt sich die Frage, ob der Nutzer hierzu genau informiert wurde und dem überhaupt zugestimmt hat. Andernfalls fehlt die rechtliche Grundlage für die Übermittlung der Daten an Drittanbieter.

Frage: Was steckt hinter der IP-Adresse?

Eine *IP-Adresse* (IP steht für Internet Protocol) identifiziert eindeutig Sender und Empfänger von Datenpaketen im Internet, ähnlich einer Postadresse. Sie verrät Informationen über den Internetanbieter und den Standort des Rechners. Der Internetanbieter wiederum kann über sie auch den Datenstrom seiner Kunden nachverfolgen. IP-Adressen lassen sich direkt oder indirekt mit Nutzern in Verbindung bringen und werden deshalb als personenbezogen eingestuft. IP-Adressen unterliegen dem Datenschutz und dürfen nicht ohne Weiteres zu Marketingzwecken vollständig gespeichert und ausgewertet werden.

Impressum

Redaktion:

Roger Naumer
Datenschutzbeauftragter

Anschrift:

ronau-it, Dipl.-Ing.(FH) Roger Naumer
Am Wiesgraben 3
67245 Lambsheim

Telefon: +49 (0)6233/459-2833
E-Mail: kontakt@ronau-it.de