DATENSCHUTZ UND DATENSICHERHEIT
ZUSAMMENFASSUNG DES MODULS

#DABEI-Geschichten – eine Initiative der Deutschen Telekom AG

ERLEBEN, WAS VERBINDET.

IMPRESSUM

HERAUSGEBER

#DABEI-Geschichten – eine Initiative der Deutschen Telekom AG
Barbara Costanzo, Vice President Group Social Engagement
Friedrich-Ebert-Allee 140, 53113 Bonn

WEITERFÜHRENDE INFORMATIONEN	STAND	STATUS
https://dabei-geschichten.telekom.com/themen/datenschutz-und-sicherheit/	09.01.2020	veröffentlicht

KONTAKT

engagement-bonn@telekom.de

GRUNDLAGEN DATENSCHUTZ

Angesichts großer Datenmengen, die jeder von uns tagtäglich hinterlässt, wird es immer wichtiger, die Kontrolle über die eigenen Daten zu wahren.

Was ist Datenschutz?

Adresse, Geburtsdatum, Kontodaten – sobald Sie sich im Internet bewegen, werden Informationen über Sie gespeichert. Doch was passiert, wenn diese Daten an andere weitergegeben werden? Wie können Sie sich schützen?

„Datenschutz“ meint nicht den Schutz der Daten selbst. Stattdessen möchte der Gesetzgeber die Menschen schützen, deren Daten erhoben, gespeichert und verwendet werden. Deshalb gibt es verschiedene Gesetze, die den Datenschutz regeln. Sie verhindern, dass Menschen die Kontrolle über ihre Daten verlieren. Laut Gesetz soll jeder selbst über seine Daten entscheiden. Das wird auch informationelle Selbstbestimmung genannt.

Internationale Unterschiede

International gibt es unterschiedliche Herangehensweisen im Zusammenhang mit Datenschutz.

Deutschland
In Deutschland galt bislang ein zentrales Datenschutzgesetz – das sogenannte „Bundesdatenschutzgesetz (BDSG)“. Ergänzt wurde es durch sektorspezifische Gesetze wie z.B. dem „Telekommunikationsgesetz (TKG)“. Seit dem 25. Mai 2018 gilt in Deutschland und in der Europäischen Union die „Datenschutz-Grundverordnung (DSGVO)“, welche die bisherigen Datenschutzgesetze im Wesentlichen ablöst. Die DSGVO gilt für alle Unternehmen die in der Europäischen Union (EU) ansässig sind und für Unternehmen, die mit Sitz außerhalb der EU Dienstleistungen in der EU anbieten.

Russland
In Russland dürfen die personenbezogenen Daten von russischen Bürgern nur auf russischen Servern gespeichert werden. So ist es auch möglich, dass Webseiten, die in Russland nicht ihren Sitz haben, keine Daten russischer Bürger speichern dürfen.

Japan
Datenschutz stößt in Japan auf großes Interesse. Die Weitergabe sensibler Daten wird eher vermieden. Behörden oder Unternehmen können persönliche Daten deshalb nur sehr eingeschränkt nutzen. Selbst in Ausnahmesituationen wie beispielsweise nach einem Zugunglück werden keine Informationen über Betroffene weitergegeben.

Brasilien
In Brasilien gilt das Gesetz „Marco Civil da Internet“ – eine Art Grundrecht für das Internet. Das Gesetz soll die Privatsphäre der Nutzer online schützen. Jedoch ist in diesem Gesetz auch die Speicherung der persönlichen Daten festgesetzt – das heißt, es gibt Hinweise auf eine dauerhafte Speicherung der Daten. Unternehmen wie E-Mail-Anbieter müssen die Daten ihrer Kunden über ein Jahr sichern und bei Bedarf an staatliche Stellen weitergeben. Kritiker sehen darin eine Verletzung der Grundrechte.

USA
In den USA gibt es wenige Gesetze, die die persönlichen Daten schützen. Allerdings haben die Menschen in den USA eine andere Haltung zum Thema Datenschutz. Firmen und Behörden dürfen die Daten dort auch ohne Zustimmung nutzen. Das ist z. B. bei Abschluss eines Arbeits- oder Mietvertrages von Bedeutung. Ein Online-Shop darf nach der Prüfung der persönlichen Daten – z. B. dem Einkommen – entscheiden, ob er einen Kaufvertrag abschließen möchte oder nicht.

Datenpannen

In der Vergangenheit gab es Vorfälle, bei denen Daten der Nutzer von verschiedenen Internetdiensten gestohlen und veröffentlicht wurden. Ziel des Datenschutzes ist es, solche Vorfälle zu verhindern und die Menschen zu schützen.

Yahoo
Namen, E-Mail-Adressen, Geburtsdaten, Passwörter – 2013 wurden diese und andere Daten von drei Milliarden Nutzerkonten der Firma „Yahoo!“ gestohlen. Die Datenpanne wurde erst drei Jahre später bekannt.

iCloud-Leaks
2014 gelang einem Hacker der Zugriff auf hunderte private Fotos von Prominenten. Er versendete einen manipulierten Link per E-Mail an die Betroffenen. Die Prominenten sollten sich wie gewohnt mit ihrer iCloud-Kennung einloggen. In Wahrheit handelte es sich um eine gefälschte Seite, die die iCloud-Kennungen der Nutzer speicherte und sie an den Hacker weiterleitete. Dieses Vorgehen nennt man auch „Phishing“. Die teils sehr intimen Bilder wurden anschließend im Internet verkauft bzw. veröffentlicht.

Ashley Madison
Das Online-Dating-Portal „Ashley Madison“ geriet 2015 in die Kritik. Damals wurden Daten von 32 Millionen Nutzern gestohlen – darunter Namen, Adressen, Suchanfragen, Kreditkartendaten und heikle Informationen über das Privatleben. Anschließend drohten die Hacker mit der Veröffentlichung der Daten.

Comdirect
Zwei Millionen Kunden der Direktbank „Comdirect“ konnten im Juli 2016 mehrere Stunden auf andere Kundenkonten zugreifen. Sie hatten dadurch Einsicht in fremde Kontostände. Abbuchen oder Überweisungen waren jedoch nicht möglich.

Paradise Papers
Dass viele Unternehmen und Einzelpersonen bei der Erledigung ihrer Steuern Schlupflöcher nutzen, haben die sogenannten „Paradise Papers“ gezeigt. Der Titel verweist auf sogenannte „Steuerparadiese“ – d. h. Staaten, die wegen ihrer niedrigen Steuern für Steuerzahler besonders attraktiv sind. Im November 2017 veröffentlichte die Süddeutsche Zeitung Informationen zu insgesamt 13,4 Millionen vertraulichen Dokumenten.

DATENSCHUTZ IN APPS UND SOZIALEN MEDIEN

Was dürfen Apps?

Ob Kontakte, berufliche Termine, Freunde oder Erinnerungsfotos – Das Smartphone kennt Sie und Ihre persönlichen Daten sehr genau. Doch würden Sie all diese Daten freiwillig an Fremde weitergeben? Nichts anderes tun Sie, wenn Sie in Ihren Smartphone-Einstellungen „App-Berechtigungen“ vergeben. Natürlich funktionieren viele Apps nur dann, wenn Sie gewisse Daten freigeben, z. B. müssen Sie einer Foto-App Zugriff auf Ihre Kamera geben. Auch ein Kartendienst macht erst dann richtig Sinn, wenn er Ihren Standort kennt. Manche Apps jedoch wollen auch Zugriff auf Daten, die sie gar nicht brauchen, wie Telefonnummern oder Kontakte. Hier müssen die Nutzer selbst aktiv werden und solche Zugriffe einschränken.
Erfahren Sie hier, welche App-Berechtigungen es gibt und wie Sie diese verändern können.

Big Data – Was ist das?

Täglich nutzen Milliarden Menschen das Internet. Dabei entstehen riesige Datenmengen. Diese nennt man auch „Big Data“.
Egal ob wir online recherchieren oder Kartendienste nutzen: jeder Internetnutzer hinterlässt viele digitale Spuren. Abgesehen von persönlichen Daten wie der Adresse oder der Telefonnummer, gehören auch andere Daten dazu: z. B. wie lange Sie auf einer bestimmten Webseite geblieben sind oder welche Produkte Sie sich häufig ansehen.

Vorsicht

Soziale Netzwerke oder Webseiten sammeln Daten – viele dieser Daten geben Sie selbst preis. Doch einige Plattformen gehen achtlos mit Nutzerdaten um. Erst im März 2018 wurde bekannt, dass mehrere Millionen Daten von Facebook-Nutzern wie das Alter oder der Wohnort weitergegeben wurden. Als Nutzer hat man die Möglichkeit, dies über Änderungen in den Einstellungen der Privatsphäre auf der Facebook-Webseite zu verhindern. So entscheiden Sie, welche Daten Sie preisgeben.

Telekom Privacy Manager

Wie viel geben Sie auf Facebook über sich preis? Und wer kann die Fotos und Posts in Ihrem Profil sehen? Der „Telekom Privacy Manager“ gibt Ihnen Antworten auf diese Fragen. Die App analysiert die Privatsphäre Ihres Facebook-Profils und gibt Ihnen Rückmeldung dazu. Zudem haben Sie die Möglichkeit, Änderungen direkt über die App vorzunehmen.

Datenschutzhinweise

Jeder Klick auf einer Webseite hinterlässt Spuren. Egal ob Sie nach neuer Kleidung oder dem nächsten Urlaubsziel suchen – die Webseite bemerkt Ihr Interesse und speichert Ihre Eingaben. Wie Unternehmen mit diesen Daten umgehen, können Sie in den Datenschutzhinweisen nachlesen.

Beispiele Datenschutzhinweise

Cookies
Beim Aufruf einer Webseite werden Sie häufig darauf hingewiesen, dass diese Cookies speichert. Cookies sind Daten, die Webseiten automatisch auf dem Endgerät eines Nutzers sichern. Wenn Sie z. B. auf einer Webseite Artikel in einen Warenkorb legen, ist der Inhalt des Warenkorbs auch beim nächsten Besuch der Seite noch vorhanden. Ähnliches kann man auch bei Spracheinstellungen beobachten. Die Einstellung der Sprache auf einer Webseite muss nur einmalig getroffen werden. Das ist einerseits hilfreich. Andererseits können dadurch Unternehmen Ihr Surfverhalten nachverfolgen und dadurch gezielt Werbung platzieren.

Browser-Daten
Webseiten speichern Daten. Sobald Sie mit Ihrem Browser, wie z. B. Mozilla Firefox, das Internet nutzen, werden automatisch Informationen an den Betreiber der Webseite weitergegeben. Dazu gehören z. B. der verwendete Browsertyp, die IP-Adresse, die Herkunft des Besuchers oder die Uhrzeit der Seitenanfrage. Die Webseiten speichern also immer, wann und wo ein Nutzer die Seite aufgerufen und wie er sich auf der Seite bewegt hat.

Social Plug-Ins
Sie haben einen interessanten Artikel gelesen und möchten Ihre Freunde darauf aufmerksam

machen. Anstatt den Link mühsam zu kopieren und jedem Ihrer Freunde einzeln zu schicken, können Sie hierfür Social Plugins verwenden. Social Plugins erleichtern das Teilen des betreffenden Artikels, ohne dabei die Webseite zu verlassen. Ein einfacher Klick auf die kleinen Symbole der Sozialen Netzwerke genügt. Aus der Perspektive des Datenschutzes sind Social Plugins nicht ganz unbedenklich: Über sie gelangen auch persönliche Daten wie das eigene Surfverhalten an die Sozialen Netzwerke.

Tracking-Tools
Viele Webseiten nutzen Tracking Tools. Dabei handelt es sich um Analyseprogramme. Die Tracking Tools sammeln dabei mit der Erlaubnis der Webseite Daten über die Benutzer und werten diese aus. Dadurch kann der Webseitenbetreiber erkennen, welche Informationen für den Nutzer interessant sind oder wie lange Besucher auf der Seite verweilen. Diese Informationen werden anschließend genutzt, um die Webseite den Interessen der Nutzer anzupassen.

Kontodaten
Kontodaten sind die Informationen, die Sie freiwillig auf einer Webseite angeben – z. B. wenn Sie sich als Nutzer mit Ihrer E-Mail-Adresse registrieren. Die Webseite speichert diese Daten und erstellt ein Benutzerkonto von Ihnen. Vor allem bei Online-Shops müssen neben dem Namen und der E-Mail-Adresse oft auch Bankdaten abgespeichert werden.

DER GLÄSERNE MENSCH

Der gläserne Mensch

Nicht immer ist auf den ersten Blick deutlich, welche Daten eine Person im Internet hinterlässt. Doch häufig geben wir auch sehr persönliche Daten preis.

Taschenlampe und Kontakte?

Anna-Lena nutzt in ihrer Freizeit verschiedene Apps auf Ihrem Smartphone. Gerade abends auf dem Heimweg nutzt sie eine Taschenlampen-App. Durch das Licht fühlt sie sich alleine sicherer. Eine Taschenlampen-App braucht auch keine Daten wie z. B. den Standort oder die Kontakte.

2013 wurde bekannt, dass der Betreiber einer Taschenlampen-App heimlich Daten der Nutzer sammelte. Den Nutzern war dabei nicht bewusst, welche Daten wann gesammelt wurden. Nach Bekanntwerden mussten die Betreiber der App alle gesammelten Daten der Nutzer löschen.

Deshalb sollten Sie immer schon bei der Installation von Apps genau nachlesen, welche Daten die App benötigt. Auch eine kurze Recherche in einer Online-Suchmaschine gibt häufig einige Hinweise: Haben sich bereits andere Nutzer über die App beschwert? Gibt es Hinweise, dass die App unseriös ist?

Werbung und Werbeanrufe

Beim Surfen stieß Anna-Lena auf ein sehr interessantes Gewinnspiel aus einer vertrauenswürdigen Quelle. Ein paar Daten wie die Adresse und die Telefonnummer reichen zur Teilnahme aus. Bereits ein paar Tage später klingelt das Telefon. Anna-Lena werden neue Smartphones und Handyverträge angeboten.

Daten, die bei Gewinnspielen erhoben werden, werden häufig für solche Zwecke genutzt. Vor allem Gewinnspiele verlangen oft nach Daten, die auf den ersten Blick gar nicht notwendig sind – z. B. die

Telefonnummer. In den Teilnahmebedingungen findet sich dann häufig folgende Formulierung:

„Mit der Teilnahme am Gewinnspiel stimme ich der kommerziellen Nutzung meiner Daten zu."

Mit Ihrer Zustimmung dürfen die Daten und Ihre Telefonnummer anschließend an Dritte weitergegeben werden.

Viren, Malware und Spam

In ihrer Freizeit beschäftigt sich Anna-Lena mit Social Media – vor allem mit neuen Trends wie z. B. Dating-Apps. Vor kurzem stößt sie auf eine neue interessante App. Nach dem Download taucht auf einmal eine Unmenge an Werbung auf ihrem Handy auf. Neben Kleidung und Handyverträgen ist auch ein Fenster mit der Warnung vor einem Virus erschienen. Dort wird nach einigen Angaben zu ihrem Gerät und ihrer Person gefragt. Nur dann könne der Virus entfernen werden.
Bei den Meldungen handelt es sich wahrscheinlich um sogenannte „Adware". Das Wort ist aus den englischen Begriffen „advertisement" (dt. Werbung) und „Software" zusammengesetzt. Häufig hat Adware einen harmlosen Grund – z. B. ein kostenloses Programm, das sich durch Werbung finanziert. Manchmal sind jedoch auch ein Virus oder ein Schadprogramm die Ursache für die Werbung. Haben Sie den Verdacht, dass Ihr Computer von einem Virus befallen sein könnte, sollten Sie reagieren. Ein Antivirenprogramm für mobile Endgeräte bietet Schutz vor Angriffen wie diesen.

Weitere Hilfe finden Sie unter anderem auch hier.

Digitale Überwachung

Im Internet geben wir – absichtlich und unabsichtlich – private Daten preis. Doch auch im Beruf oder der Freizeit werden Daten über uns gesammelt. Sicherheitskameras an vielen öffentlichen Orten (z. B. Bahnhöfen) sind weit verbreitet. Immer mehr Orte werden aus Gründen der Sicherheit videoüberwacht. Auch Drohnen kommen dabei zum Einsatz und überwachen z. B. Demonstrationen oder Tatorte aus der Luft.

Auch deshalb werden Sicherheitsmaßnahmen wie diese in der Öffentlichkeit diskutiert: Wann fühlen wir uns wirklich sicher? Wann verletzt man sie in ihrer Privatsphäre oder fühlen sie sich beobachtet?

DATENSCHUTZ-TIPPS

Datenschutz durch Datensparsamkeit

Sie haben bereits verschiedene Datenschutz-Probleme kennengelernt. Doch ganz ohne Daten kommt man im Internet nicht aus. Damit z. B. Ihre Bestellung geliefert werden kann, müssen Sie zwingend Ihre Adresse angeben. Die Frage ist deshalb nicht: Welche Daten möchte ich im Internet preisgeben? Sondern vielmehr: Welche Daten sind an welcher Stelle erforderlich?

Sichere Geräte

Datenschutz beginnt bei dem Gerät, das genutzt wird. Halten Sie die Software Ihres Smartphones, PCs oder Tablets stets auf dem neuesten Stand. Einen unberechtigten Zugriff können Sie durch PINs, Passwörter oder Fingerabdruck- bzw. Gesichtsscanner verhindern. Auch Antivirenprogramme auf mobilen Endgeräten bieten Schutz.

Klicken Sie hier für weitere Informationen zur Sicherung Ihrer Geräte.

Sichere Netzwerke

Unterwegs noch schnell die Mails checken? Öffentliche Netzwerke sind eine praktische Lösung, eine Internetverbindung aufzubauen. Einige Dinge sollten Sie dabei jedoch beachten.

Vorsicht bei offenen Netzwerken
Offene Netzwerke in Cafés oder an Bahnhöfen sind schnell und bequem, können aber unsicher sein. Über eine ungesicherte Verbindung können persönliche Daten ausgelesen werden. E-Mails oder Dienste, für die Sie sich anmelden müssen, können so nicht mehr sicher genutzt werden.

Keine automatischen Verbindungen
Unterbinden Sie die automatische Verbindung, wenn Sie unterwegs sind. Hacker können WLAN-Netze so verändern, dass sich mobile Geräte auch ohne Ihre Zustimmung mit ihnen verbinden. Die Hacker können dann z. B. Ihre Nachrichten auslesen. Die automatischen Verbindungen unterbinden Sie in den Netzwerkeinstellungen Ihrer Geräte.

Sichere Verbindungen
Nutzen Sie öffentlich nur Webseiten, die die Kommunikation mit SSL-Verbindungen verschlüsseln. Sie erkennen diese an der Bezeichnung „https“ vor dem eigentlichen Link. Solche Verbindungen verhindern, dass z. B. Anmeldedaten ausgespäht werden können.

Deaktivieren der Dateifreigabe
Bei Windows und Mac OS gibt es die Möglichkeit, Computer in einem Netzwerk miteinander zu verbinden. So können Dateien ausgetauscht werden. Das nennt man auch „Dateifreigabe“. In einem öffentlichen Netzwerk kann das aber dazu führen, dass sich Fremde Zugriff auf persönliche Daten verschaffen. Deaktivieren Sie die Dateifreigabe in Ihren Geräteeinstellungen, sobald sie öffentlich surfen.

Das Recht auf Vergessenwerden

Was ist, wenn doch einmal etwas ins Internet gerät, das Sie dort nicht haben wollen? Jeder Bürger hat das Recht, private Daten aus der Öffentlichkeit des Internets entfernen zu lassen. Durch das sogenannte „Recht auf Vergessenwerden“ können die Nutzer z. B. Verlinkungen bei Google-Suchanfragen verhindern oder Inhalte bei Facebook melden und löschen. Auf diese Weise lassen sich private Spuren im Internet entfernen.

Sie möchten Inhalte aus dem Internet entfernen? Bei Google oder Facebook geht das z. B. über ein bestimmtes Kontaktformular.

Alternative Suchmaschinen

Neben den bekannten Suchmaschinen wie Google oder Bing gibt es auch immer mehr alternative Suchmaschinen.

Einige Suchmaschinen wie DuckDuckGo oder StartPage wollen ihren Nutzern mehr Sicherheit bieten. Die Verbindung ist stets verschlüsselt und es sollen keine Daten über die Nutzer (z. B. die IP-Adresse) gespeichert werden.

Andere alternative Suchmaschinen wie Ecosia oder MetaGer betreiben ihre Server mit erneuerbarer Energie. Diese Suchmaschinen sind gemeinnützig orientiert. Der Gewinn wird z. B. an ein Regenwaldprojekt gespendet.

Datenschutz Aktuell

Datenschutz betrifft auch in Zukunft viele Bereiche des alltäglichen Lebens. Das „Internet der Dinge“ verbindet bis 2020 bis zu fünfzig Milliarden elektronische Geräte miteinander – sei es der Kühlschrank, das Navigationsgerät oder der automatische Staubsauger. Diese Geräte sollen, so fordern Datenschützer, schon in der Entwicklung und Produktion ein Augenmerk auf die Privatsphäre der Nutzer richten. Dazu gehört, dass die Nutzer genau wissen, welche Daten wann erhoben und wie diese verschlüsselt werden. Die Forderung der „Privacy by Design“ ist bereits in der Datenschutzgrundverordnung der EU (DSGVO) berücksichtigt.

Schützen Sie Ihre Daten!

Behalten Sie die Kontrolle und werden Sie aktiv! Sie haben viele Möglichkeiten in diesem Modul kennengelernt. Datenschutz ist Ihr gutes Recht – nutzen Sie es!

ERLEBEN, WAS VERBINDET.