Transkript: „Datenschutz“

Einleitung

Hallo, da sind wir wieder! Digitale Medien und Geräte sind heutzutage für viele Menschen selbstverständlich. Ständig wächst die Anzahl an neuen Apps oder Sozialen Netzwerken. Mit der steigenden Nutzung dieser Dienste nimmt auch die Menge an gesammelten, gespeicherten, verarbeiteten sowie weitergegebenen Daten zu. Wie behalten wir als Nutzer*innen eigentlich die Kontrolle über unsere Daten im Internet?

Eintauchen

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

Laut einer Studie des Bitkom fühlen sich die meisten Internetnutzer für den Schutz ihrer Daten selbst verantwortlich, sind jedoch nicht sehr zuversichtlich, ihre Geräte wie Smartphones oder Computer eigenständig vor Angriffen durch Internetkriminelle zu schützen.

Es besteht also ein Bedarf an mehr Aufklärung und Transparenz, um das Vertrauen in den Umgang mit persönlichen Daten zu stärken.

Verstehen

Wir alle hinterlassen täglich große Datenmengen. Daher wird es immer wichtiger, die Kontrolle über die eigenen Daten zu bewahren. Sobald man sich im Internet bewegt, werden viele unserer Daten gespeichert. Und das Internet weiß viel über uns. Und es vergisst nichts!

Doch was passiert eigentlich, wenn diese Daten an andere weitergegeben werden? Wie können wir uns schützen?

Darüber sprechen wir mit Thomas Tschersich, ist Chief Security Officer (CSO) der Deutschen Telekom AG sowie Chief Executive Officer (CEO) der Telekom Security .

Interview

Teachtoday: Hallo, Thomas.

Thomas Tschersich: Hallo. Grüß dich.

Teachtoday: Mensch, das ist ja ein ganz schön langer Jobtitel. Kannst du uns mal kurz sagen, Was ist denn genau deine Aufgabe eigentlich?

Thomas Tschersich: Ich kümmere mich um das Thema Sicherheit bei der Telekom, dass unsere Daten sicher sind, dass unsere Kunden sicher sind und unsere Mitarbeiter sicher sind.

Teachtoday: Alles klar. Das leitet mich auch gleich zur ersten Frage über. Was bedeutet denn Datensicherheit jetzt eigentlich genau?

Thomas Tschersich: Na ja, das ist steckt ja eigentlich im Wort schon drin. Die Sicherheit von Daten und Sicherheit hat ja mehrere Aspekte. Das hat so den Aspekt, dass die Daten nicht in falsche Hände geraten, hat aber auch den Aspekt, dass Daten zum Beispiel nicht verändert werden. Denn wenn du mal überlegst, du stellst im Internet beispielsweise deinen Lebenslauf irgendwo in einem Jobportal ein und fürchtest, jemand könnte den einfach verändern, dann wäre das ja mit Sicherheit auch nicht unbedingt positiv. Und diesen Aspekt darf man nicht vergessen, wenn man über das Thema Datensicherheit redet.

Teachtoday: Und du hast es eben schon so ein bisschen angedeutet. Warum ist denn der Schutz der eigenen Daten jetzt eigentlich so wichtig?

Thomas Tschersich: Ich vergleiche das gerne damit, wie wir unser Hab und Gut schützen. Zu Hause geht ja jeder hin und schließt bevor er in einen Urlaub fährt die Haustür ab, macht vielleicht die Rollladen runter und kümmert sich darum, dass keiner an seine eigenen Sachen so dran kommt. Jetzt sind die Sachen zu Hause materialistisch, das heißt, die kann ich anfassen und das merke ich, wenn die weg sind. Und das ist der große Unterschied bei Daten. Bei Daten merke ich es vielleicht nicht sofort, wenn sie weg sind, aber auch da können andere Leute ja eine Menge Schaden mit anrichten. Es fängt mit banalen Themen an, die offenkundig sind. Wenn jemand meine Kreditkartendaten hat, dann kann er beispielsweise auf meine Rechnung irgendwo Dinge bestellen und kaufen. Aber auch wenn er meine Ausweisdaten hat, kann er sich vielleicht für mich digital irgendwie ausgeben. Das sind ganz, ganz vielfältige Manipulations- und Missbrauchsszenarien denkbar. Und deswegen ist es genauso wichtig, sich in der digitalen Welt, das heißt mit Daten und der Sicherheit der Daten auseinanderzusetzen, wie wir das mit unserem klassischen Geldbeutel machen.

Teachtoday: Ich finde, du hast gerade schon eine schöne Metapher genannt. So das Haus abschließen, um sein Hab und Gut zu schützen. Das kann ich ja in der digitalen Welt auch sehr gut, indem ich ein Passwort mir anlege. Und das Passwort sollte natürlich am besten auch stark sein. Nimm uns da doch mal mit. Wie kann ich denn jetzt am besten starke Passwörter erstellen und wie kann ich diese dann vielleicht verwalten?

Thomas Tschersich: Der allererste Fehler ist schon - du hast gesagt, „wenn ich **ein** Passwort“ und das machen viele tatsächlich, die nehmen ein Passwort und verwenden das überall. Und das ist schon der größte Fehler, den man eigentlich begehen kann. Denn wenn das Passwort mal verloren geht, dann hat ein Angreifer Zugriff direkt auf alles. Deswegen sollte man hingehen und sollte, wenn man Passwörter gestaltet, auch darauf achtgeben, dass es eben nicht immer das Gleiche ist. Das stellt uns jetzt natürlich schon Herausforderung. Ich weiß wie es dir geht, aber ich habe gefühlt hunderte von verschiedenen Zugängen im Internet und überall jedes Mal ein neues Passwort. Ist natürlich super schwierig, sich das zu merken. Ich habe für mich eine einfache Regel. Ich habe mir ein super komplexes Passwort ausgedacht, das länger als zwölf Stellen ist, was Zahlen, Buchstaben, Groß- + Kleinschreibung und Sonderzeichen drin hat. Das habe ich mir einmal gemerkt und ich an einer ganz bestimmten Stelle in diesem Passwort bringe ich eine Varianz rein. Also beispielsweise, wenn ich bei einem großen Onlineversandhändler das Passwort benutze, habe ich an der dritten Stelle den Anfangsbuchstaben von diesem Versandhändler A. Bei einem sozialen Netzwerk habe ich dann an der dritten Stelle den Anfangsbuchstaben des sozialen Netzwerks. Also damit kriege ich dann eine Varianz rein, dass die Passwörter schon unterschiedlich und nicht immer gleich sind. Aber ich kann es mir trotzdem noch merken.

Teachtoday: Das heißt, du merkst dir tatsächlich all deine Passwörter nach diesem Schema im Kopf oder macht es jetzt auch Sinn, die sich vielleicht irgendwo zu notieren? Oder es gibt ja mittlerweile auch Apps, wo man Passwörter speichern kann. Ist das auch eine Möglichkeit oder ist es wirklich am sichersten, wenn es hier oben drin ist?

Thomas Tschersich: Sicherheit würde ich sagen, wenn es wirklich hier oben drin ist, weil das kann keiner so leicht kopieren. Noch nicht. Gott sei Dank. Wer weiß, ob wir da irgendwann mal hinkommen. Aber es gibt auch den sehr guten sogenannten Passwortmanager. Da kann ich natürlich die Passwörter hin. Die helfen mir sogar, dass ich dann nicht jedes Mal das eigentliche Passwort brauche, sondern ich muss mich einmal an Passwort Manager anmelden und der übernimmt dann wiederum das Anmelden an dem Dienst, wo ich gerade tätig sein müsste. Es gibt auch Varianten, die synchronisieren sich dann zwischen dem Mobiltelefon und dem PC zuhause beispielsweise. Aber ich persönlich bin immer noch der Überzeugung, das beste Passwort ist das, was ich im Kopf habe. Und wenn ich mir dann mit so einer einfachen Bildungsregel das leicht merken kann, dann habe ich schon was erreicht.

Teachtoday: Auf jeden Fall ein super Tipp.

Thomas Tschersich: Ja, und ein Stück weit des Problems sind natürlich auch Leute wie ich, die Sicherheitsspezialisten, die das für den Anwender komplex machen. Je komplexer wir das machen, desto mehr motivieren wir natürlich auch Leute, das aufzuschreiben. Und dann unter der Tastatur auf dem Postet haben berühmte postet und da kann man sich dann natürlich auch schon die Frage stellen was ist jetzt besser? Das kurze Passwort, was ich im Kopf hab oder das lange an den postet. Im Zweifelsfall ist es das lange im Kopf natürlich. Aber ja, den Tipp sollte man sich einfach mitnehmen.

Teachtoday: Ja, das ist auf jeden Fall ein sehr guter Tipp. Hast du denn noch andere Tipps oder andere Möglichkeiten, wie man seine Daten noch schützen könnte? Jetzt mal abgesehen von Passwörtern.

Thomas Tschersich: Wenn wir mal schauen, warum sind eigentlich Hacker erfolgreich, dann ist das ganz häufig die Ursache dafür, dass sie eine längst bekannte Schwachstelle im Computer benutzen. Das heißt, jeder Softwarehersteller, sei es für das Betriebssystem oder für irgendwelche Anwendungsprogramme, hat Fehler in den Programmen drin. Und die werden irgendwann mal bekannt. Und dann reagieren die Hersteller meistens damit, dass sie sogenannte Softwareupdates zur Verfügung stellen, mit dem ich eben diese Fehlerfehler dann beseitigen kann. Und das kennt ja jeder zu Hause. Dann kommt so eine Meldung hoch „Softwareupdate jetzt einspielen oder lieber später?“ Hand aufs Herz, die meisten klicken auf „später“. Nervt mich jetzt bitte. Ich möchte jetzt arbeiten. Und das ist genau die Zeit, wo in meinem Computer ein bekanntes Problem schlummert, was der Angreifer ausnutzen kann. Das heißt es ist super, super, super wichtig, diese bekannten Schwachstellen sehr zeitnah zu schließen. Das heißt, wenn das Update verfügbar ist, bitte immer sofort einspielen. Das bietet schon extrem guten Schutz. Ich würde so weit gehen, dass bestimmt 90 % aller erfolgreichen Angriffe heute auf so ein Thema oder auf ein Übertölpeln des Benutzers, zum Beispiel durch eine Phishing-E-Mail „Bitte gib dein Passwort ein“ zurückzuführen sind.

Das heißt also neben nicht immer dem gleichen Passwort und eine gewisse Komplexität ins Passwort reinbringen, Softwareupdates immer einspielen und vielleicht auch noch als vierten Tipp: Sei misstrauisch und nur weil in einer E-Mail steht, du musst dein Passwort irgendwo eingeben, muss man es noch lange nicht tun, sondern manchmal hilft es einfach mal die Frage zu stellen „Kann das denn jetzt wirklich sein? Macht das wirklich Sinn?“ Dann kommt man ganz oft schon dazu. „Nein, das macht jetzt gar keinen Sinn“ und dann sollte man es auch lieber lassen.

Teachtoday: Ja, das ist auf jeden Fall auch ein guter Tipp, mal ein bisschen zu reflektieren und noch mal einen Schritt zurück gucken. Jetzt ist die künstliche Intelligenz gerade in aller Munde. Und da würde mich mal interessieren - Künstliche Intelligenz und Datensicherheit, wie geht das zusammen und vor allem welche Herausforderungen bestehen bei der Anwendung von KI im Hinblick auf den Schutz sensibler Daten und welche Chancen gibt es vielleicht auch?

Thomas Tschersich: Ja, es sind super, super breites Feld und ich glaube, wir sind noch als Gesellschaft auch sehr zwiegespalten. Also das geht von wirklich, wie du sagst, der Perspektive „welche Chancen bietet uns künstliche Intelligenz“ bis hin zum Untergang der Menschheit als Risiko auf der anderen Seite. Ich glaube, man muss ein bisschen was momentan von diesem Hype einfach mal abziehen und zu sagen, das ist natürlich eine neue Technologie, die die Welt über Zeit auch ein Stück weit verändern wird, die sowohl auf der guten wie auf der bösen Seite sicherlich genutzt werden wird. Das heißt, Angreifer werden künstliche Intelligenz nutzen, um Lücken noch schneller und effizienter zu finden. Aber wir können die eben auch nutzen, um unsere Daten besser zu schützen, also auch um Lücken schneller zu finden, um sie dann eben zu schließen. Ja, also insofern weiß ich gar nicht, ob das Thema durch künstliche Intelligenz eine ganz neue Dimension in puncto Datensicherheit erreichen wird, sondern das wird sich am Ende irgendwie wieder ausgleichen. Der Angreifer benutzt es, die Verteidiger benutzen es und damit wird es wieder so pari sein.

Aber ich glaube, es gibt einen ganz anderen Aspekt noch von künstlicher Intelligenz, auf den wir aufpassen müssen. Wenn ich heute eine Suchmaschine im Internet frage nach irgendeinem Thema, dann kriege ich eine ganze Reihe von Antworten. Dann stehen da 20, 30 vielleicht, hunderte von möglichen Antworten. Wenn ich eine künstliche Intelligenz frage, dann kriege ich eine Antwort im Regelfall. Und das suggeriert natürlich dem Benutzer, es gibt nur die eine Antwort, die kann aber falsch sein. Und das ist, was für uns die Herausforderung in der Zukunft sein wird. Wie stellen wir eigentlich sicher, dass die Antworten, die künstliche Intelligenz generieren keinen Bias haben, keinen vordefinierten Mindset, mit dem die Antwort in die falsche Richtung geht? Das wird eine große Herausforderung sein. Aber ich glaube auch da steckt, so ist man, guter alter Journalismus Grundsatz wieder dahinter zu sagen: „traue nicht nur einer Quelle, sondern such bitte erst mal nach einer zweiten unabhängigen Quelle, die das Gleiche sagt, bevor du davon ausgehst, es könnte wirklich wahr sein“. Und diesen Grundsatz müssen wir, glaube ich, auch bei künstlicher Intelligenz noch viel, viel mehr im Hinterkopf behalten.

Teachtoday: Ja und hast du abschließend noch vielleicht einen ultimativen Tipp für uns, wenn es jetzt um den Schutz der eigenen Daten geht? Also was dürfen wir auf gar keinen Fall vernachlässigen?

Thomas Tschersich: Ja, einfach nicht naiv sein, würde ich sagen. Du hast es eingangs gesagt Das Internet vergisst nichts. Wir gehen manchmal sehr naiv mit unseren Daten um, aber manchmal auch ein bisschen schizophren. Wir haben Sorge, dass unsere Daten gestohlen werden. Aber auf der anderen Seite teilen wir in sozialen Netzwerken die Bilder von unserem Frühstück. Also da mal ein bisschen ausgewogener unterwegs zu sein, hilft schon viel. Und das, was ich vorhin schon gesagt habe auch mal Dinge hinterfragen, Nicht einfach alles nur hinnehmen, nur weil es in der E-Mail steht, ist es nicht wahr. Dieses Hinterfragen ist für mich eigentlich dieser ultimative Tipp. An den allermeisten Stellen kommt man sehr schnell darauf. Nein, das kann jetzt gerade nicht sein. Das lasse ich lieber mal oder ich frag mal noch mal irgendwo nach bei jemandem, der mir helfen kann. Damit wäre super viel gewonnen.

Teachtoday: Ich nehme also mit: kritisch sein bleibt die Nummer Eins an dieser Stelle. Danke Thomas, dir für dieses tolle Interview, für die wertvollen Einblicke und für die Ratschläge. Es ist auf jeden Fall klar geworden, dass Datensicherheit eine wichtige Rolle in unserer digitalen Welt spielt und dass wir alle die Verantwortung haben, dass, was du ja eben auch sagtest, wir die eigenen Daten eben schützen.

Thomas Tschersich: Danke Dir! Sehr, sehr gerne und bleibt sicher.

Entdecken

Ganz ohne Daten kommt man im Internet aber auch nicht aus. Damit z. B. die Bestellung geliefert werden kann, muss man zwingend die Adresse angeben. Die Frage ist manchmal nicht: Welche Daten möchte ich im Internet preisgeben? Sondern vielmehr: Welche Daten sind an welcher Stelle erforderlich?

Auch Soziale Netzwerke sammeln Daten – viele dieser Daten geben wir selbst preis. Doch das muss nicht sein. Für weitere Informationen schauen Sie doch hier am besten einmal in der Teachtoday Toolbox vorbei. Dort finden Sie verschiedene Materialien, Tipps und Zusatzübungen zur thematischen Vertiefung des Themas.

Handeln

Schauen wir uns nun einmal zusammen an, was ein starkes Passwort ausmacht und wie man ein solches leicht erstellen kann.

->Teachtoday Passwort-Check<-

Grundsätzlich gilt: Starke Passwörter sollten nicht nur Buchstaben und Zahlen enthalten, sondern auch Sonderzeichen sowie Groß- und Kleinschreibung.

Wie nun aber das Passwort merken? Am besten denkt man sich einen Satz aus, den man sich gut merken kann. Dann schreibt man nur die Anfangsbuchstaben auf. Am besten noch eine Zahl an den Anfang und ans Ende noch ein Sonderzeichen. Das könnte jetzt die Grundlage für Ihre Passwörter bei unterschiedlichen Diensten sein.

Ganz einfach, oder?

Starke Passwörter sind wichtig, um unsere sensiblen Daten vor Missbrauch zu schützen. Doch die Verwendung desselben Passworts für verschiedene Konten ist riskant. Für jeden Online-Account, den man hat, sollte man ein individuelles Passwort anlegen. Und auch die regelmäßige Aktualisierung unserer Passwörter ist ein entscheidender Schritt, um uns vor potenziellen Angriffen zu schützen.

Reflektieren

Halten wir noch einmal fest:

- Heutzutage sind digitale Medien für viele Menschen alltäglich geworden. Mit der zunehmenden Nutzung dieser Dienste wächst auch die Menge an gesammelten, gespeicherten, verarbeiteten und weitergegebenen Daten.
- Oftmals haben wir selbst die Kontrolle darüber, was mit unseren Daten geschieht und welche Spuren wir im Internet hinterlassen.
- In sozialen Netzwerken liegt es in unserer Hand, welche Informationen wir über uns preisgeben.
- Starke Passwörter sind wichtig, um unsere sensiblen Daten vor Missbrauch zu schützen.
- Machen Sie notwendige Updates direkt sobald sich ihr Gerät meldet. Versäumnisse solcher Updates führen zu Sicherheitslücken, die von Kriminellen leicht ausgenutzt werden können.

Und allgemein gilt: Datenschutz bleibt immer ein aktuelles Thema. In Zukunft wird es immer mehr Technologien geben, die den Schutz unserer Daten erfordern.

Abmoderation

Der Schutz persönlicher Daten ist von Bedeutung. Doch das Internet erfordert zwangsläufig das Hinterlassen von Daten. Es ist entscheidend zu erkennen, welche Daten wirklich notwendig sind und wann es besser ist, auf ihre Weitergabe zu verzichten.