Aktueller denn je: Europäischer Datenschutztag

Daten sind das moderne Gold jedes Individuums. Und ihr Wert wird angesichts der immer stärkeren Digitalisierung und Datenflut weiter steigen. Warum sich Geiz insbesondere mit persönlichen Daten auszahlt, weniger mehr ist und Bequemlichkeit aufs Sofa aber nicht in die Cyberabwehr gehört, erklären die Sicherheitsexperten von Sophos.

Wer als Passwort 123456789 nutzt (laut Hasso-Plattner-Institut das beliebteste in 2023), Fotos von Freunden ungefragt durch sein Adressbuch jagt, auf Facebook fröhlich verkündet, dass er bis 23. Juli im Urlaub ist und zudem auch noch die Neujahrsvorsätze verpasst hat, um diese digitalen Todsünden auszumerzen, bekommt mit dem Europäischen Datenschutztag noch einmal eine offizielle Chance, die eigene digitale Sicherheit und die der Allgemeinheit zu verbessern. Denn für den sicheren Umgang mit persönlichen Informationen im Netz ist der Aktionstag, der auf der Unterzeichnung der europäischen Datenschutzkonvention am 28. Januar 1981 beruht, schließlich da. Als kleine Starthilfe für alle Privacy-Muffel hier noch einmal die wichtigsten Datenschutz-Tipps auf einen Blick:

Tipp 1: Auf ein gutes Passwort kommt es an
Der Mensch neigt zur Bequemlichkeit. Das kann in vielen Bereichen auch so bleiben, nur bitte nicht beim Passwort. Der Name des Haustiers, der Geburtstag oder logische Zeichenfolgen sind zwar einfach zu merken, aber eben auch einfach zu erraten oder zu knacken. Leider sind derartige nutzlose Passwörter nach wie vor viel zu häufig in Gebrauch – sowohl privat, als auch im geschäftlichen Umfeld. Vergesslichkeit oder Fantasielosigkeit sind keine Ausreden. Wozu gibt es Passwortmanager? Sie schlagen gute Ideen vor, merken die sich sogar und schützen auch vor gefälschten Websites. Wenn beispielsweise eine Fake-Anmeldeseite einer Bank besucht wird, erkennt der Passwortmanager diese nicht, und gibt folglich auch gar kein Passwort ein. Wichtig: für jede Webseite ein anderes Kennwort wählen.
Etwas lästiger aber um Längen nützlicher, da es für den Cyberkriminellen eine nervige Hürde ist: die Nutzung einer Zwei-Faktor-Authentifizierung (F2A). 2FA erhöht die Sicherheit mit einem zusätzlichen Code, der per Textnachricht oder Authentifizierungs-App auf das Mobiltelefon gesendet wird.

Tipp 2: Geizig sein
Bei den meisten Betriebssystemen, Anwendungen und Online-Konten lässt sich festlegen, was und wie viel mit anderen geteilt werden soll. Diese Einstellung sollten grundsätzlich und wiederholt bei jeder neuen App-Installation überprüft werden. Ist es wirklich nötig, dass jede App weiß, wo ich mit meinem Handy gerade bin? Muss ich tatsächlich wochenlang auf der Lieblingswebsite angemeldet bleiben? Will ich einer App wirklich das Recht geben, den Namen auf dem Social-Media-Konto zu posten? Je weniger persönliche Informationen im Internet kursieren, desto weniger erfahren Cyberkriminelle über den Einzelnen und desto weniger haben sie die Chance, Rückschlüsse für ihre Betrugsmaschen zu ziehen.

Tipp 3: Nur über meine Erlaubnis!
Soziale Medien machen Spaß, und das sollen sie auch, aber nicht auf Kosten von anderen. Es ist verlockend, Fotos hochzuladen, auf denen andere Personen zu sehen sind. Meist haben diese auch nichts dagegen, obwohl sie das sollten, schließlich haben sie ein Recht am eigenen Bild. Wer Anstand hat, holt sich VOR dem Teilen von Informationen die Einwilligung der Abgebildeten. Denn einmal öffentlich gemachte, können Wohnort, Geburtstag oder Adresse in falsche Hände gelangen – Cyberkriminelle suchen nach gezielten Hinweisen, um ihre Opfer mit „Insider-Informationen“ zu täuschen.

Tipp 3a: Vorsicht auch bei der Arbeit
Dieser Tipp ist als Erweiterung des vorigen zu verstehen, allerdings mit einer viel höheren Tragweite und ernsteren Folgen. Das Teilen eines Fotos im Privaten, wie der beste Freund in der Kneipe vom Hocker gleitet, mag zu Unmut und einer Diskussion führen und man wünscht sich, dass man es nicht getan hätte. Aber: im Arbeitsumfeld kann das unbedarfte Weiterleiten von Fotos oder Informationen ganz andere Konsequenzen nach sich ziehen. Eine Geldstrafe in Millionenhöhe für das Unternehmen, eine Klage seitens des Betriebs an den Mitarbeiter und damit die Gefährdung des Arbeitsplatzes – alles schon passiert. Die versehentliche oder gedankenlose Weitergabe von Unternehmensdaten (Stichwort Kundenvertrauen und Aufbewahrungsauflagen) kann genau diese Folgen haben. Sorgsam mit Informationen umzugehen ist also nicht nur ein Schutz für das Unternehmen, sondern auch für den einzelnen Mitarbeiter.

Tipp 4: Daten sparen
Was sind die eigenen Daten Wert? Es erscheint (noch) fremd, dem eigenen Geburtsdatum, Namen, Hobby oder anderen persönlichen Daten einen Wert zuzuordnen. Tatsächlich sind es aber genau diese Daten, mit denen nicht wenige Konzerne ihre Millionen- und Milliardengewinne machen. Unternehmen verarbeiten und nutzen betriebswirtschaftlich die Unmengen an Daten, die jeder einzelne täglich im Internet hinterlässt. Jeder Einzelne sollte sich Gedanken machen, welche Grenze er seinen persönlichen Daten setzt.
Sicherlich ist es angemessen, dass ein Autovermieter einen Adressnachweis verlangt, bevor er die Schlüssel für ein 20.000-Euro-Fahrzeug aushändigt. Wenn aber eine Nachrichtenseite oder ein Hotspot in einem Café die eigene Postleitzahl oder das Geburtsdatum verlangt, sollten man sich fragen: Wozu brauchen die das, und warum sollte ich das überhaupt preisgeben? Kann dann aber sein, dass man ohne diese Eingabe die gewünschte Funktion nicht bekommt... Ergo ist es wichtig, die Grenzen der eigenen Privatsphäre zu definieren und diese auch ein- und auszuhalten.

Social Media von Sophos für die Presse
Wir haben speziell für Sie als Journalist*in unsere Social-Media-Kanäle angepasst und aufgebaut. Hier tauschen wir uns gerne mit Ihnen aus. Wir bieten Ihnen Statements, Beiträge und Meinungen zu aktuellen Themen und natürlich den direkten Kontakt zu den Sophos Security-Spezialisten.

Folgen Sie uns auf und

LinkedIn: https://www.linkedin.com/groups/9054356/
X/Twitter: @sophos_info

Pressekontakt:

Sophos
Jörg Schindler, PR-Manager Central & Eastern Europe
joerg.schindler@sophos.com, +49-721-25516-263

TC Communications
Arno Lücht, +49-8081-954619
Thilo Christ, +49-8081-954617
Ulrike Masztalerz, +49-30-55248198
Ariane Wendt +49-172-4536839
sophos@tc-communications.de