Am 28. Januar heißt es wieder: Den Datenschutz kritisch prüfen und geeignete Sicherheitsmaßnahmen ergreifen

Am 28. Januar jährt sich der Europäische Datenschutztag mit dem Ziel, sowohl die Unternehmen als auch die Bürger für den Schutz ihrer Daten zu sensibilisieren. Mit einem Motivationsappell gibt Sophos-Sicherheitsexperte Chester Wisniewski fünf Tipps, die wirklich jeder umsetzen kann.*

„Der Datenschutztag soll uns daran zu erinnern, wie wichtig Verschlüsselung für den Schutz unserer Daten vor unerwünschter Spionage und Datenschutzverletzungen ist. Seit der Veröffentlichung der NSA-Enthüllungen durch Edward Snowden sind nun fast 13 Jahre vergangen, und wir kämpfen immer noch um die Einhaltung der End-to-End-Verschlüsselung, zuletzt im Streit um die Chat-Kontrolle.

Backdoors sowie übermäßige Zugriffsrechte sind problematisch. Wir haben gesehen, wie zahlreiche amerikanische Technologieunternehmen von Cyberkriminellen wie LAPSUS$ und Scattered Spider getäuscht wurden, indem sie sich als Strafverfolgungsbehörden ausgaben, um vermeintlich „rechtmäßigen Zugriff" auf die persönlichen Daten von Menschen zu erhalten.

Verschlüsselung ermöglicht es uns, genau das zu teilen, was wir wann mit wem teilen wollen. Wenn der Nutzer die Kontrolle hat, kann er Daten sicher und mit seiner Zustimmung weitergeben. Der Datenschutztag ist ein guter Anlass, um die Anwendungen und Plattformen für die Speicherung von Daten, die Kommunikation und die sozialen Medien zu prüfen, und um sicherzustellen, ob sie auch in Zukunft eine sichere Wahl sind", so Chester Wisniewski, Director Global Field CISO.

Fünf Praxistipps für mehr Datensicherheit

1. Auswahl geeigneter Passwörter.
Die alten Passwörter haben ausgedient, es müssen neue her, am besten noch mit einer 2FA (Zweifaktorauthentifizierung). Da es sich meist um zahlreiche Zugänge mit jeweils eigenen Passwörtern handelt, ist ein Passwort-Manager eine gute Unterstützung zur Erstellung und Verwaltung aller Zugangsdaten. Diese schützen auch vor gefälschten Webseiten, da sie diese erkennen und im Zweifelsfall kein Passwort preisgeben. Zudem bereitet die 2FA kaum Umstände, ist aber eine größere Hürde für Betrüger.

2. Datenschutzeinstellungen überprüfen
Bei den meisten Betriebssystemen, Apps und Online-Konten kann der Nutzer selbst entscheiden, wie viel er preisgeben möchte. Darf jede App auf dem Smartphone den aktuellen Standort wissen? Will man der Bequemlichkeit halber immer im Lieblings-Online-Konto angemeldet bleiben? Hat die App die Erlaubnis, im Namen des Nutzers Beiträge in seinen sozialen Medien zu veröffentlichen? Da es hier keine übergreifende Einstellungsfunktion für alle Anwendungen gibt, bleibt nur: man muss jedes Konto prüfen und individuell entscheiden, was man erlaubt oder nicht.

3. Ohne Erlaubnis nichts teilen
Für jeden Nutzer sozialer Medien sollte diese (ungeschriebene) Regel gelten: Bevor ein Foto mit anderen Personen darauf veröffentlicht wird, erst nachfragen, ob das auch in Ordnung ist. Denn die Informationen darauf können nicht nur die Beziehungen zu Familienmitgliedern und Arbeitgebern beeinflussen, sondern auch Cyberkriminellen versehentlich Dinge wie Wohnort,

Geburtstag, Urlaube etc. verraten, die sie gegen einen verwenden können – jetzt oder lange Zeit später.

4. Besondere Vorsicht bei der Arbeit
Tipp 3 wirkt sich auf der Business-Ebene noch einmal strenger aus: Das Weitergeben von Unternehmensdaten, ob innerbetrieblich, von Kunden oder Lieferanten, kann nicht nur für Cyberkriminelle von hohem Interesse sein, sondern kann zusätzlich juristische Folgen für den Betrieb und den eigenen Arbeitsplatz haben.

5. Die eigenen Grenzen kennen
Was sind mir die eigenen Daten Wert? Mit dieser individuellen Haltung lässt sich jede Anfrage nach persönlichen Informationen klar entscheiden. Kostenersparnisse, Informationen, Bequemlichkeiten, aber auch vertragliche oder rechtliche Absicherungen benötigen mal mehr mal weniger Daten. Es ist an dem Nutzer selbst, hier nachzufragen und im Zweifel Nein zu sagen.

* Der 28. Januar erinnert an die Europäische Datenschutzkonvention von 1981, das erste rechtsverbindliche zwischenstaatliche Datenschutzabkommen und internationale Werkzeug zum Schutz personenbezogener Daten.

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, Senior PR-Manager EMEA Central
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