Was tun bei einer Datenschutzverletzung?

Diese Schritte werden Ihnen helfen, positive Veränderungen vorzunehmen, um sich selbst zu schützen.

1. Ändern Sie Ihre Passwörter

Beginnen Sie mit dem Dienst, bei dem die Datenschutzverletzung aufgetreten ist, und den Diensten, die Sie am häufigsten nutzen. Denken Sie an Online-Banking, E-Mail-Konten, Online-Shopping und soziale Netzwerke.

2. Aktivieren Sie die 2FA („Zwei-Faktor-Authentifizierung“)

Dieses Authentifizierungsverfahren erschwert anderen Personen den Zugriff auf Ihr Konto, denn es werden zwei Codes bzw. „Faktoren“ abgefragt, bevor ein Zugriff auf Ihr Konto möglich ist. Auch wenn eine Person im Besitz Ihres Passworts ist, hat sie nicht den zweiten „Faktor“ – in den meisten Fällen, ein Code, der an Ihr Smartphone gesendet wird. Auf der Website Authy[1] können Sie nach Plattformen suchen, die 2FA anbieten. Die Website führt Sie auch durch die entsprechenden Einstellungen.

3. Sperren Sie gegebenenfalls den Zugriff auf Ihre Bankkonten

Benachrichtigen Sie Ihre Bank und sperren Sie bei Bedarf Ihre Bonitätsdaten. Je nach Art der Datenschutzverletzung sollten Sie Kontakt zu Ihrer Bank und Ihrer Kreditauskunft aufnehmen (oder zu der Organisation, die in Ihrem Land über Bonitätsdaten verfügt).[2]

Dies verhindert, dass andere Personen in Ihrem Namen neue Kreditkarten beantragen. Dadurch wird das Problem nicht noch größer.

Lokale Verbraucherschutzzentralen können ebenfalls helfen. Ihre Bank wird Sie darüber informieren, ob Sie neue Kontonummern und Karten benötigen.

4. Erzählen Sie Ihrem „Kreis von Vertrauten“, was passiert ist

Damit ist die Gruppe Ihrer engen Freunde und Verwandten gemeint. Auf diese Weise sorgen Sie dafür, dass sie vor ungewöhnlichen Telefonanrufen oder E-Mails von potenziellen Betrügern auf der Hut sind.

Dann können Sie sich damit befassen, wie sich der Schaden der eigentlichen Datenschutzverletzung begrenzen lässt.

5. Sehen Sie nach, welche Daten Sie selbst online finden

Es empfiehlt sich, zu überprüfen, ob Ihre persönlichen Daten irgendwo da draußen sind. Welche Informationen finden Sie bei einer zufälligen Suche? Beginnen Sie mit Ihrer üblichen Suchmaschine und verwenden Sie Suchbegriffe, die nicht allzu viel preisgeben, d.h., suchen Sie Ihren Namen und die letzten vier Ziffern Ihrer Telefonnummer, aber nicht Ihre gesamte Telefonnummer. Mit Firefox Monitor können Sie herausfinden, ob Ihre Daten von einer Verletzung betroffen sind, und sich dort für die neuesten Meldungen zu Datenschutzverletzungen eintragen.

6. Fordern Sie Websites direkt zur Löschung Ihrer Daten auf

Angenommen, Sie haben demnächst ein Vorstellungsgespräch und sind nicht zufrieden mit dem, was Sie in den Suchergebnissen über sich sehen. Gemäß der Datenschutz-Grundverordnung (DSGVO) haben Sie das Recht, eine Website direkt zur Löschung Ihrer Daten aufzufordern. Viele Websites sind bestrebt, die neuen Datenschutzgesetze der DSGVO einzuhalten. Wenn Sie sie also auffordern, Daten von der Website zu nehmen, werden sie dies oft schnell tun, um Unannehmlichkeiten und Kosten zu vermeiden. Ganz allgemein gilt: Wenn das Produkt oder die Dienstleistung innerhalb der EU angeboten wird, dann muss die Datenverarbeitung den Vorschriften der DSGVO entsprechen, unabhängig davon, ob Sie oder das Unternehmen dort ansässig sind oder nicht.

Sie können auch Dienste nutzen, die Ihre Daten für Sie löschen lassen. Websites wie Reputation Defender, Privacy Duck und „Delete Me“ von Abine fordern andere Websites auf, Ihre Daten zu löschen. Sie berechnen Gebühren, stellen aber auch weitere Informationen darüber bereit, wie Sie sich selbst darum kümmern können.

Schritte, die Sie jederzeit unternehmen können

1. Sehen Sie nach, welche Daten von Ihnen online zugänglich sind

(Beginnen Sie mit wichtigen Konten wie E-Mail, Banking, Shopping und Chats)

Fragen Sie sich:

1. Wo habe ich überall Konten mit Daten über mich?
2. Welche Probleme könnten bei einer Datenschutzverletzung entstehen?
3. Warum sind die Daten dort? (Müssen sie dort sein?)
   Wie sicher sind die Daten dort? Rufen Sie die Datenschutzerklärung oder die Nutzungsbedingungen der Website auf und suchen Sie nach Begriffen wie „Verschlüsselung im Ruhezustand“ (encryption at rest) oder „Verschlüsselung bei der Übertragung“ (encryption in transit), was bedeutet, dass Ihre Daten sicher gespeichert werden.
4. Welche Zugriffsrichtlinien gibt es und wie lange werden die Daten gespeichert?
   Steht in den Nutzungsbedingungen, ob alle Mitarbeiter auf Ihre Daten zugreifen können? Welche Datenaufbewahrungsrichtlinien gelten? Wenn auf einer Website nicht angegeben ist, wie lange Ihre Daten gespeichert werden, dann lautet die Antwort wahrscheinlich: für immer.

2. Räumen Sie Ihre Daten regelmäßig auf und reduzieren Sie die Datenmenge

Wenn Dienste Ihre Daten nicht haben, dann sind ein Datenverlust oder eine Datenschutzverletzung ausgeschlossen. Wenn sie nur über Daten der letzten drei Monate verfügen, können auch nur diese Daten von einer Verletzung betroffen sein. Es empfiehlt sich daher Ihre Online-Daten regelmäßig aufzuräumen. Fragen Sie sich: „Warum sollte ich diese Daten behalten?“ Löschen Sie, was Sie nicht benötigen, und laden Sie alles Übrige herunter, damit Sie die Daten von der Website oder aus der App entfernen können.

3. Überprüfen Sie Ihren Schutz

Kann ich meinen Schutz durch sicherere Passwörter und 2FA verbessern?

4. Fordern Sie Unternehmen auf, besser auf Ihre Daten achtzugeben

So mancher ist der Meinung, dass es Datenschutzverletzungen immer geben wird, so wie es immer Verbrechen geben wird. Unternehmen können aber auch mehr für den Schutz Ihrer Daten tun. Durch eine Kontaktaufnahme mit den Unternehmen können Sie diesen bewusst machen, dass sie zuhören und handeln müssen. So könnten Sie den Unternehmen beispielsweise auf Twitter schreiben: „Wir wollen wissen, wie lange Sie unsere Daten speichern. Sicherlich nicht für immer, oder? “

[1] Oder https://twofactorauth.org

[2] Für Luxemburg: Rufen Sie SIX Payment Services (24 Stunden am Tag, 7 Tage die Woche) so schnell wie möglich unter der Telefonnummer (+352) 49 10 10 an und benachrichtigen Sie Ihre Bank.

Übersetzung:

BEE SECURE HELPLINE Tel: 8002 1234

LE GOUVERNEMENT DU GRAND-DUCHÉ DE LUXEMBOURG

Co-financed by the European Union Connecting Europe Facility

Konzept und Inhalt:

TACTICAL TECH

DATA DETOX #datadetox datadetoxkit.org