Bundesamt
für Sicherheit in der
Informationstechnik

Aktueller Cyber-Vorfall - Empfehlungen für Betroffene von Datenleaks

Datum 08.01.2019

Am 4. Januar 2019 ist die Veröffentlichung hunderter überwiegend privater und persönlicher Datensätze von Prominenten, Journalisten und Politikern öffentlich bekannt geworden.

Nach aktuellen Stand der Ermittlungen, ist davon auszugehen, dass Zugangsdaten zu u.a. privaten Postfächern, Cloud-Diensten und Sozialen Netzwerken gestohlen oder erraten wurden. So konnten beispielsweise Kontakte und Fotos abgegriffen und veröffentlicht werden.

Was kann ich als Betroffener eines Datenleaks tun?

Wenn Sie begründeten Verdacht haben, dass sich unbefugte Dritte Zugriff auf eines oder mehrere Online-Konten verschafft haben, um zum Beispiel Ihre persönlichen oder sensible Daten zu entwenden, empfiehlt das BSI, folgende Schritte durchzuführen:

Verschaffen Sie sich einen Überblick: Überpüfen Sie in einem ersten Schritt, welche Ihrer Online-Konten betroffen sind oder betroffen sein könnten?

Reihenfolge festlegen: Priorisieren Sie daraufhin Ihre Online-Accounts nach dem Kriterium, ob Sie diese für die Wiederherstellung von Passwörtern anderer Online-Konten benötigen oder nicht. Denn die Reihenfolge, mit der Zugangsdaten verschiedener Accounts geändert werden, ist entscheidend.

Ändern Sie daraufhin der Reihe nach die Passwörter:

Starten Sie mit den Accounts, die Sie für das Zurücksetzen von Passwörtern verwenden. Meistens sind dies Ihre E-Mail-Postfächer.

Ändern Sie im Anschluss die Passwörter von Online-Profilen, die Sie für "Single-Sign-On" verwenden. Ein Beispiel hierfür ist Facebook, dessen Account verwendet wird, um sich bei anderen Diensten anzumelden.

Anschließend setzen Sie in loser Folge die restlichen Accounts zurück.

Führen Sie diesen Schritt nicht nur für Accounts durch, die vom Datenleak betroffen sind, sondern alle, die Sie mit denselben Passwörtern benutzten, oder deren Passwort-Zurücksetzen-Funktion auf ein kompromittiertes Postfach verweist.

Verwenden Sie für jeden Account ein unterschiedliches und starkes Passwort. Beachten Sie hierfür unsere Tipps zu sicheren Passwörtern.

Es ist empfehlenswert, die Änderung der Passwörter in einem Zug durchzuführen. Mimimieren Sie so die Zeit, in der unbefugte Dritte Ihnen zuvor kommen und den Zugriff auf Ihre Konten behalten.

Kontrollieren Sie abschließend, ob in Ihren Online-Konten Einstellungen verändert worden sind. Kritisch wären zum Beispiel automatische Weiterleitungen von Nachrichten an aus Ihrer Sicht fremde E-Mail-Adressen oder ergänzte Rückfalloptionen wie Telefonnumern zum Zurücksetzen von Passwörtern. Korrigieren Sie diese Einstellungen.

Beobachten Sie im Anschluss Ihre Online-Konten. Wenn Ihnen keine seltsamen Informationen mehr auffallen, ist davon auszugehen, dass der Fremdzugriff aufgehört hat.

Informieren Sie zudem Ihre Kontakte über Ihre Vermutung oder Ihre verifizierte Betroffenenheit – am besten telefonisch. Idealerweise führt dann auch Ihr Freundes- und Bekanntenkreis die oben benannten Schritte durch.

Wichtig: Alle oben benannten Tipps beziehen sich auf Datenleaks durch Fremdzugriffe, die nicht mit Schadprogrammen durchgeführt wurden. Lesen Sie hierfür unsere Tipps zur Beseitigung einer Infektion durch Schadcode.

Wie kann ich den Täter anzeigen?

Strafanzeigen geben Sie bei der Polizei auf. Nehmen Sie idealerweise direkt Screenshots sowie umfängliche Informationen mit, um den Fall möglichst genau zu schildern. Ansprechparter der Polizeien finden Sie hier.

Weitere Informationen:

- Aktueller Cyber-Vorfall - Empfehlungen zum Schutz vor Datendiebstählen

Seite teilen
