- Sollte dieser Newsletter bei Ihnen nicht einwandfrei angezeigt werden, beachten Sie bitte die beigefügte Version als PDF.

Data Leak – 70 000 Zugangsdaten gestohlen und veröffentlicht

Art der Bedrohung

Für die Nutzung von online-Diensten ist oftmals die Eingabe von Zugangsdaten (Mailadresse, Benutzername) erforderlich. Die zur Gegenprobe hinterlegten Daten befinden sich dabei in einer Datenbank auf dem Server. Gerade diese Datenbanken sind oftmals aufgrund schlecht gewarteter Systeme und unter Ausnützung von bekannten Sicherheitslücken das Angriffsziel von Tätern im Internet.

Modus Operandi und Folgen einer Veröffentlichung

Aufgrund eines aktuellen Anlassfalles erlauben wir darauf hinzuweisen, dass für die Verwendung von Anmeldedaten im Internet entsprechende Vorsichtsmaßnahmen und Verhaltensregeln als verständlich gelten sollen.

Man muss davon ausgehen, dass einmal bei einem Internet-Dienst gespeicherte Daten weiterhin dort verfügbar sind, auch wenn die Webseite gerade nicht online ist oder man einen solchen Account schon länger (auch über Jahre) nicht verwendet hat. Der (unberechtigte) Zugriff auf die Daten durch Dritte unter Ausnutzung einer Sicherheitslücke (z.B. SQL-Injection) kann den Diebstahl / Verlust und die ungewollte Weiterverwendung / Veröffentlichung dieser Daten zur Folge haben. Werden solche persönlichen Daten durch die Täter erst einmal veröffentlicht, ist das Vertrauen in den Dienstanbieter / Webseitenbetreiber oftmals nicht mehr vorhanden.

Man sollte sich auch der Tragweite bei der Preisgabe von persönlichen Daten bewusst sein, dass im Falle einer Veröffentlichung oder widerrechtlichen Nutzung nicht nur die Zugangsdaten selbst, sondern auch Adressen und Telefonnummern, unter Umständen auch hinterlegte Zahlungsmittel (Kreditkartendaten) veröffentlicht werden könnten. Diese (vollständigen) Datensätze eignen sich idealerweise für die Vorbereitung und Durchführung anderen strafbaren Handlungen im Internet.

Geben Sie daher bei der Anmeldung bei Dienstleistern im Internet nur jene Daten an, welche unbedingt erforderlich sind. Erkundigen Sie sich vorab über den Dienstleister selbst und allenfalls verfügbare Informationen über seine Handhabung in Bezug auf Datensicherheit.

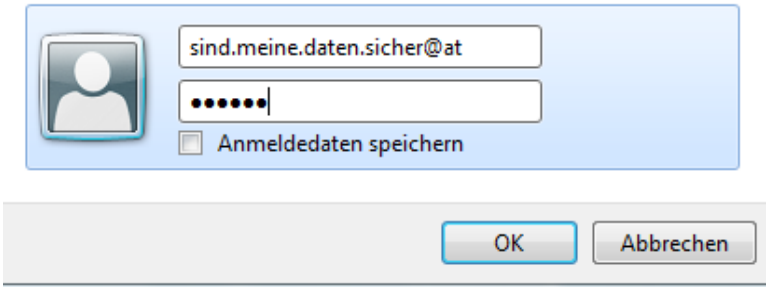
Empfohlene Vorgangsweisen für Unternehmer und Datenhalter:

- Halten Sie die Zugriffsmöglichkeiten bei Ihrer Applikation / Webseite so gering wie möglich
- Halten Sie Ihr Betriebssystem / Server aktuell und führen Sie regelmäßig die notwendigen Sicherheits-Updates für die verwendete Software durch
- Nahezu regelmäßig erscheinende Informationen über erkannte Sicherheitslücken bei SQL / MySQL und Derivaten sollten Sie ernst nehmen! Ist das Schließen derselben nicht sofort möglich, legen Sei besonderes Augenmerk auf die Daten und Zugriffe.
- Wurden Sie Opfer eines Datendiebstahls z.B. durch „SQL-Injection“, informieren Sie unverzüglich die betroffenen Benutzer und fordern Sie diese zum sofortigen Passwort-Wechsel auf.
- Erstatten Sie Anzeige auf einer der Polizeiinspektionen. Geben Sie der Anzeige die für Ermittlungen notwendigen Daten, nach Möglichkeit in elektronischer Form, bei (Log-Files und sonstige vom Täter hinterlassen Spuren (Script´s, Texte)).

Empfohlene Vorgangsweisen für Benutzer und Datengeber:

- Ändern Sie regelmäßig Ihre Zugangsdaten, verwenden Sie unterschiedliche und komplexe Passwörter für verschiedene Accounts und Anwendungen.
- Für Portale mit hinterlegten Zahlungsmöglichkeiten (Web-Shops, Dienstleister) oder Finanzdienstleister (Banken, online-Bezahldienste wie PayPal usw.) verwenden Sie ausschließlich einzigartige Passwörter mit hoher Komplexität.
- Komplexe Passwörter bestehen aus mindestens 8 Zeichen, beinhalten sowohl Groß- und Kleinbuchstaben in Kombination mit Zahlen und Sonderzeichen. Derartige Passwörter können Sie unter anderem mit einem Passwortmanager erstellen und verwalten, oder Sie legen sich eine eigene Passwortstrategie zurecht.
- Eigene komplexe Passwörter erstellt man z.B. durch die Verwendung einer Lieblingsphrase oder Zeile eines Gedichts und fügt an gleichen vordefinierten Stellen noch Sonderzeichen ein. Wird das Passwort mehrmals hintereinander verwendet, wird es nahezu automatisch aus dem Gedächtnis abgerufen. Und für den Passwortwechsel nimmt man den nächsten Absatz des Gedichts, oder eine andere Phrase / Liedertext. (Warum ich so bin, wie ich bin? = Wisb,wib? = *Wisb,wib?* = ?).
- Wenn Sie einen Account nicht mehr benötigen, lösen Sie diesen auf und fordern Sie den Betreiber zur Löschung Ihrer persönlichen Daten auf.
- Überprüfen Sie in unregelmäßigen Abständen, ob Ihre Mail-Adresse(n) unter Umständen kompromittiert ist. Dies können Sie unter anderem auf der Webseite www.botfrei.de, einem kostenlosen Service des eco – Verband der Internetwirtschaft Deutschland, unter der Rubrik Werkzeuge mit den Tools „';--have i been pwned?“ und „HPI Identity Leak Checker“ durchführen.

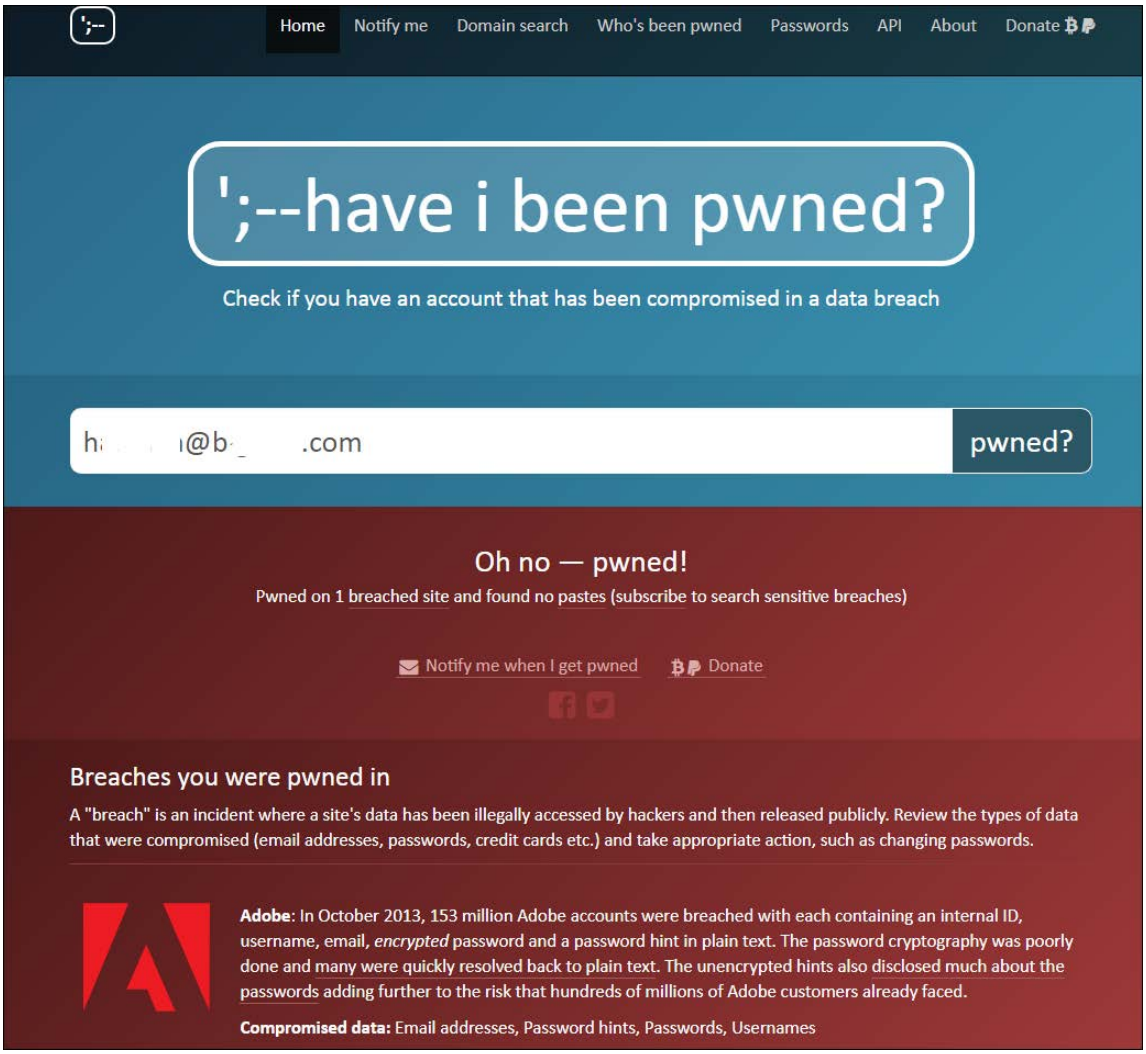
Beachten Sie des Weiteren die allgemeinen Sicherheitshinweise und Tipps für einen Sicheren Umgang mit dem Internet und Schutz vor IT-Kriminalität der Kriminalprävention auf den Webseiten des Bundeskriminalamts.



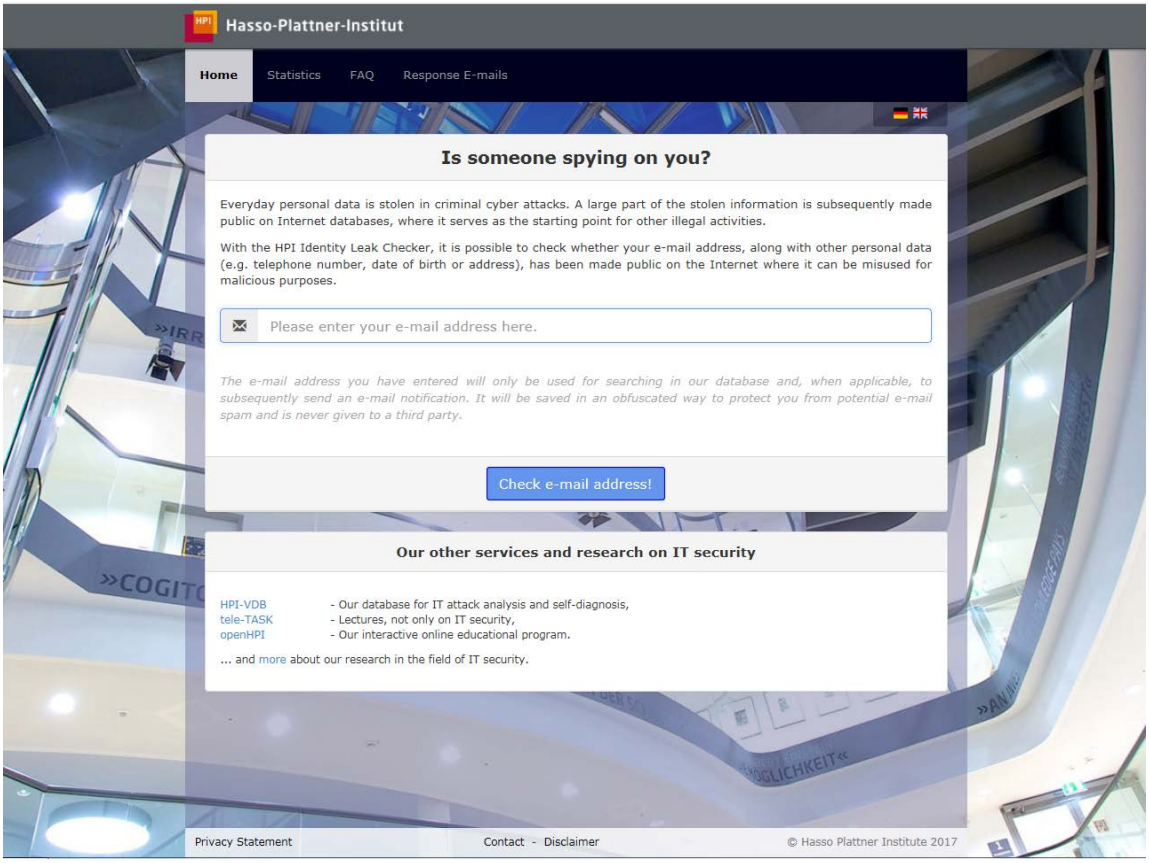
Sind Ihre Daten sicher? Verwenden Sie ein komplexes Passwort? Wann haben Sie dieses zuletzt gewechselt? ***Bitte, beachten Sie die allgemeinen Sicherheitshinweise!***

Möglichkeiten um festzustellen, ob meine E-Mail-Adresse kompromittiert ist:

https://haveibeenpwned.com/



https://sec.hpi.uni-potsdam.de/ilc/search?lang=de/



HERAUSGEBER: Bundesministerium für Inneres
Bundeskriminalamt
A-1090 Wien, Josef Holaubek Platz 1
Tel.: +43 1 24836 986500

FEEDBACK

NEWSLETTER AN-/ABMELDUNG