



openHPI-Kurs „Digitale Identitäten“ Identitätsdiebstähle – Angriffe auf Digitale Identitäten

Prof. Dr. Christoph Meinel
Hasso-Plattner-Institut, Universität Potsdam

Identitätsdiebstahl (1/2)

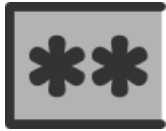
- Gelangt ein Dritter in den Besitz der digitalen Identität eines Nutzers, kann er in dessen Namen alle Dienste und Ressourcen nutzen, für die der Nutzer eine Berechtigung hat, z.B.
 - Online Shopping
 - Banküberweisungen tätigen
 - Videos anschauen
 -
- Anders als bei physischen Identitäten ist es relativ leicht, die geraubte digitale Identität zu **missbrauchen**

Identitätsdiebstahl (2/2)

Aufgrund des hohen Missbrauchspotentials sind Identitätsdiebstähle sehr attraktiv für Cyberkriminelle:

- mit gestohlenen digitalen Identität hat der cyberkriminelle Dieb alle Rechte – **Autorisation** –des rechtmäßigen Besitzers
- da Internetdienste allein auf Basis der digitalen Identität autorisieren, kann Dieb auf Kosten des rechtmäßigen Besitzers die Dienste nutzen

Angriffsziel: Identitätsdaten



Passwort



Anschrift



Email Adresse



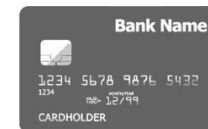
Telefonnummer



Pass-/Ausweisdaten



Kontodaten



Kreditkartendaten

Herkunft gestohlener Identitätsdaten (1/3)

- Diebstahl der **Account-/Kundendatenbank** von Internetdiensten
 - Cyberkriminelle verschaffen sich Zugriff auf das System eines Onlinediensteanbieters und kopieren sich die Datenbank von dessen Autorisationssystem mit allen Identitätsdaten
 - Häufig ausgeführt durch sogenannte „SQL Injection“
- Datendiebstahl mittels **Malware**, z.B.
 - „Spyware“ sammelt Daten direkt vom Computer des Nutzers – von besonderem Interesse sind Identitätsdaten
 - „Keylogger“ lesen Daten – insbesondere Passworte – direkt bei Eingabe mit und übermitteln sie an Cyberkriminelle
 - ...
- ...

Herkunft gestohlener Identitätsdaten (2/3)

■ **Phishing**

- Nutzer werden in gutem Glauben auf eine bösartige Webseite gelockt, die sich fälschlich als legitime Seite ausgibt
- Dort wird Nutzer zur Eingabe von persönlichen Identitätsdaten aufgefordert

■ Offenbarung in **Sozialen Netzwerken** und **Foren**

- Nutzer stellen leichtgläubig sämtliche Daten über sich, einschließlich der Identitätsdaten, in Netzwerke wie Facebook, Twitter, ...
- Jeder dort Angemeldete kann dann die Daten einsehen und stehlen

■ ...

Herkunft gestohlener Identitätsdaten (3/3)

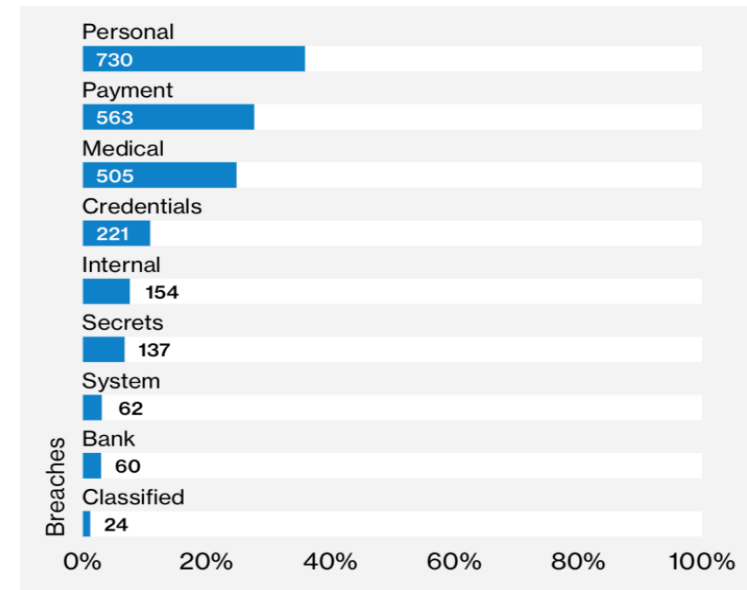
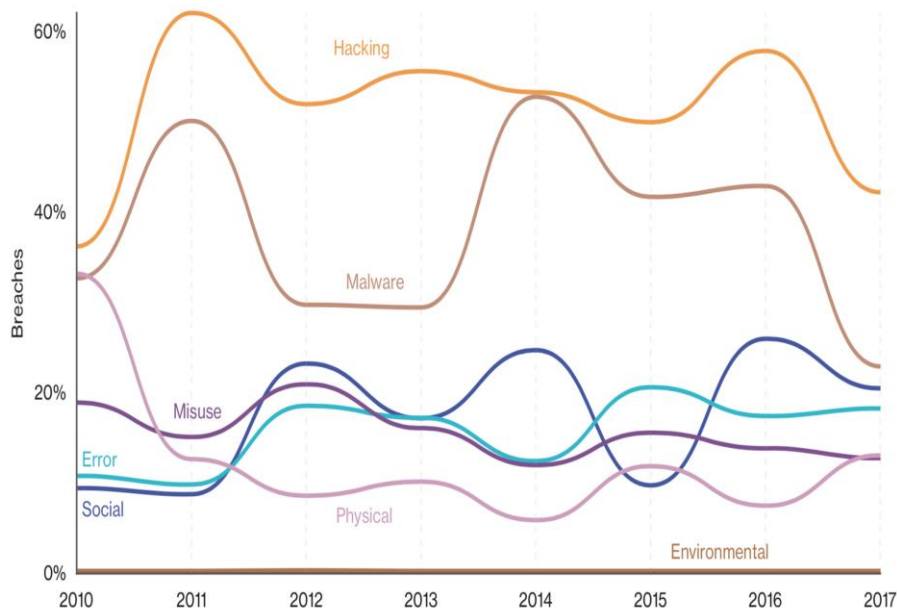
- Diebstahl oder Verlust von **Datenträgern**
 - gespeicherte persönliche Daten werden nicht richtig gegen physikalischen Zugriff abgesichert
 - bei Diebstahl oder Verlust von Speichermedien gelangen auch sämtliche Identitätsdaten in die Hände des Diebes
- **Social Engineering**
 - Manipulation von Personen, damit diese sensible Daten offenlegen
- ...

Sicherheitsvorfälle – kleine Statistik

Verzion veröffentlicht jedes Jahr eine Analyse von Sicherheitsvorfällen

■ Vorfälle 2017

- 53,000 Sicherheitsvorfälle
- 2,216 bestätigte Datendiebstähle



Quelle: 2018 Data Breach Investigations Report (Verizon)

HPI Identity Leak Checker (1/3)

- Internetdienst des Hasso-Plattner-Instituts, der nach frei zugänglichen und unrechtmäßig im Internet veröffentlichten Identitätsdaten(banken) („Leaks“) Ausschau hält
- Dienst wurde im Rahmen eines Forschungsprojekts zur Erkennung von Cyberangriffen von HPI-Forschern an meinem Lehrstuhl für „Internet-Technologien und System“ entwickelt mit dem Ziel, Nutzer zu warnen, wenn ihre Identitätsdaten frei im Internet zugänglich sind und von jedem missbraucht werden können
- Start: Mai 2014, erreichbar unter <https://sec.hpi.de>

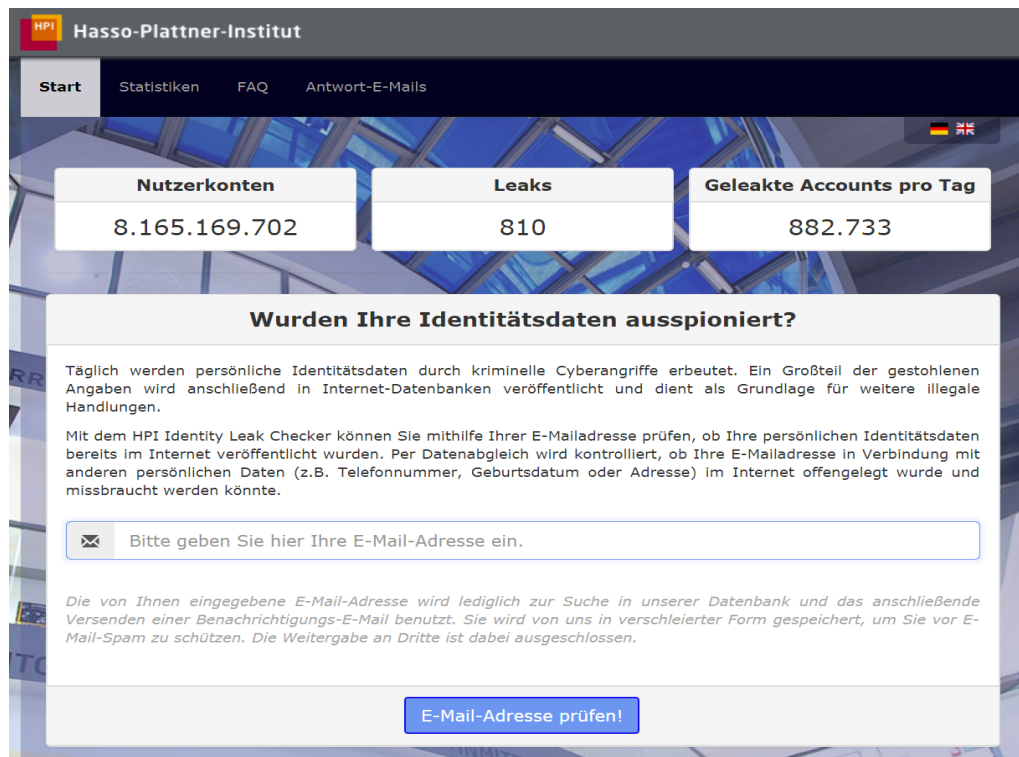
Identity Leak
Checker

by Hasso-Plattner-Institut



HPI Identity Leak Checker (2/3)

Nach Eingabe Ihrer Emailadresse bei <https://sec.hpi.de> erhalten Sie kurz danach eine Email mit der Information, ob Ihre Identitätsdaten in einer unrechtmäßig veröffentlichten und vom HPI erfassten Identitätsdatenbank gefunden wurden



The screenshot shows the HPI Identity Leak Checker interface. At the top, there is a navigation bar with links: Start, Statistiken, FAQ, and Antwort-E-Mails. Below this, three white boxes display statistics: 'Nutzerkonten' (8.165.169.702), 'Leaks' (810), and 'Geleakte Accounts pro Tag' (882.733). The main section is titled 'Wurden Ihre Identitätsdaten ausspioniert?' and contains a paragraph explaining the service. Below the text is a form with a text input field and a button labeled 'E-Mail-Adresse prüfen!'. A small disclaimer at the bottom of the form states that the email address is only used for searching the database and is stored in an encrypted form to protect against spam.

Nutzerkonten	Leaks	Geleakte Accounts pro Tag
8.165.169.702	810	882.733

Wurden Ihre Identitätsdaten ausspioniert?

Täglich werden persönliche Identitätsdaten durch kriminelle Cyberangriffe erbeutet. Ein Großteil der gestohlenen Angaben wird anschließend in Internet-Datenbanken veröffentlicht und dient als Grundlage für weitere illegale Handlungen.

Mit dem HPI Identity Leak Checker können Sie mithilfe Ihrer E-Mailadresse prüfen, ob Ihre persönlichen Identitätsdaten bereits im Internet veröffentlicht wurden. Per Datenabgleich wird kontrolliert, ob Ihre E-Mailadresse in Verbindung mit anderen persönlichen Daten (z.B. Telefonnummer, Geburtsdatum oder Adresse) im Internet offengelegt wurde und missbraucht werden könnte.

Bitte geben Sie hier Ihre E-Mail-Adresse ein.

Die von Ihnen eingegebene E-Mail-Adresse wird lediglich zur Suche in unserer Datenbank und das anschließende Versenden einer Benachrichtigungs-E-Mail benutzt. Sie wird von uns in verschlüsselter Form gespeichert, um Sie vor E-Mail-Spam zu schützen. Die Weitergabe an Dritte ist dabei ausgeschlossen.

E-Mail-Adresse prüfen!

HPI Identity Leak Checker (3/3)

Erfahrungen aus dem Projekt

- Seit Mai 2014 haben wir mehr als **7.000** Identitätsdatenbanken frei zugänglich im Internet gefunden
- Davon besitzen die größten Datenbanken mehr als **2 Milliarden** Identitätsdatensätze
- Aktuell erfassen wir rund **8,2 Milliarden** Datensätze – gestohlene Identitäten – aus mehr als 800 im Internet frei verfügbaren geleakten Identitätsdatenbanken
- Die am häufigsten geleakten Datentypen sind:
 - Emailadresse, Passwörter, Anschrift, Telefon, ...

Motivation von Identitätsdiebstahl (1/2)

■ Ansehen

- Cyberkriminelle wollen zeigen, was sie können
- erbeutete Daten werden öffentlich ins Netz gestellt als Beweis, dass ein Dienst geknackt wurde

■ Profit

- Daten können gewinnbringend auf Schwarzmarkt verkauft werden
- Nutzung (von Dritten) für kriminelle Zwecke
 - Versand von Spam
 - Abbuchung von Finanzdiensten
 - Nutzung einer falschen Identität

Motivation von Identitätsdiebstahl (2/2)

■ **Hacktivismus**

- Kampf für meist verquastenes politisches / ideologisches Ziel
- Schädigung des Ansehens des Opfers
 - z.B. Anonymous

■ **Rache**

- jemandem wurde Unrecht angetan
- möchte sich durch Diebstahl und Veröffentlichung von persönlichen Details dieser Person rächen

■ ...

Zusammenfassung: Identitätsdiebstähle

- Identitätsdiebstahl bedeutet, dass ein Angreifer die digitale Identität eines Nutzers übernimmt, sodass er in dessen Namen alle Dienste und Ressourcen nutzen kann, für die der Nutzer eine Berechtigung hat
- Je mehr Informationen ein Angreifer über das Opfer hat, umso leichter kann er dessen digitale Identität missbrauchen
- Angreifer haben verschiedene Möglichkeiten, an Identitätsdaten zu gelangen
 - Diebstahl von Passwortdatenbanken
 - Malware
 - Phishing, Social Engineering, Soziale Netzwerke
 - Diebstahl von Datenträgern