Hasso Plattner Institut
Digital Engineering · Universität Potsdam

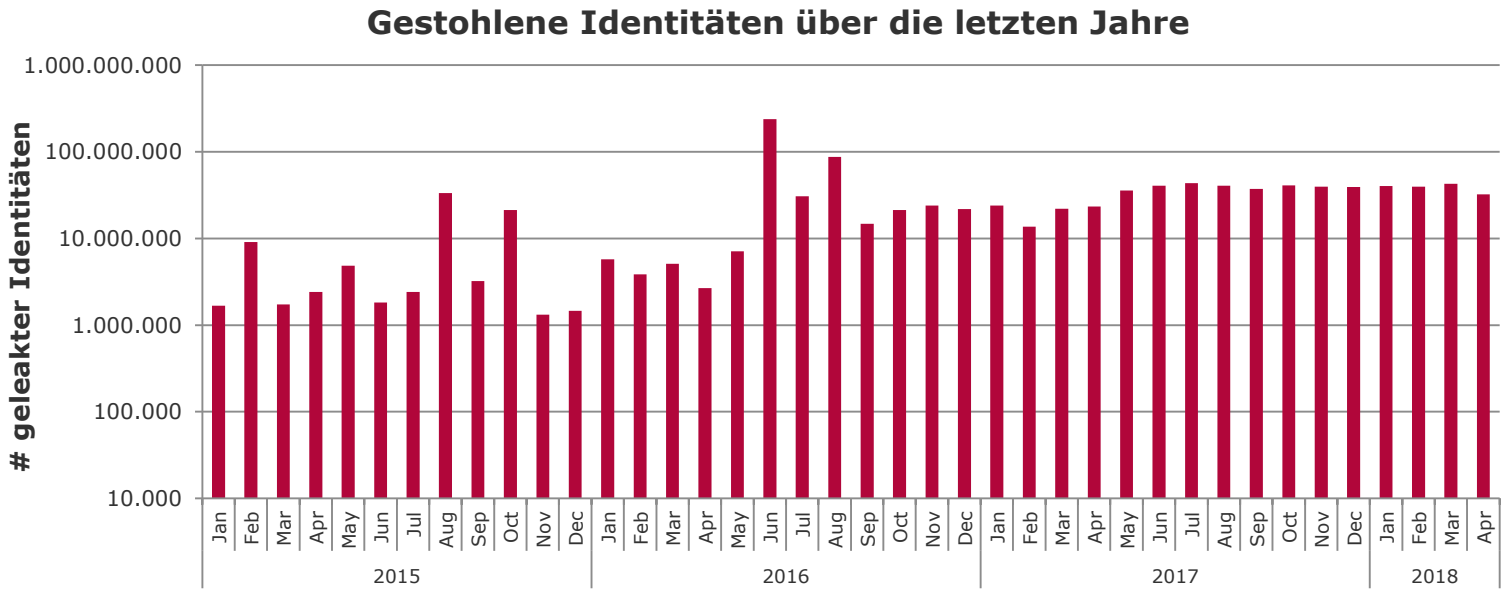
Die Gefahr von Identitätsdiebstählen

HPI Identity Leak Checker

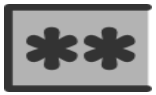
David Jaeger
IT Security Engineering Team
Hasso-Plattner-Institut, Potsdam

Identitätsdiebstähle haben massiv zugenommen

- Fast wöchentlich riesige Datendiebstähle in der Medienberichterstattung
- Täglich zahlreiche kleinere Diebstähle, ohne dass man davon hört
- **im Durchschnitt > 20.000.000 geleakte Identitäten/ Monat**



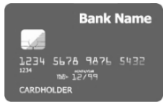
Identitätsdiebstahl umfasst viele Arten persönlicher Daten



Zugangsdaten/
Passwörter

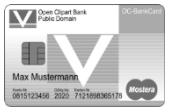
E-Mail Adressen

Anschriften



Kreditkartendaten

Im speziellen Interesse bei Cyberkriminellen



Kontodaten

Pass-/Ausweisdaten

Telefonnummern

Umwissenheit als Nährboden für Cyberkriminalität

- Opfer von Datendiebstählen **bekommen häufig gar nicht mit**, dass Ihre Daten im Internet veröffentlicht wurden
- Sie **sorgen sich nicht** um Medienberichte über große Identitätsdiebstähle
- Sie **wissen nicht** was ein Identitätsdiebstahl für sie konkret bedeutet und wie zu handeln ist

- Veröffentliche Nutzerkontodaten werden von Cyberkriminellen **missbraucht**
  - **Verkauf auf Schwarzmarkt**
  - Veröffentlichung der Daten zur **Erlangung von Anerkennung**
  - Login in Finanzdienste und **Abheben von Geldern**
  - Login in **Dienstaccounts**, die gleiches Passwort haben
  - …

Ansatz zur Stärkung des Sicherheitsbewusstseins

Ziel: Stelle einen Webdienst bereit, bei denen Personen überprüfen können, ob sie Opfer eines Identitätsdiebstahls geworden sind

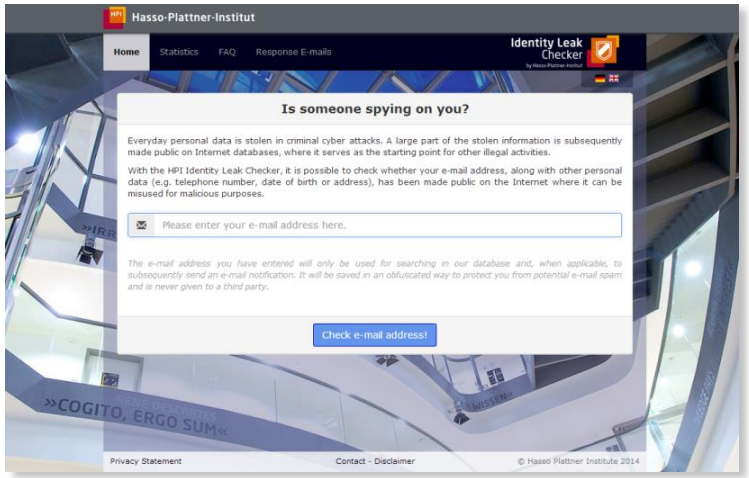
Adressierte Probleme

- **Sammlung** öffentlicher verfügbarer Daten von Identitätsdiebstählen
- **Normalisierung** von Identitätsdaten
- **Informierung** von Personen auf Anfrage, ob ihre Daten von einem Leak betroffen sind unter Beachtung der Privatsphäre der Opfer
- **Vorschlag von empfohlenen Aktionen** im Fall von Identitätsdiebstahl
- Bereitstellung von **Passwortstatistiken** (Top 100, Häufige Domänen, …)

HPI Identity Leak Checker (1/2)

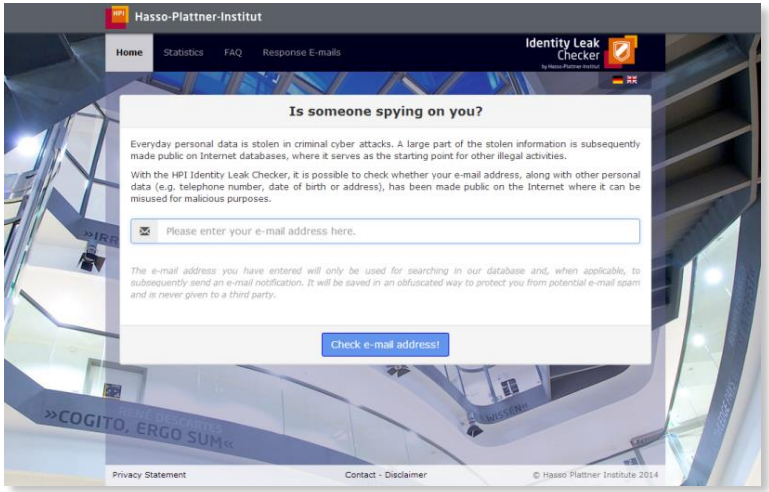
- Ermöglicht **Überprüfung von E-Mail-Adressen** auf Vorhandensein in veröffentlichten Identitätsleaks
- Sendet **E-Mail mit Prüfungsergebnissen** an die anfragende E-Mail-Adresse
- Stellt **Passwortstatistiken** bereit

Identity Leak Checker
by Hasso-Plattner-Institut



HPI Identity Leak Checker (2/2)

- Online seit Mai 2014
- Rund **7,2 Millionen** Anfragen
- Rund **1,3 Million** Personen wurden informiert, dass ihre Daten öffentlich im Internet geleakt wurden
- Normalisierung von **5,3 Milliarden Identitäten** aus mehr als **650 Leaks**
- **Ca. 5.000 Identitätsleaks**, die noch nicht normalisiert wurden



Die Gefahr von Identitäts-diebstählen

Hasso-Plattner-Institut

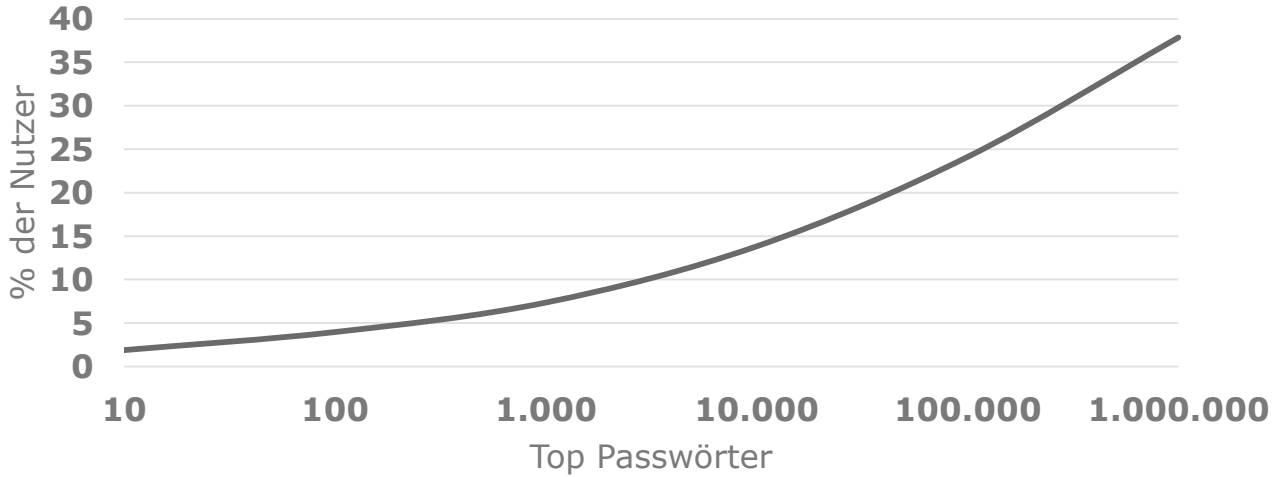
Analyse von Passworthäufigkeiten (1/2)

#	Password	Frequency
1	123456	4.48‰
2	123456789	1.50‰
3	111111	0.78‰
4	qwerty	0.76‰
5	12345678	0.63‰
6	123123	0.57‰
7	000000	0.54‰
8	password	0.46‰
9	1234567890	0.45‰
10	1234567	0.45‰

- Ausreißer bei Passwörtern wurden aussortiert, z.B. "*adobe123*"
- Top Passwörter basieren häufig auf Zahlenreihen und Tastatursequenzen

Analyse von Passworthäufigkeiten (2/2)

- **Datenquelle:** >2 Milliarden Nutzerdaten, ~600 Leaks
- 37% der Nutzer verwenden Passwörter aus den Top 1 Million



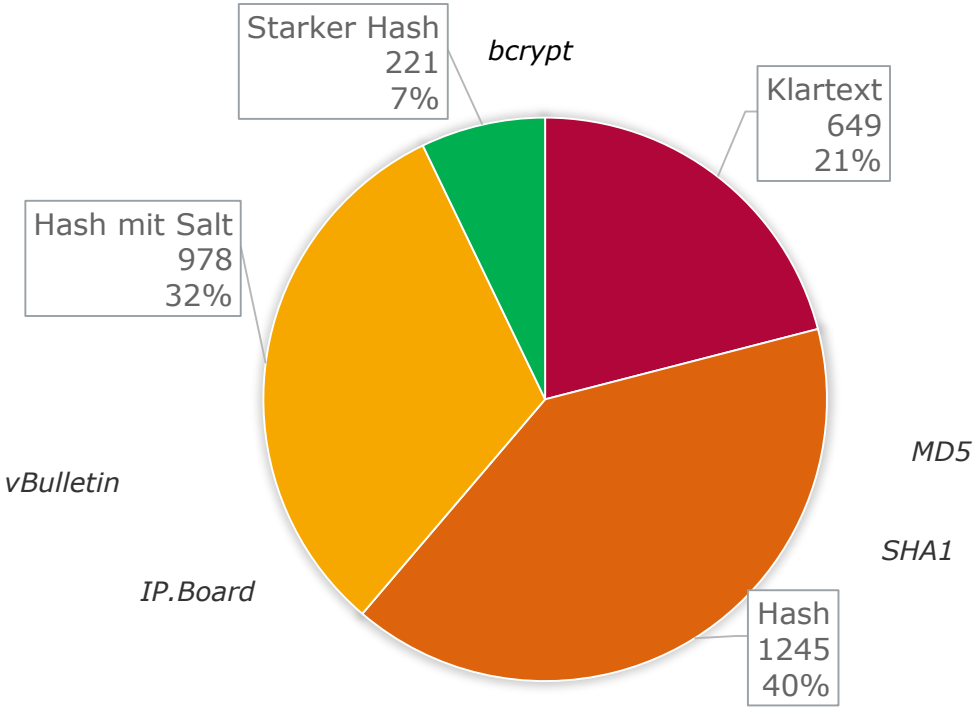
Analyse von regionalen Passwörtern

- In verschiedenen Regionen können spezielle Passwörter beobachtet werden
  - Chinesisch: Hohe Anzahl von numerischen Passwörtern
  - Russisch: Eintippen auf russischer Tastatur mit englischem Layout
  - UK: Fußballvereine

Email-TLD	Sprache	Top 3 Passwörter
uk	British English	liverpool, arsenal, chelsea
fr	Französisch	azerty, marseille, doudou
de	Deutsch	passwort, f***en, qwertz
it	Italienisch	juventus, andrea, francesco
nl	Niederländisch	welkom, welkom01, wachtwoord
cn	Chinesisch	5201314, woaini, 1314520
ru	Russisch	qwertyuiop, 1q2w3e4r5t

Analyse von Passworthashroutinen

- Analyse von 3093 Identitätsleaks



Analyse der Passwortwiederverwendung (1/2)

- Problem: **63%** von Datendiebstählen sind unsachgemäßer Passwortnutzung geschuldet (Verizon Breach Report, 2016)
  - Kritisch ist vor allem Passwortwiederverwendung
  - aktuelles Beispiel: gekaperte Datenbank des ownCloud-Forums

- Haben 1 Milliarde Passwörter von Nutzern untersucht
  - 68 Milliarde Nutzer mit mindestens zwei Accounts
- Beobachtung
  - **20%** der Nutzer verwenden **identische Passwörter** mehrmals
  - **27%** der Nutzer verwenden **ähnliche Passwörter** mehrmals
  - Aber: Bei **ähnlichen Diensten** liegt Wiederverwendung bei teils **50%**

Analyse der Passwortwiederverwendung (2/2)

- Passwortwiederwendung zwischen Dienstpaaren

1	-																			
2	22.1	-																		
3	18.7	44.5	-																	
4	23.6	39.2	57.1	-																
5	18.9	3.8	21.3	22.0	-															
6	7.1	10.0	23.6	17.5	22.4	-														
7	22.8	23.1	38.9	39.4	17.2	14.3	-													
8	13.1	13.5	42.9	28.6	34.0	15.2	22.1	-												
9	14.2	18.0	30.0	23.9	22.9	15.7	26.0	37.9	-											
10	20.6	33.4	58.6	53.8	28.6	15.4	33.3	15.2	38.4	-										
11	13.5	10.9	18.4	15.6	42.0	20.0	17.5	31.8	32.3	32.0	-									
12	14.7	17.3	24.4	30.3	25.6	7.3	20.3	22.7	26.1	24.2	15.9	-								
13	17.7	13.3	23.5	23.9	19.0	8.4	17.7	16.7	18.2	22.4	16.7	14.0	-							
14	21.0	26.4	20.8	36.0	45.7	19.4	24.5	35.0	41.7	41.3	40.6	27.4	22.4	-						
15	26.9	45.1	61.4	49.4	21.0	14.4	34.3	33.5	41.9	40.1	35.2	28.1	20.4	42.6	-					
16	20.1	19.7	21.9	33.7	33.7	6.2	23.4	10.1	20.9	18.8	16.7	25.2	11.6	31.7	44.2	-				
17	19.7	9.6	2.5	3.8	5.6	6.6	0.0	7.6	24.8	22.9	12.4	19.9	15.2	25.3	42.0	26.4	-			
18	14.7	33.3	61.6	51.0	20.3	17.7	33.6	37.5	18.1	46.5	14.3	13.1	14.6	26.4	52.3	11.6	6.0	-		
19	17.6	14.0	32.9	33.6	22.7	5.2	26.4	27.5	29.4	31.6	24.2	16.0	13.7	31.4	23.9	14.6	12.1	29.2	-	
20	22.7	48.1	70.0	58.9	20.8	25.4	36.3	40.2	39.5	64.3	23.6	30.5	28.5	38.2	59.9	30.8	34.7	59.4	40.6	-
21	37.8	49.9	56.1	52.0	48.0	13.7	36.8	25.1	36.9	43.7	37.1	24.2	23.0	46.8	52.5	52.8	49.2	41.0	21.5	60.2	-
ID	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21

Chinesisch

Dating

ID	Source	ID	Source
1	000webhost.com	12	mpgh.net
2	17.media	13	myspace.com
3	51cto.com	14	naughtyamerica.com
4	aipai.com	15	nexusmods.com
5	ashleymadison.com	16	r2games.com
6	badoo.com	17	sprashivai.ru
7	csdn.net	18	tianya.cn
8	gawker.com	19	vk.com
9	imesh.com	20	xiaomi.com
10	linkedin.com	21	xsplit.com
11	mate1.com		

BKA Meldung über 500 Millionen Nutzerdaten

- BKA hat Datensatz über 500 Millionen Nutzerdaten im Darkweb gefunden (ca. 49 Millionen .de-Adressen)
- Daten wurden kurzfristig in unseren Checker übernommen
- Riesige Medienresonanz und Millionen von Anfragen auf unseren Dienst
- Innerhalb 1 Woche: 3 Millionen Anfragen

SPIEGEL ONLINE DER SPIEGEL SPIEGEL TV Anmelden

BKA findet 500 Millionen gestohlene Datensätze

So prüfen Sie, ob Ihr Account gestohlen wurde

Es ist ein brisanter Fund: Das Bundeskriminalamt hat im Internet eine Sammlung mit einer halben Milliarde E-Mail-Adressen und Passwörtern entdeckt. Ob Sie betroffen sind, können Sie online prüfen.

Passwortabfrage auf einem Laptop

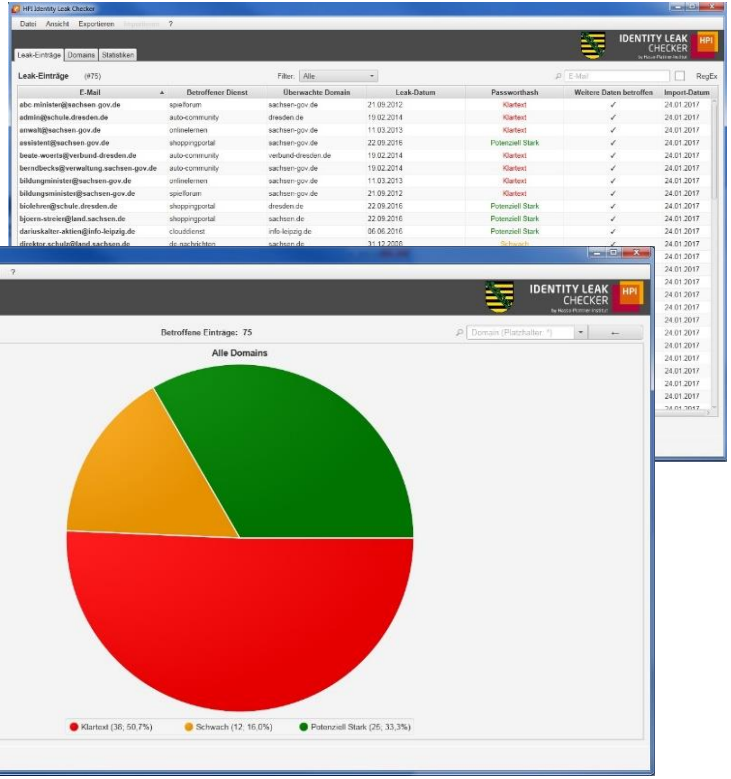
Teilen Twittern E-Mail

Freitag, 07.07.2017 14:20 Uhr Drucken Nutzungsrechte Feedback Kommentieren

Mit einer ungewöhnlichen Meldung erinnert das Bundeskriminalamt (BKA) an die Grundregeln der Passwortnutzung im Internet: Vergeben Sie für jeden Onlinedienst ein anderes Passwort, und ändern Sie Ihre Passwörter regelmäßig.

NEU: Identity Leak Checker Desktop Client

- Überwachung eigener Domänen
- Listet betroffene E-Mail-Adressen auf
- Visualisiert Sicherheitslage einer einzelnen Domäne oder eines Unternehmens



- Kooperationsprojekt mit dem Freistaat Sachsen

Danke für die Aufmerksamkeit!

HPI IT-Security Engineering Team

security-analytics@hpi.de

Online Services: https://sec.hpi.de

https://sec.hpi.de/reams/

https://sec.hpi.de/leak-checker/

https://sec.hpi.de/vulndb/