How to not get Bundestaghacked™

öffentliche Daten nützen
Private Daten schützen

Speaker notes

unsere Motivation vorstellen
Hackerethik
WIR sind die guten

Der bei Weitem größte Unsicherheitsfaktor in puncto Hacking ist der Mensch.

Speaker notes

Motivation der heutigen Besucher

- “Bundestaghack™”
- Datensparsamkeit
- Account absichern
  - Passwortlisten geleaked
  - Passwortsicherheit
  - Das richtige Passwort
  - Die falschen Sicherheitsfragen
  - Zwei-Faktor-Authentisierung
  - Passwortmanager einrichten
- Andere wichtige Themen
- Eure Fragen

Speaker notes

Ablauf vorstellen

“Bundestaghack™”

- Hack?
- Doxing!

Speaker notes

Was versteht man eigentlich unter einem Hack?
kein Hack im wirklichen Sinn (Einbruch)
Sammlung von Adressen und Telefonnummern
Doxing ist der Fachbegriff
Große Aufregung weil Politiker betroffen

Das hilft nicht

- Hackback
- andere machen lassen (Cyberabwehrzentren)

Datensparsamkeit

- nur unbedingt notwendige Daten angeben
- Angriffsflächen klein halten
- keine/wenig persönlichen Informationen
- Nutzung von sozialen Netzen ist das Gegenteil
- DSGVO

Speaker notes

- Geburtstag, Wohnort
  - öffentliche Daten/Accounts
  - (DSGVO) Download aller Daten eines Dienstes
  - DEMO facebook/twitter
  - DEMO https://pipl.com/api/demo
  - Lesen: https://gizmodo.com/c/goodbye-big-five

Account absichern

****

Passwortlisten

Speaker notes

erst:
770 Millionen Adressen
dann:
1 TB Daten
2,1 Milliarden verschiedene E-Mail-Adressen
zahlreiche Passwörter / Mailadresse

Woher kommen die Listen?

- Daten-Einbruch
- nicht gesicherte Datenbanken
- Phising

Speaker notes

Fenster luschern
spezielle Suchmaschinen für Datenbanken
https://sec.hpi.uni-potsdam.de/ilc/
https://monitor.firefox.com/

Speaker notes

NIEMALS beide Infos (Benutzer/Passwort) zusammen eingeben

Passwortsicherheit

Ist mein Passwort beim Anbieter sicher?

Speaker notes

Kein Anbieter kann 100% Sicherheit bieten
Wie wurden Passwörter bei Anbietern gespeichert? (Klartext, als Hash)
Passwortbeschränkungen können ein Indiz für schlechtes abspeichern sein
Passwort vergessen -> altes Passwort lesbar per Mail bekommen -> blöd
Hashes erklären

e22a63fb76874c99488435f26b117e37

- password
- e22a63fb76874c99488435f26b117e37
- ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ?

Speaker notes

Von Passwort zum Hash zum Passwort
google suche liefert das wort

ID	Name (Algorithm)	#Hashes	Left	Found	Recovered	Updated
37	Ohmedia.my SHA1	51'382	137	51'245	99.73%	2018.12.24 14:28:02
36	Punto.pe SHA1	110'669	860	109'809	99.22%	2019.01.20 08:40:02
35	Zoosk.com MD5	29'013'020	265	29'012'755	100%	2018.12.19 18:14:01
34	TomSawyer.com MD5	12'257	756	11'501	93.83%	2018.12.18 18:30:02
33	Renault.com.ar SHA1	37'552	25'169	12'383	32.98%	2019.01.28 22:31:01
32	MilitarySingles.com MD5	118'383	534	117'849	99.55%	2019.01.10 17:08:01
31	Last.fm 2012 MD5	2'507'741	245'578	2'262'163	90.21%	2019.01.28 11:04:02
30	ImsResearch.com MD5	30'223	2'338	27'885	92.26%	2018.12.24 16:24:01
29	Booz Allen Hamilton SHA1	141'526	8'639	132'887	93.9%	2019.01.28 22:31:01

Speaker notes

Listen mit Hashes zu Wörtern -> Rainbowtables
lehren daraus

Das richtige Passwort

- nicht im Wörterbuch
- besser viele zusammenhanglose Wörter hintereinander
- so lang wie möglich
- Buchstaben, Zahlen, Zeichen, Alles was die Tastatur hergibt
- jeder Dienst ein eigenes Passwort
- Bonuspunkte: jeder Dienst eine eigenen E-Mail

Speaker notes

Ziel ist die Anzahl der möglichen Zeichenkombinationen zu erhöhen

Die falschen Sicherheitsfragen

- Nichts Persönliches

Speaker notes

Angaben aus sozialen Netzen richtig kombinieren ist unter Umständen keine große Hürde
Datensparsamkeit
Falsche Freunde kennen die Antworten

Zwei-Faktor-Authentisierung

- Etwas das man weiß
- Etwas das man hat
- twofactorauth.org

Speaker notes

DEMO
Hat: Zweiten Kanal: SMS TAN/ M-TAN
Hardware: Yubikey, Token
Software: TOTP

Passwortmanager

Unsere Empfehlung:

- KeePass 2 / KeePassXC
- Android: Keepass2Android
- iOS: MiniKeePass

Speaker notes

Keepass ist im Bugbounty Programm der EU (erklären)

Andere wichtige Themen

- Verschlüsselung
- Backup

Eure Fragen

danach Workshop ...

Danke

hacklabor.de
twitter.com/hacklabor
fb.me/hacklabor
instagram.com/hacklabor.de
hacklabor.de/youtube