ATHENE
National Research Center for Applied Cybersecurity

Digitalisierung, aber sicher:

Wie Systeme angegriffen werden, und was wir tun sollten

Prof. Dr. Haya Shulman

ATHENE | Goethe-Universität Frankfurt | Fraunhofer SIT

Cybersicherheitslage in Deutschland

Bundesamt für Sicherheit in der Informationstechnik

IT-Sicherheitslage bleibt angespannt bis kritisch

bitkom research

Jährliche Schäden deutlich über **200 Mrd. Euro**

- **Spionage, Erpressung, Denial of Service, Sabotage**
- **Digitalisierung vergrößert Angriffsfläche**
- **Geopolitische/wirtschaftliche Lage erhöht Gefahr**

Überblick

- **Einführung**
- **Wie werden Systeme angegriffen?**
  - Kompromittierte Konten
  - Schwachstellen
- **Empfehlungen**

Wie werden Systeme angegriffen?

Ransomware | Data Breaches | Hacks | Spionage

Ransomware gang threatens to expose police informants if ransom is not paid

Nvidia data breach exposes data of 71,000 employees: Report

Hack durch ein kompromittiertes VPN Konto

medibank

TELSTRA

Dialog
INFORMATION TECHNOLOGY

VINOMOFO

Überblick

- **Einführung**
- **Wie werden Systeme angegriffen?**
  - Kompromittierte Konten
  - Schwachstellen
- **Empfehlungen**

Kompromittierte Konten als Einfallstor

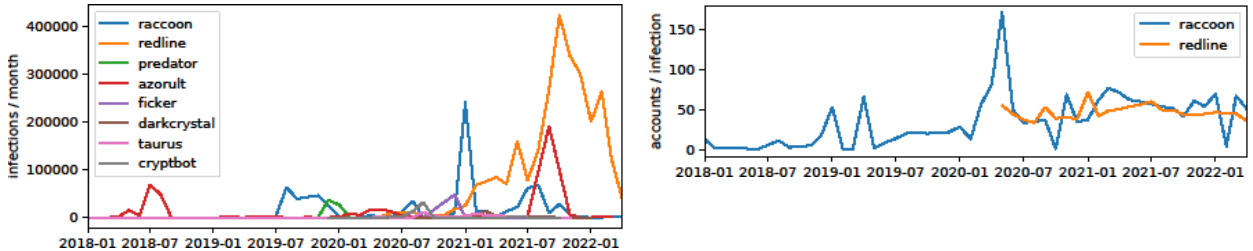
Eindringen und Ausbreiten innerhalb der Opferorganisation

- Infostealers
- Data Dumps
- Durchprobieren schwacher Passwörter
- Durchsuchen von Cloud / Repositories / Code nach abgelegten Passwörtern
- Social Engineering und Phishing
- Innentäter: Bestechung, Umgehen von MFA, Installieren von Malware

Kompromittierte Konten als Einfallstor

Infostealers

- Infostealers
- Data Dumps
- Durchprobieren schwacher Passwörter
- Durchsuchen von Cloud / Repositories / Code nach abgelegten Passwörtern
- Social Engineering und Phishing
- Innentäter: Bestechung, Umgehen von MFA, Installieren von Malware



Kompromittierte Konten als Einfallstor

Passwörter in Data Dumps

- Infostealers
- Data Dumps
- Durchprobieren schwacher Passwörter
- Durchsuchen von Cloud / Repositories / Code nach abgelegten Passwörtern
- Social Engineering und Phishing
- Innentäter: Bestechung, Umgehen von MFA, Installieren von Malware

Kompromittierte Konten als Einfallstor

Durchprobieren schwacher Passwörter

- Infostealers
- Data Dumps
- **Durchprobieren schwacher Passwörter**
- Durchsuchen von Cloud / Repositories / Code nach abgelegten Passwörtern
- Social Engineering und Phishing
- Innentäter: Bestechung, Umgehen von MFA, Installieren von Malware

Kompromittierte Konten als Einfallstor

Passwörter in Cloud / Repositories / Code

- Infostealers
- Data Dumps
- Durchprobieren schwacher Passwörter
- Durchsuchen von Cloud / Repositories / Code nach abgelegten Passwörtern
- Social Engineering und Phishing
- Innentäter: Bestechung, Umgehen von MFA, Installieren von Malware

Kompromittierte Konten als Einfallstor

Social Engineering und Phishing

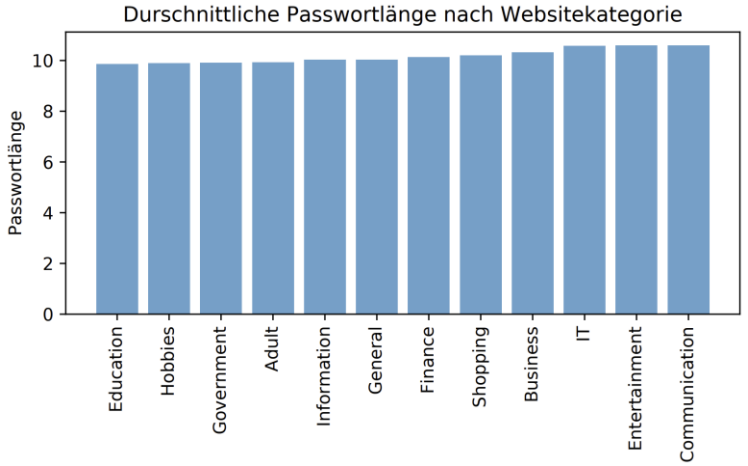
- Infostealers
- Data Dumps
- Durchprobieren schwacher Passwörter
- Durchsuchen von Cloud / Repositories / Code nach abgelegten Passwörtern
- **Social Engineering und Phishing**
- Innentäter: Bestechung, Umgehen von MFA, Installieren von Malware

Kompromittierte Konten als Einfallstor
Innentäter

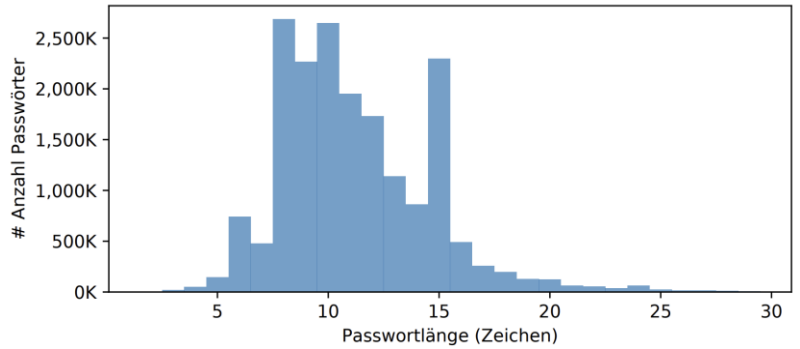
- Infostealers
- Data Dumps
- Durchprobieren schwacher Passwörter
- Durchsuchen von Cloud / Repositories / Code nach abgelegten Passwörtern
- Social Engineering und Phishing
- Innentäter: Bestechung, Umgehen von MFA, Installieren von Malware

Wie sehen „geleakte“ Passwörter aus?

- **Analyse von Datenlecks zwischen Januar 2018 und April 2022**
  - 4 Millionen Einträge
  - Passwörter meistens 8-12 Zeichen
  - Entropie von 30-50 bits (∅ 4,3 bits/Zeichen)
  - Ähnlich in allen Sektoren, stärkere PW in IT, AI, Web-Hosting

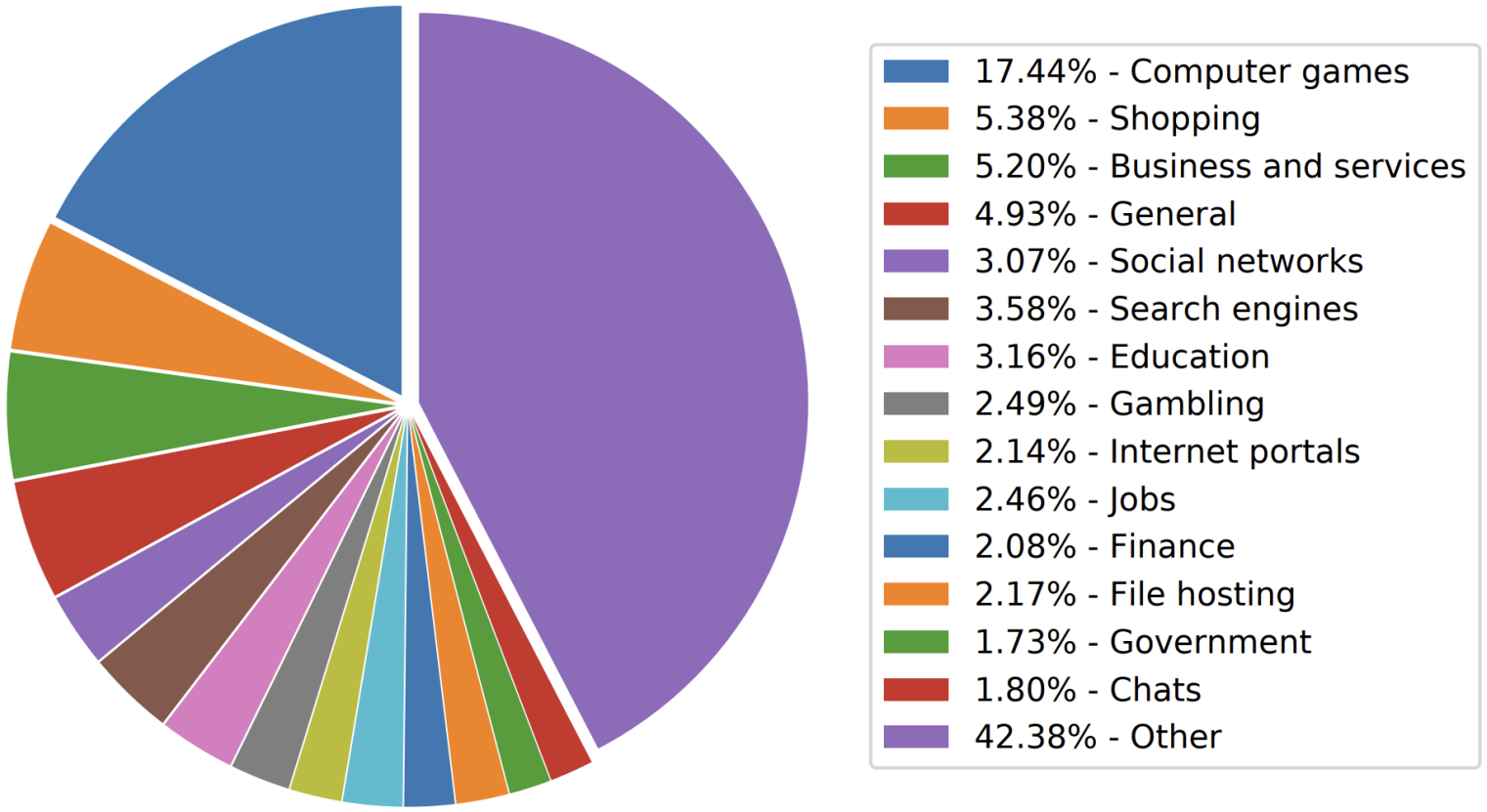


- **Wie lange dauert es, einen Passwort-Hash zu brechen?**
  - Nvidia RTX 3090 GPU mit 9746 MHz:
    SHA256 mit 45 bits Entropie: 1 Stunde
    SHA256 mit 40 bits Entropie: 113 Sekunden



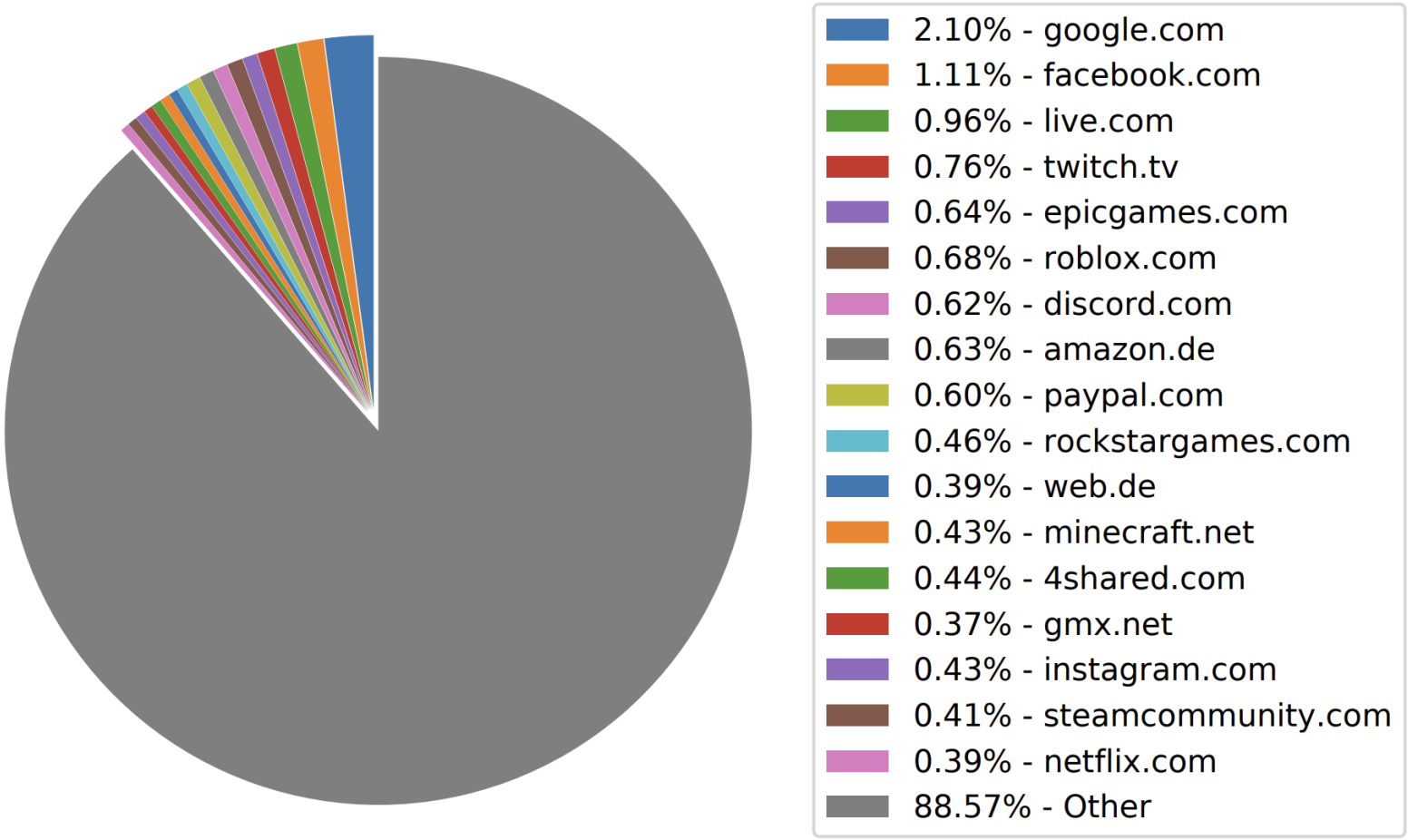
Wie sehen „geleakte“ Passwörter aus?

Anzahl geleakter Konten nach Kategorien



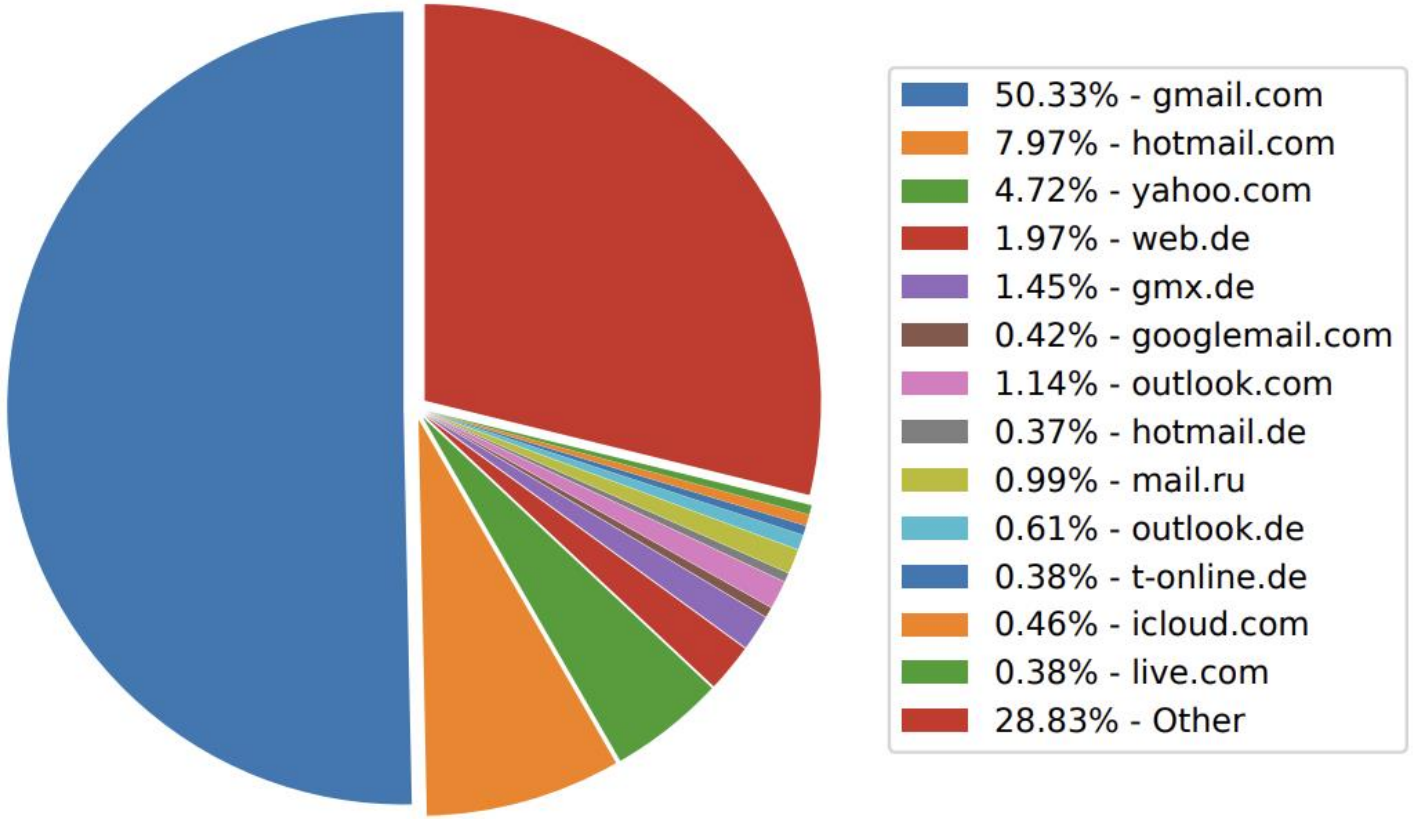
Wie sehen „geleakte“ Passwörter aus?

Anzahl kompromittierter Konten nach Website



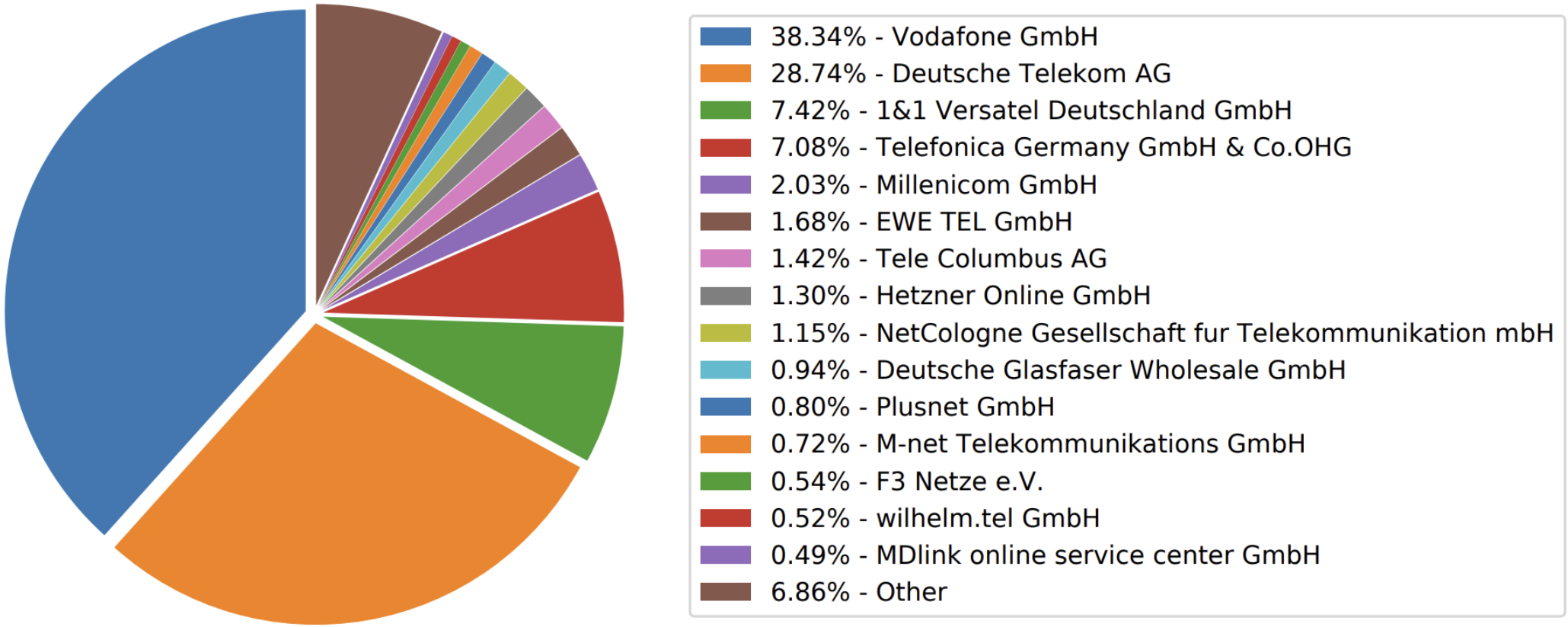
Wie sehen „geleakte“ Passwörter aus?

Anzahl geleakter Konten nach Mailprovider des Nutzers



Wie sehen „geleakte“ Passwörter aus?

Anzahl Infostealer-Infektionen nach Internetprovider



Wie sehen die Passwörter aus, die Kriminelle durchprobieren?

- **Analyse der Passwörter, die Angreifer tatsächlich durchprobieren**
  - Vorwiegend aus dem „RockYou2021"-Datenleck
  - + einfache Variationen dieser Passwörter

- **Analyse der Angriffe**
  - Angriffe mit geringem Aufwand und geringen Kosten
  - Vorwiegend automatisierte Werkzeugen
  - Angriffe sind meistens sehr einfach

Was sollten Organisationen und wir daraus lernen?

1. Eigene Konten gegen Passwort Dumps testen
2. Sichere Multifaktor-Authentifizierung (MFA) verwenden
3. Keine Passwörter mehrfach oder mit einfachen Variationen für verschiedene Dienste verwenden

Überblick

- **Einführung**
- **Wie werden Systeme angegriffen?**
  - Kompromittierte Konten
  - Schwachstellen
- **Empfehlungen**

Schwachstellen patchen

Oder: wie sollte man Pentests durchführen

- **Wir kontrollieren und testen nicht alles**
  - Schwachstellen oft in IT-Anbieter, APIs, Komponenten von Drittparteien
- **Hersteller warten oft mit Patches**
- **Unsere Forschung zeigt:**
  - 15 (43%) der beliebten Router sind verwundbar
  - 11 Router erfüllen nicht Standards
- **Immer noch keine Patches!**
  - Unwirtschaftlich für Hersteller

% of Identified	% of Total	Absolute	Generic match	Vulnerable	Router
41.62%	0.59%	405	x	x	Tenda
24.25%	0.34%	236	x	x	Huawei
15.42%	0.22%	150	x	x	Fritzbox
12.13%	0.17%	118	x	x	Mercusys
1.54%	0.02%	15	x		Linksys AC2200
1.34%	0.02%	13			Xiaomi Mi router
1.23%	0.02%	12		x	Draytek
1.13%	0.02%	11			Speedport Smart
0.72%	0.01%	7		x	Netgear R6120
0.21%	0.00%	2			D-Link DIR-600
0.10%	0.00%	1			Teltonika
0.10%	0.00%	1			Linksys AC1000
0.10%	0.00%	1		x	Centurylink
0.10%	0.00%	1			ASUS ROG
100.00%	1.42%	973	-	95.48%	Identified
-	98.58%	67482	-	-	Not Identified
-	100.00%	68455	-	1.36%	Total

Vendor	Model	Has cache	version.bind	Attacks: Any attack	Misinterpretation injection: direct \.	direct \000	direct \.	CNAME \000	TXID forward	Fixed UDP port	CD=1 to disable DNSSEC	Non-standard
Home/SOHO routers												
Asus	GT-AC2900	✓	dnsmasq	-	-	-	-	-	-	-	-	-
AVM	Fritz!Box 6660	✓	-	✓	✓	-	-	-	-	-	-	-
AVM	Fritz!Box 7312	✓	-	✓	✓	-	-	-	-	-	-	-
AVM	Fritz!Box 7520	✓	-	✓	✓	-	-	-	-	-	-	-
AVM	Fritz!Box 7590	✓	-	✓	✓	-	-	-	-	-	-	-
Cudy	WR1300	✓	-[1]	-	-	-	-	-	-	-	-	-
D-Link	N150 (DIR-600)	✓	-[1]	-	-	-	-	-	-	-	-	-
D-Link	N300 (DWR-920)	✓	-[1]	-	-	-	-	-	-	-	-	-
DrayTek	Vigor2120	✓	-	✓	✓[5]	✓[5]	-	-	✓	-	✓	(h)
Edimax	N300	-	-	✓	-	-	-	-	-	✓(1027)	-	(h)
Linksys	E5350 (AC1000)	✓	dnsmasq-2.40	-	-	-	-	-	-	-	-	-
Linksys	EA8300 (AC2200)	✓	dnsmasq-2.78	-	-	-	-	-	-	-	-	-
Mercusys	MW305R	-	-	✓[2]	-	-	-	-	no[2]	-	-	(h)
Netgear	AC1200 / R6120	-	-	-	-	-	-	-	-	-	-	-
Netis	AC1200	✓	dnsmasq-2.79	-	-	-	-	-	-	-	-	-
STRONG	Wi-Fi Router 300	-	-	✓	-	-	-	-	-	✓(1027)	-	(h)
Tenda	AC10v3	✓	-	✓	✓	✓	-	-	-	✓(62066)	✓	(f),(h)
Tenda	F3	✓	-	✓	✓	✓	-	-	-	✓(50387)	✓	(f),(h)
TP-Link	Archer C7 (AC1750)	-	-	-	-	-	-	-	-	-	-	-
TP-Link	TL-WR841N	-	-	-	-	-	-	-	-	-	-	-
Trendnet	TW100-S4W1CA	✓	-	✓	-	-	-	-	-	✓(5530)	✓	(f),(h)
Xiaomi	MiRouter4A	✓	dnsmasq-2.71	-	-	-	-	-	-	-	-	-
Zyxel	Speedlink 5501	✓	dnsmasq-2.57	-	-	-	-	-	-	-	-	-
ISP-branded home routers												
Actiontec	MI424WR	-	-	✓	-	-	-	-	no[2]	✓(1024)	-	(h)
CenturyLink	C3000Z	✓	-	✓	✓	✓	-	-	✓	✓[3]	✓	(g),(h)
Telekom	Speedport Smart 3	✓	-[1]	-	-	-	-	-	-	-	-	-
Vodafone	Station TG3442DE	✓	dnsmasq-2.78	-	-	-	-	-	-	-	-	-
Small business routers												
Bintec	RS353a	✓	-	✓	-	-	✓	✓	-	-	-	(f),(h)
Cisco	RV260	✓	dnsmasq-2.78	-	-	-	-	-	-	-	-	-
Grandstream	GWN7000	✓	dnsmasq-2.78	-	-	-	-	-	-	-	-	-
Synology	RT2600AC	✓	dnsmasq-2.78	-	-	-	-	-	-	-	-	-
Ubiquiti	EdgeRouter4	✓	dnsmasq-2.78	-	-	-	-	-	-	-	-	-
Mobile/4G routers												
Huawei	5G CPE 5 Pro 2	✓	-	✓	-	✓[5]	-	-	-	-	-	(g)
Level421	TARKAN	✓	dnsmasq-2.51	-[4]	-[4]	-	-[4]	-	-	-	-	-
Teltonika	RUT950U022C0	✓	dnsmasq-2.81	-	-	-	-	-	-	-	-	-
SUM(✓)	35 100%	28 80%	-	15 43%	8 23%	5 14%	1 3%	1 13%	4 11%	7 20%	5 14%	11 31%

✓: vulnerable/yes. -: not vulnerable/no. [1]: hidden dnsmasq version, [2]: uses sequential TXIDs, [3]: Port selected randomly at boot. [4]: ISP network vulnerable. [5]: Query section mismatch. (f): CNAME chain merging. (g): EDNS can cause broken responses. (h): No TCP support.

Überblick gewinnen und behalten

Umfangreiche Studien zu IT-Infrastrukturen

Binding Operational Directive 23-01 - Improving Asset Visibility and Vulnerability Detection on Federal Networks

Oktober 2022: Richtlinie für US Bundesbehörden:

- Automated asset discovery every 7 days
- Vulnerability enumeration across discovered assets every 14 days

https://www.cisa.gov/binding-operational-directive-23-01

2020:

Studie der Cybersicherheit aller im Bundestag vertretenen Parteien, auf allen Ebenen

2022:

Studie der Bundesländer, Univ. und Forschungseinrichtungen

Überblick

- **Einführung**
- **Wie werden Systeme angegriffen?**
  - Kompromittierte Konten
  - Schwachstellen
- **Empfehlungen**

Kein IT-System ist 100% sicher

Mit genug Aufwand ist jedes IT-System „hackbar“

- **Security by Design für SW, HW, Netze**

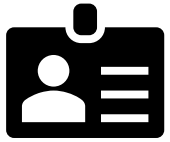
Wie kann man dennoch Cybersicherheit verbessern?

- **Überblick gewinnen und behalten:**
  Wissen um eigenen IT und Verwundbarkeiten
- **Vorsorge treffen:**
  Organisation, Training, Business Continuity vis-a-vis Cyberangriffen
- **Resiliente Cybersicherheitsarchitekturen:**
  Umstieg auf Zero Trust Architekturen
- **Gemeinschaftliche Abwehr:**
  Aktive Cyberabwehr, z.B. Verkehrsumlenkungen

Zero Trust Architektur der US-Bundesregierung

Veröffentlicht 2022, verbindlich umzusetzen bis Ende 2024

- **Umfassende Ende-zu-Ende Verschlüsselung, ohne VPNs**



- **Zero Trust Authentifizierung von Nutzern, Systemen, Geräten**
  - Multifaktor-Authentifizierung, möglichst ohne Passwörter, mit Tokens
  - Komplexe Passwort-Policies sind hinderlich

- **Rechteminimierung, rollen- und attributbasierte Zugriffsrechte**

- **“Trust but verify” – Alles soll überprüft werden**
- **Explizite Schwachstellenprozesse**

Fazit

Die Lage ist ernst,
jedes System ist verwundbar

Aber die Lage ist nicht hoffnungslos

Es gibt Strategien zu einer resilienteren Cybersicherheit

תודה רבה!

Merci beaucoup!

çok teşekkürler

谢谢

Thank you very much!

Vielen Dank!

Dank je wel!

Muchas gracias

ありがとうございます

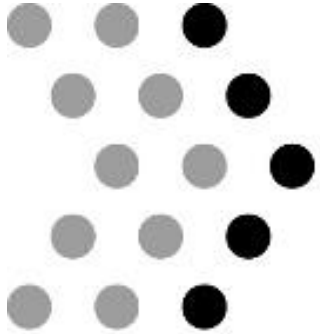
Dziękuję!

zor spas

شكرا لك

Grazie mille!

Was ist ATHENE?



ATHENE

Nationales Forschungszentrum für angewandte Cybersicherheit

Ein Forschungszentrum der Fraunhofer-Gesellschaft

mit besonderer Beteiligung von Hochschulen

finanziert von BMBF und HMWK