pegasus IT
Member of ITventive Group

Mit Phishing-Resistant-MFA und Passkeys gegen MiTM-Attacken bestens geschützt

pegasus IT
Member of ITventive Group

Alexander Karls
Cloud- und Security-Consultant
Mail: a.karls@pegasus-gmbh.de
Tel.: +49 9402 503-214

Kurzprofil:

- Über 20 Jahre in der IT tätig
- Mehr als 15 Jahre Erfahrung in leitender Funktion
- Langjährige Erfahrung aus selbständiger Tätigkeit
- Vorfall-Experte im CSN des BSI
- Erfahrener Trainer und Coach
- Podcast-Host von BlueScreen – Der Tech-Podcast

Cyber-Sicherheitsnetzwerk

Allianz für Cyber-Sicherheit
Teilnehmer

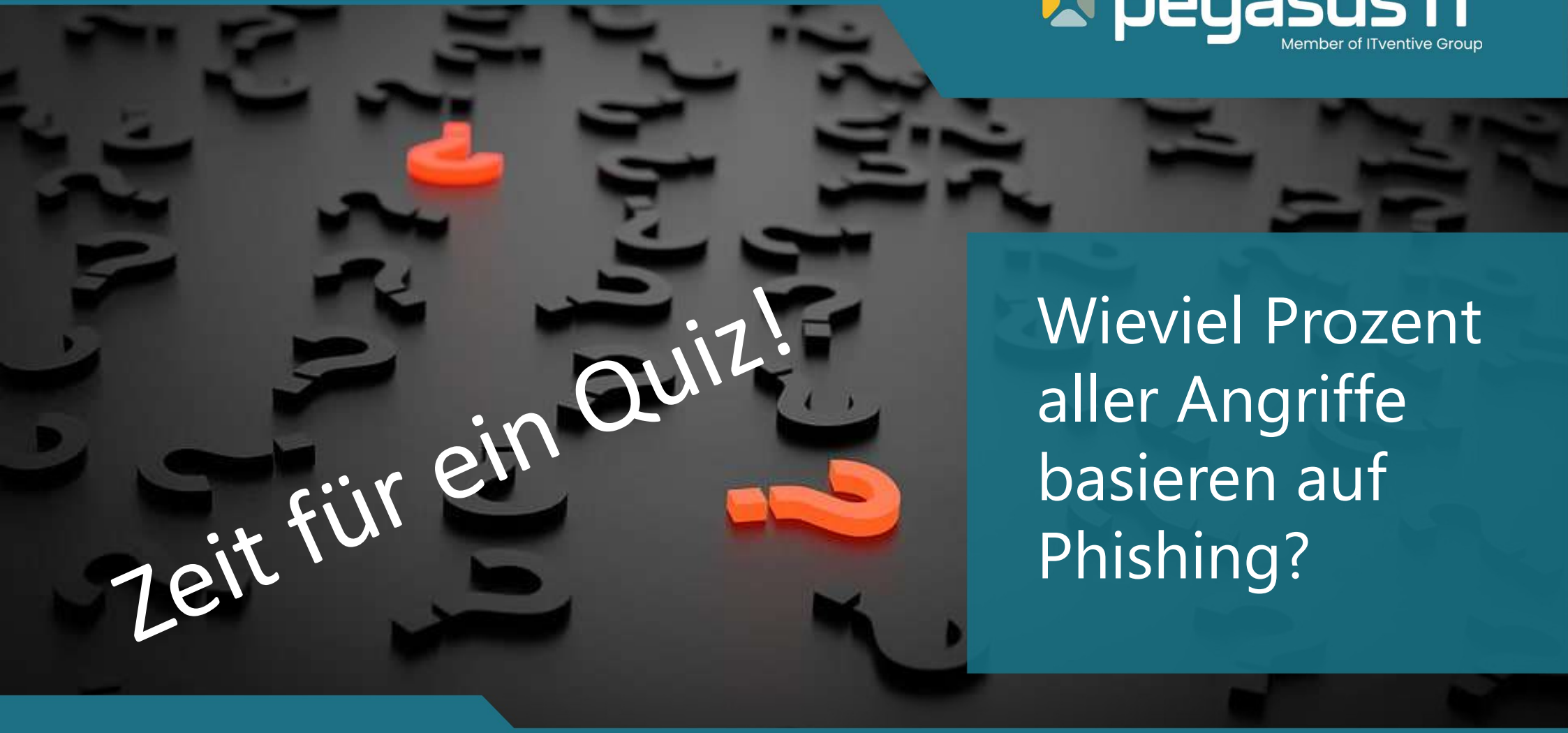
Mitarbeiterzahl	100
Zertifizierung	ISO 9001 / 27001 / 27018
Standorte	Regenstauf (pegasus GmbH / pegasus IT / IQ) Ludwigsburg (EVIATEC Systems AG) Bern (EVIATEC Digital Solutions AG) Brøndby / Koppenh. (EVIATEC Scandinavia ApS)
Rechenzentren	3
Einsatzgebiet	Europaweit / Weltweit
Vernetzung	> 1500 Standorte weltweit
Geschützte Anwender	> 50.000
Server im RZ	> 500
Kundengröße / Schnitt	25 - 1000

Regensburg / DE

Ludwigsburg / DE

Bern / CH

Koppenhagen / DK



pegasus IT
Member of ITventive Group

Wieviel Prozent aller Angriffe basieren auf Phishing?

Wieviel Prozent aller Angriffe basieren auf Phishing?

Cybercrime Statistics 2024

$10.5 Trillion

projected cost of cybercrimes by 2025.

$1.5 Trillion

Amount **earned by cybercriminals** for cybercrime activities yearly.

80%

of cybercrimes are **phishing attacks** in the technology sector.

2.7 billion hours

Total time **spent resolving cybercrimes;** average of 6.7 hours daily.

$5.09 Million

Is the highest cost of a data breach in U.S.A. in 2023.

$30 billion

Cost of Crypto-crime annually by 2025.

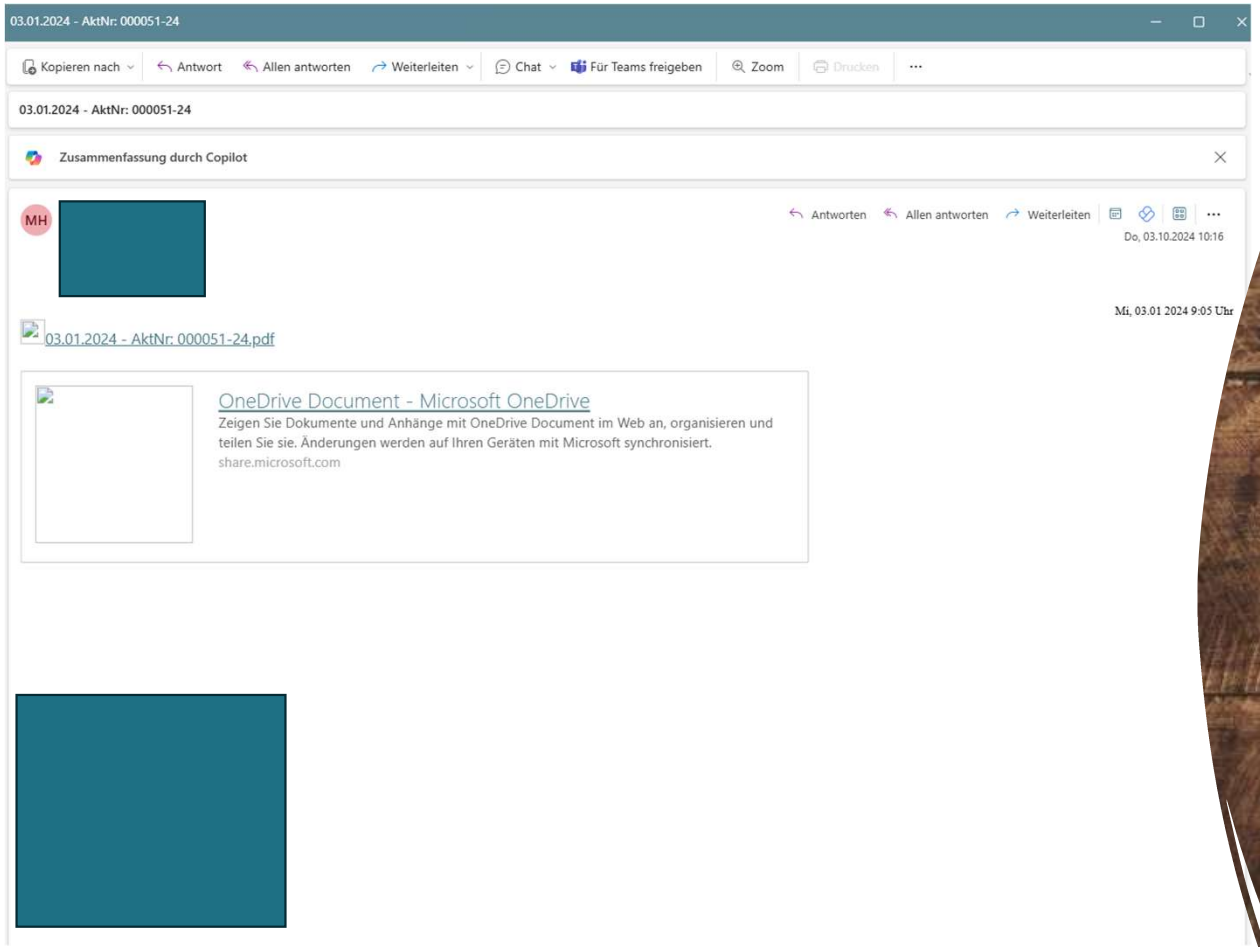
$265 Billion is the estimated annual cost of ransomware to victims by 2031.

Quelle: getastra.com

pegasus IT
Member of ITventive Group

„Ich habe nichts gemacht
und auf einmal war alles kaputt!“

Das Problem – Eintrittsvektor E-Mail



Das Problem – Umleitung zu „OneDrive“ > Canva

Die [redacted] GmbH hat Ihnen ein neues Dokument zur Verfügung gestellt.

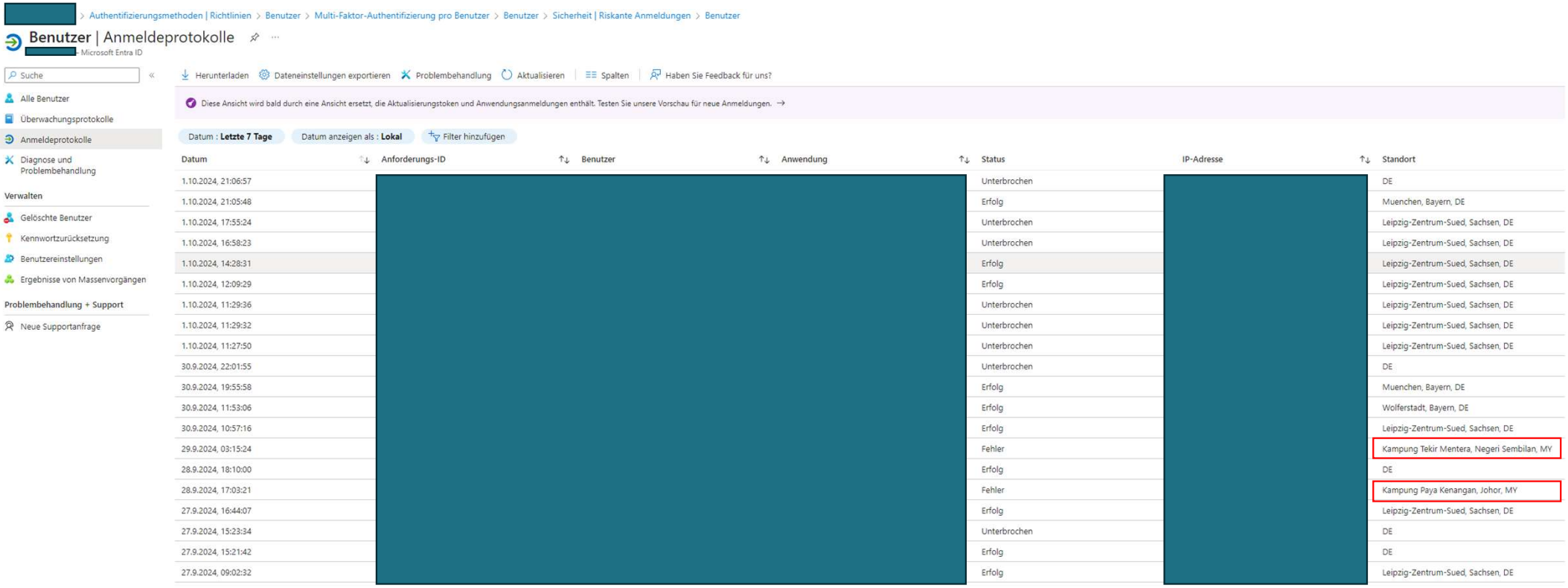
DOKUMENT: AW240098

DATUM: Donnerstag, 3. Oktober 2024

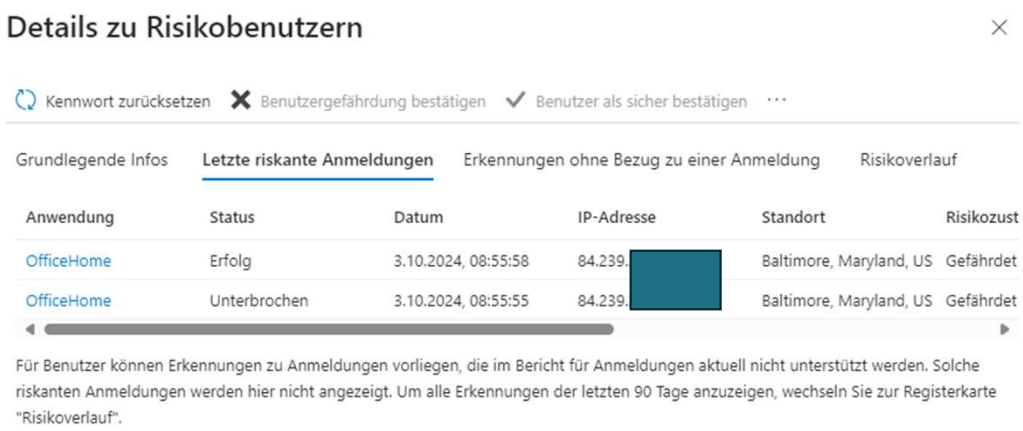
Eine PDF-Datei des Dokuments finden Sie im Scan.

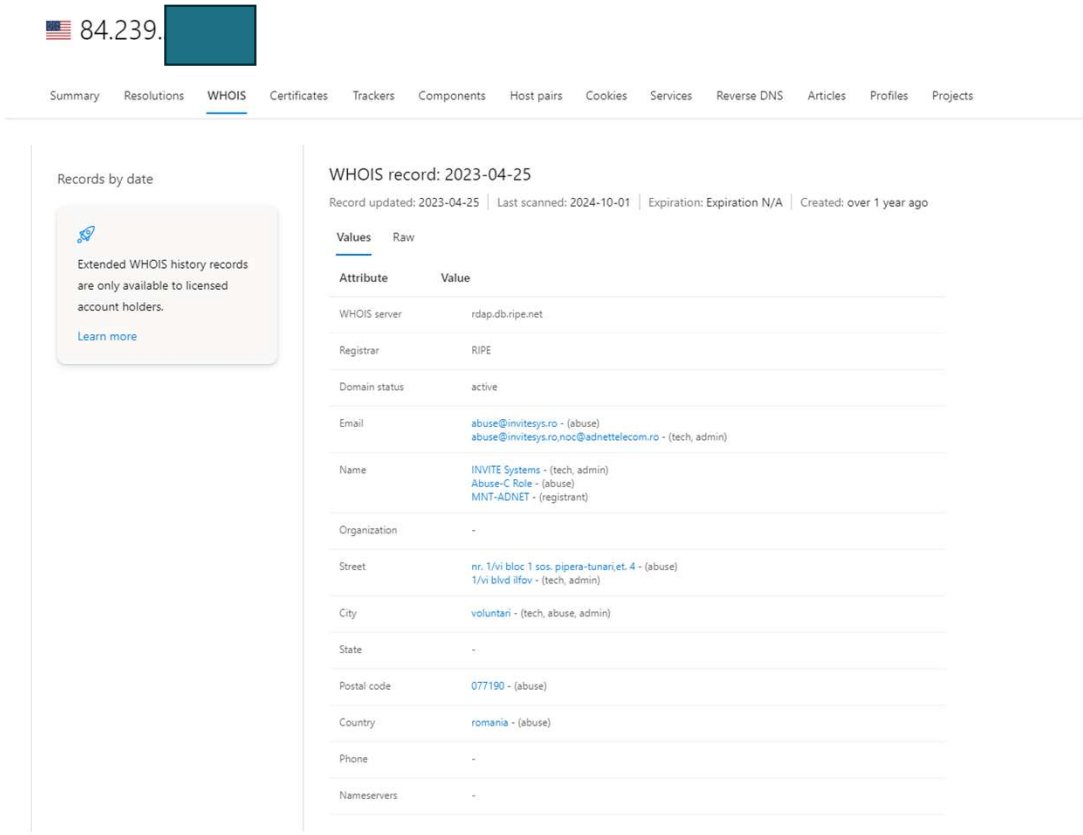
DOKUMENT ANZEIGEN

Das Problem – Erste Login-Versuche



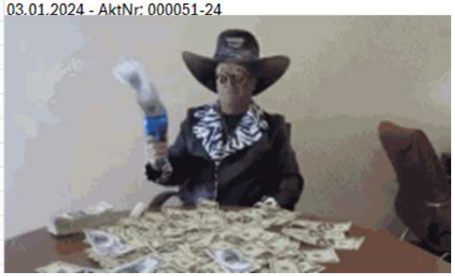
Das Problem – Treffer!





Das Problem – Feuer frei! (ca. 250.000 Mails…)

MessageId	Received	SenderAddress	RecipientAddress	Subject
<A03E390D-FD67-45E7-B503-B333A4B95C14@	03.10.2024 10:17		b	03.01.2024 - AktNr: 000051-24
<A03E390D-FD67-45E7-B503-B333A4B95C14@	03.10.2024 10:17		'-	03.01.2024 - AktNr: 000051-24
<A03E390D-FD67-45E7-B503-B333A4B95C14@	03.10.2024 10:17		k	03.01.2024 - AktNr: 000051-24
<A03E390D-FD67-45E7-B503-B333A4B95C14@	03.10.2024 10:17		g	03.01.2024 - AktNr: 000051-24
<A03E390D-FD67-45E7-B503-B333A4B95C14@	03.10.2024 10:17		g	03.01.2024 - AktNr: 000051-24
<A03E390D-FD67-45E7-B503-B333A4B95C14@	03.10.2024 10:17		m	03.01.2024 - AktNr: 000051-24
<A03E390D-FD67-45E7-B503-B333A4B95C14@	03.10.2024 10:17		j.	03.01.2024 - AktNr: 000051-24
<A03E390D-FD67-45E7-B503-B333A4B95C14@	03.10.2024 10:17		t	03.01.2024 - AktNr: 000051-24
<A03E390D-FD67-45E7-B503-B333A4B95C14@	03.10.2024 10:17		u	03.01.2024 - AktNr: 000051-24
<A03E390D-FD67-45E7-B503-B333A4B95C14@	03.10.2024 10:17		s	03.01.2024 - AktNr: 000051-24
<A03E390D-FD67-45E7-B503-B333A4B95C14@	03.10.2024 10:17		d	03.01.2024 - AktNr: 000051-24
<A03E390D-FD67-45E7-B503-B333A4B95C14@	03.10.2024 10:17		s	03.01.2024 - AktNr: 000051-24
<A03E390D-FD67-45E7-B503-B333A4B95C14@	03.10.2024 10:17		m	03.01.2024 - AktNr: 000051-24
<A03E390D-FD67-45E7-B503-B333A4B95C14@	03.10.2024 10:17		r	03.01.2024 - AktNr: 000051-24
<A03E390D-FD67-45E7-B503-B333A4B95C14@	03.10.2024 10:17		c	03.01.2024 - AktNr: 000051-24
<3808D010-CA09-4258-AC7E-1F1E777F0874@r	03.10.2024 10:17		m	03.01.2024 - AktNr: 000051-24
<3808D010-CA09-4258-AC7E-1F1E777F0874@r	03.10.2024 10:17		c	03.01.2024 - AktNr: 000051-24
<3808D010-CA09-4258-AC7E-1F1E777F0874@r	03.10.2024 10:17		k	03.01.2024 - AktNr: 000051-24
<3808D010-CA09-4258-AC7E-1F1E777F0874@r	03.10.2024 10:17		in	03.01.2024 - AktNr: 000051-24
<3808D010-CA09-4258-AC7E-1F1E777F0874@r	03.10.2024 10:17		in	03.01.2024 - AktNr: 000051-24
<3808D010-CA09-4258-AC7E-1F1E777F0874@r	03.10.2024 10:17		k	03.01.2024 - AktNr: 000051-24
<3808D010-CA09-4258-AC7E-1F1E777F0874@r	03.10.2024 10:17		a	03.01.2024 - AktNr: 000051-24
<3808D010-CA09-4258-AC7E-1F1E777F0874@r	03.10.2024 10:17		n	03.01.2024 - AktNr: 000051-24
<3808D010-CA09-4258-AC7E-1F1E777F0874@r	03.10.2024 10:17		in	03.01.2024 - AktNr: 000051-24
<3808D010-CA09-4258-AC7E-1F1E777F0874@r	03.10.2024 10:17		h	03.01.2024 - AktNr: 000051-24
<3808D010-CA09-4258-AC7E-1F1E777F0874@r	03.10.2024 10:17		n	03.01.2024 - AktNr: 000051-24
<3808D010-CA09-4258-AC7E-1F1E777F0874@r	03.10.2024 10:17		h	03.01.2024 - AktNr: 000051-24
<3808D010-CA09-4258-AC7E-1F1E777F0874@r	03.10.2024 10:17		a	03.01.2024 - AktNr: 000051-24
<3808D010-CA09-4258-AC7E-1F1E777F0874@r	03.10.2024 10:17		js	
<3808D010-CA09-4258-AC7E-1F1E777F0874@r	03.10.2024 10:17		d	
<3808D010-CA09-4258-AC7E-1F1E777F0874@r	03.10.2024 10:17		h	
<3808D010-CA09-4258-AC7E-1F1E777F0874@r	03.10.2024 10:17		e	
<3808D010-CA09-4258-AC7E-1F1E777F0874@r	03.10.2024 10:17		s	
<3808D010-CA09-4258-AC7E-1F1E777F0874@r	03.10.2024 10:17		c	
<3808D010-CA09-4258-AC7E-1F1E777F0874@r	03.10.2024 10:17		fa	
<3808D010-CA09-4258-AC7E-1F1E777F0874@r	03.10.2024 10:17		t	
<3808D010-CA09-4258-AC7E-1F1E777F0874@r	03.10.2024 10:17		jo	
<3808D010-CA09-4258-AC7E-1F1E777F0874@r	03.10.2024 10:17		m	



Red Flags – everywhere!

Eine PDF-Datei des Dokuments finden Sie im Scan.

DOKUMENT ANZEIGEN

03.01.2024 - AktNr: 000051-24.pdf

OneDrive Document - Microsoft OneDrive

Zeigen Sie Dokumente und Anhänge mit OneDrive Document im Web an, organisieren und teilen Sie sie. Änderungen werden auf Ihren Geräten mit Microsoft synchronisiert.

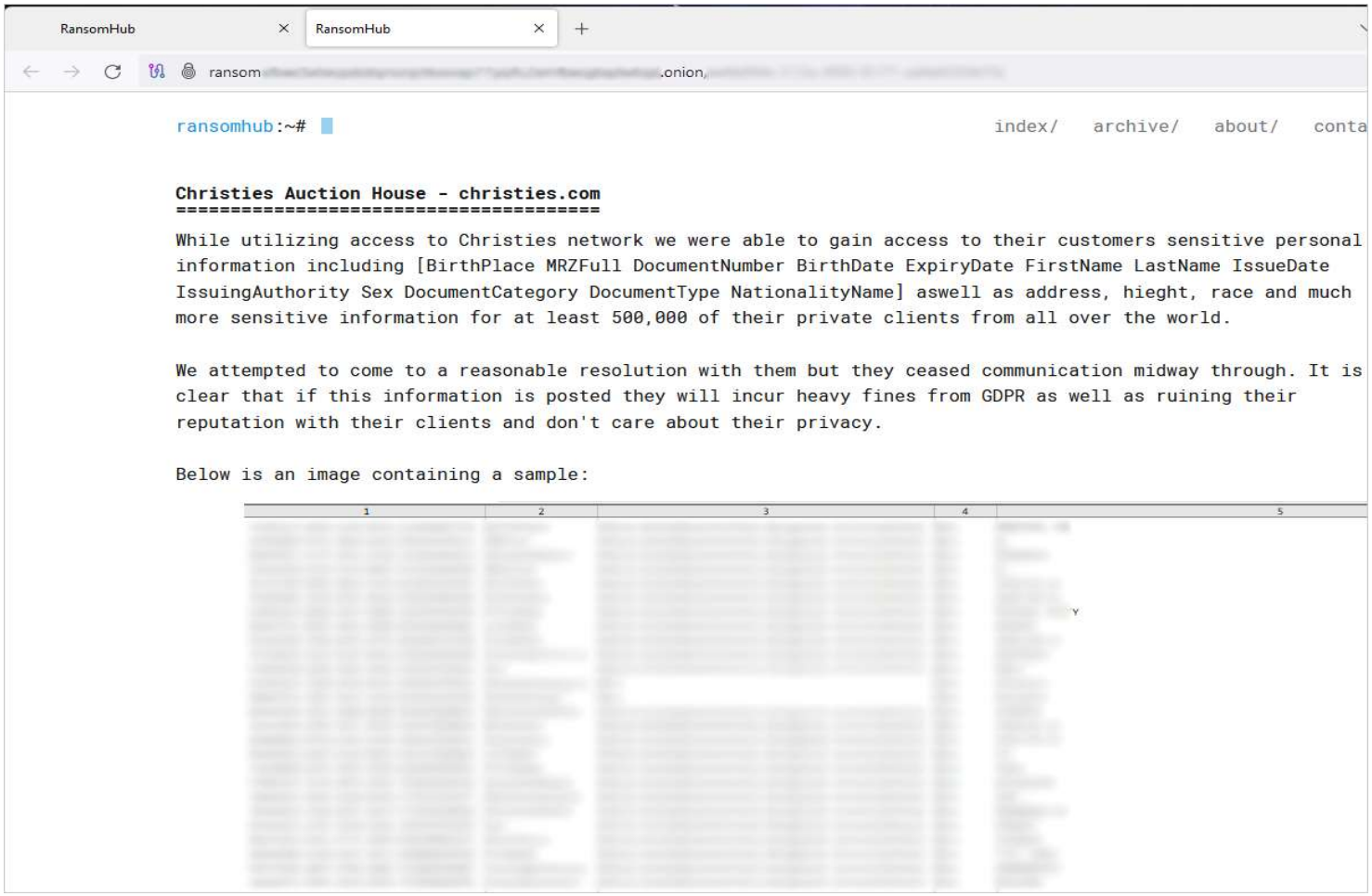
share.microsoft.com

https://www.canva.com/link?target=https://xzl5ivdazwobdg6qmgjvaqcpwbgzcdsuwpqt3rzwsgejp

pegasus IT
Member of ITventive Group

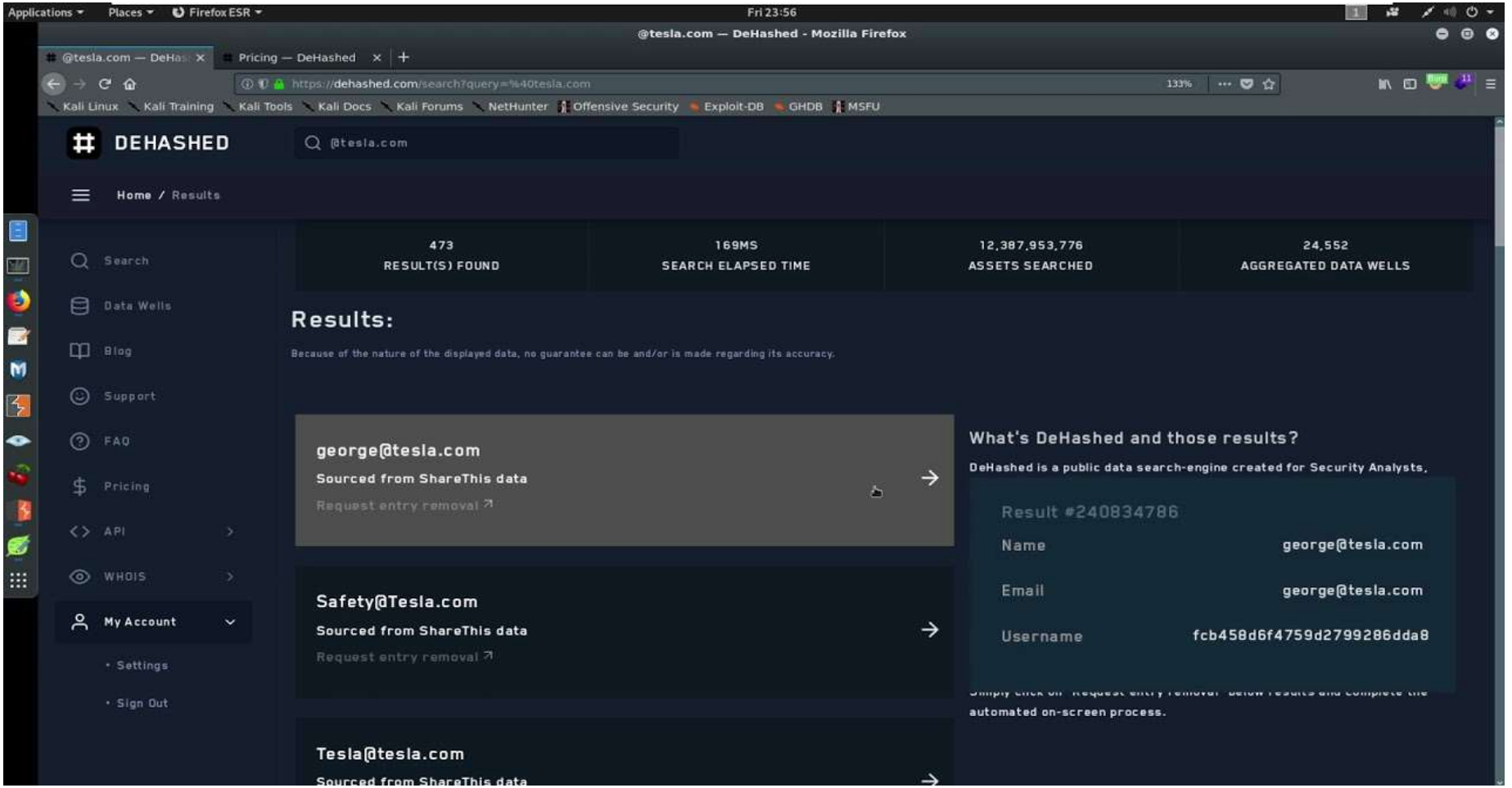
„Wie machen die Angreifer das?“

This is how they do it! Also, so oder so ähnlich ;)



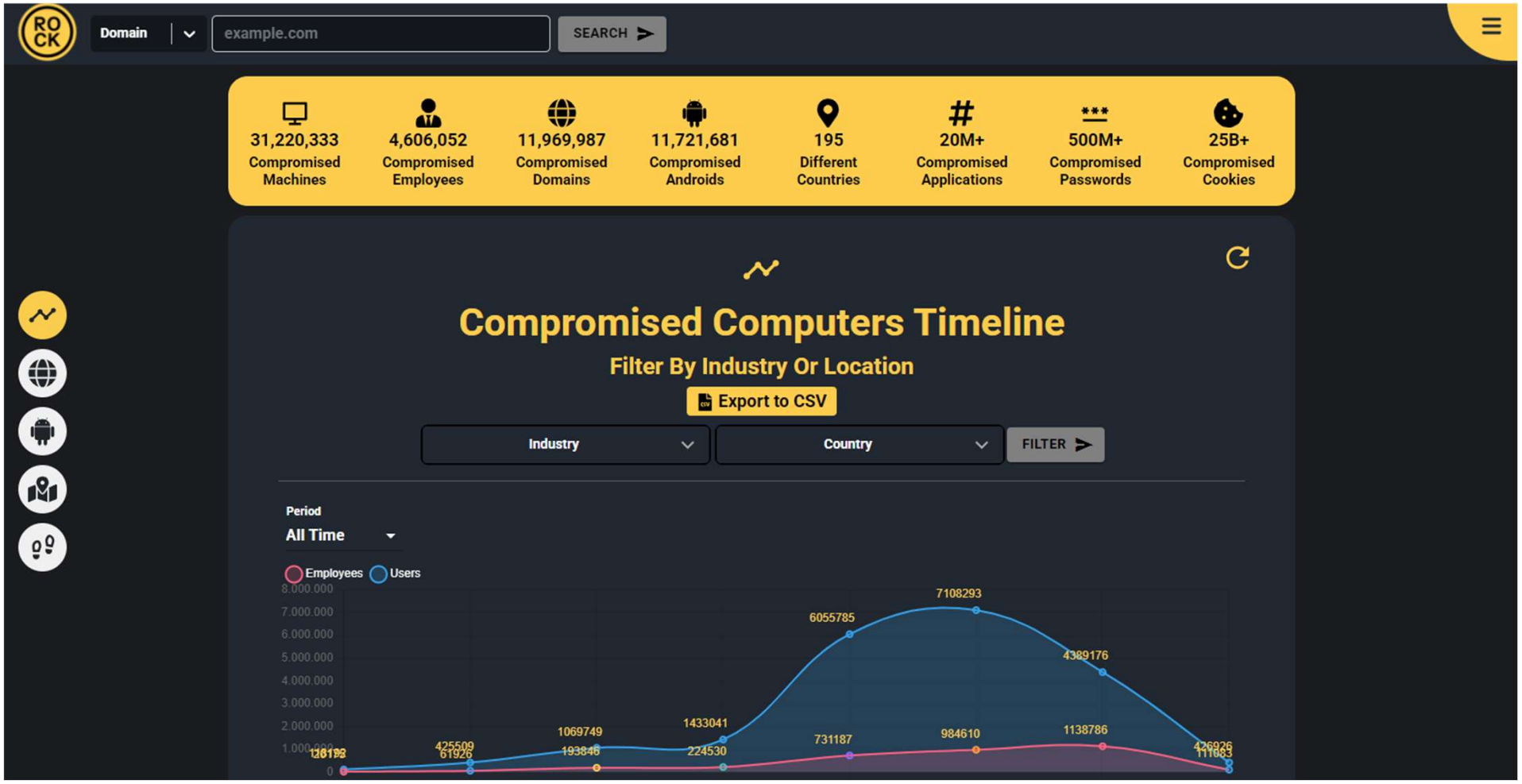
Quelle: RansomHub

This is how they do it! Also, so oder so ähnlich ;)



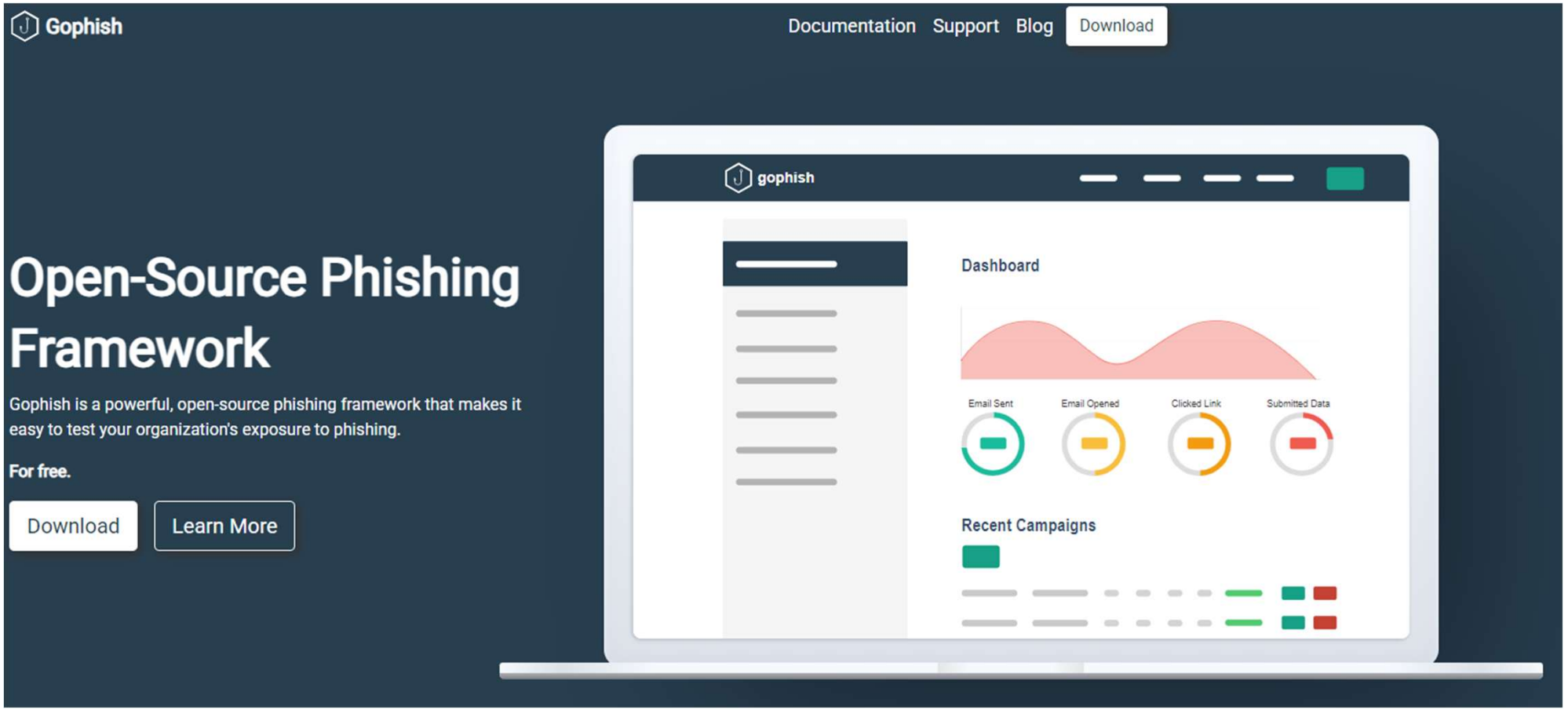
Quelle: DeHashed

This is how they do it! Also, so oder so ähnlich ;)



Quelle: Hudson Rock

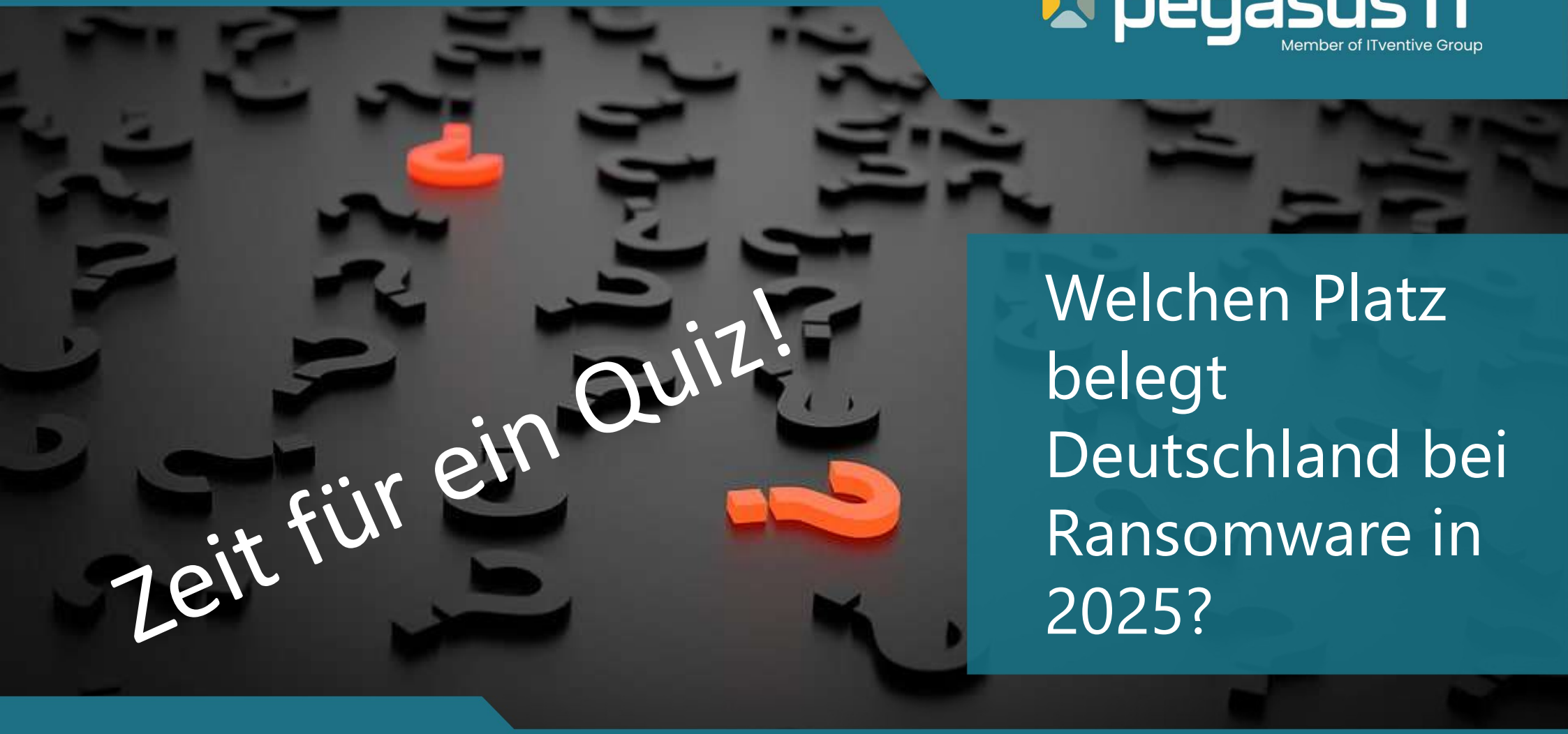
This is how they do it! Also, so oder so ähnlich ;)



Quelle: Gophish

pegasus IT
Member of ITventive Group

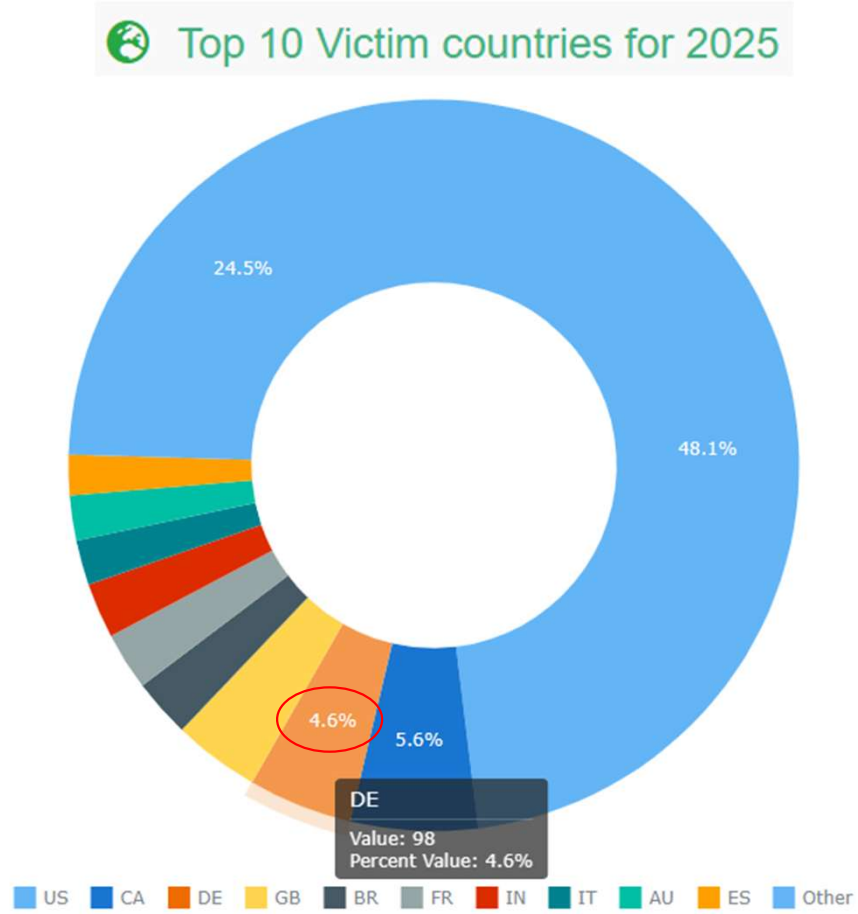
Demo Gophish



pegasus IT
Member of ITventive Group

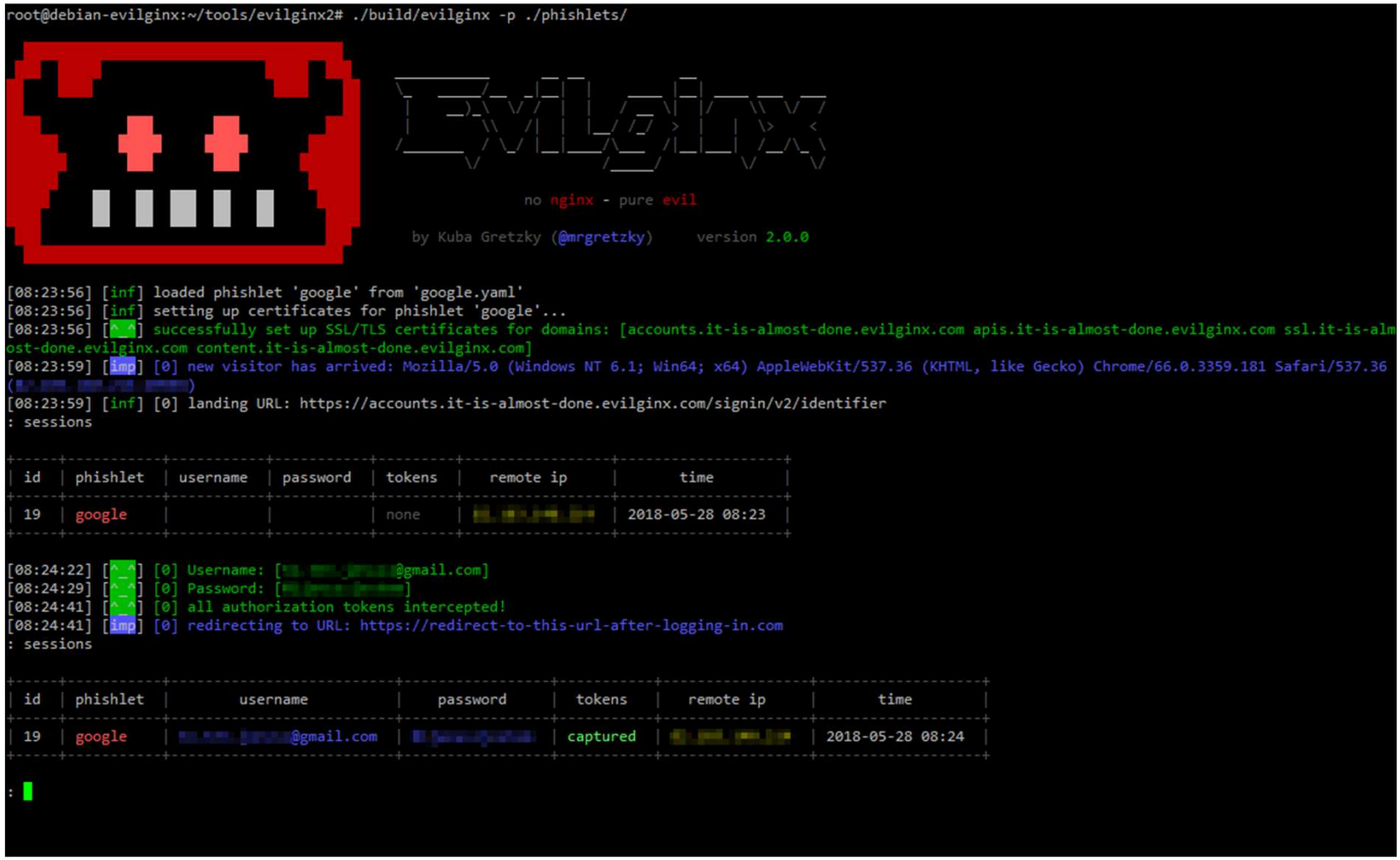
Welchen Platz belegt Deutschland bei Ransomware in 2025?

Welchen Platz belegt Deutschland bei Ransomware in 2025?



Quelle: ransomware.live

This is how they do it! Also, so oder so ähnlich ;)



Quelle: Evilginx

This is how they do it!

Evilginx 3.0

Evilginx is a man-in-the-middle attack framework used for phishing login credentials along with session cookies, which in turn allows to bypass 2-factor authentication protection.

This tool is a successor to Evilginx, released in 2017, which used a custom version of nginx HTTP server to provide man-in-the-middle functionality to act as a proxy between a browser and phished website. Present version is fully written in GO as a standalone application, which implements its own HTTP and DNS server, making it extremely easy to set up and use.

https://github.com/kgretzky/evilginx2

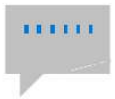
Quelle: Evilginx

„Aber wir haben doch MFA?“

Bad: Password

123456
Qwertz
password
P@ssw0rd
iloveyou
Sars-Cov-2
Covid-19

Good: Password +



SMS

Voice

Better: Password +

Push Notification

Soft Tokens OTP

Hard Tokens OTP

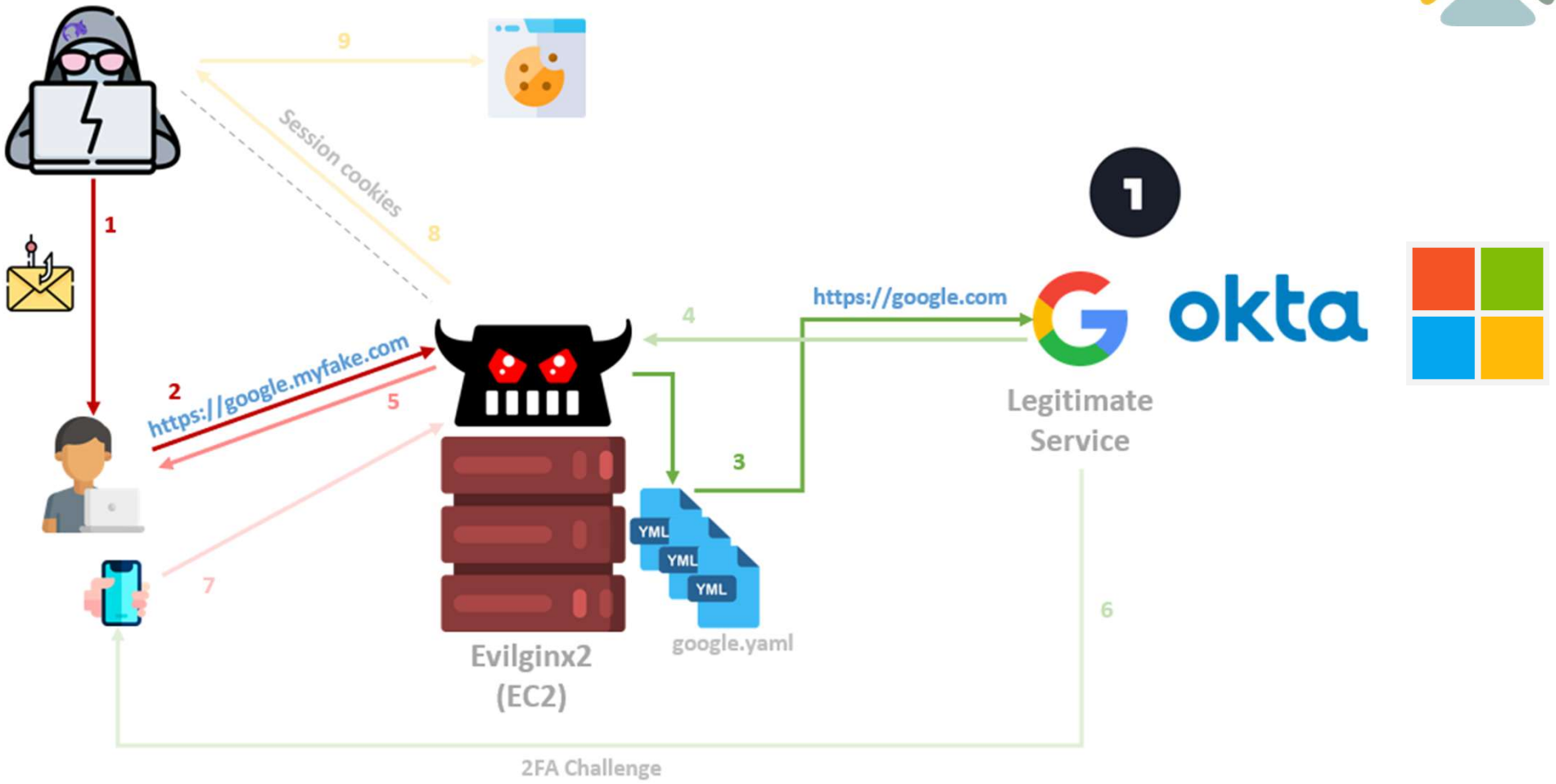
Best:

Microsoft Authenticator

Windows Hello

FIDO2 Security key

Technische Details



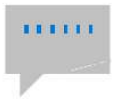
Quelle: Evilginx

„Aber wir haben doch MFA?“

Bad: Password

123456
Qwertz
password
P@ssw0rd
iloveyou
Sars-Cov-2
Covid-19

Good: Password +



SMS

Voice

Better: Password +

Push Notification

Soft Tokens OTP

Hard Tokens OTP

Best:

Microsoft Authenticator

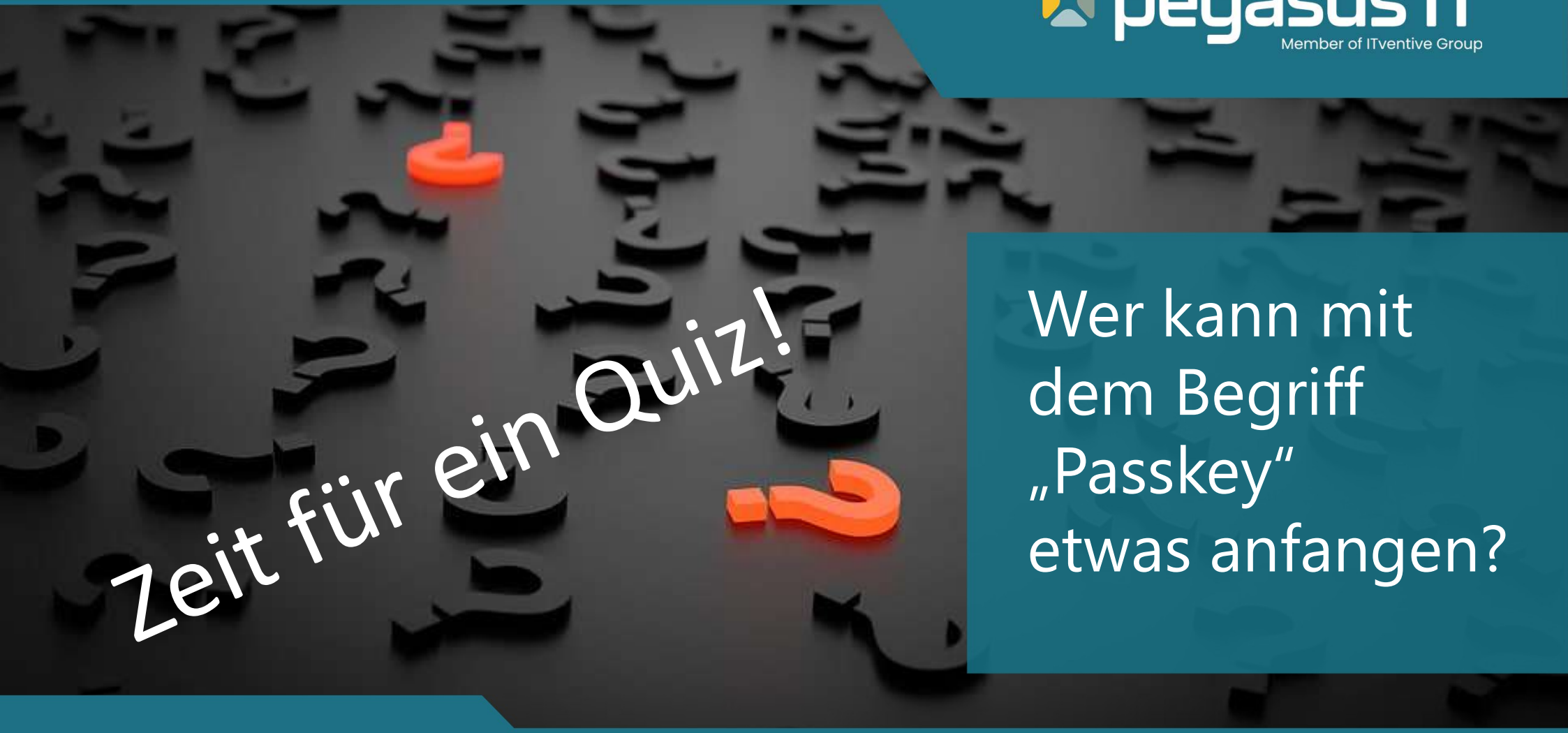
Windows Hello

FIDO2 Security key

Phishing-Resistant MFA!

pegasus IT
Member of ITventive Group

Demo
EvilGinx



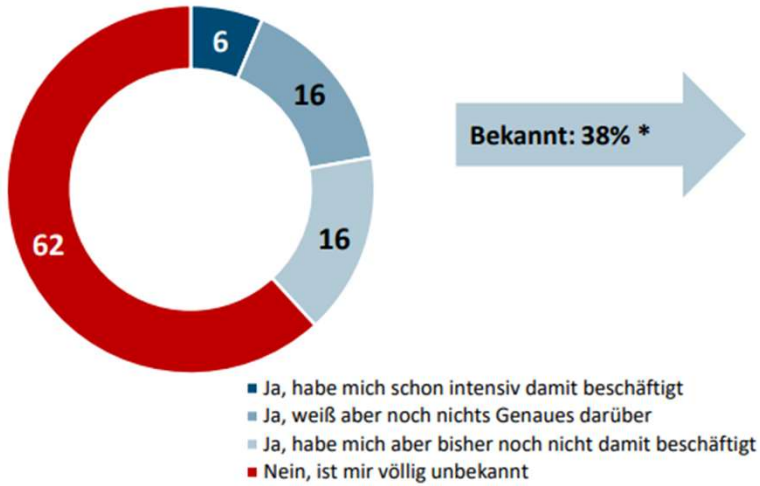
pegasus IT
Member of ITventive Group

Wer kann mit dem Begriff „Passkey“ etwas anfangen?

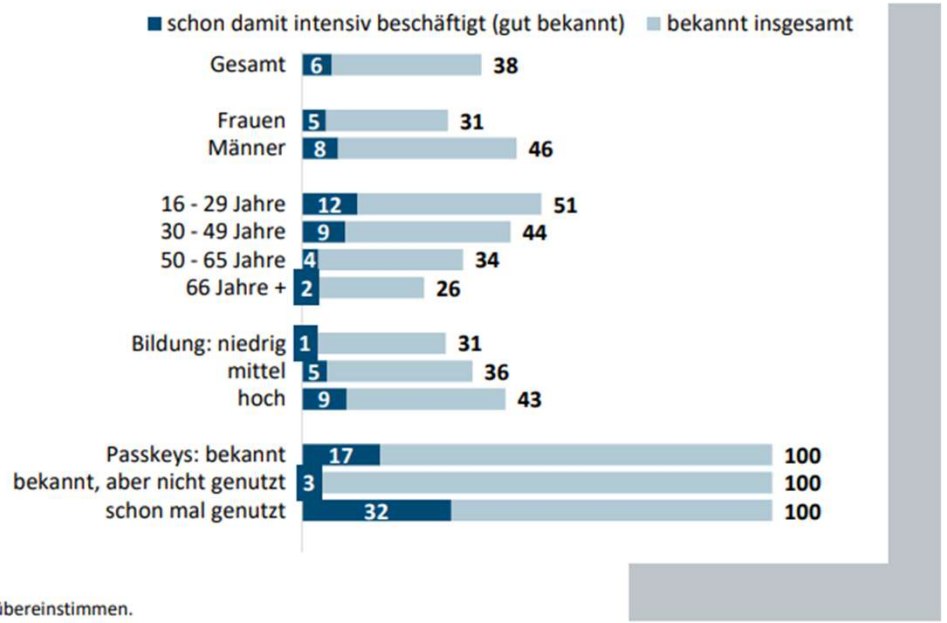
Wer kann mit dem Begriff „Passkey“ etwas anfangen?

Passkeys: Gestützte Bekanntheit (*nach Beschreibung*)

Über einem Drittel ist Passkeys zumindest vom Begriff her bekannt. Von den Passkeys-Nutzenden hat sich die überwiegende Mehrheit noch nicht intensiv damit beschäftigt.



Bekannt: 38% *



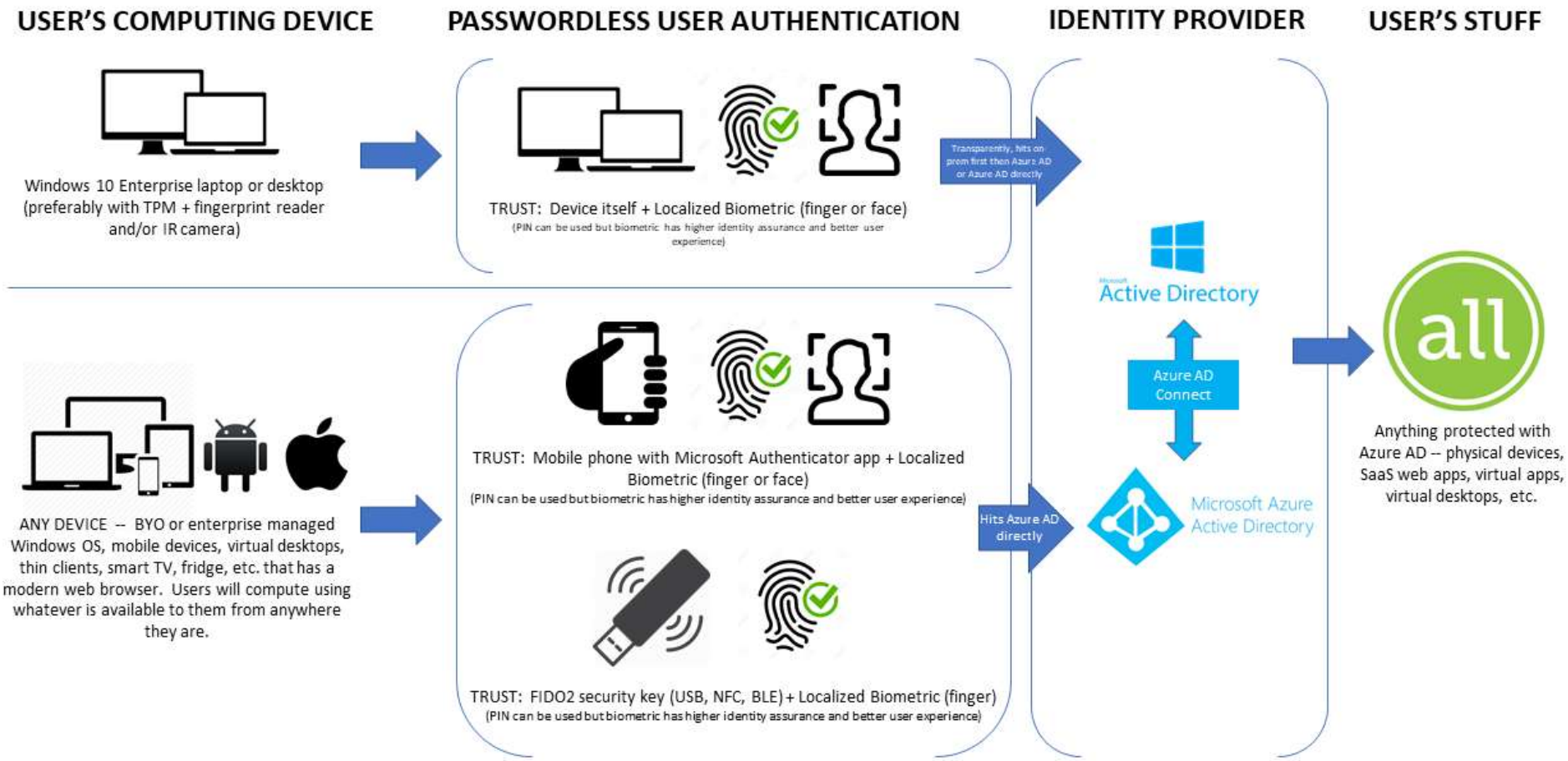
PK2. Kennen Sie diese Möglichkeit, sich mit Passkeys bei Online-Diensten und deren Apps anzumelden?
Basis: Gesamt n= 1.519 | Angaben in %, * Die Selbsteinschätzung wird evtl. nicht mit den realen Anteilen übereinstimmen.

Bundesamt für Sicherheit in der Informationstechnik

Deutschland Digital•Sicher•BSI•

Quelle: BSI

Passkeys / Hardware-Based Authentication

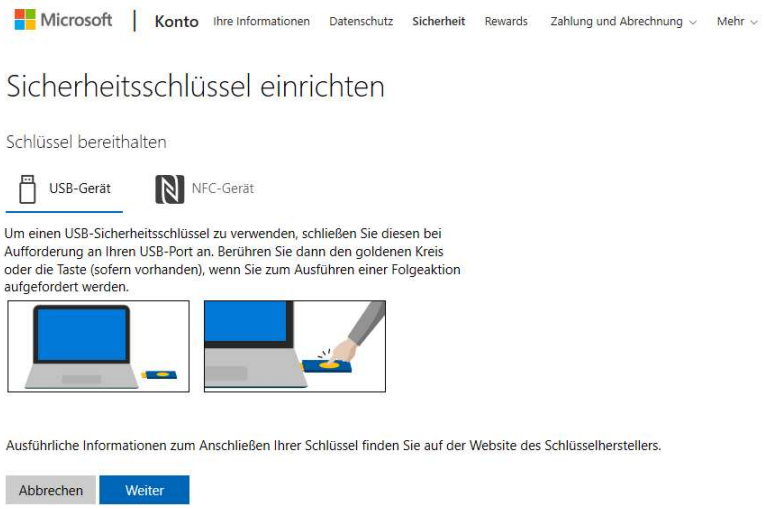


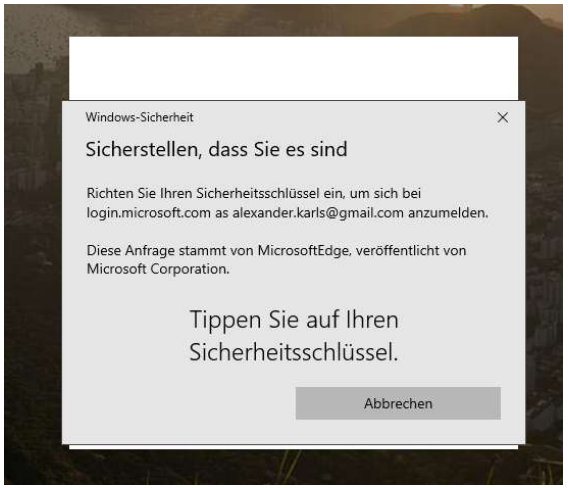
Quelle: FIDO Alliance

Token-Hardware (Bsp. Yubikey)

Quelle: Yubikey

Token-Hardware (Bsp. Yubikey)





Quelle: Yubico

Weitere Anwendungsfälle

Use cases:

- 2FA für Bitlocker (PIN + statischer Key)

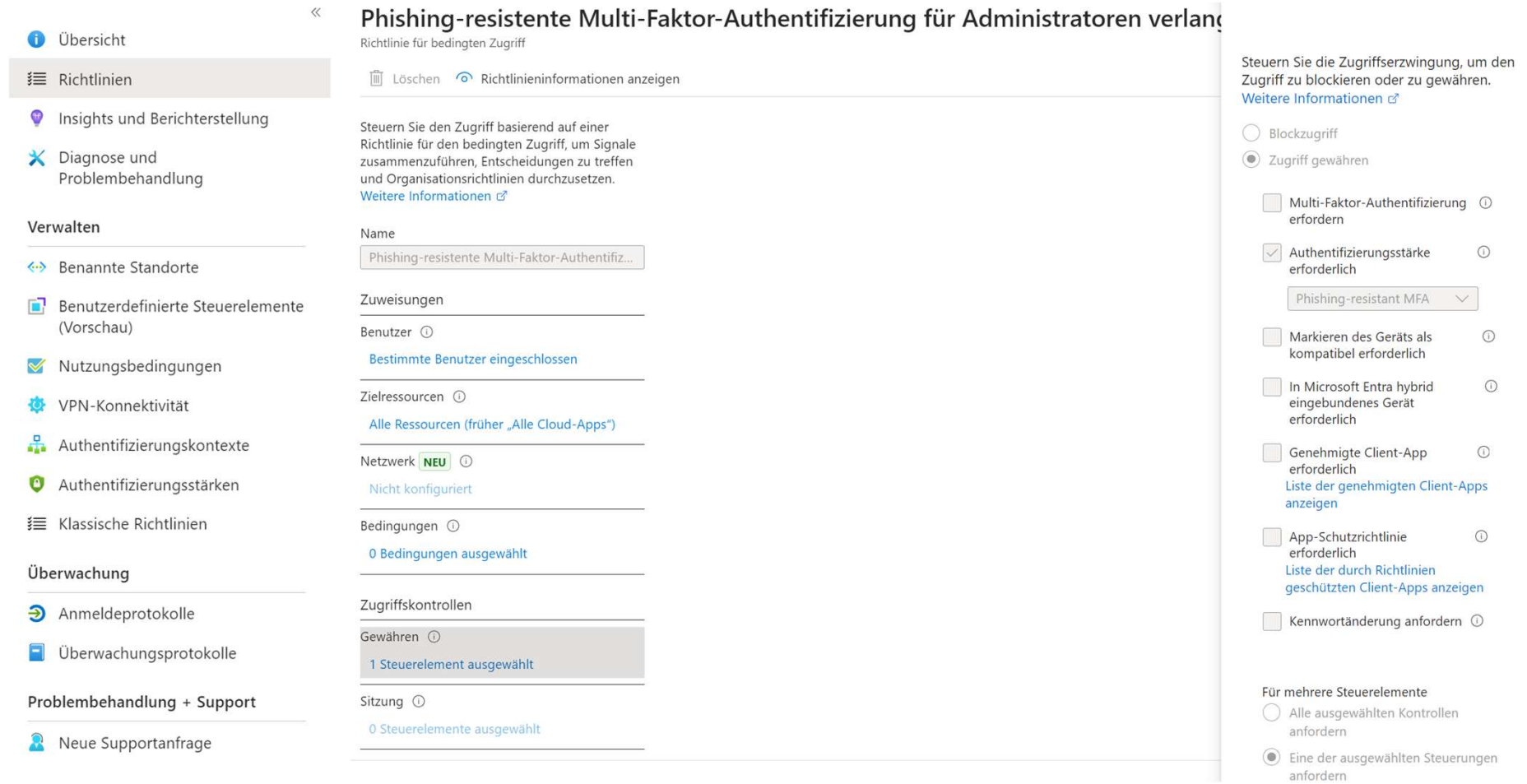
- Smart Card mit Domänen-Zertifikat + PIN zur Domänen-Anmeldung (wahlweise mit eigener PKI / CA oder öffentlicher CA)

- Authentifizierung / MFA-Absicherung geschäftlicher Cloud Accounts wie z.B. Microsoft Office 365, Azure, AWS, GitHub, Citrix..

- Authentifizierung / MFA-Absicherung privater Cloud Accounts wie z.B. G Suite, Facebook, Dropbox, KeePass, EA Online, Instagram..

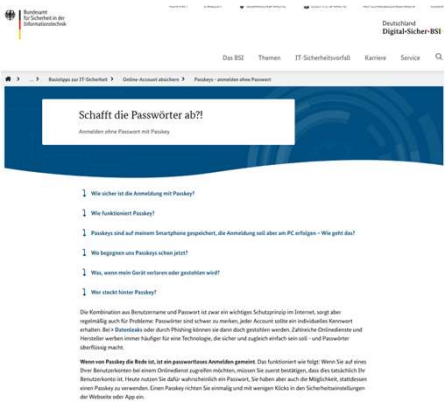
(Alle Services siehe > https://www.yubico.com/works-with-yubikey)

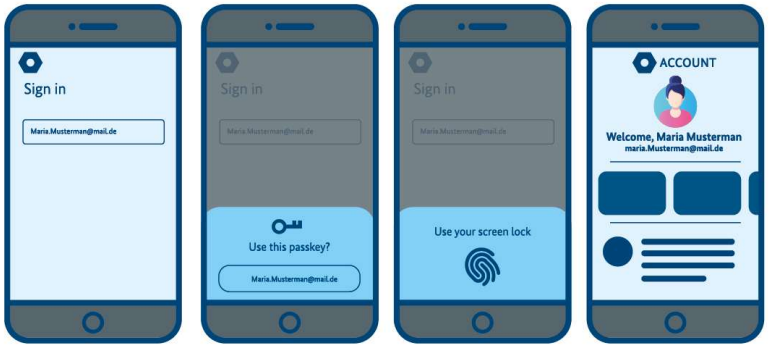
On-Top-Enforcement: Zero Trust (Conditional Access)

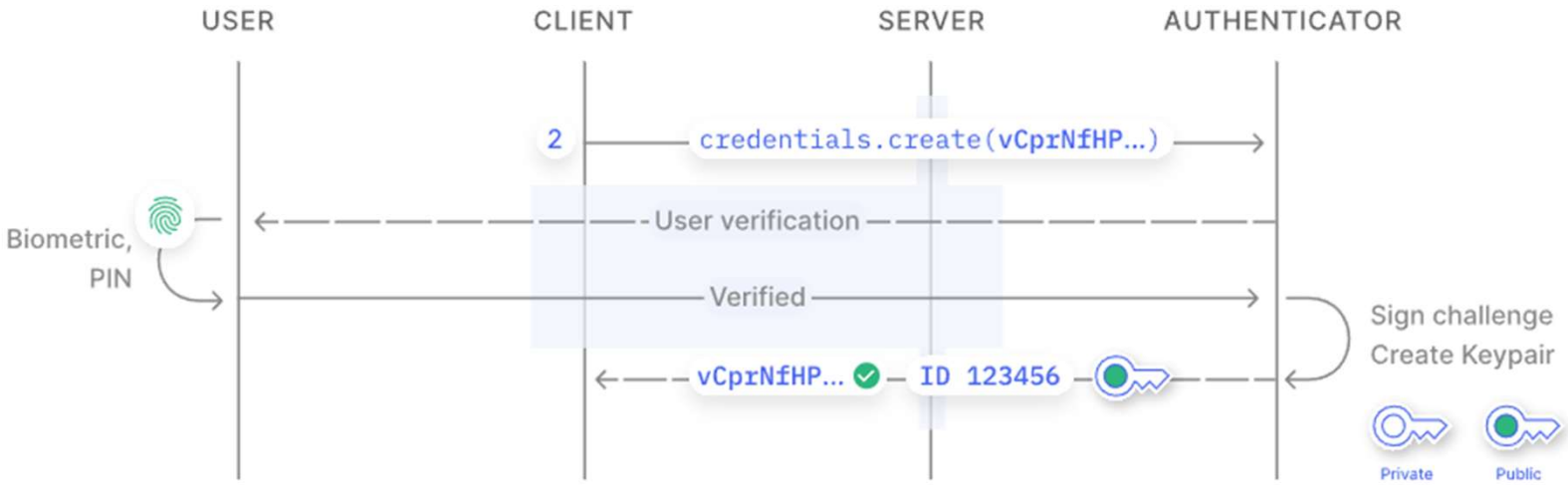


Quelle: Microsoft

„Was ist mit Passkeys auf dem Smartphone?“

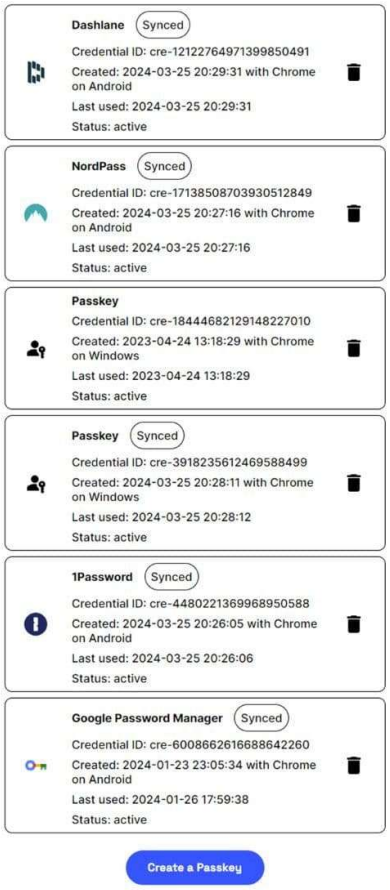






Quelle: BSI

„Was ist mit Passkeys auf dem Smartphone?“

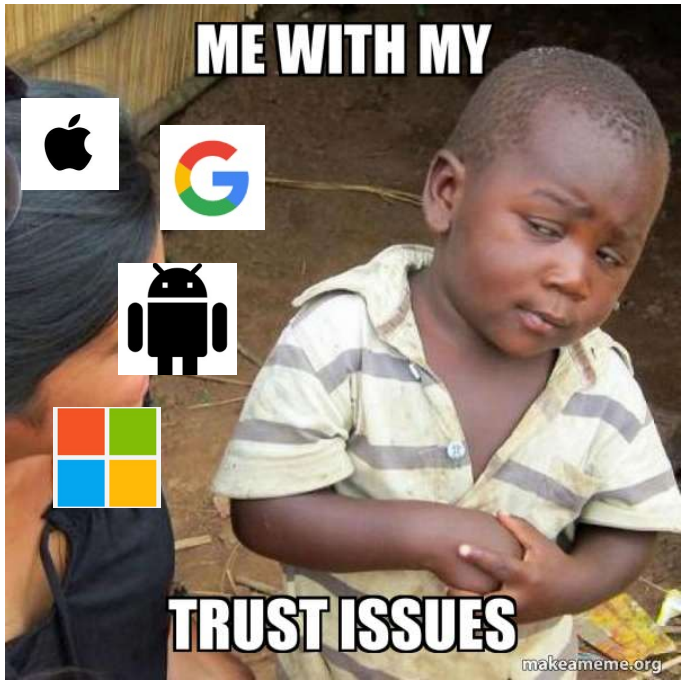


	Android 14	iOS 17.4	Web (Windows 11 + Chrome Extension)
First-Party Passkey Provider			
Apple iCloud Keychain	No	Yes	Yes
Google Password Manager	Yes	No	Yes
Windows Hello	No	No	Yes
Third-Party Passkey Provider			
1Password	Yes	Yes	Yes
Bitwarden	No	No?	Yes
Dashlane	Yes	Yes	Yes
Enpass	Yes	Yes	Yes (requires running desktop app in the background)
Keeper	Yes	Yes	Yes
KeePassXC	n/a	n/a	Yes
LastPass	No	No	No
Nordpass	Yes	Yes	Yes
Proton	Yes	Yes	Yes
Samsung Pass	Yes	n/a	n/a (error message)

Quelle: FIDO Alliance

„Was ist mit Passkeys im Browser?“

„Trau, schau, wem!“



Quelle: Yubico

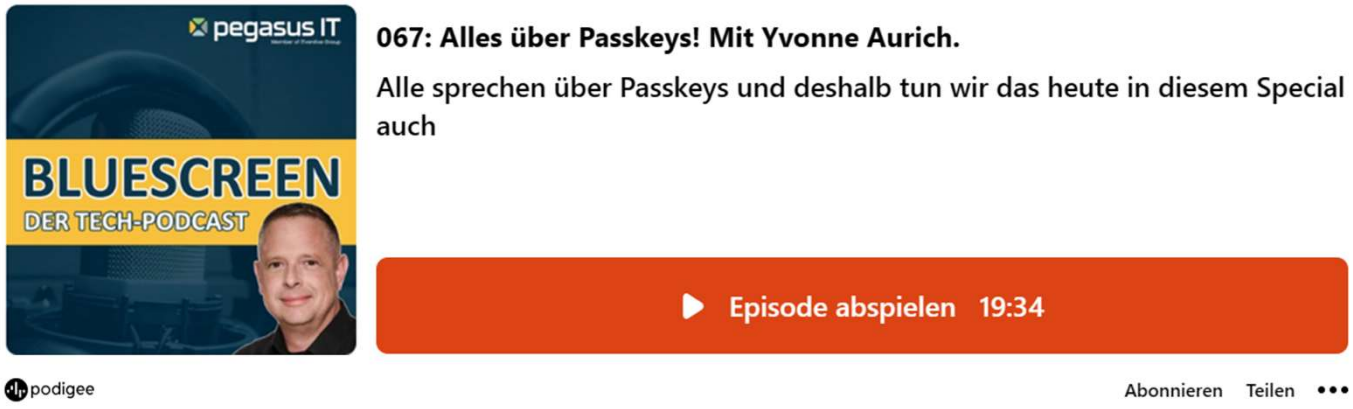
Unsere Social Media Kanäle

SOCIAL MEDIA KANÄLE DER PEGASUS IT

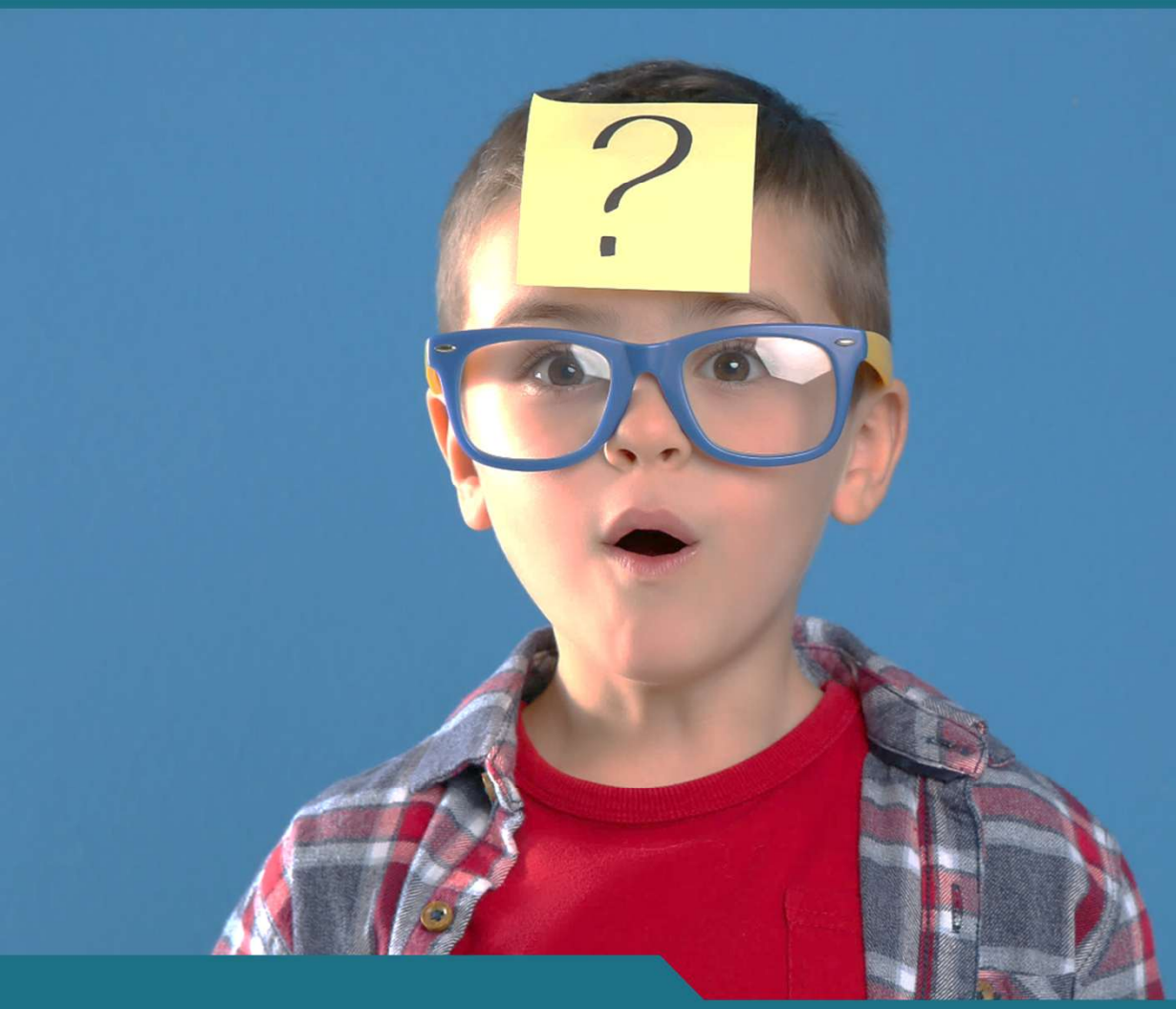
Auf unseren Social Media Kanälen veröffentlichen wir neueste Informationen zu aktuellen IT-Themen, innovativen Produkten sowie unseren pegasus Events. Zudem erhalten Sie immer wieder Einblicke in unsere Arbeit, Zusammenarbeit mit Partnern und Insights vom Team der pegasus.

Folgen Sie uns auf Facebook, Twitter, Xing & Co und bleiben stets uptodate rund um das Thema IT.

BLUESCREEN – UNSER TECH PODCAST



pegasus IT
Member of ITventive Group



Haben Sie Fragen oder Anregungen?

pegasus IT – Member of ITVentive Group

ITventive Group

eviatec Systems AG, Monreposstrasse 57, D-71634 Ludwigsburg
pegasus GmbH, Bayernstrasse 10, D-93128 Regenstauf
eviatec Digital Solutions AG, Uferweg 17, CH-3013 Bern
eviatec Scandinavia ApS, Park Alle 295, 2. floor, DK-2605 Brøndby

pegasus-gmbh.de