# Live-Hacking

# 30:00

*“Wir möchten heute nicht über Cyberangriffe reden.*
*Wir möchten einen durchführen.“*

PENTARIS SECURITY

# Cyber Defense Horizons –

“Full Circle: Wie Angreifer Ihre gesamte Infrastruktur sehen“

Sebastian Froede – Cyber Defense Horizons 2026 – 29.09.2026

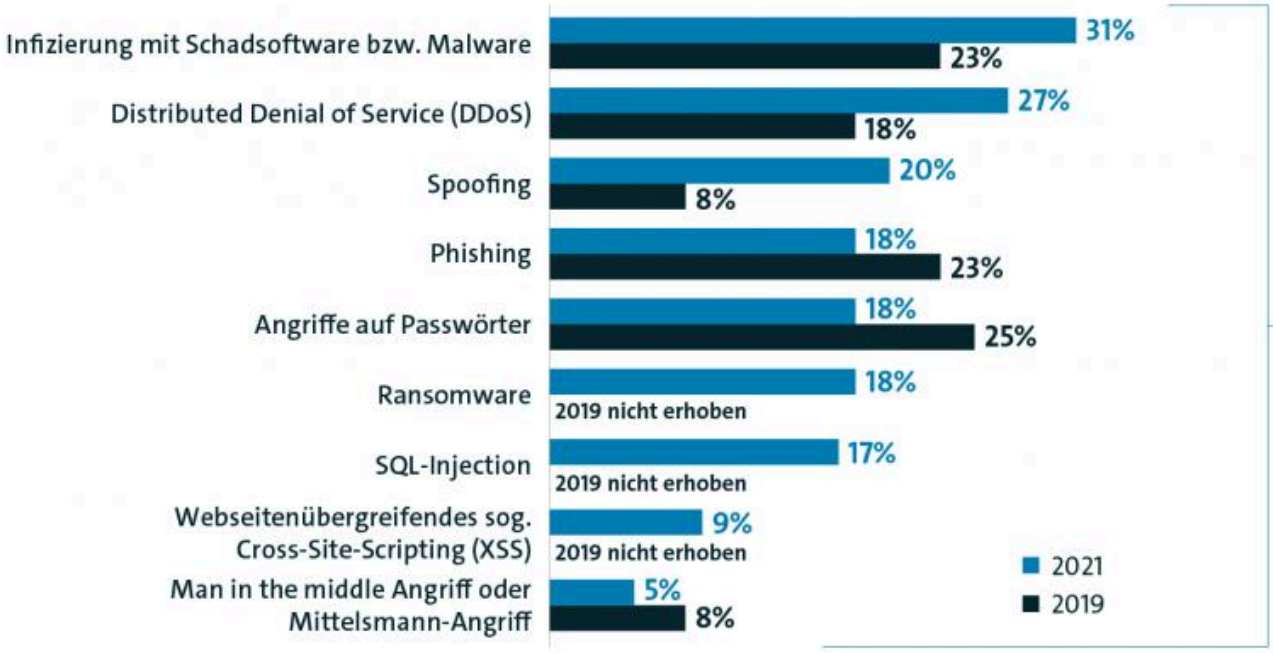
# IT-Crashtest



# Cyberangriffe

## Cyberangriffe betreffen nahezu 9 von 10 Unternehmen

Welche der folgenden Arten von Cyberangriffen haben innerhalb der letzten 12 Monaten in Ihrem Unternehmen einen Schaden verursacht?




Cyberangriffe haben bei

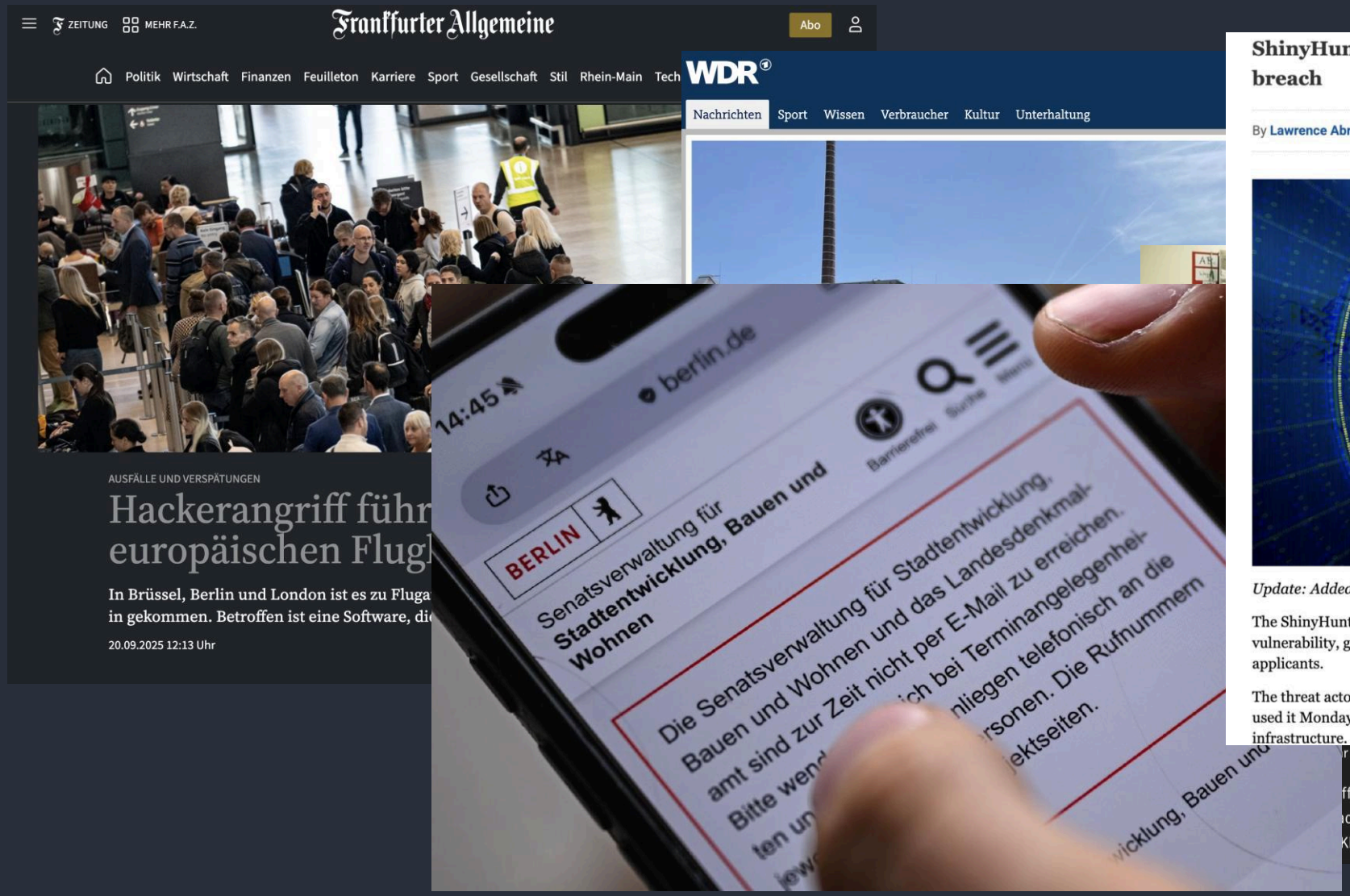
**86%**

der Unternehmen einen Schaden verursacht – **2019** waren es erst **70%**.

Basis: Alle befragten Unternehmen (2021: n=1.067; 2019: n=1.070); Mehrfachnennungen in Prozent, 2017 und 2019: innerhalb der letzten zwei Jahre
Quelle: Bitkom Research 2021

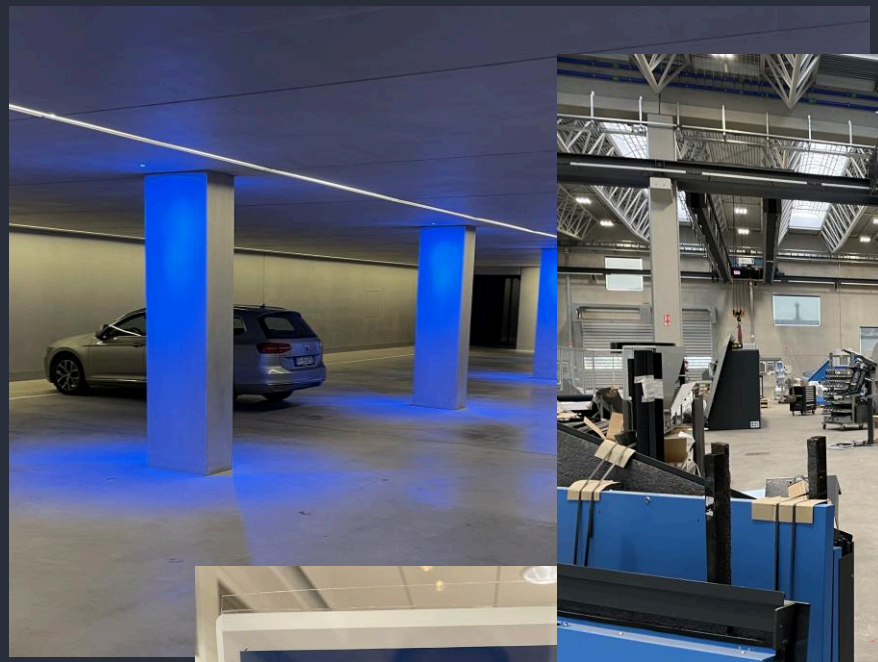
bitkom

# Mehr Cyberangriffe

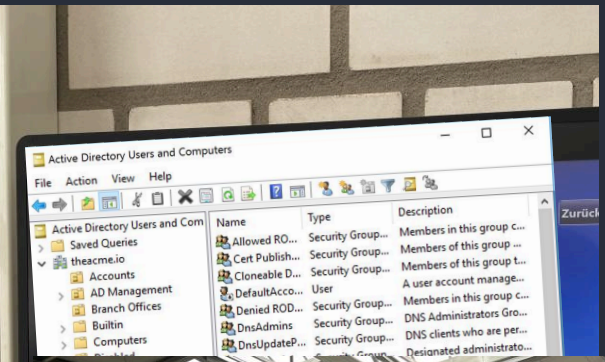





# Best Of Attack

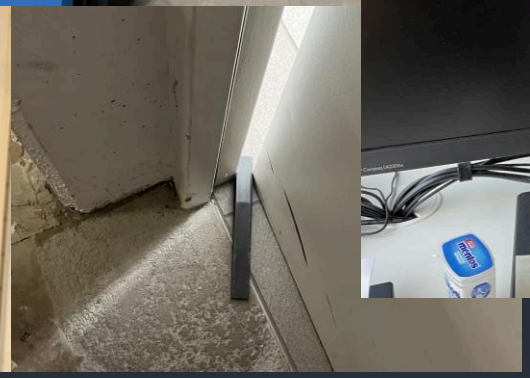


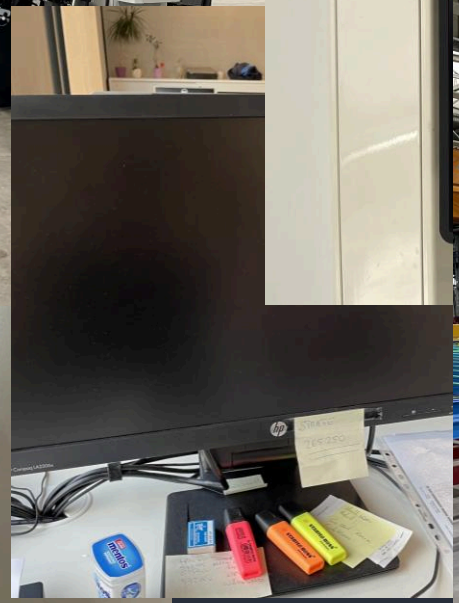














# Cyberangriffe

**OSINT**
Informationen aus öffentlichen Quellen sammeln.

**Vishing**
Anruf eines Support Mitarbeiters

**ScripT**
AutoIT Skript ausführen

**DatA-Upload**
Hochladen der Daten ins Darknet

**Phishing**
E-Mail mit maliziösem Link, QR-Code oder Anhang.

**Remote Support**
Installation Anydesk und Remotezugriff

**Cyber Angriff**
Datendiebstahl und Verschlüsselung

# Live-Hacking

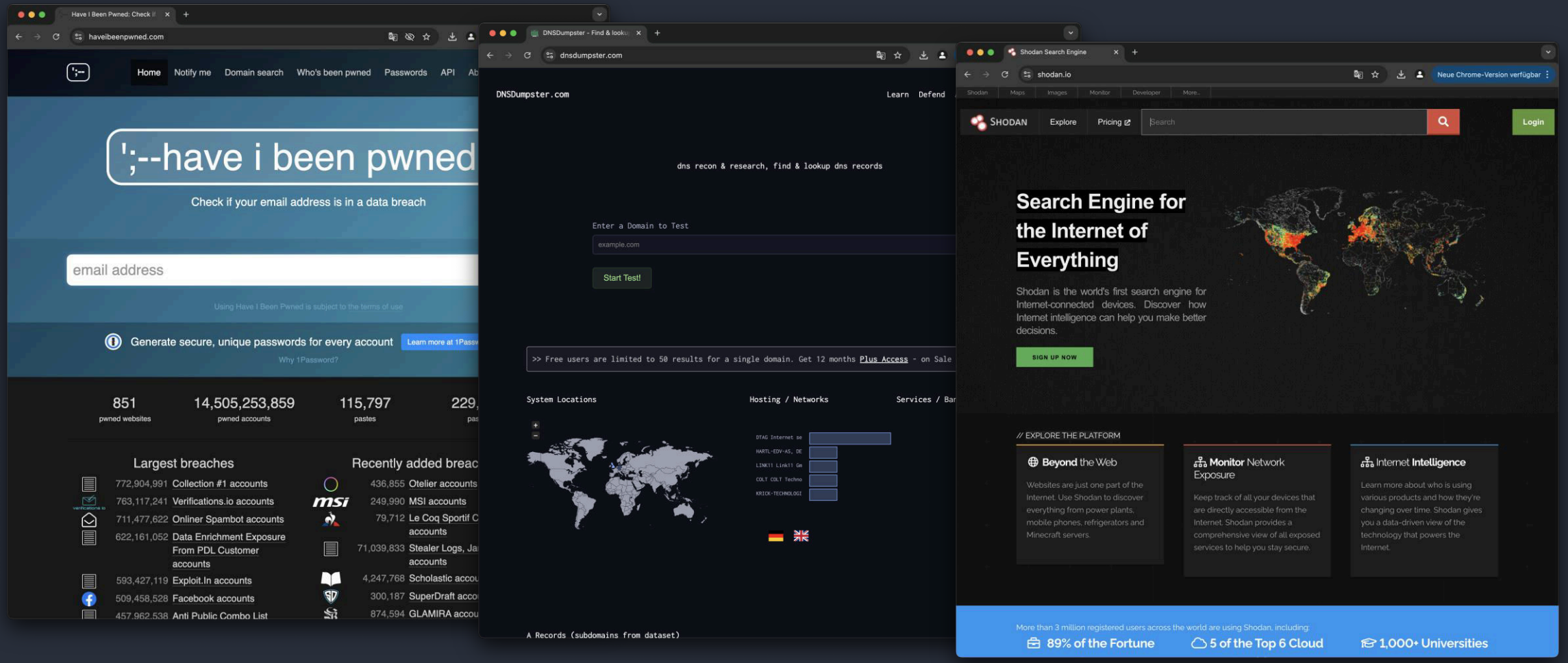


*„Würdest du ihn einstecken?“*

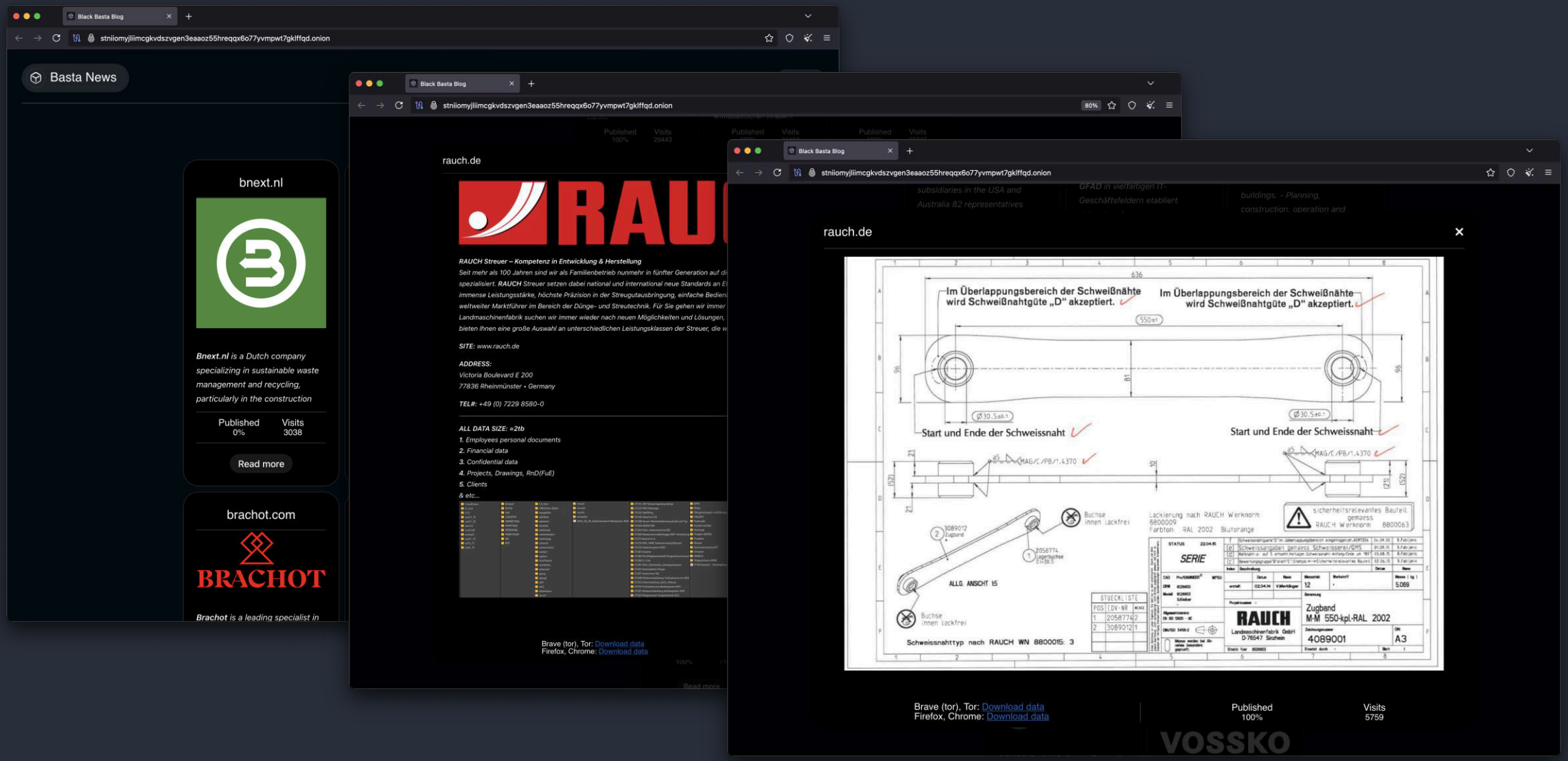
# Live-Hacking Regeln

- Keine Einzelperson
- Keine Behörde
- Hauptsitz D-A-CH

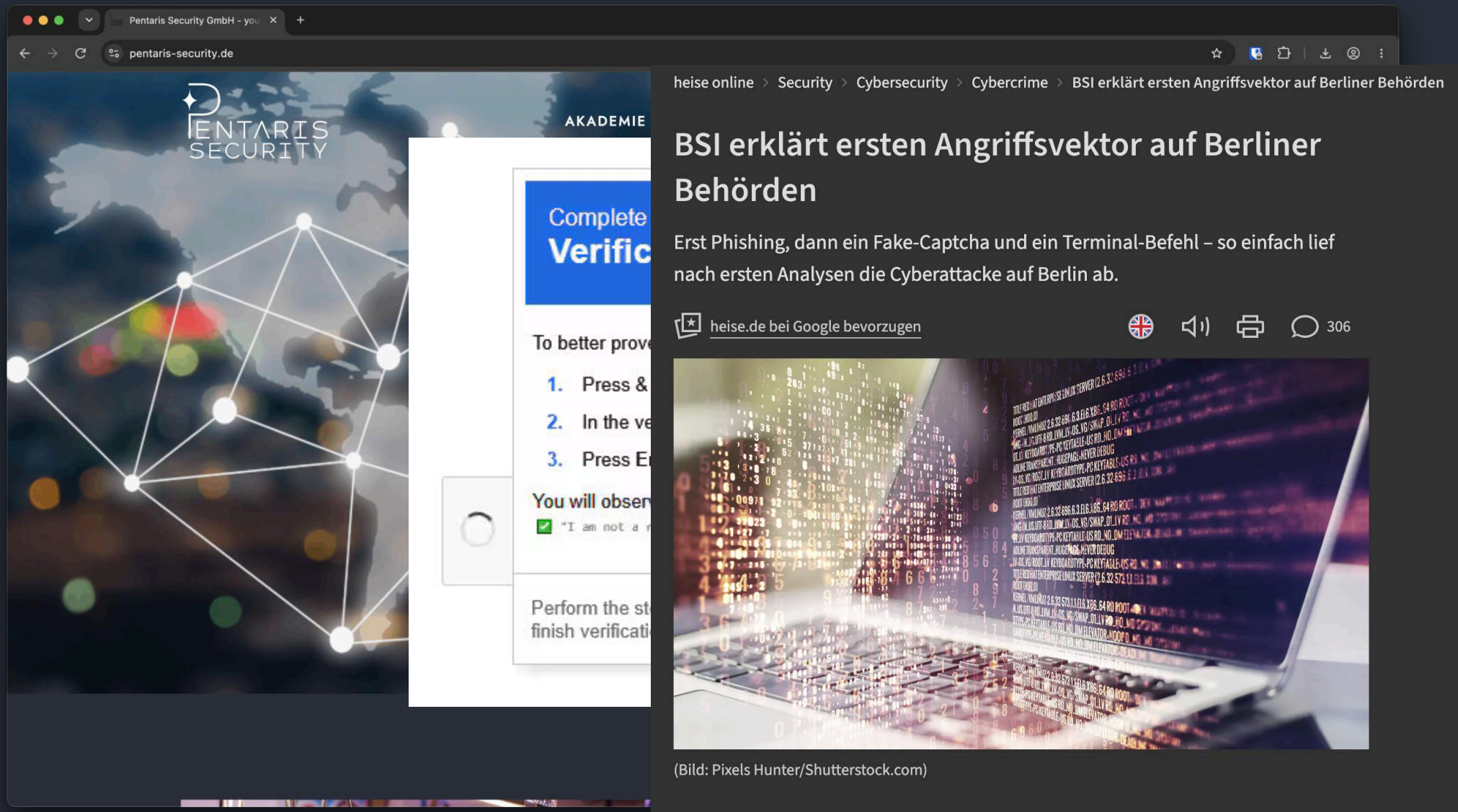
# OSINT


haveibeenpwned.com
Home
Notify me
Domain search
Who's been pwned
Passwords
API
';--have i been pwned
Check if your email address is in a data breach
email address
Generate secure, unique passwords for every account
851
pwned websites
14,505,253,859
pwned accounts
115,797
pastes
Largest breaches
772,904,991 Collection #1 accounts
763,117,241 Verifications.io accounts
711,477,622 Onliner Spambot accounts
622,161,052 Data Enrichment Exposure From PDL Customer accounts
593,427,119 Exploit.In accounts
509,458,528 Facebook accounts
457,962,538 Anti Public Combo List
Recently added breac
436,855 Otelier accounts
249,990 MSI accounts
79,712 Le Coq Sportif C accounts
71,039,833 Stealer Logs, Ja accounts
4,247,768 Scholastic accou
300,187 SuperDraft accou
874,594 GLAMIRA accou
dnsdumpster.com
DNSDumpster.com
Learn
Defend
dns recon & research, find & lookup dns records
Enter a Domain to Test
example.com
Start Test!
>> Free users are limited to 50 results for a single domain. Get 12 months Plus Access - on Sale
System Locations
Hosting / Networks
Services / Bar
A Records (subdomains from dataset)
shodan.io
Neue Chrome-Version verfügbar
SHODAN
Explore
Pricing
Search
Login
Search Engine for the Internet of Everything
Shodan is the world's first search engine for Internet-connected devices. Discover how Internet intelligence can help you make better decisions.
SIGN UP NOW
// EXPLORE THE PLATFORM
Beyond the Web
Websites are just one part of the Internet. Use Shodan to discover everything from power plants, mobile phones, refrigerators and Minecraft servers.
Monitor Network Exposure
Keep track of all your devices that are directly accessible from the Internet. Shodan provides a comprehensive view of all exposed services to help you stay secure.
Internet Intelligence
Learn more about who is using various products and how they're changing over time. Shodan gives you a data-driven view of the technology that powers the Internet.
More than 3 million registered users across the world are using Shodan, including:
89% of the Fortune
5 of the Top 6 Cloud
1,000+ Universities

# OSINT


Black Basta Blog
stniiomyjliimcgkvdszvgen3eaaoz55hreqqx6o77yvmpwt7gklffqd.onion
Basta News
bnext.nl
Bnext.nl is a Dutch company specializing in sustainable waste management and recycling, particularly in the construction
Published 0%
Visits 3038
Read more
brachot.com
BRACHOT
Brachot is a leading specialist in
rauch.de
RAUCH Streuer – Kompetenz in Entwicklung & Herstellung
SITE: www.rauch.de
ADDRESS:
Victoria Boulevard E 200
77836 Rheinmünster • Germany
TEL#: +49 (0) 7229 8580-0
ALL DATA SIZE: ≈2tb
1. Employees personal documents
2. Financial data
3. Confidential data
4. Projects, Drawings, RnD(FuE)
5. Clients
& etc...
Brave (tor), Tor: Download data
Firefox, Chrome: Download data
Im Überlappungsbereich der Schweißnähte wird Schweißnahtgüte „D" akzeptiert.
Start und Ende der Schweissnaht
Zugband M-M 550-kpl-RAL 2002
4089001
Published 100%
Visits 5759
VOSSKO

# Click-/Terminal-Fix




heise online › Security › Cybersecurity › Cybercrime › BSI erklärt ersten Angriffsvektor auf Berliner Behörden

## BSI erklärt ersten Angriffsvektor auf Berliner Behörden

Erst Phishing, dann ein Fake-Captcha und ein Terminal-Befehl – so einfach lief nach ersten Analysen die Cyberattacke auf Berlin ab.

heise.de bei Google bevorzugen 306

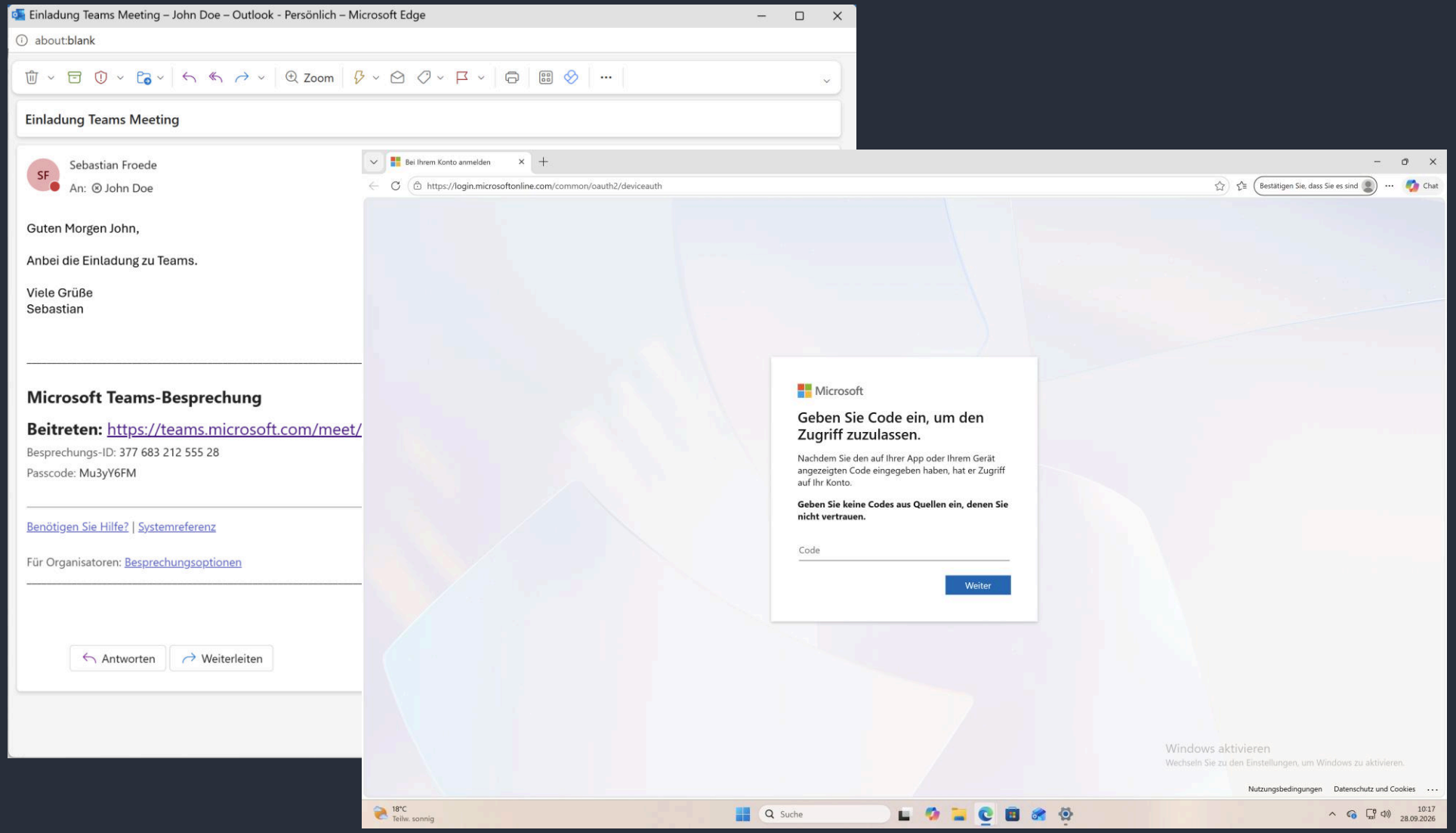


(Bild: Pixels Hunter/Shutterstock.com)

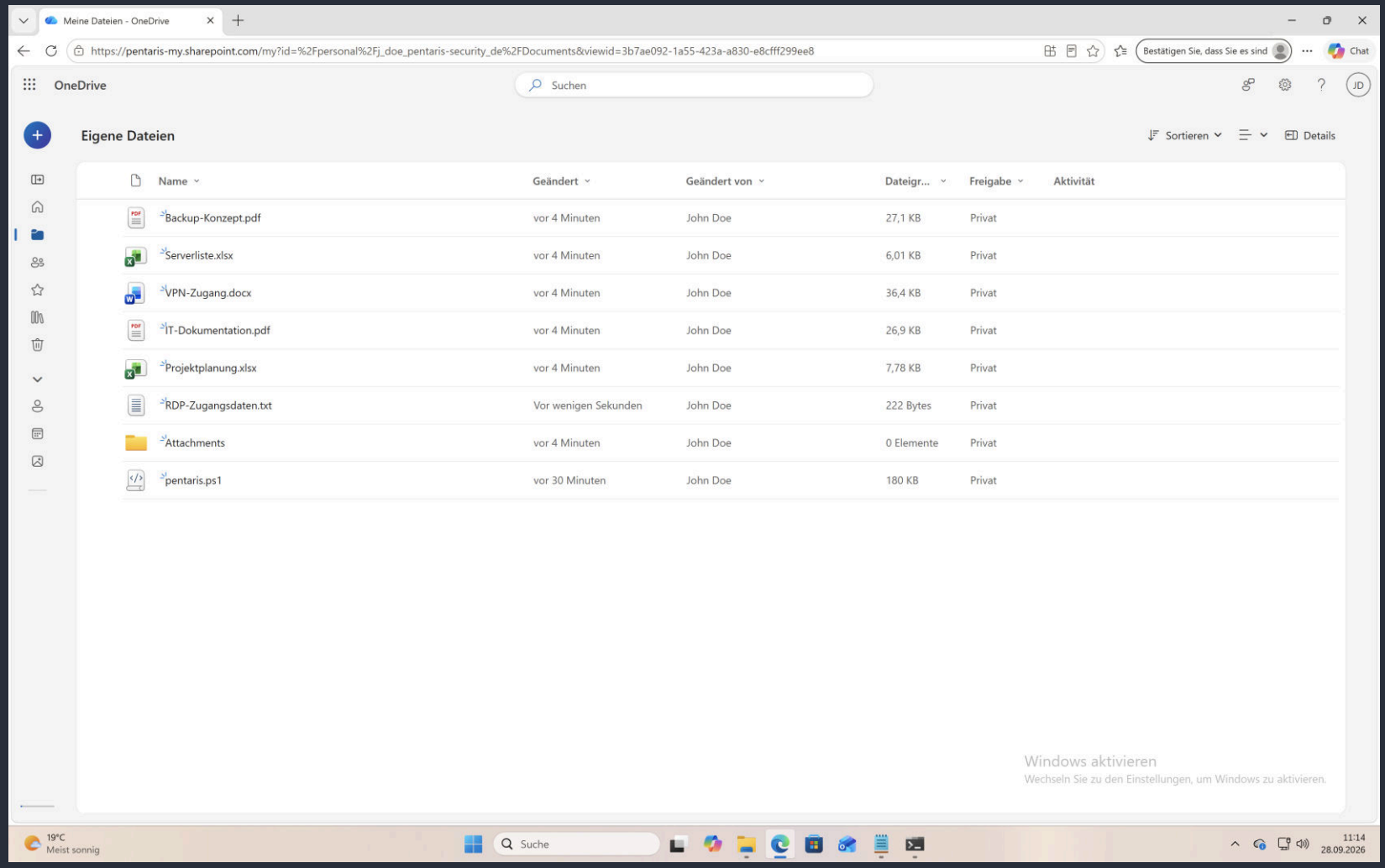
**07.09.2026, 16:26 Uhr Lesezeit: 5 Min.**

*Von Nico Ernst*

# John Doe


Einladung Teams Meeting – John Doe – Outlook - Persönlich – Microsoft Edge
about:blank
Zoom
Einladung Teams Meeting
SF
Sebastian Froede
An: John Doe
Guten Morgen John,
Anbei die Einladung zu Teams.
Viele Grüße
Sebastian
Microsoft Teams-Besprechung
Beitreten: https://teams.microsoft.com/meet/
Besprechungs-ID: 377 683 212 555 28
Passcode: Mu3yY6FM
Benötigen Sie Hilfe? | Systemreferenz
Für Organisatoren: Besprechungsoptionen
Antworten
Weiterleiten
Bei Ihrem Konto anmelden
https://login.microsoftonline.com/common/oauth2/deviceauth
Bestätigen Sie, dass Sie es sind
Chat
Microsoft
Geben Sie Code ein, um den Zugriff zuzulassen.
Nachdem Sie den auf Ihrer App oder Ihrem Gerät angezeigten Code eingegeben haben, hat er Zugriff auf Ihr Konto.
Geben Sie keine Codes aus Quellen ein, denen Sie nicht vertrauen.
Code
Weiter
Windows aktivieren
Wechseln Sie zu den Einstellungen, um Windows zu aktivieren.
Nutzungsbedingungen
Datenschutz und Cookies
18°C
Teilw. sonnig
Suche
10:17
28.09.2026

# One-Drive


Meine Dateien - OneDrive
https://pentaris-my.sharepoint.com/my?id=%2Fpersonal%2Fj_doe_pentaris-security_de%2FDocuments&viewid=3b7ae092-1a55-423a-a830-e8cfff299ee8
Bestätigen Sie, dass Sie es sind
Chat
OneDrive
Suchen
JD
Eigene Dateien
Sortieren
Details
Name
Geändert
Geändert von
Dateigr...
Freigabe
Aktivität
Backup-Konzept.pdf vor 4 Minuten John Doe 27,1 KB Privat
Serverliste.xlsx vor 4 Minuten John Doe 6,01 KB Privat
VPN-Zugang.docx vor 4 Minuten John Doe 36,4 KB Privat
IT-Dokumentation.pdf vor 4 Minuten John Doe 26,9 KB Privat
Projektplanung.xlsx vor 4 Minuten John Doe 7,78 KB Privat
RDP-Zugangsdaten.txt Vor wenigen Sekunden John Doe 222 Bytes Privat
Attachments vor 4 Minuten John Doe 0 Elemente Privat
pentaris.ps1 vor 30 Minuten John Doe 180 KB Privat
Windows aktivieren
Wechseln Sie zu den Einstellungen, um Windows zu aktivieren.
19°C
Meist sonnig
Suche
11:14
28.09.2026

# Passwörter

RDP-Zugangsdaten.txt

```
RDP ZUGANGSDATEN
================================

Konto: rdp.kunde.demo
Benutzername: admin
Passwort: XgtaUvtqpiRcuuyqtfVjcvPqqpgYknnHkpfQwv!2024

Benutzername: admin
Passwort: WfszTuspohQbttxpseUibuOppofXjmmGjoePvu!2025
```

*„Wie sieht wohl das Passwort für 2026 aus?“*

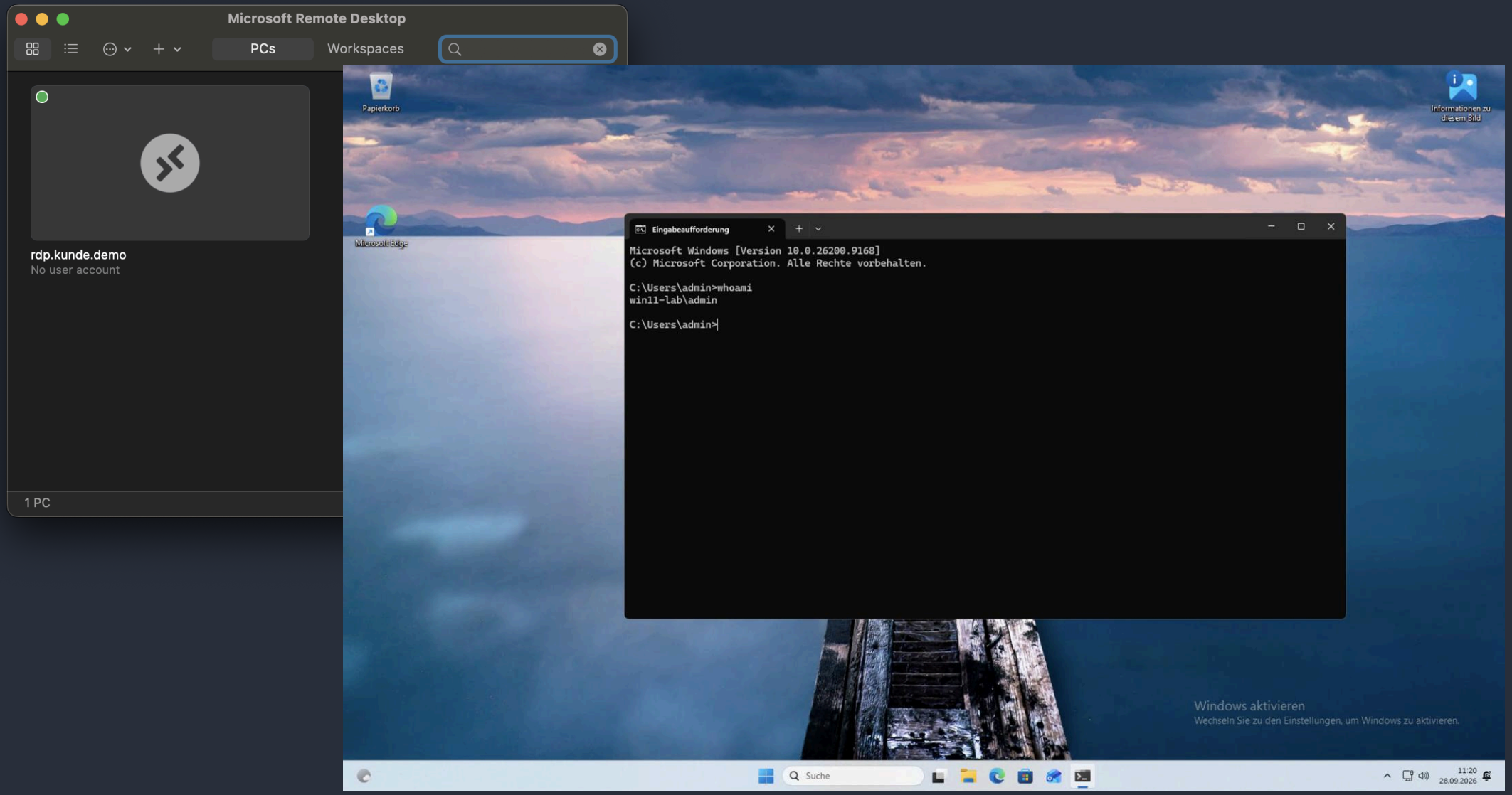
**VeryStrongPasswordThatNooneWillFindOut!2026**

# Passwortstärke

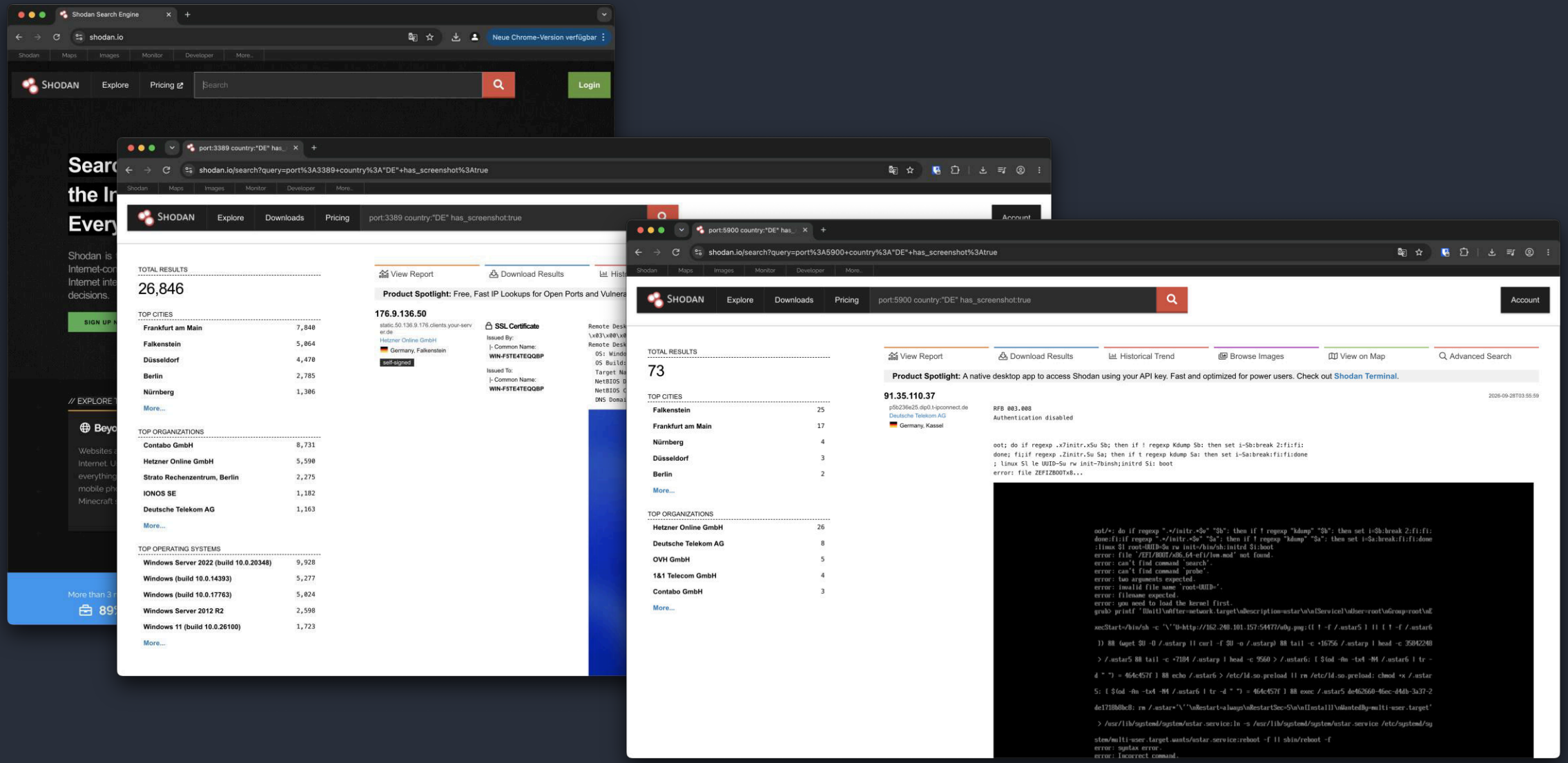
| Passwortlänge (Zeichen) | nur Zahlen | nur Kleinbuchstaben | Klein- & Großbuchstaben | Zahlen und Klein-/Großbuchstaben | Zahlen, Klein-/Großbuchstaben und Symbole |
|---|---|---|---|---|---|
| 4 | Sofort | Sofort | Sofort | Sofort | Sofort |
| 5 | Sofort | Sofort | 46 Minuten | 2 Stunden | 3 Stunden |
| 6 | Sofort | 37 Minuten | 2 Tage | 5 Tage | 1 Woche |
| 7 | Sofort | 16 Stunden | 3 Monate | 10 Monate | 2 Jahre |
| 8 | Sofort | 2 Wochen | 12 Jahre | 50 Jahre | 132 Jahre |
| 9 | 2 Stunden | 1 Jahr | 636 Jahre | 3k Jahre | 9k Jahre |
| 10 | 20 Stunden | 32 Jahre | 33k Jahre | 191k Jahre | 645k Jahre |
| 11 | 1 Woche | 839 Jahre | 1 Mio Jahre | 11 Mio Jahre | 45 Mio Jahre |
| 12 | 3 Monate | 21k Jahre | 89 Mio Jahre | 737 Mio Jahre | 3 Mrd Jahre |
| 13 | 2 Jahre | 567k Jahre | 4 Mrd Jahre | 45 Mrd Jahre | 221 Mrd Jahre |
| 14 | 23 Jahre | 14 Mio Jahre | 241 Mrd Jahre | 2 Bio Jahre | 15 Bio Jahre |
| 15 | 229 Jahre | 383 Mio Jahre | 12 Bio Jahre | 175 Bio Jahre | 1 Brd Jahre |
| 16 | 2k Jahre | 9 Mrd Jahre | 653 Bio Jahre | 10 Brd Jahre | 75 Brd Jahre |
| 17 | 22k Jahre | 259 Mrd Jahre | 33 Brd Jahre | 675 Brd Jahre | 5 Trio Jahre |
| 18 | 228k Jahre | 6 Bio Jahre | 1 Trio Jahre | 41 Trio Jahre | 372 Trio Jahre |

HiVe Systems

# RDP


Microsoft Remote Desktop
PCs
Workspaces
rdp.kunde.demo
No user account
1 PC
Papierkorb
Informationen zu diesem Bild
Microsoft Edge
Eingabeaufforderung
Microsoft Windows [Version 10.0.26200.9168]
(c) Microsoft Corporation. Alle Rechte vorbehalten.
C:\Users\admin>whoami
win11-lab\admin
C:\Users\admin>
Windows aktivieren
Wechseln Sie zu den Einstellungen, um Windows zu aktivieren.
Suche
11:20
28.09.2026

# Shodan


Shodan Search Engine
shodan.io
Neue Chrome-Version verfügbar
SHODAN
Explore
Pricing
Search
Login
port:3389 country:"DE" has_screenshot:true
shodan.io/search?query=port%3A3389+country%3A"DE"+has_screenshot%3Atrue
Downloads
Account
TOTAL RESULTS
26,846
TOP CITIES
Frankfurt am Main 7,840
Falkenstein 5,064
Düsseldorf 4,470
Berlin 2,785
Nürnberg 1,306
More...
TOP ORGANIZATIONS
Contabo GmbH 8,731
Hetzner Online GmbH 5,590
Strato Rechenzentrum, Berlin 2,275
IONOS SE 1,182
Deutsche Telekom AG 1,163
More...
TOP OPERATING SYSTEMS
Windows Server 2022 (build 10.0.20348) 9,928
Windows (build 10.0.14393) 5,277
Windows (build 10.0.17763) 5,024
Windows Server 2012 R2 2,598
Windows 11 (build 10.0.26100) 1,723
More...
View Report
Download Results
Product Spotlight: Free, Fast IP Lookups for Open Ports and Vulnera
176.9.136.50
Germany, Falkenstein
self-signed
SSL Certificate
Issued By:
Common Name:
WIN-F5TE4TEQQBP
Issued To:
Common Name:
WIN-F5TE4TEQQBP
port:5900 country:"DE" has_screenshot:true
shodan.io/search?query=port%3A5900+country%3A"DE"+has_screenshot%3Atrue
TOTAL RESULTS
73
TOP CITIES
Falkenstein 25
Frankfurt am Main 17
Nürnberg 4
Düsseldorf 3
Berlin 2
More...
TOP ORGANIZATIONS
Hetzner Online GmbH 26
Deutsche Telekom AG 8
OVH GmbH 5
1&1 Telecom GmbH 4
Contabo GmbH 3
More...
View Report
Download Results
Historical Trend
Browse Images
View on Map
Advanced Search
Product Spotlight: A native desktop app to access Shodan using your API key. Fast and optimized for power users. Check out Shodan Terminal.
91.35.110.37
Deutsche Telekom AG
Germany, Kassel
RFB 003.008
Authentication disabled

# Wer interessiert sich schon für meine Daten?

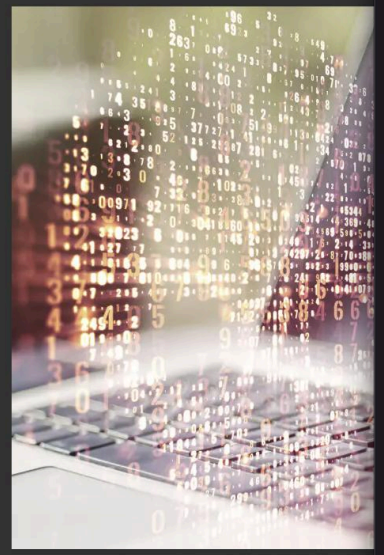
# Berlin Cyberangriff

heise online > Security > Cybersecurity > Cybercrime > BSI erklärt ersten Angriffsvektor auf Berliner Behörden

## BSI erklärt ersten Angriffsvektor auf Berliner Behörden

Erst Phishing, dann ein Fake-C
nach ersten Analysen die Cybe

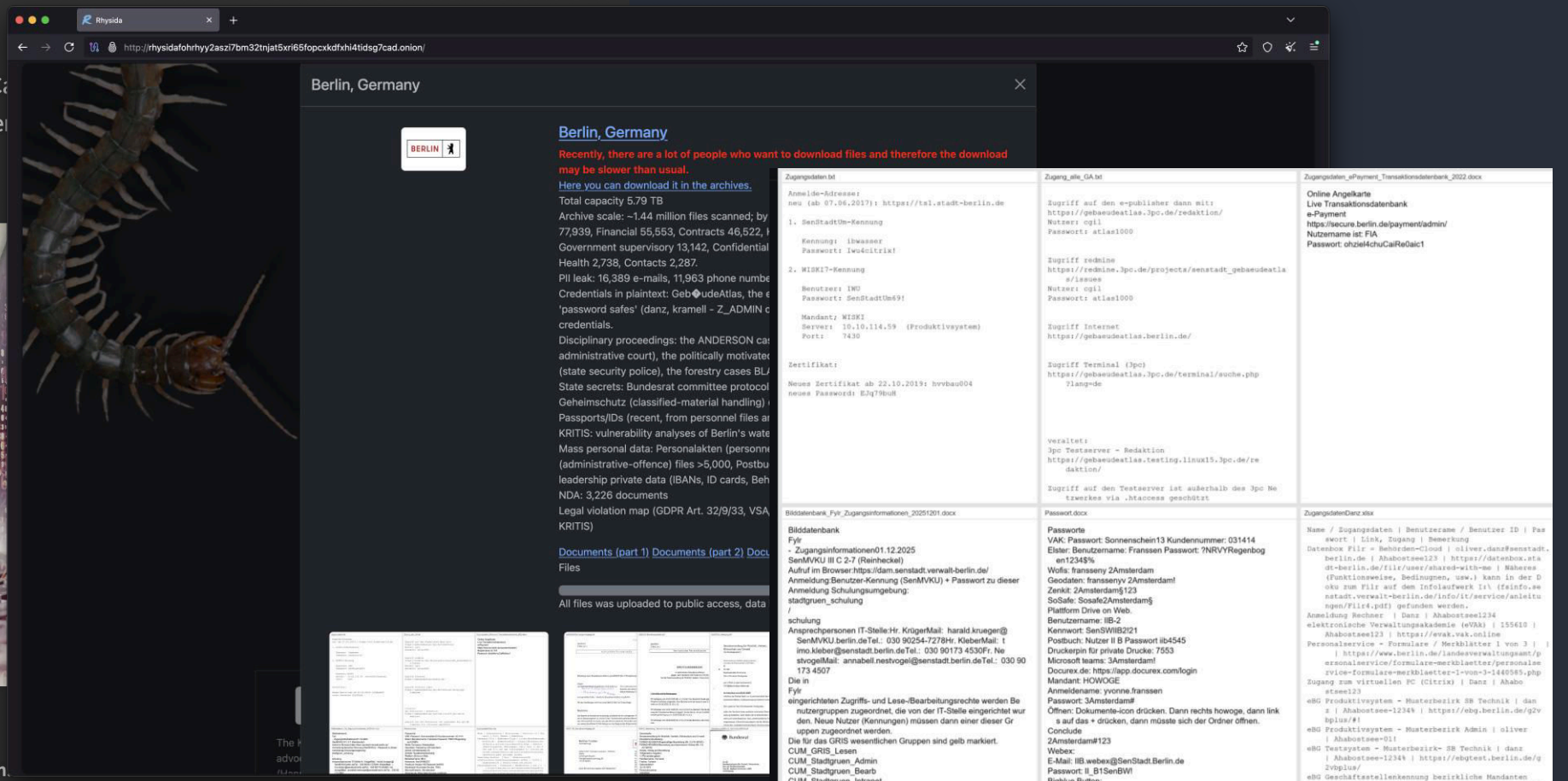
heise.de bei Google bevorzugen



(Bild: Pixels Hunter/Shutterstock.com)

**07.09.2026, 16:26 Uhr  Lesezeit: 5 Min**

*Von Nico Ernst*



# USB Kabel



*„Was wäre wenn es gar kein UBS-Stick wäre?“*

# Abwehrmethoden

| | |
|---|---|
| **OSINT** | – Angriffsoberfläche minimieren |
| **Fake Captcha** | – Web Application Control |
| **Device Code Auth** | – Conditional Access |
| **Account Takeover** | – Awareness / Monitoring |
| **Credentials** | – Passwortmanager |
| **RDP** | – Keine öffentliche Exposition |
| **Admin** | – Least Privilege |
| **Data** | – DLP / Monitoring |

# Fragen?



## Vielen Dank!

PENTARIS SECURITY

*Beim Wölfelsbrunnen 8*
*66346 Püttlingen*

***Telefon: 06806 – 937300***
***E-Mail: office@pentaris-security.de***