
ACP
WILLKOMMEN
BEI ACP
IT for
innovators.

ACP & Deutsche Cyber-Sicherheitsorganisation GmbH

INTERNET EXPOSURE MONITORING DER DCSO

Kurt Brunschweiger

Carsten Maas

ACP | IT FOR INNOVATORS

IT for innovators.

stärken Sie Ihre Sicherheitslage

Made in Berlin
Deutscher / europäischer Fokus

130+
Mitarbeitende

2015
Gegründet

250+
Kunden

24/7
Managed SOC Service aus Deutschland

Ganzheitlich
& souverän

ZERTIFIZIERUNGEN

BSI C5 Testat Typ 2
Full Scope für alle Services und Standorte

ISO 27001:2022
Full Scope für alle Dienstleistungen

TISAX®
Full Scope für Verarbeitung von Informationen

DCSO-CERT
Partner „NoMoreRansomware“ Kampagne (u. a. EUROPOL)



Überblick

ACP | IT FOR INNOVATORS

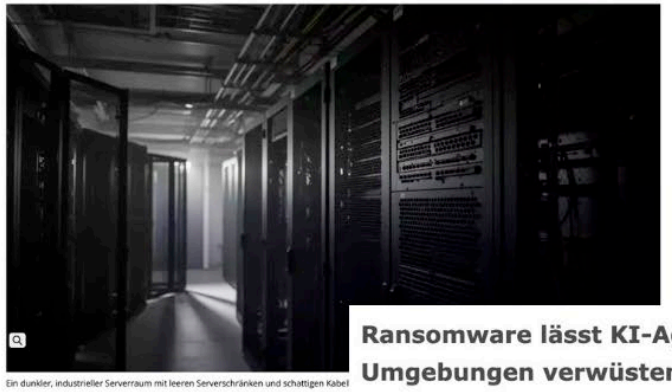
IT for innovators.

GEFAHREN AUS DER SCHATTENWELT

Warlock-Ransomware, Hosts

Warlock-Ransomware: 40 Hosts in zwei Stunden infiziert, 33 verschlüsselt

Die Gruppe nutzt vier SharePoint-Schwachstellen und kompromittierte in einem dokumentierten Fall 40 Hosts binnen zwei Stunden.



Ein dunkler, industrieller Serverraum mit leeren Serverschränken und schattigen Kabel

Eine Ransomware-Gruppe namens Warlock, die auch unter de
ist, führt derzeit gezielte Angriffe auf Organisationen in spanisc
mehrere Sicherheitsmedien übereinstimmend berichten, nutz
rePoint Server aus.

NEWS

Vermehrt Fälle von "Clickfix"-Infektionen

BACS warnt vor Ransomware-Angriffen mittels Fake-Fehlermeldungen

Mi 30.09.2026 - 12:03 Uhr
von Julia Meyer und cka

Das Bundesamt für Cybersicherheit erhält seit mehreren Wochen vermehrt Meldungen von Ransomware-Angriffen durch sogenannte "Clickfix"-Infektionen. Ausserdem mehren sich Fälle, bei denen Cyberkriminelle versuchen, Personen beim Bewerbungsprozess zum Herunterladen von Schadsoftware zu bewegen.



tel / Flickr.com)

ochen melden Betroffene dem Bundesamt für Cybersicherheit (BACS)
n Ransomware-Angriffen. In einer aktuellen Warnung schreibt das BACS vor
usprägungen von Ransomware-Attacken: "Clickfix"-Angriffe sowie Fälle, bei
im Bewerbungsprozess zum Herunterladen von Schadsoftware gebracht

griffe über Websites

Ransomware lässt KI-Agenten gezielt Azure-Umgebungen verwüsten

Eine Ransomware-Gruppe hat begonnen, Azure-Umgebungen mit KI-gestützten Angriffen gezielt zu verwüsten. Bisher konnten nur die Aktivitäten selbst beobachtet werden, über die Hintergründe liegen noch kaum Erkenntnisse vor.

PDF

Christian Kahle, 29.09.2026 12:20 Uhr



NDR

tur Geschichte

nabrück Kommunalwahl 2026



Cyberangriff: Mindestens sechs Kliniken in Niedersachsen betroffen

Stand: 28.05.2026 18:42 Uhr

Bei einem Angriff von Cyberkriminellen auf den Abrechnungsdienstleister Unimed sind tausende Patientendaten gestohlen worden. In Niedersachsen sind mindestens sechs Kliniken betroffen, unter anderem in Hannover, Göttingen und Oldenburg.

CYBERCRIME ÖKOSYSTEM

Akteure



Motivation

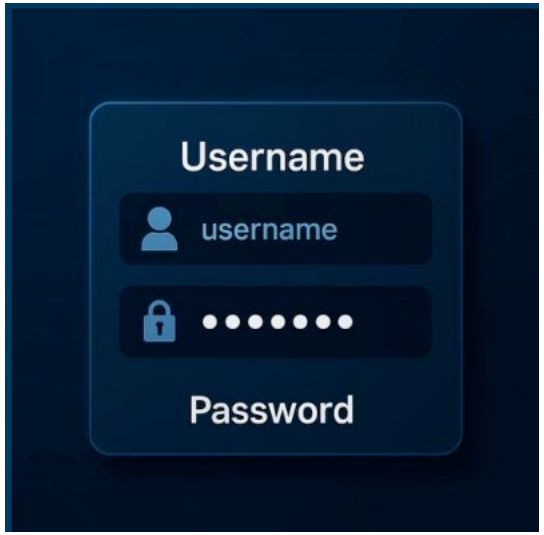


Nicht nur Angreifer



Skalierung des Problems:
52% aller befragten Unternehmen weltweit hatten in den letzten 12 Monaten ein Datenleck…in **Deutschland 48%** (Bitdefender Survey 2023)

ACP | IT FOR INNOVATORS



16 Milliarden Login Credentials 2025

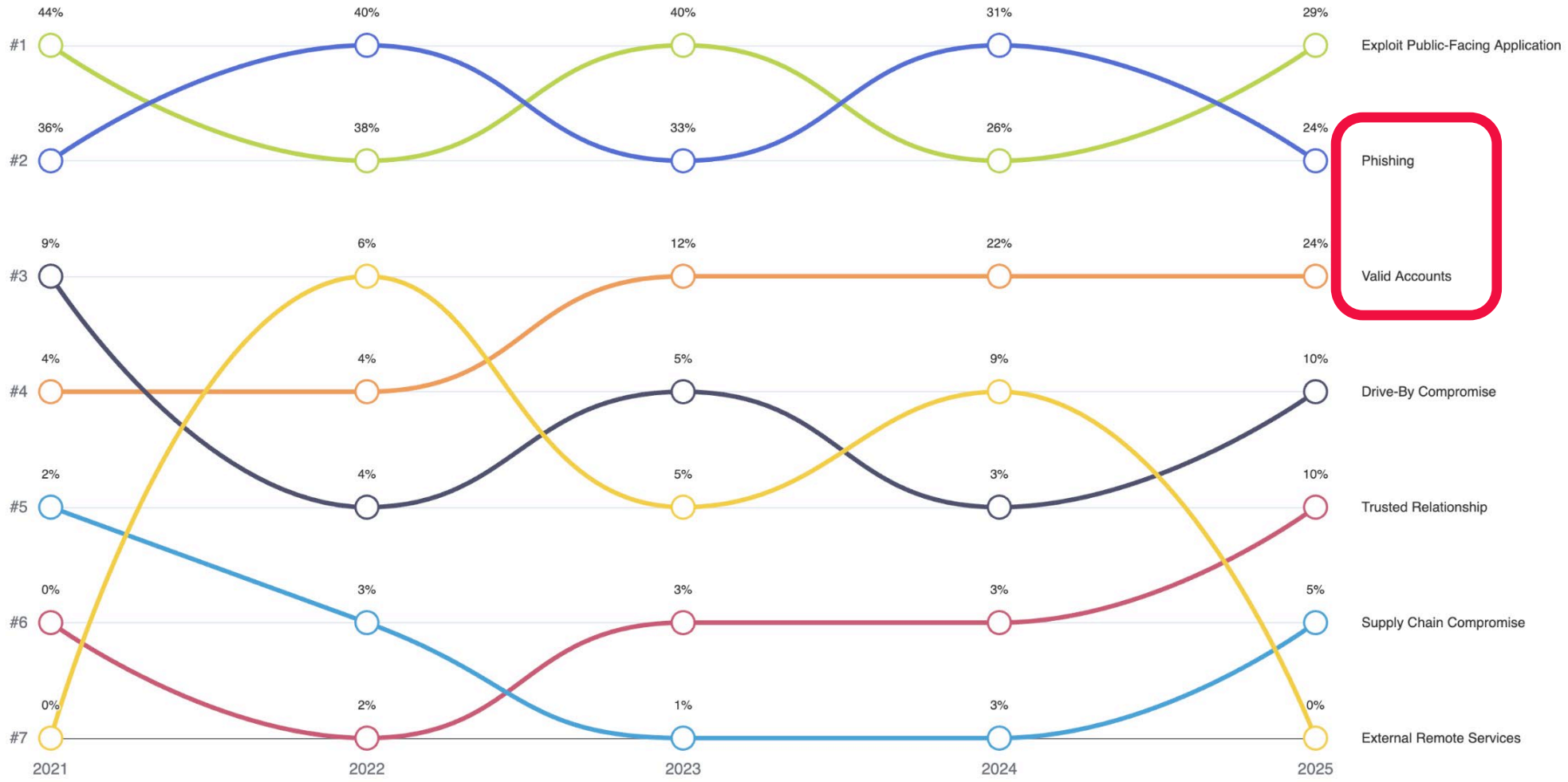


60% der Seiten: illegale Aktivitäten



74,6% betreffen deutsche Opfer

Phishing und **Valid Accounts** als **Erstzugriff** durch Angreifer wird in etwa bei der **Hälfte aller erfolgreichen Angriffe** verwendet.



ACP | IT FOR INNOVATORS

DEUTSCHLAND IST TOP-ZIEL

- **21%** der kompromittierten Daten in StealerLogs stammen aus Deutschland
- Kosten pro Vorfall: ca. **5-5,5 Mio. Euro**
- 2023 mehr als 7,5 Mrd. Informationen gehandelt oder verfügbar gemeldet → **+45%** ggü. 2022



ACP | IT FOR INNOVATORS



Samsung Deutschland – Leak aus altem Credentials Diebstahl

- GHNA veröffentlicht ca. 270.000 Kundendaten aus dem Support System von Samsung DE
- Kein aktueller Zero-Day, sondern älterer „Infostealer“-Log
- Bei frühzeitigem Monitoring wäre der Schaden minimierbar gewesen



Angebote für vollständige Admin-Zugänge

- 2025 wurden Angebote von Admin-Zugängen zu Online-Shops entdeckt
- Deutsche Shops basierend auf Gambio CMS
- Veränderung von Zahlungsdaten, Auslesen von Kundendaten etc. möglich
- Bei frühzeitigem Monitoring wäre der Schaden minimierbar gewesen

ACP | IT FOR INNOVATORS

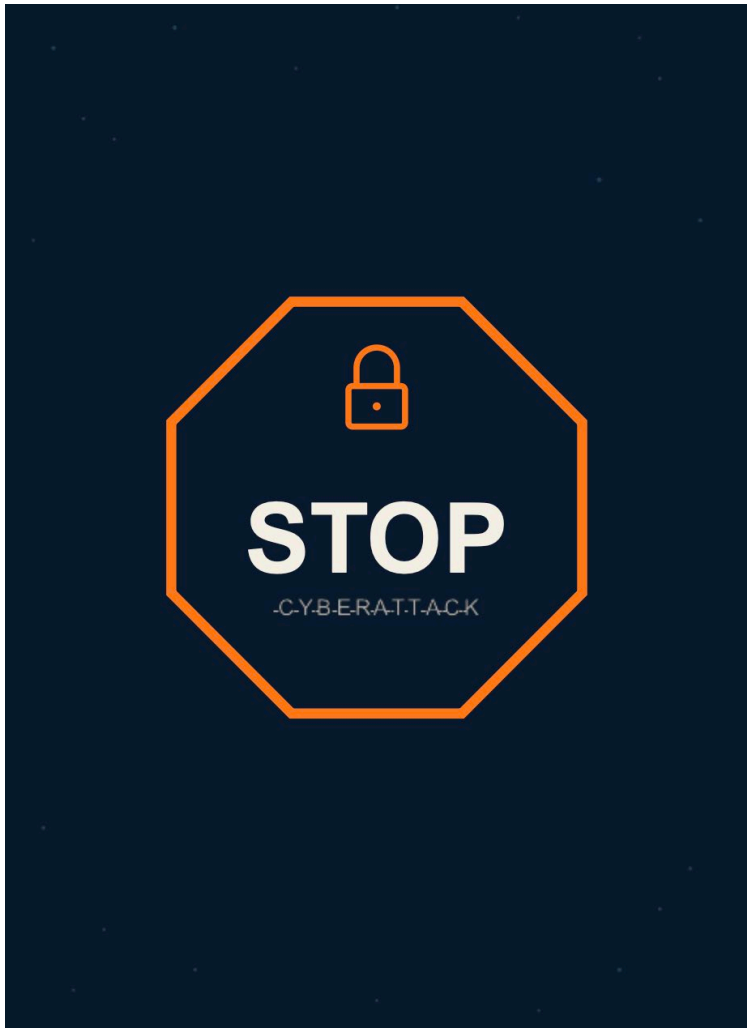
VERMUTLICHE MISSKONFIGURATION

- 2021: Ransomware-Angriff durch „Pay or Grief“ (Ex Evil Corp. -> Russland)
- Verschlüsselung der Server & Datenbanken
- 9. Juli 2021: Ausruf des Katastrophenfalls
- Über 200 Tage kein normaler Betrieb
- Bei einem frühzeitigen Monitoring wäre der Schaden minimierbar gewesen

Als Podcast zu finden unter:

„You are fucked – Deutschlands erste Cyberkatastrophe“





Gegenmaßnahmen & Prävention

Managed Service „Internet Exposure Monitoring“

ACP | IT FOR INNOVATORS

IT for innovators.

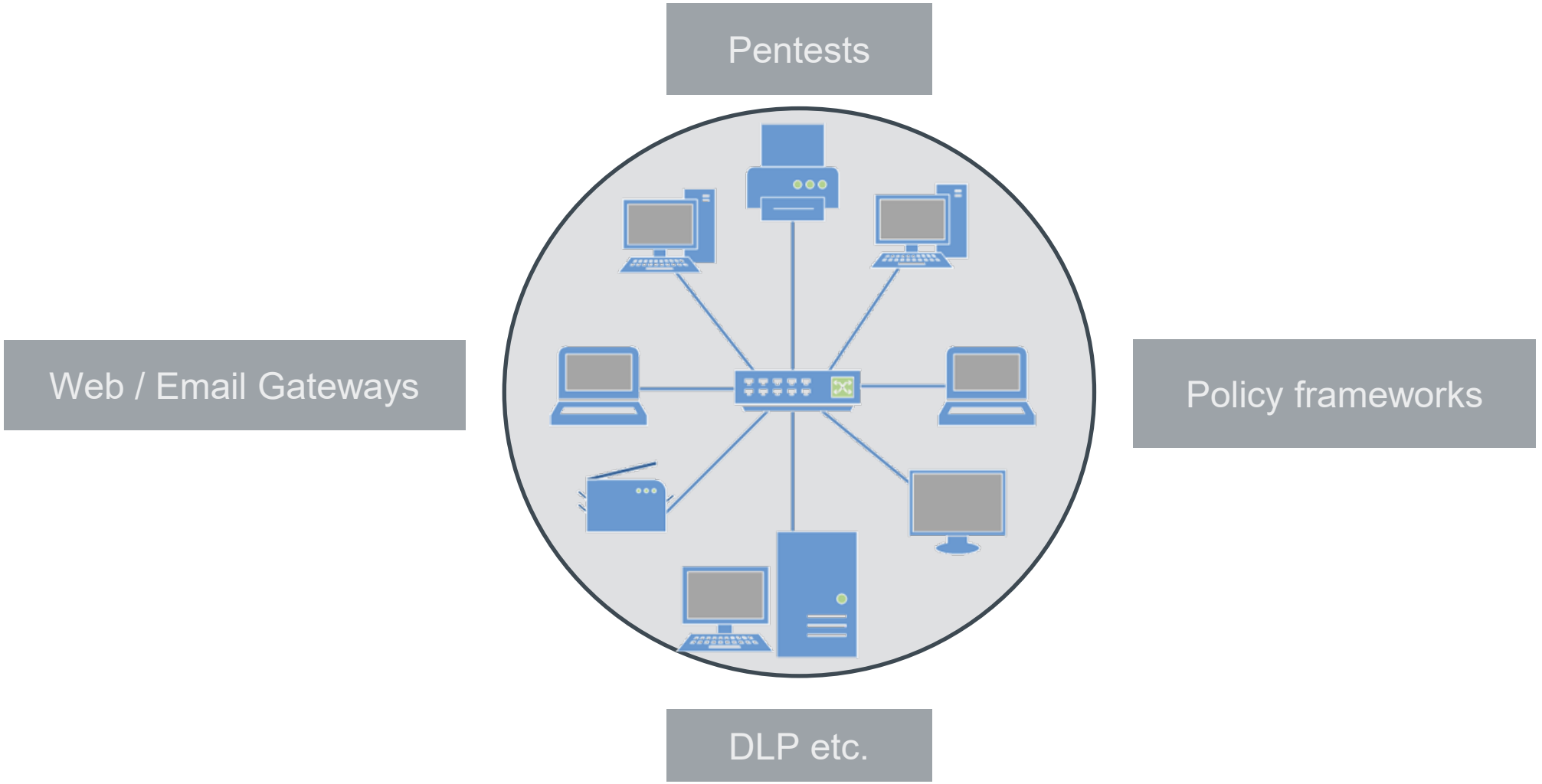
MANAGED SERVICE „INTERNET EXPOSURE MONITORING“

- **24/7 Monitoring:** kontinuierliche Überwachung von Dark Web Markplätzen, Foren, Leaks, InfoStealer etc.
- **Bestimmte Indikatoren:** Firmenname, Domain, Mitarbeiter-E-MailAdressen, Zugangsdaten, Admin-Zugänge, interne Dokumente etc.
- **Einsatz von Tools & HUMINT:** mittels automatisierter Tools PLUS menschliche Analyse, eine Gefährdung bewerten



ACP | IT FOR INNOVATORS

Vertrauliche Daten sind im internen, geschützten Bereich



ACP | IT FOR INNOVATORS

Ein Blick hinter die Kulissen ist wichtig!



Shadow IT / Shadow Clouds

Pastebins

Misconfigured connected storage

Social Media

3rd Party

Code Repositories

BYOD

DCSO
INTERNET EXPOSURE MONITORING

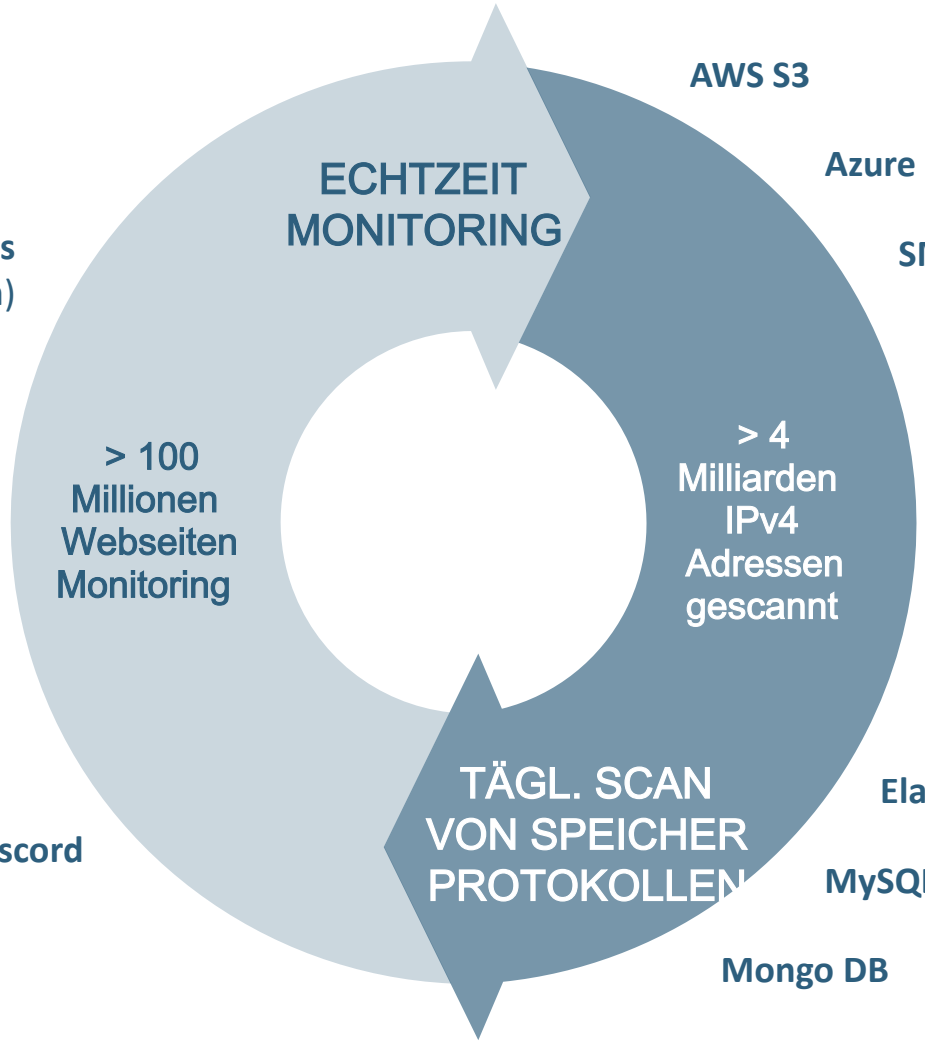
Paste Sites
(e.g. pastebin.com)

Document Shares
(e.g. DropBox, Google Drive, OneDrive)

Source Code Repositories
(e.g., Github)

Dark Web & Social Media Forums

Instant Messaging: Telegram, Discord



AWS S3

Azure Blob

SMB

FTP (S)

NFS

rsync

SQL

PostgreSQL

ElasticSearch

MySQL

Mongo DB

ACP | IT FOR INNOVATORS

DCSO
INTERNET EXPOSURE MONITORING

Information Leakage Monitoring

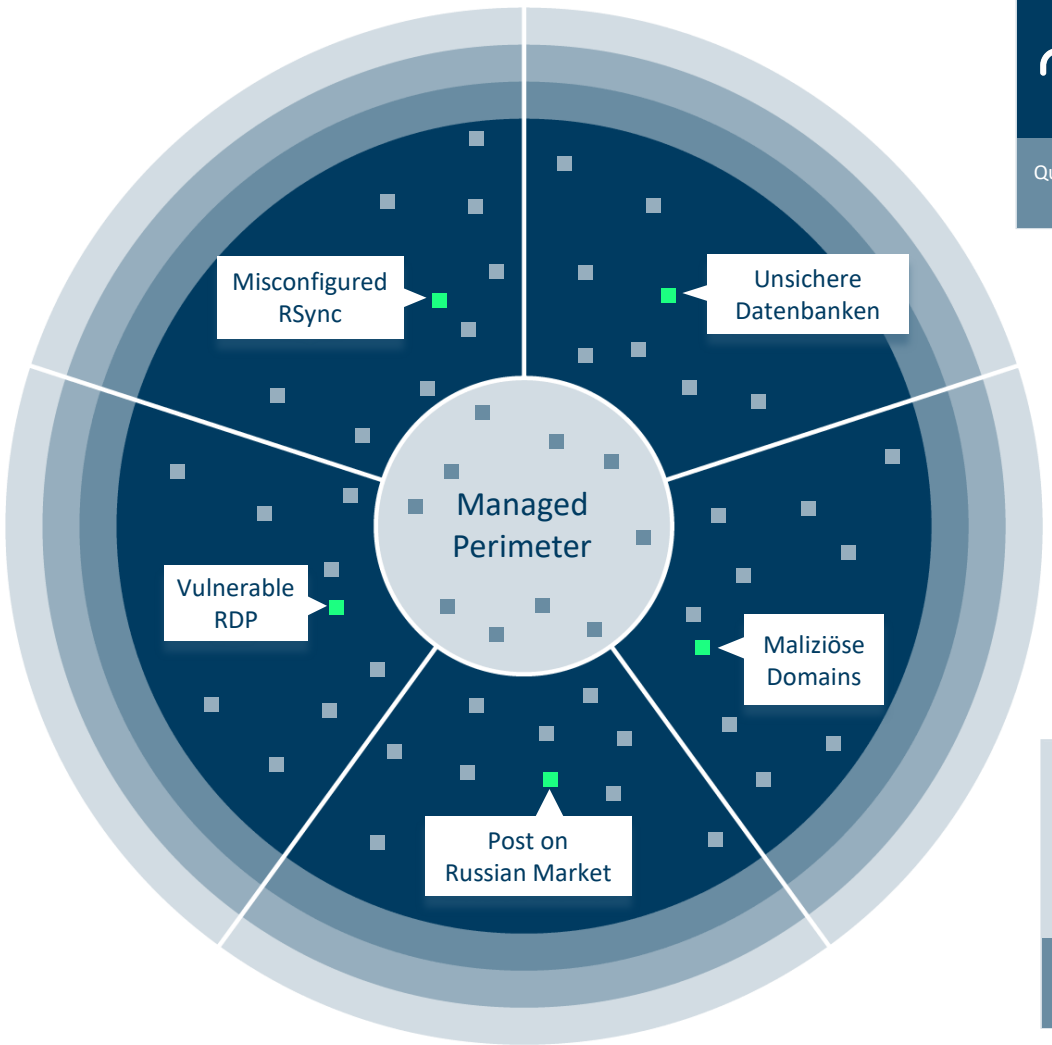
Überwachen, erkennen und sichern **öffentlich zugänglicher sensibler Daten**, bevor sie gebreached werden.

Quellen: SMB • FTP(S) • GCS • AWS S3 • MySQL • Azure Storage • ElasticSearch • MongoDB

Asset Discovery & Monitoring

Erkennen und absichern **anfälliger Schattendienste,** bevor sie gehackt werden.

Quellen: RDP • TeamViewer • Modbus • Fox • Bacnet • Dicom • Telnet • Docker



Identity Leakage Monitoring *

Erkennen **kritischer Datenlecks und infizierter Mitarbeiter**, bevor sie kompromittiert werden.

Quellen: HUMINT • Public leaks • Paste sites • Ransomware gangs • Criminal marketplaces

Domain Protection

Überwachen, erkennen und löschen **bösartiger Domains**, um Ihre Marke zu schützen.

Quellen: Zone files • Passive DNS feeds • Certificate transparency logs

Dark Web Monitoring/ 3rd Party Risk Radar

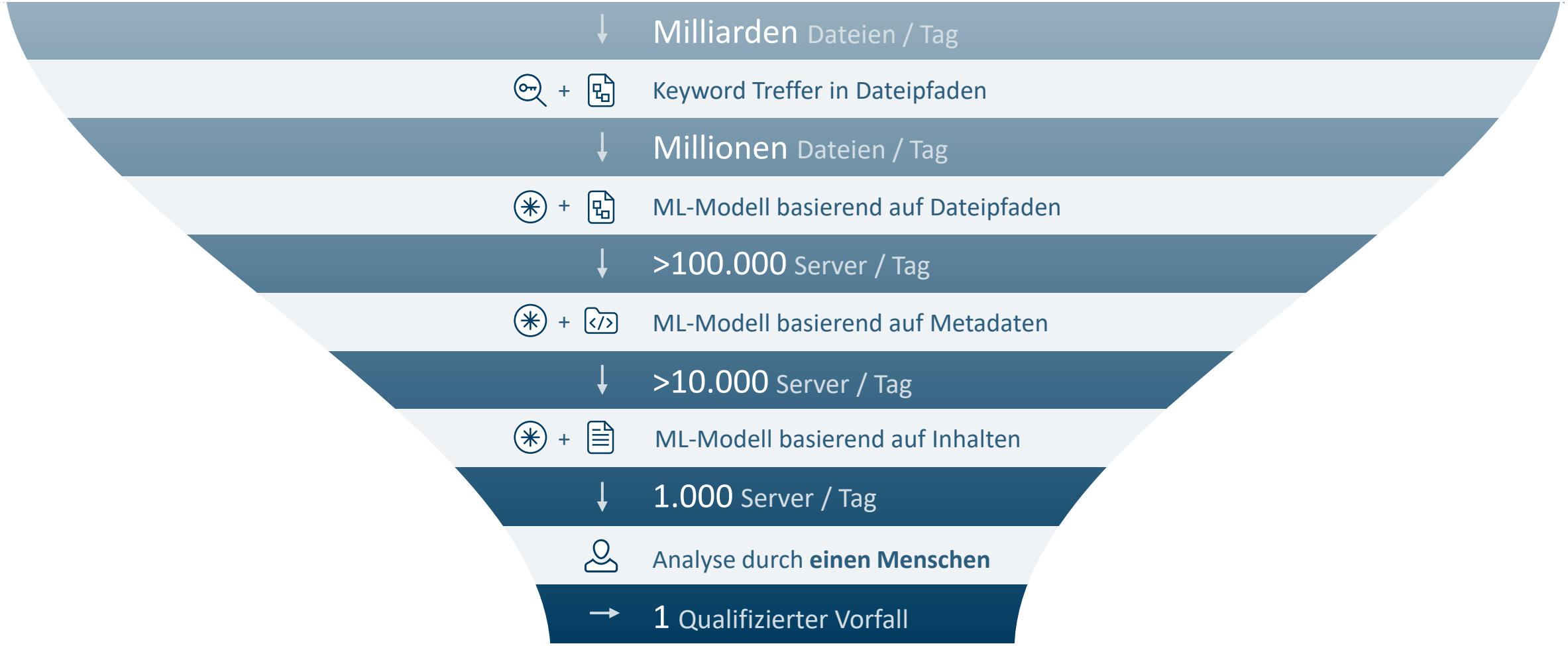
Erkennen von **geplanten, gezielten Angriffen** in Dark Web-Foren, Messaging-Apps usw..

Quellen: Tor Foren • Boards • IRC • Telegram • Discord

*Identity Leakage Monitoring ist **technisch** ein separates Modul

Umfangreiche IPV4 & virtuelle Hosts Scanning | ML-unterstütztes Vorfiltern | Manuelle Untersuchung & Kontextualisierung

ACP | IT FOR INNOVATORS



ACP | IT FOR INNOVATORS

MANAGED SERVICE „INTERNET EXPOSURE MONITORING“

- Reduzierung des Lärms
- Rund um die Uhr Beobachtung
- Klassifizierung nach Risiko
- Reporting & konkrete Handlungsempfehlungen



ACP | IT FOR INNOVATORS

DCSO & ACP – IDENTITY HEALTH CHECK

Was wir prüfen (einmalig)

- Gestohlene Identitäten & Passwörter im Dark Web
- Exfiltrierte Zugangsdaten durch Info-Stealer-Malware
- Kompromittierte Unternehmenszugänge

Ergebnisse

Sie enthalten unter anderem:

- Kompromittierte E-Mail-Adressen & Passwörter
- Ziel-URLs der infizierten Accounts
- IP-Adressen infizierter Geräte
- Zeitpunkt der Kompromittierung

Ihre Vorteile

- Automatisierte Auswertung & Datenbereinigung
- Priorisierte Fundstücke für schnellen Handlungsbedarf
- Abschlussbericht mit Empfehlungen

Rahmenbedingungen

- Check von bis zu 5 Unternehmensdomains
- Max. 25.000 Mitarbeitende
- Ab Auftragseingang 4 Wochen Analysezeitraum

ACP | IT FOR INNOVATORS

Wollen wir darüber sprechen?



ACP | IT FOR INNOVATORS

IT for innovators.

ACP

VOLLE KRAFT

FÜR UNSERE ZUSAMMENARBEIT



IT for innovators.