DCSO

Deutsche Cyber-Sicherheitsorganisation (DCSO)

Gefahren aus der Schattenwelt…

Carsten Maas, Senior PreSales Engineer

Über uns

Gemeinschaftliche Verbesserung der Cyber-Sicherheit durch Managed Services & Austausch

Berlin

122 Mitarbeiter

Gegründet 2015
durch deutsche Unternehmen

150+ Kunden

- Mittelstand
- KRITIS
- Öffentliche Einrichtungen & Hochschulen
- Internationale Konzerne

CIO / CISO Austausch im Fachbeirat (4x jährl.)

ALDI SÜD · Allianz · axel springer · BASF · BAYER · BDI · Bundesamt für Sicherheit in der Informationstechnik · COMMERZBANK · EVONIK Leading Beyond Chemistry · Fraunhofer · FRESENIUS · Henkel · HILTI · KFW · otto group · SCHOTT · SCHWARZ · SIEMENS · SIEMENS energy · thyssenkrupp · VOLKSWAGEN AKTIENGESELLSCHAFT · WÜRTH GROUP · ZEISS · ZF

Full-Cycle Cyber Defense aus einer Hand

Mit unserer in-house Expertise können wir durchgängig den Schutz über den gesamten Angriffszyklus abdecken.

Connect

DCSO-Community

- Aktiver Austausch
- Vorträge
- Lokale Treffen

Advisory Board

- Zukunft mitgestalten
- Ausblicke in die Weiterentwicklung

Defend

Managed Detection & Response

- Angriffserkennung & Eindämmung (mSOC)
- Managed Edge Node (SIEM lite/embedded SIEM)
- Internet Exposure Monitoring

Incident Response

- Active Incident Response (24/7)
- Ransomware Resilience Review
- Compromise Assessment (inkl. M365)

Threat Intelligence

- Reports / Lagefeststellung
- Advanced (Feeds) / Expert Community
- Managed TI Plattform

Improve

Security Assessments

- Information Security Assessment
- Cold Start Capability Assessment
- IT Security Architecture Review

Security Technology

- Zugriff auf Testdatenbank (Hersteller/Produkte)
- Expert Community
- Security Portfolio Review

Security Consulting

- Incident Management
- Krisenstabstraining
- Incident Response Readiness Exercise
- u.v.m.

BSI Lagebericht 2025

IT-Sicherheitslage in Deutschland

Bundesamt
für Sicherheit in der
Informationstechnik

BSI-Präsidentin Claudia Plattner über die aktuelle Bedrohungslage:

*„Die Cybersicherheitslage ist **messbarer geworden**. Unser Lagebericht stellt erstmals konsequent statistische Indikatoren in den Vordergrund.*

*Wahr ist aber auch: Wir alle gemeinsam – Staat, Wirtschaft, Wissenschaft und Gesellschaft – haben noch ein **großes Stück Arbeit** vor uns. Wenn wir es **nicht kurzfristig schaffen**, uns und unsere Angriffsflächen zu verteidigen, werden wir **verwundbar bleiben**.“*

Quelle: BMI / Henning Schacht

Quelle: Die Lage der IT-Sicherheit in Deutschland 2025
vom 10.11.2025

Warum Dark Web Monitoring überlebenswichtig ist!

Deep Web, Dark Web, Underground Foren

Dark…was!?

- **Deep Web:**
  nicht indexierte Inhalte im Web, z.B. Datenbanken, Shares etc.
- **Dark Web:**
  versteckter Teil des Internets, der nicht über klassische Suchmaschinen zugänglich ist und i.d.R. anonym und illegal ist
- **Underground Foren:**
  Foren, in denen gestohlene Daten und Zugangsdaten gehandelt werden oder Angriffe verabredet werden

Cybercrime Ökosystem

Akteure

Motivation

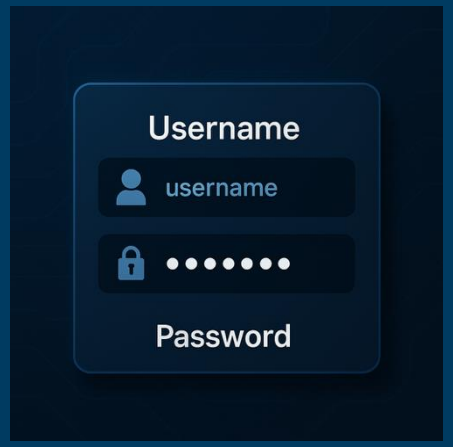
Nicht nur Angreifer

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

(Bitdefender Survey 2023)

Zahlen & Trends

16 Milliarden Login Credentials 2025

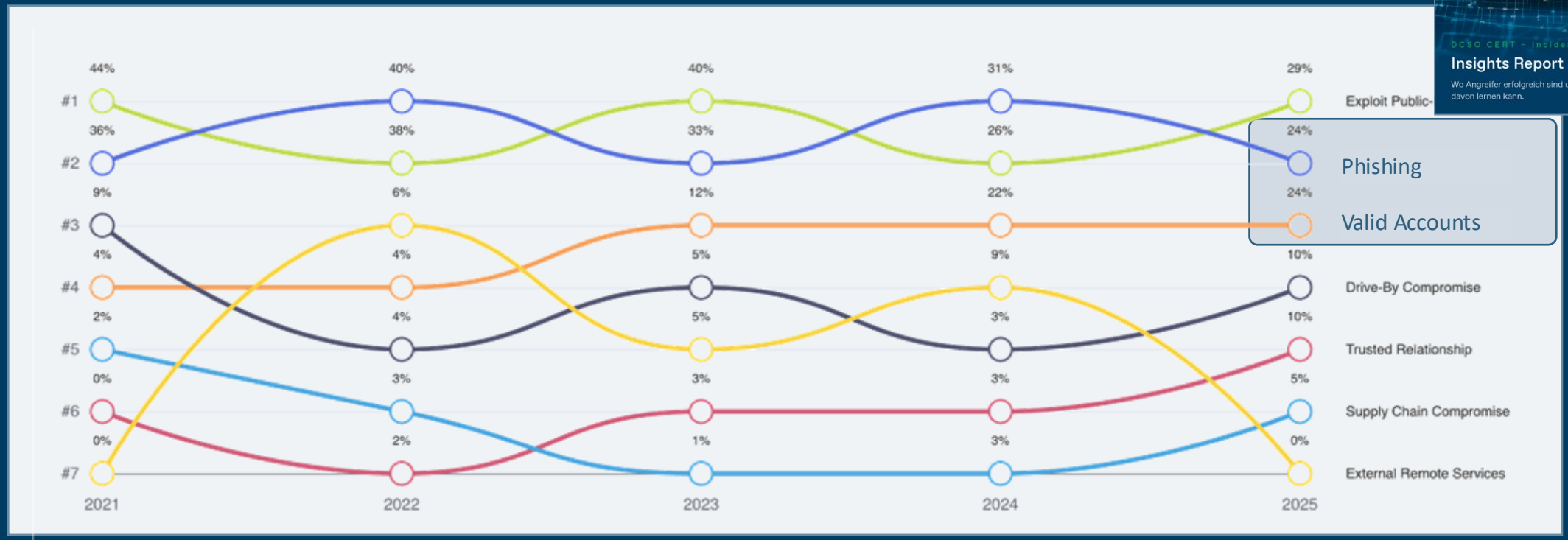


60% der Seiten: illegale Aktivitäten

74,6% betreffen deutsche Opfer

Beobachtungen aus dem DCSO-Lagebericht

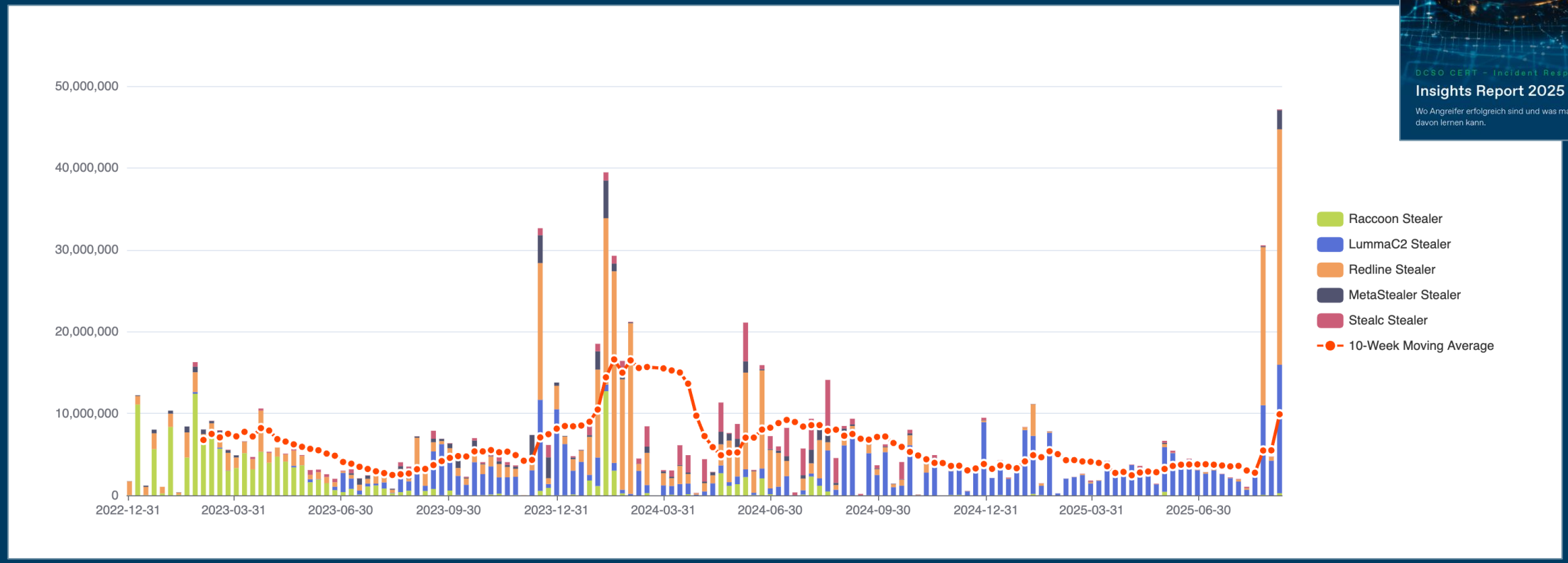
Klick –>



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

Beobachtungen aus dem DCSO-Lagebericht

Klick –>



In einem Zeitraum von 30 Monaten hat die DCSO
5-10 Millionen neue & einzigartige **Einträge pro Woche** überprüft

Deutschland ist Top-Ziel

- **21%** der kompromittierten Daten in Stealer-Logs 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

Große Leaks

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

Große Leaks

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

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“

Auswirkungen

Finanzielle Verluste

Reputation & Vertrauen

Angreifbarkeit & Kettenreaktion

Minimalmaßnahmen

- Ordentliche Passwort-Hygiene
- Einsatz von MFA
- Mitarbeiter sensibilisieren

Erweiterte Maßnahmen

- Black Box/Honeypots
- Notfall- & Incident Response Plan definieren
- Partnerschaft mit einem Dark Web Monitoring Service-Anbieter

Managed Service „Dark Web Monitoring“

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

Managed Service „Dark Web Monitoring“

Managed Service „Dark Web Monitoring“

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

Wollen wir darüber sprechen?

DCSO
Engineering Security.
Together.