THOMAS KRENN®

IT-Sicherheit Rückblick 2023

Webinar am 17.01.2024

Christoph Mitasch, Thomas-Krenn.AG

THOMAS KRENN®

Christoph Mitasch

- seit 2005 bei der Thomas-Krenn.AG, Niederlassung Österreich
- Diplomstudium Computer- und Mediensicherheit
- Erfahrung in Web Operations, Linux und HA
- Cyber-Security-Practitioner (v1)
- IT-Sicherheitsbeauftragter

Agenda

Lagebericht BSI und BKA

Ransomware

Angriff Microsoft Cloud: Storm-0558

KeePass-Malvertising

SMTP Smuggling

Lagebericht BSI 2023

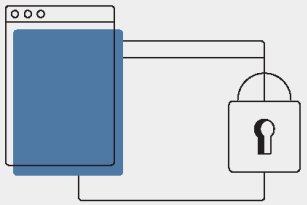
- „Insgesamt zeigte sich im aktuellen Berichtszeitraum eine **angespannte bis kritische Lage**.“
- „Die Bedrohung im Cyberraum ist damit **so hoch wie nie zuvor**. “
- „**Ransomware** blieb die **Hauptbedrohung**“
- **Big Game Hunting** hat **abgenommen**
  -> Fokus auf KMUs, Kommunen, Hochschulen
- „**Weg des geringsten Widerstands**“ – leicht angreifbare Opfer
- „Durch ihren **Black-Box-Charakter** stellen **große KI-Sprachmodelle** eine Schwachstelle an sich dar.“

https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Lagebericht/lagebericht_node.html

Ransomware

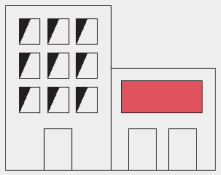
ist weiterhin die größte Bedrohung.

2 **Ransomware-Angriffe** auf Kommunalverwaltungen oder kommunale Betriebe wurden durchschnittlich pro Monat bekannt.

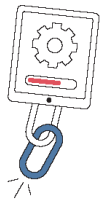


68 erfolgreiche **Ransomware-Angriffe auf Unternehmen** wurden bekannt.

15 davon richteten sich gegen **IT-Dienstleister**.

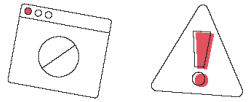


Mehr als **2.000** **Schwachstellen** in Software-Produkten **(15 % davon kritisch)** wurden im Berichtszeitraum durchschnittlich im Monat bekannt. Das ist ein **Zuwachs von 24 %.**



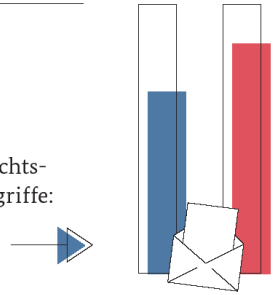
Eine Viertelmillion

neue **Schadprogramm-Varianten** wurden durchschnittlich an jedem Tag im Berichtszeitraum gefunden.



66%

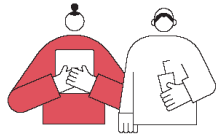
aller **Spam-Mails** im Berichtszeitraum waren Cyberangriffe:
34% Erpressungsmails,
32% Betrugsmails

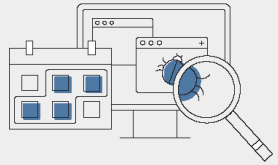


84%

aller betrügerischen E-Mails waren **Phishing-E-Mails** zur Erbeutung von Authentisierungsdaten, meist bei Banken und Sparkassen.

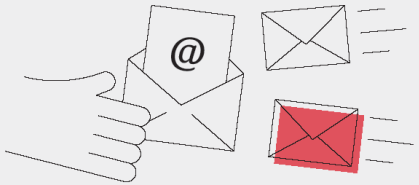
Top 3-Bedrohungen je Zielgruppe:

Gesellschaft	Wirtschaft	Staat und Verwaltung
		
Identitätsdiebstahl	***Ransomware***	***Ransomware***
Sextortion	Abhängigkeit innerhalb der IT-Supply-Chain	APT
Phishing	Schwachstellen, offene oder falsch konfigurierte Online-Server	Schwachstellen, offene oder falsch konfigurierte Online-Server



Rund **21.000** **infizierte Systeme** wurden täglich im Berichtszeitraum erkannt und vom BSI an die deutschen Provider gemeldet.

Durchschnittlich rund **775** **E-Mails mit Schadprogrammen** wurden an jedem Tag im Berichtszeitraum in deutschen Regierungsnetzen abgefangen.



370 **Webseiten** wurden im Durchschnitt an jedem Tag des Berichtszeitraums für den Zugriff aus den Regierungsnetzen gesperrt. **Der Grund:** Die Seiten enthielten Schadprogramme.

6.220 2022

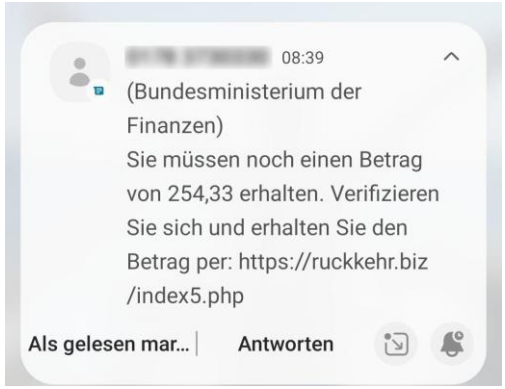
5.100 2021

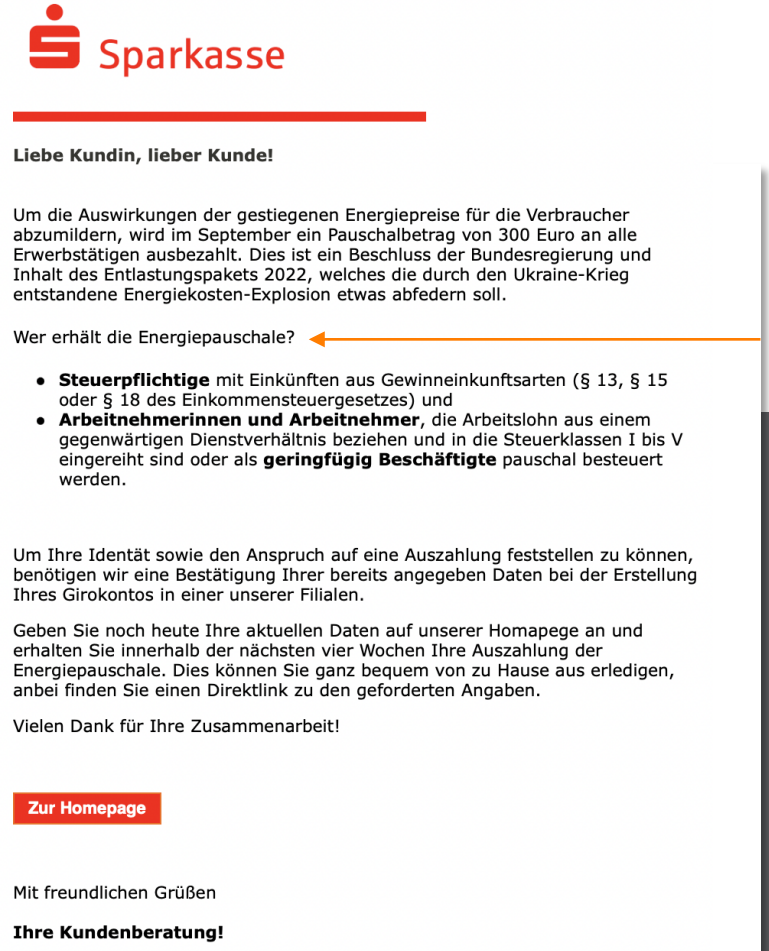
7.120 Teilnehmer hatte die **Allianz für Cyber-Sicherheit** im Jahr 2023.

Deutschland **Digital•Sicher•BSI•**

Phishing

- KI sorgt für weniger Rechtschreib- und Grammatik Fehler
- Interaktionsraten bei KI-generierten E-Mails sogar höher als bei menschlich erstellten E-Mails
- Angreifer informiert vorab per Telefon über kommendes Email, auch via Deepfake

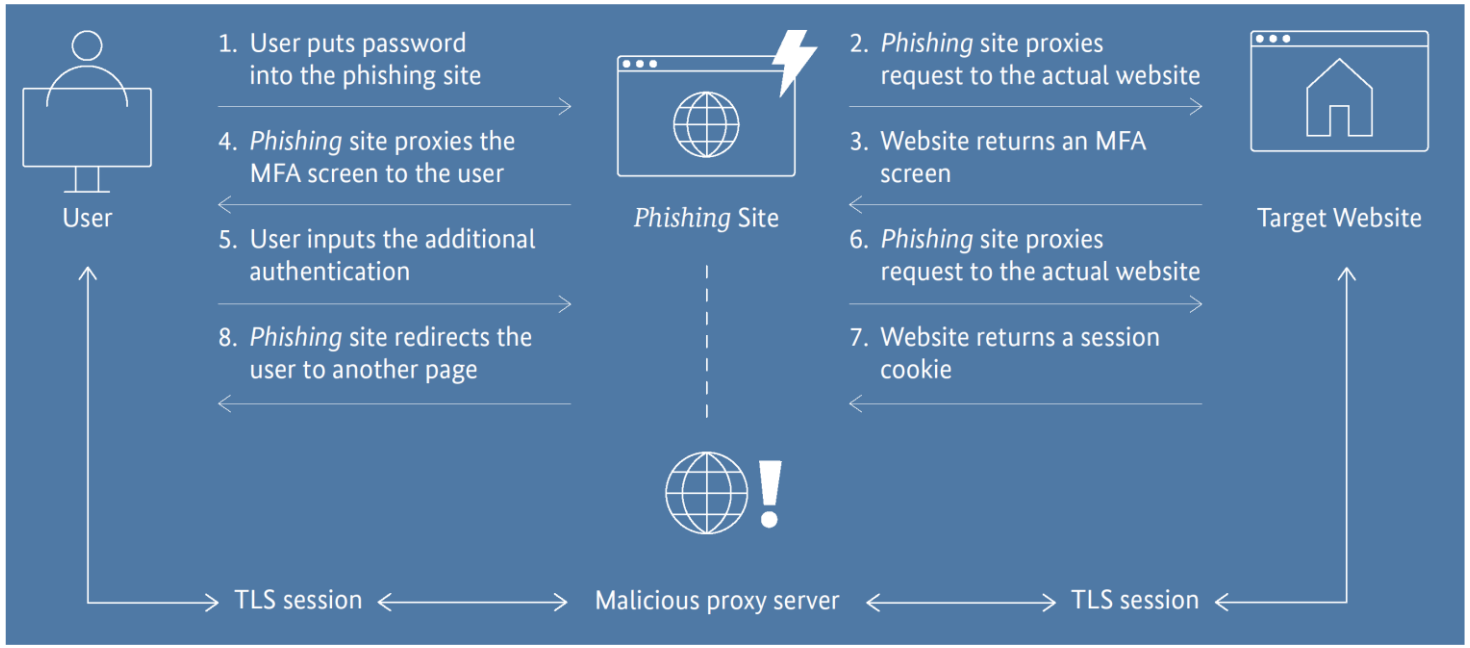




https://sosafe-awareness.com/de/ueber-sosafe/presse/jeder-fuenfte-klickt-auf-ki-erstellte-phishing-mails/
https://www.verbraucherzentrale.nrw/geld-versicherungen/phishingradar-archiv-71872
https://www.verbraucherzentrale.nrw/aktuelle-meldungen/digitale-welt/betrug-phishingmails-und-falsche-sms-von-ministerien-und-behoerden-76907

Phishing-as-a-Service (PhaaS)

- Phishing-Proxy-Service als Man-in-the-Middle
  - Login-Simulation u.a. für: Google, Microsoft, Python PackageIndex, Github, …
  - dadurch auch Supply-Chain-Angriffe via modifizierten Code möglich

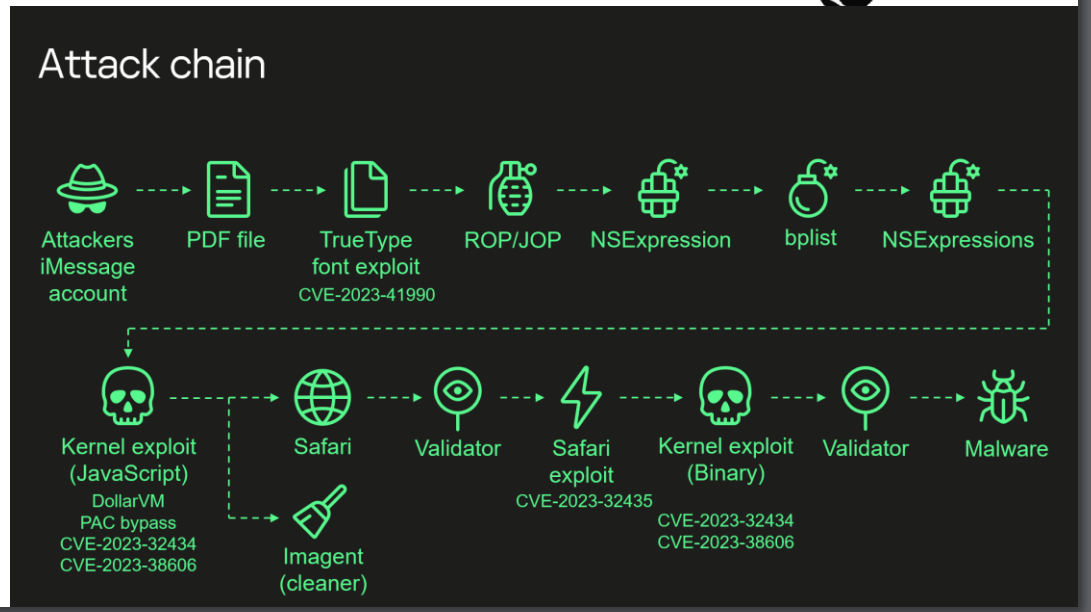


https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2023.html

https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Lageberichte/lagebericht_node.html
https://downfall.page/
https://usa.kaspersky.com/blog/triangulation-37c3-talk/29590/

Hardware-Sicherheit

- Hardware Zero-Day in Exynos-Modemchips (CVE-2023-24033)
  - in Smartphones und Fahrzeugen
  - Angreifer kann Programme auf den mobilen Geräten auszuführen
  - für Angriff reicht die Telefonnummer
  - Ohne Security Fix: WLAN-Anrufe und Voice-over-LTE deaktivieren
- CPU Microcode Updates
  - Downfall (CVE-2022-40982) / Intel
  - Zenbleed (CVE-2023-20593) / AMD Zen CPUs
  - Inception (CVE-2023-20569) / AMD
  - Reptar (CVE-2023-23583) / Intel, Ausbruch aus Gast-VM
- Operation Triangulation bei Apple
  - undokumentierte Prozessorregister in Apple ARM-Chips
  - Kombination von vier 0-day-Lücken
  - iOS und MacOS betroffen



Bundeslagebericht BKA 2022

Rückgang der erfassten Cyberstraftaten um 6,5% (Inlands-PKS). Auslandstaten steigen an.

Die Aufklärungsquote für Cybercrime bewegt sich mit ca. 29% auf dem Niveau des Vorjahres.

Kriminelle Infrastrukturen zerschlagen und Aktivitäten von Cybertätern nachhaltig eindämmen.

Schaden in Deutschland – Täter im Ausland.
Der internationale Aspekt der Cyberkriminalität tritt weiter in den Vordergrund.

Nur 18% der durch Cybercrime betroffenen Privatpersonen haben die Straftat angezeigt.

Agenda

Lagebericht BSI und BKA

Ransomware

Angriff Microsoft Cloud: Storm-0558

KeePass-Malvertising

SMTP Smuggling

Ransomware

- BSI rät ausdrücklich vor Lösegeld-Zahlung ab
- ausgeleitete Daten müssen grundsätzlich als kompromittiert betrachtet werden
- Access-as-a-Service (AaaS)
  Zugangsdaten über Access Broker (z.b. RDP-Login)
  10 bis 60 US-Dollar pro Log
- statt Office-Dokumenten mit Makros oft ISO, IMG oder OneNote-Dateien (.ONE)
- Daten der Betroffenen offen durchsuchbar im Internet (z.B. Raas Alphv)
- Weltweiter Ransomware-Angriff auf ESXi-Server

https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2022.html?nn=28110

Vorfall Südwestfalen-IT

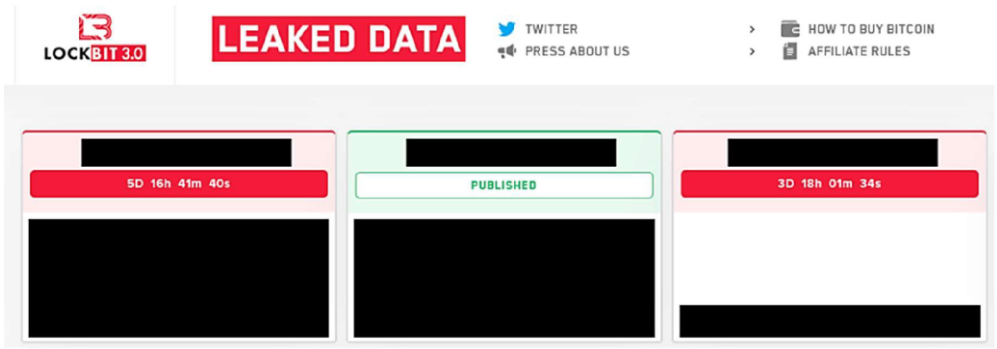

Die Monitore ausgeschaltet, dafür vollbehangen mit Zetteln, die PC-Tastatur ausgestöpselt, dafür Tippen an der Schreibmaschine. So sah in den Tagen nach dem Hackerangriff die Arbeit im Lennestädter Rathaus aus. © Puspas

- einer der größten Angriffe auf die öffentliche Verwaltung in Deutschland
  - 153 Organisationen aus NRW und Niedersachsen betroffen
  - 11 Kreisverwaltungen, 105 Gemeinden, 26 Unternehmen und Verbände, 10 Standesämter
- Angriff Ende Oktober 2023
- 11.1.2024: Der Zeitpunkt, ab wann ein Normalbetrieb läuft, ist derzeit leider noch nicht absehbar
- „Insgesamt arbeiten nahezu **170 Personen** bei der Südwestfalen-IT an der Bewältigung der Auswirkungen des Cyberangriffs. **Neun externe Dienstleister** unterstützen diese Arbeiten. **Mehrere Hundert Server und Tausende Clients** müssen neu aufgebaut und installiert werden.“
- Akira Hackergruppe wird dahinter vermutet
- Zugang oft über Cisco VPNs (CVE-2023-20269), Cisco ASA und FTD
- Keine Lösegeldzahlungen

https://notfallseite.sit.nrw/
https://www.sauerlandkurier.de/kreis-olpe/hackerangriff-suedwestfalen-it-lennestadt-puspas-interview-reisepass-sterbeurkunde-92750578.html

Lösegeld-Zahlungen

- Durchschnitt Lösegeldsumme 2022: 276.619 US-Dollar
- Unternehmen gehen seltener auf Forderungen ein
  -> Einbußen versucht durch Erhöhung auszugleichen (35%)
- DLS („Dedicated Leak Site“)



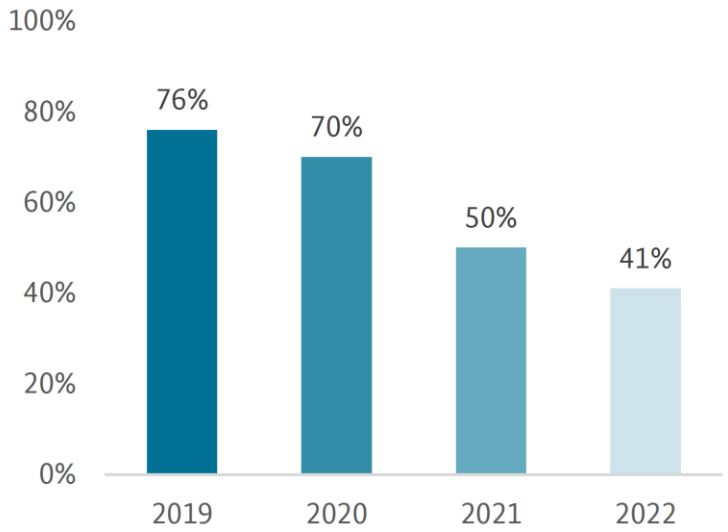


Abbildung 12: Anteil an Unternehmen, die nach einem Ransomware-Angriff Lösegeld gezahlt haben. Anmerkung: Nach Daten von Coveware in Chainalysis (2023). The 2023 Crypto Crime Report

https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2022.html?nn=28110

Ransomware-as-a-Service

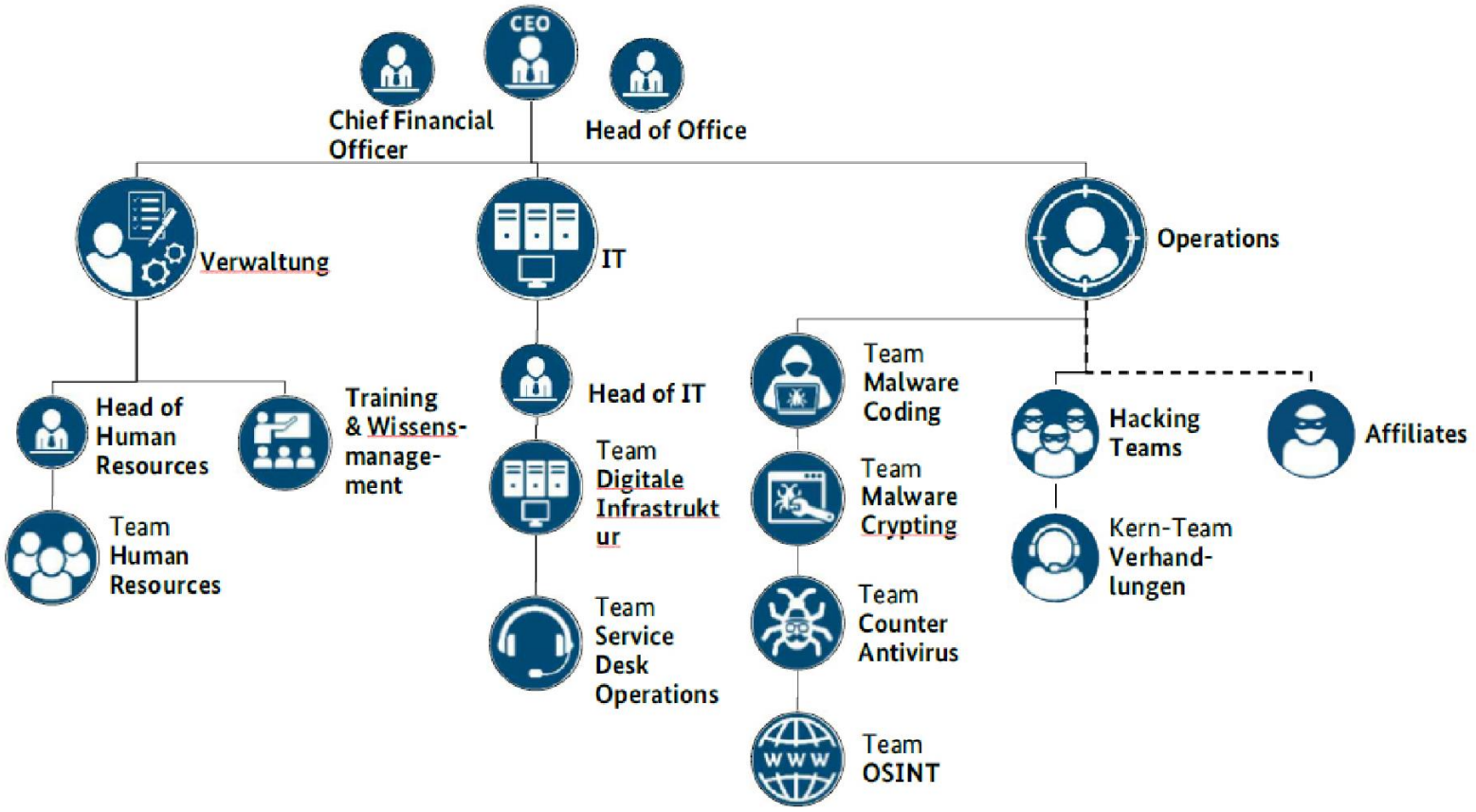


Abbildung 14: Arbeitsteilung innerhalb einer RaaS-Gruppierung analog der Struktur eines mittelständischen Unternehmens mit ca. 30-100 Mitarbeitern

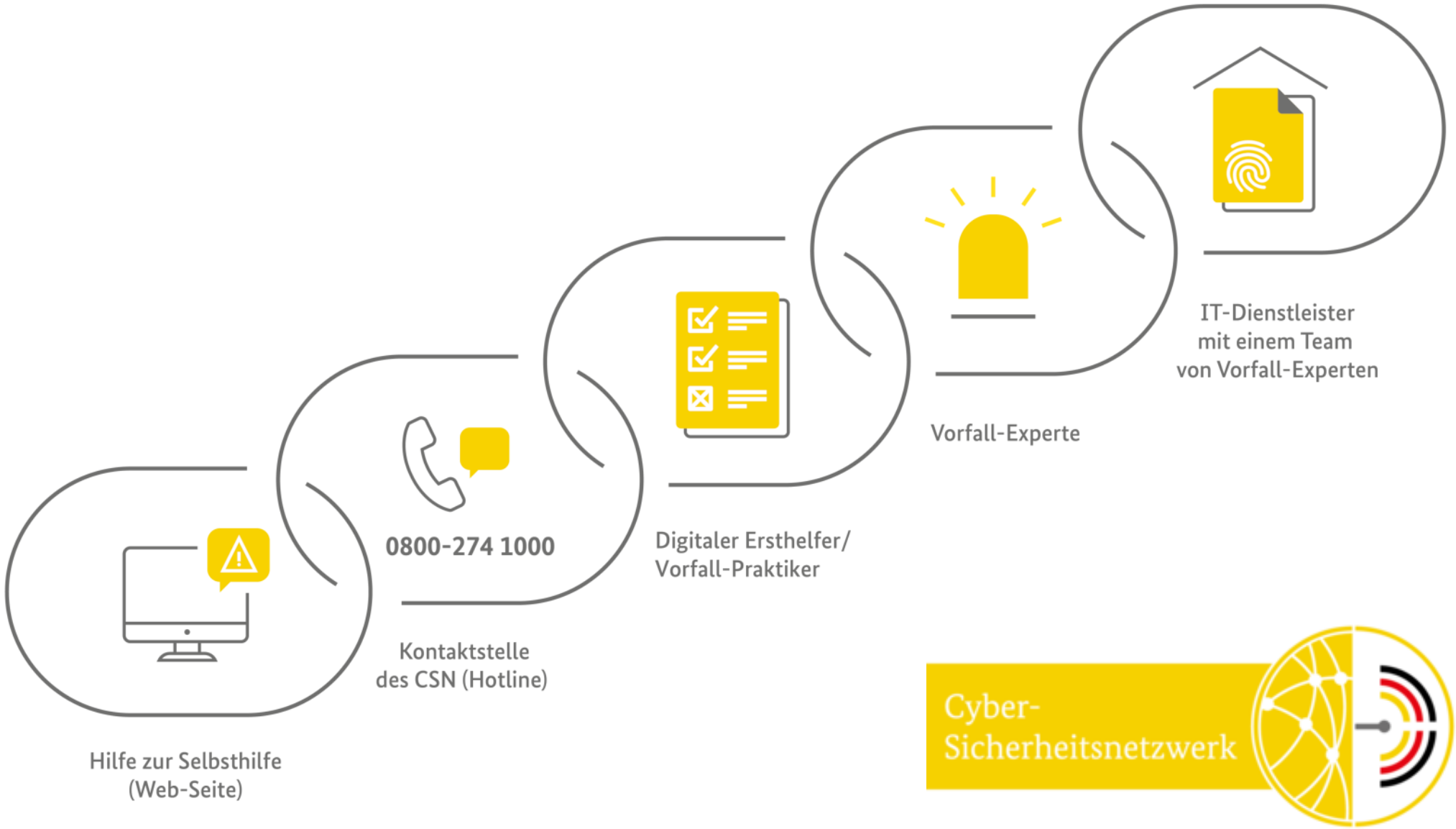
https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2022.html?nn=28110

Gegenmaßnahmen

- Updates
- MFA – auch für VPN, Phishing-resistente Methoden
- Windows Domänen-Admin nicht für Clientverwaltung -> LAPS, Admin Tiering
- Offline-Backup
- Notfallpläne (NEU 2023: BSI-Standard 200-4 Business Continuity Management)

https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2022.html?nn=28110

Digitale Rettungskette



Agenda

Lagebericht BSI und BKA

Ransomware

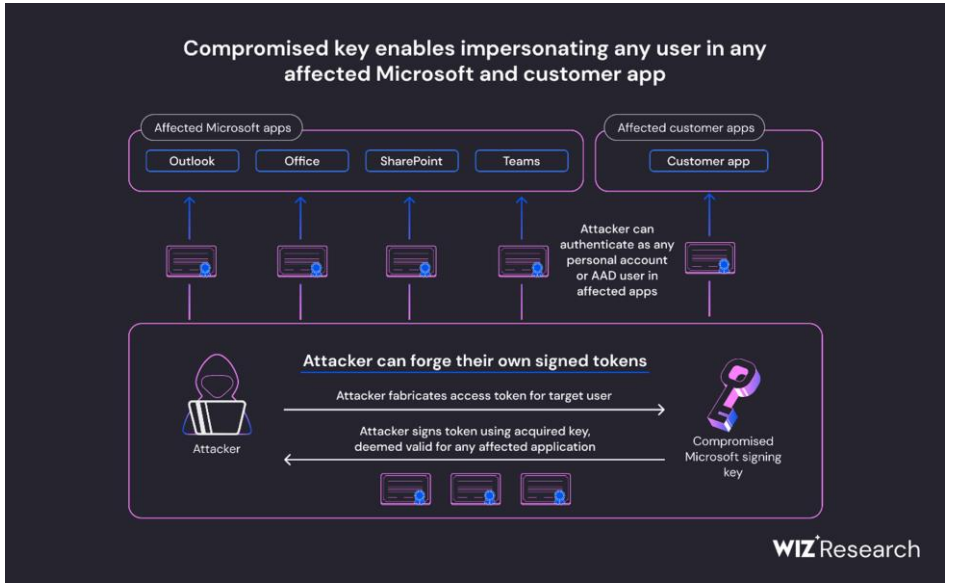
Angriff Microsoft Cloud: Storm-0558

KeePass-Malvertising

SMTP Smuggling

Angriff Microsoft Cloud: Storm-0558

- Master Signing Key: 2016 erstellt und 2021 abgelaufen
- Speicherdump mit Master Signing Key
- Dump landet aus abgesichertem Bereich in Microsoft Netzwerk
- Rechner von MS Mitarbeiter mit Zugriff darauf wird kompromittiert
- Logs von 2021 sind nicht mehr vorhanden
  um weitere Details prüfen zu können
- Aufarbeitung war zu Beginn nicht transparent
  „Microsoft mitigates China-based threat actor Storm-0558 targeting of customer email“
- „If you have not been contacted, our investigations indicate that you have not been impacted.”



https://www.wiz.io/blog/storm-0558-compromised-microsoft-key-enables-authentication-of-countless-micr
https://msrc.microsoft.com/blog/2023/07/microsoft-mitigates-china-based-threat-actor-storm-0558-targeting-of-customer-email/
https://www.flickr.com/photos/48932385@N07/31534968303

Agenda

Lagebericht BSI und BKA

Ransomware

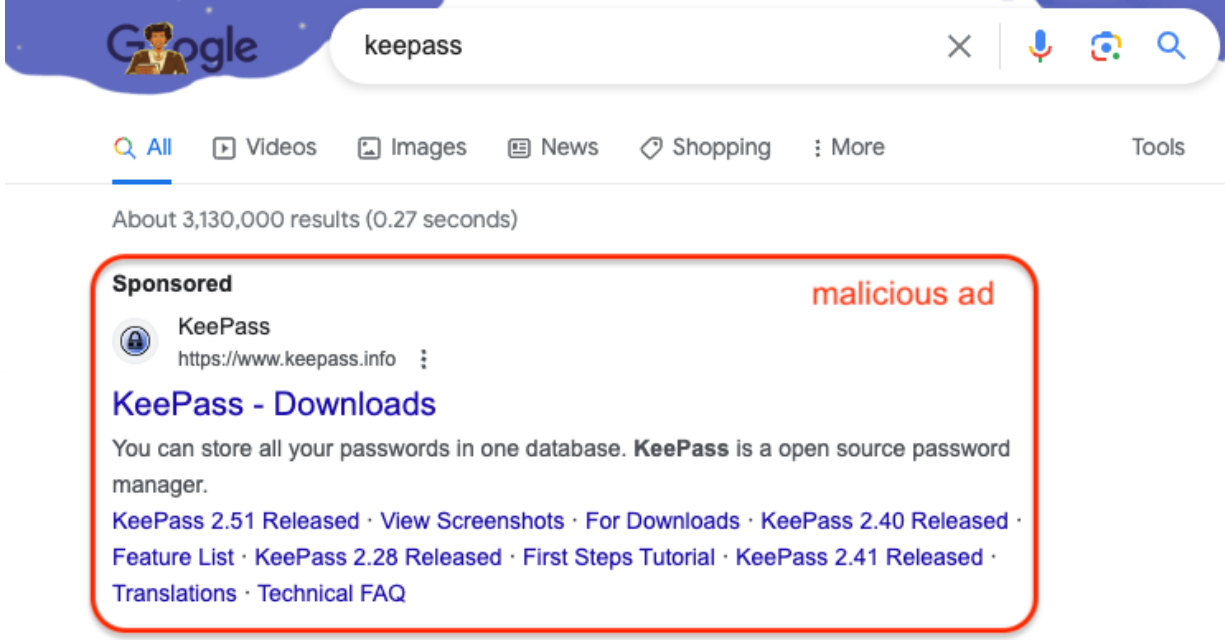
Angriff Microsoft Cloud: Storm-0558

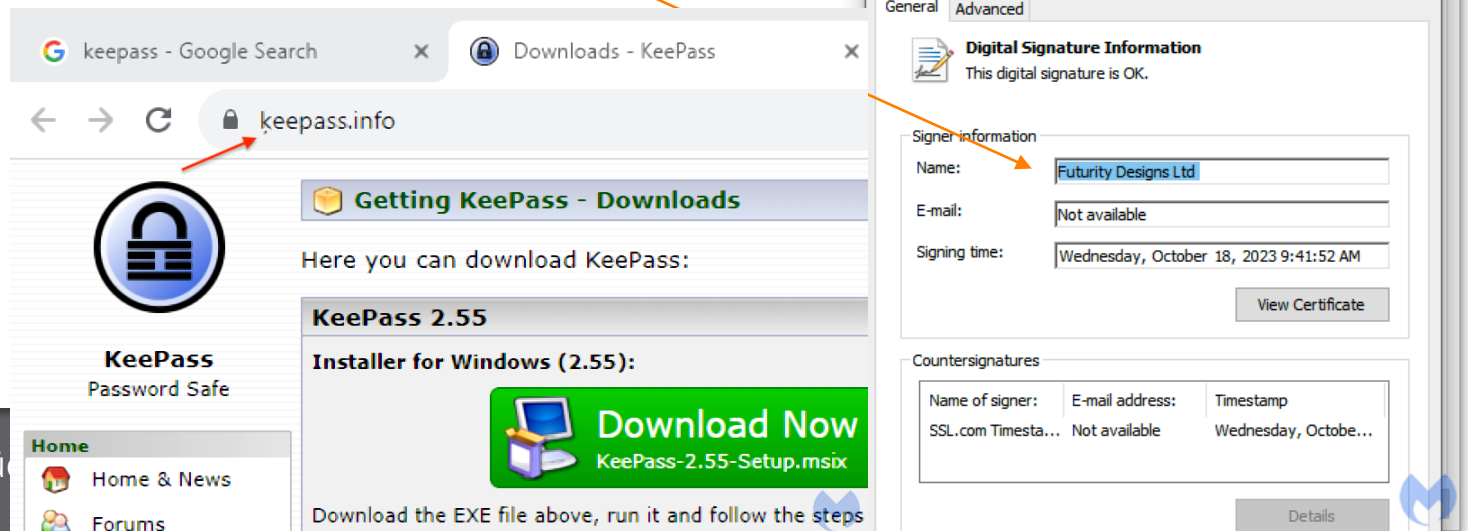
KeePass-Malvertising

SMTP Smuggling

KeePass Malvertising

- Google Werbung für KeePass Download
- IDN Domain ḳeepass.info (xn--eepass-vbb.info)
- Download mit gültiger digitaler Signatur
- Verbindung zu C&C Server aufgebaut
- PunyCode in Browser anzeigen lassen
  - Firefox: network.IDN_show_punycode
  - Chrome: entscheidet selbst ob Punycode gezeigt wird
  - Extensions, welche die Anzeige erzwingen





https://www.malwarebytes.com/blog/threat-intelligence/2023/10/clever-malvertising-attack-uses-punycode-to-look-like-legitimate-website

Agenda

Lagebericht BSI und BKA

Ransomware

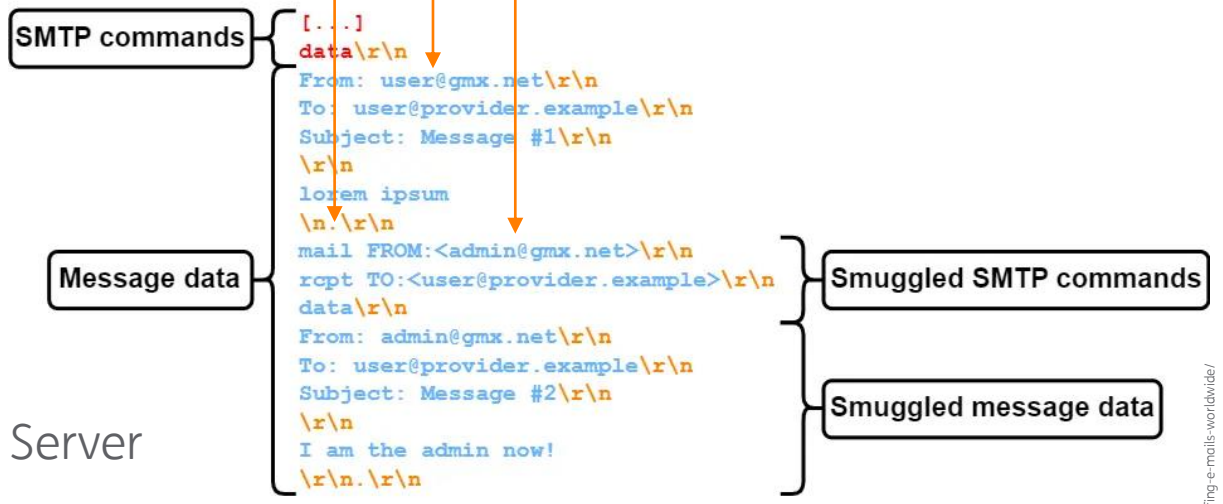
Angriff Microsoft Cloud: Storm-0558

KeePass-Malvertising

SMTP Smuggling

SMTP Smuggling

- Inspiriert von HTTP request smuggling
- CarriageReturn (\r) und LineFeed (\n)
- Cloud erlaubte cross-domain smuggling
  z.b. GMX -> admin@web.de
  MS365 -> admin@tesla.com
- DKIM, SPF, DMARC sind dabei gültig
- 2 Szenarien: Inbound und Outbound SMTP Server



2023-07-26:	Contacting MSRC
2023-07-27:	Contacting Cisco
2023-07-29:	Contacting GMX.
2023-08-10:	GMX fixed the issue
2023-08-17:	Contacting CERT Coordination Center (CERT/CC) for further discussion with Cisco
2023-08-23:	Microsoft responds and rates the vulnerability with moderate risk
2023-09-13:	CERT/CC accepts the case
2023-10-16:	SMTP smuggling in Exchange Online is fixed

12 Tage

82 Tage

https://sec-consult.com/blog/detail/smtp-smuggling-spoofing-e-mails-worldwide/

SMTP Smuggling

- für Phishing, CEO Fraud, … sehr problematisch
- OnPrem Mailserver
  - Postfix (CVE-2023-51764)
    - Fix und Workaround https://www.postfix.org/smtp-smuggling.html
  - Sendmail (CVE-2023-51765) -> kein Fix
  - Exim (CVE-2023-51766)
    - Fix mit 4.97.1 - https://bugs.exim.org/show_bug.cgi?id=3063
    - nur bei Konfiguration mit „pipelining“ betroffen
- Test-Tools
  - https://github.com/The-Login/SMTP-Smuggling-Tools
- Zeigt allgemein die Schwachstellen von E-Mail-Verkehr auf
  -> solche Probleme wären mit digitalen Signaturen vermeidbar (S/MIME, GPG/PGP)

https://sec-consult.com/blog/detail/smtp-smuggling-spoofing-e-mails-worldwide/

UMFRAGE

Anteil an digital signierten E-Mails in Ihrem Unternehmen

- < 5%
- 5-25%
- 26-50%
- 51-75%
- 76-100%

THOMAS KRENN®

Ausblick und Empfehlungen

- NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG)
  - Veröffentlichung im März 2024 geplant
  - muss bis 17. Oktober 2024 in Kraft treten
  - Nachweisprüfungen ab 2027 erwartet
- Qualifiziertes IT-Sicherheitspersonal entscheidend
- KI – Freund und Feind
- Heise Security Pro

https://sosafe-awareness.com/de/ressourcen/reports/cyberarime-trends-2023/

THOMAS KRENN®

Vielen Dank für Ihre Aufmerksamkeit!