Landesamt für Sicherheit in der Informationstechnik

Quo Vadis, IT-Sicherheit?

Dr. Thomas Kaiser / Abteilungsleiter Cybersicherheit/Technik
Landesamt für Sicherheit in der Informationstechnik

Agenda

- Vorstellung LSI
- Aktuelle Sicherheitslage
- Umgebung bayerisches Behördennetz
- Ausblick Cloud

Vorstellung LSI

- Bayern erstes Bundesland mit eigenem Landesamt
- LSI ist dem StMFH nachgeordnet – wie BayernServer
- Gründungszeitpunkt: 01.12.2017
- Ca. 155 Mitarbeiter

Nürnberg Ast. Bad Neustadt a.d.Saale Ast. Würzburg

Die Keimzelle

- Das Bayern-CERT aus 2003
- Mitglied im deutschen Cert-Verbund
- Mitglied im Verwaltungs-Cert-Verbund
- Seit Juli 2022 akkreditiert: TF-CSIRT

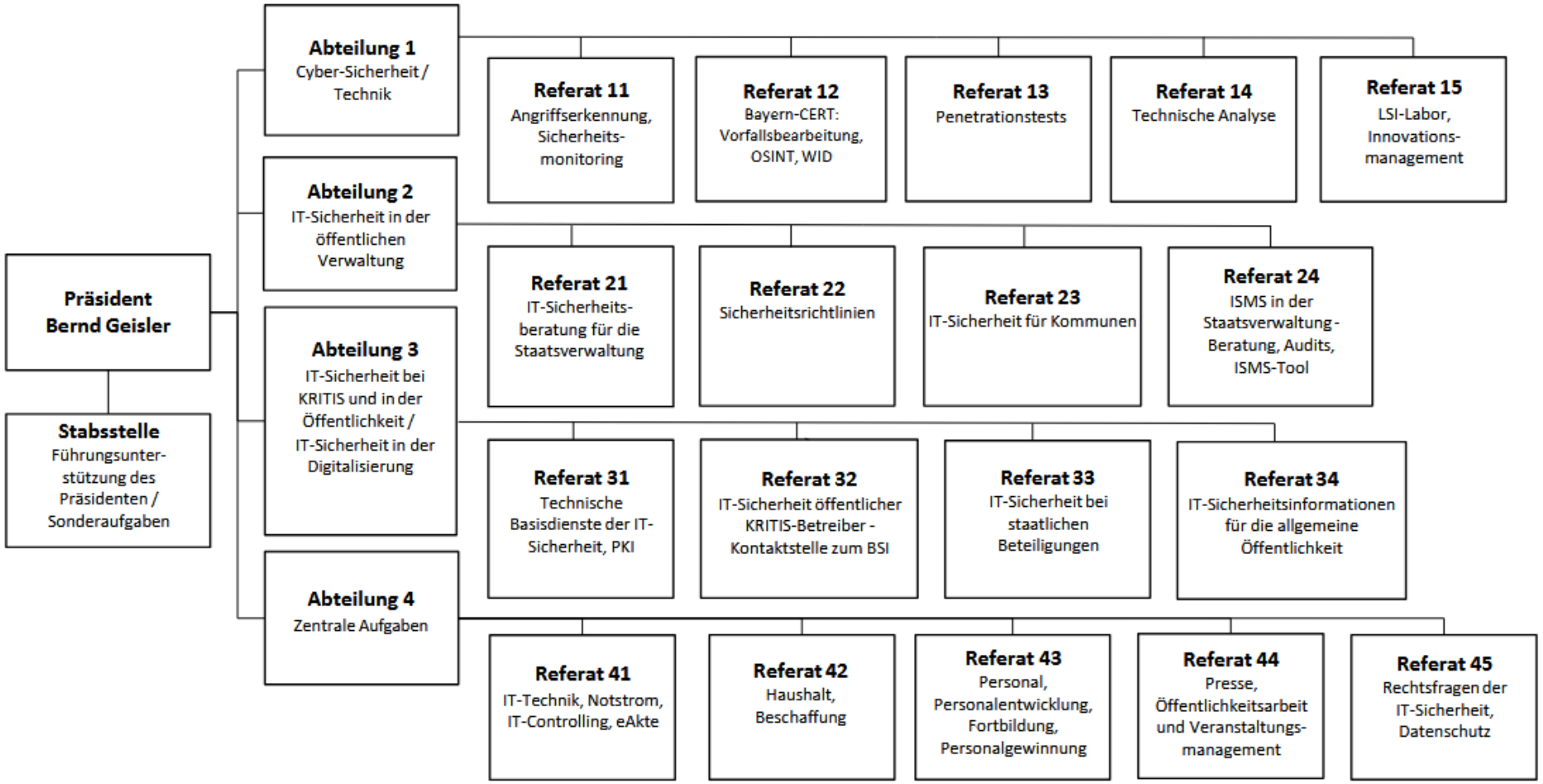
Aufgaben des LSI

- BayDiG Art. 42
- (1) Das Landesamt hat
  1. Gefahren für die Sicherheit der Informationstechnik an den Schnittstellen zwischen Behördennetz und anderen Netzen abzuwehren,
  2. die staatlichen und die sonstigen an das Behördennetz angeschlossenen Stellen bei der Abwehr von Gefahren für die Sicherheit in der Informationstechnik zu unterstützen,

     …
  7. als Computer-Notfallteam (CSIRT) im Sinne von Art. 10 der Richtlinie (EU) 2022/2555 die Aufgaben nach Art. 11 Abs. 3 der Richtlinie (EU) 2022/2555 wahrzunehmen

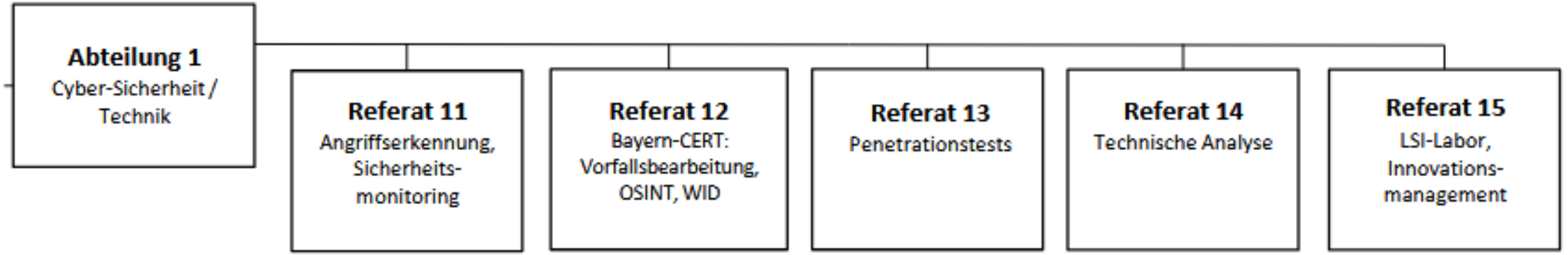
Organigramm des Landesamts für Sicherheit in der Informationstechnik

Stand 01.06.2024



Organigramm des Landesamts für Sicherheit in der Informationstechnik

Stand 01.06.2024



Landesamt für Sicherheit in der Informationstechnik

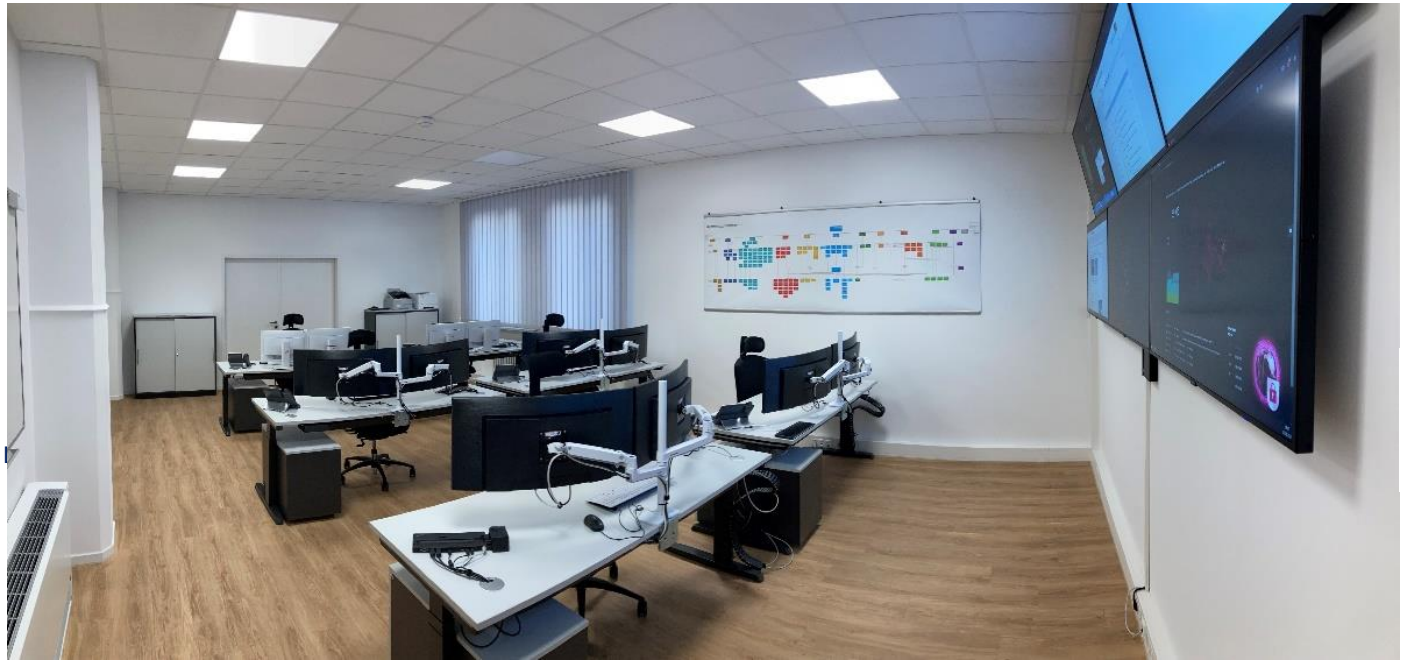
Unterstützung durch das Bayern-CERT / LSI Lagezentrum

LSI – Lagezentrum / Bayern-CERT

Telefon: 0911 / 21549-**999**
E-Mail: cert@bayern.de
Web: lsi.bybn.de / lsi.bayern.de

Erreichbarkeit

Mo. – Do.:	07:30 - 17:00 Uhr
Fr.:	07:30 - 15:00 Uhr



ACCREDITED BY TRUSTED INTRODUCER

VCV VerwaltungsCERTVerbund

CERT Bund

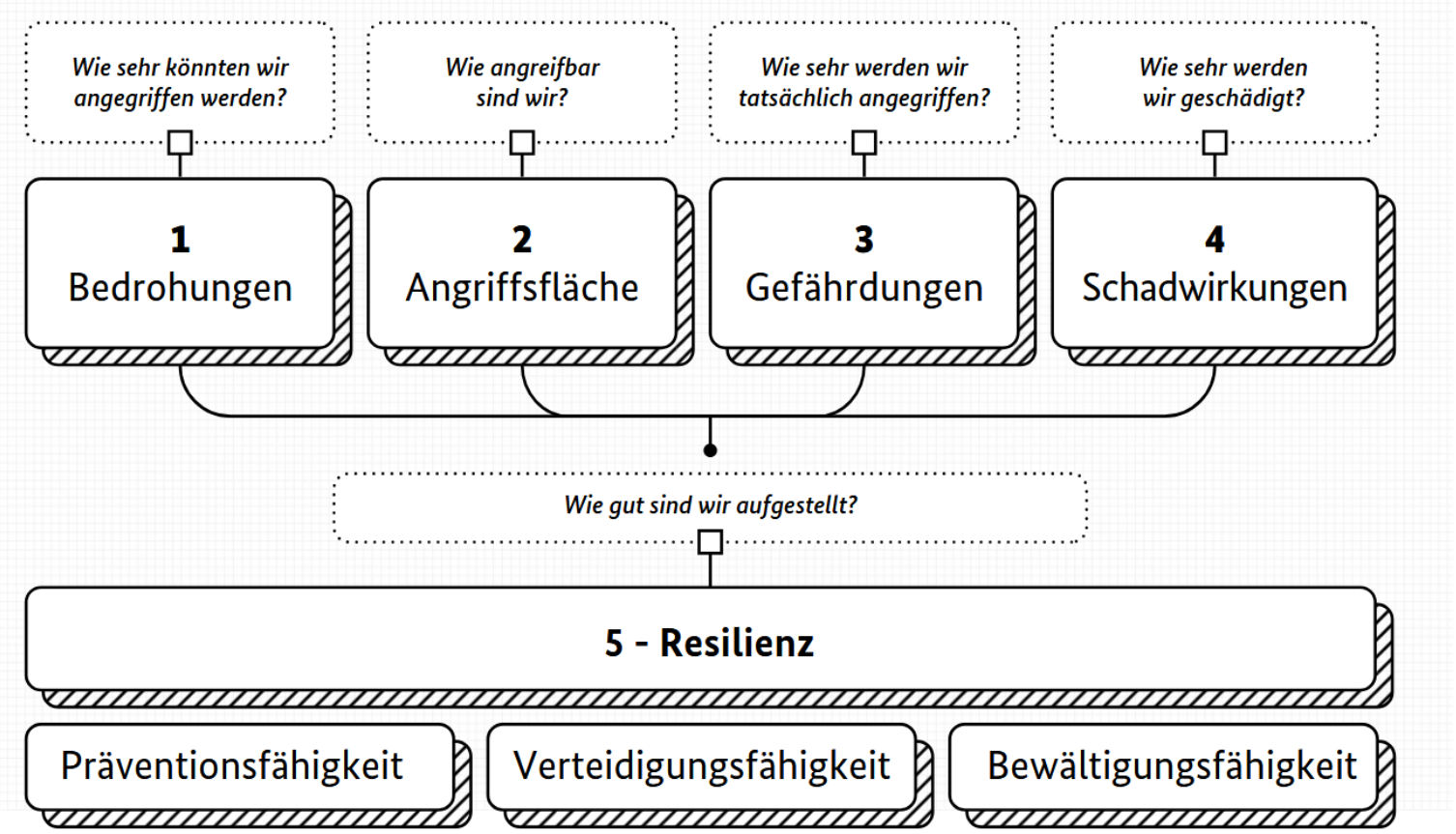
Auswirkungen NIS2.0

- EU-Richtline Netz- und Informationssicherheit
- Betroffenheit nach Umsatz und Mitarbeiter in der Wirtschaft
- Verwaltung nur Einrichtungen mit besonderer Bedeutung für den Binnenmarkt (EBB)
- Einbindung der Kommunen per BayDiG
- LSI Ausweitung der Erreichbarkeit

Agenda

- Vorstellung LSI
- Aktuelle Sicherheitslage
- Umgebung bayerisches Behördennetz
- Ausblick Cloud

BSI-Bericht 2024 Systematik



https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2024.html

BSI-Bericht 2024

- Bedrohungslage
  - Ransomware und APTs
- Angriffsfläche
  - Anstieg der Schwachstellen (insbesondere Sicherheitskomponenten)
- Gefährdungslage
  - DDoS
  - Ransomware

BSI-Bericht 2024 (II)

- Gefährdungslage
  - DDoS-Angriffe
  - Ransomware-Angriffe
  - Angriffe auf Cloud-Infrastrukturen
  - Angriffe auf Politische Organisationen
- Schadwirkungen
  - Ausfall kommunaler Dienstleister
  - Anstieg der Datenleaks aus Ransomware

BSI-Bericht 2024 (III)

- Resilienz
  - Takedowns von Akteuren
  - Resilienz in der Bundesverwaltung
  - Resilienz in Cloud-Infrastrukturen

Microsoft Digital Defense Report 2024

- Report basierend auf Windows Telemetry
- Internationaler Blick auf IT-Sicherheit
- Anstieg der Identity Attacks
- AI basierende Attacken
- Secure Future Initiative (SFI)

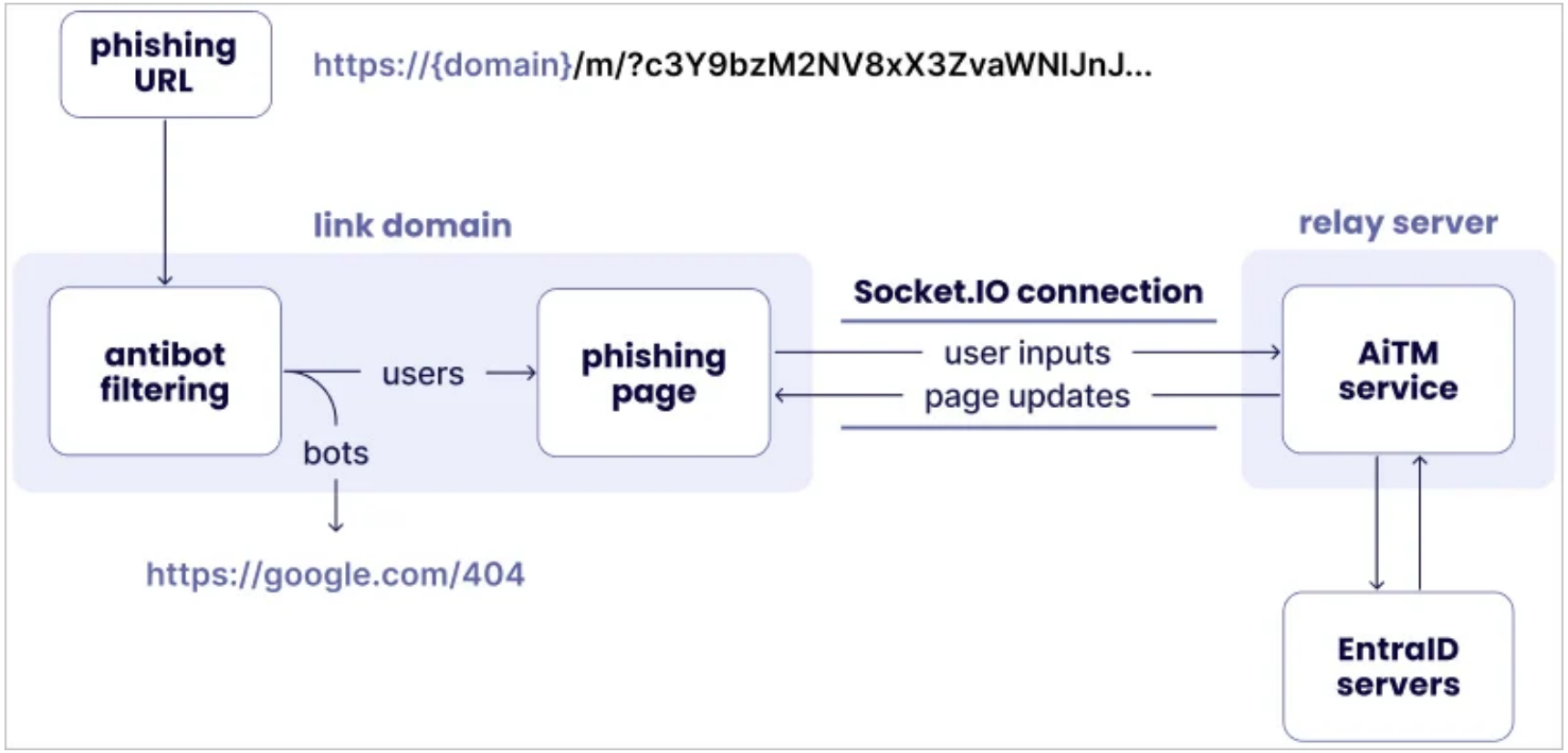
- Vorfälle Sommer 2023 CISA Bericht: https://www.cisa.gov/sites/default/files/2024-04/CSRB_Review_of_the_Summer_2023_MEO_Intrusion_Final_508c.pdf

https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2024

Angriffsvektoren der Vorfälle im LSI

- SW-Fehler in Sicherheitskomponenten
- Abfangen von MFA /TOTP
- Kommunale Vorfälle
  - Admin Accounts mit schwachen Passwörtern am VPN-GW
  - Ungepatchte Sicherheitskomponenten
  - Schwache Passwörter/Phishing
- Angriffsversuche per Spear-Phishing

Adversary in the Middle: Mamba 2FA



Source: Sekoia

Verschiedenste Angriffe auf die IT-Systeme

- Angriffe auf Anwendungen
  - Fachverfahren → z.B. Log4j
  - Mitarbeiterplattformen → z.B. ProxyLogon/ProxyShell gegen Exchange-Plattform
- Angriffe auf Sicherheitskomponenten & Infrastruktur
  - Firewalls & VPN-Zugangssysteme
    → z.B. Kampagne gegen Sonicwall-VPN oder Ivanti-Geräte
  - DDoS-Angriffe
- Angriffe auf den User
  - Social Engineering
  - Phishing/Smishing
  - Nachrichten mit standalone Schadcode

Aktuelle Vorfälle

USA: AT&T, Verizon und Co. angeblich von chinesischer Spionagegruppe infiltriert

US-Netzbetreiber sollen ins Visier einer chinesischen Cyberspionagegruppe geraten sein. Sie sei in Überwachungssysteme eingedrungen.

12

(Bild: Gorodenkoff/Shutterstock.com)

07.10.2024, 07:38 Uhr Lesezeit: 1 Min. | Security

Wegem schwerem Cyberangriff auf US-Provider: FBI wirbt für Verschlüsselung

Die mutmaßlich aus China stammenden Angreifer auf US-Provider sind noch immer in den Netzen. Nun plädiert das FBI dafür, Kommunikation zu verschlüsseln.

41

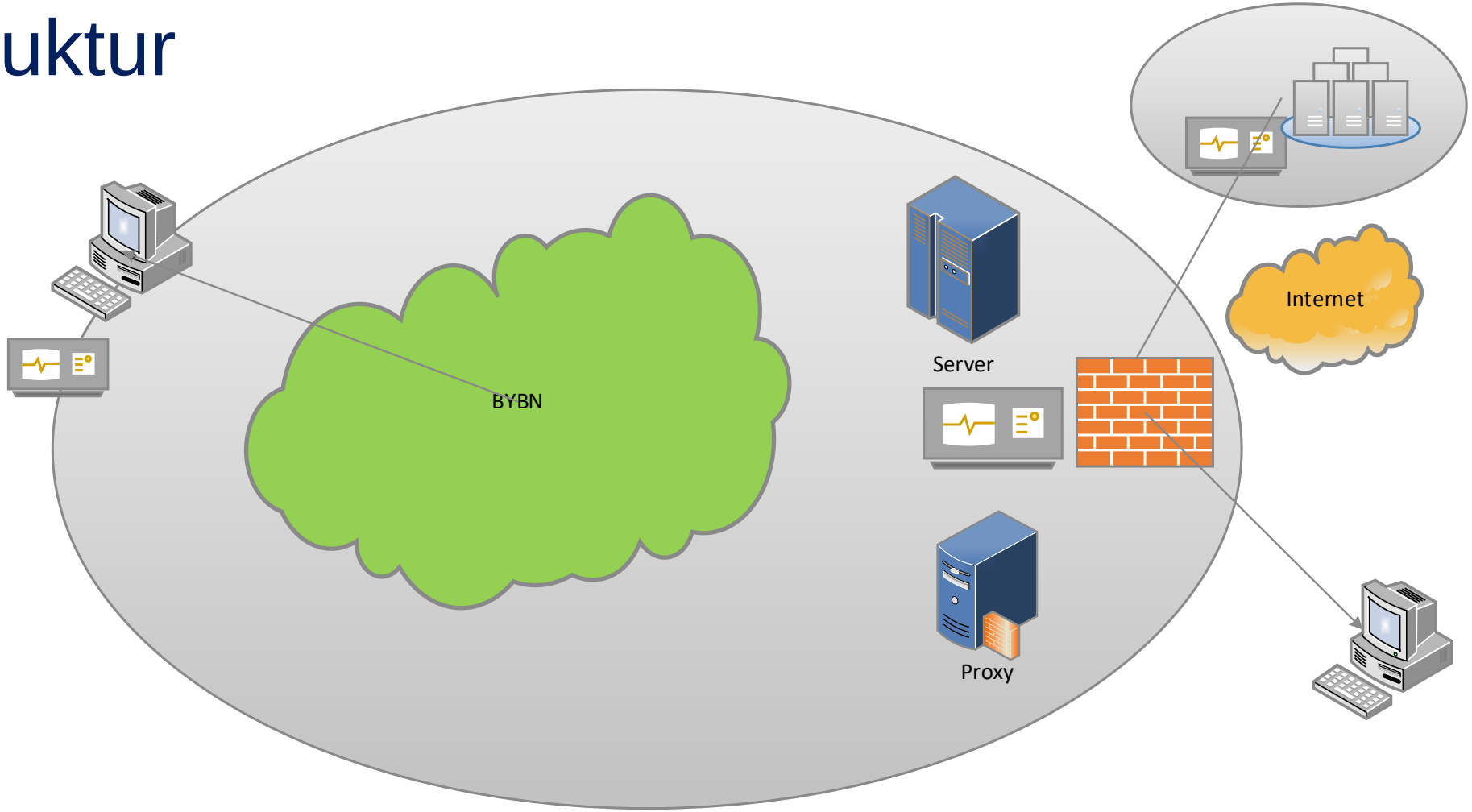
(Bild: Skorzewiak/Shutterstock.com)

07:07 Uhr Lesezeit: 3 Min.

Agenda

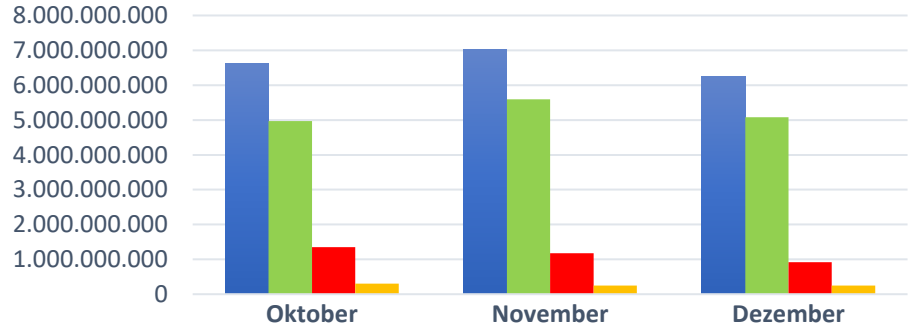
- Vorstellung LSI
- Aktuelle Sicherheitslage
- Umgebung bayerisches Behördennetz
- Ausblick Cloud

Infrastruktur



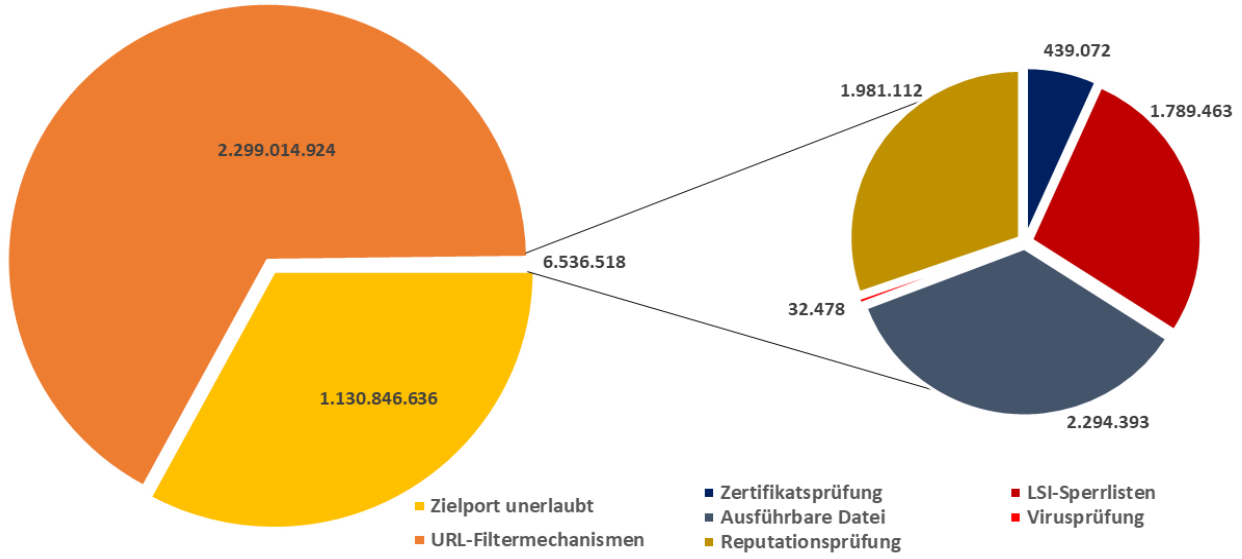
Kennzahlen zu zentralen Sicherheitsinstanzen

Anzahl der URL-Aufrufe nach Ergebnis

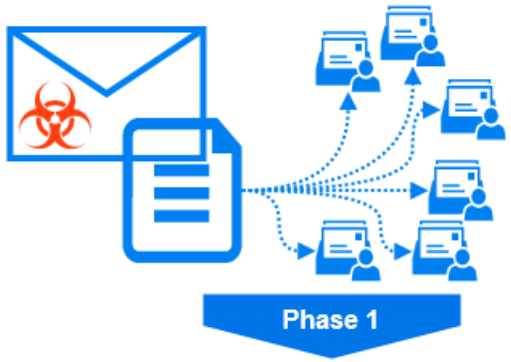


	Oktober	November	Dezember
Aufrufe gesamt	6.625.173.222	7.015.887.678	6.251.046.525
Aufrufe erfolgreich	4.966.853.346	5.600.077.206	5.082.805.214
Aufrufe geblockt	1.351.820.345	1.169.349.844	915.008.353
Aufrufe fehlerhaft	301.584.927	241.320.546	248.271.329

Anzahl geblockter URL-Aufrufe nach Ursache



Emotet – ein typisches Angriffsszenario



Phase 1

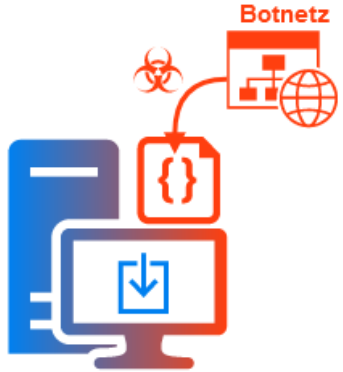
Spear-Phishing

- Versand von schadhaften E-Mails an viele Empfänger
- Nutzung zuvor abgeflossener E-Mail-Kommunikation und Kontaktbeziehungen
- Versand erfolgt in Kampagnen/Wellen

Einfallsvektor Mensch

- Durch Vortäuschung valider Inhalte wird der Empfänger dazu gebracht Links aufzurufen und/oder Dokumente zu öffnen

Phase 2



Phase 3

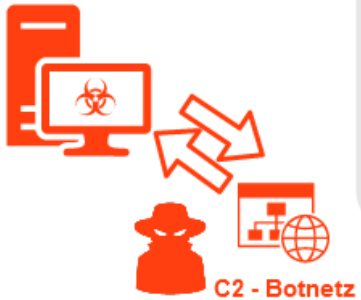
Infektion des Endgeräts

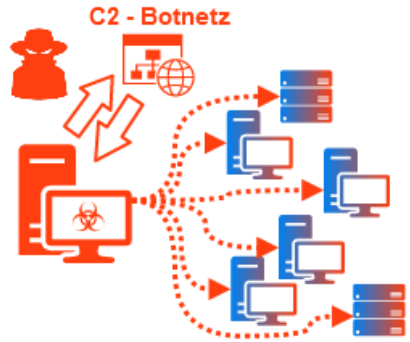
- Durch eingebettete Makros oder das direkte Öffnen ausführbarer Dateien kommt es zur Ausführung eines initialen Schadcodes, der weiteren Schadcode vom Botnetz des Angreifers nachlädt

Kontrolle durch den Angreifer

- Es wird eine Verbindung zu sog. Command-and-Control-Servern (C2) aufgebaut
- Der Angreifer hat damit die volle Kontrolle über den Rechner des Nutzers
- Es werden Nutzerdaten wie Mails, Passwörter usw. exfiltriert

Phase 4





Phase 5

Verbreitung im Netzwerk

- Einmal im Netz versuchen sich die Angreifer auf weitere Systeme im Netz auszubreiten
- Es wird versucht die Rechte auf den Endgeräten und im Netzwerk zu erweitern

Verschlüsselung und Erpressung mit Ransomware

- Es kommt zur Verschlüsselung von Endgeräten und Netzwerkspeichern
- Anschließend wird das Opfer sowohl mit den abgeflossenen internen Daten als auch der Herausgabe des Decryption-Keys erpresst

Phase 6

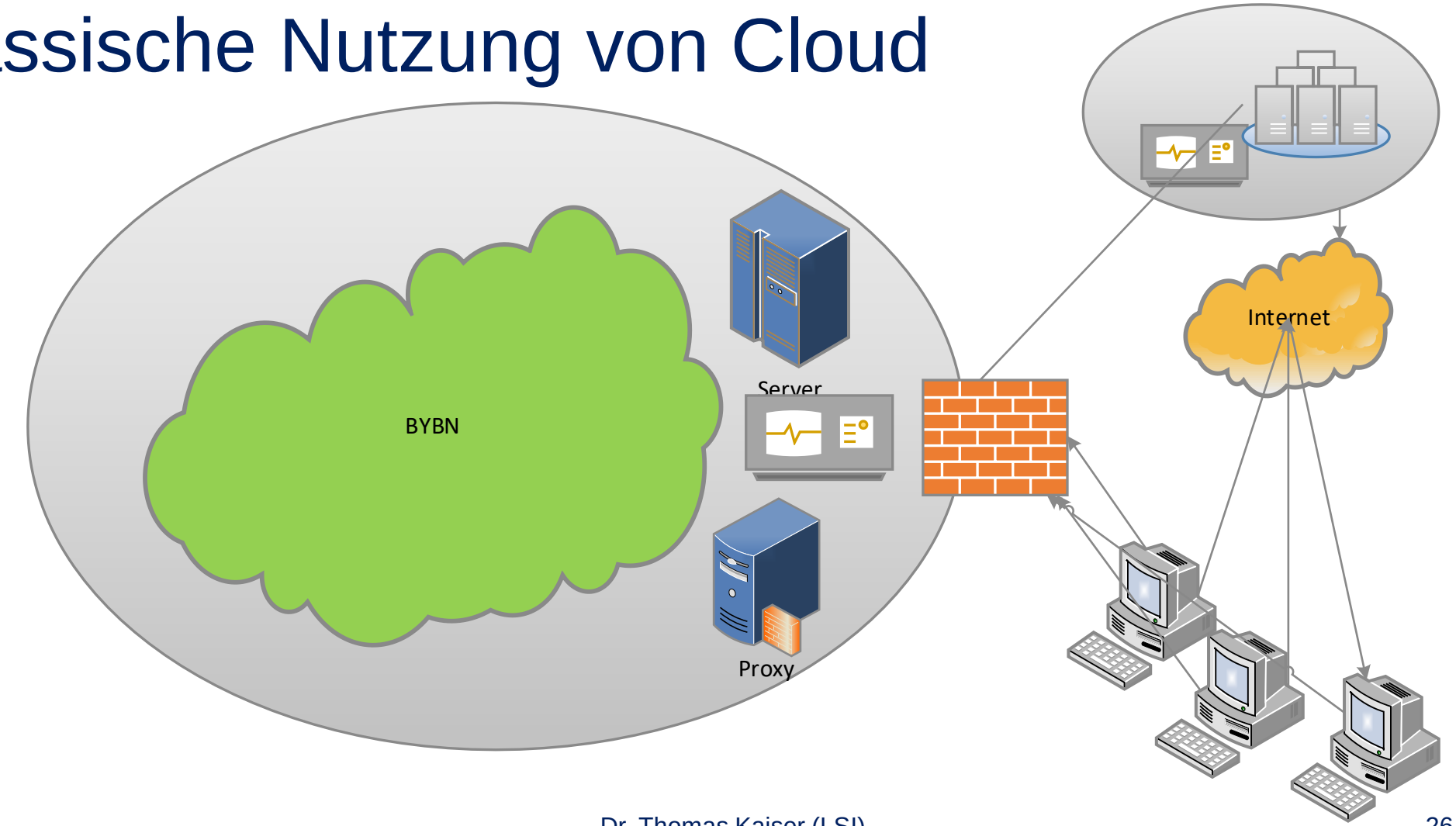
Status Quo IT-Sicherheit im BYBN

- Stark kontrollierte Netzwerkumgebung in Betrieb des IT-DLZ:
  - Mehrstufige Firewalls
  - Proxy mit statischer/dynamischer Filterliste aus IoC-Gewinnung
  - Mail-GW/Sandbox mit dynamischer Einspielung IoCs
  - Laufende Nachsteuerung der Infrastruktur
  - Überwachung des internen Netzverkehrs auf Auffälligkeiten
- Dezentrales Clientmanagement aus Sicht LSI

Agenda

- Vorstellung LSI
- Aktuelle Sicherheitslage
- Umgebung bayerisches Behördennetz
- Ausblick Cloud

Klassische Nutzung von Cloud



Hybrid BYBN / Cloud

- Cloud
  - Zero-Trust als wesentlicher Baustein „Identity Perimeter“
  - Client zentral gemanaged und per EDR überwacht
  - Netzwerk kaum überwacht
  - Starke Absicherung der Anwendungen und Monitoring
  - Fehlende Segmentierung
- Mehrstufige Absicherung nicht mehr möglich

Herausforderungen Cloud

- Cloud ist stark exponiert
- Kaum Segmentierung von Kunden in der Cloud
- Hochdynamisches Umfeld, kontinuierliches Patchen
- Starke Virtualisierung der Umgebung
- SaaS „as is“, keine kundenspezifischen Sicherheitsmechanismen
- „Digitale Souveränität“?

Digitale Souveränität ⇔ Komfort

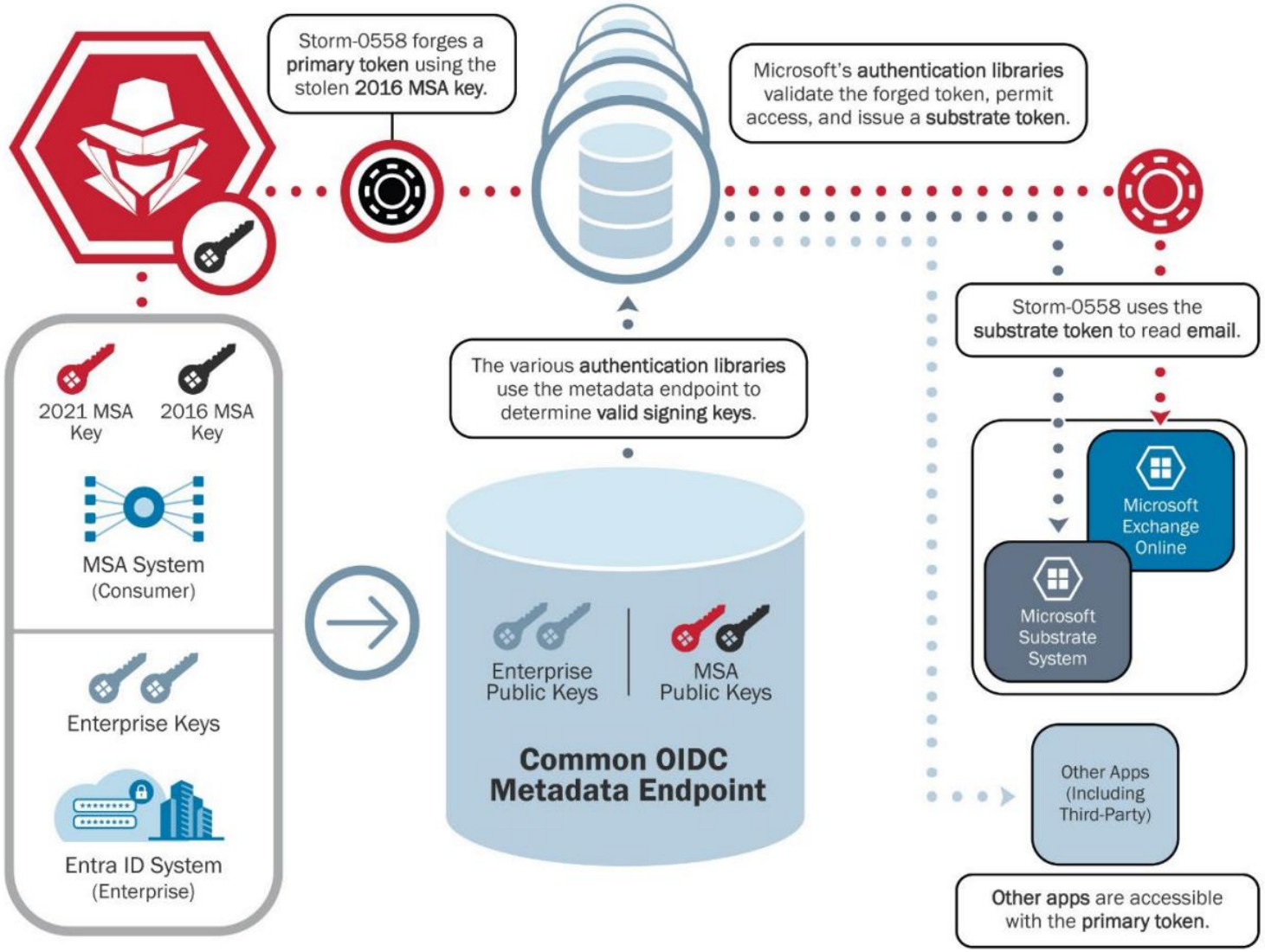
- Allgemeine Public-Cloud nur für öffentliche Daten!
- Zusatzmaßnahmen notwendig
- Einführung starke MFA
- Verschlüsselung
  - Transport
  - At Rest
  - At Use
- OpenSource als Lösung?

Microsoft: Betrachtete Sicherheitsvorfälle

1. Vorfälle Sommer 2023 (MSA Token, Storm 0558)
   https://www.dhs.gov/news/2024/04/02/cyber-safety-review-board-releases-report-microsoft-online-exchange-incident-summer
2. Midnight Blizzard/APT29 Januar 2024
   https://www.cisa.gov/news-events/directives/ed-24-02-mitigating-significant-risk-nation-state-compromise-microsoft-corporate-email-system

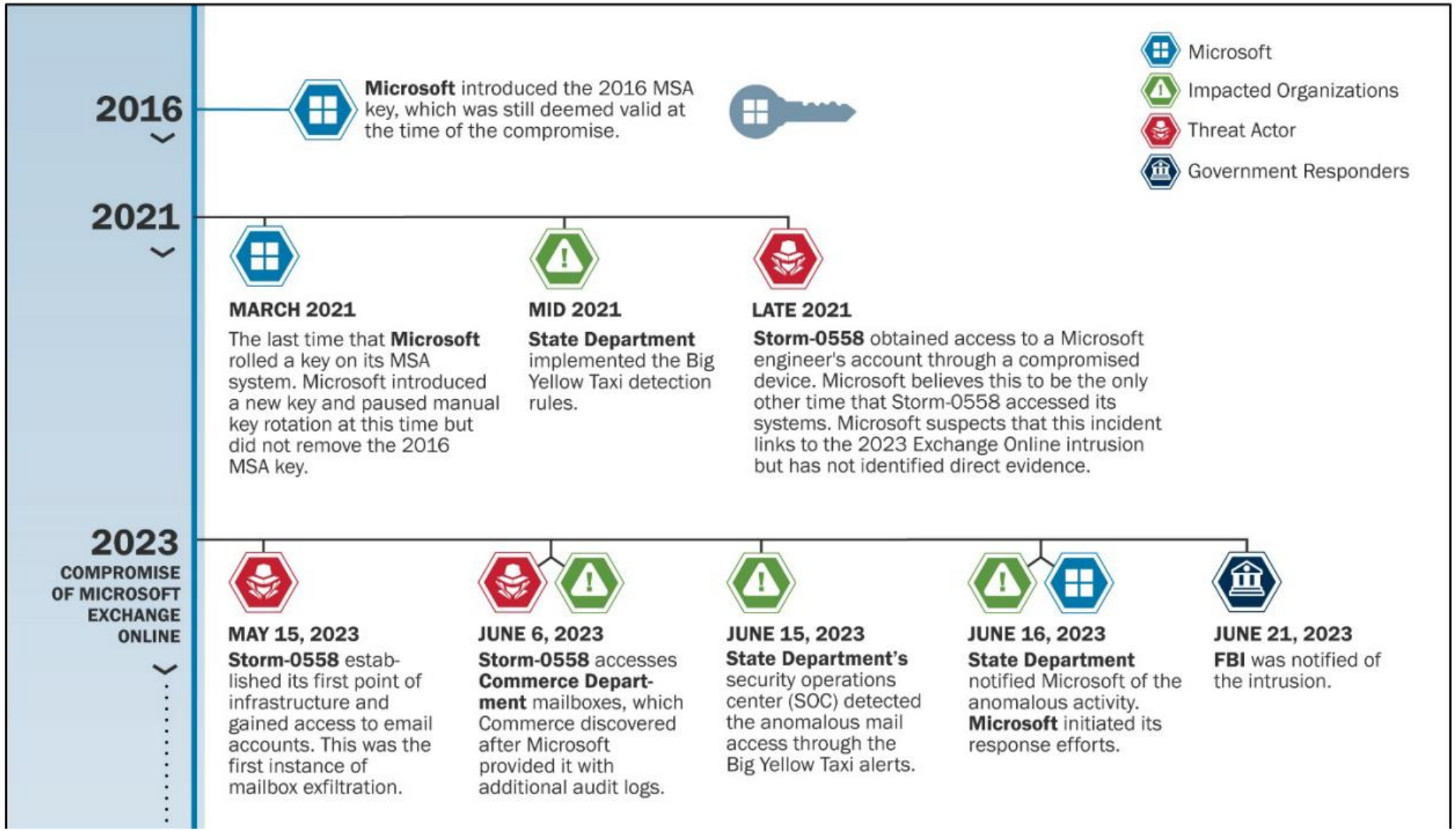
Ablauf

* Aus CSRB Report



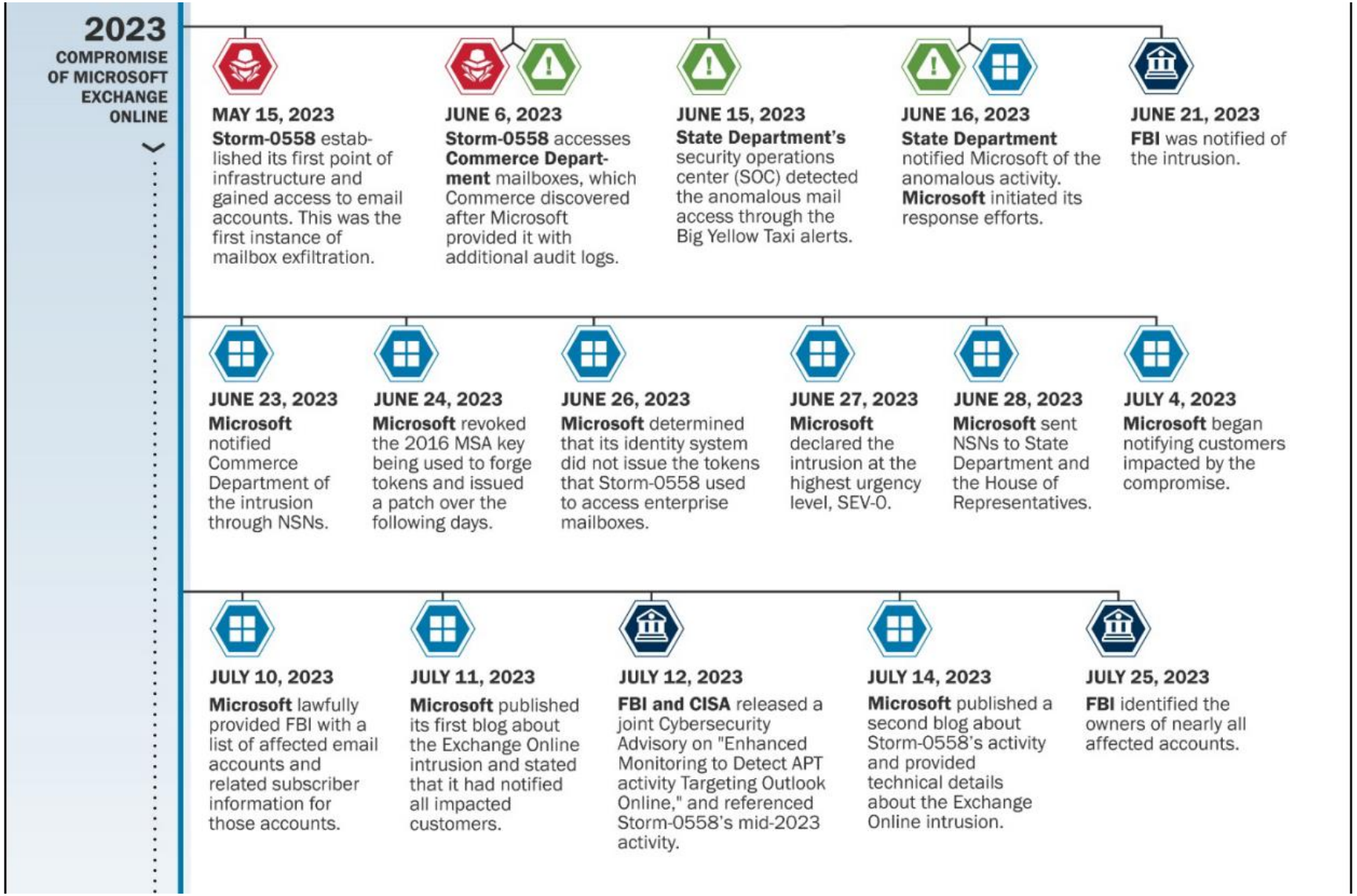
Zeitlicher Ablauf

* Aus CSRB Report



Zeitlicher Ablauf

* Aus CSRB Report



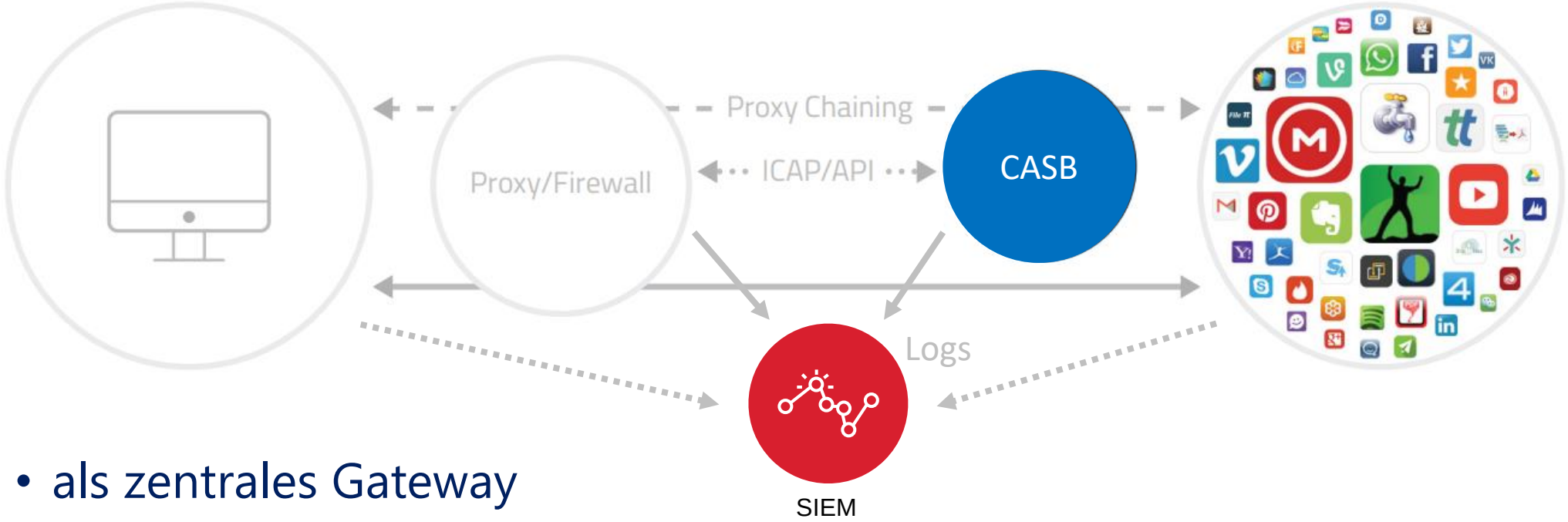
Risiken Microsoft/M365

- Schwerpunkt SaaS, Sicherheitsmechanismen vorgegeben
- „Insecure by Default“, siehe CISA Bericht
- Keine mehrstufige Abwehr „Defense of Depth“
- Beispiele für Vorfälle
  - Zugriff auf interne Systeme und Code (APT29) in März 2024
  - Zugriff auf interne Mails (APT29) in Januar 2024
  - Abfluss interner Daten von MS (Zugriffsproblem) in September 2023
  - Verlust Signing Key (STORM-0558) festgestellt Juni 2023

Ausblick Cloud-Nutzung im BYBN

- Cloud wird allgegenwärtig
- Abgestufte Nutzung notwendig, datenorientierter Ansatz
- Voraussetzungen der Industrie fehlen noch
  - Etabliertes Zero Trust
  - Zentrales Clientmanagement
- Einführung neuer Schutzmechanismen ZTNA//SASE/CASB insbesondere für SaaS-Dienste

CASB - Einsatzmodelle



- als zentrales Gateway
- als API-Anwendung

Quo Vadis, IT-Sicherheit?

- Nutzung von Cloud-Diensten steigt
- Sicherheitstechnische Kompensation ist notwendig
- Einführung MFA, am besten starke MFA
- Überlegter Umgang bei Nutzung externer Dienste
- IT-Sicherheit ist notwendige Voraussetzung

Vielen Dank für Ihre Aufmerksamkeit!
Fragen?