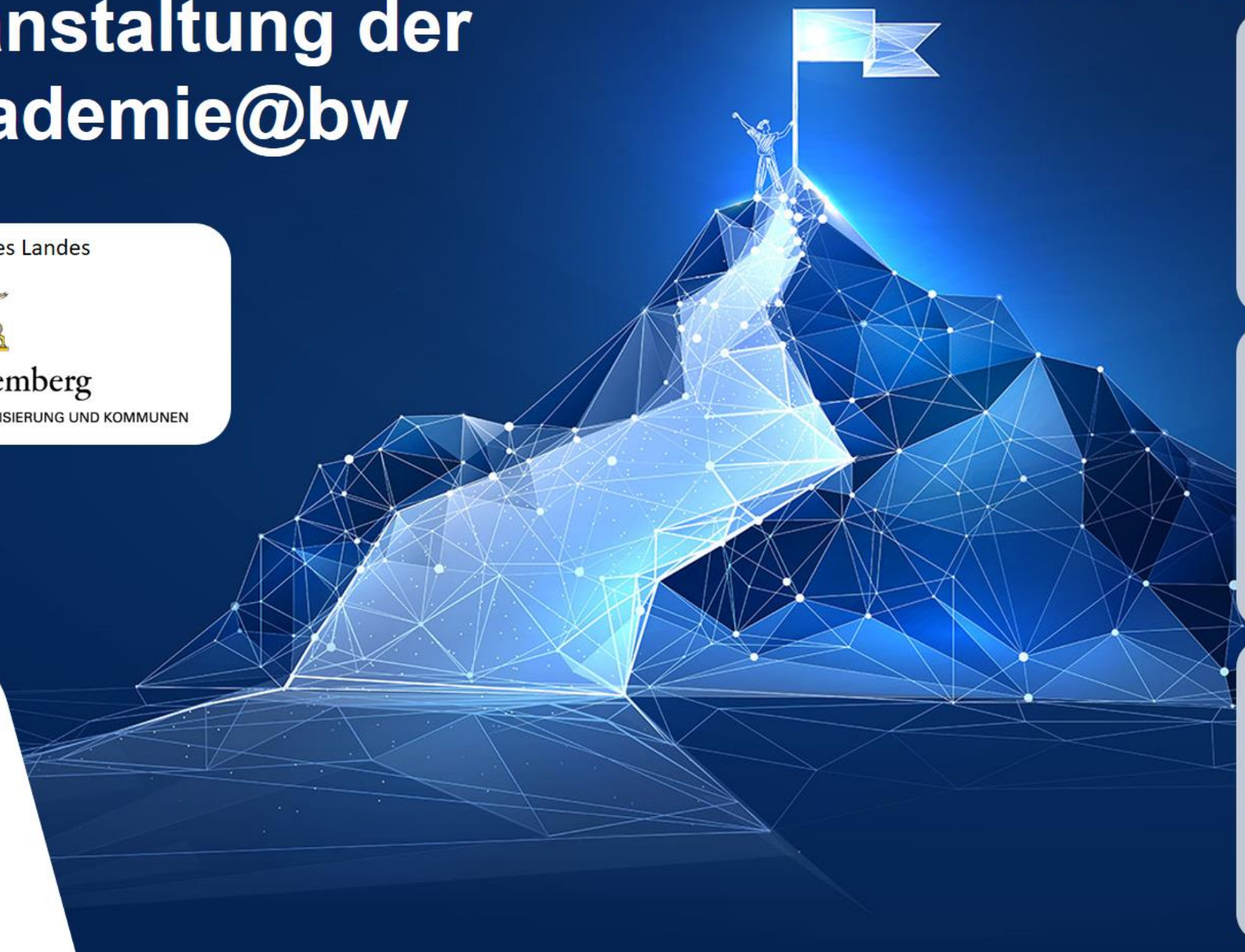
Eine Veranstaltung der Digitalakademie@bw

Ein Förderprojekt des Landes

Baden-Württemberg

MINISTERIUM DES INNEREN, FÜR DIGITALISIERUNG UND KOMMUNEN



digitalakademie@bw

Immer auf dem Laufenden bleiben …

LinkedIn

Instagram

Website

Torsten Seeberg

Landeskriminalamt Baden-Württemberg

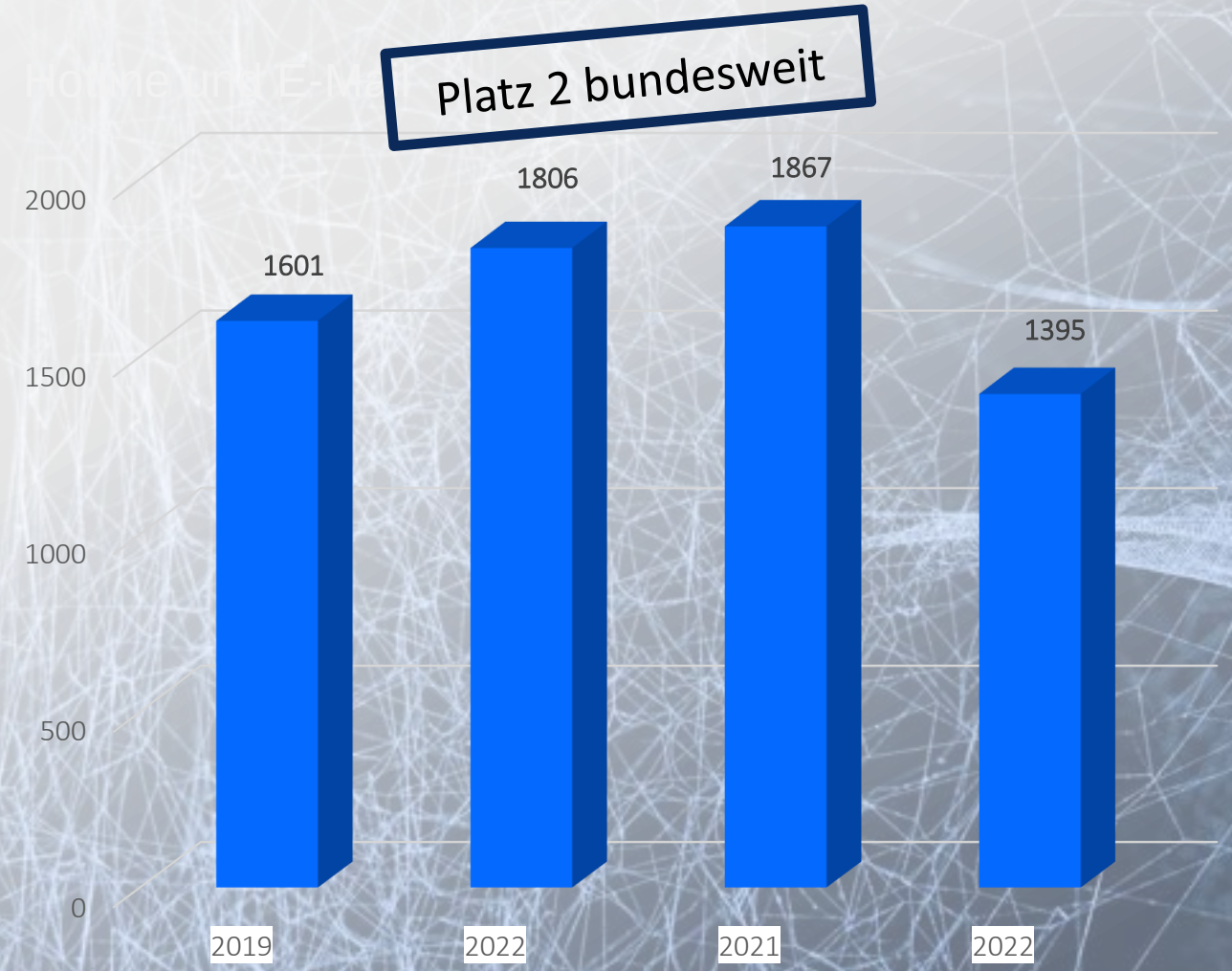
Zentrale Ansprechstelle Cybercrime (ZAC)

Taubenheimstraße 85 · 70372 Stuttgart
Telefon: 0711 5401 - 2444
Webseite: lka.polizei-bw.de/zac

Zentrale Ansprechstelle Cybercrime (ZAC)

- polizeiliche Kontaktstelle für Institutionen in BW
- 24/365
- Beratung und Anzeigenaufnahme
- Prävention: Unterlagen, Warnmeldungen, Awareness-Vorträge, Übungen für KRITIS, Messestände
- Einrichtung im Jahr 2012
- national und international vernetzt
- 17 ZAC-Dienststellen bundesweit (www.polizei.de/zac)

Zentrale Ansprechstelle Cybercrime (ZAC)

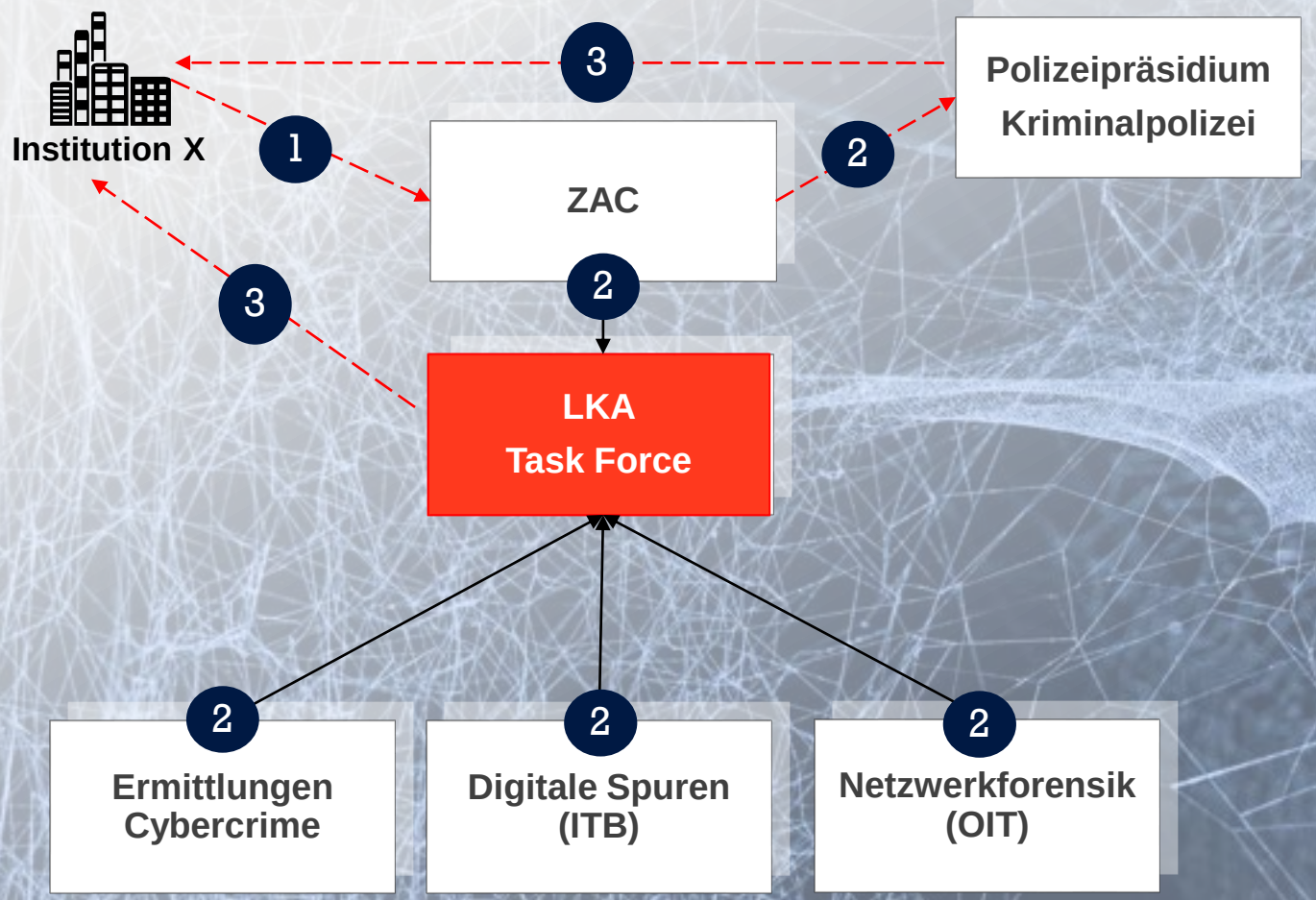


Kritische Sektoren

„Kritische Infrastrukturen (KRITIS) sind Organisationen oder Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden."

KRITIS-Definition der Bundesressorts

Kritische Sektoren

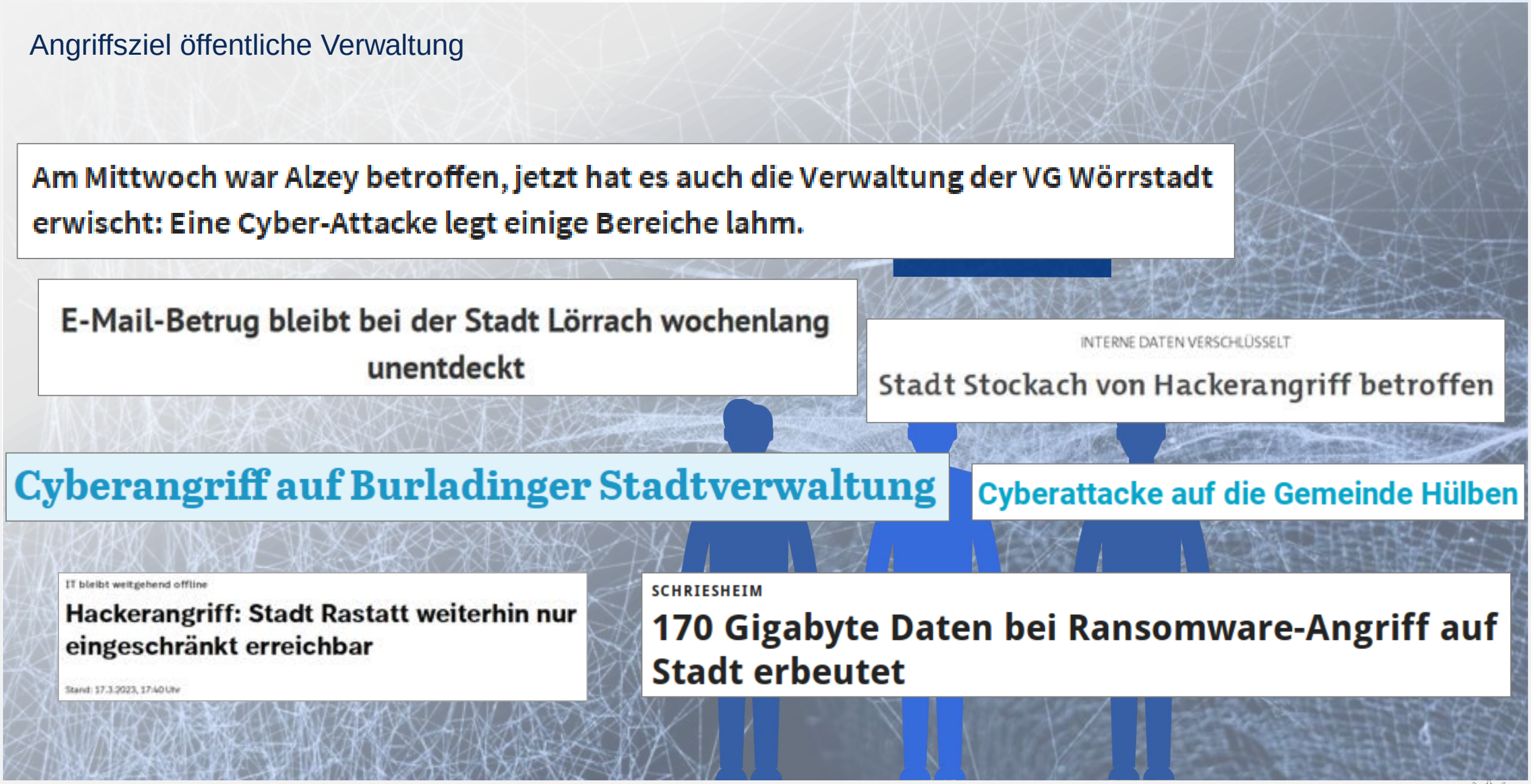


Angriffsziel öffentliche Verwaltung

Art. 28 II GG - Kommunale Selbstverwaltung

- Kommunen sind Adressaten eventueller Schadenersatzforderungen betroffener Bürger und Institutionen gem. Art. 82 DSGVO

Angriffsziel öffentliche Verwaltung



Angriffsziel öffentliche Verwaltung – Cyberangriff gegen Rechenzentrum mehrerer NRW-Kommunen

WDR

Wetter

Nachrichten | Sport | Wissen | Verbraucher | Kultur | Unterhaltung

Hackerangriff stellt NRW-Kommunen weiter vor große Probleme

Stand: 02.11.2023, 16:42 Uhr

Nach dem Hackerangriff am Wochenende können Bürgerinnen und Bürger in verschiedenen Städten und Gemeinden kaum Behördengänge erledigen. Betroffen sind vor allem das südliche und östliche Nordrhein-Westfalen, aber auch einzelne Kommunen im Ruhrgebiet.

Angriffsziel öffentliche Verwaltung – Cyberangriff gegen Rechenzentrum mehrerer NRW-Kommunen

Angriffsziel öffentliche Verwaltung – Cyberangriff gegen Rechenzentrum mehrerer NRW-Kommunen

- Protokollierungsintervall unzureichend (3 Wochen)
- Protokollierung teilweise deaktiviert (Events, interne Firewall)
- zufällige interne IP-Zuweisung

---> Vereitelung valider forensisch fundierter Ergebnisse, überwiegend Vermutungen + Rückgriff auf Malware-Logs erforderlich…

Angriffsziel öffentliche Verwaltung – Cyberangriff gegen Rechenzentrum mehrerer NRW-Kommunen

- VPN veraltet + ohne MFA
- Keine Segmentierung
- keine weitere interne Authentisierung
- Bruteforce @ VPN-Konten möglich
- Passwort Domänen-Admin seit 2014 unverändert in GPO
- Veraltete Firewallverwaltung - CISCO ASA (0-day???)

Angriffsziel öffentliche Verwaltung – Cyberangriff gegen Rechenzentrum mehrerer NRW-Kommunen

- **18.10.23 Kompromittierung**
- Login mittels User-Account (VPN) mit IPs aus USA und NL
- Erlangung Domain-Admin-Status innerhalb Domäne
- Eine Domäne für 770 Server und 4176 Clients
- RDP-Login mehrere Domänen-Controller
- vielfältige Verwendung Powershell
- Advanced IP-Scanner initialisiert – durch EPP detektiert, jedoch administrativ nicht unterbunden.
- NetScan und weitere Tools initialisiert
- Hunderte SMB-Login-Versuche
- versuchter Zugriff auf Veeam
- erfolgreiche Manipulation (Exlusion) der AV für C:
- AV detektiert Ransomware, jedoch administrativ nicht unterbunden.
- **29.10.23 Verschlüsselung** mehrerer Domain-Controller mittels w.exe unter Verwendung Powershell ---> mind. 12 Tage nach Intrusion

Angriffsziel öffentliche Verwaltung – Cyberangriff gegen Rechenzentrum mehrerer NRW-Kommunen

Home / Cisco Security / Security Advisories

Cisco Security Advisory

Cisco Adaptive Security Appliance Software and Firepower Threat Defense Software Remote Access VPN Unauthorized Access Vulnerability

Medium

Advisory ID:	cisco-sa-asaftd-ravpn-auth-8LyfCkeC	CVE-2023-20269
First Published:	2023 September 6 16:00 GMT	
Last Updated:	2023 October 11 14:59 GMT	
Version 1.4:	Final	
Workarounds:	Yes	
Cisco Bug IDs:	CSCwh23100	
	CSCwh45108	
CVSS Score:	Base 5.0	

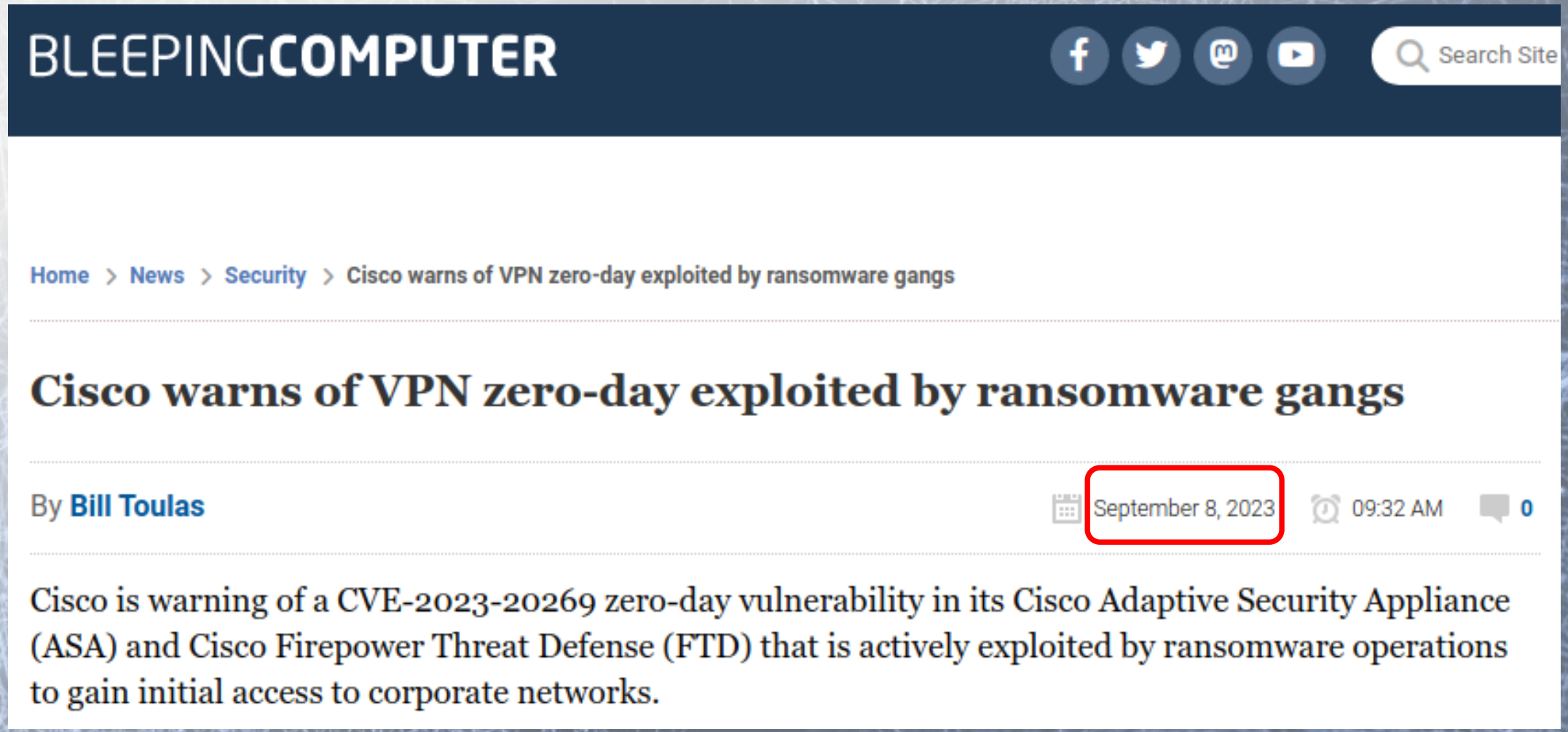
Angriffsziel öffentliche Verwaltung – Cyberangriff gegen Rechenzentrum mehrerer NRW-Kommunen

Auszug Cisco-Warnmeldung:

- Establish a clientless SSL VPN session (only when running Cisco ASA Software Release 9.16 or earlier).

verwendet wurde 9.12x

Angriffsziel öffentliche Verwaltung – Cyberangriff gegen Rechenzentrum mehrerer NRW-Kommunen



BLEEPINGCOMPUTER

Search Site

Home > News > Security > Cisco warns of VPN zero-day exploited by ransomware gangs

Cisco warns of VPN zero-day exploited by ransomware gangs

By **Bill Toulas**

September 8, 2023 09:32 AM 0

Cisco is warning of a CVE-2023-20269 zero-day vulnerability in its Cisco Adaptive Security Appliance (ASA) and Cisco Firepower Threat Defense (FTD) that is actively exploited by ransomware operations to gain initial access to corporate networks.

Angriffsziel öffentliche Verwaltung – Cyberangriff gegen Rechenzentrum mehrerer NRW-Kommunen

The medium severity zero-day vulnerability impacts the VPN feature of Cisco ASA and Cisco FTD, allowing unauthorized remote attackers to conduct brute force attacks against existing accounts.

By accessing those accounts, the attackers can establish a clientless SSL VPN session in the breached organization's network, which can have varying repercussions depending on the victim's network configuration.

Last month, BleepingComputer reported that the Akira ransomware gang was breaching corporate networks almost exclusively through Cisco VPN devices, with cybersecurity firm SentinelOne speculating that it may be through an unknown vulnerability.

Mitigating the flaw

Cisco will release a security update to address CVE-2023-20269, but until fixes are made available, system administrators are recommended to take the following actions:

- Use DAP (Dynamic Access Policies) to stop VPN tunnels with DefaultADMINGroup or DefaultL2LGroup.
- Deny access with Default Group Policy by adjusting vpn-simultaneous-logins for DfltGrpPolicy to zero, and ensuring that all VPN session profiles point to a custom policy.
- Implement LOCAL user database restrictions by locking specific users to a single profile with the 'group-lock' option, and prevent VPN setups by setting 'vpn-simultaneous-logins' to zero.

Cisco also recommends securing Default Remote Access VPN profiles by pointing all non-default profiles to a sinkhole AAA server (dummy LDAP server) and enabling logging to catch potential attack incidents early.

Finally, it is crucial to note that multi-factor authentication (MFA) mitigates the risk, as even successfully brute-forcing account credentials wouldn't be enough to hijack MFA-secured accounts and use them to establish VPN connections.

Allgemeine Prävention: Schwerpunkt Phishing

Angriffstaktiken „Phishing“

- Massendelikt: SPAM-Nachrichten
  - E-Mail
  - Karriereportale, Social Messenger-Dienste, Whatsapp…
  - SMS (Paketbenachrichtigung, Zoll-Gebühren…)

  SPAM-Anrufe
  - „Microsoft“-Scam
  - „Interpol“
  - Paypal
  - IT-“Support“

  Online
  - Search-Engine-Poisoning
  - PopUps

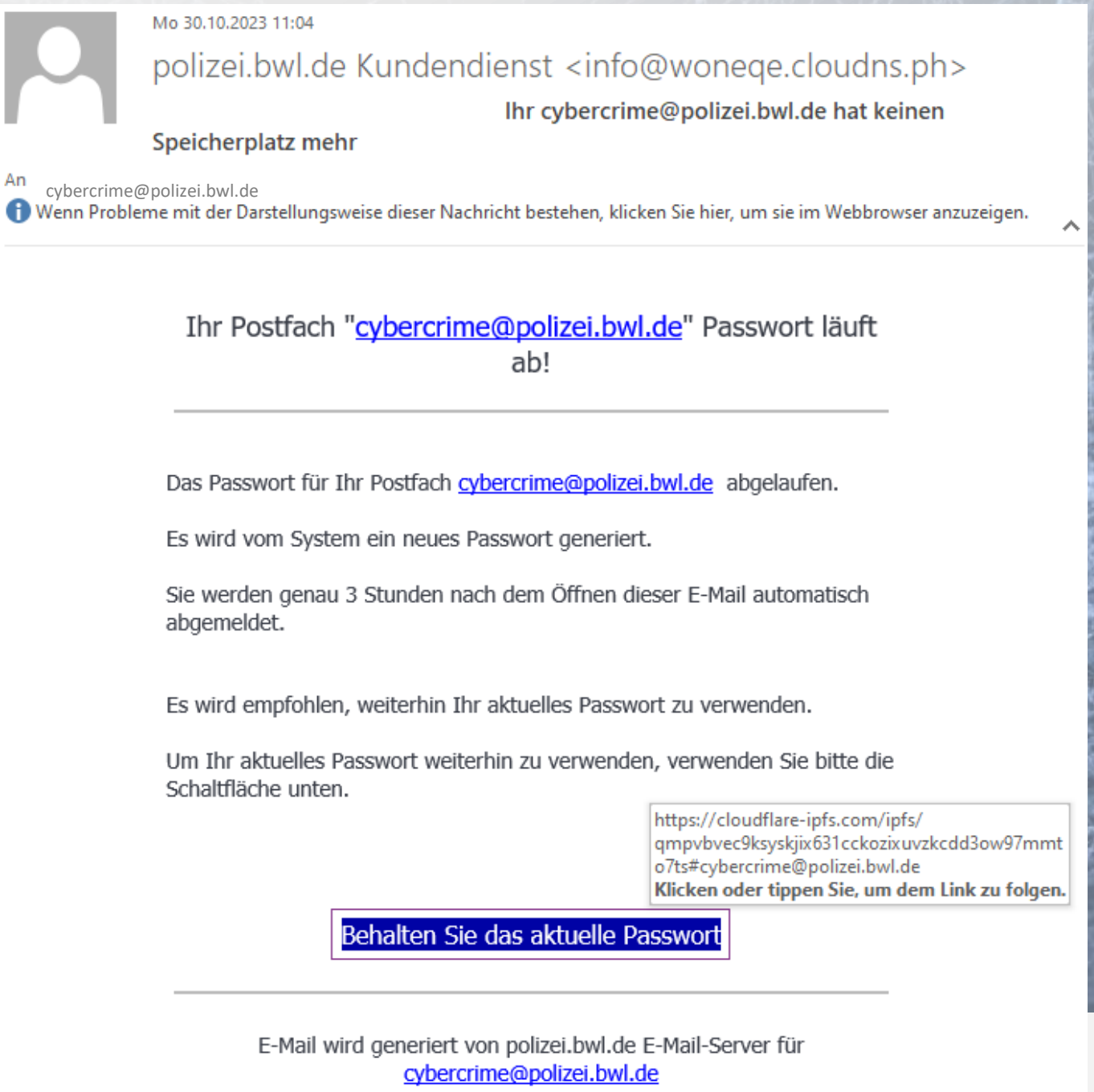
Allgemeine Prävention: Schwerpunkt Phishing

Angriffstaktiken „Phishing“

- Professionell: Aufklärung
  - betriebsinterne sachliche Zuständigkeit und Funktion (Webseitenrecherche, Karriereportale, Geschäftsberichte, Fachpublikationen…)
  - Abhängigkeiten (Vorgesetztenverhältnis, IT-Verantwortliche…)
  - Geschäftskontakte

  Vorbereitung
  - Szenario
  - inhaltliche Präparierung
  - technische Präparierung (Account-Kompromittierung oder Registrierung namensähnlicher Domains, Spoofing, Nutzung von Cloud-Diensten, QR-Generierung…)

Schwerpunkt Phishing



Mo 30.10.2023 11:04

polizei.bwl.de Kundendienst <info@woneqe.cloudns.ph>

Ihr cybercrime@polizei.bwl.de hat keinen Speicherplatz mehr

An cybercrime@polizei.bwl.de

Wenn Probleme mit der Darstellungsweise dieser Nachricht bestehen, klicken Sie hier, um sie im Webbrowser anzuzeigen.

Ihr Postfach "cybercrime@polizei.bwl.de" Passwort läuft ab!

Das Passwort für Ihr Postfach cybercrime@polizei.bwl.de abgelaufen.

Es wird vom System ein neues Passwort generiert.

Sie werden genau 3 Stunden nach dem Öffnen dieser E-Mail automatisch abgemeldet.

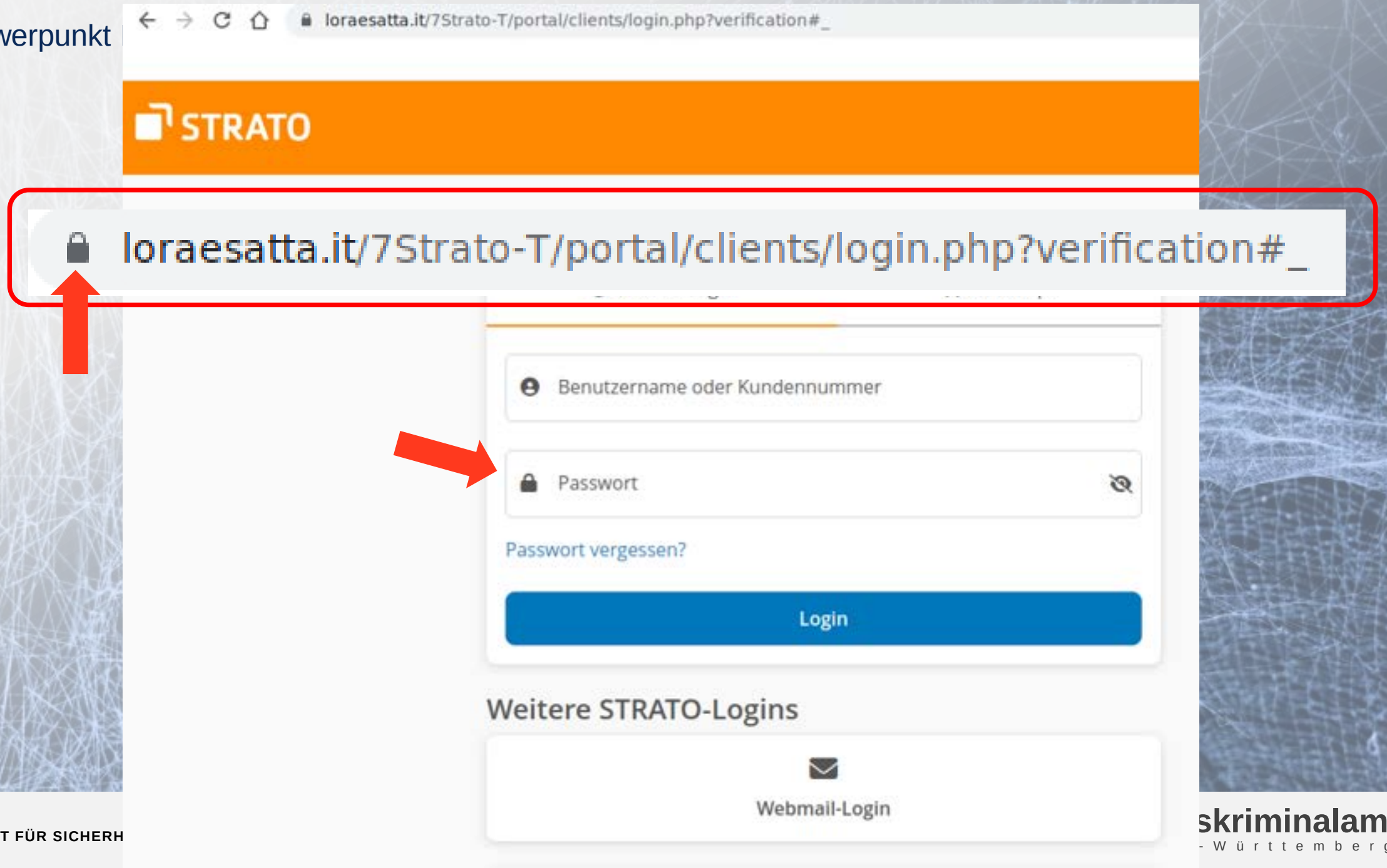
Es wird empfohlen, weiterhin Ihr aktuelles Passwort zu verwenden.

Um Ihr aktuelles Passwort weiterhin zu verwenden, verwenden Sie bitte die Schaltfläche unten.

https://cloudflare-ipfs.com/ipfs/qmpvbvec9ksyskjix631cckozixuvzkcdd3ow97mmto7ts#cybercrime@polizei.bwl.de
Klicken oder tippen Sie, um dem Link zu folgen.

Behalten Sie das aktuelle Passwort

E-Mail wird generiert von polizei.bwl.de E-Mail-Server für cybercrime@polizei.bwl.de


loraesatta.it/7Strato-T/portal/clients/login.php?verification#_
STRATO
loraesatta.it/7Strato-T/portal/clients/login.php?verification#_
Benutzername oder Kundennummer
Passwort
Passwort vergessen?
Login
Weitere STRATO-Logins
Webmail-Login

Schwerpunkt Phishing: Prüfung Web-Adressen (Domain-Check)

Relevant sind Schrägstriche (“Slash”) und Punkte (“Dot”)
Merke: *http(s)* und *www* sowie alle zwischenstehenden Zeichen sind irrelevant und werden ignoriert

Schritt 1: Identifizierung erster Schrägstrich
Schritt 2: Identifizierung linksseitig zweiter Punkt (sofern vorhanden)

Zwischenbereich = relevante Domain
Alle anderen Zeichen sind für die Bewertung irrelevant!

Ergebnis Adressenprüfung: Domain der Adresse lautet loraesetta.it

Ergebnis: ohne Bezug zum vorgetäuschten Dienst (hier: Strato) und demnach unseriöse Adresse/Webseite

Schwerpunkt Phishing: Prüfung Web-Adressen (Domain-Check)

E-Mail-Adressen: Relevant sind **Punkte** (“Dot”)

Domain

Domain Check E-Mail-Adresse: beispiel@loraesatta.it

Domain: Ab dem letzten Zeichen und linksseitig bis vor dem @

Domain

Domain Check E-Mail-Adresse mit mehr als einem Punkt nach dem @: beispiel@text.loraesatta.it

Domain: Ab dem letzten Zeichen und linksseitig bis vor zweitem Punkt

Aussichtslose Cybercrime-Ermittlungsverfahren?

E-Mail-Betrug im Lörracher Rathaus: Verdächtiger wird in Lahr festgenommen

FBI und Europol zerschlagen mit Partnern das Qakbot-Netzwerk

BKA schaltet weltweit größten Geldwäschedienst im Darknet ab

DoppelPaymer: internationales Hacker-Netzwerk enttarnt

Nachrichten

Drogen-Marktplatz im Darknet ausgehoben – fast 300 Festnahmen

Polizei nimmt deutschen DDOS-Hoster offline

Informationsquellen für IT-Verantwortliche

- Handlungsempfehlungen der Polizei gegen Verschlüsselungsangriffe und E-Mail-Betrug
  www.lka-bw.de/zac
- Bundesamt für Sicherheit in der Informationstechnik (BSI)
  Basis Absicherung Kommunalverwaltung (V3.0)
  Checklisten IT-Basisabsicherung Kommunen
  Sicherheitsberatung für Kommunen
- CSBW
  www.cybersicherheit-bw.de/beratungsangebote-fuer-kommunen
- Fachforum für kommunale IT-Sicherheitsbeauftragte
  www.it-sibe-forum.de
- Cybersicherheitskompass für Kommunen
  www.cybersicherheitskompass.de
- Warn- und Informationsdienst (CERT Bund)
  https://wid.cert-bund.de/portal/wid/kurzinformationen
- CISA (Cybersecurity & Infrastructur Security Agency -englisch-)
  www.cisa.gov

Angriffsziel öffentlicher Sektor: Risikobewusstsein

§ 30 IV NIS2G (2024) – fakultative Orientierung

- Risikoanalyse und Sicherheit für Informationssysteme
- Bewältigung von Sicherheitsvorfällen
- Aufrechterhaltung und Wiederherstellung, Backup-Management, Krisen-Management
- Sicherheit der Lieferkette, Sicherheit zwischen Einrichtungen, Dienstleister-Sicherheit
- Sicherheit in der Entwicklung, Beschaffung und Wartung, Management von Schwachstellen
- Bewertung der Effektivität von Cybersicherheit und Risiko-Management
- Schulungen Cybersicherheit und Cyberhygiene
- Kryptografie und Verschlüsselung
- Personalsicherheit, Zugriffskontrolle und Anlagen-Management
- Multi-Faktor Authentisierung und kontinuierliche Authentisierung
- Sichere Kommunikation (Sprach, Video- und Text)
- Sichere Notfallkommunikation

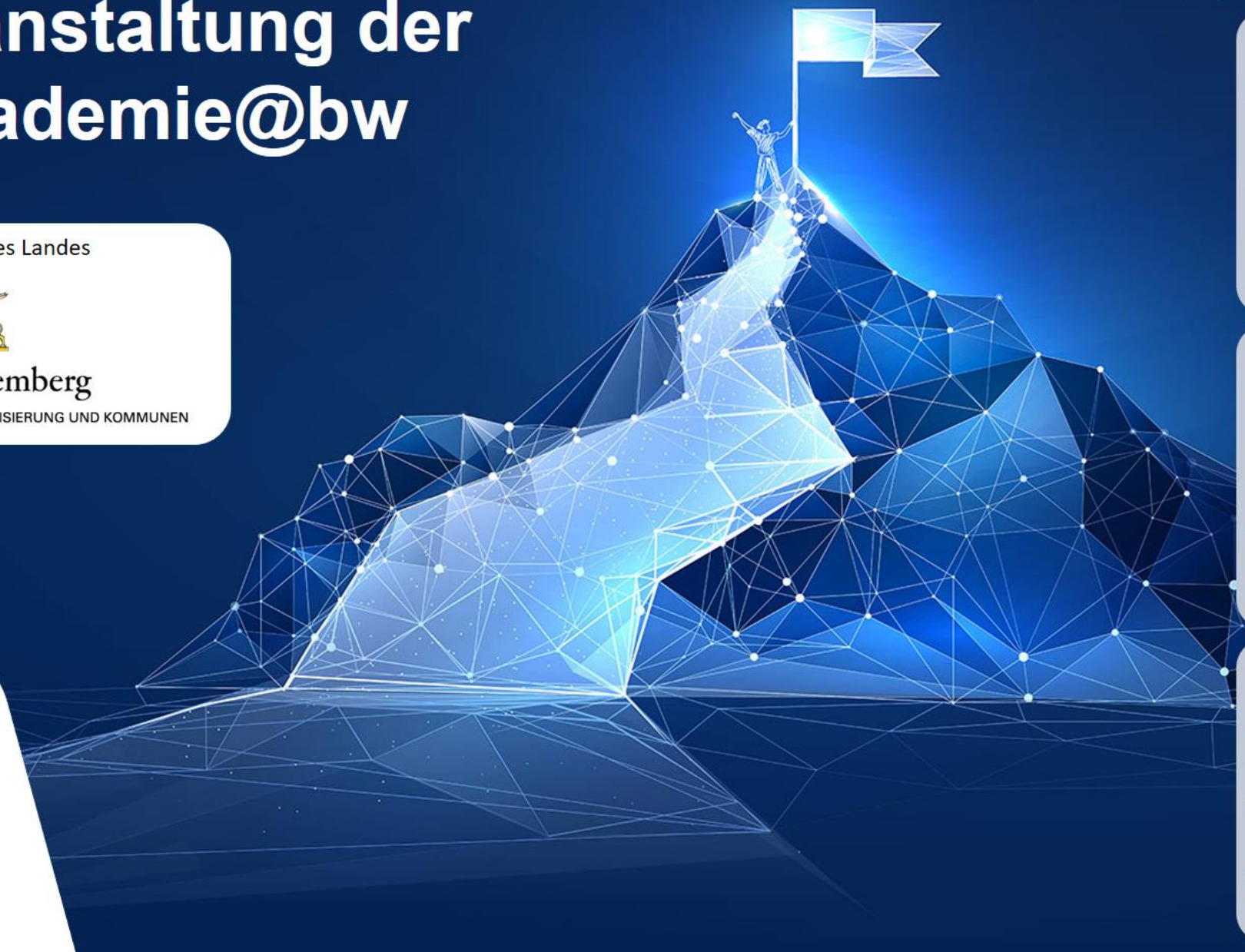
www.LKA.POLIZEI-BW.DE/ZAC

Eine Veranstaltung der Digitalakademie@bw

Ein Förderprojekt des Landes

Baden-Württemberg

MINISTERIUM DES INNEREN, FÜR DIGITALISIERUNG UND KOMMUNEN



digitalakademie@bw

Immer auf dem Laufenden bleiben …

LinkedIn

Instagram

Website