Cyber-Krisenmanagement

12. März 2026

Bettina Zimmermann

wpo WirtschaftsPortalOst

GU Sicherheit & Krisenmanagement

Bettina Zimmermann

CEO / Mitinhaberin
EMBA in Executive Management

GU Sicherheit & Partner AG
Sirnacherstrasse 7
CH-9500 Wil
www.gu-sicherheit.ch

- Seit 2009 Beraterin für **Unternehmen** in den Bereichen **Krisenmanagement**, **Krisenkommunikation**, **Bedrohungsmanagement** und **Risk-** und **Business Continuity Management (BCM)**
- Begleitung und Unterstützung von **über 300 Krisenfällen** in Unternehmen
- **Aufbau, Training** von **Krisenstäben** und **Führungsunterstützungsteams in Unternehmen im DACH-Raum**
- **Dozentin** an diversen Bildungsinstituten (HSLU, ZHAW, FHNW, Rochester Universität Bern, hft)
- **Verwaltungsrätin**
- **Ehem. Gemeinderätin** (Exekutive)
- **Mitautorin**
  - «NOT-BOOK – Wenn das Wetter zum Feind wird» 2025,
  - «NOT-BOOK – Vorbereitet für den Cyber-Ernstfall» 2023,
  - «NOT-BOOK – Im Blackout einen Schritt voraus» 2022,
  - «Praxishandbuch Krisenmanagement» 2016
- **Autorin**
  - «Emotionen – das Salz in der Krise» 2018,
  - «Weiblich und mit Biss – Erfolgsstrategien für Frauen» 2015

Sport Live

Millia
Cybe
Rove

Der Cybera
der wirtsch

Lesezeit: 1 M

Teilen Merker

Gefährliche Cyber-Angriffe

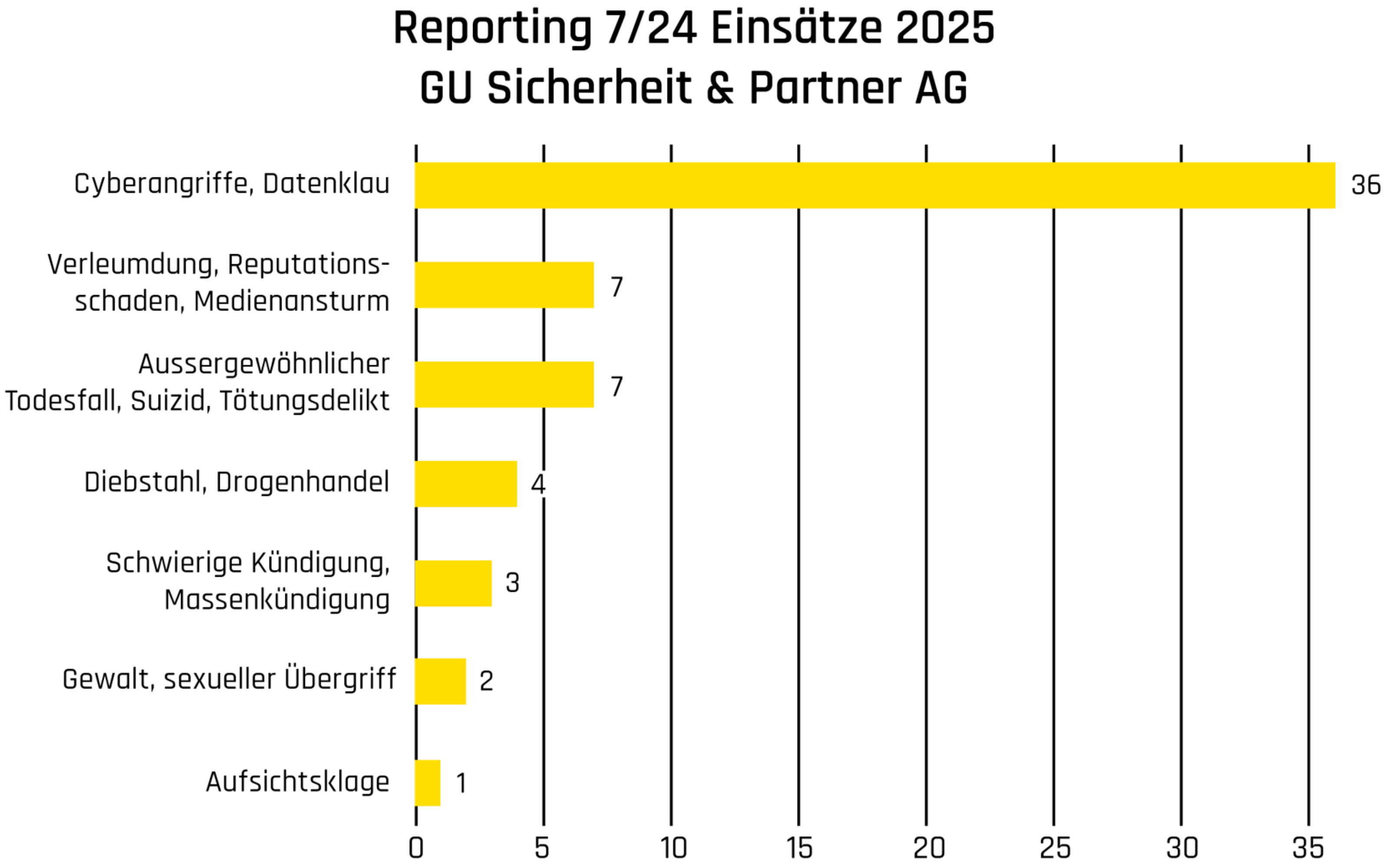
Hunderte Angriffe gegen kritische Infrastrukturen in der Schweiz

Seit April 2025 sind dem Bund über 260 Angriffe gegen kritische Infrastrukturen gemeldet worden. Hauptsächlich betroffen sind Behörden, IT- und Telekommunikationsfirmen sowie Banken.

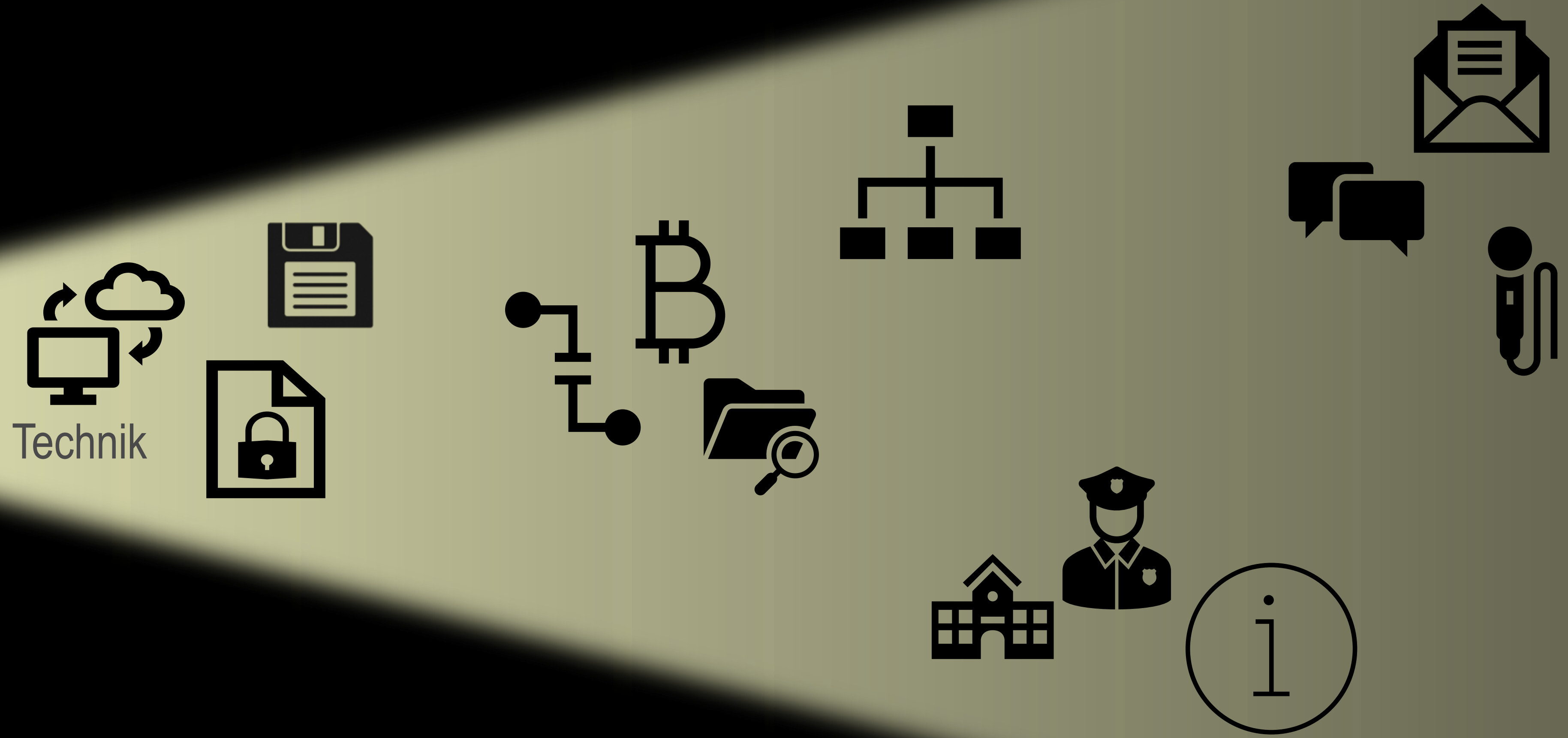
Publiziert: 08.02.2026 um 06:53 Uhr | Aktualisiert: 08.02.2026 um 19:26 Uhr

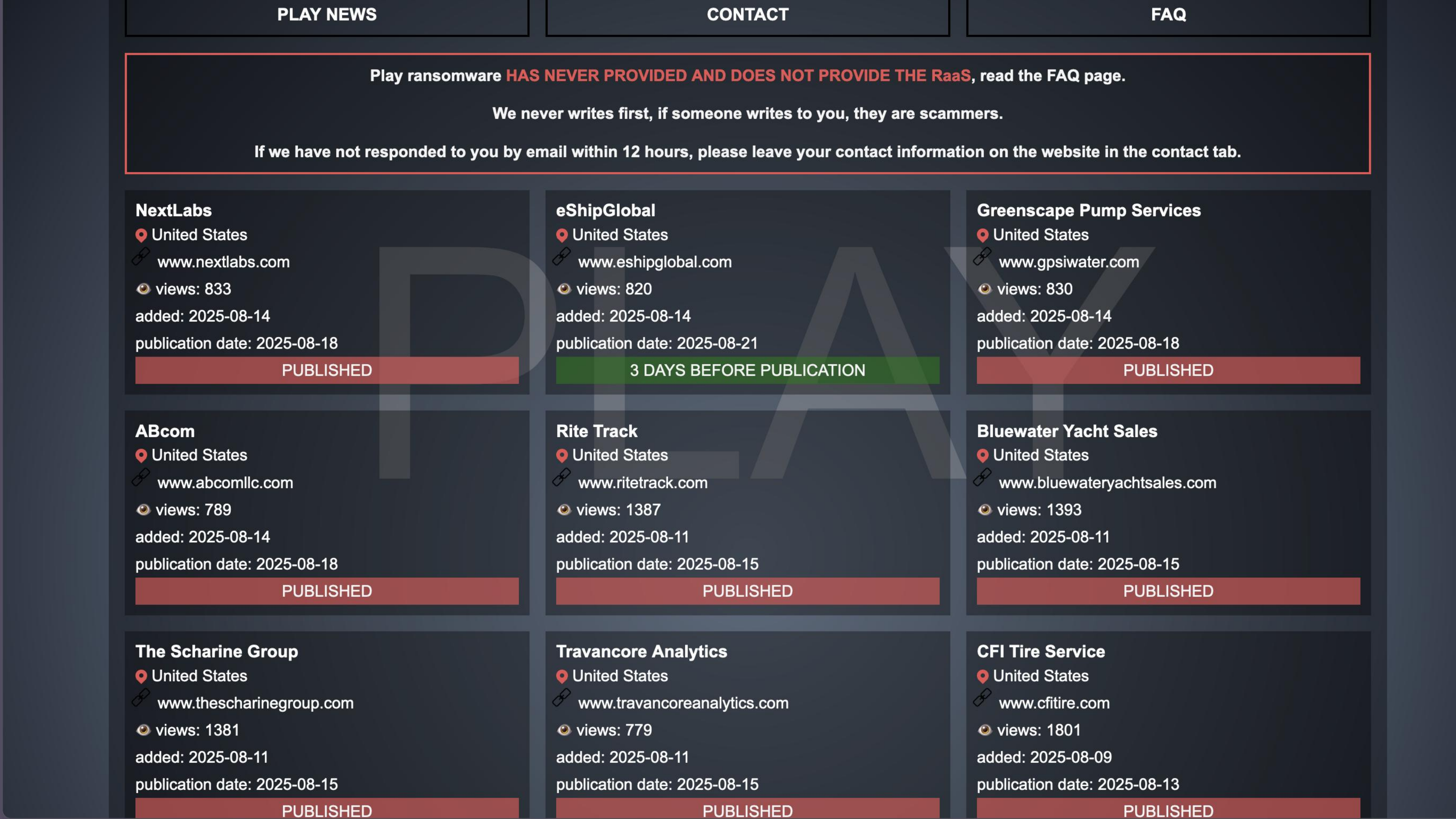
Teilen Anhören 8 Kommentieren

Einsatzstatistik GU Sicherheit



Dimension Ransomware-Angriff





Play ransomware HAS NEVER PROVIDED AND DOES NOT PROVIDE THE RaaS, read the FAQ page.

We never writes first, if someone writes to you, they are scammers.

If we have not responded to you by email within 12 hours, please leave your contact information on the website in the contact tab.

NextLabs

📍 United States

🔗 www.nextlabs.com

👁 views: 833

added: 2025-08-14

publication date: 2025-08-18

PUBLISHED

eShipGlobal

📍 United States

🔗 www.eshipglobal.com

👁 views: 820

added: 2025-08-14

publication date: 2025-08-21

3 DAYS BEFORE PUBLICATION

Greenscape Pump Services

📍 United States

🔗 www.gpsiwater.com

👁 views: 830

added: 2025-08-14

publication date: 2025-08-18

PUBLISHED

ABcom

📍 United States

🔗 www.abcomllc.com

👁 views: 789

added: 2025-08-14

publication date: 2025-08-18

PUBLISHED

Rite Track

📍 United States

🔗 www.ritetrack.com

👁 views: 1387

added: 2025-08-11

publication date: 2025-08-15

PUBLISHED

Bluewater Yacht Sales

📍 United States

🔗 www.bluewateryachtsales.com

👁 views: 1393

added: 2025-08-11

publication date: 2025-08-15

PUBLISHED

The Scharine Group

📍 United States

🔗 www.thescharinegroup.com

👁 views: 1381

added: 2025-08-11

publication date: 2025-08-15

PUBLISHED

Travancore Analytics

📍 United States

🔗 www.travancoreanalytics.com

👁 views: 779

added: 2025-08-11

publication date: 2025-08-15

PUBLISHED

CFI Tire Service

📍 United States

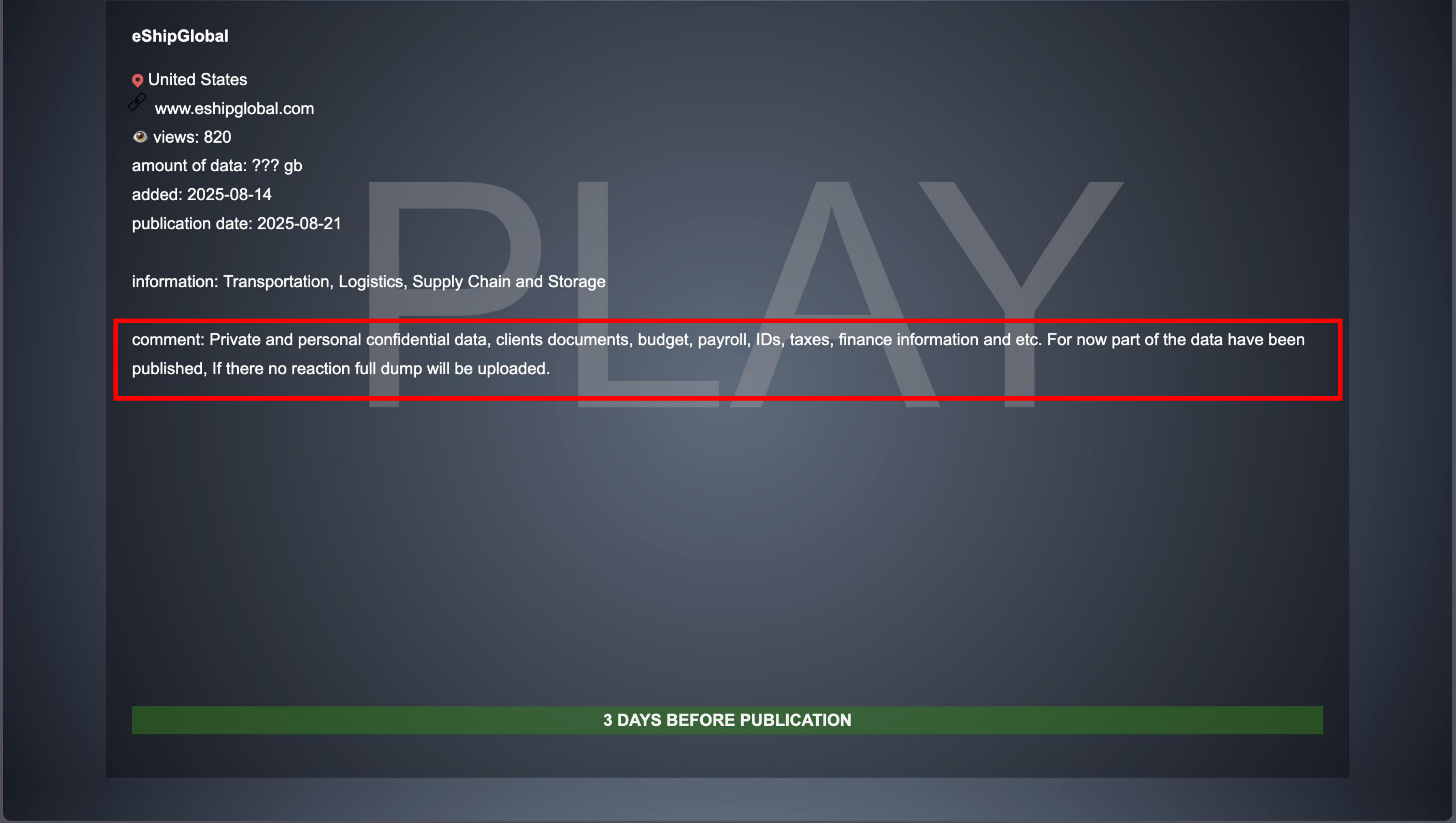
🔗 www.cfitire.com

👁 views: 1801

added: 2025-08-09

publication date: 2025-08-13

PUBLISHED



eShipGlobal

📍 United States

🔗 www.eshipglobal.com

👁 views: 820

amount of data: ??? gb

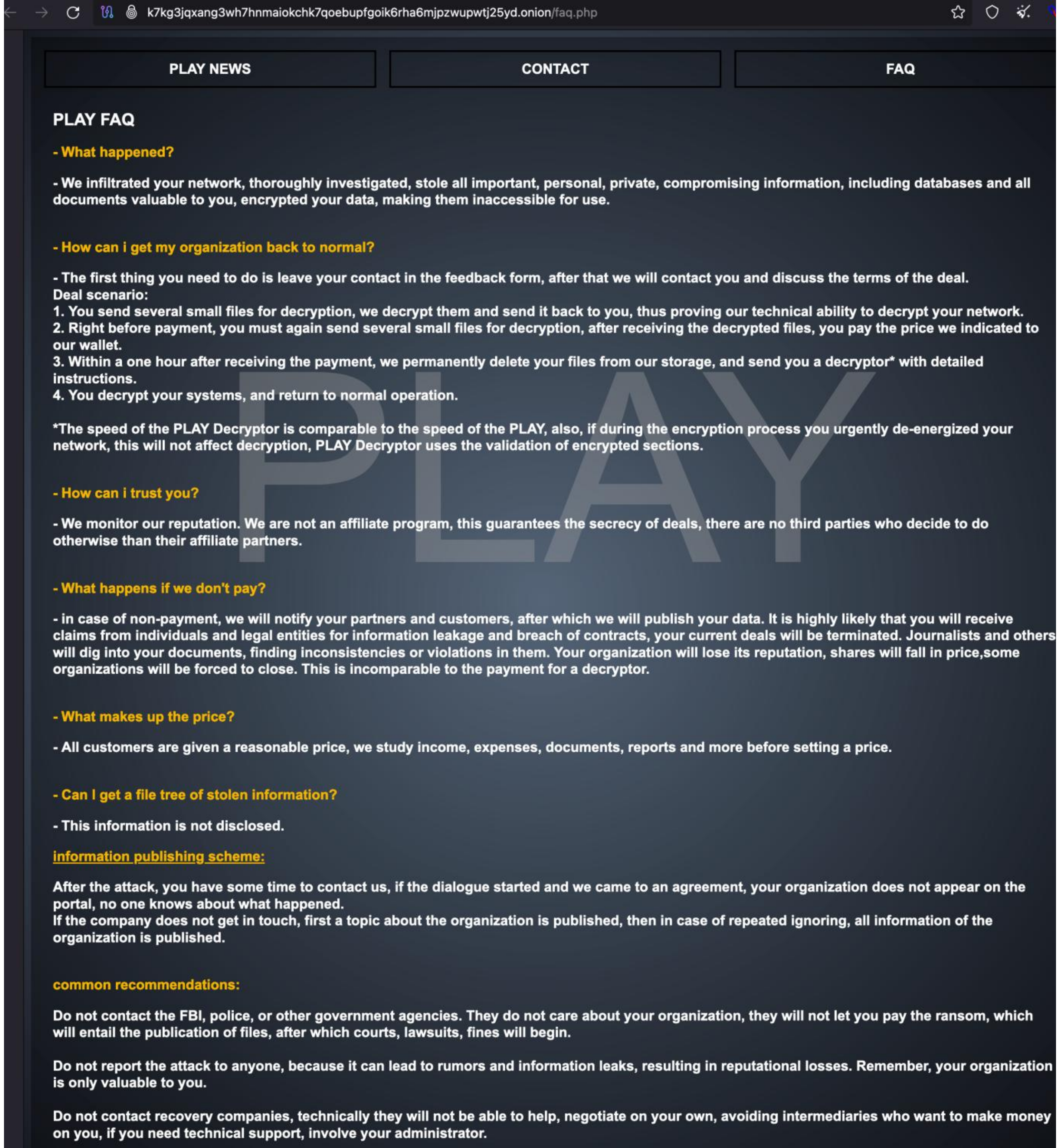
added: 2025-08-14

publication date: 2025-08-21

information: Transportation, Logistics, Supply Chain and Storage

comment: Private and personal confidential data, clients documents, budget, payroll, IDs, taxes, finance information and etc. For now part of the data have been published, If there no reaction full dump will be uploaded.

3 DAYS BEFORE PUBLICATION


k7kg3jqxang3wh7hnmaiokchk7qoebupfgoik6rha6mjpzwupwtj25yd.onion/faq.php
PLAY NEWS
CONTACT
FAQ
PLAY

PLAY FAQ

- What happened?

- We infiltrated your network, thoroughly investigated, stole all important, personal, private, compromising information, including databases and all documents valuable to you, encrypted your data, making them inaccessible for use.

- How can i get my organization back to normal?

- The first thing you need to do is leave your contact in the feedback form, after that we will contact you and discuss the terms of the deal.
Deal scenario:
1. You send several small files for decryption, we decrypt them and send it back to you, thus proving our technical ability to decrypt your network.
2. Right before payment, you must again send several small files for decryption, after receiving the decrypted files, you pay the price we indicated to our wallet.
3. Within a one hour after receiving the payment, we permanently delete your files from our storage, and send you a decryptor* with detailed instructions.
4. You decrypt your systems, and return to normal operation.

*The speed of the PLAY Decryptor is comparable to the speed of the PLAY, also, if during the encryption process you urgently de-energized your network, this will not affect decryption, PLAY Decryptor uses the validation of encrypted sections.

- How can i trust you?

- We monitor our reputation. We are not an affiliate program, this guarantees the secrecy of deals, there are no third parties who decide to do otherwise than their affiliate partners.

- What happens if we don't pay?

- in case of non-payment, we will notify your partners and customers, after which we will publish your data. It is highly likely that you will receive claims from individuals and legal entities for information leakage and breach of contracts, your current deals will be terminated. Journalists and others will dig into your documents, finding inconsistencies or violations in them. Your organization will lose its reputation, shares will fall in price,some organizations will be forced to close. This is incomparable to the payment for a decryptor.

- What makes up the price?

- All customers are given a reasonable price, we study income, expenses, documents, reports and more before setting a price.

- Can I get a file tree of stolen information?

- This information is not disclosed.

information publishing scheme:

After the attack, you have some time to contact us, if the dialogue started and we came to an agreement, your organization does not appear on the portal, no one knows about what happened.
If the company does not get in touch, first a topic about the organization is published, then in case of repeated ignoring, all information of the organization is published.

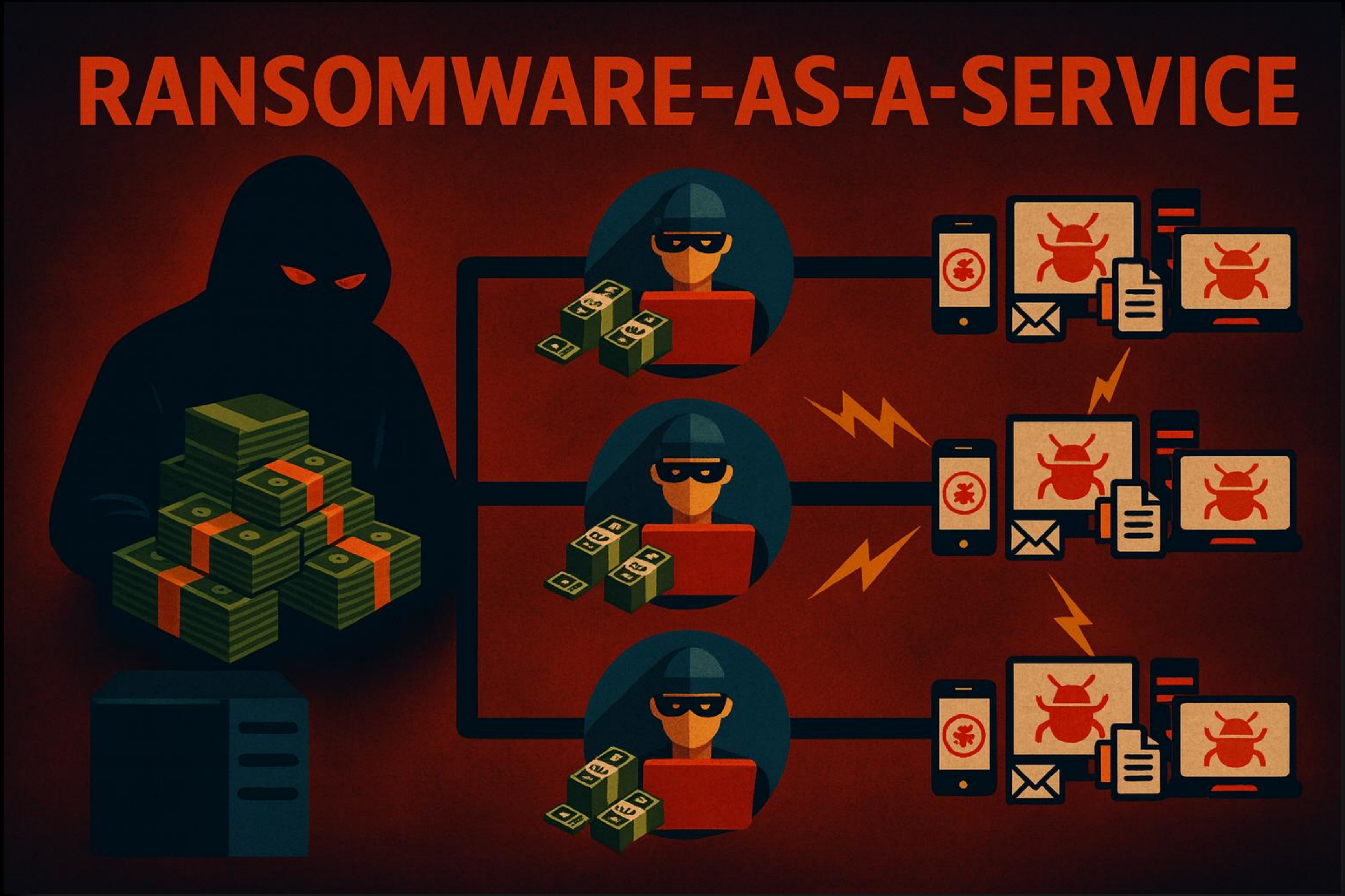
common recommendations:

Do not contact the FBI, police, or other government agencies. They do not care about your organization, they will not let you pay the ransom, which will entail the publication of files, after which courts, lawsuits, fines will begin.

Do not report the attack to anyone, because it can lead to rumors and information leaks, resulting in reputational losses. Remember, your organization is only valuable to you.

Do not contact recovery companies, technically they will not be able to help, negotiate on your own, avoiding intermediaries who want to make money on you, if you need technical support, involve your administrator.

Hackerangriff als Business Modell

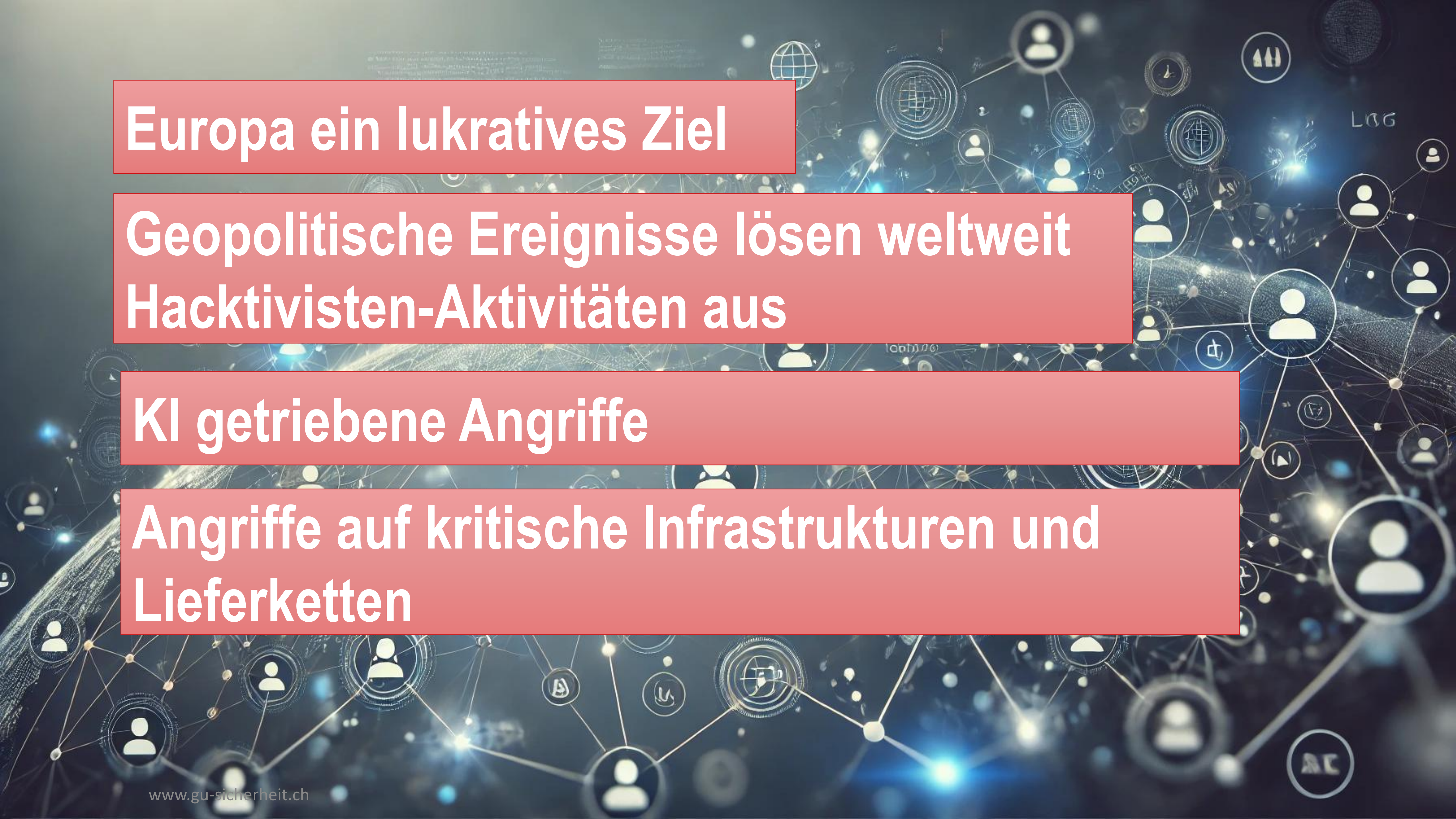


Gewalt als Business Modell

VIOLENCE-AS-A-SERVICE

Krisenmanagement beginnt lange vorher…

Prävention	Ereignisbewältigung	Nachbearbeitung
Sicherheitsüberprüfungen	IT-Spezialist, ev. IT-Forensik	Auswertung / Erkenntnisse / Lehren
IT-Sicherheit aktueller Stand	Umgang mit Cyber Erpressung	
Awareness	Krisenmanagement	
Aufbau und Training Krisenorganisation	Krisenkommunikation (intern)	
Checklisten für den Krisenfall	Krisenkommunikation (extern)	



Europa ein lukratives Ziel

Geopolitische Ereignisse lösen weltweit Hacktivisten-Aktivitäten aus

KI getriebene Angriffe

Angriffe auf kritische Infrastrukturen und Lieferketten

Take aways

- Grundsatz: Kultur des Hinschauens
- Risiken identifizieren, Szenarien ableiten und durchdenken
- IT-Sicherheit: technisch, organisatorisch und Faktor Mensch!
- BCM
- Bereit sein für die Krisenbewältigung
  - Krisenstab, der Kenntnisse der Führungsprozesse hat
  - einsatzbereite Infrastruktur
- Partner kennen für den Ernstfall