Wenn der Albtraum Realität wird – Cyberangriffe in Unternehmen

Donnerstag, 06.11.2025

Michelle Zimmermann

HIF

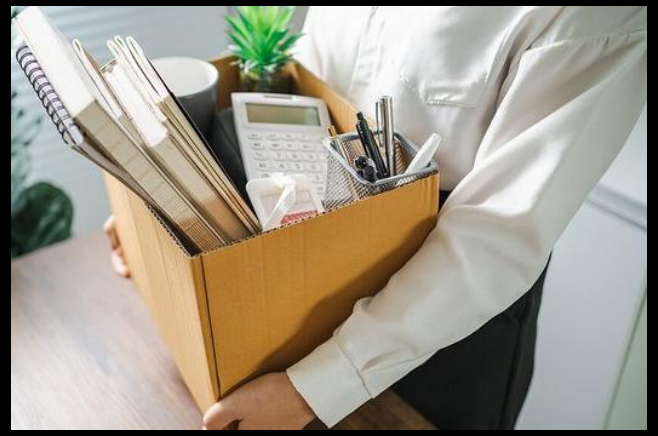
GU Sicherheit & Krisenmanagement

Referentin GU Sicherheit & Partner AG

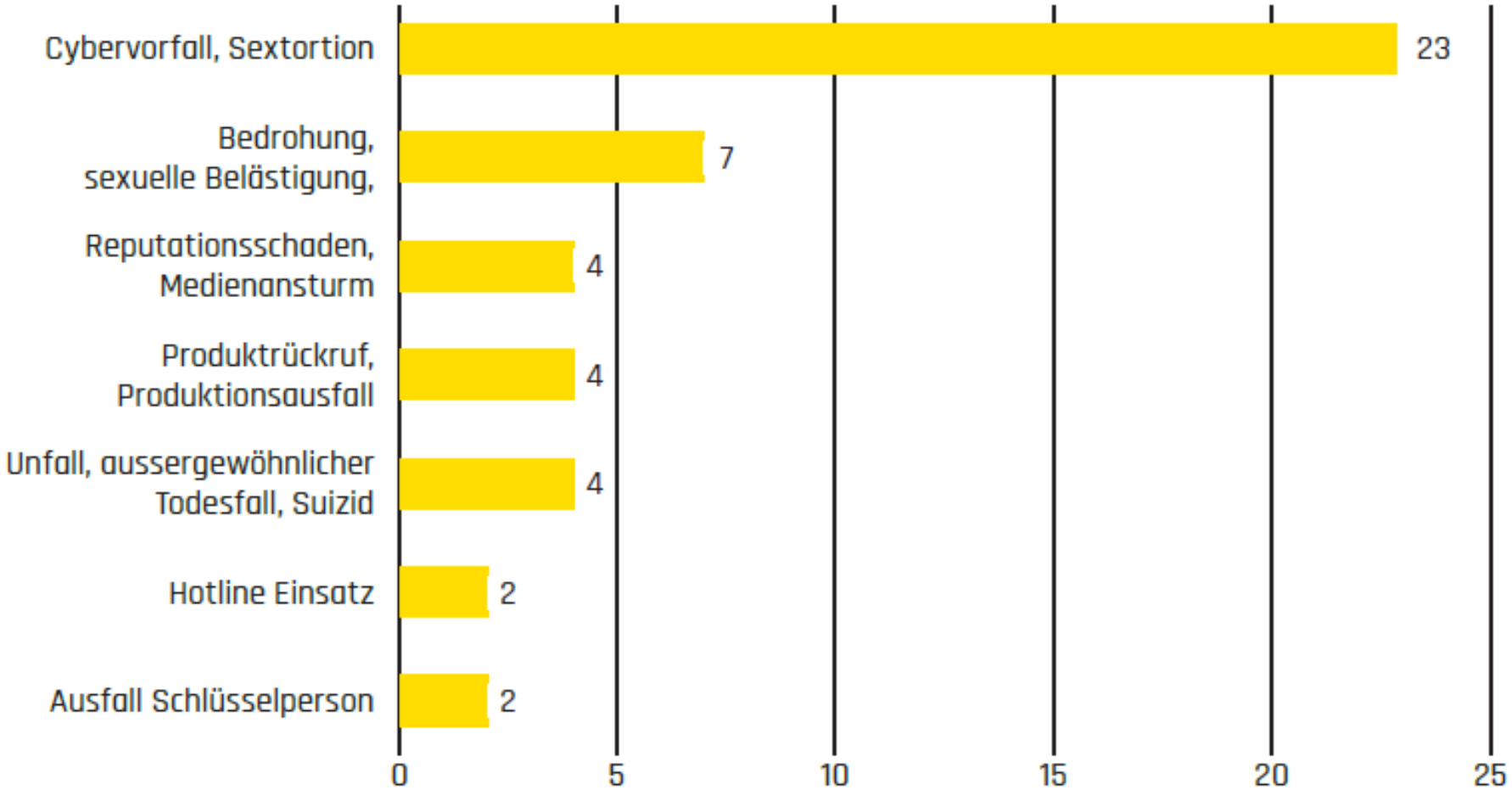
Michelle Zimmermann
Consultant / Mitglied der GL

- Unterstützt und **berät Unternehmen und Behörden** in den Bereichen Krisenmanagement, Business Continuity Management, Risikomanagement und bei der Erstellung von Sicherheitskonzepten
- Im **Team 7/24** «Unterstützung von Unternehmen im Krisenfall»
- **Bachelor of Science in Business Administration**, Vertiefung Value Network Management
- **CAS** in Krisenmanagement & Organisationale Resilienz
- **CAS** in Governance, Risk & Compliance
- Zertifizierte **Business Continuity Managerin**
- **Sachbearbeiterin HR und Pensionskasse** bei der SRG SSR
- **Assistentin Geschäftsleitung** in einer Patentanwaltskanzlei
- **Kauffrau EFZ**
- **Mitautorin** «NOT-BOOK, wenn das Wetter zum Feind wird», 2025, 1. Auflage, «NOT-BOOK, Vorbereitet für den Cyber-Ernstfall», 2023, 1. Auflage & «NOT-BOOK, im Blackout einen Schritt voraus», 2022, 5. Auflage

Krisen sind vielfältig - Fälle aus unserer Praxis



Einsatzstatistik GUS 2024



Ransomwa

Von Katharina Jochur

SECURITY RANS

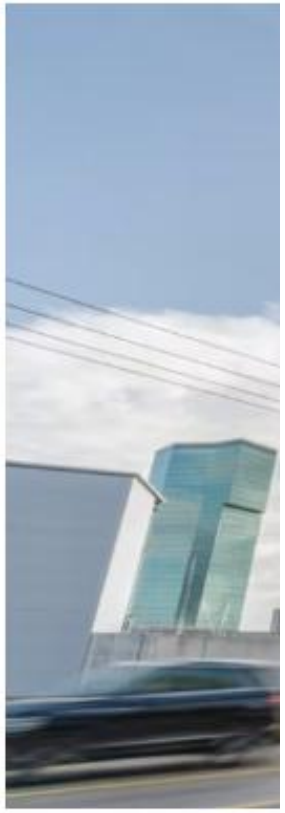


Foto: Cistec

Nach einem C
Systeme heru
laut dem Unte

Home

Cyberar

Spe
Pro
köl

Die Sup
Geräte
tangiert

Publiziert: 1

Cyberangriff

Hacker ver
UBS und ar

Fabian von Allmen
Mittwoch, 18.06.2025, 15:26 Uh
Aktualisiert um 18:12 Uhr

- Hacker haben Da
  veröffentlicht.
- Betroffen ist die
- Gemäss weltweit
  ab.

Die Grossbank UBS,
sind von einem grös
Branchenmedium «I

Milliardenkosten durch Cyberangriff auf Jaguar Land Rover

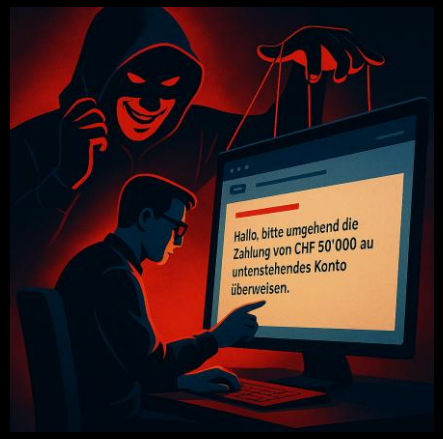
Der Cyberangriff auf den britischen Autobauer Jaguar Land Rover war der wirtschaftlich schädlichste in der Geschichte des Landes.

Lesezeit: 1 Minute

Teilen Merken Drucken Kommentare

Cyberangriffe können viele Formen haben…

Spear-Phishing



Social Engineering / CEO Fraud

Ransomware

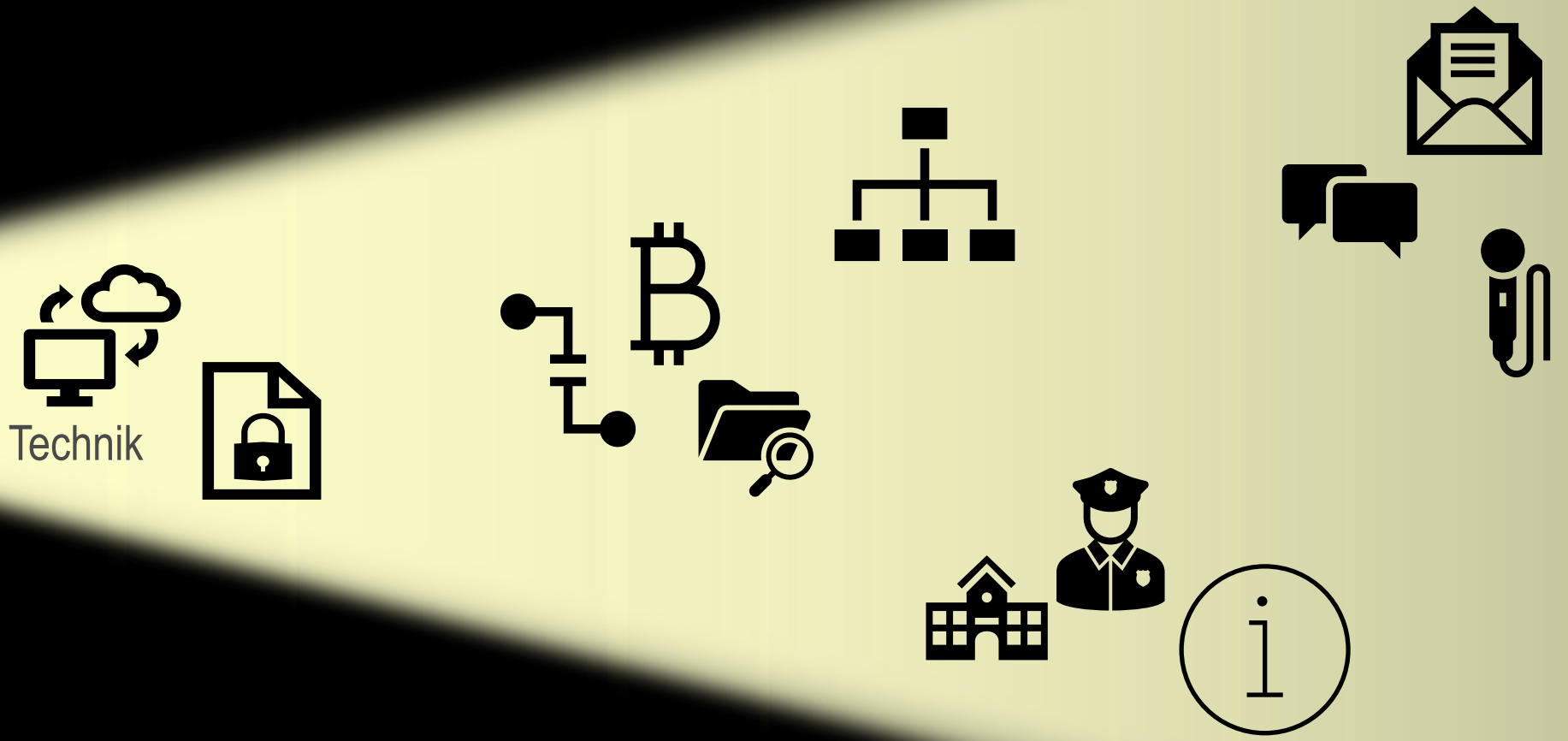
Distributet Denial of Service (DDoS)

Man-in-the-Middle

Brute-Force-Angriff

Bildquelle: GUS - Generiert mit Chatgpt

Dimensionen



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

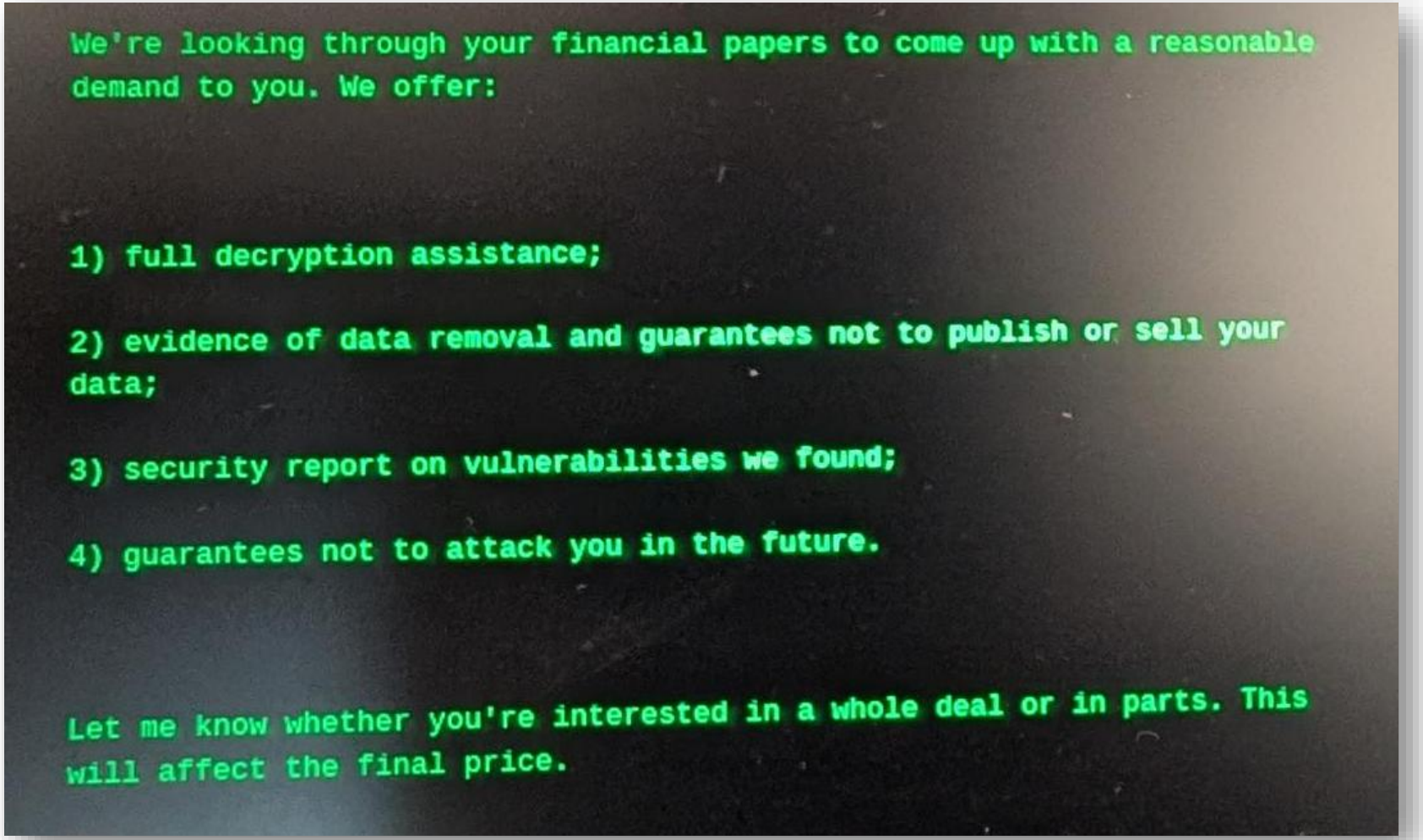
publication date: 2025-08-21

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

Lösegeldzahlung – jetzt modulartig!



Warum steigen Cyberangriffe so stark an?

- Zunehmende Digitalisierung → Abhängigkeit von Daten
- Hybride Kriegsführung
- Professionalisierung der Hackergruppen
- Künstliche Intelligenz

PLAY NEWS | CONTACT | FAQ

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

Bildquelle: GUS - Generiert mit Chatgpt

CipherWolf
New Member

Joined: September 14, 2025
Messages: 2
Reaction score: 1
Points: 3

October 4, 2025

Thread Author #1

CipherWolf

Hello everyone

CipherWolf has been released RaaS
CipherWolf is written in rust
The program has been tested extensively on heavy loads and has worked very well.
So anyone interested in working with us, we are happy to help.

Required conditions:

```
Access to a system with important data
```

We provide you with a dashboard with custom ransomware.
Within the dashboard, you'll find all your data, devices, withdrawal features, and account revenue allocations.
You don't need to create a ransomware program for each victim. We provide a single version that targets any victim.

Operating system:

```
All Windows systems
```

How does the program work and what algorithms are used?:

Algorithms that the program works on in AES-GCM 256
We also provide the process of connecting to a dedicated server to transfer the victim files. You do not need to transfer them manually or compress them.
The program does everything effectively, while ensuring that they are not lost when using the encryption currency.
You have full control over the program's operation, targeting methods, and the process paths mechanism.
When the program is running, it deletes shadow copies, backups, and web services. It stops more than 100 processes. The number is not fixed.

Operating system:

`All Windows systems`

How does the program work and what algorithms are used?:

Algorithms that the program works on in AES-GCM 256
We also provide the process of connecting to a dedicated server to transfer the victim files. You do not need to transfer them manually or compress them.
The program does everything effectively, while ensuring that they are not lost when using the encryption currency.
You have full control over the program's operation, targeting methods, and the process paths mechanism.
When the program is running, it deletes shadow copies, backups, and web services. It stops more than 100 processes. The number is not fixed.
Dealing with Work Group active directory

Profit share:

The percentage that is withdrawn to us is 5-10%, but since I am in the launch phase of the project, the first 3 people will only receive 1%.

✅ Stop a process
✅ Delete shadow copies and backups
✅ Dealing with networks
✅ Control the work of the program
✅ The dashboard is free
✅ Raise powers to the system
❌ The negotiation board is not fully developed.

Note: You are not responsible for the delegation, but we are the ones who do that manually.

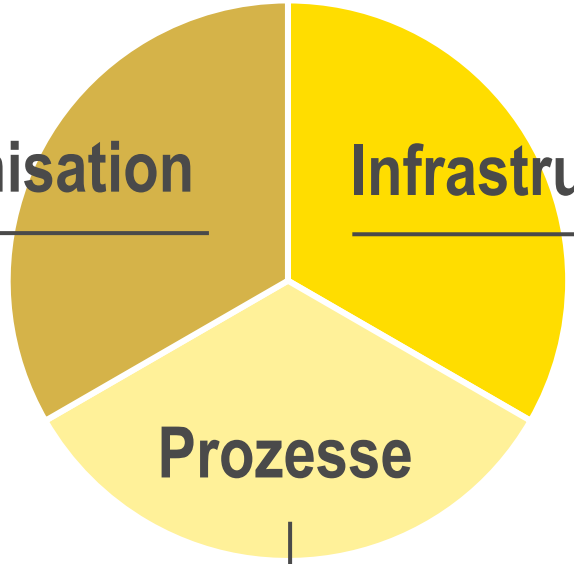
Our website : b63zgpxrwqttrr6ti3jvvezqdzahuirkkjuundu26gz4krtrrkncqjad.onion
Our id on TOX : 0FDCE2F2E213A62A46FB9DBE703D631444CAC1A2FF39FB44FB5A19CAB121F36AB5435EBEAB48

SpecterWire

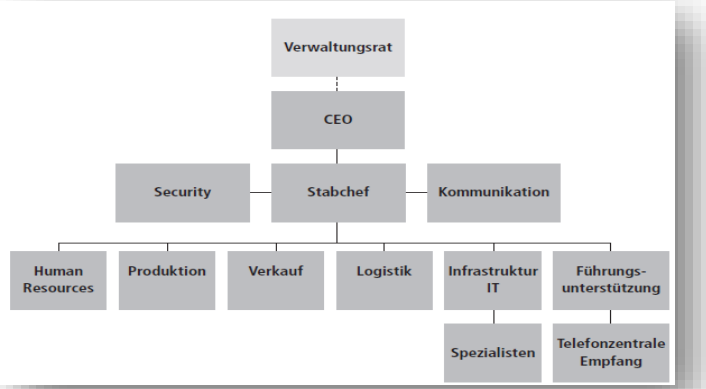
Krisenmanagement beginnt lange vorher…

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

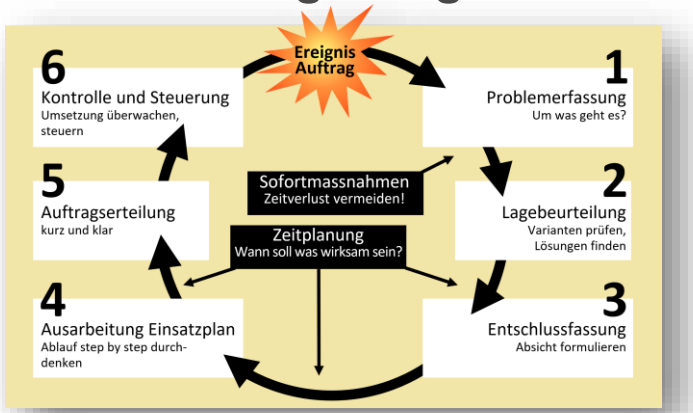
Krisenmanagement | Voraussetzungen



Krisenstab



Führungstätigkeit



Führungsstandort

Take aways

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

Herzlichen Dank

GU Sicherheit & Partner AG

Michelle Zimmermann, Mitglied der Geschäftsleitung

Sirnacherstrasse 7 I CH – 9500 Wil / SG

m.zimmermann@gu-sicherheit.ch I +41 71 913 27 66

www.gu-sicherheit.ch