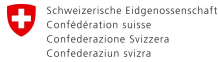


# Cyber Threat Exchange Liechtenstein

## 26. September 2023



### Wie das NCSC für mehr Sicherheit sorgt



26. September 2023 / Avantec Security Event



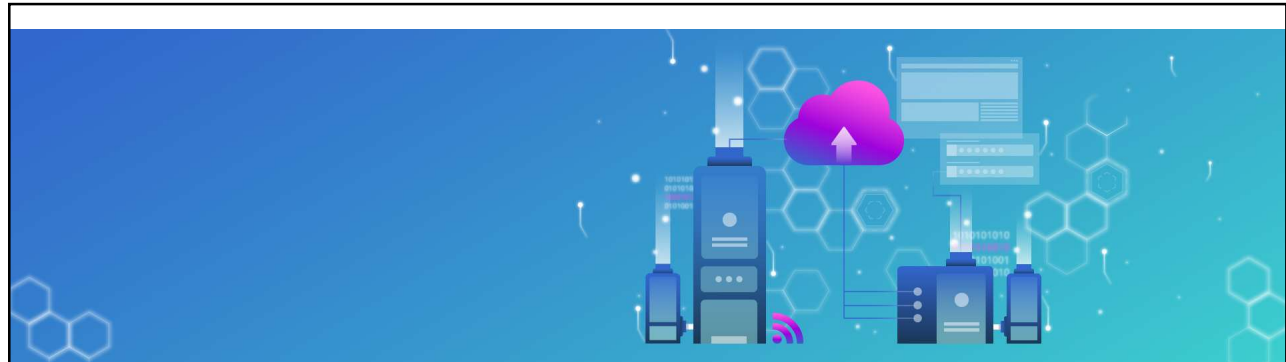
### Programm



1. Aus dem NCSC wird das Bundesamt für Cybersicherheit BACS
2. Lage national und international / Akteure / Angriffsvektoren
3. DDoS-Angriffe vom Juni 2023
4. Ransomwaregruppe «Play»
5. Meldepflicht für Cybervorfälle
6. So unterstützt das NCSC liechtensteinische Unternehmen
7. Zum Schluss noch dies...

# Cyber Threat Exchange Liechtenstein

## 26. September 2023



### 1. Aus dem NCSC wird das BACS

Eidgenössisches Finanzdepartement EFD  
Nationales Zentrum für Cybersicherheit NCSC

3



## Transformation des NCSC ins BACS

Das NCSC wird zu einem Bundesamt im VBS

02.12.2022 - Aufgrund der zunehmenden Bedeutung der Cybersicherheit und der guten Aufbaubarkeit, die das Nationale Zentrum für Cybersicherheit (NCSC) in den vergangenen Jahren im Eidgenössischen Finanzdepartement (EFD) geleistet hat, soll das NCSC in ein Bundesamt überführt werden. An seiner Sitzung vom 2. Dezember 2022 hat der Bundesrat festgelegt, dass das Bundesamt im Eidgenössischen Departement für Verteidigung, Bevölkerungsschutz und Sport (VBS) angesiedelt werden soll. Er hat das VBS beauftragt, in Zusammenarbeit mit dem EFD bis Ende März 2023 die Strukturen des neuen Bundesamtes zu erarbeiten.



Die Bedeutung der Cybersicherheit hat in den vergangenen Jahren auf allen Ebenen stark zugenommen. Dabei ist die Gewährleistung der Cybersicherheit zu einer unverzichtbaren Aufgabe des Bundes geworden. 2019 hat der Bundesrat mit der Schaffung des NCSC als Einheit des Generalsekretariats des

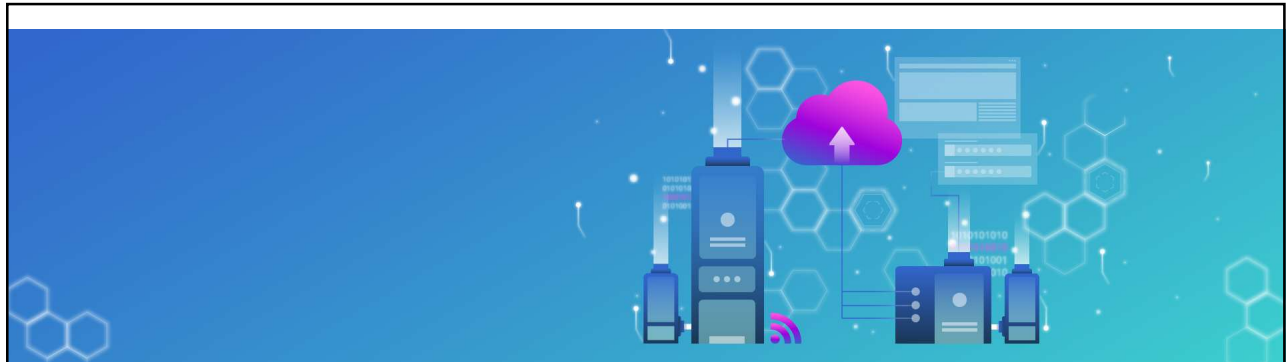
- Bundesratsbeschluss vom 02.12.2022
- Das NCSC wird per 01.01.2024 in ein Bundesamt für Cybersicherheit BACS überführt
- Neuansiedelung im VBS
- Alle Mitarbeitenden werden übernommen
- Vorerst «nur» organisatorische Eingliederung
- Amtsdirektor: Florian Schütz (bisher Delegierter des Bundes für Cybersicherheit)

Eidgenössisches Finanzdepartement EFD  
Nationales Zentrum für Cybersicherheit NCSC

4

# Cyber Threat Exchange Liechtenstein

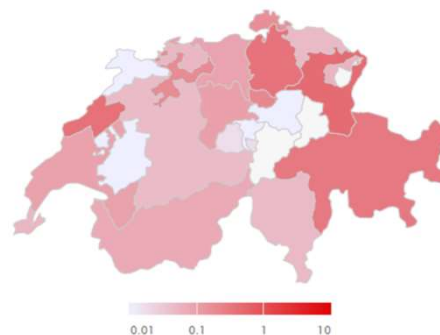
## 26. September 2023



## 2. Lage national und international / Akteure / Angriffsvektoren

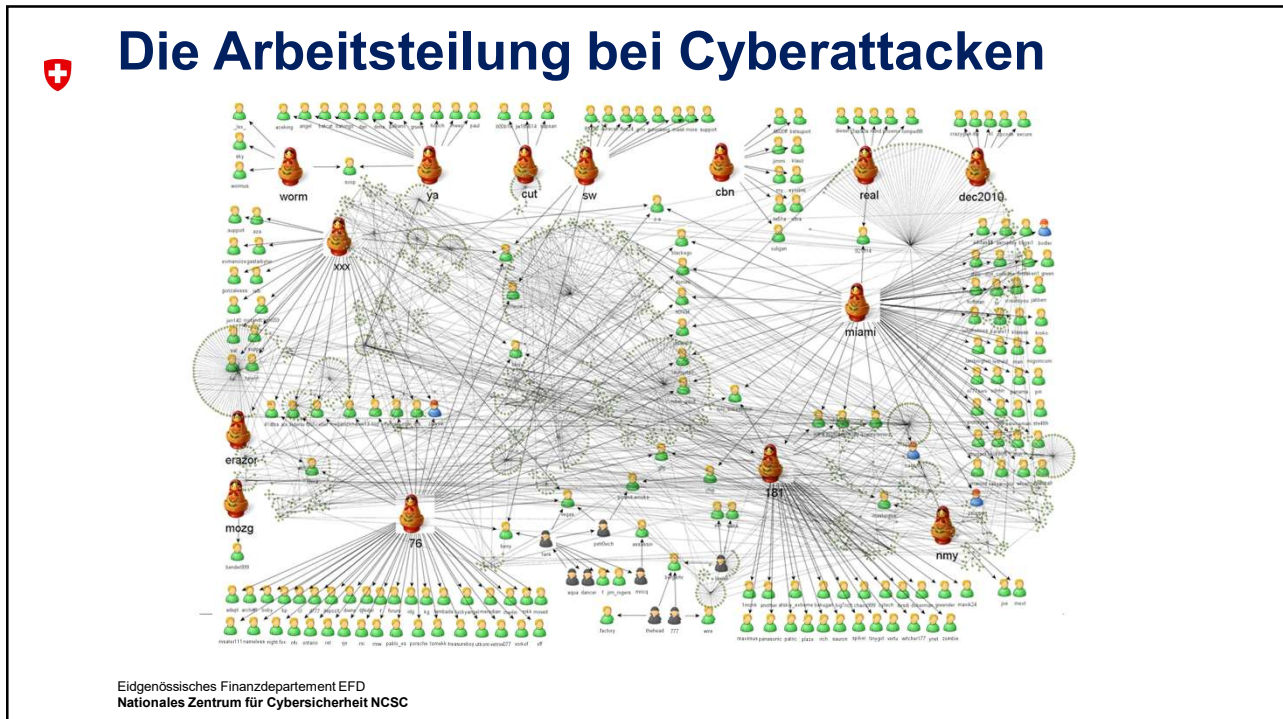
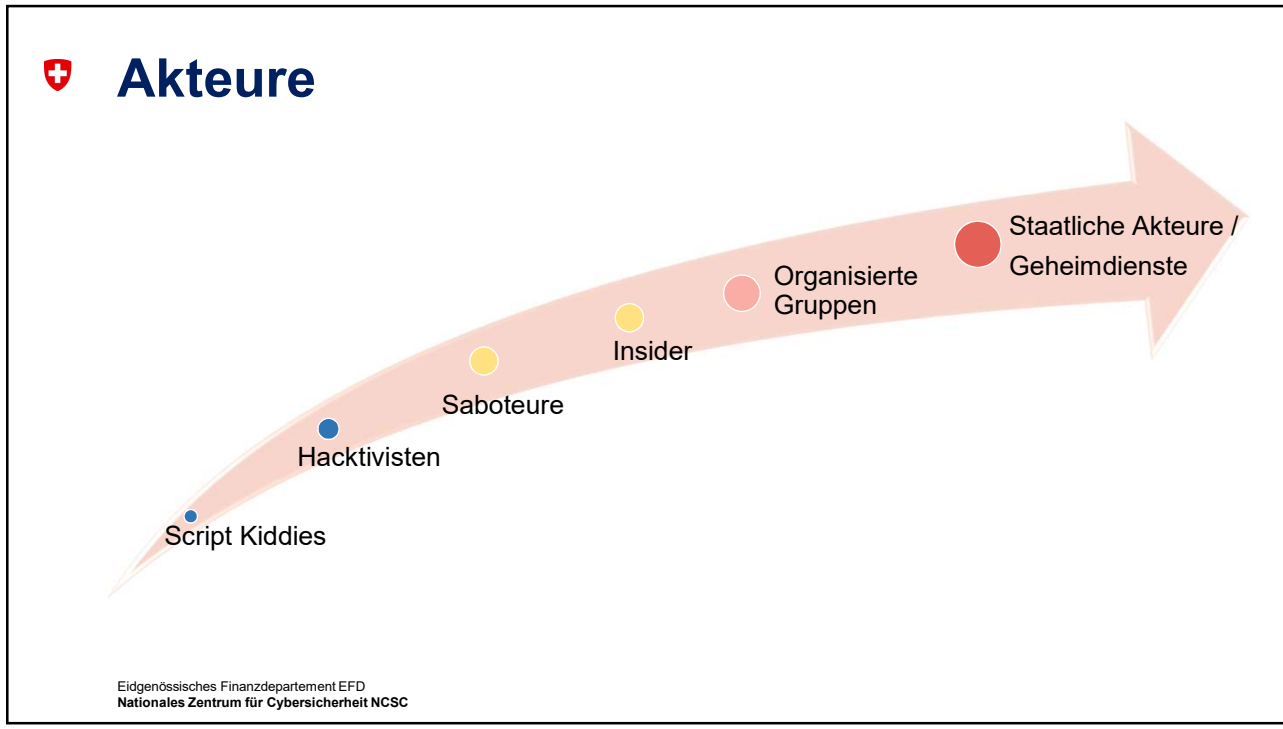


## Aktuelle Bedrohungslage



# Cyber Threat Exchange Liechtenstein

## 26. September 2023



# Cyber Threat Exchange Liechtenstein

## 26. September 2023

### Angriffsvektoren



**COMPROMISED CREDENTIALS**  
describe a case where user credentials, such as usernames and passwords, are exposed to unauthorized entities.

**WEAK AND STOLEN CREDENTIALS**  
Weak passwords and password reuse make credential exposure a gateway for initial attacker access and propagation.

**MALICIOUS INSIDERS**  
an employee who exposes private company information and/or exploits company vulnerabilities.

**POOR ENCRYPTION**  
leads to sensitive information including credentials being transmitted either in plaintext, or using weak cryptographic ciphers or protocols.

**MISCONFIGURATION**  
Misconfiguration is when there is an error in system configuration. Misconfigured devices and apps present an easy entry point for an attacker to exploit.

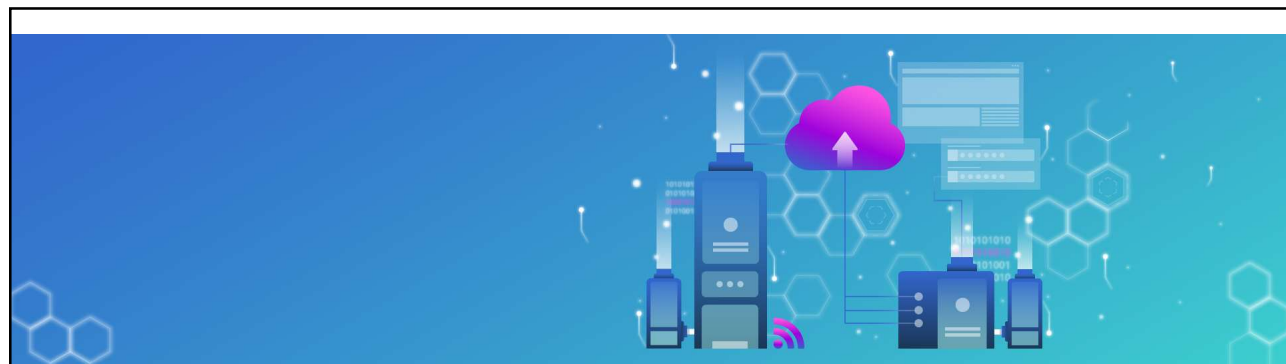
**RANSOMWARE**  
is a form of cyber-extortion in which users are unable to access their data until a ransom is paid.

**PHISHING**  
is a cybercrime tactic in which the targets are contacted by email, telephone or text message by someone posing as a legitimate institution to lure individuals into providing sensitive data

**TRUST RELATIONSHIPS**  
an attacker exploits the trust between two entities to gain unauthorized access to a system or network.



Eidgenössisches Finanzdepartement EFD  
Nationales Zentrum für Cybersicherheit NCSC



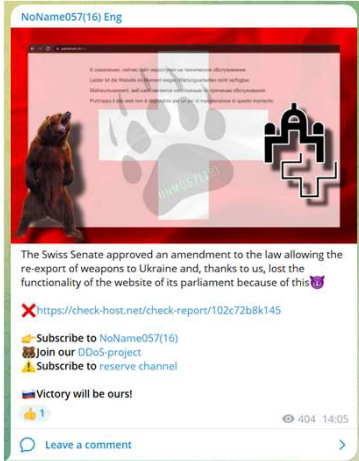
### 3. DDoS-Angriffe vom Juni 2023

# Cyber Threat Exchange Liechtenstein

## 26. September 2023



### DDoS www.parlament.ch



- Angriff vom 7. Juni 2023
- Hintergrund: Zwischenentscheid des Ständerates bezüglich Revision des Kriegsmaterialgesetzes
- Urheber: «NoName057/16»



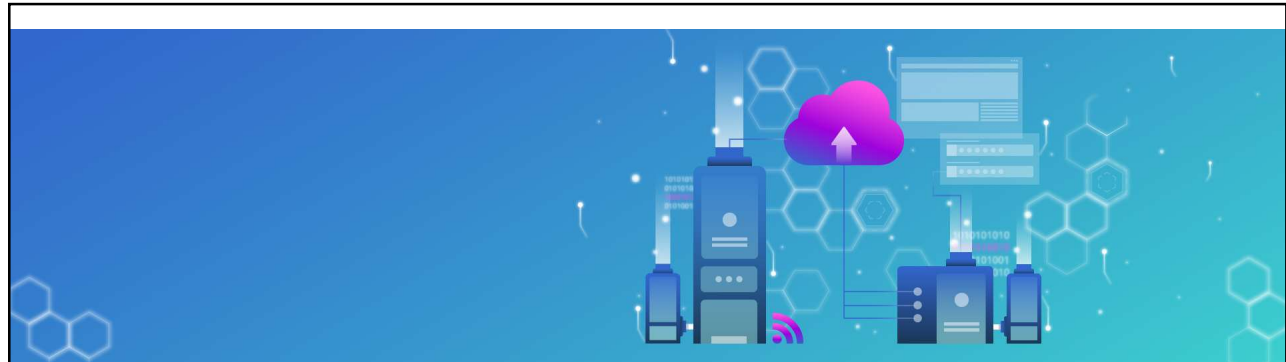
### DDoS gegen zahlreiche Bundes-Websites



- Angriff vom 12. Juni 2023
- Hintergrund: Geplante Online-Rede des ukrainischen Präsidenten vor der Bundesversammlung.
- Urheber: «NoName057/16»
- Weitere Betroffene: Grossunternehmen, Flughäfen, Gemeinden

# Cyber Threat Exchange Liechtenstein

## 26. September 2023



### 4. Ransomwaregruppe «Play»



### Ransomwaregruppe «Play»

<b>EAI</b> USA www.eaiweb.com views: 112 added: 2023-08-10 publication date: 2023-08-14 3 DAYS BEFORE PUBLICATION	<b>Algory Zappia &amp; Associates</b> New South Wales, Australia www.algoryzappia.com.au views: 103 added: 2023-08-10 publication date: 2023-08-16 5 DAYS BEFORE PUBLICATION
<b>Birch, Horton, Bittner &amp; Cherot</b> Alaska, United States www.birchhorton.com views: 2175 added: 2023-08-01 publication date: 2023-08-06 PUBLISHED	<b>Aapd</b> Australia www.aapd.com.au views: 2293 added: 2023-08-01 publication date: 2023-08-06 PUBLISHED
<b>Xplain</b> Switzerland www.xplain.ch views: 20093 added: 2023-07-29 publication date: 2023-08-05 PUBLISHED FULL	<b>Grupo MH</b> Barcelona, Spain www.grupmh.com views: 3926 added: 2023-07-24 publication date: 2023-07-29 PUBLISHED FULL

# Cyber Threat Exchange Liechtenstein

## 26. September 2023





### 5. Meldepflicht für Cybervorfälle


Eidgenössisches Finanzdepartement EFD  
Nationales Zentrum für Cybersicherheit NCSC

15

## Meldepflicht für Cybervorfälle



Schweizerische Eidgenossenschaft  
Confédération suisse  
Confederazione Svizzera  
Confederaziun svizra



BBI 2020  
www.bundesrecht.admin.ch  
Mängeln ist die signierte  
elektronische Fassung

- Bundesrat überweist Botschaft zur Meldepflicht für Cyberangriffe bei kritischen Infrastrukturen
- Vernehmlassung vom 12.01. – 14.02.2022
- Breite Unterstützung bei den KI-Betreibern
- Aktuell abschliessende Beratungen im Parlament

**Bundesgesetz  
über die Informationssicherheit beim Bund  
(Informationssicherheitsgesetz, ISG)**

Änderung vom ...

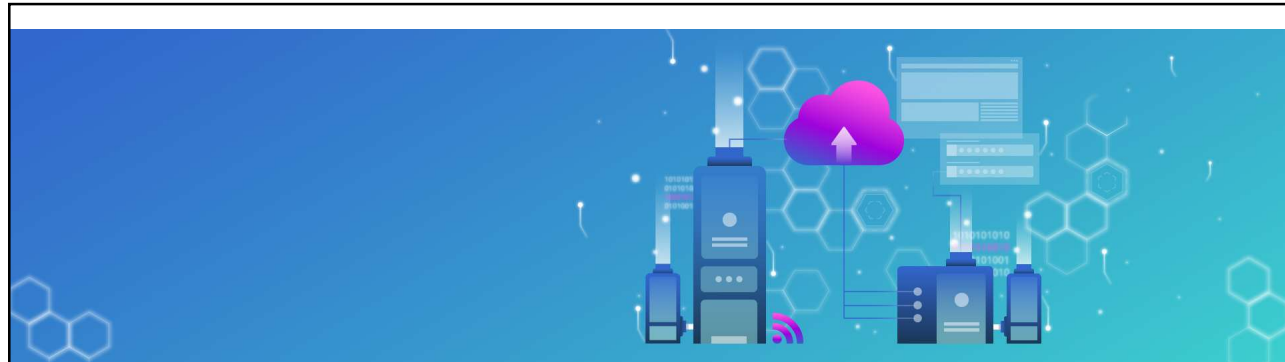
Eidgenössisches Finanzdepartement EFD  
Nationales Zentrum für Cybersicherheit NCSC

16



# Cyber Threat Exchange Liechtenstein

## 26. September 2023



### 6. So unterstützt das NCSC liechtensteinische Unternehmen



### Unterstützung durch das NCSC: Grundlage und Bedingungen

- Grundlage:
  - Bilaterales Abkommen CH / FL betr. subsidiärem Schutz kritischer Infrastrukturen vor Cyberangriffen.
- Bedingungen für den Beitritt in den «geschlossenen Kundenkreis»:
  - Zugehörigkeit zu einem der vom BABS als kritisch definierten Sektoren <https://www.babs.admin.ch/de/aufgabenbabs/ski/kritisch.html>
  - Unternehmen mit Sitz in der CH oder im FL
  - Mindestens eine Person im Unternehmen muss eine IT-Rolle wahrnehmen (z.B. CISO, IT-Leiter, Netzwerkadministrator usw.)
- Bei Interesse: E-Mail an [ncsc-useraccounts@gs-efd.admin.ch](mailto:ncsc-useraccounts@gs-efd.admin.ch)

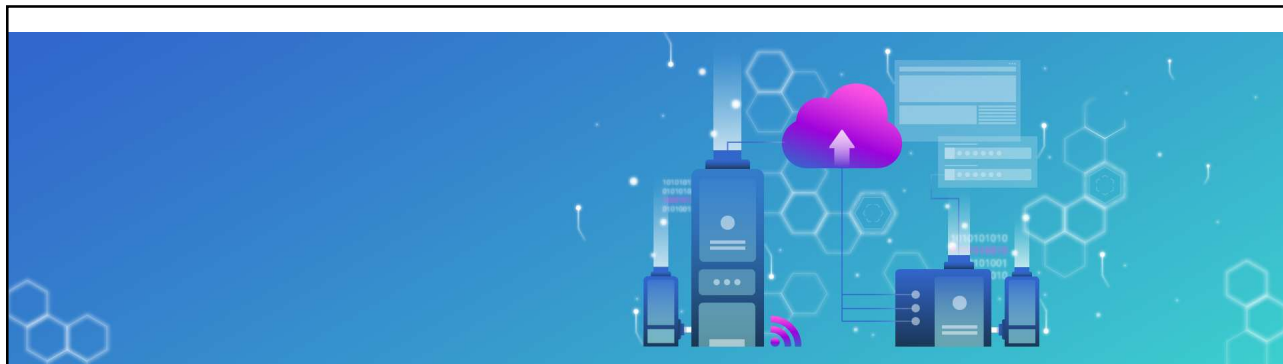
# Cyber Threat Exchange Liechtenstein

## 26. September 2023



### Unterstützung durch das NCSC: Dienstleistungen

Vorteile	Nachteile
<p><b>Prävention/Detektion:</b></p> <ul style="list-style-type: none"><li>• Zugriff auf öffentlich nicht zugängliche Informationen</li><li>• Alle Informationen sind verifiziert</li></ul> <p><b>Incident Handling:</b></p> <ul style="list-style-type: none"><li>• Pikett-Nummer (7x24) / Notfall-Mailadresse</li><li>• Unterstützung beim Incident Handling</li><li>• Auf Wunsch Beratung vor Ort</li><li>• Vermittlung von Kontakten zur Strafverfolgung</li></ul> <p><b>Sonstiges:</b></p> <ul style="list-style-type: none"><li>• Weekly Cyber Security Briefing / Roundtables</li><li>• Keine Mitwirkungspflicht</li><li>• Kostenlose Dienstleistungen</li></ul>	<ul style="list-style-type: none"><li>• Best Effort</li></ul>

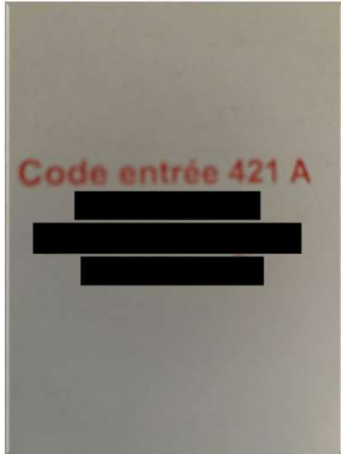


## 7. Zum Schluss noch dies...

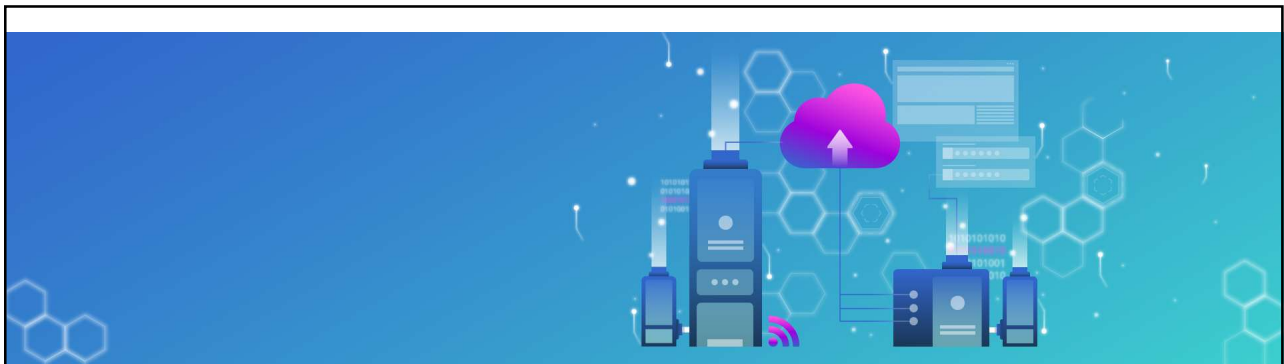
# Cyber Threat Exchange Liechtenstein

## 26. September 2023

### Ein Beispiel für sinnlose Security



Eidgenössisches Finanzdepartement EFD  
Nationales Zentrum für Cybersicherheit NCSC



**Vielen Dank für Ihre Aufmerksamkeit**

Eidgenössisches Finanzdepartement EFD  
Nationales Zentrum für Cybersicherheit NCSC

22