ARES

CYBER INTELLIGENCE

Emitec ITMK 2023

“Prepared for the unknown”

Jürgen Weiss

> 200 Incidents

Cyber Crisis Manager // Negotiations // Cybercrime Profiler

Open Source & Darknet Intelligence

Cyber Crisis Mgt. (NIST USA)

Negotiations, Profiling (Israel)

est. 2019

WIR

Gründung2019
Headquarter Traun (AT)
Security Operations (RO)

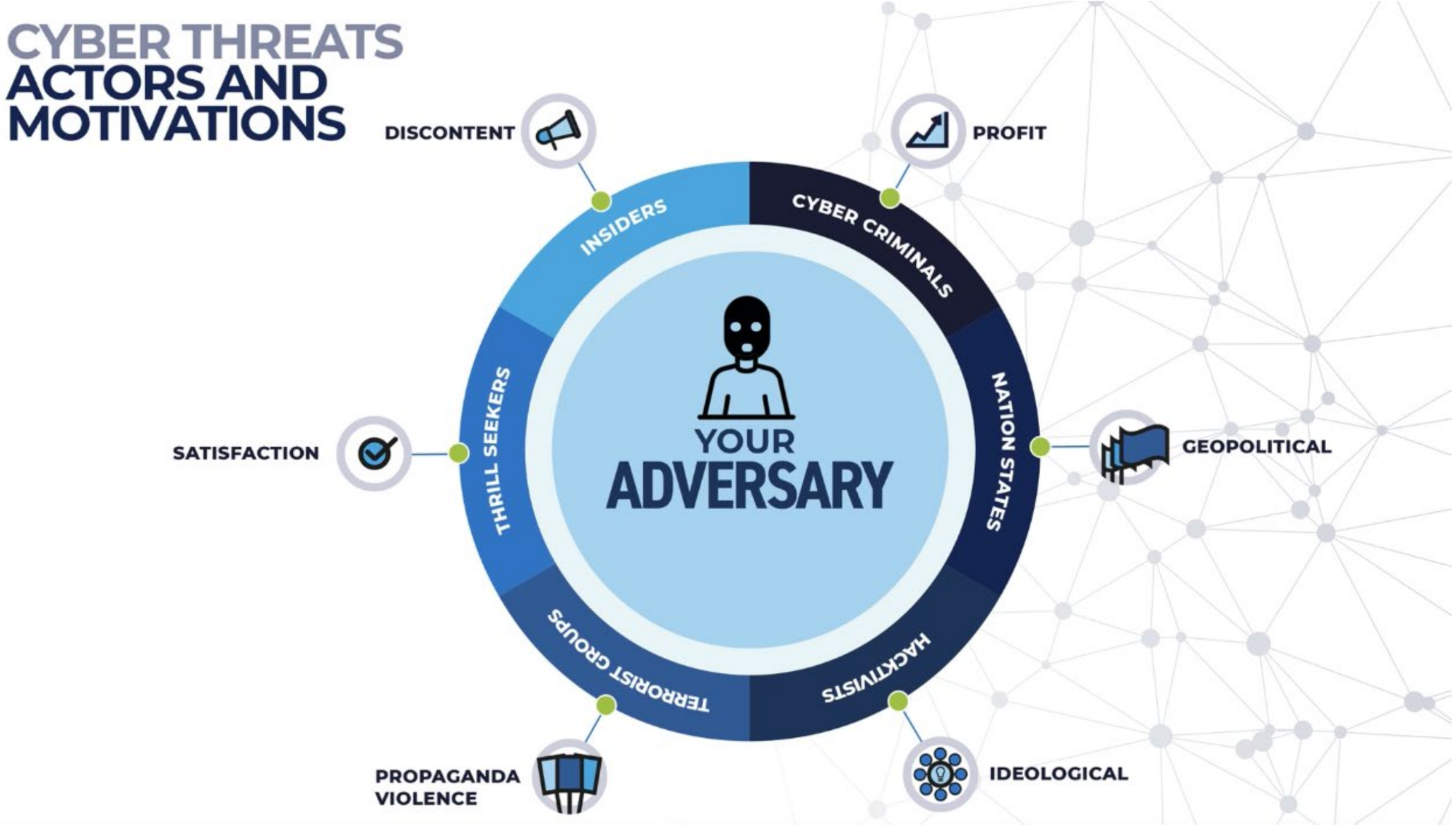
ENYO Cyber Intelligence AG (CH)
ELYRION LLC (UAE

est. 2019

ares-ci.com

PREPARED FOR THE UNKNOWN

CYBER Criminals (HACKER)



THE UNDERGROUND CYBERCRIME ECONOMY

ORGANISATIONAL LEADERS
Often "People Persons" without technical skills. The leaders assemble the team and choose the target

PROGRAMMERS
Who develop the exploits and malware to commit cybercrimes

TELLERS
Who are charged with transferring and laundering illicitly gained proceeds through digital/crypto currency services and different world currencies.

DISTRIBUTORS
Who trade and sell stolen data and act as escrows for the goods/services provided by other specialists

MONEY MULES
Who complete electronic transfers between bank accounts. The money mules often use students and a combination of "witting" and "unwitting" agents

TECH EXPERTS
Who maintain the criminal enterprise's IT infrastructure, including servers, encryption technologies, databases and more

CASHIERS
Who control drop accounts and provide names and accounts to other criminals for a fee

HACKERS
Who search for and exploit applications, systems and network vulnerabilities

HOSTED SYSTEM PROVIDERS
Who offer safe hosting "bullet proof hosting" of illicit content servers and sites

FRAUDSTERS
Who create and deploy various social engineering schemes, such as phishing and spam

CYBERCRIME PRICELIST

ATTACK TOOLS

MALWARE

BASIC BANKING TROJAN KIT WITH SUPPORT	€100	OFFICE MACRO DOWNLOADER GENERATOR	€5
PASSWORD STEALING TROJAN	€25-100	MALWARE CRYPTER SERVICE (MAKE HARD TO DETECT)	€20-40
ANDROID BANKING TROJAN	€200	RANSOMWARE KIT	€10-1800

RANSOMWARE

SOPHISTICATED LICENSE FOR WIDESPREAD ATTACK	€200	PC MALWARE INSTALLATION	€1
UNSOPHISTICATED LICENSE FOR TARGETED ATTACK	€50	1 MILLION MALICIOUS SPAM	€400

SOFTWARE

REMOTE DESKTOP CONTROL TOOL	€100	DISTRIBUTED DENIAL OF SERVICE ATTACK SOFTWARE	€700

PAYMENT

CREDIT/ DEBIT CARD FOR ONLINE USE	€5	BANK ACCOUNT LOG-IN WITH ACCESS TO MAIL, SECURITY ANSWER, ETC	€25
CREDIT/DEBIT CARD INFO THAT CAN BE CLONED ON PLASTIC	€10	EXISITNG PAYPAL ACCOUNT	€1
BANK ACCOUNT LOG-IN (USERNAME AND PASSWORD)	€5		

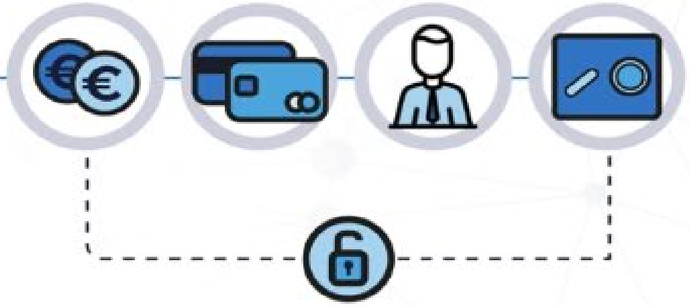
DATA

PERSONAL INFORMATION

SOCIAL SECURITY AND DATE OF BIRTH VERIFICATION	€3	CREDIT REPORT 750+ CREDIT SCORE	€150

DATABASE RECORDS

1 MILLION COMPROMISED EMAIL / PASSWORDS	€25



SERVICES

HACKING

EMAIL ACCOUNT	€100	SOCIAL MEDIA ACCOUNT	€100
CMS WEBSITE ('WORDPRESS,ETC)	€300		

MALWARE

PC MALWARE INSTALLATION	€1	MALICIOUS FILE ENCRYPTION	€25

USER OBFUSCATION

BULLET PROOF HOSTING IN A LAX JURISDICTION (CHINA, EASTERN EUROPE, ETC)	€150	VIRTUAL PRIVATE NETWORK (VPN)	€20

FAKE DOCUMENTS

DIGITAL COPY OF FAKE CREDIT / DEBIT CARD	€25	DIGITAL COPY OF FAKE UTILITY BILL OR SOCIAL SECURITY CARD	€15
DIGITAL COPY OF FAKE DRIVER'S LICENSE OR PASSPORT	€25		

DDoS

DDoS SERVICE 24 HR DURATION	€50-1000

SPAM

500 SMS (FLOODING)	€20	1 MILLION EMAIL SPAM	€200
500 PHONE CALLS (FLOODING)	€20		

Cyber Threats

Industrie „eSpionage“

- Insider Threat / State Actors

- Gefälschte eMails – Spear Phishing
- Infiltrieren der IT-Infrastruktur
- Übernahme eMail Accounts und Weiterleitung der eMails

- Diebstahl von IP´s
- Diebstahl von Geschäftsgeheimnissen
- Verkauf oder Verwendung

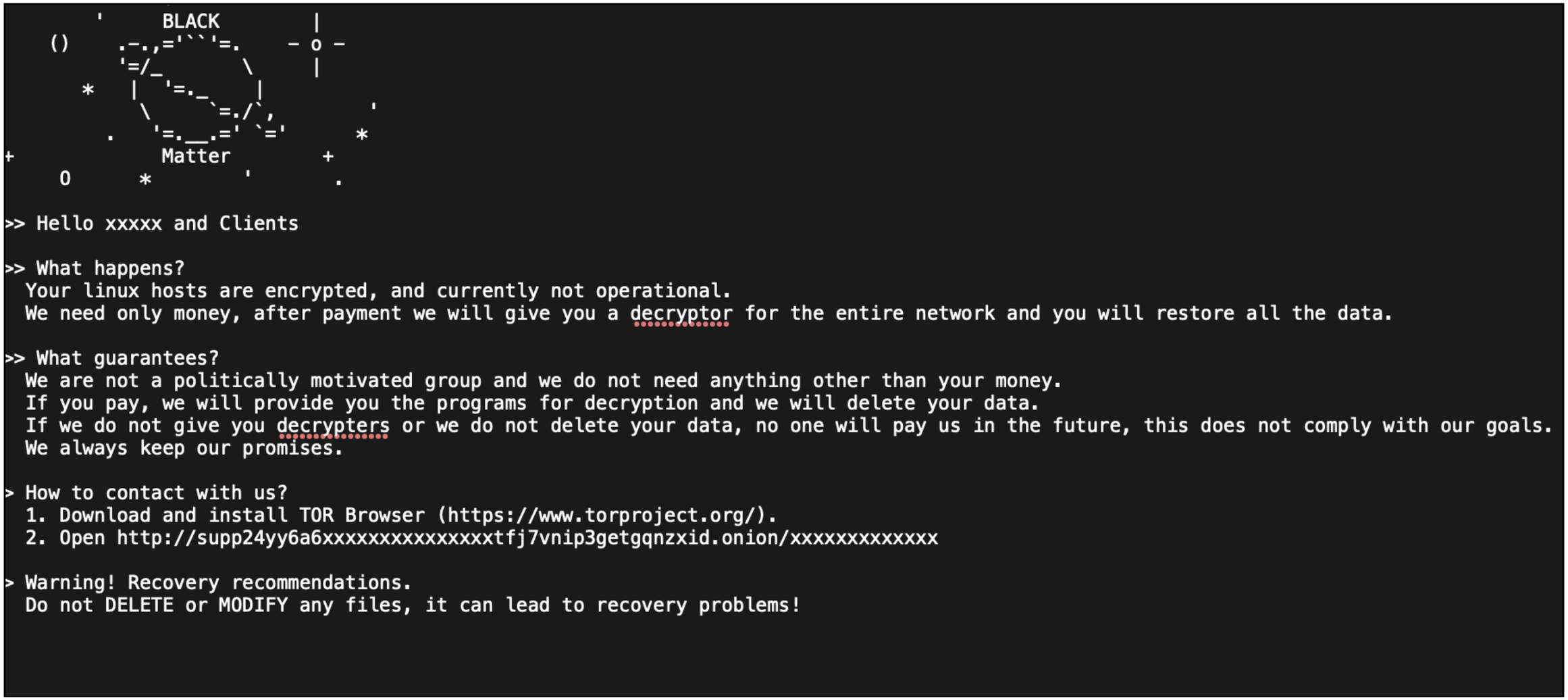
Ransomware

- Attackieren IT/OT-Systeme
- Verschlüsseln Server, Datenbanken und Backups
- Datenlöschung/-zerstörung
- Datenexfiltration
- Datenverkauf an Dritte
- Industrie Spionage

„HOW DOES IT FEEL?“

Incident Response Team

- Cyber Crisis Manager
- Forensik
- Malware Analyst
- Reverse Engineer
- IT-Spezialist
- OT-Spezialist
- Compliance


BLACK
Matter
>> Hello xxxxx and Clients
>> What happens?
Your linux hosts are encrypted, and currently not operational.
We need only money, after payment we will give you a decryptor for the entire network and you will restore all the data.
>> What guarantees?
We are not a politically motivated group and we do not need anything other than your money.
If you pay, we will provide you the programs for decryption and we will delete your data.
If we do not give you decrypters or we do not delete your data, no one will pay us in the future, this does not comply with our goals.
We always keep our promises.
> How to contact with us?
1. Download and install TOR Browser (https://www.torproject.org/).
2. Open http://supp24yy6a6xxxxxxxxxxxxxxxtfj7vnip3getgqnzxid.onion/xxxxxxxxxxxx
> Warning! Recovery recommendations.
Do not DELETE or MODIFY any files, it can lead to recovery problems!

Via Darknet!

Hello!

You have to pay $950 000 to our Bitcoin address.
After payment you will get:
1) Decryption software
2) We will not use the information obtained from your network
3) All data downloaded from your network will be deleted
4) Your company will not be attacked anymore
5) You will get security advice and a list of vulnerabilities that were used to attack your network

We have downloaded a large amount of confidential data from your network.
A complete list of files and samples will be provided upon request.

We can decrypt a couple of files for free.
The size of each file must be no more than 5 megabytes.

Via Mail

Ransomware Profiling

- Profi oder Beginner?
- Art der Kommunikation?
- Agressiv oder Passiv?
- Bekannte oder neue Eigenheiten?
- Zeitpunkt der Kommunikation?
- Qualifizierung von Datendiebstahl?
- Lösegeldforderung?

Auf was kommts an?

- Schnelle Reaktion auf den Vorfall
- Erfahrung durch Spezialisten
- Qualifikation der Bedrohungsart
- Analyse der Angriffsvektoren
- Qualität des Backups
- Gezielte Kommunikation intern/extern
- Absicherung der Assets
- Stufenweiser gesicherter Wiederbetrieb

DECISION MAKING

COST OF **NO** DEAL

- Keine Lösegeldzahlung!
- Folgenabschätzung (Zeit, Kosten,…)
- Abschätzung der Gefahr durch Datenverkauf an Dritte
- Abschätzung der Gefahr durch Data Leakage (IP)
- Reputationsschaden
- Geldbuße lt. Behörde/NIS2 (min. 500K)
- Maßnahmen zu Sicherung, Monitoring, etc.
- Investitionen IT-Neu

COST OF DEAL

- Verhandlungsoptionen/-ziele definieren
- Bewertung von Proofs
- Bewertung des Decryptors
- Transaktion Digitale Währung (Bitcoin, Monero)
- Vorbereitung Transaktion (Wallet) durch externe DL (KYC)
- Behörden informieren - Geldwäschegesetz
- Testsystem und Produktivsystem NEU aufsetzen
- Abschätzung Zeitaufwand für Decryption, Säubern, Datenbewertung
- Kostenschätzung neue IT-Infrastruktur

CASE #1

Produzierendes Unternehmen, ca. 500 Mitarbeiter

Ransomware: **LV** Lösegeldforderung USD 500.000.- in Bitcoins
Verlust/ Tag: EUR 600.000.--

10 Tage – Einzelunternehmer als „Krisenexperte“ im Einsatz

Fehlende Erfahrung in Verhandlungsführung und Bewertung des Schadens, keine Forensik-Ausbildung
Lösegeldzahlung ohne Entscheidungsgrundlage und Bewertung des Decryptors durchgeführt
Unnötiger „Produktverkauf“

Schaden für Unternehmen bei EUR 6 Mio
+ Lösegeld
+ neue Produkte wie Firewalls und Antiviren Software

ARES DFIR Team
Neues Lagebild erstellen, Bewertung des Decryptors, Migration Office365 binnen 4 Stunden, Wiederanlauf der Produktion binnen 72 Stunden in gesicherten Modus

CASE #2

Produzierendes Unternehmen, ca. 150 Mitarbeiter

Ransomware: **Decrypt4you** Lösegeldforderung USD 50.000.- in Bitcoins
Verlust/ Tag: EUR 70.000.--

IT-Dienstleister als Ersthelfer im Einsatz

Unqualifiziertes Einspielen des einzig unbeschädigten Backups auf kompromittierte Infrastruktur!
Keine vorherige Analyse und Lagebilderhebung

FAZIT – letztmögliches Backup verschlüsselt

ARES DFIR Team
Erstgespräch Freitags Vormittag, Bewertung der Bedrohung und Lagebild, Infrastruktur NEU aus gesicherten DataCenter, Forensik analysiert Verschlüsselung durch Reverse Engineering binnen 24 Stunden wurde das Backup wiederhergestellt.

ERP-Datenbank gerettet – KEINE Insolvenzanmeldung!

CASE #3

Internationales Unternehmen, ca. 250 Mitarbeiter

Ransomware: **LOCKBIT 3.0** Lösegeldforderung USD 700.000.- in Bitcoins
Verlust/ Tag: EUR 100.000.--

Unternehmen liefert Dokumentation und Beschreibungen an Luftfahrtindustrie

Verdacht auf Industriespionage // Verdacht auf Innentäter oder Mitwissenden

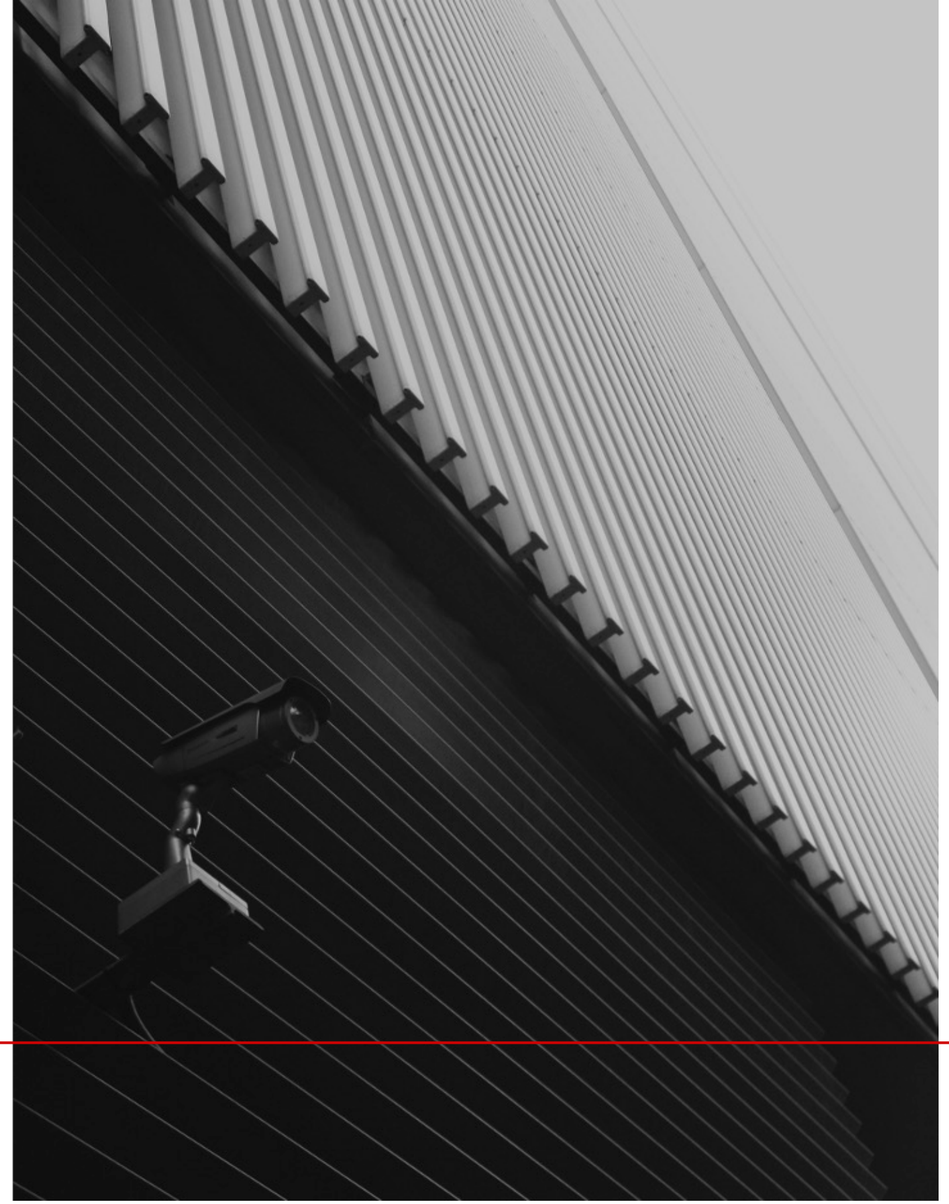
ARES DFIR Team

Einsatz vor Ort, Erstellung des Lagebildes und der Infrastruktur, Bewertung vorhandener Informationen wie LOG-Files
Verhandlungsführung auf 2 Kanälen (Käufer von Daten / Lösegeldverhandlung)

Analyse Schadensausmaß und Wiederherstellungskonzept, sowie Absicherung unversehrter Assets

Zielperson Identifikation, Personen Background Check, Observation

GET IN TOUCH



www.myincident.ai

emergency@arescti.com

+43 800 0800 22

est. 2019