In the Line of Fire

Lernen Sie Ihre neuen Gegner frühzeitig kennen.

Thorsten Urbanski, Head of Communication DACH
Leiter der TeleTrusT Arbeitsgruppe IT Security made in EU

Digital Security
Progress. Protected.

Wer wir sind:

- **Nummer Eins** EU Cybersecurity Hersteller im Business-Segment
- **1Milliarde+** Internetnutzer werden weltweit durch ESET-Technologien geschützt.
- **400K+** Unternehmenskunden
- **110M** Millionen Anwender

MITSUBISHI MOTORS
Drive your Ambition

Allianz
Suisse

Canon
Canon Marketing Japan Group

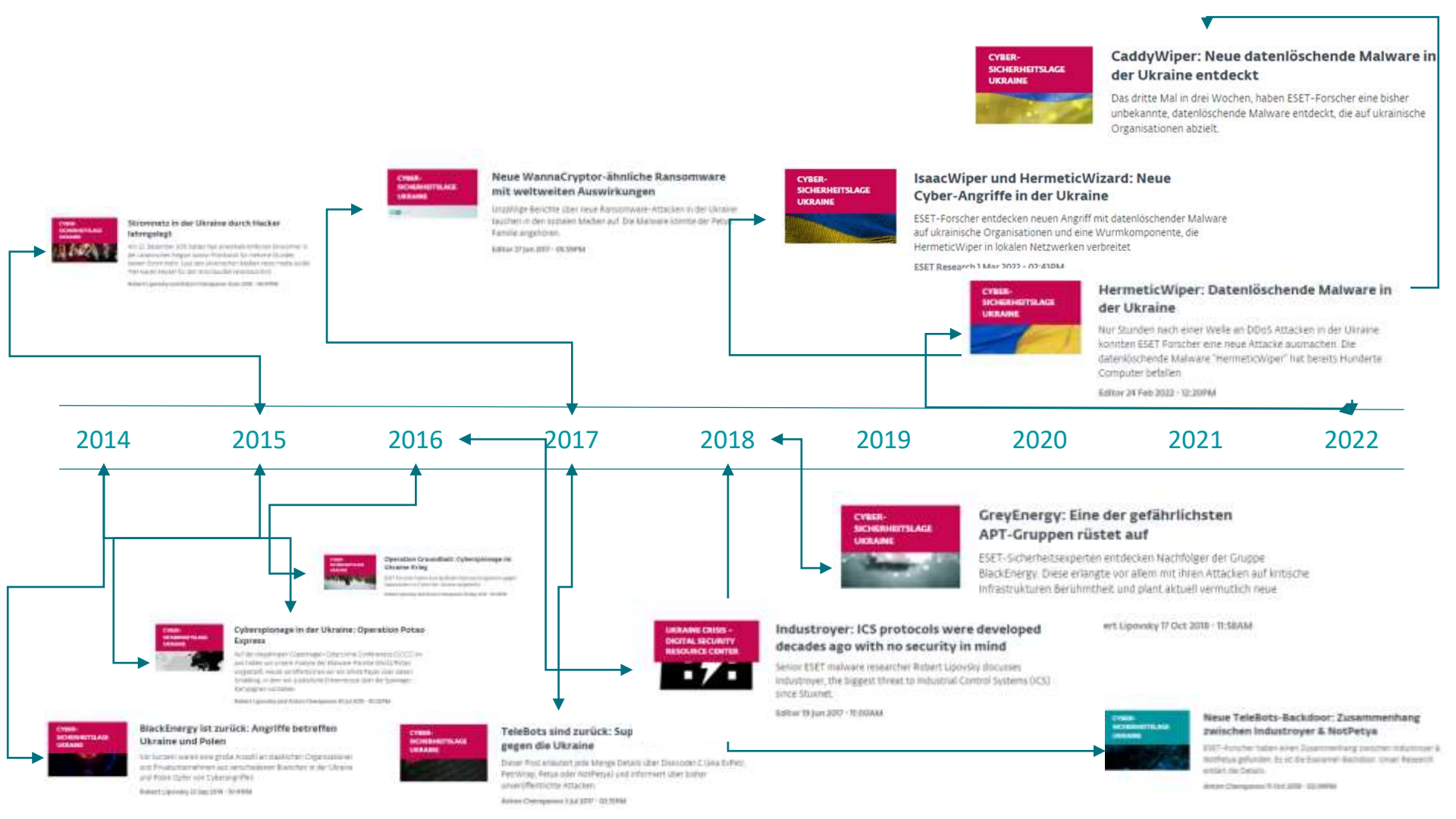
T . .

Globale Ausrichtung

- In 202 Ländern weltweit vertreten
- 13 Global R&D Centres
- Offices in 23 Ländern
- 100 % Made in EU
- 30 Jahre ESET Technolgie

UKRAINE: CHRONOLOGIE

Digital Security
Progress. Protected.

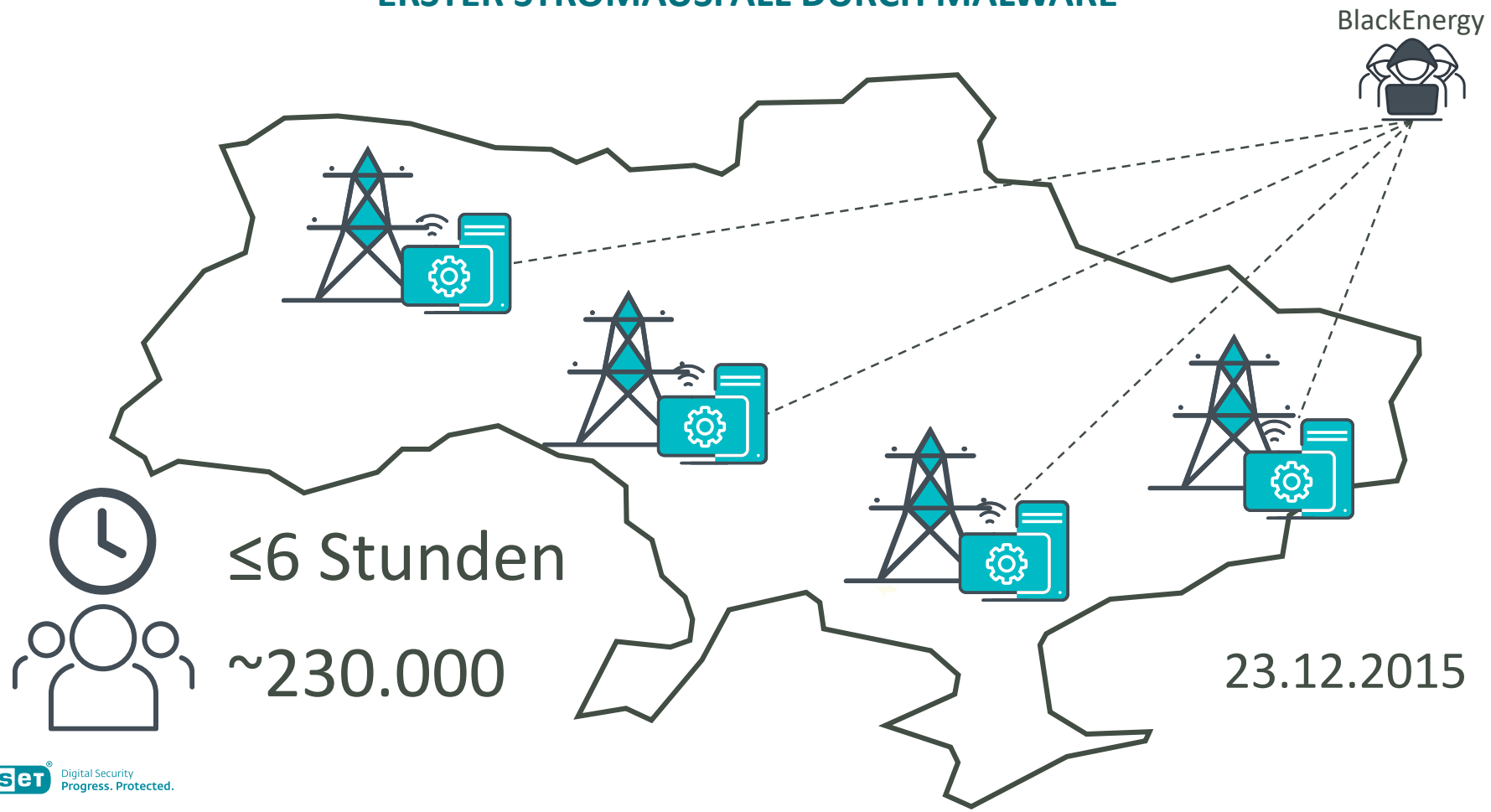

CaddyWiper: Neue datenlöschende Malware in der Ukraine entdeckt
Das dritte Mal in drei Wochen, haben ESET-Forscher eine bisher unbekannte, datenlöschende Malware entdeckt, die auf ukrainische Organisationen abzielt.
Neue WannaCryptor-ähnliche Ransomware mit weltweiten Auswirkungen
IsaacWiper und HermeticWizard: Neue Cyber-Angriffe in der Ukraine
ESET-Forscher entdecken neuen Angriff mit datenlöschender Malware auf ukrainische Organisationen und eine Wurmkomponente, die HermeticWiper in lokalen Netzwerken verbreitet
HermeticWiper: Datenlöschende Malware in der Ukraine
Nur Stunden nach einer Welle an DDoS Attacken in der Ukraine konnten ESET Forscher eine neue Attacke ausmachen. Die datenlöschende Malware "HermeticWiper" hat bereits Hunderte Computer befallen
2014
2015
2016
2017
2018
2019
2020
2021
2022
GreyEnergy: Eine der gefährlichsten APT-Gruppen rüstet auf
ESET-Sicherheitsexperten entdecken Nachfolger der Gruppe BlackEnergy. Diese erlangte vor allem mit ihren Attacken auf kritische Infrastrukturen Berühmtheit und plant aktuell vermutlich neue
Cyberspionage in der Ukraine: Operation Potao Express
Industroyer: ICS protocols were developed decades ago with no security in mind
Senior ESET malware researcher Robert Lipovsky discusses Industroyer, the biggest threat to Industrial Control Systems (ICS) since Stuxnet.
BlackEnergy ist zurück: Angriffe betreffen Ukraine und Polen
TeleBots sind zurück: Sup gegen die Ukraine
Neue TeleBots-Backdoor: Zusammenhang zwischen Industroyer & NotPetya

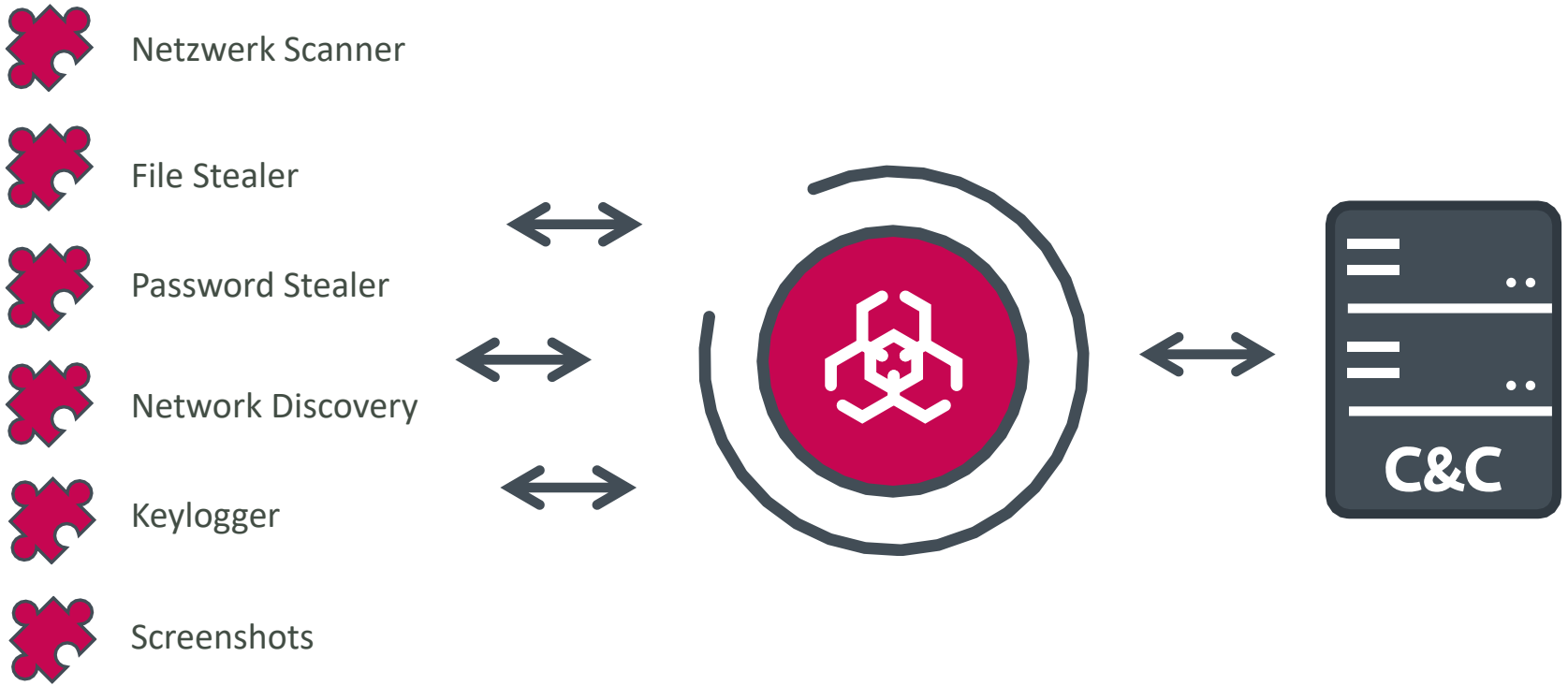
UKRAINE: 2015

Digital Security
Progress. Protected.

BlackEnergy

ERSTER STROMAUSFALL DURCH MALWARE




Netzwerk Scanner
File Stealer
Password Stealer
Network Discovery
Keylogger
Screenshots
C&C
Module
BlackEnergy

GAMECHANGER 2016

Digital Security
Progress. Protected.

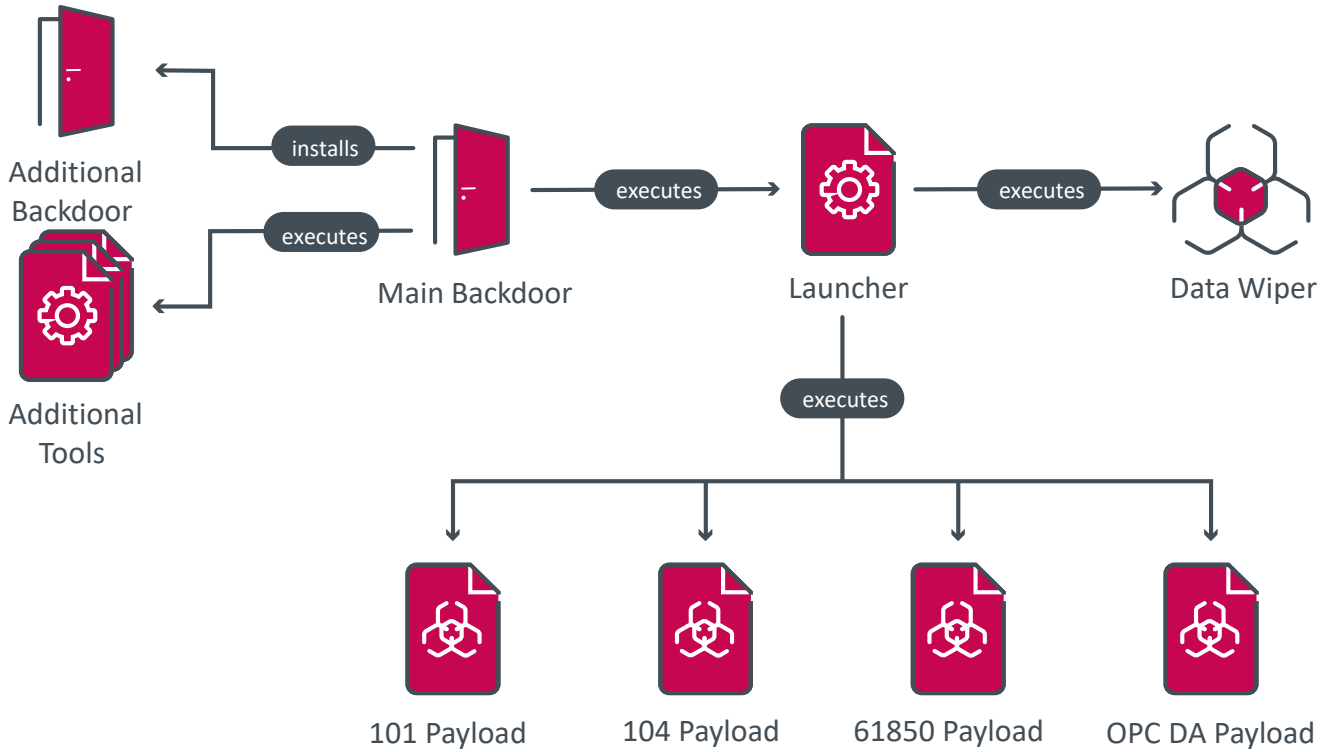
17. Dezember 2016

Angriffsziel:
KRITIS; Stromversorgung in Kiew

Auswirkungen:
Blackout

INDUSTROYER

Industroyer Architektur



WAS IST SO BESONDERS AN INDUSTROYER?

INDUSTROYER

2022: WIPER-MALWARE

Digital Security
Progress. Protected.

HermeticWiper-Kampagne

HermeticWiper

HermeticWizard

HermeticRansom

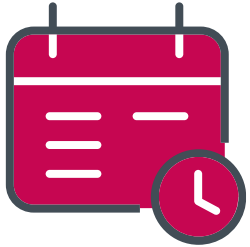
HermeticWiper

>100

Systeme

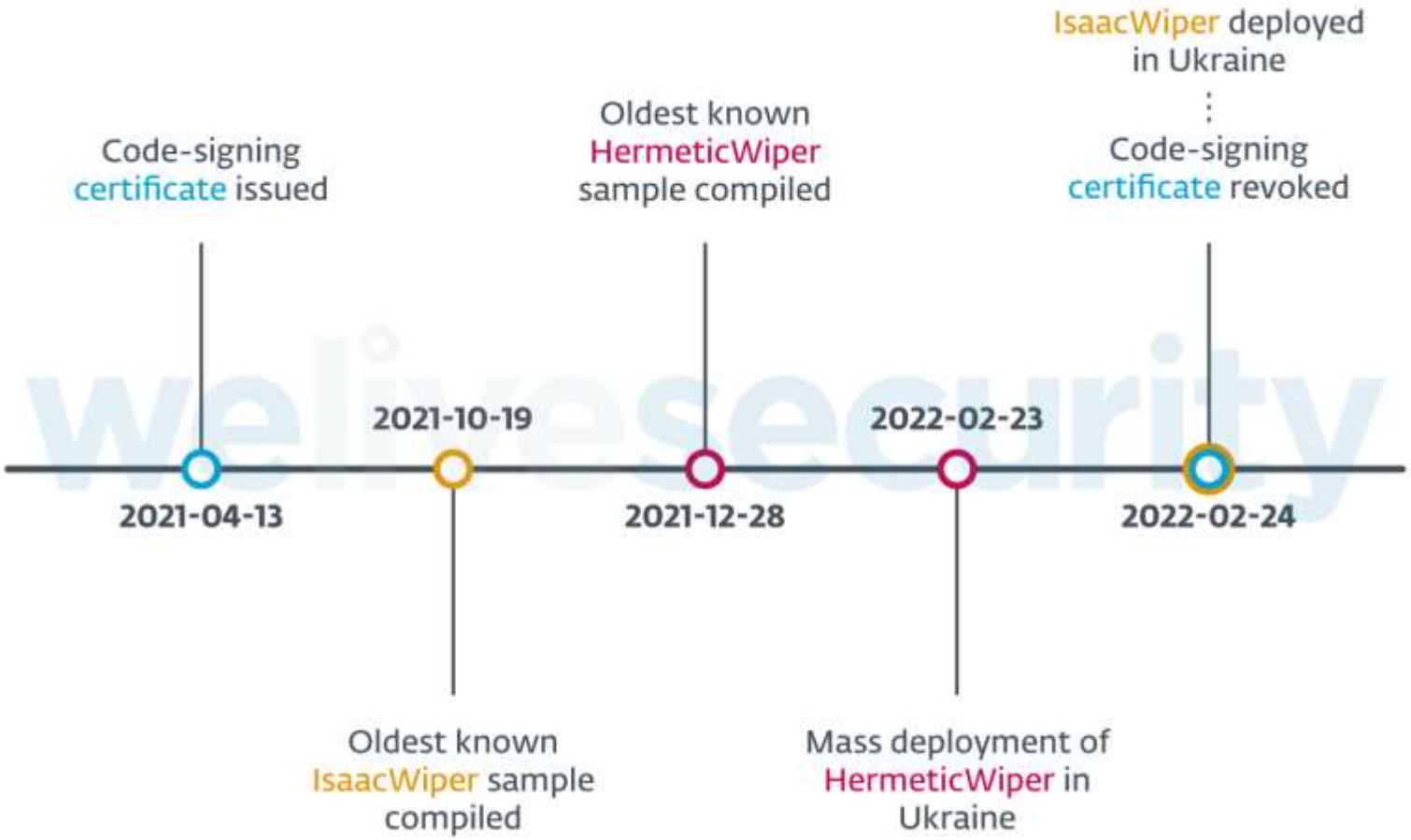
5+

Organisationen



28. Dez. 2021

Compilation Timestamp


IsaacWiper deployed in Ukraine
Code-signing certificate issued
Oldest known HermeticWiper sample compiled
Code-signing certificate revoked
2021-10-19
2022-02-23
2021-04-13
2021-12-28
2022-02-24
Oldest known IsaacWiper sample compiled
Mass deployment of HermeticWiper in Ukraine

STAATLICHE AKTEURE!

Digital Security
Progress. Protected.

Energetic Bear

The Dukes
Cozy Bear/APT29

Sandworm
Telebots
/Voodoo Bear

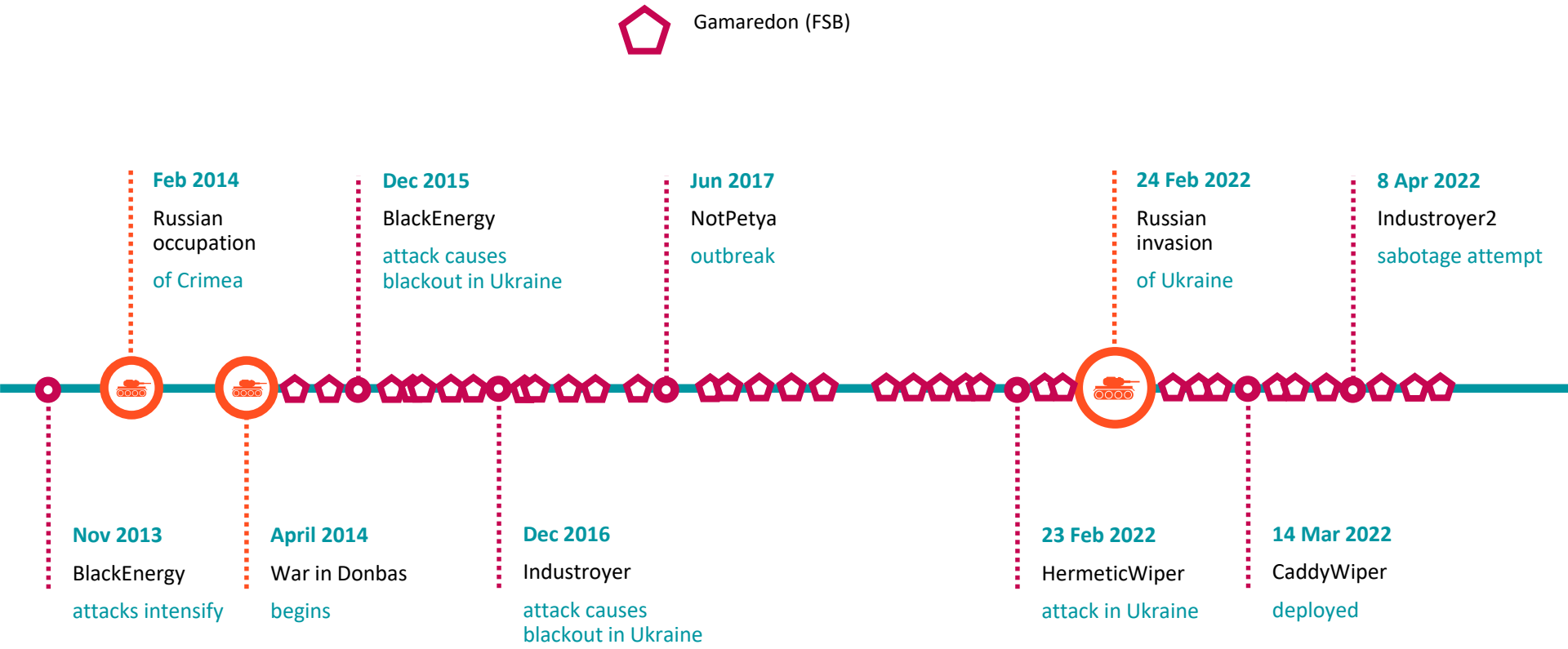
Turla

InvisiMole

Sednit
Fancy Bear/APT28

Gamaredon

Buhtrap


Gamaredon (FSB)
Feb 2014
Russian occupation of Crimea
Dec 2015
BlackEnergy attack causes blackout in Ukraine
Jun 2017
NotPetya outbreak
24 Feb 2022
Russian invasion of Ukraine
8 Apr 2022
Industroyer2 sabotage attempt
Nov 2013
BlackEnergy attacks intensify
April 2014
War in Donbas begins
Dec 2016
Industroyer attack causes blackout in Ukraine
23 Feb 2022
HermeticWiper attack in Ukraine
14 Mar 2022
CaddyWiper deployed

Buhtrap

InvisiMole

Energetic Bear

The Dukes

Cozy Bear/APT29

Sandworm

Telebots
/Voodoo Bear

Turla

Sednit

Fancy
Bear/APT28

Gamaredon

FSB

SVR

GRU

Sources:

FBI

National Cyber Security Centre

Militaire Inlichtingen en Veiligheidsdienst

SECURITY SERVICE OF UKRAINE

Microsoft

RELEVANZ FÜR DEUTSCHLAND
STATUS UND RÜCKBLICK

Digital Security
Progress. Protected.

MÖGLICHE AUSWIRKUNGEN

- **Bei einer weiteren Eskalation des Konflikts könnten andere Länder stärker als zuvor in den Fokus staatlich motivierter Cyberangriffe geraten.**
- **Es ist nicht auszuschließen, dass Computersysteme kleinerer Versorgungsunternehmen, z.B. lokale Energieversorger bereits erfolgreich infiltriert wurden.**

Presse

253 IT-Störungen

Zahl der IT-Störungen Kritischer Infrastrukturen

Inneres und Heimat/Antwort - 12.10.2022 (hib 532/2022)

Berlin: (hib/STO) Dem Bundesamt für Sicherheit in der Informationstechnik (BSI) sind laut Bundesregierung seit dem Beginn des russischen Angriffskrieges gegen die Ukraine am 24. Februar dieses Jahres bis zum 9. September insgesamt 253 IT-Störungen Kritischer Infrastrukturen gemeldet worden. Neben Cyber-Angriffen zählen dazu auch Ausfälle von Hard- und Software oder IT-Störungen allgemeiner Art, wie aus der Antwort der Bundesregierung (20/3762) auf eine Kleine Anfrage der CDU/CSU-Fraktion (20/3308) weiter hervorgeht. Danach ist das BSI gemäß Paragraf 8b des BSI-Gesetzes die zentrale Meldestelle für Betreiber Kritischer Infrastrukturen in Angelegenheiten der Sicherheit in der Informationstechnik.

Herausgeber

Deutscher Bundestag, Parlamentsnachrichten

Verantwortlich: Christian Zentner (V.i.S.d.P.)
Redaktion: Lisa Brüßler, Claudia Heine, Alexander Heinrich, Nina Jeglinski, Claus Peter Kosfeld, Hans-Jürgen Leersch, Johanna Metz, Elena Müller, Sören Christian Reimer, Sandra Schmid, Michael Schmidt, Helmut Stoltenberg, Alexander Weinlein

› Herausgeber "heute im bundestag" (hib)

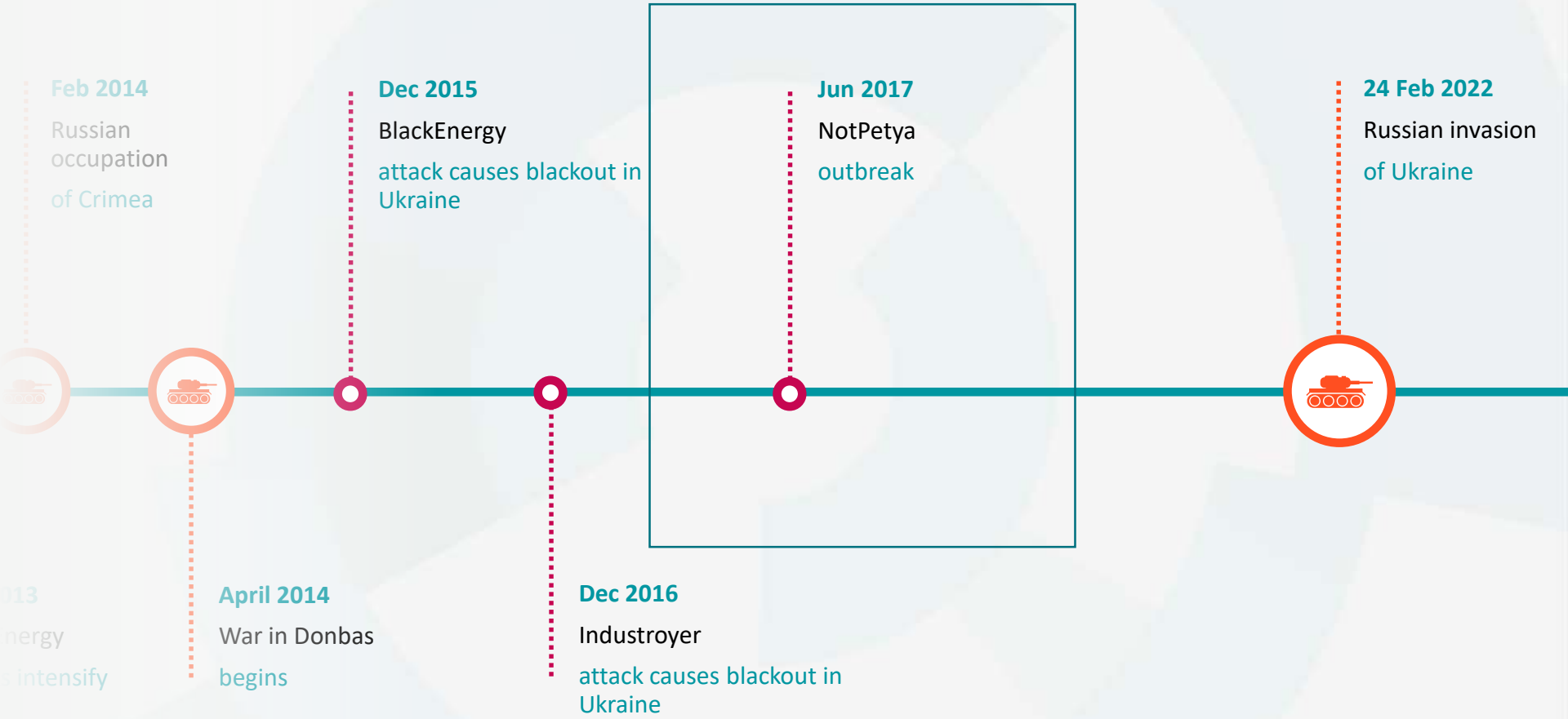
Abonnement

› Newsletter abonnieren
› RSS-Dienste

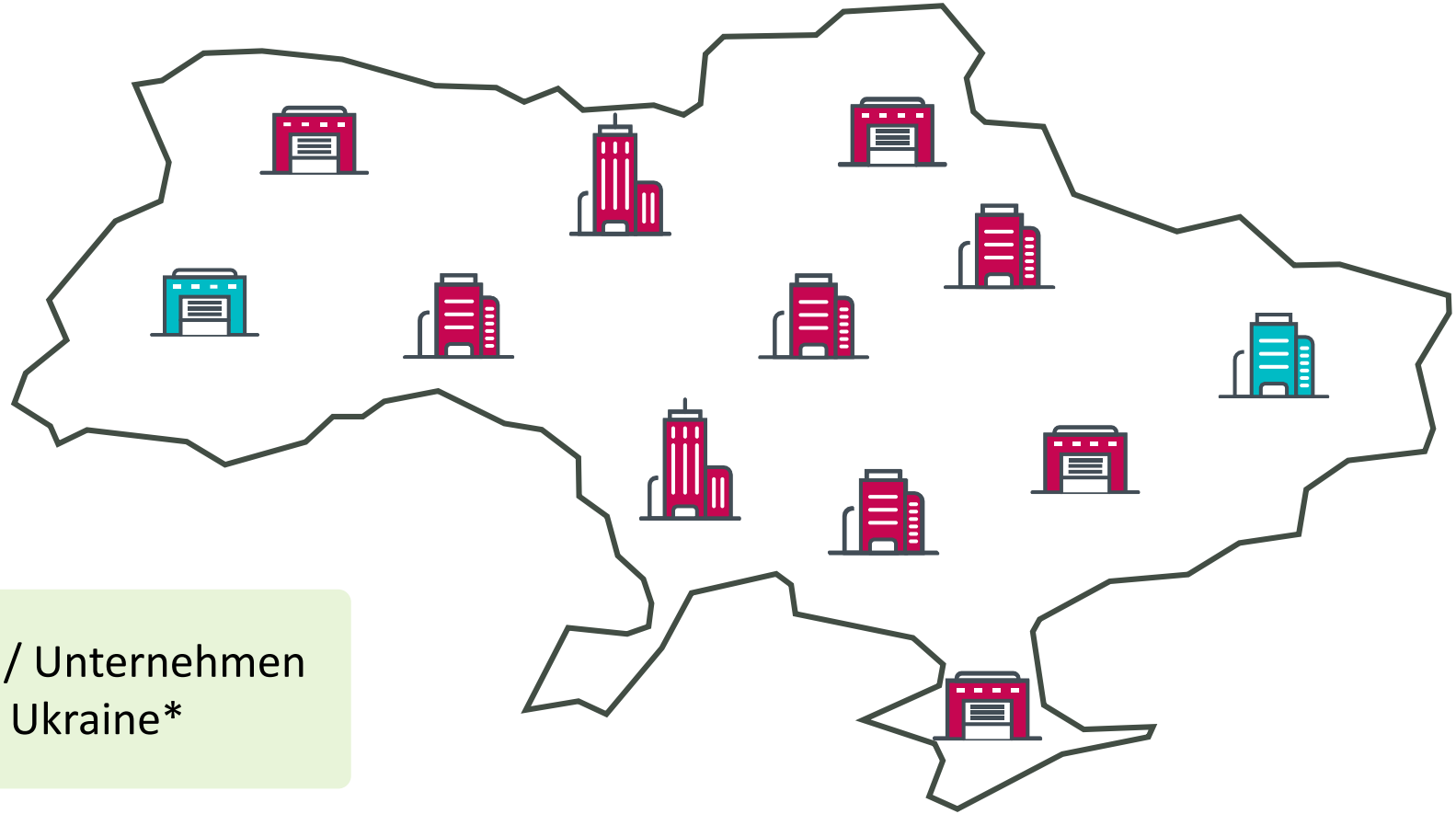
KOLLATERALSCHÄDEN?!?

NOTPETYA RANSOMWARE

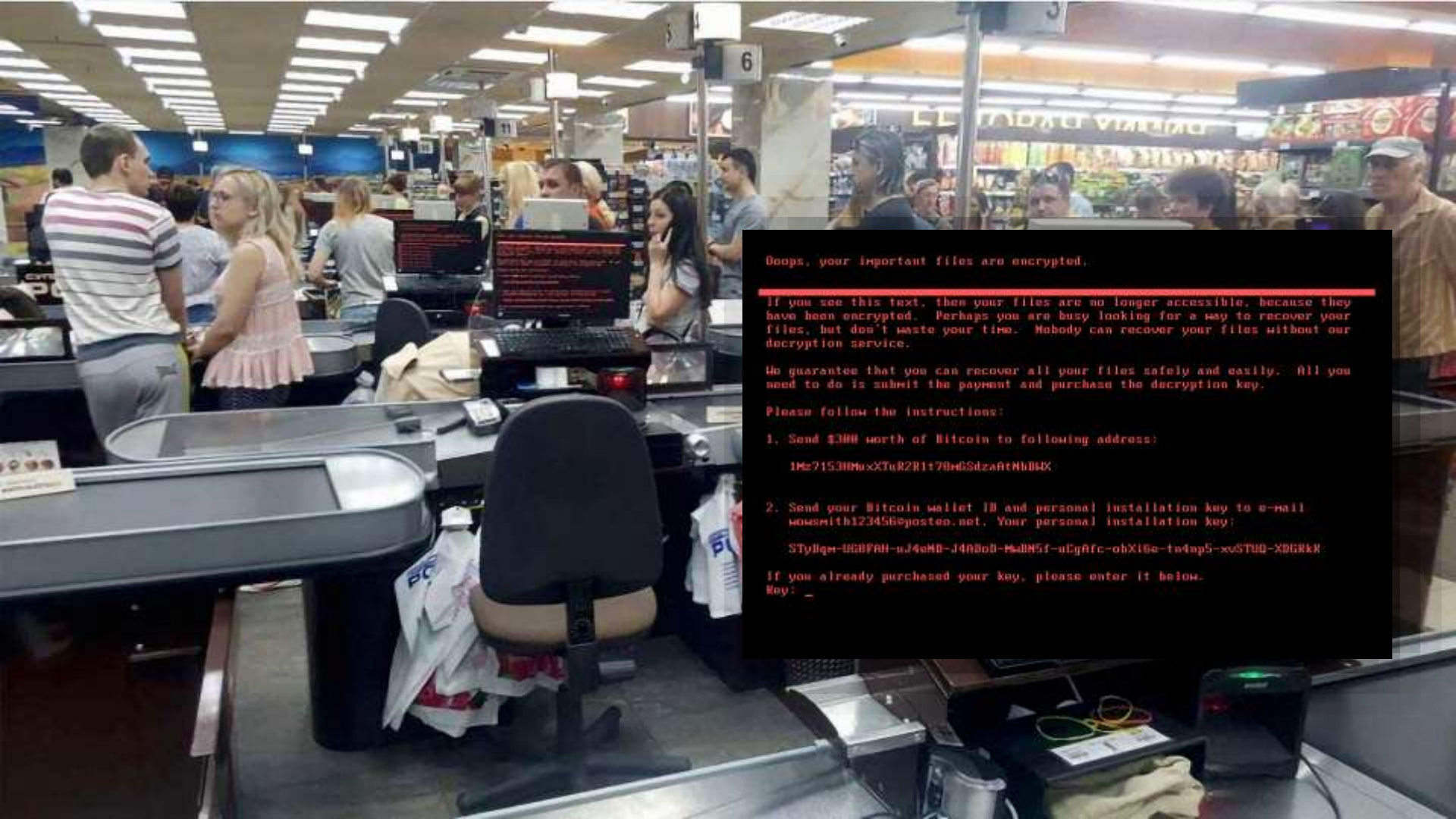
Digital Security
Progress. Protected.


Feb 2014
Russian occupation of Crimea
April 2014
War in Donbas begins
Dec 2015
BlackEnergy attack causes blackout in Ukraine
Dec 2016
Industroyer attack causes blackout in Ukraine
Jun 2017
NotPetya outbreak
24 Feb 2022
Russian invasion of Ukraine

NotPetya’s initial vector



~80% / Unternehmen in der Ukraine*


Ooops, your important files are encrypted.
If you see this text, then your files are no longer accessible, because they have been encrypted. Perhaps you are busy looking for a way to recover your files, but don't waste your time. Nobody can recover your files without our decryption service.
We guarantee that you can recover all your files safely and easily. All you need to do is submit the payment and purchase the decryption key.
Please follow the instructions:
1. Send $300 worth of Bitcoin to following address:
1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX
2. Send your Bitcoin wallet ID and personal installation key to e-mail wowsmith123456@posteo.net. Your personal installation key:
If you already purchased your key, please enter it below.
Key: _

SCHADEN DURCH NOTPETYA

10 Milliarden USD

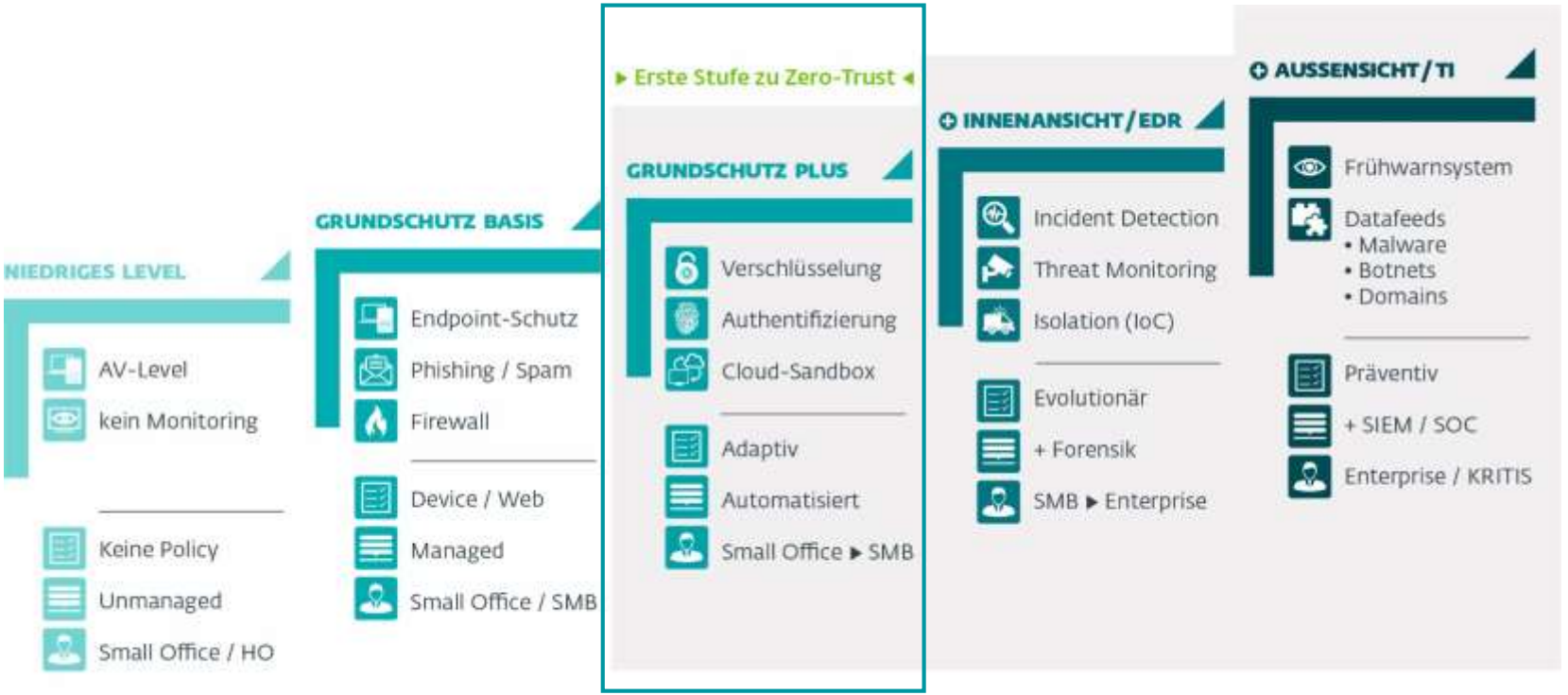
MERCK FedEx Corporation MAERSK durex

*„Weniger als **10 Prozent** vom IT-Budget wird für IT-Sicherheit investiert.“*

BMWi Deutschland

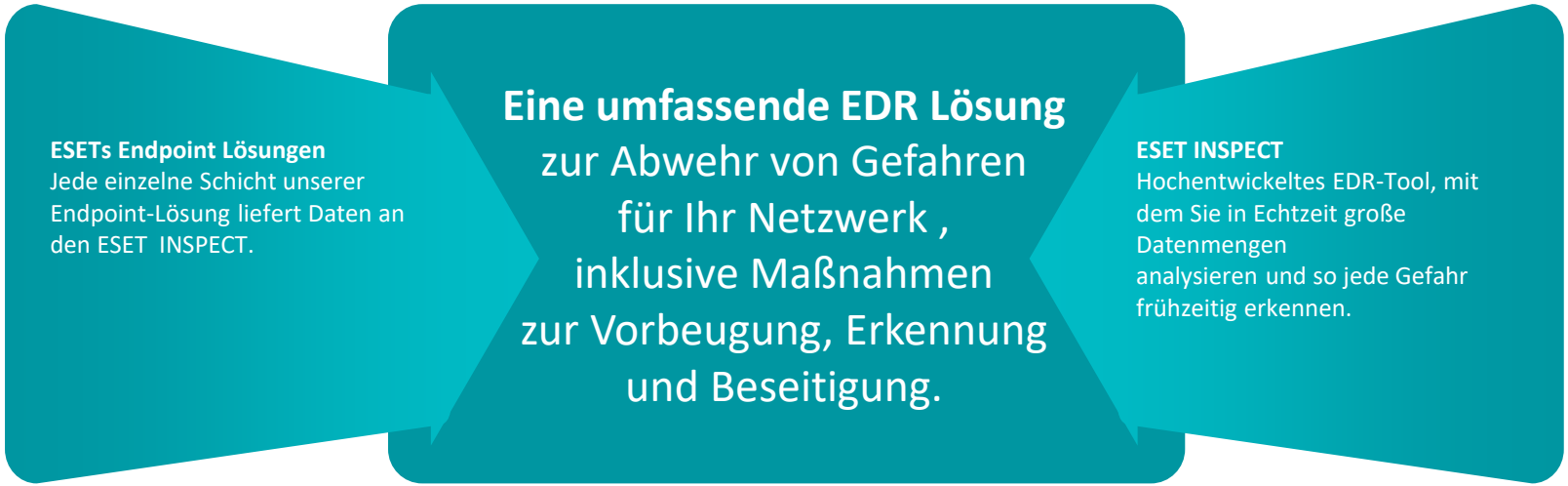
ZERO-TRUST-SECURITY

Digital Security
Progress. Protected.

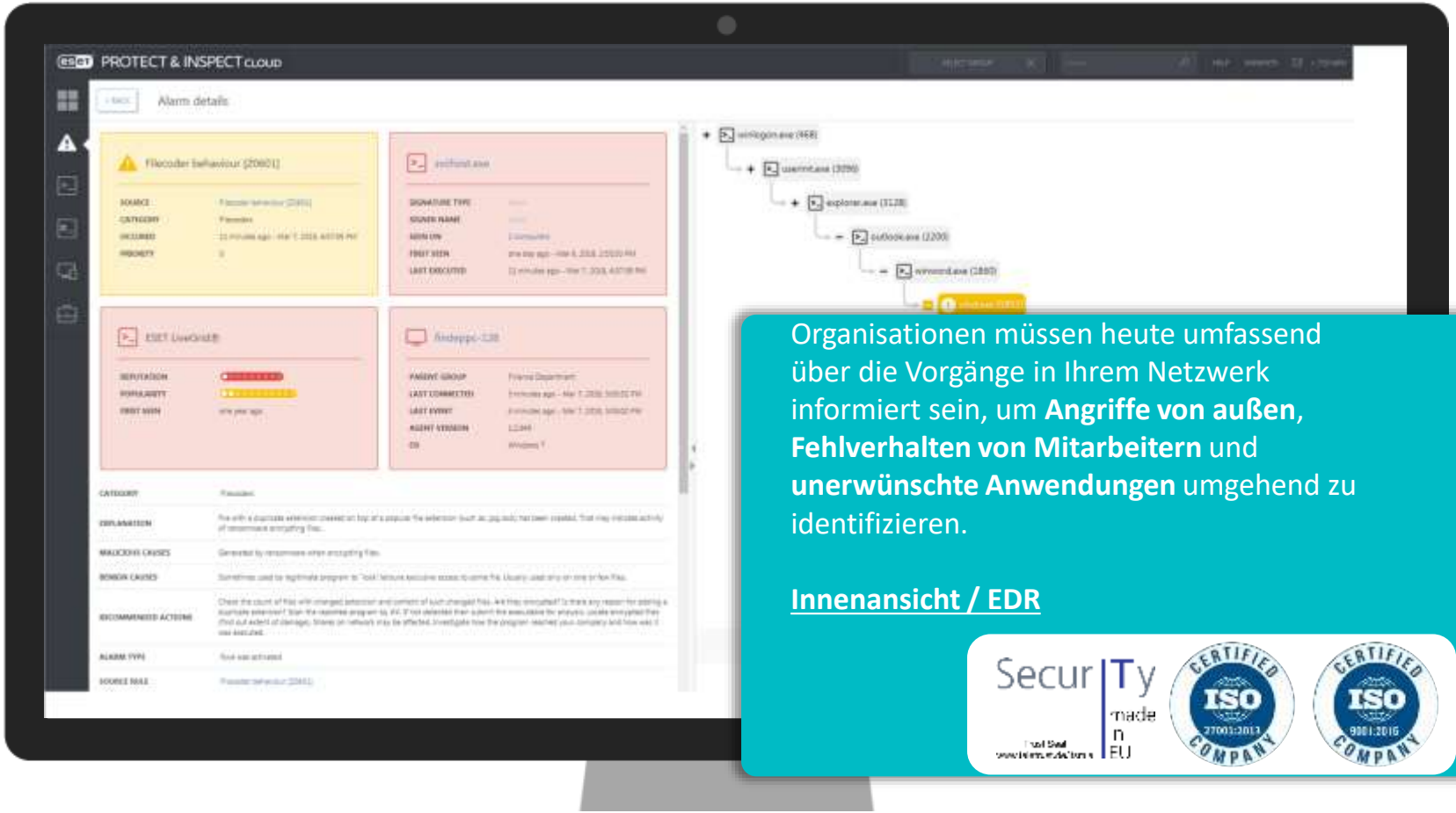


INNENANSICHT

Digital Security
Progress. Protected.



Innenansicht / EDR



Organisationen müssen heute umfassend über die Vorgänge in Ihrem Netzwerk informiert sein, um **Angriffe von außen**, **Fehlverhalten von Mitarbeitern** und **unerwünschte Anwendungen** umgehend zu identifizieren.

Innenansicht / EDR

Secur|Ty made in EU

CERTIFIED ISO 27001:2013 COMPANY

CERTIFIED ISO 9001:2015 COMPANY

AUSSENANSICHT

Digital Security
Progress. Protected.

Außensicht / TI

WAS HEIßT DAS IN LÖSUNGEN?

Digital Security
Progress. Protected.

ESET PORTFOLIO

Datafeeds + APT-Reports
ESET Threat Inteligence

Endpoint Detection & Response
On-Premises: ESET Inspect*
Cloud: ESET Inspect Cloud*

Managed Detection & Response
ESET Security Services

Cloud-Sandboxing
ESET LiveGuard Advanced

Microsoft 365 Bedrohungsschutz
ESET Cloud Office Security*

Verschlüsselung
ESET Endpoint Encryption*
ESET Full Disk Encryption

Multi-Faktor-Authentifizierung
ESET Secure Authentication*

Schutz von Clients & Mobilgeräten
ESET Endpoint Security
ESET Endpoint Antivirus

Schutz von Fileservern
ESET Server Security

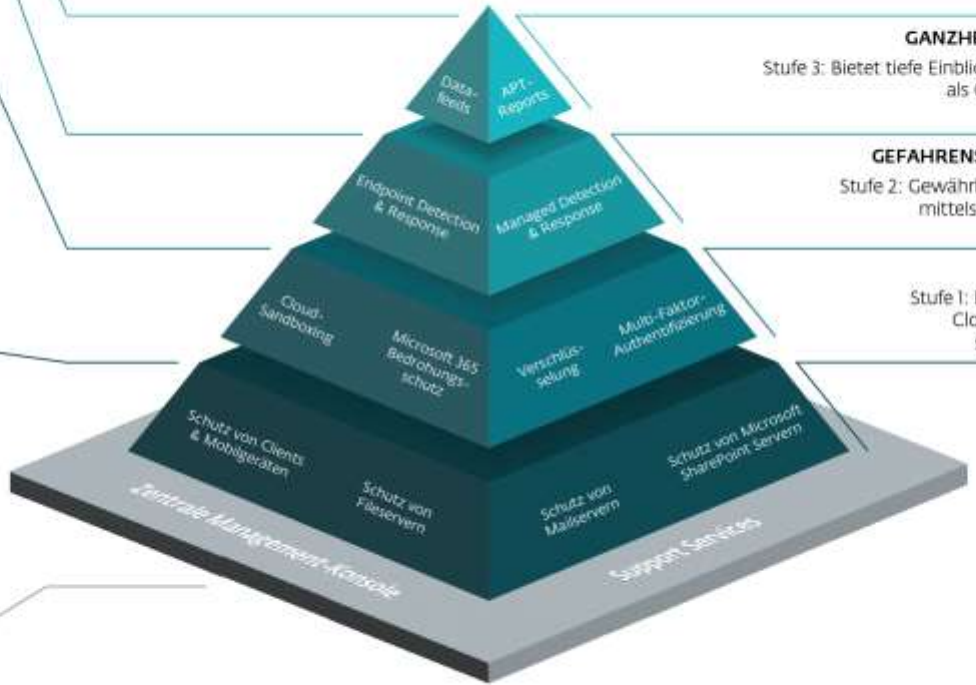
Schutz von Mailservern
ESET Mail Security

Schutz von Microsoft SharePoint Servern
ESET Security for Microsoft SharePoint Server

Zentrale Management-Konsole
On-Premises: ESET PROTECT
Cloud: ESET PROTECT Cloud

Support Services
Technischer Support PREMIUM
ESET Premium Support
ESET Upgrade & Deployment
ESET Healthcheck

*Verwaltung über separate Management-Konsole



GANZHEITLICHES LAGEBILD – AUSSENSICHT

Stufe 3: Bietet tiefe Einblicke in die globale Bedrohungslandschaft als Grundlage für einen SOC-/SIEM-Betrieb

GEFAHRENSUCHE UND ABWEHR – INNENSICHT

Stufe 2: Gewährleistet die Wirksamkeit der IT-Sicherheit mittels Anomalie-Erkennung, Schwachstellen-analyse und Incident Management

GRUNDSCHUTZ PLUS

Stufe 1: Empfohlene zusätzliche Absicherung für Cloud-Anwendungen, Daten und Zugänge sowie erweiterter Schutz vor Zero-Days

GRUNDSCHUTZ BASIS

Stufe 0: Mindestabsicherung für Endgeräte und Server

eset®

Digital Security
Progress. Protected.

ESET.DE | ESET.AT | ESET.CH

IT-Sicherheit ist Vertrauenssache

ESET 100% Made in EU IT-Security

25.-27. Oktober in Nürnberg

Besuchen Sie ESET am Stand 7-530

itsa EXPO CONGRESS

HOME OF IT SECURITY

ESET®

Digital Security
Progress. Protected.

Digital Security

Progress. Protected.