kaspersky

Industrial Cyber Security – Durch die Brille eines Angreifers

Stephan Gerling

9.12.2021

33,8%

Weltweite Angriffe gegen ICS Computer

Industrial Cyber Security

Durch die Brille eines Angreifers

Stephan Gerling

Senior Security Researcher ICS-Cert

Stephan.Gerling@Kaspersky.com
Twitter: @ObiWan666

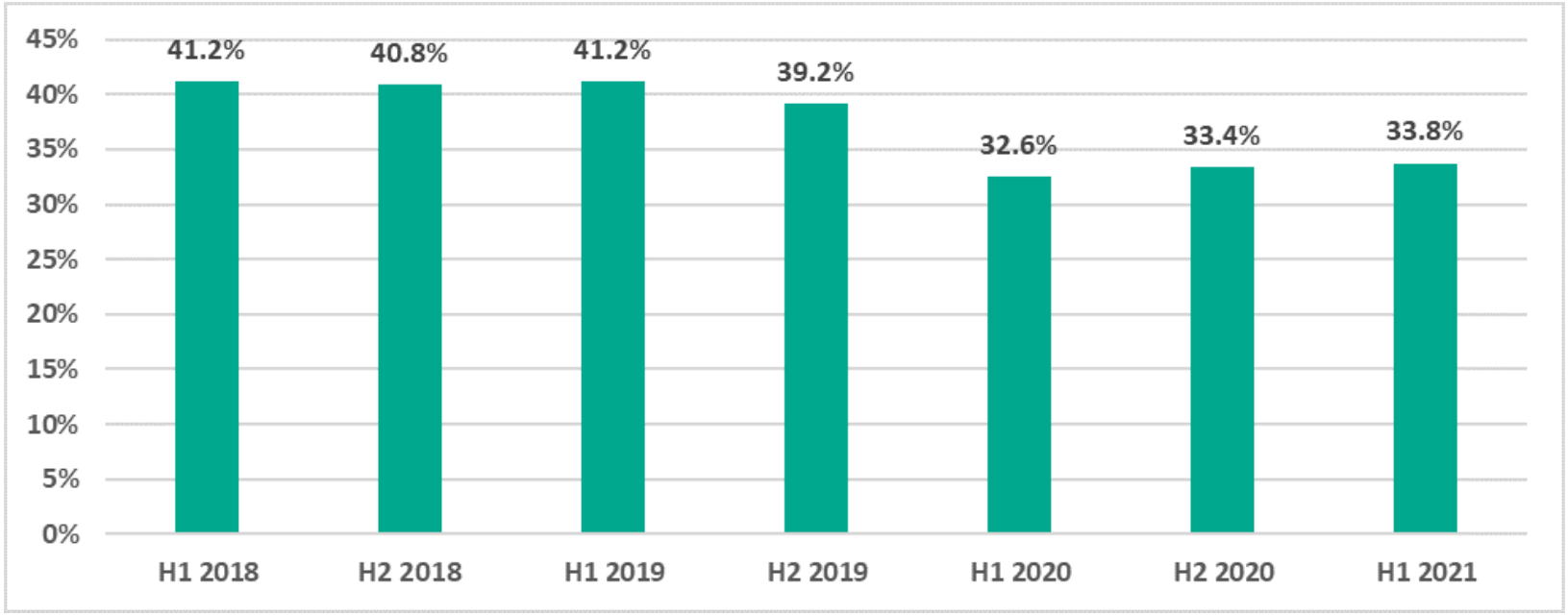
Übersicht bekannter Angriffe

7.12.2021	Stadtreinigung Leipzig
3.12.2021	Stadtwerke Pirna
20.10.2021	Stadt Witten
15.10.2021	Stadt Schwerin
1.10.2021	Stadtwerke Wismar
12.05.2020	Ludwigshafen TWL inkl 500GB Daten veröffentlicht

Weltweit Anstieg der Anriffe zu 2020

33.8% Angriffe gegen ICS Computer im ersten halbjahr 2021 (H1 2021)

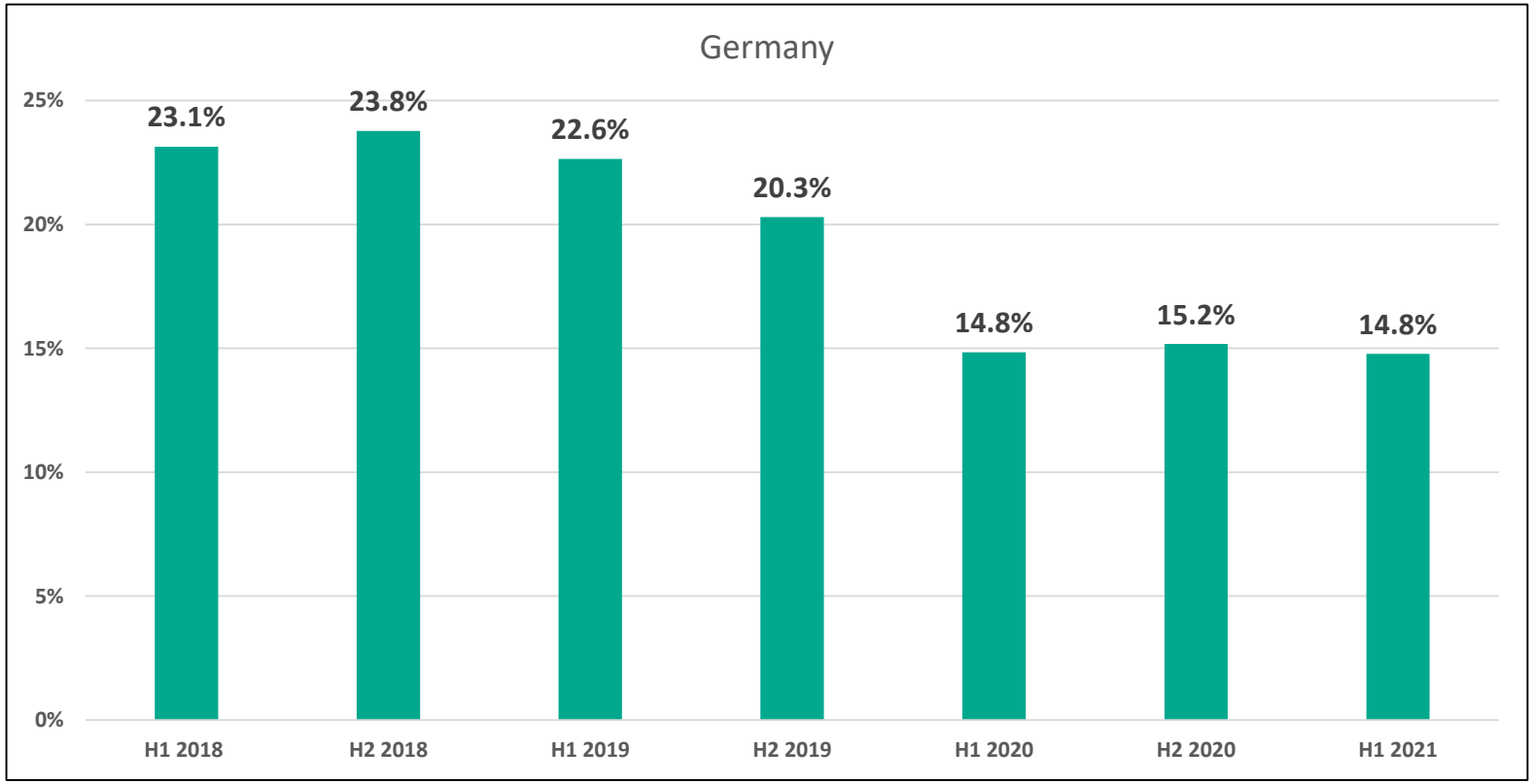
Eine Steigerung von 0,4% zu H2 2020.



Kaspersky | ICS Bedrohungslage 2021

ICS Bedrohung in Deutschland

Bedrohung in Deutschland eher gleichbleibend

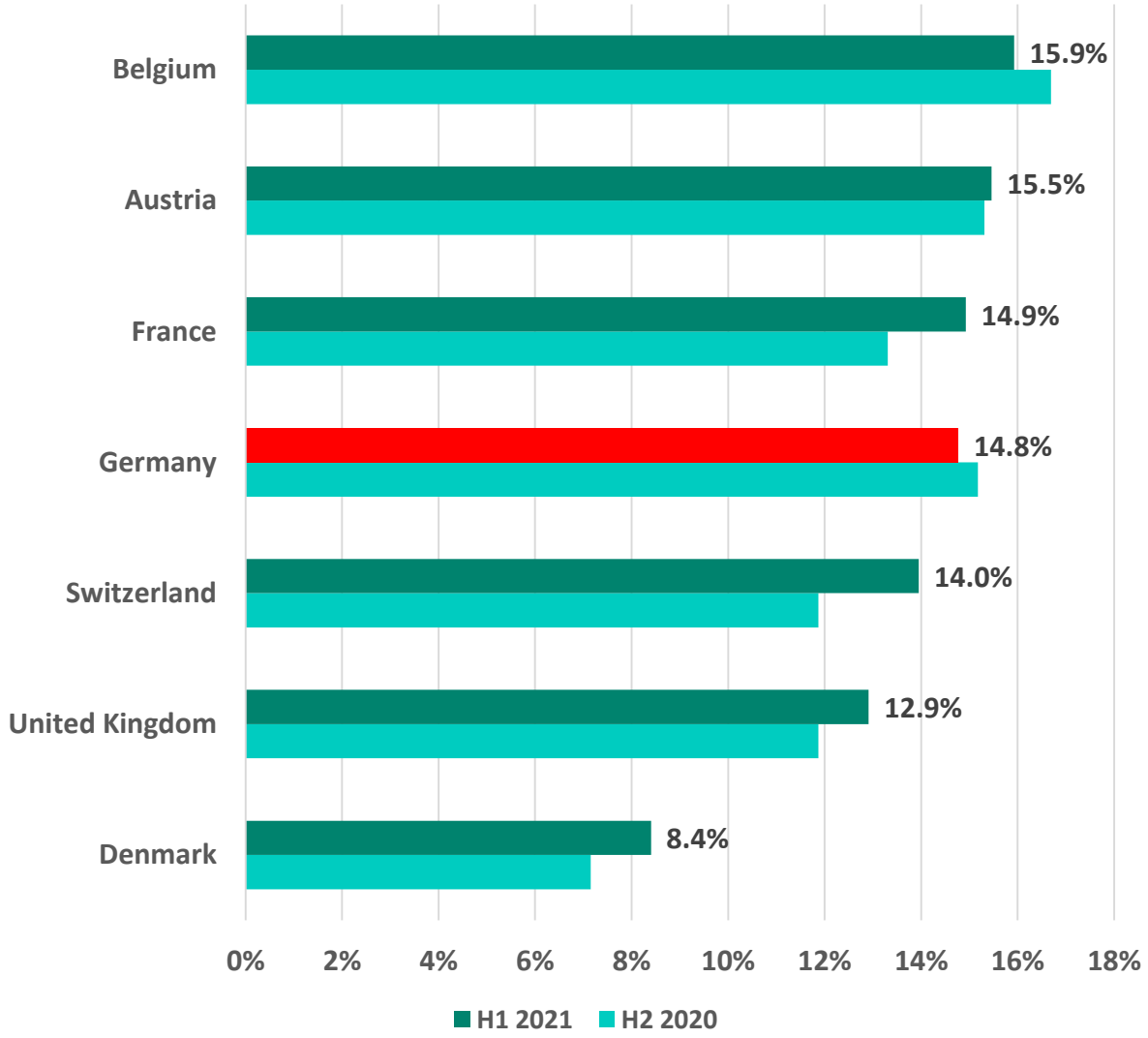


Europa im Vergleich

Nur in Deutschland ging der Trend Scheinbar zurück.

Trend für Europa ist eher Zunahme der Angriffe

Angreifer Verhalten hat sich geändert



Kaspersky | ICS Bedrohungslage 2021

Veränderung in der Bedrohung

hin zu:

RaaS – Ransomware as a Service

- Weg von Massen Infektion hin zu gezielten Angriffen
- High Profile Targeted Ransomware Attacks
- Proof of Compromise
- Doppelte Erpressung
- Verkauf der Zugangsdaten

Ransomware Anstieg

Ransomware Anstieg um 767% von 2019 – 2020

https://www.kaspersky.com/about/press-releases/2021_the-era-of-targeted-ransomware-attacks-on-high-profile-victims-grows-nearly-eightfold-from-2019-to-2020

Kaspersky | ICS Bedrohungslage 2021

Anstieg der Lösegelder

Von 500$ vor ein paar Jahren bis >70Mio$ aktuell

Verdoppelung von 2019 mit ~15Mio$ → 2020 mit >30Mio$

Nochmalige Verdoppelung in Schadenshöhe 2021 >70Mio$

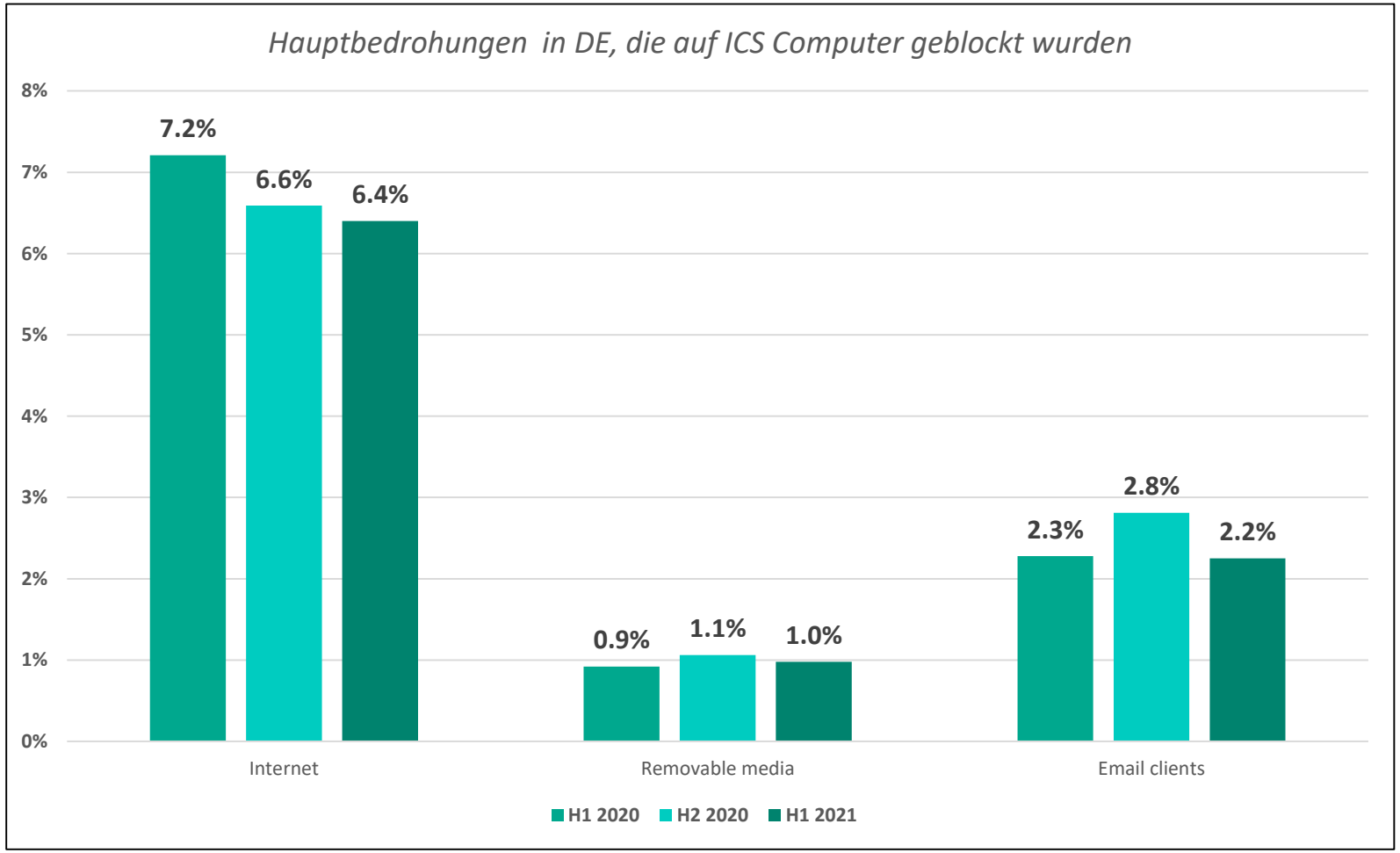
Angreifer spezialisieren sich zunehmend auf Ziele mit hohen Gewinnaussichten

Angriffsmethoden

Internet

E-Mail

Mobile Datenträger



Kaspersky | ICS Bedrohungslage 2021

Demo

OSINT vs. Industrial Security

Schwächen der ICS-Security

Wie kommt es zu solchen Fehlern :

- Vergessene Test oder Support Zugänge
- Probebetrieb der Live geht
- Der Punkt „Security“ soll später konfiguriert werden, es soll erst mal Funktionieren – gerät dann aber in Vergessenheit.

Schwächen der ICS-Security

Oft fehlt es an strukturiertem Vorgehen und folgenden Maßnahmen:

- Verzeichnen aller IT/OT-Komponenten in einem Netzplan
- Regelmäßige Durchführung und Anpassung von Notfallplänen
- Vollständige Verbreitung von Prozessen zum Change- und Patch-Management
- Kommunikation relevanter Dokumente an betroffene Mitarbeiter
- Netzwerksegmentierungen
- Awareness

Danke!

Fragen?

Stephan Gerling **Senior Security Researcher**

Stephan.Gerling@Kaspersky.com **Twitter: @ObiWan666**

kaspersky

Thank you!

kaspersky.com