HanseSecure
CHOOSE THE INTRUDER!


# Cyber Kill Chain

## wie 90% der Unternehmen gehackt werden!

→ CompTIA Community Treffen 03/2024

19.03.2024

# FLORIAN HANSEMANN

Über **10 Jahre** Erfahrung in Sicherheitsanalysen aller Branchen und Unternehmensgrößen
→ von kleiner Steuerkanzlei, über Mittelstand mit 50 Mitarbeitern bis hin zu **Banken**, **Raumfahrt**, **Militär** und **Atomkraftwerken**

Veröffentlichung von Schwachstellen
→ z.B. Sophos, Datev, **Intel**, **Microsoft**, Fujitsu

**National wie International** bekannt und mehrfach ausgezeichnet
→ Top 21 Security Experten Weltweit

Dauerhafte Beratungsmandate als **Trusted Advisor** bei internationalen Unternehmen mit Sitz in Deutschland

**Umfassendes Netzwerk** aus **Experten** jeglicher Fachrichtung im Bereich **Cybersecurity**

# BEKANNT AUS


# AUSWAHL VON TITELN

**Top 21 Security Twitter Accounts weltweit**
(https://www.sentinelone.com/blog/21-cybersecurity-twitter-accounts-you-should-follow/

**Keynote Speaker „Best of the World in Security“**
(https://hansesecure.de/2021/05/best-of-the-world-in-security-keynote-speaker/)

**Top 100 einflussreichsten Cybersecurity Brands weltweit**
(https://onalytica.com/blog/posts/whos-who-in-cybersecurity-2/)

**Top 21 Quellen für Security Teams weltweit**
(https://techbeacon.com/security/modern-red-teaming-21-resources-your-security-team)

# ÜBER HanseSecure

HanseSecure versteht sich als effektiver IT Security-Partner und bietet dir eine individuelle Angebots- und Zielanpassung an.
Durch die Vereinigung von Kompetenzen eröffnen wir ein ganzheitliches Leistungsspektrum. Dieses reicht von Penetrationstests bis hin zu Strategieberatung.
Wir beraten dich gewissenhaft, welche Leistungen und in welchem Umfang diese für dein Unternehmen sinnvoll und effektiv sind.

**Follower auf Twitter**
**75.000+**

**Unterstützte Unternehmen**
**350+**

**Kundenzufriedenheit**
**99%**

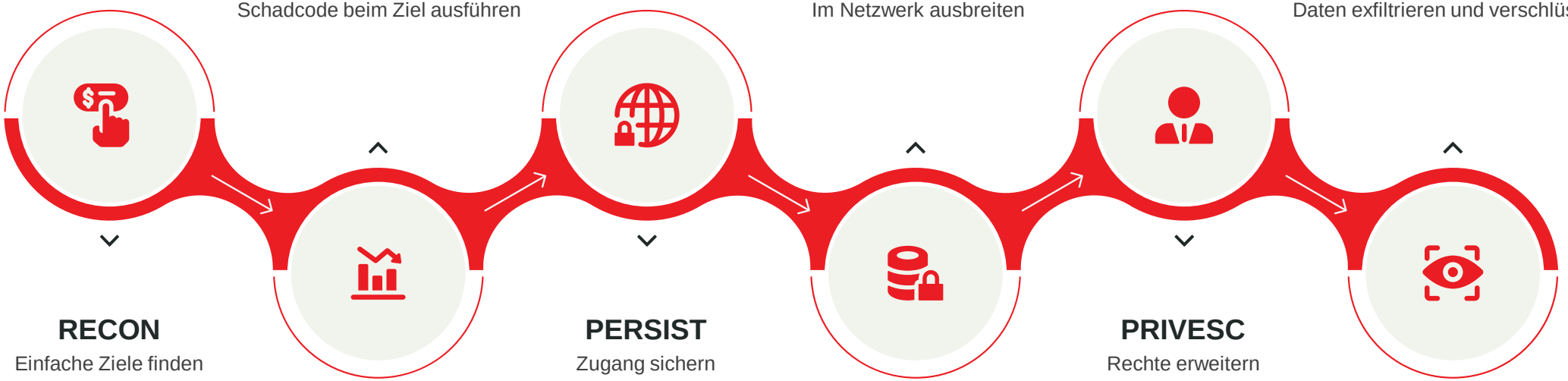
# Schon wieder Cyber

HanseSecure
CHOOSE THE INTRUDER!

# Agenda

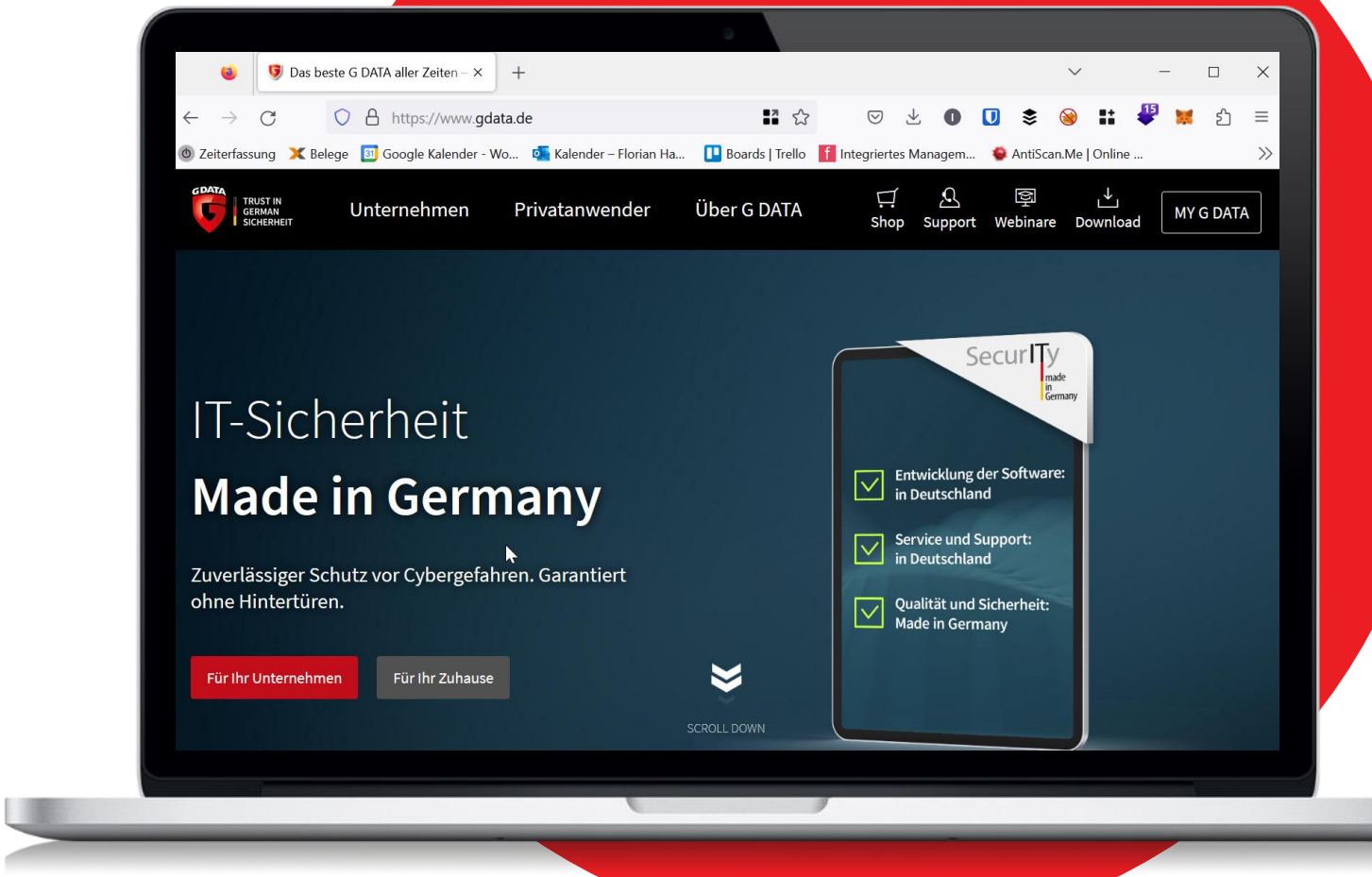
- KILLCHAIN DEFINITION
- RECON
- ATTACK
- PERSIST
- LATERAL MOVEMENT
- PRIVESC
- EXFILTRIATION
- DEFENSE SUMUP

# CyberKillChain

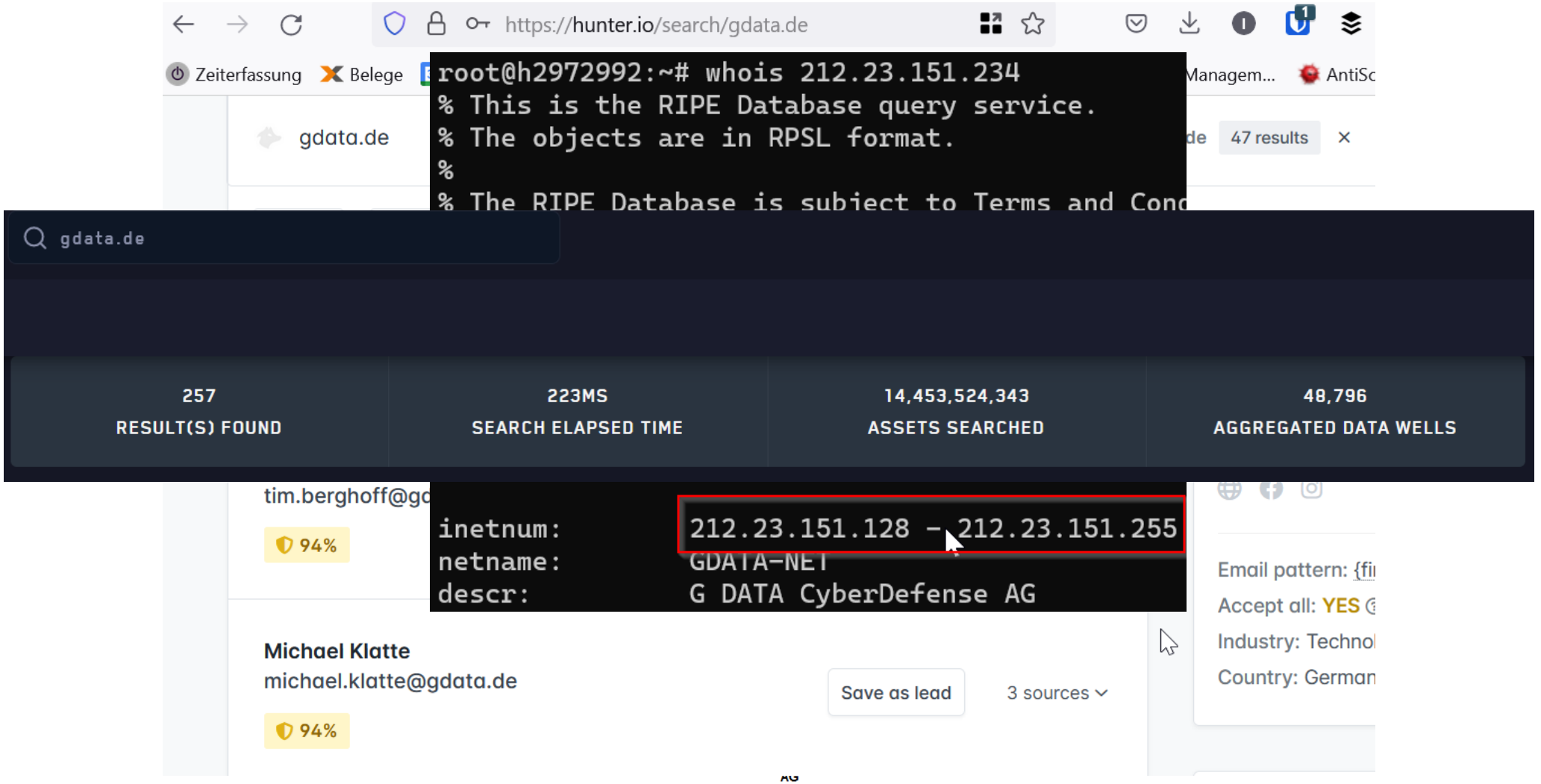


# RECON

- Alle erreichbaren Systeme
- Relevante Mitarbeiter
- Verwendete Software
- Lierferanten/ Parnter/ Kunden



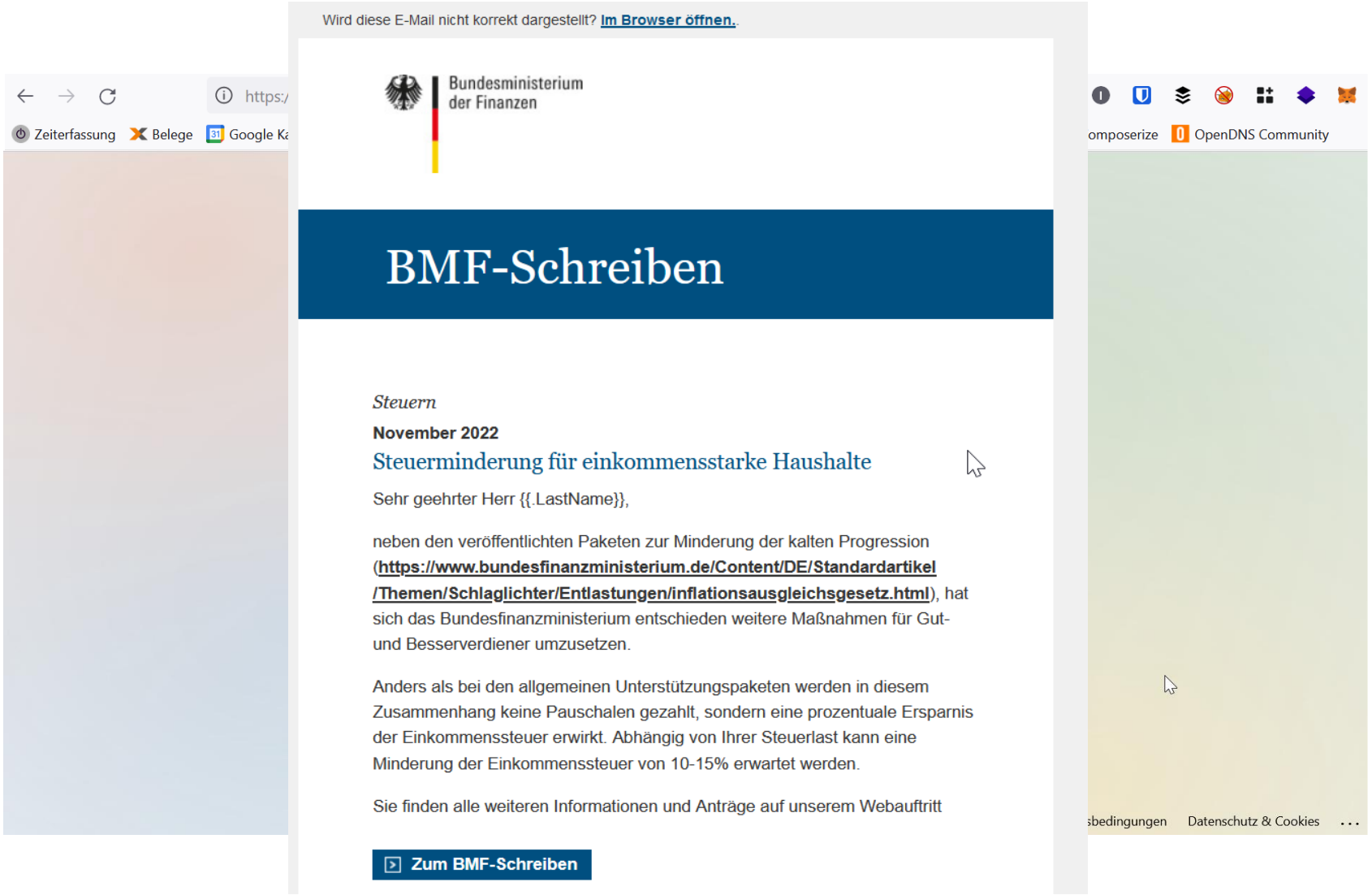
# RECON


https://hunter.io/search/gdata.de
Zeiterfassung
Belege
root@h2972992:~# whois 212.23.151.234
% This is the RIPE Database query service.
% The objects are in RPSL format.
%
% The RIPE Database is subject to Terms and Cond
gdata.de
47 results
gdata.de
257
RESULT(S) FOUND
223MS
SEARCH ELAPSED TIME
14,453,524,343
ASSETS SEARCHED
48,796
AGGREGATED DATA WELLS
tim.berghoff@gd
94%
inetnum: 212.23.151.128 - 212.23.151.255
netname: GDATA-NET
descr: G DATA CyberDefense AG
Michael Klatte
michael.klatte@gdata.de
94%
Save as lead
3 sources
Email pattern: {fi
Accept all: YES
Industry: Technol
Country: German

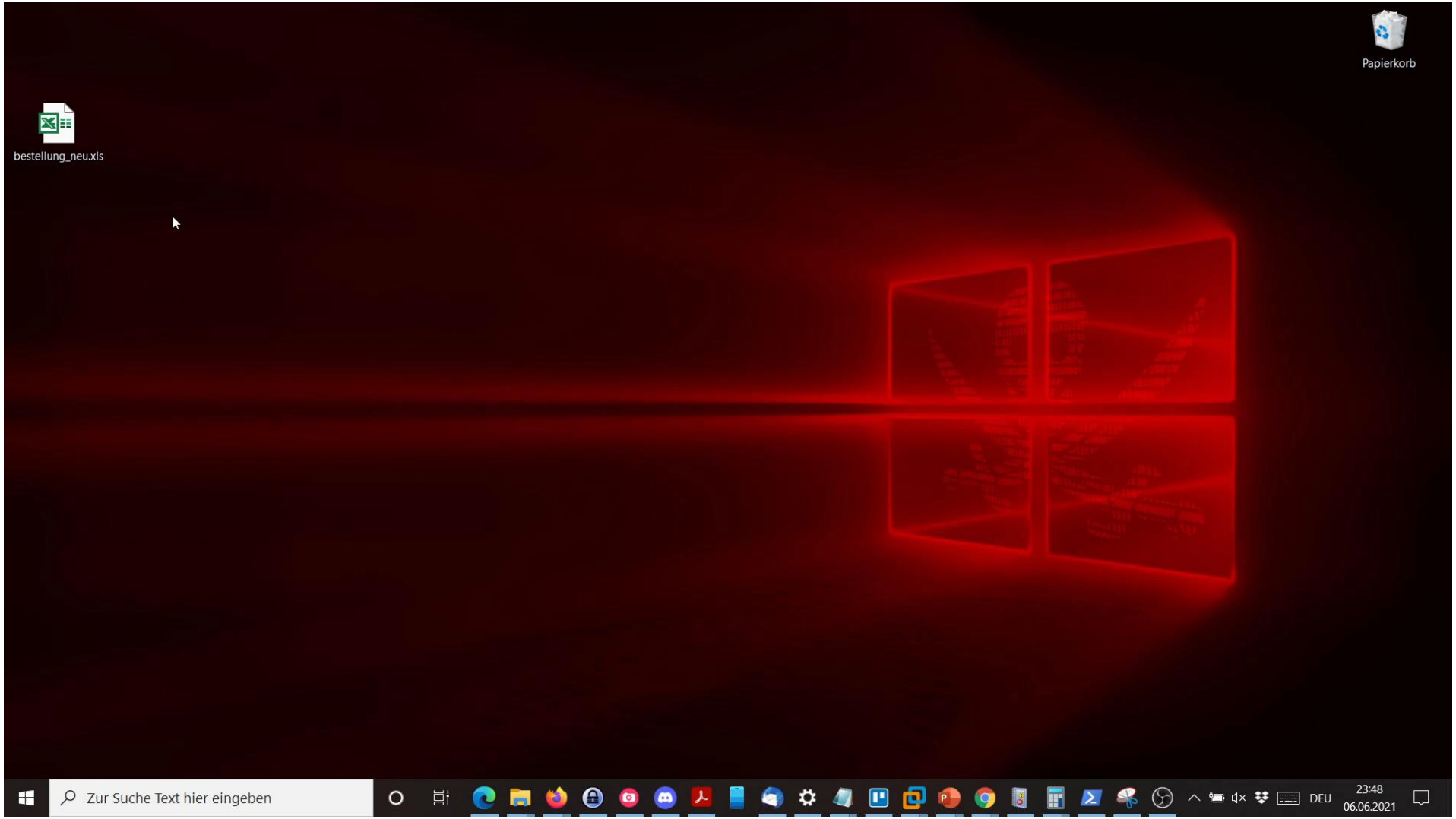
# ATTACK

- Keine easy-hackable Systems
- Einige Systeme extern gehostet
- ggf. CISCO-VPN Logins ☺ = Phishing!

# ATTACK


Wird diese E-Mail nicht korrekt dargestellt? Im Browser öffnen.
Zeiterfassung
Belege
Google Ka
omposerize
OpenDNS Community
Bundesministerium der Finanzen
BMF-Schreiben
Steuern
November 2022
Steuerminderung für einkommensstarke Haushalte
Sehr geehrter Herr {{.LastName}},
neben den veröffentlichten Paketen zur Minderung der kalten Progression (https://www.bundesfinanzministerium.de/Content/DE/Standardartikel/Themen/Schlaglichter/Entlastungen/inflationsausgleichsgesetz.html), hat sich das Bundesfinanzministerium entschieden weitere Maßnahmen für Gut- und Besserverdiener umzusetzen.
Anders als bei den allgemeinen Unterstützungspaketen werden in diesem Zusammenhang keine Pauschalen gezahlt, sondern eine prozentuale Ersparnis der Einkommenssteuer erwirkt. Abhängig von Ihrer Steuerlast kann eine Minderung der Einkommenssteuer von 10-15% erwartet werden.
Sie finden alle weiteren Informationen und Anträge auf unserem Webauftritt
Zum BMF-Schreiben
sbedingungen
Datenschutz & Cookies

# ATTACK


Papierkorb
bestellung_neu.xls
Zur Suche Text hier eingeben
DEU
23:48
06.06.2021

# PERSIST

- Powershellprofile
- Aufgabenplanung
- Autostart
- Registry Key
- Wordvorlage
- Anwendungstausch

# PERSIST

# LATERAL MOVEMENT

- PS-Remoting
- MSSQL
- SSH/TELNET
- SMB
- Shares
- RDP
- Citrix und Co

# PRIVESC

- Veraltete Software
- 3rd Party
- Fehlkonfigurationen
- Shares

# EXFIL/ Ransom

# DEFENSE SUMUP

## RECON

- IPS
- GEO-Blocking
- ICMP/ Portscan Blocken
- Risikobewusstsein

## ATTACK

- Härtung
- EDR
- MFA
- Awareness

## LATERAL MOVEMENT

- Netzsegmentierung
- Lokale Ports sperren
- Uniq Zugangsdaten

## PRIVESC

- Client+
- Lateral Movement+
- Domain Hygiene
- Passwort Management

## EXFIL/ RANSOM

- DPL
- Backup

## OVERALL

- Patch- und Assestmanagement
- SIEM/ SOC

"Successful people do what unsuccessful people are not willing to do.

Don't wish it were easier, wish you were better“

Jim Rohn

HanseSecure
CHOOSE THE INTRUDER!

# GET IN TOUCH


- MÜNCHEN
- https://hansesecure.de/termin
- info@hansesecure.de
- https://hansesecure.de/



HanseSecure
CHOOSE THE INTRUDER!