ATHENE
National Research Center for Applied Cybersecurity

Die Cybersicherheitslage und wie wir sie verbessern können

Prof. Dr. Haya Shulman

ATHENE | Goethe-Universität Frankfurt a.M. | Fraunhofer SIT

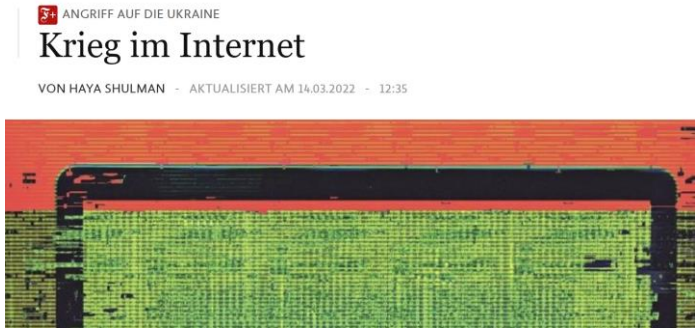
Cybersecurity-Day am 26.01.2023, München, Bayern

Überblick

1. Lage der Cybersicherheit
2. Wie werden Organisationen infiltriert:
   → Passwörter
   → Schwachstellen
3. Unsere Forschung zur nachhaltigen Verbesserung der Cybersicherheit

COVID-19 und dann Krieg

- **Ungeordnete Digitalisierung vergrößert Angriffsfläche**
- **Geopolitische und wirtschaftliche Lage erhöht Gefahr**



Haya Shulman:
Krieg im Internet;
Frankfurter Allgemeine Zeitung, 14. März 2022

Bundesamt für Sicherheit in der Informationstechnik

„Die Bedrohungslage im Cyber-Raum ist angespannt, dynamisch und vielfältig und damit so hoch wie nie."

bitkom research

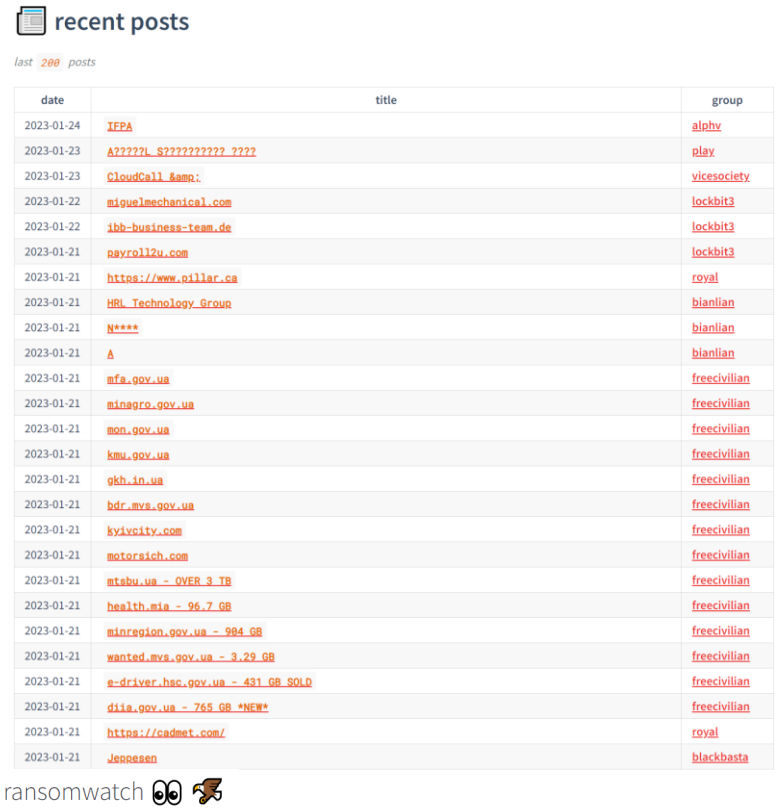
„203 Milliarden Euro Schaden pro Jahr durch Angriffe auf deutsche Unternehmen"

- **Kriminelle und fremdstaatlich gesteuerte Angreifer**

Cyberangriffe nehmen zu

Auswahl von *ransomwatch:*

- 138 Opfer von Ransomware-Angriffen seit 1. Januar 2023
- Durchgeführt von 20 Hackergruppen
- Allein am 21 Januar 24 Cyberangriffe



recent posts

last 200 posts

date	title	group
2023-01-24	IFPA	alphv
2023-01-23	A?????L S?????????? ????	play
2023-01-23	CloudCall &	vicesociety
2023-01-22	miguelmechanical.com	lockbit3
2023-01-22	ibb-business-team.de	lockbit3
2023-01-21	payroll2u.com	lockbit3
2023-01-21	https://www.pillar.ca	royal
2023-01-21	HRL Technology Group	bianlian
2023-01-21	N****	bianlian
2023-01-21	A	bianlian
2023-01-21	mfa.gov.ua	freecivilian
2023-01-21	minagro.gov.ua	freecivilian
2023-01-21	mon.gov.ua	freecivilian
2023-01-21	kmu.gov.ua	freecivilian
2023-01-21	gkh.in.ua	freecivilian
2023-01-21	bdr.mvs.gov.ua	freecivilian
2023-01-21	kyivcity.com	freecivilian
2023-01-21	motorsich.com	freecivilian
2023-01-21	mtsbu.ua - OVER 3 TB	freecivilian
2023-01-21	health.mia - 96.7 GB	freecivilian
2023-01-21	minregion.gov.ua - 904 GB	freecivilian
2023-01-21	wanted.mvs.gov.ua - 3.29 GB	freecivilian
2023-01-21	e-driver.hsc.gov.ua - 431 GB SOLD	freecivilian
2023-01-21	diia.gov.ua - 765 GB *NEW*	freecivilian
2023-01-21	https://cadmet.com/	royal
2023-01-21	Jeppesen	blackbasta

ransomwatch

0mega
alphv
bianlian
blackbasta
blackbyte
clop
daixin
everest
freecivilian
hiveleak
karakurt
lockbit3
lorenz
mallox
nokoyawa
play
ransomhouse
royal
snatch
vicesociety

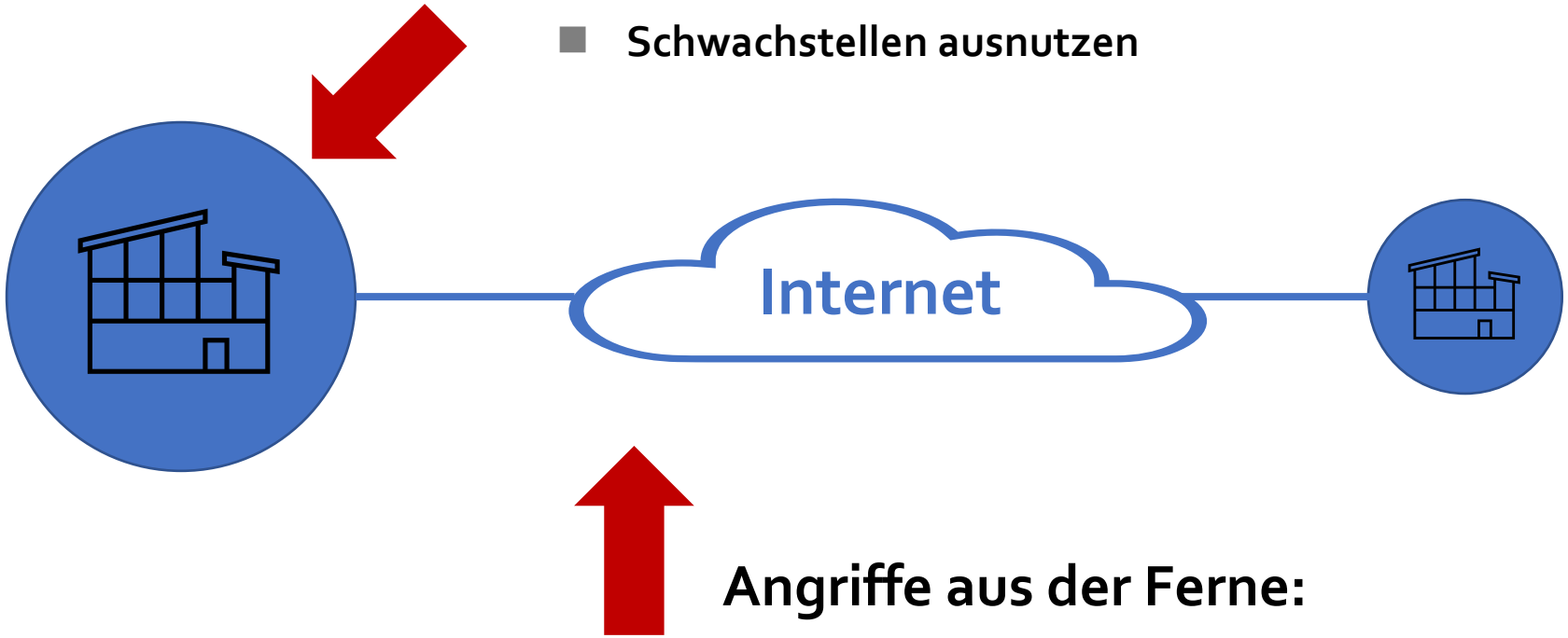
Überblick

1. Lage der Cybersicherheit
2. Wie werden Organisationen infiltriert:
   → Passwörter
   → Schwachstellen
3. Unsere Forschung zur nachhaltigen Verbesserung der Cybersicherheit

Was sind die wesentlichen Angriffsvektoren?

Infiltrieren der Zielorganisation:

- Erbeuten von Passwörter
- Schwachstellen ausnutzen



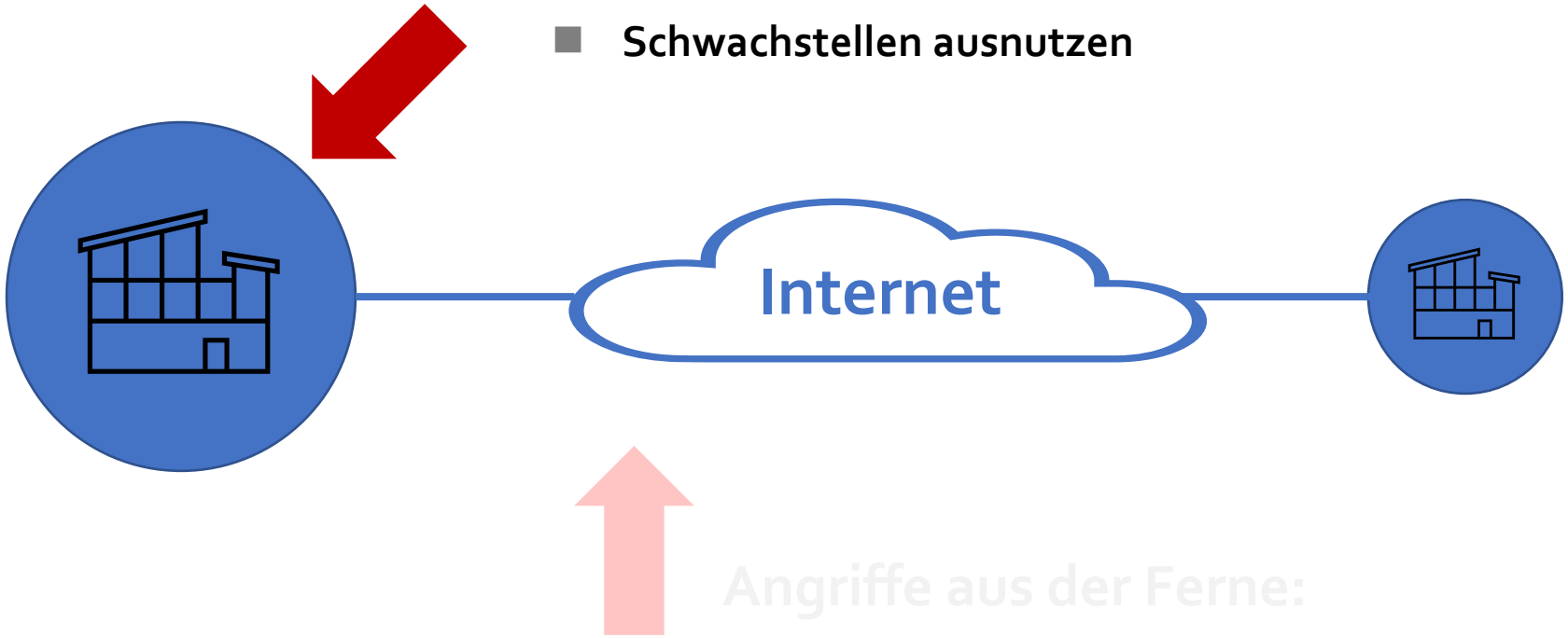
Angriffe aus der Ferne:

- **DDoS** (Distributed Denial of Service)
- **Verkehrsumlenkungen (Hijacks)** im Internet

Was sind die wesentlichen Angriffsvektoren?

Infiltrieren der Zielorganisation:

- Erbeuten von Passwörter
- Schwachstellen ausnutzen



Angriffe aus der Ferne:

- **DDoS** (Distributed Denial of Service)
- **Verkehrsumlenkungen (Hijacks)** im Internet

Wie kommen Hacker an Passwörter

Eindringen und Ausbreiten innerhalb der Opferorganisation

- Infostealers
- Data Dumps
- Durchprobieren schwacher Passwörter
- Durchsuchen von Cloud / Repositories / Code nach abgelegten Passwörtern

okta

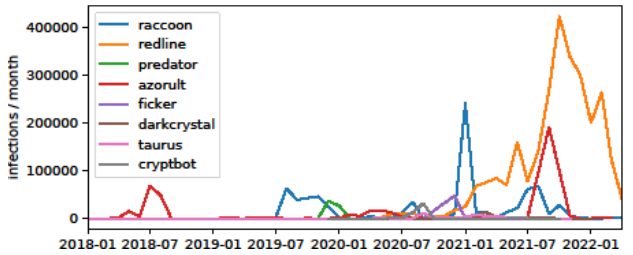
Wie kommen Hacker an Passwörter
Infostealers

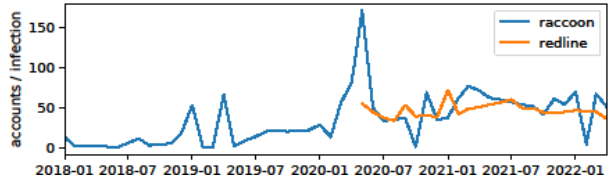
- Infostealers

- **Verteilung von Infostealers durch infizierten Programme**

  Anydesk, Dropbox, Telegram, OpenOffice, Adobe acrobat pro, Wondershare, 3DMark, 3DVista Virtual , Tour Pro, MAGIX Sound , Afterburner, Github, Repositories (npm, PyPI,…)

Family	# Advertisements	Buying Channels	# Features	Selected features
Redline	210	Telegram,Telegram Bot	24	FTP,Openlink,RDP,browser,credit cards,crypto,discord
Raccoon	51	Darknet,Telegram	9	FTP,browser,credit cards,crypto,geo,os,screenshot
Vidar	24	Darknet	11	FTP,browser,crypto,discord,email clients,file grabber,os,screenshot
Oski	22	Github	9	FTP,browser,crypto,downloader,executer,file grabber,os,screenshot
Hunter Stealer	22	Darknet	10	browser,discord,file grabber,geolocation,os,screenshot,steam,telegram
DarkCrystal	1	Darknet	9	browser,downloader,executer,keylogger,microphone,open shell,os





Google Ad Exploited to Deliver Infostealing Malware

GIMP.org Lookalike Site Tricks Users into Downloading Malicious Executable.

Google PPC Ads Used to Deliver Infostealers

Wie kommen Hacker an Passwörter

Passwörter in Data Dumps

- Infostealers
- Data Dumps
- Durchprobieren schwacher Passwörter
- Durchsuchen von Cloud / Repositories / Code nach abgelegten Passwörtern

Wie kommen Hacker an Passwörter
Durchprobieren schwacher Passwörter

- Infostealers
- Data Dumps
- **Durchprobieren schwacher Passwörter**
- Durchsuchen von Cloud / Repositories / Code nach abgelegten Passwörtern

Wie kommen Hacker an Passwörter

Passwörter in Cloud / Repositories / Code

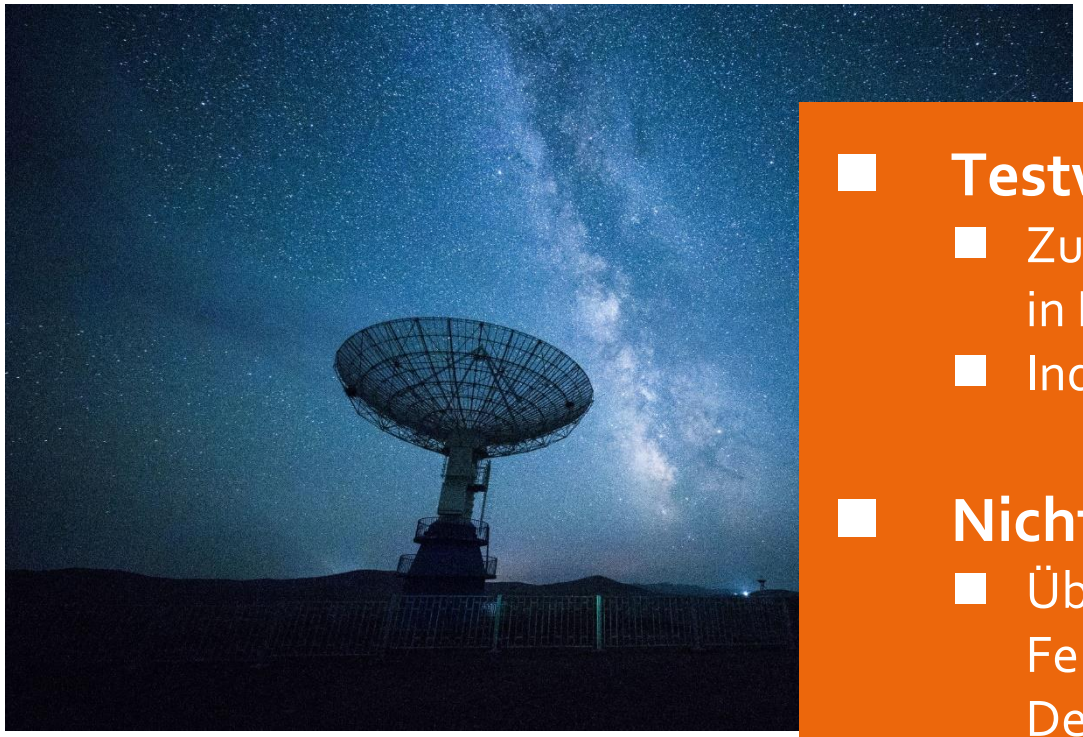
- Infostealers
- Data Dumps
- Durchprobieren schwacher Passwörter
- Durchsuchen von Cloud / Repositories / Code nach abgelegten Passwörtern

Überblick

1. Lage der Cybersicherheit
2. Wie werden Organisationen infiltriert:
   → Passwörter
   → Schwachstellen
3. Unsere Forschung zur nachhaltigen Verbesserung der Cybersicherheit

Studie zu Schwachstellen als Einfallstor

Überblick gewinnen und behalten



- **Testwerkzeuge**
  - Zu gefundenen Schwachstellen in Netzen, Hardware, Software
  - Individuell und für Internet-weite Studien
- **Nicht-intrusive large-scale Studien**
  - Über 1000 verschiedenen Schwachstellen und Fehlkonfigurationen in 50 DAX Unternehmen in Deutschland
  - Verwundbarkeit spezifischer Sektoren, z.B. politische Parteien (2020), Landesverwaltungen und Forschungseinrichtungen (2022)

Studie der Sicherheit von politischen Parteien (2020)

Vorfeld Bundestagswahl, seither für diverse Organisationen wiederholt

- **Positive, konstruktive Reaktion aller Parteien**
- **Probleme ähneln sich über alle Parteien … und letztlich fast alle Organisationen hinweg**
  - Unvollständige Sicht
  - Bekannte Schwachstellen
  - Nicht umgesetzte Sicherheitsstandards
  - Geleakte Passwörter
  - Schwachstellen in Dienstleistern
  - Wenig Schutz gegen fortgeschrittene Angriffe

Überblick

1. Lage der Cybersicherheit
2. Wie werden Organisationen infiltriert:
   - → Passwörter
   - → Schwachstellen
3. Unsere Forschung zur nachhaltigen Verbesserung der Cybersicherheit

Wie kann man dennoch Cybersicherheit verbessern?

Strategie zu einer resilienteren Cybersicherheit

- **Eigene Konten gegen Darknet Leaks testen**
- **Keine Passwörter mehrfach oder mit einfachen Variationen für verschiedene Dienste verwenden**
- **Sichere Multifaktor-Authentifizierung (MFA), möglichst ohne Passwörter, mit Tokens**

  Nicht alle MFA sind sicher
- **Überblick über Schwachstellen gewinnen**

  Wissen um die Verwundbarkeiten von IT, insbesondere der eigenen
- **Vorsorge treffen**

  Organisation, Awareness, Übung, Business Continuity
- **Dienstleister für Infrastruktur**


Digitec

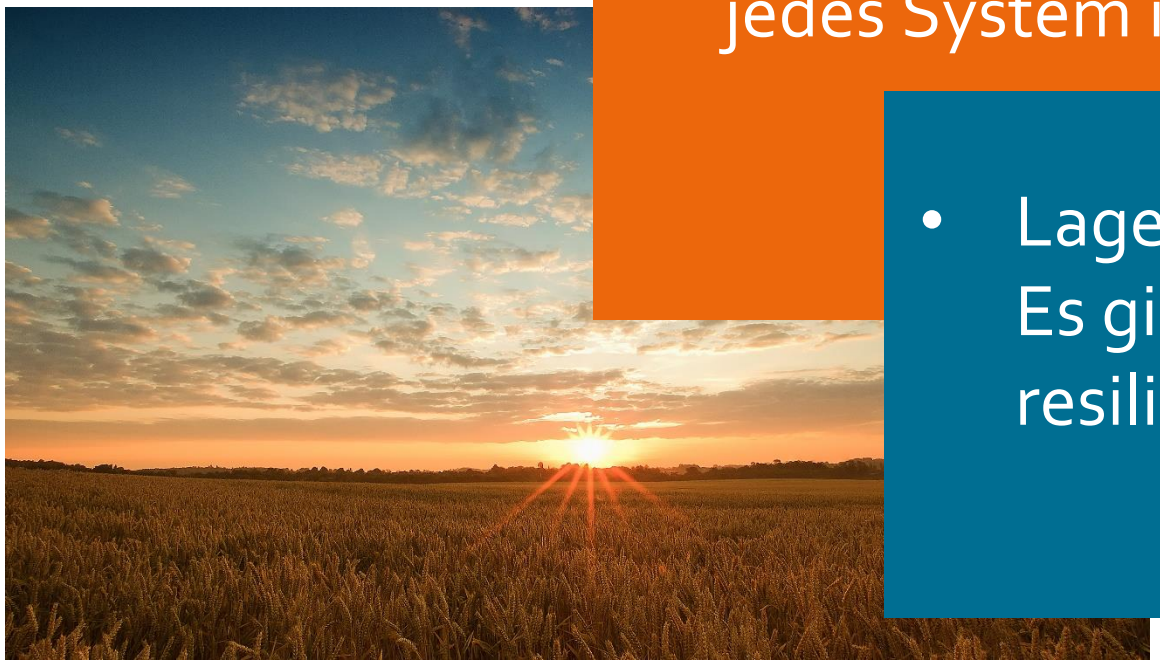
Was vor Cyberangreifern wirklich schützt

Wie sicher unsere Passwörter sind. Und warum auch ein derzeit angesagter Ansatz anfälliger ist als gedacht.

Von Haya Shulman und Michael Waidner

Haya Shulman, Michael Waidner:
Was vor Cyberangreifern wirklich schützt;
Frankfurter Allgemeine Zeitung, 28. November 2022

Fazit



- Die Lage ist ernst,
  jedes System ist verwundbar.

- Lage ist aber nicht hoffnungslos.
  Es gibt Strategien zu einer resilienteren Cybersicherheit.

תודה רבה!

Merci beaucoup!

çok teşekkürler

谢谢

Thank you very much!

Vielen Dank!

Dank je wel!

Muchas gracias

ありがとうございます

Dziękuję!

zor spas

شكرا لك

Grazie mille!