



DIGITIZE YOUR BUSINESS

www.RiT.de



DIGITIZE YOUR BUSINESS

Geiselnahme digital: Wie Sie sich und Ihr Unternehmen gezielt vor Verschlüsselungstrojanern schützen

Vortrag im Rahmen der Roadshow Cybercrime am 13. Juni 2018 – Tobias Rademann, M.A.



last Christmas...

Agenda

1. Was steht auf dem Spiel?
2. Wie funktioniert die digitale Geiselnahme?
3. Wer sind die Geiseln?
4. Wie schütze ich mich davor?
5. Was ist im Ernstfall zu tun?

Kurzprofil

- **Name:** Tobias Rademann, M.A.
- **Funktion:** Geschäftsführer R.iT GmbH
- **Fokus:** iT-Unternehmensberatung für den digitalen Wandel
- **gegründet:** 2001, Spin-Off der Ruhr-Universität
- **Zertifizierung:** BMWi-autorisiert für iT-Sicherheit und digitale Geschäftsprozesse

- **Engagement:**

networker  NRW
Der IT Verband 

Microsoft Partner
Silver Midmarket Solution Provider
Silver Datacenter

 nrw-units
Netzwerkpartner

 eco
VERBAND DER
UNTERNEHMERSCHAFT
MITGLIED

 BVMW
Bundesverband
mittelständische Wirtschaft

Gefördert durch:



aufgrund eines Beschlusses
des Deutschen Bundestages



Was steht auf dem Spiel?

Was steht auf dem Spiel?

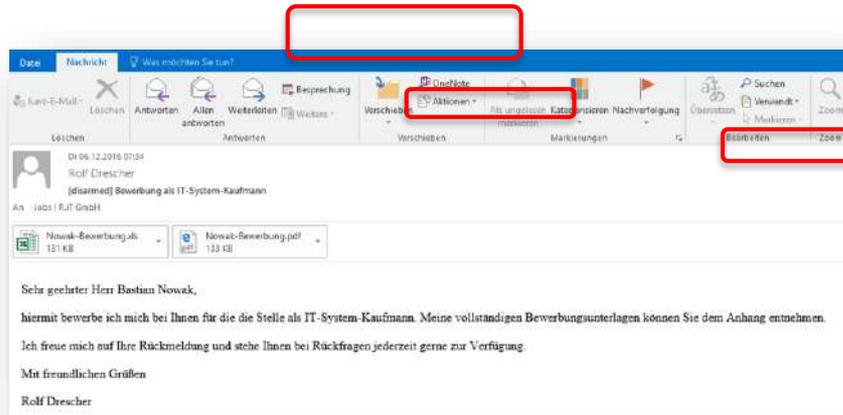




Wie funktioniert die digitale Geiselnahme?

Funktionsweise Verschlüsselungstrojaner

- **Ziel:** Daten als Geiseln (durch Verschlüsselung)
- **Erpressung:** Lösegeld zahlen (= Entschlüsselungs-Code) *oder* Totalverlust
- **Wie:**





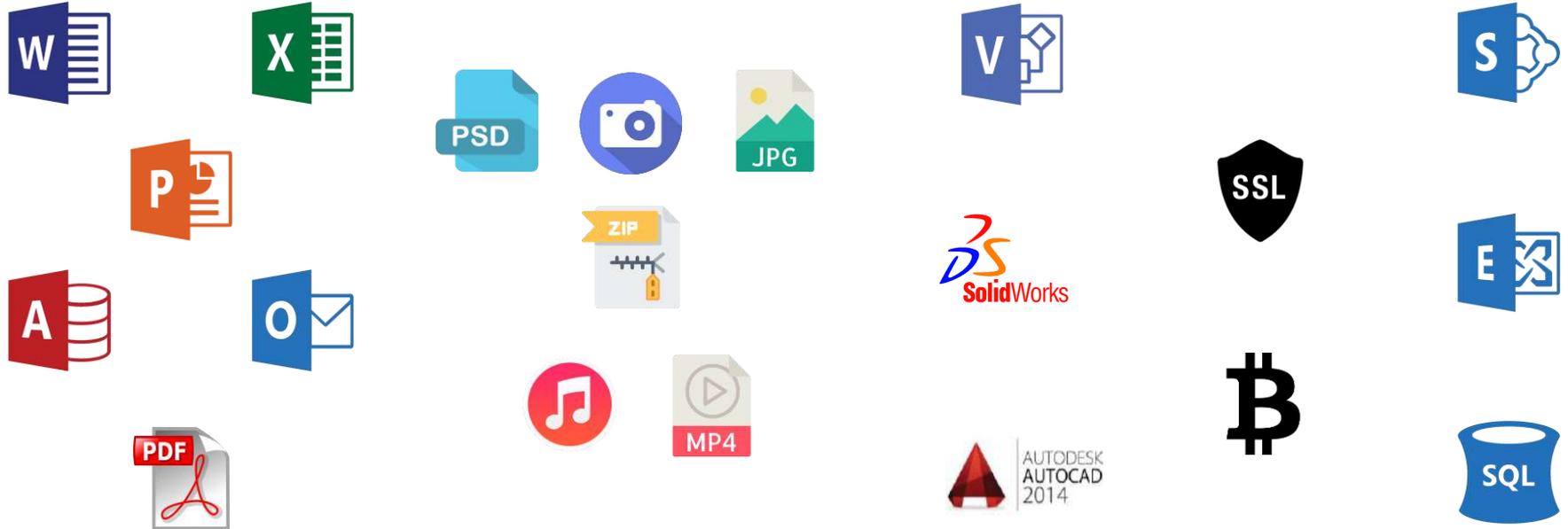
Video: Angriff durch Verschlüsselungstrojaner

An dieser Stelle wurde während der Präsentation ein Video gezeigt, das in der Druckversion aus naheliegenden Gründen nicht enthalten ist 😊.

Wer sind die Geiseln?



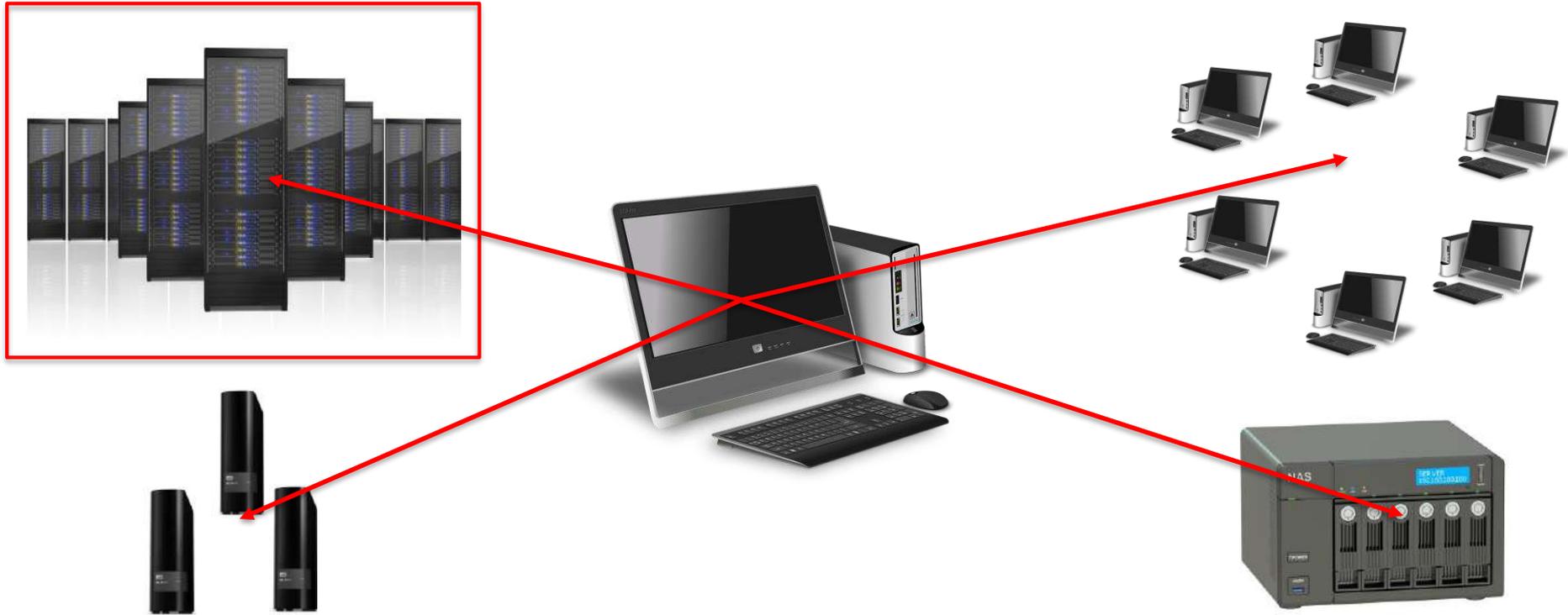
Wer sind die Geiseln?



Wer sind die Geiseln?



Wer sind die Geiseln? / 2





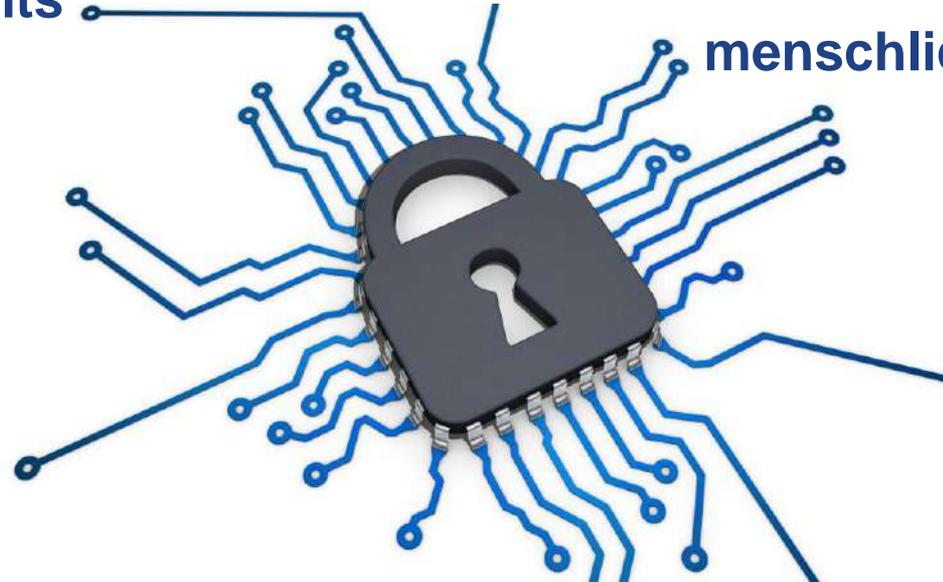
Wie schütze ich mich davor?

Das Wichtigste zuerst...

**Ergebnis:
kein Schutz möglich –
es bleibt ein erhebliches Restrisiko!**

Einschränkungen

Zero-Day Exploits

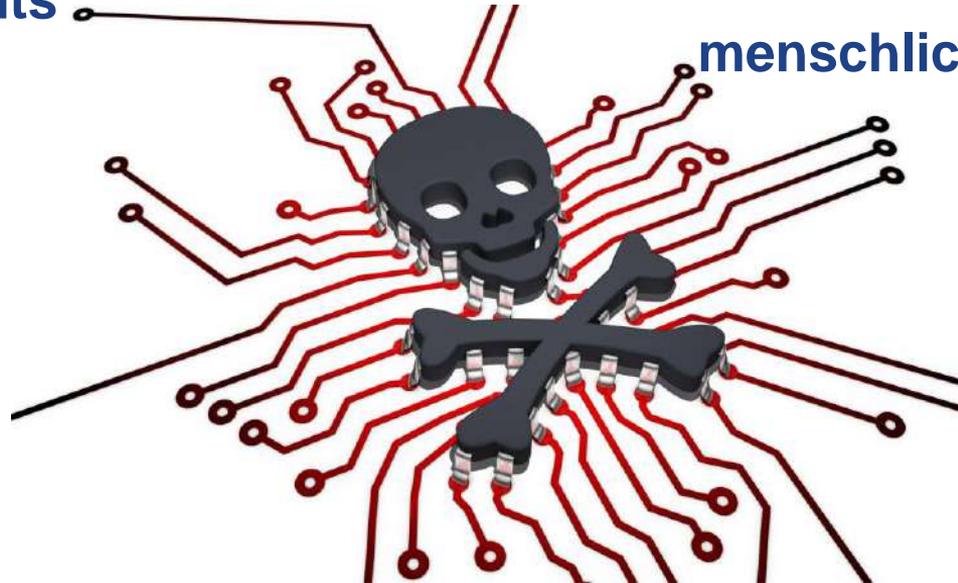


menschliches Versagen

mutwillige Aktionen

Einschränkungen

Zero-Day Exploits



menschliches Versagen

mutwillige Aktionen

Schadensminimierung



Kernziel: handlungsfähig bleiben



Kernziel: handlungsfähig bleiben



Schritt 1: Datensicherung

- Nutzung rotierender Medien
- Offline-Schalten der Ziele
- umsichtige Anbindung der Backupziele
- Trennung der Backupbenutzer von normalen Nutzern
- regelmäßige Durchführung
- Mehrgenerationen-Prinzip

Kernziel: handlungsfähig bleiben

Schritt 2: Wiederherstellung

- regelmäßig getestet
- schnell (d.h. v.a. granular)



weitere Schutzmaßnahmen / I: Anwendersensibilisierung



weitere Schutzmaßnahmen / II: Softwareupdates



weitere Schutzmaßnahmen / III: Firewalls, Viren- und Endgeräteschutz



weitere Schutzmaßnahmen / IV: Makros deaktivieren



The image shows two overlapping dialog boxes from Microsoft PowerPoint. The left dialog is 'PowerPoint-Optionen' (PowerPoint Options) with the 'Trust Center' tab selected. The right dialog is 'Trust Center' with the 'Makroinstellungen' (Macro Settings) tab selected. Red boxes highlight the 'Trust Center' tab in the left dialog, the 'Makroinstellungen' tab in the right dialog, and the radio button for 'Alle Makros mit Benachrichtigung deaktivieren' in the right dialog.

PowerPoint-Optionen

Trust Center

Trust Center

Makroinstellungen

- Alle Makros ohne Benachrichtigung deaktivieren
- Alle Makros mit Benachrichtigung deaktivieren
- Alle Makros außer digital signierten Makros deaktivieren
- Alle Makros aktivieren (nicht empfohlen, weil potenziell gefährlicher Code ausgeführt werden kann)



Was ist im Ernstfall zu tun?

Vorgehen im Ernstfall



Vorgehen im Ernstfall



... und zusätzlich:



Abteilung 4

Cybercrime-
Kompetenzzentrum (cccc)
Ermittlungsunterstützung

... alternativ:

 *bitcoin*

The Bitcoin logo, which is an orange circle containing a white 'B' with two vertical lines through it, followed by the word 'bitcoin' in a bold, italicized, dark grey sans-serif font.

Paysafe 

The Paysafe logo, featuring the word 'Paysafe' in a bold, black sans-serif font, followed by a green icon consisting of three curved lines radiating from a central point.



offene Fragen / Diskussion

Vielen Dank für Ihre Zeit und Ihre Aufmerksamkeit!

Bei Rückfragen wenden Sie sich gerne an:



DIGITIZE YOUR BUSINESS

Tobias Rademann, M.A.

R.iT GmbH • www.RiT.de

Zentrale: Amtmann-lbing-Str. 10, 44805 Bochum

Tel.: (0234) 43 88 00-0, Fax: -29

NL Nord: Tremskamp 5, 23611 Bad Schwartau

Tel.: (0451) 203 68-500, Fax: -499

eMail: Tobias.Rademann@RiT.de

Quellen- und Bildverzeichnis

- Folie 3: © "Christmas with dark background" von Fortyforks, Shutterstock.com;
- Folie 5: © "networker NRW logo" von networker NRW e.V.;
"nrw uniTs Logo" nrw uniTs
"bvmw Logo" von Bundesverband für mittelständische Wirtschaft / CC BY 3.0;
© "eco Logo" von eco - Verband der Internetwirtschaft e.V.;
"BMWi Logo" von Bundesministerium für Wirtschaft und Energie;
© "Microsoft Partner Logo" von Microsoft Company
- Folie 6: © "Kidnapped Businessman" von BlueSkyImage, Shutterstock.com
- Folie 7: © "Baustellenschild Uhr" von JiSign, Fotolia.com;
© "Case full of money" von Franz Pfluegl, Fotolia.com;
© "HDD zerstören" von 3dkombinat, Fotolia.com;
© "Mann steht auf riesigem Schutthaufen" von lassedesignen, Fotolia.com
- Folie 8: © "Terrorist or car thief" von Daniel Jedzura, Shutterstock.com
- Folie 9: "Firefox" von Mozilla / CC-BY 3.0
"Internet Explorer ®" von Microsoft Company
"Chrome ®" von Google Inc.
- Folie 11: © "Boy blindfolded" Jan H Andersen, Shutterstock.com
- Folie 12,13: "Word ®", "Excel ®", "PowerPoint ®", "Access ®", "Outlook ®", "Visio ®",
"SharePoint ®", "Exchange ®" und "SQL Server ®" von Microsoft Company;
© "SolidWorks Logo" von Dassault Systemes Deutschland GmbH;
© "AutoCAD Logo" von Autodesk GmbH;
"bitcoin" von Dave Gandy von flaticon / CC BY 3.0;
"pdf", "mp4" & "jpg" von madebyoliver von flaticon / CC BY 3.0;
"zip" von Freepik von flaticon / CC BY 3.0;
"SSL certificate" von Icon8 / CC BY 3.0
- Folie 14: © "NAS with six disks" von alexlrx, Fotolia.com;
© "Image of many server racks" von Andrey_Popov, Shutterstock.com;
© "HDD" von Western Digital;
"Desktop" von OpenClipart-Vectors / CC0 1.0
- Folie 15: © "police with gunbelt" von RUCHUDA BOONPLIEN, Shutterstock.com
- Folie 17: © "Sicherheitsschloss" von asrawolf , Fotolia.com
- Folie 18: © "Virus" von asrawolf , Fotolia.com
- Folie 19: © "Hand stops domino effect" von oatawa, Shutterstock.com
- Folie 20: © "Sheep cloning" von Jason Benz Bennee, Shutterstock.com
- Folie 21: © "Backup button" von Olivier Le Moal, Shutterstock.com
- Folie 22: © "Disaster recovery plan" von Olivier Le Moal, Shutterstock.com
- Folie 23: © "Recruitment idea concept" von turgaygundogdu, Shutterstock.com
- Folie 24: © "Application update Concept" von thodonal, Fotolia.com
- Folie 25: © "Protection concept" von jijomathadesigners, Shutterstock.com
- Folie 27: © "Special police team" von bibiphoto, Shutterstock.com
- Folie 28: © "Bin dann mal weg!" von DOC RABE Media, Fotolia.com
- Folie 29: © "Disaster recovery plan" von Olivier Le Moal, Shutterstock.com;
© " Finger about to press a power button" von Olivier Le Moal, Shutterstock.com;
© "Innovative technologies in science and medicine" von Sergey Nivens, Shutterstock.com
- Folie 30: "Landeskriminalamt NRW Logo" von LKA NRW Abteilung 4
- Folie 31: "bitcoin Logo" von bitcoin / CC0 1.0;
© "Paysafe Logo" von paysafe.com