



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 13. iT Trends Sicherheit – 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 Dalacenter



Gefördert durch:



aufgrund eines Beschlusses
des Deutschen Bundestages



Was steht auf dem Spiel?

Was steht auf dem Spiel?



Was steht auf dem Spiel?



Was steht auf dem Spiel?



Was steht auf dem Spiel?



Was steht auf dem Spiel?

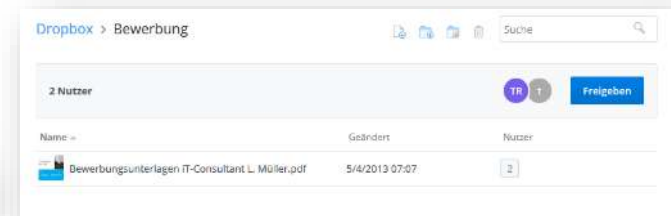
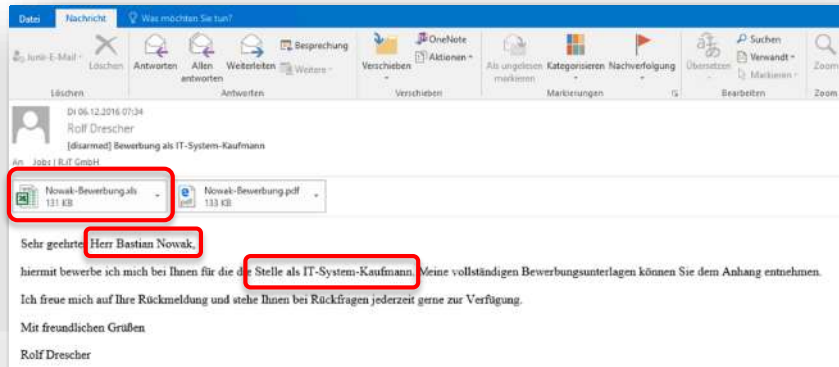




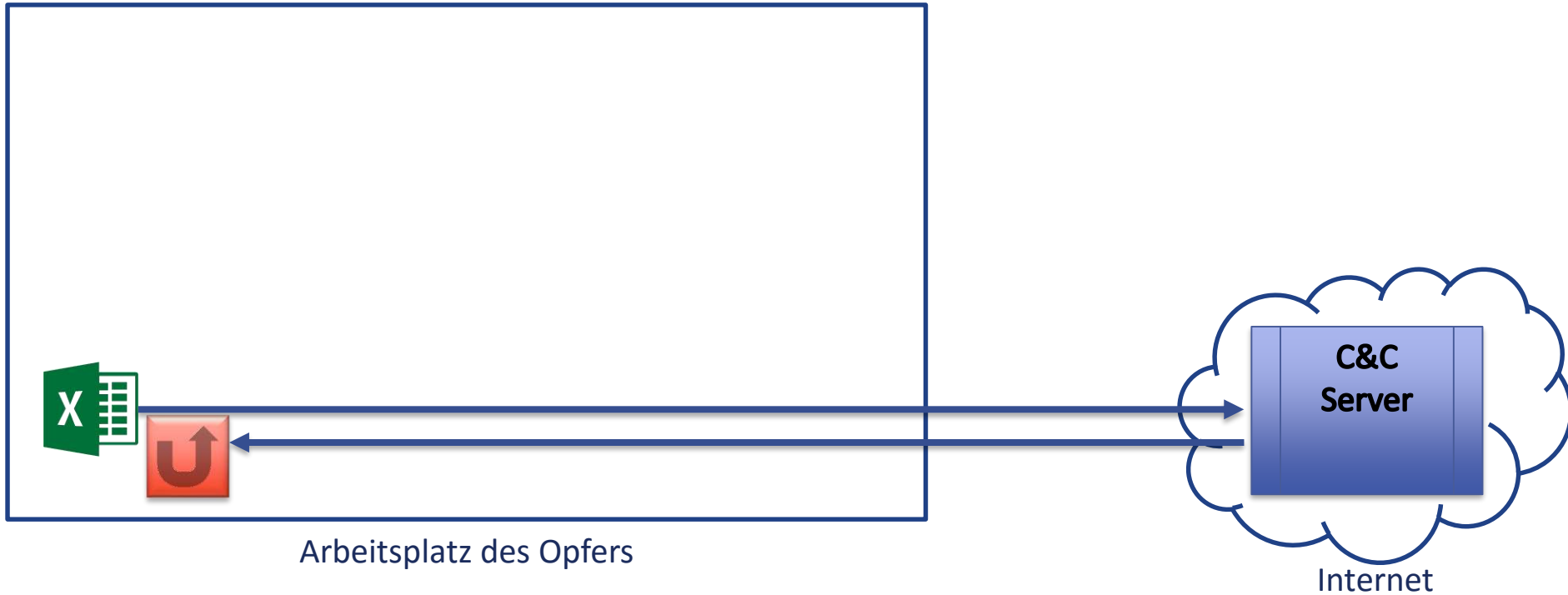
Wie funktioniert die digitale
Geiselnahme?

Funktionsweise Verschlüsselungstrojaner

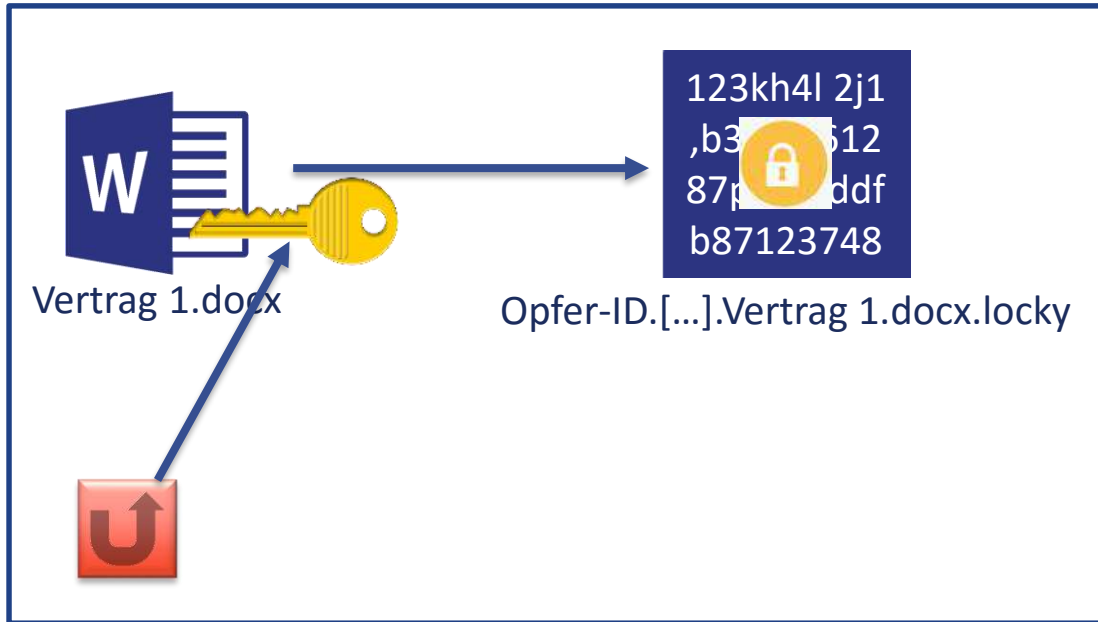
- **Ziel:** Daten als Geiseln (durch Verschlüsselung)
- **Erpressung:** Lösegeld zahlen (= Entschlüsselungs-Code) *oder* Totalverlust
- **Wie:**



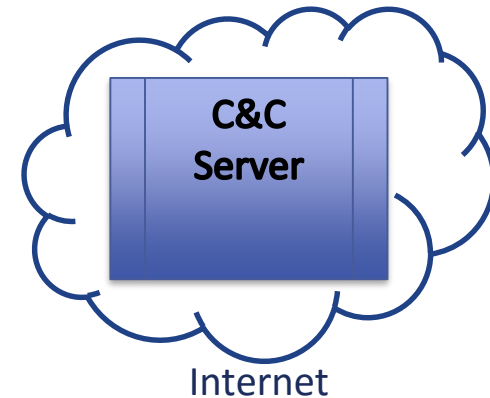
Funktionsweise am Beispiel Locky



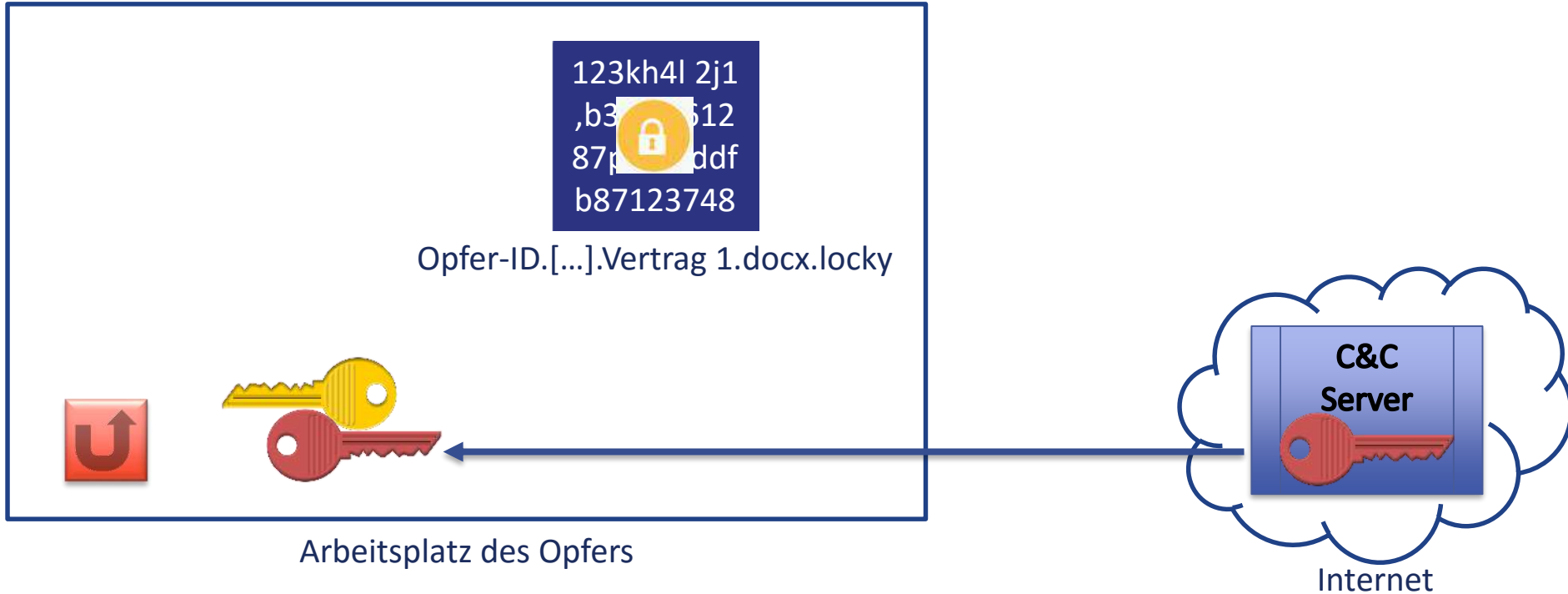
Funktionsweise am Beispiel Locky



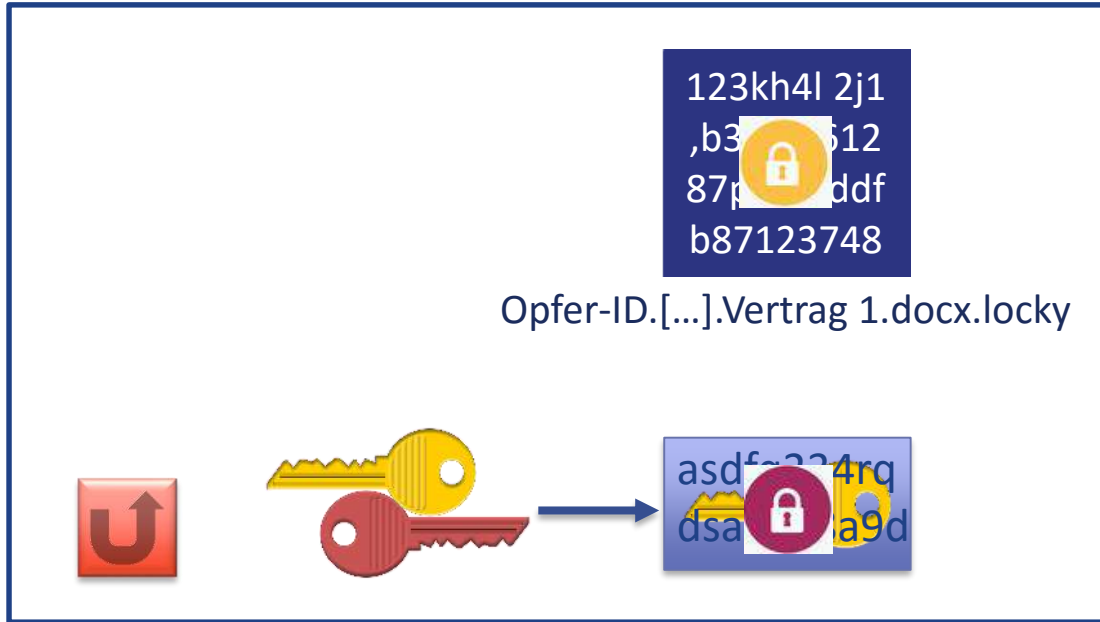
Arbeitsplatz des Opfers



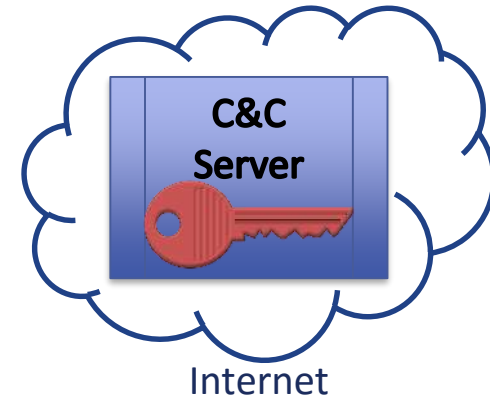
Funktionsweise am Beispiel Locky



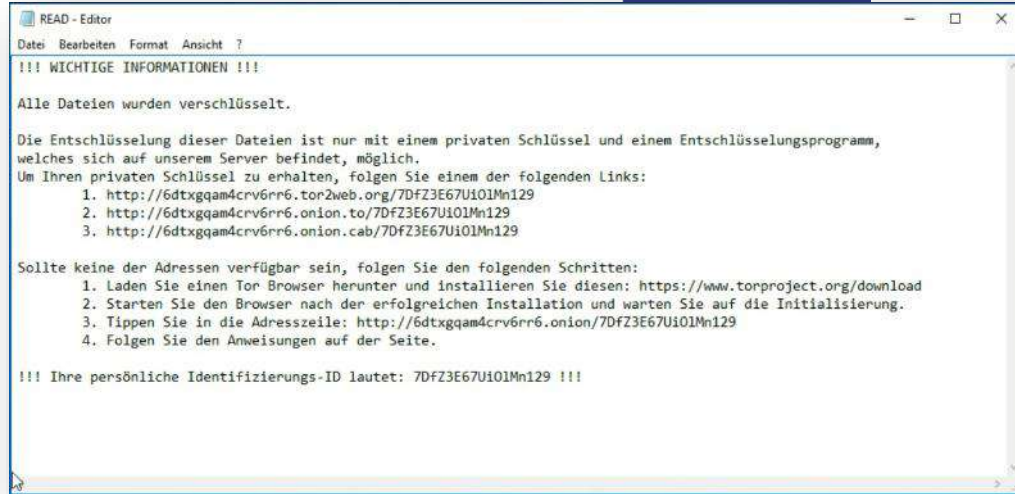
Funktionsweise am Beispiel Locky



Arbeitsplatz des Opfers



Funktionsweise am Beispiel Locky



```
READ - Editor
Datei Bearbeiten Format Ansicht ?

!!! WICHTIGE INFORMATIONEN !!!

Alle Dateien wurden verschlüsselt.

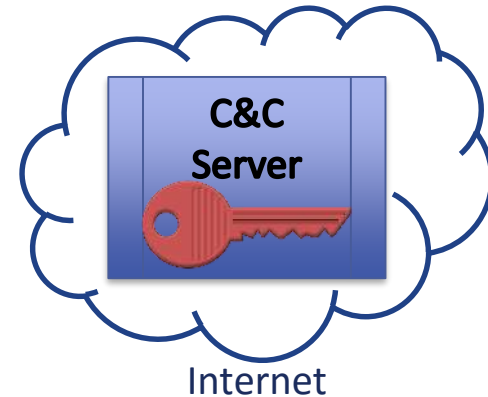
Die Entschlüsselung dieser Dateien ist nur mit einem privaten Schlüssel und einem Entschlüsselungsprogramm,
welches sich auf unserem Server befindet, möglich.

Um Ihren privaten Schlüssel zu erhalten, folgen Sie einem der folgenden Links:
1. http://6dtxgqam4crv6rr6.tor2web.org/7DfZ3E67Ui01Mn129
2. http://6dtxgqam4crv6rr6.onion.to/7DfZ3E67Ui01Mn129
3. http://6dtxgqam4crv6rr6.onion.cab/7DfZ3E67Ui01Mn129

Sollte keine der Adressen verfügbar sein, folgen Sie den folgenden Schritten:
1. Laden Sie einen Tor Browser herunter und installieren Sie diesen: https://www.torproject.org/download
2. Starten Sie den Browser nach der erfolgreichen Installation und warten Sie auf die Initialisierung.
3. Tippen Sie in die Adresszeile: http://6dtxgqam4crv6rr6.onion/7DfZ3E67Ui01Mn129
4. Folgen Sie den Anweisungen auf der Seite.

!!! Ihre persönliche Identifizierungs-ID lautet: 7DfZ3E67Ui01Mn129 !!!
```

Arbeitsplatz des Opfers



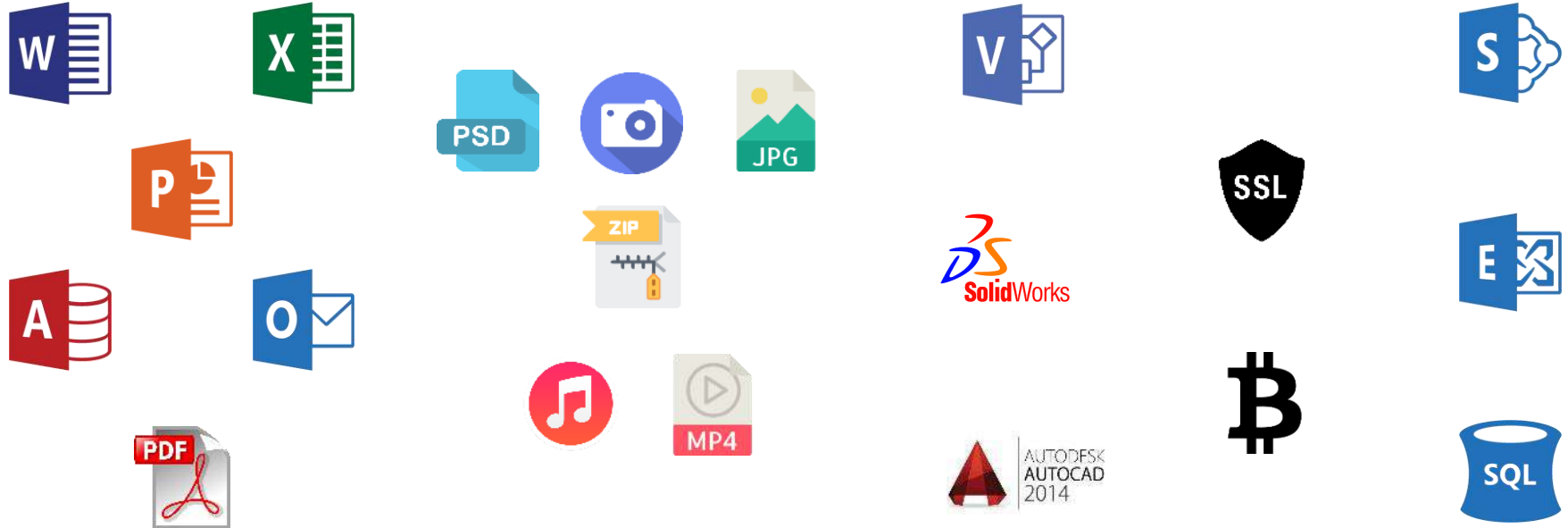
Video: Angriff durch Verschlüsselungstrojaner

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

Wer sind die Geiseln?



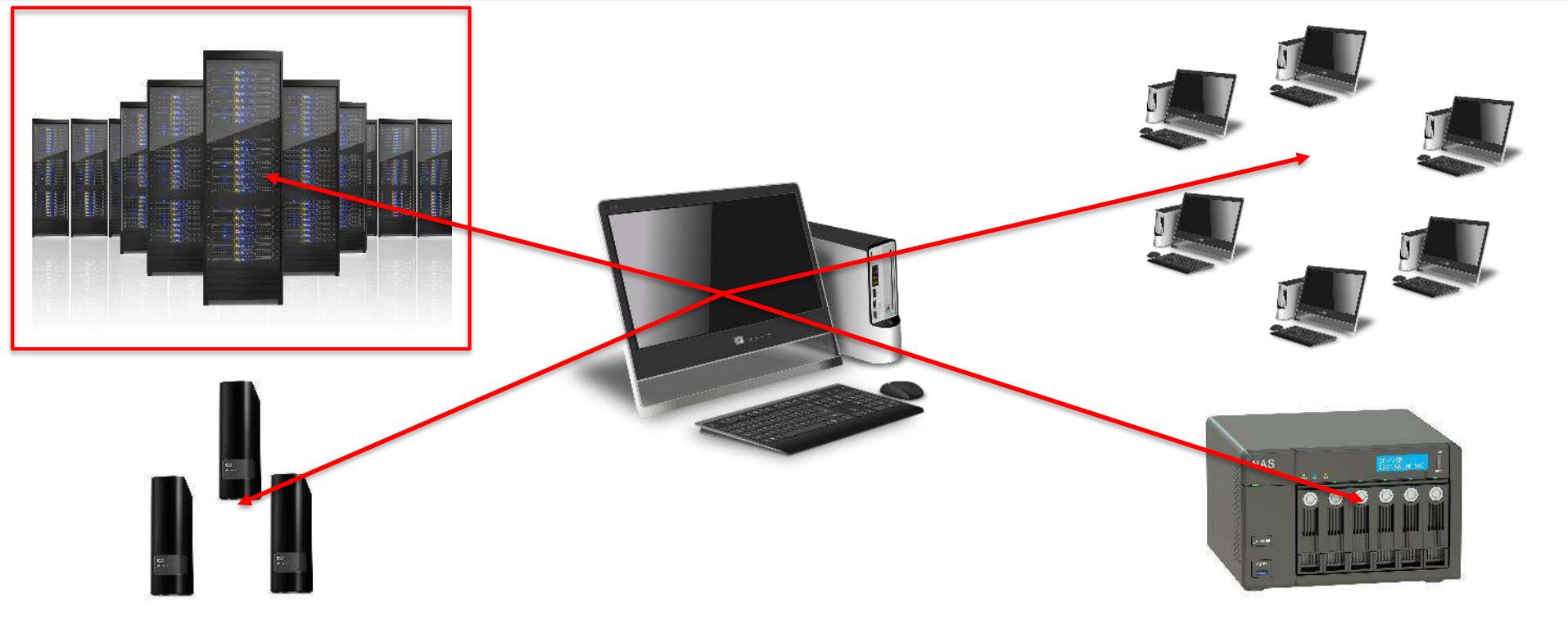
Wer sind die Geiseln?



Wer sind die Geiseln?



Wer sind die Geiseln? / 2





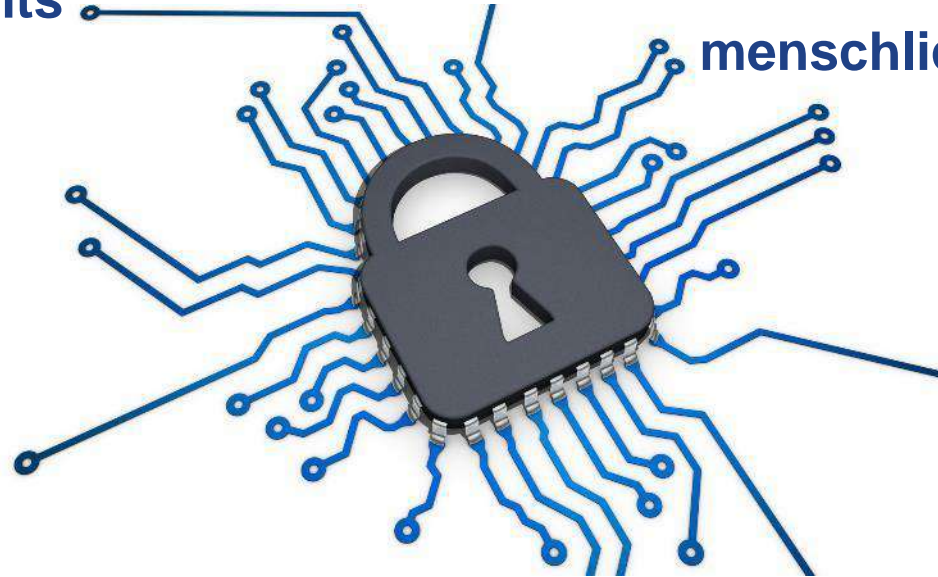
Wie schütze ich mich davor?

Das Wichtigste zuerst...

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

Einschränkungen

Zero-Day Exploits

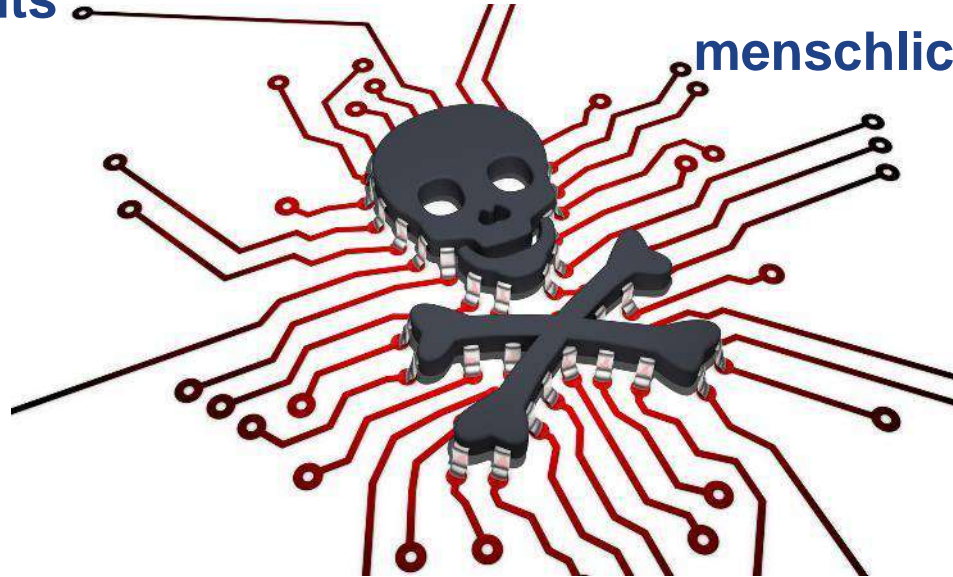


menschliches Versagen

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**



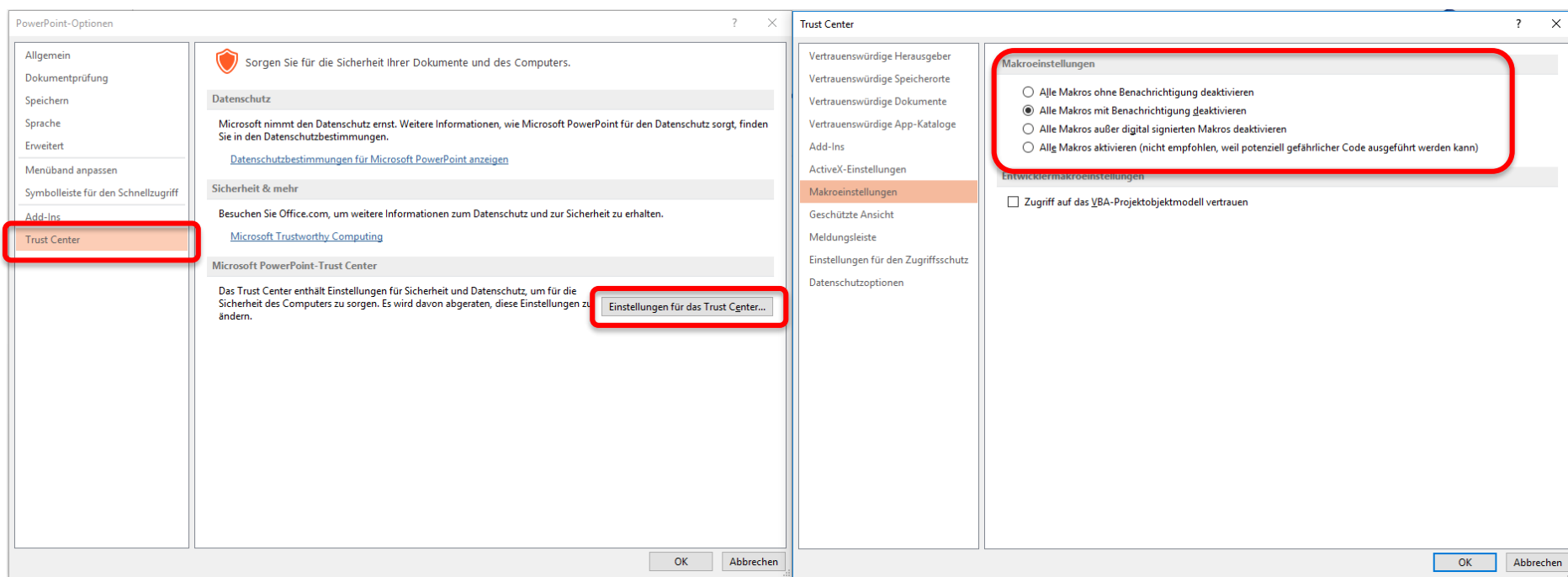
weitere Schutzmaßnahmen / II: Softwareupdates



weitere Schutzmaßnahmen / III: Firewalls, Viren- und Endgeräteschutz



weitere Schutzmaßnahmen / IV: Makros deaktivieren





Was ist im Ernstfall zu tun?

Vorgehen im Ernstfall



Vorgehen im Ernstfall



... und zusätzlich:



Abteilung 4

Cybercrime-
Kompetenzzentrum (cccc)
Ermittlungsunterstützung

... alternativ:



Offene Fragen / Diskussion

**Vielen Dank für
Ihre Zeit und Ihre Aufmerksamkeit!**

Stand Nr. 7

Bei Rückfragen wenden Sie sich gerne an:



DIGITIZE YOUR BUSINESS

Tobias Rademann, M.A.

R.iT GmbH

www.RiT.de

Amtmann-Ibing-Str. 10

44805 Bochum

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

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
- Folie 8: © "Case full of money" von Franz Pfluegl, Fotolia.com
- Folie 9: © "HDD zerstören" von 3dkombinat, Fotolia.com
- Folie 10: © "Mann steht auf riesigem Schutthaufen" von lassedesignen, Fotolia.com
- Folie 11: © "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 12: © "Terrorist or car thief" von Daniel Jedzura, Shutterstock.com
- Folie 13: "Firefox" von Mozilla / CC-BY 3.0
 "Internet Explorer ®" von Microsoft Company
 "Chrome ®" von Google Inc.
- Folie 14: © "Lock sign icon" von irina, Fotolia.com;
 "Word ®", "Excel ®" von Microsoft Company
- Folie 16: © "Boy blindfolded" Jan H Andersen, Shutterstock.com
- Folie 17,18: "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 19: © "NAS with six disks" von alexlmx, Fotolia.com;
 © "Image of many server racks" von Andrey_Popov, Shutterstock.com;
 © "HDD" von Western Digital;
 "Desktop" von OpenClipart-Vectors / CC0 1.0
- Folie 20: © "police with gunbelt" von RUCHUDA BOONPLIEN, Shutterstock.com
- Folie 22: © "Sicherheitsschloss" von asrawolf , Fotolia.com
- Folie 23: © "Virus" von asrawolf , Fotolia.com
- Folie 24: © "Hand stops domino effect" von oatawa, Shutterstock.com
- Folie 25: © "Sheep cloning" von Jason Benz Bennee, Shutterstock.com
- Folie 26: © "Backup button" von Olivier Le Moal, Shutterstock.com
- Folie 27: © "Disaster recovery plan" von Olivier Le Moal, Shutterstock.com
- Folie 28: © "Recruitment idea concept" von turgaygundogdu, Shutterstock.com
- Folie 29: © "Application update Concept" von thodonai, Fotolia.com
- Folie 30: © "Protection concept" von jijomathadesigners, Shutterstock.com
- Folie 32: © "Special police team" von bibiphoto, Shutterstock.com
- Folie 33: © "Bin dann mal weg!" von DOC RABE Media, Fotolia.com
- Folie 34: © "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 35: "Landeskriminalamt NRW Logo" von LKA NRW Abteilung 4
- Folie 36: "bitcoin Logo" von bitcoin / CC0 1.0;
 © "Paysafe Logo" von paysafe.com