

IT-SECURITY

Die Achillesferse
im Unternehmen

Prof. Dr.
Dominik Herrmann

Privacy and Security Group @ Uni Bamberg

 @herdom

Folien: dhgo.to/achillesferse



„Erklären Sie ihnen einfach, wie sie sich am besten schützen können!“

...



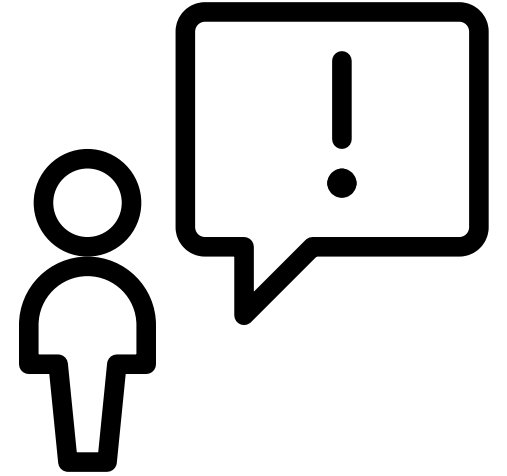
OK, kein Problem.

231 Sicherheitsexperten wurden befragt:

Was sind die 3 wichtigsten Ratschläge, die Sie einem technisch nicht versierten Benutzer geben würden?

Ergebnis

152 verschiedene Ratschläge...



Was davon ist wichtig?

Was wird schon getan und warum reicht das nicht?

WIK-Studie

IT-Sicherheit in KMU

2017

IT-Ausfall Erpressung

nachlässige MA

Virenangriff

Innentäter

Außentäter

Verlust mobiler
Geräte

WIK-Studie

IT-Sicherheit in KMU

Antivirus

Backup

Verschlüsselung

kein Zeit

kein Geld

Firewall

Antispam

Sensibilisierung

kein Überblick

Passwörter

Zugriffskontrolle

Monitoring

<5000 EUR / Jahr

Zwei Handlungsebenen

1

Auf Ebene der
Organisation





2

**Auf Ebene
individueller
Mitarbeiter**

1

Auf Ebene der
Organisation



Auszug aus den 152 Ratschlägen

Überall unterschiedliche
Passwörter!

Automatische Updates
aktivieren!

Nur Software aus ver-
trauenswürdigen Quellen!

Nicht auf Links klicken bzw.
vorher nachdenken!

Keine unerwarteten
Anhänge öffnen!

**zweifelhafter Nutzen
bzw. kaum umsetzbar**

Compliance-Kultur

IT-Grundschutz / ISO 2700x
DSGVO

„Wir müssen etwas tun“
Best Practices
überlieferter Nutzen

nicht effektiv

nicht effizient





Was sehen Sie hier?





Wir haben Backups!

Können Sie sie auch zurückspielen?

Auch Ausfallsicherheit durch Redundanz und Diversität?

Verlust mobiler Geräte

Festplattenverschlüsselung für Laptops?

Auch für USB-Sticks, Smartphones, Tablets!

Überall starke Passwörter oder biometrische Authentifizierung?

Bitlocker (Win), FileVault (Mac), Veracrypt

Schadsoftware

PETYA RANSOMWARE - St... x +

Verschlüsselungstrojaner

petya[redacted].onion/N[redacted]

Start Bezahlung FAQ Hilfe Deutsch

Ihr Computer wurde verschlüsselt

Die Festplatten Ihres Computers wurden mit einem sicheren Verschlüsselungsalgorithmus verschlüsselt. Es ist unmöglich, Ihre Daten ohne einen speziellen Schlüssel wiederherzustellen. Diese Seite hilft Ihnen mit dem Kauf dieses Schlüssels und wird Sie bei der vollständigen Entschlüsselung Ihres Computers unterstützen.

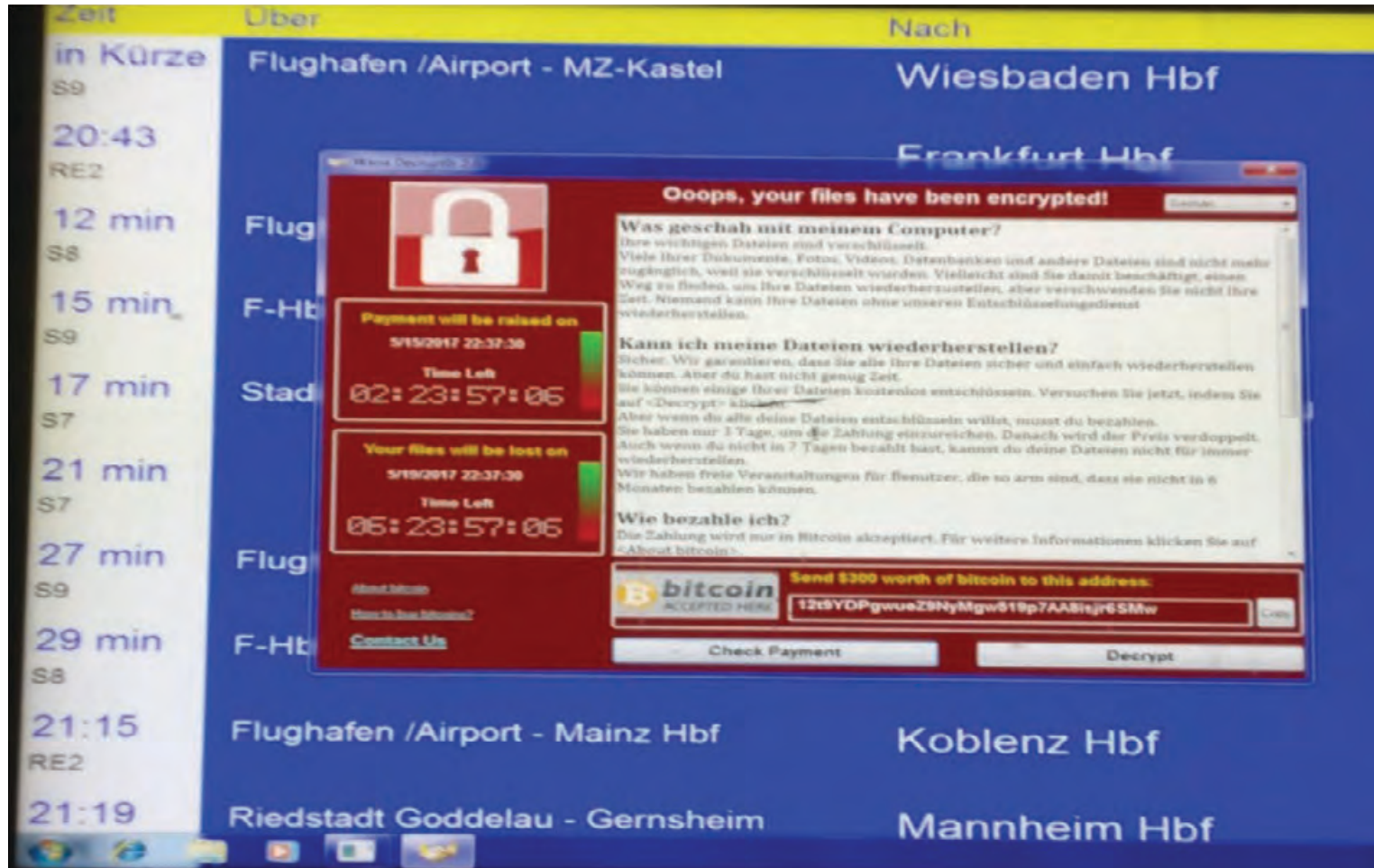
⌚ Der Preis wird verdoppelt in:

6 Tagen 12 Stunden 2 Minuten 24 Sekunden

[Mit der Entschlüsselung beginnen](#)

Wir haben doch schon einen Virens Scanner!

... und wiederherstellbare Backups haben wir auch!



Auch einen Notfallplan zur schnellen Wiederherstellung?

Online Pay eG  

 Archive -

Dominik Herrmann - Online Pay eG automatische Lastschrift konnte n

To: Dominik Herrmann


Sehr geehrte/r Dominik Herrmann,

die ausstehende Überweisung erwarten wir bis spätestens 12.09.2018. Kö
Überweisung bestätigen, sehen wir uns gezwungen Ihre Forderung an ein
Kosten gehen zu Ihrer Last.



04.09.2018
Online...eG.zip

„aktuellen Virens Scanner verwenden“



2 engines detected this file

SHA-256 02172875a3c8b73cc1563e1137244d09c703e8f0c05e80e2d7b47c78128d7687

File name soledad.zip

File size 1.18 MB

Last analysis 2017-09-02 01:29:06 UTC

2 / 58

Virenscanner

häufig wirkungslos



Lösung: Mitarbeiter sensibilisieren?

„Unverlangte Mails mit **Links oder Anhängen**
sorgfältig prüfen. Auch von Kollegen!“

Sender anrufen
und nachfragen

Anhang zu *virustotal.com*
hochladen oder mit
docs.google.com öffnen

E-Mail-Header
analysieren

Return-Path: <inkasso@onlinepay.com>

X-Original-To: dh@myserver.de

Received: from server.myserver.de ([127.0.0.1])

by localhost (server.myserver.de [127.0.0.1]) (amavisd-new, port 10024)

with ESMTPE id w5KM04U2LGJA for <dh@myserver.de>;

Wed, 5 Sep 2018 01:21:29 +0200 (CEST)

X-policyd-weight: NOT_IN_SBL_XBL_SPAMHAUS=-1.5 NOT_IN_SPAMCOP=-1.5 CL_IP_EQ_HELO_IP=-2

Received: from kvm21229.hv9.ru (cp.uplinkweb.ru [89.108.83.199])

by server.myserver.de (Postfix) with ESMTPE

for <dh@myserver.de>; Wed, 5 Sep 2018 01:21:28 +0200 (CEST)

Received: by kvm21229.hv9.ru (Postfix, from userid 500)

id 840A71A7D45; Wed, 5 Sep 2018 06:21:29 +0700 (+07)

Date: Wed, 5 Sep 2018 06:21:29 +0700 (+07)

To: Dominik Herrmann <dh@myserver.de>

From: Online Pay eG <inkasso@onlinepay.com>

Subject: Dominik Herrmann - Online Pay eG: Ihre persönliche Lastschrift konnte nicht vorgenommen werden.

Message-ID: <f5577137f00e3d656f8a4ad60a505795@testomsk.uplinkweb.ru>

MIME-Version: 1.0

Content-Type: multipart/mixed; boundary="b1_f5577137f00e3d656f8a4ad60a505795"

Content-Transfer-Encoding: 8bit

Für Technikgläubige: cloudbasierte Sandbox

Datenschutzfolgenabschätzung nötig?

PAYLOAD SECURITY Home Submissions Contact FAQ Search (MD5, SHA2) More

August 28 2015, 5:15 (CDT) Input **newoe2**
PE32 executable (GUI) Intel 80386, for MS Windows
69a0ade25b4e7ef6e1208c554872198f59507a443933db8529d6c243e57e7ed4

Threat level **malicious**

Summary Threat Score: **69/100**
AV Detection: **Unknown** ←
Matched 31 Signatures

Countries

Environme... Windows 7 32 bit (EN)

August 28 2015, 5:05 (CDT) Input **PaymentReceipt.xls**
Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.2, Co ...
a526a54bf62269162c0130a044b65a156461f7887773b883541940b23886f398

Threat level **malicious**

Summary Threat Score: **100/100**
AV Detection: **8%** ←
Matched 42 Signatures
Classified as *LooksLike.Macro.Malware*

Countries

Environme... Windows 7 32 bit (EN)

Effektiv: Defense in Depth



In E-Mails nur PDF-Anhänge akzeptieren
Rest abweisen oder löschen – auch intern

Strikte Netzwerk-Segmentierung
mit VLANs und Firewall-Regeln

Separater Rechner oder Virtuelle Maschine (VM)
für Kommunikation mit Externen

(öffentlich erreichbare)
Angriffsfläche reduzieren



Outdated versions of WordPress and Drupal led to the Panama Papers leak

Unpatched Magento Stores hacked to mine Monero and steal card details

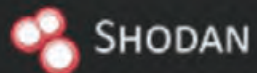
More than 1000 Magento sites hacked to leak credit card details and infect visitors' PCs with malware.

Asset-Management für
gute Übersicht und
zuverlässige Updates

Internet-of-Things-
Geräte isolieren
(Netzwerk-Segment.)

Nur erlaubte Anwendungen
ausführen (Whitelist mit
AppLocker bzw. WDAC)

Öffentlich erreichbare
Dienste und Informationen
regelmäßig prüfen ...

[Explore](#)[Downloads](#)[Reports](#)[Pricing](#)[Enterprise Access](#)[My Account](#)[Exploits](#)[Maps](#)[Images](#)[Share Search](#)[Download Results](#)[Create Report](#)

TOTAL RESULTS

0

TOP COUNTRIES



New Service: Keep track of what you have connected to the Internet. Check out [Shodan Monitor](#)

93.206.102.222

p5DCE66DE.dip0.t-ipconnect.de

Deutsche Telekom AG

Added on 2019-11-02 14:41:28 GMT

Germany, Rottenbach



Wartung in
0 h

Wasser EIN
82.0 °C

Fern-Wartung
aktiv
Fenster schließen

Gas Verbrauch
173.4 m³/h

Abgas 1
715.7 °C

Gasvordruck
-21.6 mbar

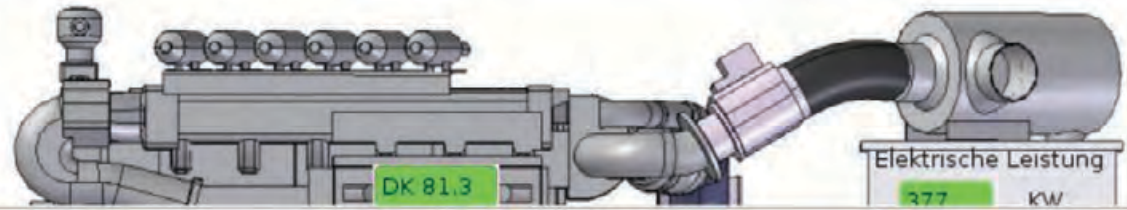
Venturi
65.5 %

Aufstellhöhe
483 N.N.

Gemisch
45.6 °C

Ladedruck
Ist
1.073 bar

Ladedruck
Soll
1.076 bar



Leistung eingestellt über Gassack !

100% Leistung	Reduzier 2 380 KW
MOTOR STOP	MOTOR NOTAUS !



You are here: [Home](#) > [Projects](#) > [SSL Server Test](#) > mpsserver.eu

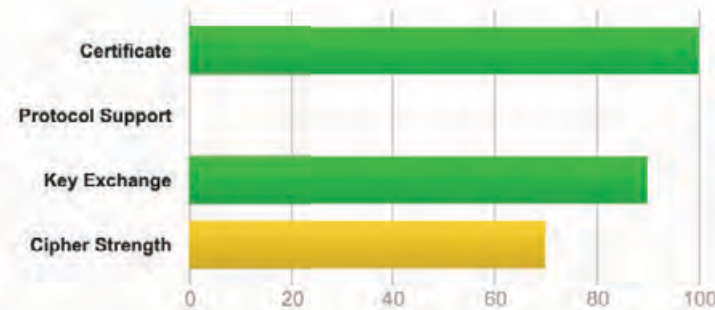
SSL Report: mpsserver.eu (92.65.9.118)

Assessed on: Thu, 07 Nov 2019 15:56:59 UTC | [Clear cache](#)

[Scan Another »](#)

Summary

Overall Rating



Visit our [documentation page](#) for more information, configuration guides, and books. Known issues are documented [here](#).

This server supports SSL 2, which is obsolete and insecure, and can be used against TLS (DROWN attack). Grade set to F. [MORE INFO »](#)

The server supports only older protocols, but not the current best TLS 1.2. Grade capped to C. [MORE INFO »](#)

This server accepts RC4 cipher, but only with older protocols. Grade capped to B. [MORE INFO »](#)

This server does not support Authenticated encryption (AEAD) cipher suites. Grade capped to B. [MORE INFO »](#)

This server supports TLS 1.0. Grade will be capped to B from January 2020. [MORE INFO »](#)

crt.sh Identity Search [Group by Issuer](#)

Criteria Identity LIKE "%.bahn.de"

Certificates	crt.sh ID	Logged At	Not Before	Not After	Identity	Issuer Name
	2078513846	2019-11-06	2019-11-06	2020-02-04	www-ak.bahn.de	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	2078513739	2019-11-06	2019-11-06	2020-02-04	www-ak.bahn.de	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	2051844707	2019-10-29	2019-10-29	2020-01-27	mailing.bahn.de	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	2048665785	2019-10-29	2019-10-29	2020-01-27	mailing.bahn.de	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	2041173015	2019-10-26	2019-10-26	2020-01-24	fahrkarten1.bahn.de	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	2041173015	2019-10-26	2019-10-26	2020-01-24	fahrkarten1b.bahn.de	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	2041173015	2019-10-26	2019-10-26	2020-01-24	fahrkarten1c.bahn.de	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	2041173015	2019-10-26	2019-10-26	2020-01-24	fahrkarten1d.bahn.de	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	2041173015	2019-10-26	2019-10-26	2020-01-24	fahrkarten2.bahn.de	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	2041173015	2019-10-26	2019-10-26	2020-01-24	fahrkarten2b.bahn.de	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	2041173015	2019-10-26	2019-10-26	2020-01-24	fahrkarten2c.bahn.de	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	2041173015	2019-10-26	2019-10-26	2020-01-24	fahrkarten2d.bahn.de	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	2041173015	2019-10-26	2019-10-26	2020-01-24	fahrkarten3.bahn.de	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	2041173015	2019-10-26	2019-10-26	2020-01-24	fahrkarten3b.bahn.de	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	2041173015	2019-10-26	2019-10-26	2020-01-24	fahrkarten3c.bahn.de	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	2041173015	2019-10-26	2019-10-26	2020-01-24	fahrkarten3d.bahn.de	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	2041173015	2019-10-26	2019-10-26	2020-01-24	fahrkarten4.bahn.de	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	2041173015	2019-10-26	2019-10-26	2020-01-24	fahrkarten4b.bahn.de	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	2041173015	2019-10-26	2019-10-26	2020-01-24	fahrkarten4c.bahn.de	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	2041173015	2019-10-26	2019-10-26	2020-01-24	fahrkarten4d.bahn.de	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	2035913613	2019-10-26	2019-10-26	2020-01-24	fahrkarten1.bahn.de	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	2035913613	2019-10-26	2019-10-26	2020-01-24	fahrkarten1b.bahn.de	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	2035913613	2019-10-26	2019-10-26	2020-01-24	fahrkarten1c.bahn.de	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	2035913613	2019-10-26	2019-10-26	2020-01-24	fahrkarten1d.bahn.de	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	2035913613	2019-10-26	2019-10-26	2020-01-24	fahrkarten2.bahn.de	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	2035913613	2019-10-26	2019-10-26	2020-01-24	fahrkarten2b.bahn.de	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	2035913613	2019-10-26	2019-10-26	2020-01-24	fahrkarten2c.bahn.de	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	2035913613	2019-10-26	2019-10-26	2020-01-24	fahrkarten2d.bahn.de	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	2035913613	2019-10-26	2019-10-26	2020-01-24	fahrkarten3.bahn.de	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	2035913613	2019-10-26	2019-10-26	2020-01-24	fahrkarten3b.bahn.de	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	2035913613	2019-10-26	2019-10-26	2020-01-24	fahrkarten3c.bahn.de	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	2035913613	2019-10-26	2019-10-26	2020-01-24	fahrkarten3d.bahn.de	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	2035913613	2019-10-26	2019-10-26	2020-01-24	fahrkarten4.bahn.de	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3

Deutsche Bahn: bahn.de - Ihr ...

https://www-ak.bahn.de/p/view/index.shtml

Startseite | bahn.de/aktuell | Hilfe & Kontakt | Sitemap | Deutsch

Tickets & Angebote | Reise & Services | BahnCard | Geschäftskunden | Urlaub & Städte | Meine Bahn | Login

Gst Buddy Java Test "test3_publishOnBahnDe" BAHN.DE TITLE

Gst Buddy Java Test "test3_publishOnBahnDe" BAHN.DE TEXT

Zu [bahn.de/aktuell](#)

Reiseauskunft | Sparpreis-Finder | Ist mein Zug pünktlich? | Meine Buchungen

von Bahnhof / Haltestelle / Adresse nach Bahnhof / Haltestelle / Adresse

Do, 07.11.19 17:08 Ab An



CCDCOE

NATO Cooperative Cyber Defence
Centre of Excellence Tallinn, Estonia

Teemu Väisänen, Lorena Trinberg and Nikolaos Pissanidis

I accidentally malware - what should I do... is this dangerous?

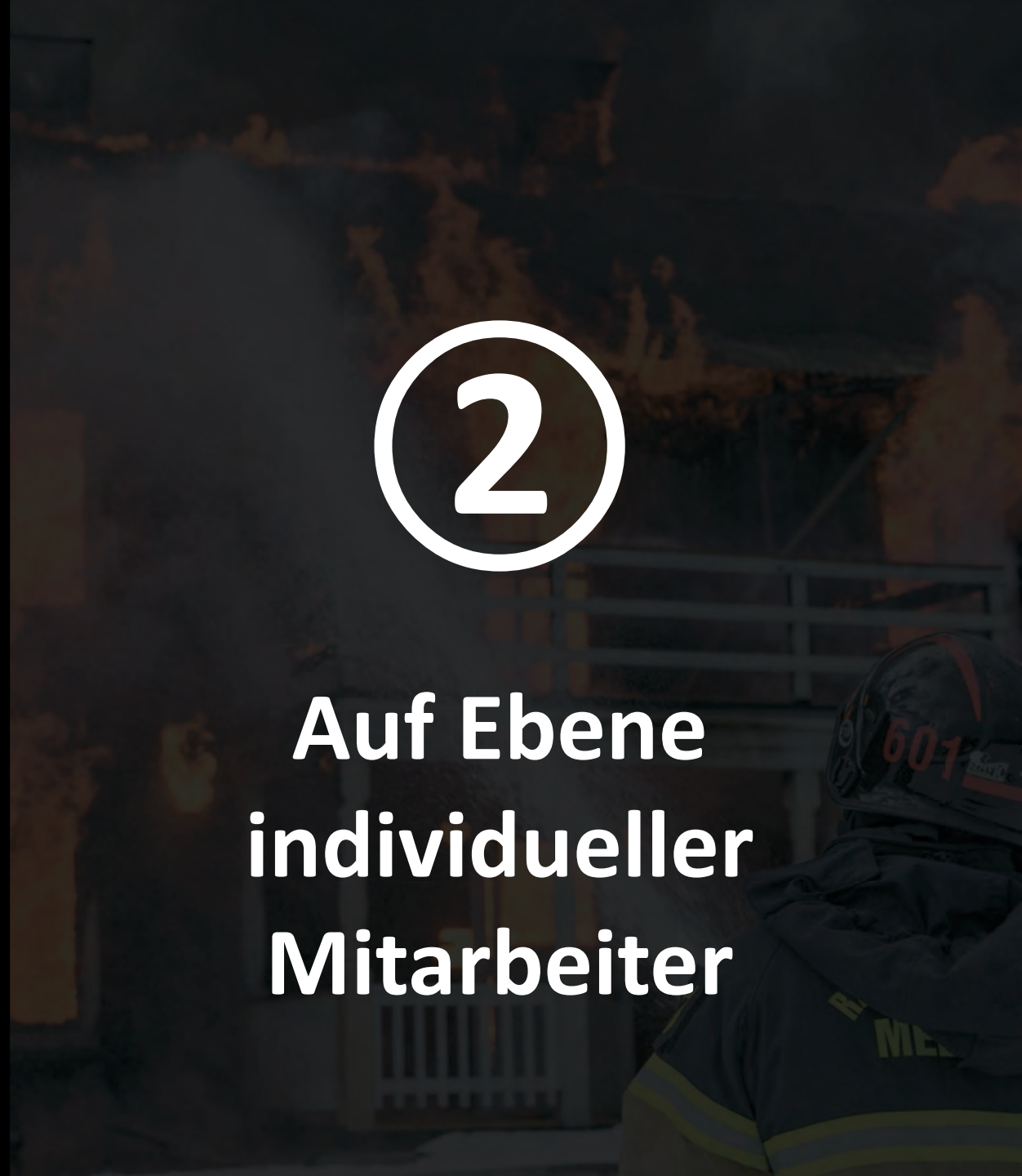
Overcoming inevitable risks of electronic communication

Weitergehende
Sicherheitsmaßnahmen



2

**Auf Ebene
individueller
Mitarbeiter**



i got the nuttiest new CCV code

For Customer Service (U.S.) - 800.786.8787

Int'l Direct - 800.STTRAVEL (800.7887.2835)



007



suntrust.com

Authorized Signature

Not Valid Unless Signed

By use of this card, you agree to the Fee Schedules and all Regulations that govern all SunTrust Deposit Accounts.

F1057884 06/18 cpi-co

ICA-12302

17-40-000-06



mastercard.



Neulich
auf Twitter

Mitarbeiter-Sensibilisierung: Skepsis und Misstrauen

Cui bono?

USB Sticks
- 128 GB -
kostenlos



This \$3 DIY USB Device Will Kill Your Computer

June 27th 2018

[TWEET THIS](#)



Schnell zugreifen
bevor sie weg sind?

Effektiv: CEO-Betrugsmasche

https://www.cnbc.com/video/3000537848

From: Tom Kemp [<mailto:tom.kemp@centrfiy.com>]
Sent: Wednesday, September 16, 2015 8:56 AM
Subject: Payment Instruction

Dear Tim,

I will need you to process an urgent payment, which needs to go out today as a same value day payment.

Let me know when you are set to proceed, so i can have the a

tom.kemp@centrfiy.com]
er 16, 2015 8:56 AM
on NER

Jennifer,

Process a wire of \$357,493.41 to the attached a

Thanks
Tim

NER
Forwarded message -----



NER TOM KEMP
CENTRIFY CEO
PRODUCED BY CNBC

Hilft Sensibilisierung
zum Schutz vor
(Spear-)Phishing?

Vorschlag: Fake-Phishing-Kampagne

Schulungen und
Ermahnungen
sich „sicher“
zu verhalten:
wenig effektiv

- ① Compliance-Budget
- ② Vorfälle treten (zu) selten ein
aber: hohe Schutzkosten
Produktivitätsverlust
längere Antwortzeiten
Vertrauensverlust
Entfremdung

Schulungen und
Ermahnungen
sich „sicher“
zu verhalten:
wenig effektiv

Sinnvoller:

Organisatorische Maßnahmen

- ① **Sichere Messenger (z.B. Signal)**
- ② **Zwei-Faktor-Authentifizierung
für Cloud-Dienste **und** intern
(aber: Notfallplan erforderlich
„2. Faktor nicht verfügbar“)**

Was ist ein gutes Passwort?

„Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen“
„Passwort regelmäßig ändern“

hallo123

passwort

Hallo123!

Passwort.4

12345

2010-Auggust

master

123456

Ibi=zEd4

schlechter als

mehlbalkontisch

Warum?

Warum?





Wie viele Rate-Versuche?
(alle Möglichkeiten durchprobieren)

! " # \$ % & ' () * + , -
. / 0 1 2 3 4 5 6 7 8 9 : ;
< = > ? @ A B C D E F G H I
J K L M N O P Q R S T U V W
X Y Z [\] ^ _ ` a b c d e
f g h i j k l m n o p q r s
t u v w x y z

90 Zeichen

lbi=zEd4 (8 Stellen)

4.304.672.100.000.000

Versuche (höchstens)

lbi=zEd4 (8 Stellen)

4.304.672.100.000.000

Versuche (höchstens)

mehlbalkontisch (15 Stellen)

1.677.259.342.285.725.925.376

Versuche (nur Kleinbuchstaben)

Angreifer
sind schlau.



aaaaaaaaaaaaaaaaa**a** ... aaaaaaaaaaaaaaaaaa**b** ...

mehlbalkontisch ... zzzzzzzzzzzzzzzzzzzzz

1.677.259.342.285.725.925.376 Versuche

aachenaachenaachen ... aachenaachenaal ...

mehlbalkontisch ... zuziehenzuziehenzuziehen

125.000.000.000.000.000 Versuche

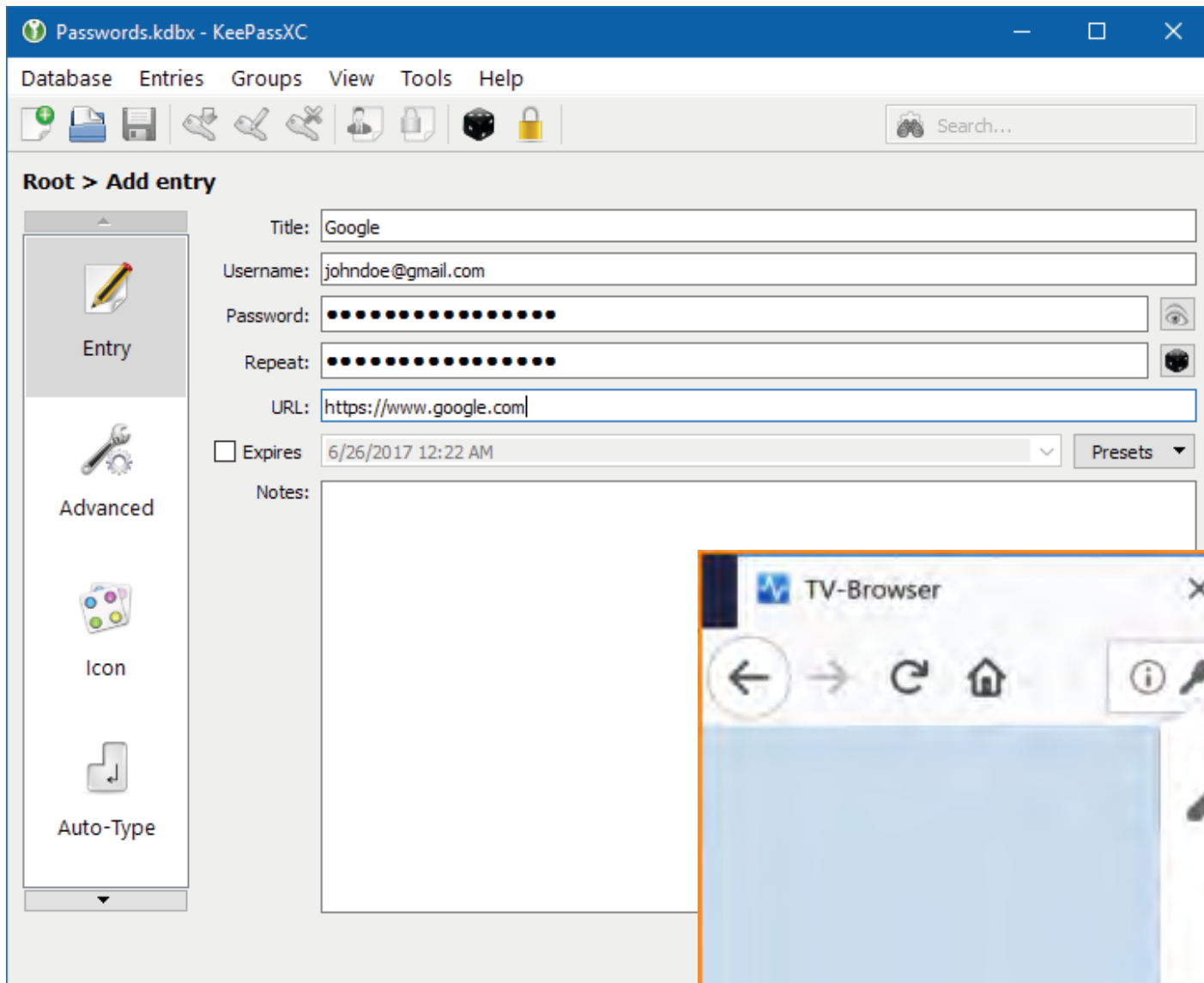
lbi=zEd4 4.304.672.100.000.000 Versuche

Leicht merkbare Passwörter?

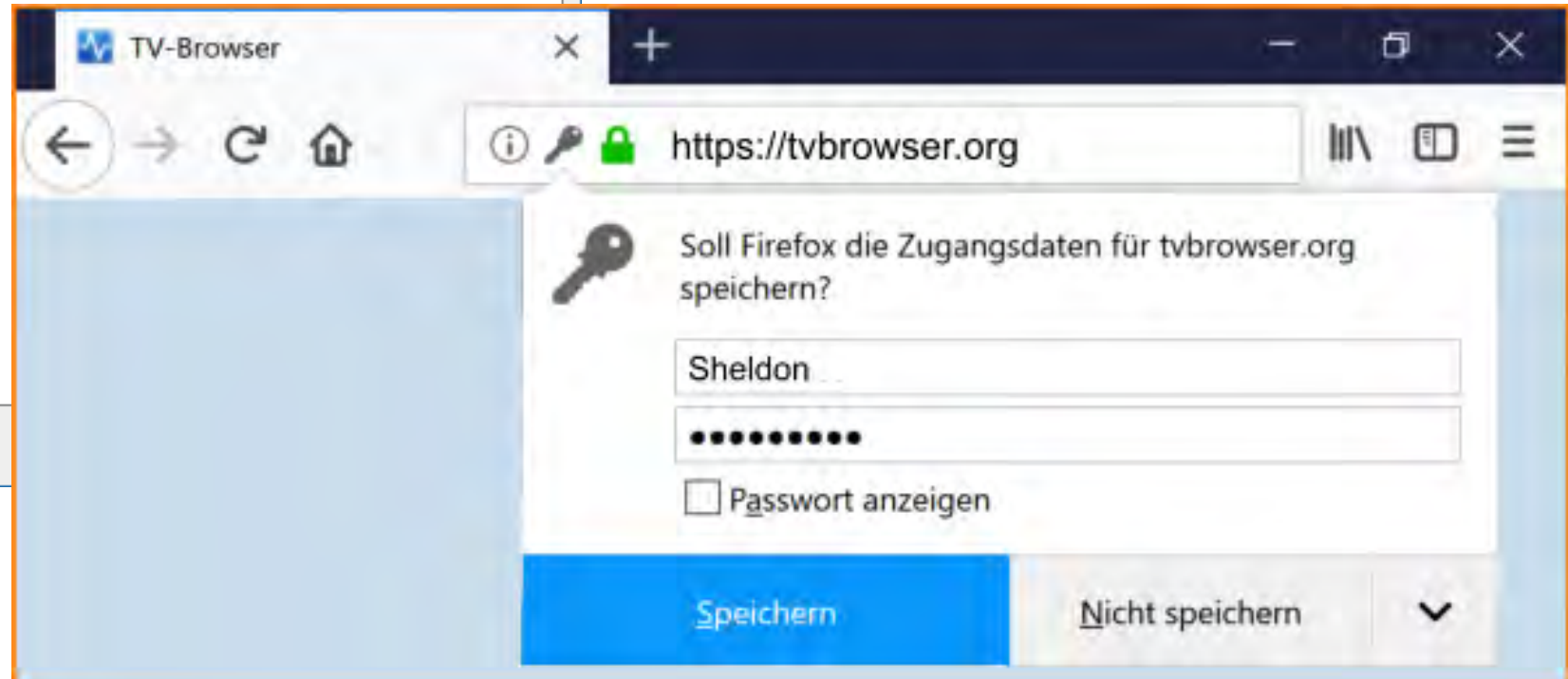
Reime

rubinose keine taschenlampe deine

werwasweisskriegteinschokoeis



Passwort- manager



Werden Sie nicht
übermütig!

Anwender mit Antiviren-
Software, Thunderbird und
Passwort-Manager häufiger
infiziert als andere!

DeKoven et al. Measuring Security Practices
and How They Impact Security, IMC 2019.



Werden Sie nicht übermütig!

Oder doch?

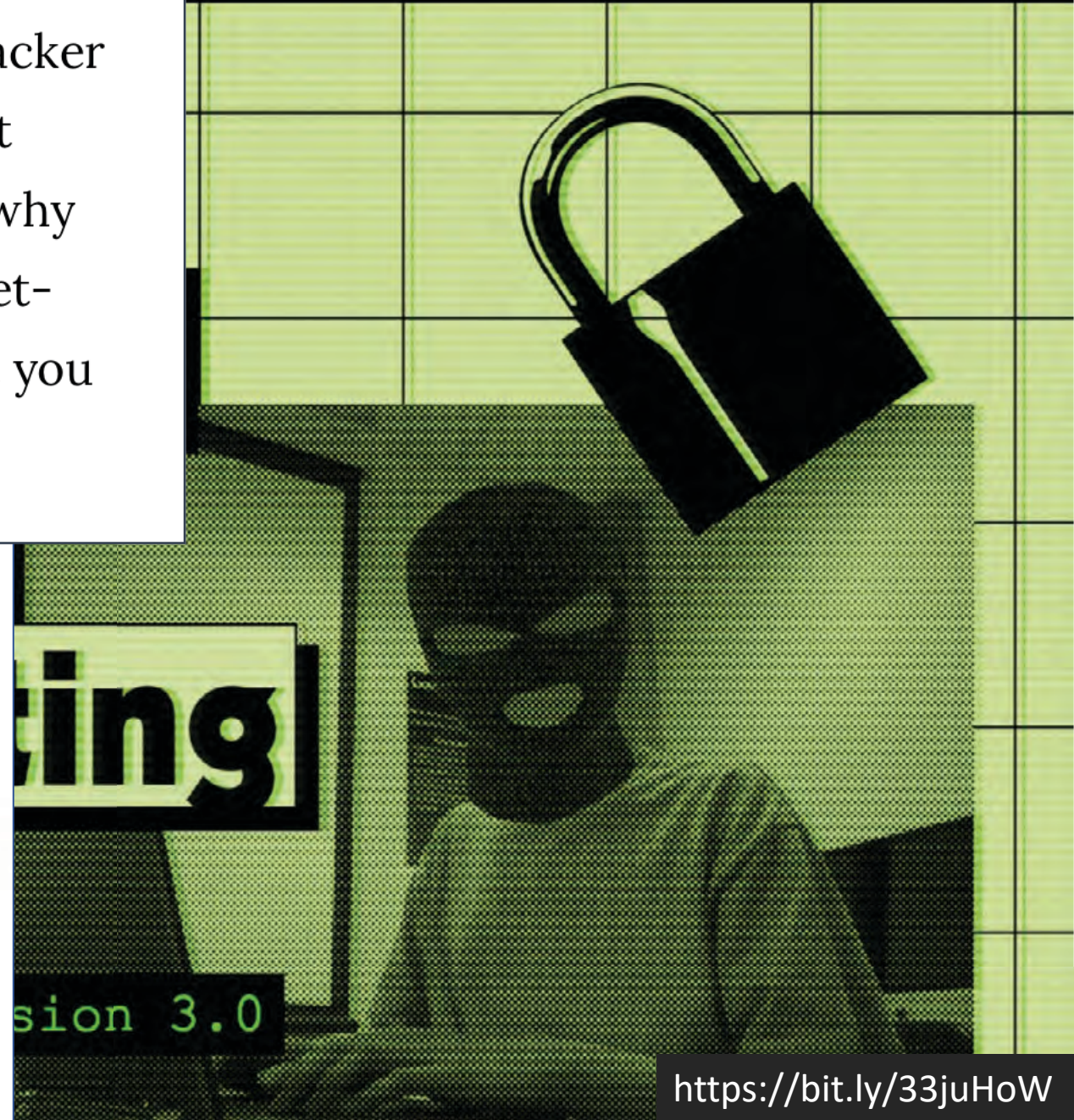
Mac-Anwender 4x seltener infiziert
als Windows-Anwender

Weitere Empfehlungen

Do use an adblocker...: Sometimes, all a hacker needs to pwn you is to get you to the right website—one laden with malware. That's why it's worth using a simple, install-and-forget-about-it **adblocker**, which should protect you from **malware embedded in advertising**

IF YOU CAN, GET AN iPhone

Pretty much everyone in the world of cybersecurity— **except perhaps the engineers working on Android**—believes that iPhones are the most secure cellphone you can get. There are a few reasons why, but the main







IT-SECURITY

Die Achillesferse
im Unternehmen

Prof. Dr.

Dominik Herrmann

Privacy and Security Group @ Uni Bamberg



@herdom

Folien: dhgo.to/achillesferse