

# Sensibilisierungsveranstaltung Informationssicherheit

Referent: Götz Sattler



## Götz Sattler

Studium der Informatik

Seit 1999 Trainer Anwendersoftware

Seit 2005 Improvisations- und Businesstheater L.U.S.T. Freiburg

Seit 2010 Trainer / Berater Informationssicherheit

Konzeption und Durchführung von Sensibilisierungsmaßnahmen

Ausbildung behördlicher Sicherheitsbeauftragter / Datenschützer (BAköV)

Lehraufträge an der DHBW Lörrach

## Motivation



## Informationssicherheit im LRA Waldshut



Alles wird leicht.

## Sicherheitsorganisation im LRA Waldshut

### Sicherheitsgremium

- ISB Herr Hajden



- Leitung Haupt- und Personalamt  
Frau Dorfmeister
- Personalrat Herr Weis
- Amt für Kreisschulen und  
Liegenschaften
- Datenschutzbeauftragte Frau Alt

### Sicherheitsteam

- Herr Fischer
- Herr Fox
- Frau Köhler

## Dokumente zum Thema

...finden Sie im INTRANET

- Dienstanweisung IT
- Dienstanweisung Internet
- Dienstvereinbarung Internet

DA-IT Landratsamt Waldshut

### Inhaltsverzeichnis:

<b>Vorwort und Sicherheitsleitlinie der Behördenleitung</b>	Seite 2
<b>I. Geltungsbereich</b>	Seite 7
<b>II. Organisation</b>	Seite 7
1. Zuständigkeiten	Seite 7
2. EDV-Abteilung beim Haupt- und Personalamt	Seite 12
3. Zusammenarbeit	Seite 12
4. Verfügbarkeit der vorgehaltenen Einrichtungen	Seite 13
<b>III. Betrieb von IT-Einrichtungen</b>	Seite 13
1. Dienstliche Nutzung der IT-Einrichtungen	Seite 13
2. Behandlung der IT-Einrichtungen	Seite 17
3. Einsatz von Software	Seite 17
4. Berechtigungsverwaltung Dialogverfahren KIVBF	Seite 18
5. Verzeichnisverzeichnis/ Softwarefreigabe/ Programmprüfung	Seite 19
6. Organisation Sicherheitsmanagement	Seite 22
7. Datenschutz	Seite 23
8. Meldung besonderer Vorkommnisse	Seite 24
9. Protokollierung	Seite 24
10. Dokumentation	Seite 24
<b>IV. Schlussbestimmungen</b>	Seite 26
1. Inkrafttreten/Rechtsgrundlage	Seite 26

## Aktuelle Meldungen im Intranet

LANDRATSAMT  
WALDSHUT

AKTUELLES   AKTIV & GESUND   PERSONALRAT   ARBEITSUMFELD   KARRIERE   **DA-Internet**

**Aktuelles**

Wichtige Hinweise zum Hard- und Softwarewechsel des zentralen Telefonsystems am 16.03.2022

Am zentralen Telefonsystem am Standort in der Kaiserstraße 110 (Rufnummer +497751 / 86-0) werden am Abend des 16.03.2022 neue Server in Betrieb genommen, welche die aktuelle Hard- und Software des Telekommunikationssystems ablösen werden.... [mehr..](#)

Begrüßung neuer Kolleginnen und Kollegen >

Schon gewusst? - wt-Super-Ticket >

Umgang mit „Reichsbürger“ oder „Selbstverwalter“ >

**IT Meldungen**

Wartungsarbeiten auf service-bw

Kommunikation mit der Justiz gestört [mehr..](#)

[weitere IT-Meldungen](#)

**Mitteilungen des Personalrats**

Das Personalratsinfo Februar 2022

Alternierende Telearbeit, mobiles Arbeiten, Umfrage unter dem Personalrat, JAV [mehr..](#)

Die JAV hat sich in ihrer Sitzung am >

**Mitarbeiterinformationen Corona**

Letzte Aktualisierung: 17.01.2022 - QR-Code für die Meldung eines Immunisierungsstatus

- > Update Corona-Regeln 06.07.2021
- > Maßnahmen- und Hygienekonzept
- > Corona-Schutzimpfung
- > Durchführung von Antigen-Schnelltests
- > Informationen und Anträge
- > Schutzverordnung

**Tipp: Suchfunktion nutzen**

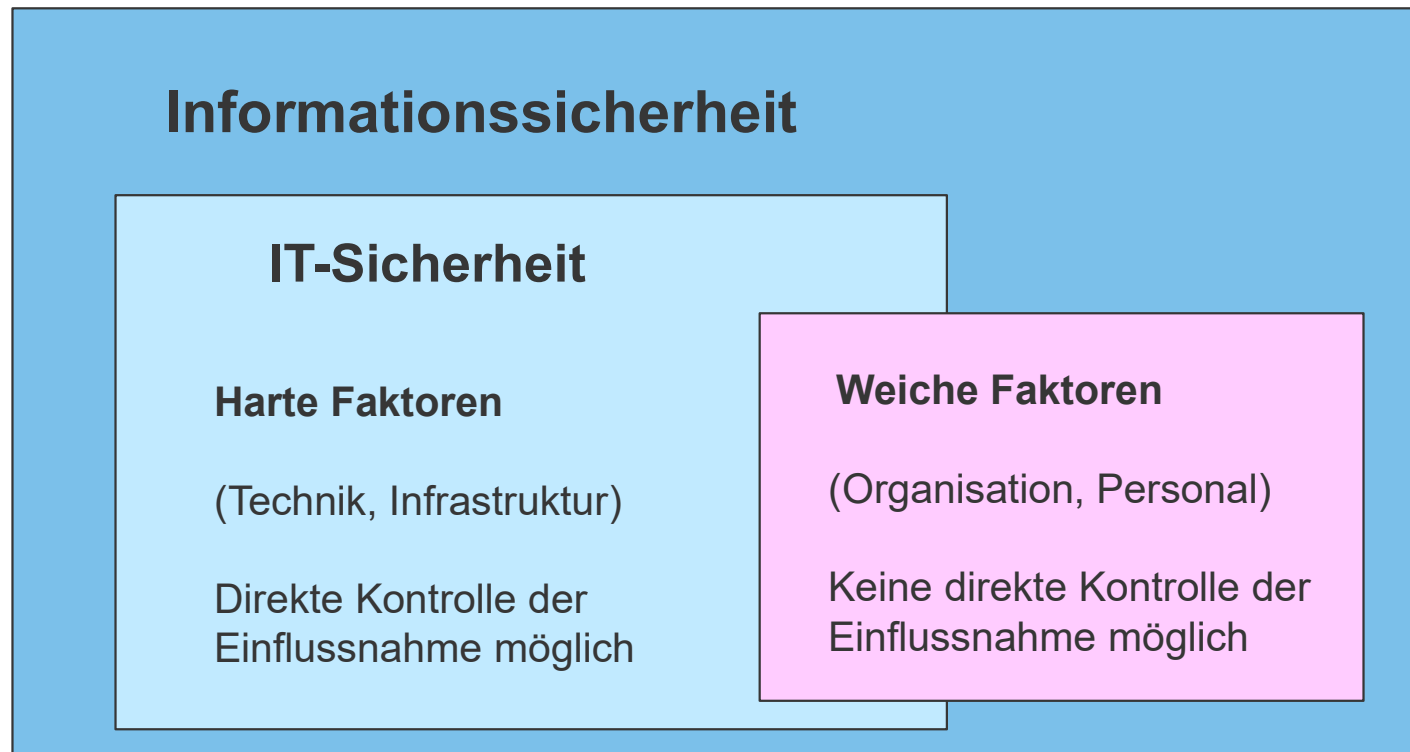
## Automatische Maßnahmen

Regelmäßige Sicherheitsupdates (Ivanti)

Regelmäßige Datensicherung um 7 und 12 Uhr täglich

Voraussetzung: Datei wurde benannt und gespeichert 😊

# Informationssicherheit / IT-Sicherheit



## Grundlagen

Was wollen wir schützen?

**Vertraulichkeit**

**Verfügbarkeit**

**Integrität**

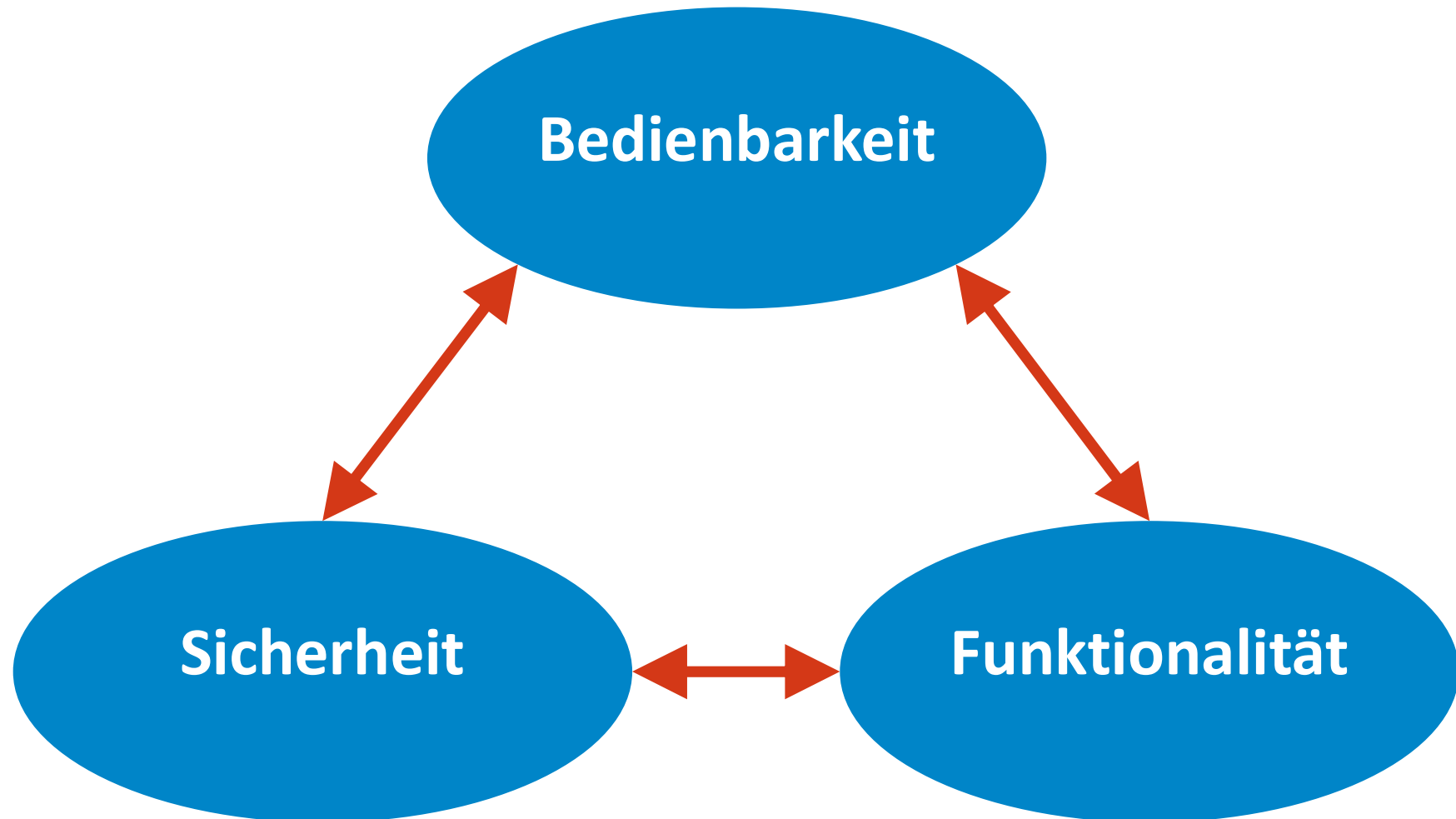
**Grundwerte der  
Informationssicherheit**

Welche Daten sind besonders schützenswert?

Welchen Daten verarbeiten Sie?

---

## Spannungsfeld Funktion / Bedienbarkeit / Sicherheit



## Die drei „Z“

### **ZUGRIFF** - auf Daten

- Rechte / Rollen
- Sensible Informationen aufräumen / wegschließen

### **ZUGANG** - zum System

- Rechner sperren
- herunterfahren

### **ZUTRITT** - „Physisch“

- Türen / Fenster schließen
- Besucher begleiten
- Besucher in sensiblen Bereichen beaufsichtigen

## Motivation / Bedrohungen



Alles wird leicht.

# Motivation / Bedrohungslage

## Bedrohungslage

Immer professionellere Internetkriminalität

Zunahme von Sicherheitslücken → Zero Day Angriffe

Download Attacken auch auf seriösen Webseiten

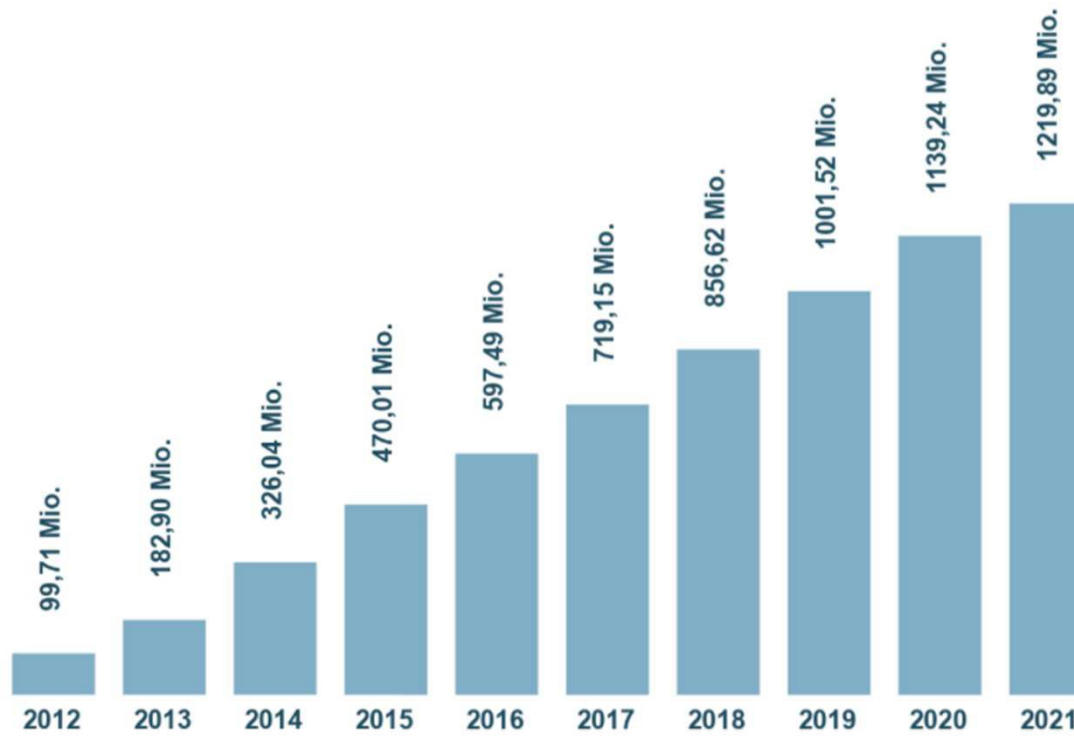
Schadprogramme werden immer komplexer

...oder immer einfacher einsetzbar → z.B. Turkojan

Umgang mit persönlichen Daten, z.B. in sozialen Netzwerken

Social Engineering

## Malware insgesamt



Quelle: AV-Test.org

## Motivation / Bedrohungslage

	<p align="center"><b>Bronze Edition</b></p> <ul style="list-style-type: none"> <li>This product is the improved version of Turkojan 3.0 and it has some limitations(Webcam - audio streaming and mic sniffer doesn't work for this version).</li> <li>1 month replacement warranty if it gets detected by any antivirus</li> <li>7/24 online support via e-mail</li> <li>Supports only Windows 95/98/ME/NT/2000/XP</li> <li>Realtime Screen viewing(controlling is disabled)</li> </ul> <p>Price : 99\$ (United State Dollar)</p>
	<p align="center"><b>Silver Edition</b></p> <ul style="list-style-type: none"> <li>4 months (maximum 3 times) replacement warranty if it gets detected by any antivirus</li> <li>7/24 online support via e-mail and instant messengers</li> <li>Supports 95/98/ME/NT/2000/XP/Vista</li> <li>Webcam streaming is available with this version</li> <li>Realtime Screen viewing(controlling is disabled)</li> <li>Notifies changemnts on clipboard and save them</li> </ul> <p>Price : 179\$ (United State Dollar)</p>
	<p align="center"><b>Gold Edition</b></p> <ul style="list-style-type: none"> <li>6 months (unlimited) or 9 months(maximum 3 times) replacement warranty if it gets detected by any antivirus (you can choose 6 months or 9 months)</li> <li>7/24 online support via e-mail and instant messengers</li> <li>Supports Windows 95/98/ME/NT/2000/XP/Vista</li> <li>Remote Shell (Managing with Mc-Dos Commands)</li> <li>Webcam - audio streaming and mic sniffer</li> <li>Controlling remote computer via keyboard and mouse</li> <li>Notifies changemnts on clipboard and save them</li> <li>Technical support after installing software</li> <li>Viewing pictures without any download(Thumbnail Viewer)</li> </ul> <p>Price : 249\$ (United State Dollar)</p>



**Aldi Bot Builder**

**Aldi Bot**

URL: http://

Intervall: 180

Mutex: [Masked]

Registry Name: MSN 2011

ActiveX: { [Masked] }

Drop Name: MSN\_2011

Firewall deaktivieren (XP + Vista)

Packen mit UPX

**Beenden** **Erstellen**

Stub wurde nicht gefunden!

## Grundsätze der Informationssicherheit

**Es gibt keine 100%ige Sicherheit**

**Sicherheit kann nie bewiesen werden, sondern nur Unsicherheit**

**Sicherheit – ein ständiger Prozess**

**Schutzmaßnahmen – eine Kosten-/Nutzenrechnung**

**Informationssicherheit wird beeinflusst durch  
Menschen, Prozesse und Technologie**

## Motivation / Bedrohungslage Ein Veteran: Captn Crunch



## aktuell



BSI  
@BSI\_Bund

Mit Bezug zu den Russland-Sanktionen sind nun auch betrügerische E-Mails im Namen von Banken im Umlauf. Die Kriminellen geben bspw. vor, dass man kontrollieren müsse, ob sich die Kundinnen und Kunden an Sanktionen halten. Dabei handelt es sich in jedem Fall um #Phishing-Versuche!



Sehr geehrter Sparkassen-Kunde,

---

Durch das aktuelle Vorgehen der russischen Regierung und den damit einhergehenden Sanktionen der Europäischen Union, sind alle Banken in der EU dazu verpflichtet sicherzustellen, dass alle ihre Kunden sich an die neuen Sanktionen halten.

Deswegen ist eine erneute Verifikation ihrer Daten notwendig.

Bei ausbleibender Identifikation bis zum 14.03.2022, sind wir nach EU Recht dazu verpflichtet, Ihr Konto zu schließen und Ihr Guthaben einzufrieren.

Nach erfolgreicher Verifizierung wird sich ein Kundenberater mit Ihnen in Verbindung setzen, um den Vorgang abzuschließen.

[Weiter zur Website](#)

Mit freundlichen Grüßen  
Ihr Service Team

## aktuell

heise online › News › 03/2022 › **Ukraine-Krieg: BSI warnt vor Kasperskys Sicherheits- und...**

# Ukraine-Krieg: BSI warnt vor Kasperskys Sicherheits- und Antiviren-Software

Wer Antiviren-Software des russischen Herstellers einsetzt, sollte auf alternative Produkte ausweichen, heißt es in der offiziellen BSI-Warnung.

## Motivation / Bedrohungslage

### Sicherheitsloch im Herzschrittmacher

 heise Security 11.01.2017 18:09 Uhr - Ronald Eikenberg

 vorlesen



Ein Firmware-Update soll Patienten mit Herzschrittmachern oder implantierten Defibrillatoren davor schützen, dass Hacker die Kontrolle über die Geräte übernehmen. Es gibt jedoch Zweifel daran, dass die Geräte nach dem Update sicher sind.

## Motivation / Bedrohungslage



[News](#) ▾ [Hintergrund](#) [Tools](#) [Foren](#)

### DDoS-Attacke legt Twitter, Netflix, Paypal, Spotify und andere Dienste lahm

21.10.2016 22:13 Uhr - Holger Bleich

 vorlesen



# „Internet of Things“ - Angriff der Kaffeemaschinen

NEWS

## University attacked by its own vending machines, smart light bulbs & 5,000 IoT devices

A university, attacked by its own malware-laced soda machines and other botnet-controlled IoT devices, was locked out of 5,000 systems.



### MORE LIKE THIS



IoT botnet bogs down college campus network



Data breaches through wearables put target squarely on IoT in 2017



Rise of the IoT machines



VIDEO  
Ransomware: What you need to know now | Salted Hash Ep 1, Pt 4

## Motivation / Bedrohungslage

### Süddeutsche Zeitung

28. März 2017, 17:00 Uhr Netz-Sicherheit

## Hackerangriff auf den Bundestag



## Motivation / Bedrohungslage

The screenshot shows the FlexiSPY website with the following content:

- Header: FLEXISPY
- Main headline: **Spy on Mobile Phones & Tablets**
- Sub-headline: FlexiSPY is the only mobile monitoring software that can spy on 9 instant messengers.
- Image: A hand holding a tablet displaying a monitoring interface.
- Left sidebar: **Catch Cheaters**
- Right sidebar: **Protect Children**
- Top right banner: Don't be an April Fool 5% off

**mSpy für Smartphones**

- ✓ Erhalten Sie Daten der GPS Ortung
- ✓ Sehen Sie IM Chats
- ✓ Checken Sie E-Mails im Vorbeigehen
- ✓ Sehen Sie Anrufe & Kontakte

**JETZT ZUSCHNAPPEN**

## Motivation / Bedrohungslage



# Motivation / Bedrohungslage

heise online > News > 04/2018 > Milliarden vertraulicher Dokumente frei im Netz auffindbar

## Milliarden vertraulicher Dokumente frei im Netz auffindbar

06.04.2018 11:23 Uhr - Fabian A. Scherschel

vorlesen



Viele Unternehmen sind unfreiwillig freizügig mit internen Daten. (Bild: Pixabay)

Falsch konfigurierte Web- und File-Server, Firewalls und S3 Buckets sorgen dafür, dass viele Firmen unbemerkt vertrauliche Daten öffentlich ins Netz laden.

Milliarden von internen Firmendokumenten sind ohne Zugriffsbeschränkungen im Netz von

## Internet / WWW



Alles wird leicht.

## Internet / WWW

Bin ich auf der richtigen Seite?

 www.paypal.de|

 <http://www.paypai.de/> — Aufrufen

 www.paypal.de

## Internet / WWW

Verlinkungen prüfen

Bookmarks

Verschlüsselte Verbindungen nutzen

Firewall nicht ausschalten bei Netzzugang

# Email



Alles wird leicht.

## E-Mail – hausgemachte Probleme

Wer bekommt die Email? Dürfen alle Empfänger die Emailadressen aller anderer Empfänger sehen? („CC“)



The screenshot shows an email composition interface. At the top, there are buttons for 'Senden', 'Rechtschreibprüfung', and 'Entwurf speichern'. The 'Von:' field contains 'Andrea A. [redacted]'. The 'An:' field contains '[redacted] Andrea' x'. The 'Bcc:' field contains '[redacted] Andrea' x' and is circled in red. Below the 'Bcc:' field is a 'Cc hinzufügen' button. The 'Betreff:' field contains 'Bccversenden'. At the bottom, there is an 'Anhang hinzufügen' button. On the right side, there are checkboxes for 'HTML-Modus' (unchecked) and 'Speichern in Gesendet' (checked), along with a 'Priorität: Normal' dropdown and a 'Weitere Funktionen' dropdown.

## E-Mail

**Wie wird die Email angezeigt?**

**Sind Grafiken und Formatierungen sichtbar?**

## E-Mail

**Anhänge** können Schadsoftware enthalten oder unerwünschtes Verhalten auf Ihrem Rechner auslösen

**Links in E-Mails** sind immer mit Vorsicht zu genießen.

Nur nutzen, wenn man sie angefordert hat,

z.B. bei

- Bestätigungsmails nach Anmeldung auf einer Website
- Zurücksetzen des Passwortes
- Downloadlink einer zuvor bestellten Software

...

## E-Mail - Beispiel Phishing

Hallo!

Wie Sie vielleicht bemerkt haben, habe ich Ihnen eine E-Mail von Ihrem Konto gesendet. Das bedeutet, dass ich vollen Zugriff auf Ihr Konto habe.

Ich beobachte dich jetzt seit ein paar Monaten.

Tatsache ist, dass Sie über eine von Ihnen besuchte Website für Erwachsene mit nkrat infiziert wurden.

Wenn Sie damit nicht vertraut sind, erkläre ich es Ihnen.

Nkrat gibt mir vollen Zugriff und Kontrolle über Ihr Gerät.

Das heißt, ich kann alles auf Ihrem Bildschirm sehen, Kamera und Mikrofon einschalten, aber Sie wissen nichts davon.

Ich habe auch Zugriff auf alle Ihre Kontakte und Ihre gesamte Korrespondenz.

Ich habe ein Video gemacht, das zeigt, wie Sie sich in der linken Hälfte des Bildschirms befriedigen, und in der rechten Hälfte sehen Sie das Video, das Sie sich angesehen haben.

Mit einem Mausklick kann ich dieses Video an alle Ihre E-Mails und Kontakte in sozialen Netzwerken senden.

Ich kann auch den Zugriff auf alle Ihre E-Mail-Korrespondenz und Messenger, die Sie verwenden, posten.

Wenn Sie dies verhindern möchten,

den Betrag von 1500 EUR an meine Bitcoin-Adresse überweisen (wenn Sie nicht wissen, wie das geht, schreiben Sie an Google: „Bitcoin kaufen“).

Meine Bitcoin-Adresse (BTC Wallet) lautet: 1F6ijAdtNhXdqy7HRsYK6Z6X88SwhWckd6

Nach Erhalt der Zahlung werde ich das Video löschen und Sie werden mich nie wieder hören. Ich gebe Ihnen 48 Stunden Zeit, um zu bezahlen.

Ich habe eine Benachrichtigung, die diesen Brief liest, und der Timer wird funktionieren, wenn Sie diesen Brief sehen.

Irgendwo eine Beschwerde einzureichen, macht keinen Sinn, da diese E-Mail nicht wie meine Bitcoin-Adresse verfolgt werden kann. Ich mache keine Fehler.

Wenn ich feststelle, dass Sie diese Nachricht mit jemand anderem geteilt haben, wird das Video sofort verbreitet.

Mit freundlichen Grüßen!

## E-Mail



Mo 16.01.2017 13:42

Sachbearbeiter Online Pay GmbH &lt;info@giropay.de&gt;

Konto-Lastschrift Nummer 95496349 konnte nicht durchgeführt werden 16.01.2017

An Götz Sattler

16.01.2017 Götz Sattler...  
366 KB

Sehr geehrte(r) Götz Sattler,

bedauerlicherweise mussten wir gerade feststellen, dass unsere Aufforderung NR. 954963496 bislang ohne Reaktion Ihrerseits blieb. Jetzt bieten wir Ihnen hiermit letztmalig die Chance, den nicht gedeckten Betrag unseren Mandanten Online Pay GmbH zu begleichen.

Aufgrund des bestehenden Zahlungsrückstands sind Sie verpflichtet zuzüglich, die durch unsere Beauftragung entstandene Kosten von 56,41 Euro zu bezahlen. Bei Fragen oder Anregungen erwarten wir eine Kontaktaufnahme innerhalb von 24 Stunden. Um zusätzliche Mahnkosten zu vermeiden, bitten wir Sie den ausstehenden Betrag auf unser Konto zu überweisen. Berücksichtigt wurden alle Buchungen bis zum 13.01.2017.

**Personalia:****Götz Sattler**Fe  
79

Tel. 07

**Korrekte Anschrift und Telefonnummer  
→ Zugeschnittener Angriff („Spear Phishing“)**

Wir erwarten die gesamte Überweisung bis spätestens 19.01.2017 auf unser Girokonto. Falls wir bis zum genannten Datum keine Zahlung bestätigen, sehen wir uns gezwungen Ihren Mahnbescheid an ein Gericht abzugeben. Sämtliche damit verbundenen Kosten gehen zu Ihrer Last.

**Eine vollständige Kostenaufstellung NR. 954963496, der Sie alle Buchungen entnehmen können, ist beigelegt.**

Mit freundlichen Grüßen

Sachbearbeiter Noah Carlstadt

## E-Mail

**Von:** PayPal [<mailto:service@paypal-deutschland.de>] 

**Gesendet:** Donnerstag, 19. Dezember 2013 04:14

**Betreff:** PayPal-Mitteilung

**Anhang:** Zugriffsversuche.pdf 

Guten Tag, 

leider haben wir in letzter Zeit Zugriffsversuche von Dritten auf Ihr Konto festgestellt. Zu Ihrer Sicherheit haben wir Ihr Konto vorerst eingeschränkt.

Wir bitten Sie, Ihre Identität unter folgendem Link zu bestätigen.

[PayPal - Verifikation](#) 

**ACHTUNG!** Sollten Sie Ihre Identität nicht zeitnah bestätigen, wird Ihr Konto samt möglichem Guthaben dauerhaft gesperrt!

Mit freundlichen Grüßen,

PayPal

# Mobile Datenträger



Alles wird leicht.

## mobile Datenträger

### Gefährdungen

Datenverlust oder -diebstahl

Infektion mit Schadprogrammen durch mobile Datenträger

## mobile Datenträger

Was sind denn mobile Datenträger?

USB-Sticks

Speicherkarten

Aber auch...

Digitalkameras

MP3-Player

Mobile Telefone

...etc

Alles, auf dem ich Daten transportieren kann!

→ **Also auch Papier!**

## Umgang mit Datenträgern

### **Sorgfältige Aufbewahrung und Entsorgung**

- Papierentsorgung über Papierkorb, alles wird geschreddert
- Sonderfall EU-Zahlstelle: wird vom Sachbearbeiter persönlich in die Box zur ordnungsgemäßen Vernichtung gebracht
- Entsorgung von Datenträgern:  
Datenträger, die nicht mehr gebraucht werden, an die Abteilung EDV zur Entsorgung schicken (keine Unterscheidung)
- USB-Sticks zurückgeben, wenn sie nicht gebraucht werden



# mobile Datenträger

**SPIEGEL ONLINE** DER SPIEGEL SPIEGEL TV 🔍 Anmelden

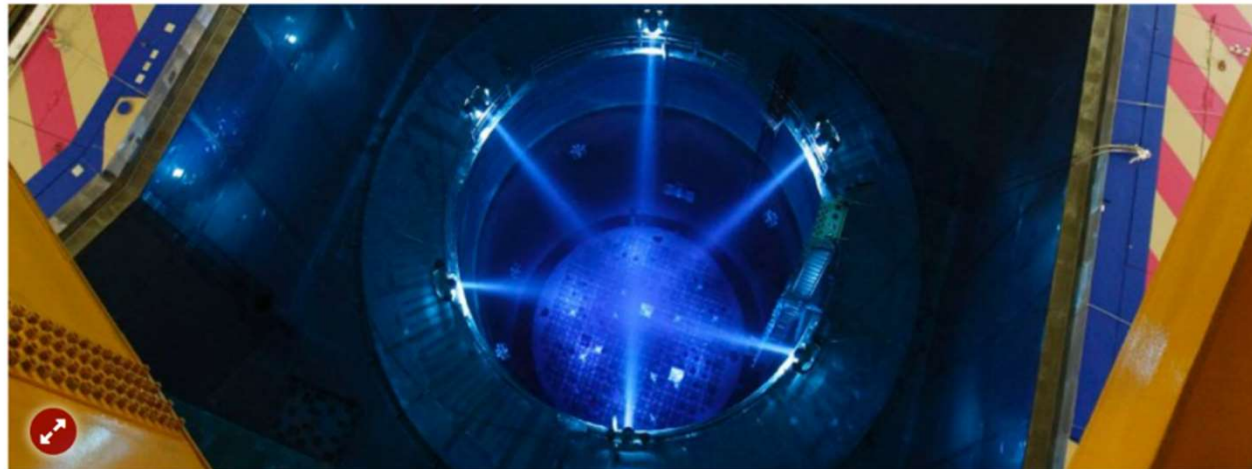
☰ NETZWELT Schlagzeilen | Wetter | DAX 12.409,36 | TV-Programm | Abo

Nachrichten > Netzwelt > Web > Computerviren > Gundremmingen: Virus im Atomkraftwerk kam über USB-Stick

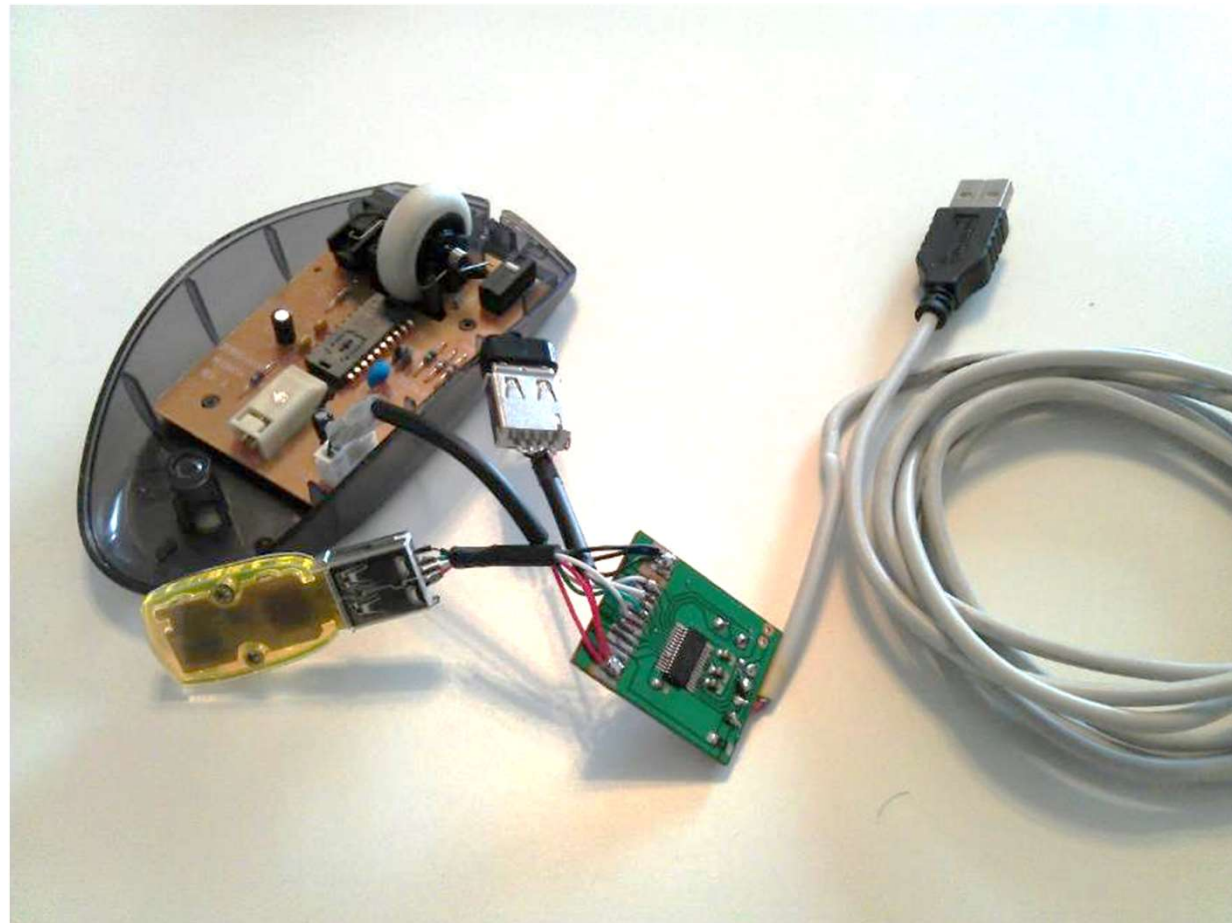
**Gundremmingen**

## **Virus im Atomkraftwerk kam über USB-Stick**

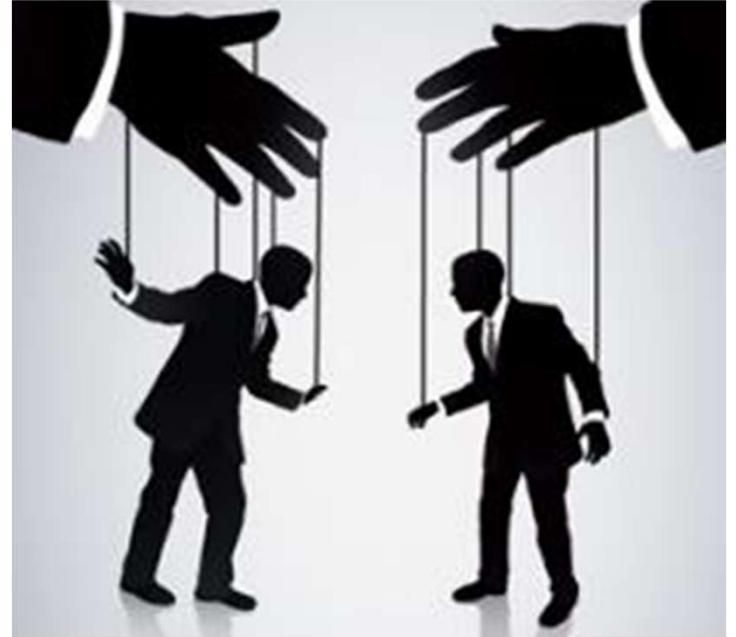
**Die Quelle ist ausgemacht: Die Schadsoftware, die im bayerischen Atomkraftwerk Gundremmingen entdeckt worden war, gelangte laut Innenministerium über einen USB-Stick auf das Computersystem.**



## Eine Maus, die es „in sich“ hat



## Social Engineering



Alles wird leicht.

## Social Engineering



## Social Engineering

**Foto-Panne bei Trumps Personalsuche**

**Ministerkandidat offenbart Anti-Terror-Pläne**



Der republikanische Hardliner Kris Kobach will Heimatschutzminister im Trump-Kabinett werden. Seine Strategie zur inneren Sicherheit hielt er nun

## Social Engineering



The screenshot shows the homepage of 'FAKE MY PHONE'. The header includes the logo 'FAKE MY PHONE' with a signal icon, and navigation links: 'Fake Anruf', 'Free', 'Kaufen', 'Features', 'Wie funktioniert's', and 'Login'. A German flag icon is in the top right. The main content area features the title 'Fake Telefon' and the text: 'Anrufe von einer gefälschten Nummer. Verbirg deine Telefonnummer, es ist einfach und funktioniert mit jedem Telefon!'. Below this are two buttons: 'Gratis Fake Anruf' (orange) and 'Los geht's' (teal). On the right, a cartoon character of a yellow smartphone wearing a brown trench coat and hat, holding a German flag, is shown.

# Social Engineering



## Goldeneye nutzt Informationen vom Arbeitsamt für äußerst gezielte Angriffe

07.12.2016 14:54 Uhr - Fabian A. Scherschel



(Bild: [Bundesagentur für Arbeit](#))

**Alles deutet darauf hin, dass die Angreifer hinter der sich rasant verbreitenden Ransomware Goldeneye Daten missbrauchen, die von der Bundesagentur für Arbeit stammen. Die Anschreiben sind so realistisch, dass sie eine handfeste Gefahr darstellen.**

Die Drahtzieher hinter dem Erpressungstrojaner [Goldeneye](#) schreiben gezielt Personalverantwortliche an und beziehen sich detailliert auf offene Stellenausschreibungen, um die Personaler dazu zu bringen, den Trojaner auszuführen. Die Kriminellen bedienen sich dabei an Daten, die vermutlich von der Bundesagentur für Arbeit stammen. Im Zuge der Recherchen von heise Security erreichten uns mehr als zweihundert Erfahrungsberichte von Betroffenen und mehrere Leser beteuern, dass die Erpresser in ihren Mails Daten und Mailadressen

## Social Engineering

### Sicherheitstipps

Seien Sie zurückhaltend mit Auskünften

Lassen Sie sich nicht unter Druck setzen

Trauen Sie sich ein Gespräch zu beenden

Überprüfen Sie die Identität eines Anrufers

Sichern Sie sich ab

## Social Engineering

### Sicherheitstipps (2)

Achten Sie auf sensible Dokumente

Seien Sie schweigsam in der Öffentlichkeit

Sprechen Sie fremde Personen an

Sicherheit geht vor Höflichkeit

Seien Sie auch in der Freizeit wählerisch mit den Gesprächsthemen

# Passwörter



Alles wird leicht.

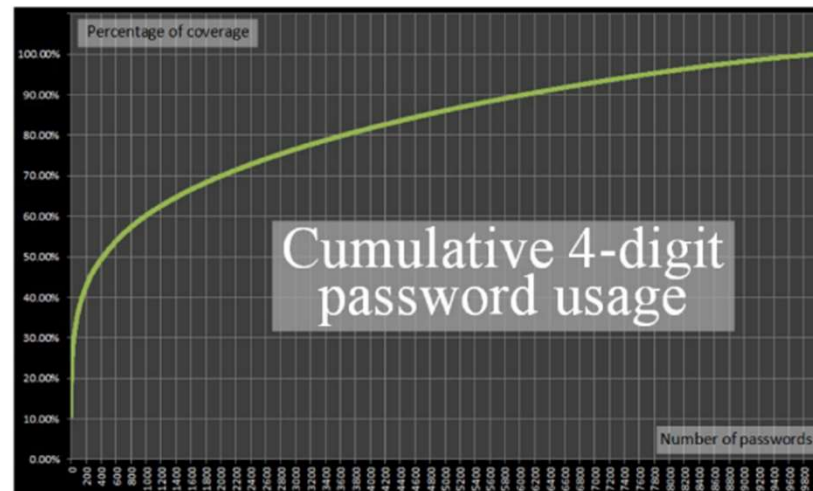
# Vorab: PINs

## häufigste

	PIN	Freq
#1	1234	10.713%
#2	1111	6.016%
#3	0000	1.881%
#4	1212	1.197%
#5	7777	0.745%
#6	1004	0.616%
#7	2000	0.613%
#8	4444	0.526%
#9	2222	0.516%
#10	6969	0.512%
#11	9999	0.451%
#12	3333	0.419%
#13	5555	0.395%
#14	6666	0.391%
#15	1122	0.366%
#16	1313	0.304%
#17	8888	0.303%
#18	4321	0.293%
#19	2001	0.290%
#20	1010	0.285%

## seltenste

	PIN	Freq
#9992	9480	0.001042%
#9993	6793	0.001012%
#9994	8398	0.000982%
#9995	0738	0.000982%
#9996	7637	0.000953%
#9997	6835	0.000953%
#9998	9629	0.000953%
#9999	8093	0.000893%
#10000	8068	0.000744%



Quelle: datagenetics.com

## Passwortsicherheit

### Vorgaben Passwort-Sicherheit LRA WT

Mind. 8 Zeichen

90 Tage Laufzeit

keine Nutzung der letzten 24 Passwörter

Zahlen, Groß- und Kleinbuchstaben, Sonderzeichen

Wahl und Bildung sicherer Passwörter

Verschiedene Passwörter für jedes System/Anwendung

## Passwortsicherheit

### Bewertungskriterien Passwort-Sicherheit

keine ABC- und Zahlenreihen

Kein Geburtsdatum / Kfz-Kennzeichen usw.

Keine privaten Passwörter dienstlich nutzen!

Passwörter verdeckt eingeben / unbeobachtet

Das Passwort darf nicht zu simpel sein

( §Passwort! / 1Passwort! / AaBb12345 )

Passwörter nicht an andere Mitarbeiter weitergeben

## Passwortsicherheit

### Warum so komplex?

„Brute Force“ – Angriffe erschweren

Bsp. Zahlenschloss

1 Ring	0 – 9	max. 10 Versuche
2 Ringe	00 – 99	max. 100 Versuche
3 Ringe	000 – 999	max. 1000 Versuche
4 Ringe	0000 – 9999	max. 10000 Versuche

d.h., jeder Ring zusätzlich macht das Schloss 10 mal besser

→ **Bei vollem Zeichenumfang über 80 Möglichkeiten / Stelle**

## Passwortsicherheit

Beispiel für ein gutes Passwort

19 Stellen, gut zu merken ;-)

**PL:2\*3m86,wwW&3m89e**

Kleiner Tipp:

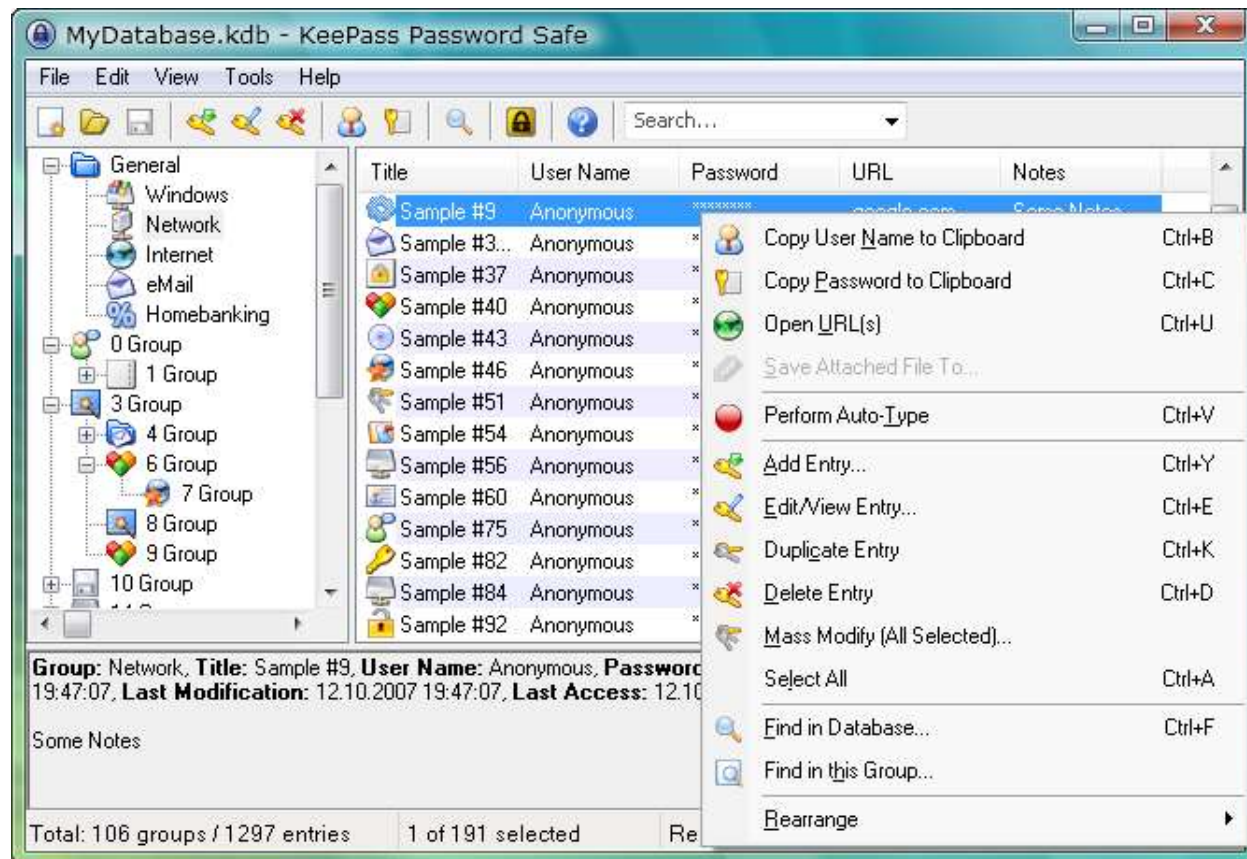


## Zeiten zum Knacken eines Passwortes

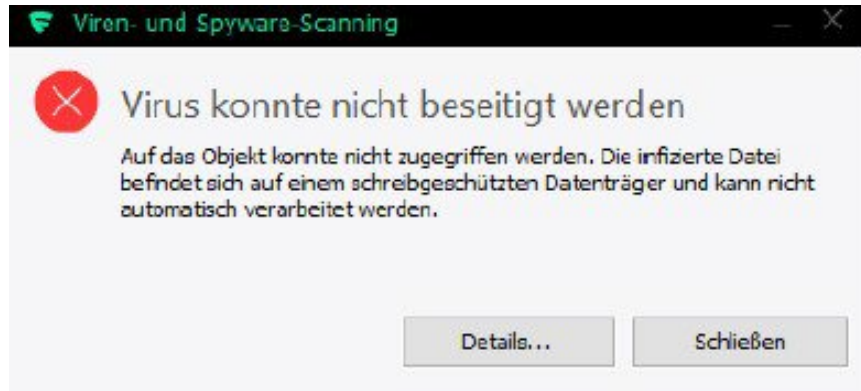
<b>Passwortlänge</b> <b>Alphabet: 84 Zeichen</b>	<b>t(max)</b> <b>9 Mrd. Hashes/s (NTLM)</b>
<b>4</b>	<b>5 ms</b>
<b>5</b>	<b>464 ms</b>
<b>6</b>	<b>39 sek.</b>
<b>7</b>	<b>54 min.</b>
<b>8</b>	<b>3 Tage</b>
<b>9</b>	<b>8 Monate</b>
<b>10</b>	<b>61 Jahre</b>
<b>11</b>	<b>5176 Jahre</b>
<b>12</b>	<b>0,4 Mio. Jahre</b>
<b>13</b>	<b>36 Mio. Jahre</b>
<b>14</b>	<b>3,1 Mrd. Jahre</b>

# Passwortsicherheit

## Passwortsafe, z.B. KeePass



## Was tun Bei Vorfall oder Verdachtsfall?



- Bei Virenmeldung: Nichts verändern!
- Meldung machen an: Telefon 11 11, notfalls auf Band sprechen
- Bei verdächtigen Angelegenheiten / Anrufen / Mails:  
[hotline@landkreis-waldshut.de](mailto:hotline@landkreis-waldshut.de)
- Fachamtsbetreuung

# Haben Sie Fragen?

## Weitere Informationsquellen

**Cyberfibel**

[www.cyberfibel.de](http://www.cyberfibel.de)

**Secupedia**

[www.secupedia.info](http://www.secupedia.info)

**Heise Security**

[www.heise.de/security](http://www.heise.de/security)

**Statistiken zu Malware**

[www.av-test.org/de/statistiken](http://www.av-test.org/de/statistiken)

## Tools – für den **PRIVATEN** Einsatz

**VeraCrypt (Verschlüsselung)**

<http://veracrypt.codeplex.com/>

**KeePass – Passwortverwaltung**

<http://keepass.info/>

**HTTPS Everywhere**

<http://www.heise.de/download/https-everywhere.html>

**Spoofmail (Einmal-Email-Adressen)**

<https://spoofoemail.de/>