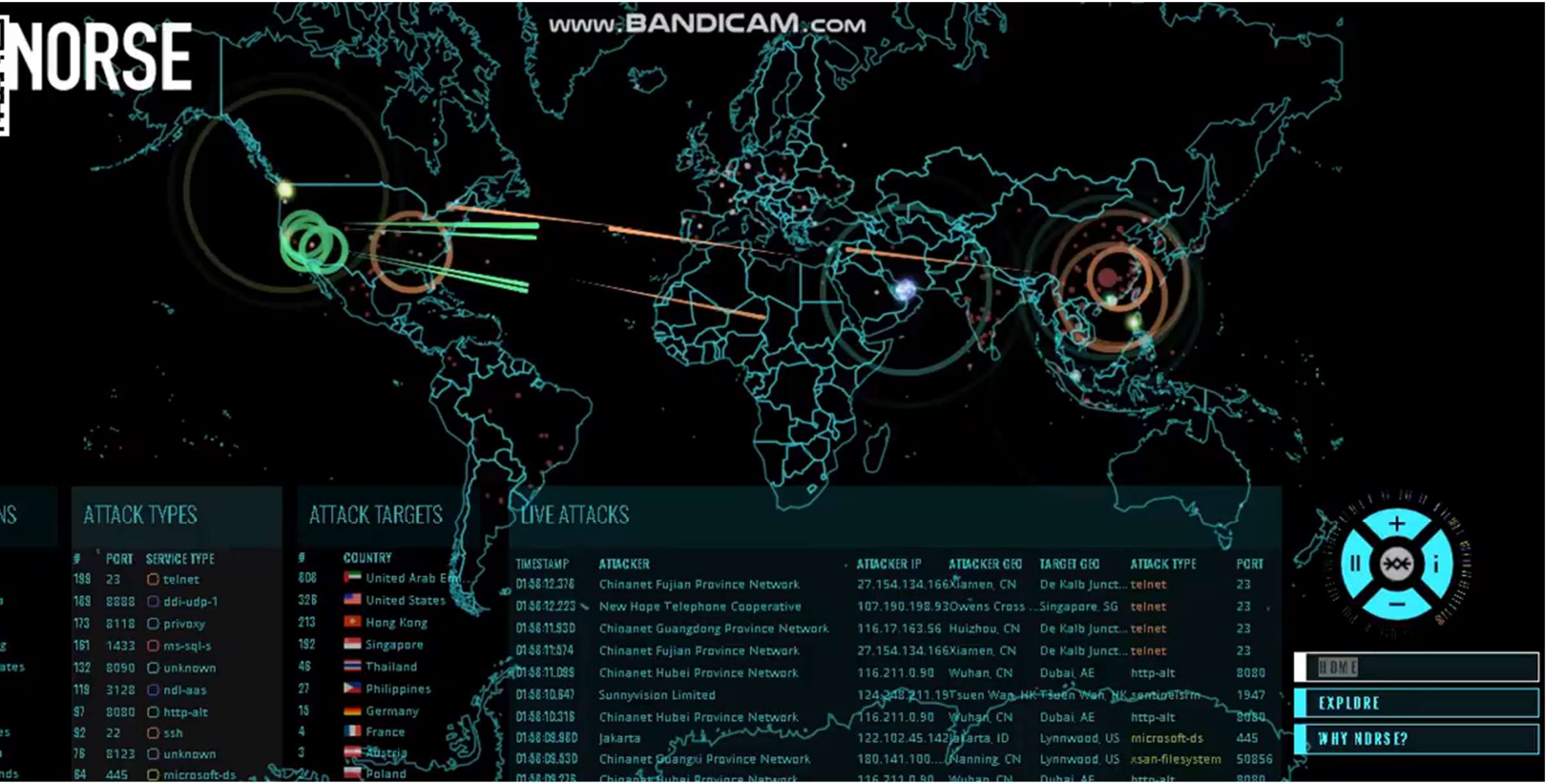
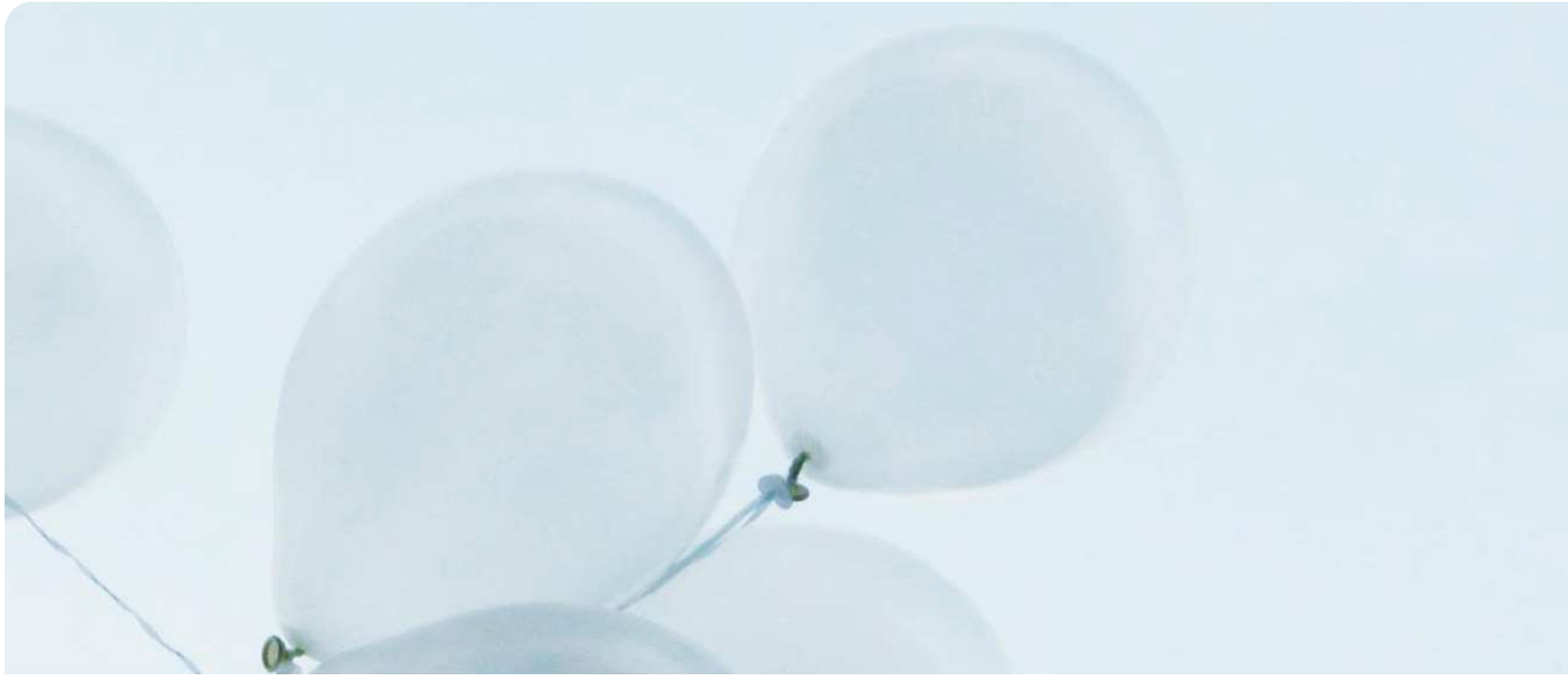

NORSE
www.BANDICAM.com
ATTACK TYPES
PORT SERVICE TYPE
199 23 telnet
169 8888 ddi-udp-1
173 8118 privoxy
161 1433 ms-sql-s
132 8090 unknown
119 3128 ndl-aas
97 8080 http-alt
92 22 ssh
78 8123 unknown
64 445 microsoft-ds
ATTACK TARGETS
COUNTRY
808 United Arab Em...
326 United States
213 Hong Kong
192 Singapore
46 Thailand
27 Philippines
15 Germany
4 France
3 Austria
Poland
LIVE ATTACKS
TIMESTAMP ATTACKER ATTACKER IP ATTACKER GEO TARGET GEO ATTACK TYPE PORT
01:58:12.378 Chinanet Fujian Province Network 27.154.134.166 Xiamen, CN De Kalb Junct... telnet 23
01:58:12.223 New Hope Telephone Cooperative 107.190.198.93 Owens Cross ... Singapore, SG telnet 23
01:58:11.930 Chinanet Guangdong Province Network 116.17.163.56 Huizhou, CN De Kalb Junct... telnet 23
01:58:11.574 Chinanet Fujian Province Network 27.154.134.166 Xiamen, CN De Kalb Junct... telnet 23
01:58:11.099 Chinanet Hubei Province Network 116.211.0.90 Wuhan, CN Dubai, AE http-alt 8080
01:58:10.647 Sunnyvision Limited 124.248.211.19 Tsuen Wan, HK Tsuen Wan, HK sentinelsrm 1947
01:58:10.316 Chinanet Hubei Province Network 116.211.0.90 Wuhan, CN Dubai, AE http-alt 8080
01:58:09.980 Jakarta 122.102.45.142 Jakarta, ID Lynnwood, US microsoft-ds 445
01:58:09.530 Chinanet Guangxi Province Network 180.141.100.... Nanning, CN Lynnwood, US xsan-filesystem 50856
EXPLORE
WHY NORSE?

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

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

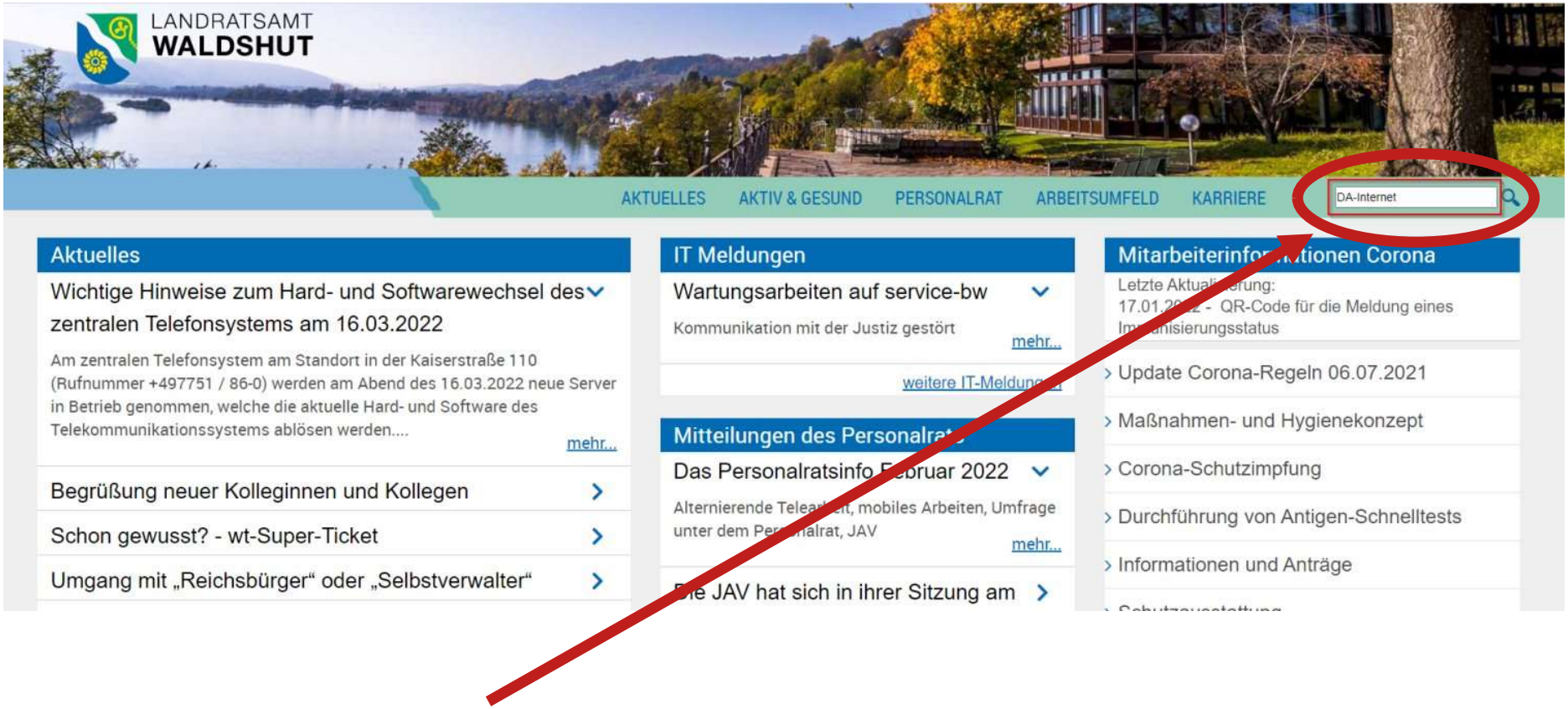
…finden Sie im INTRANET

- Dienstanweisung IT
- Dienstanweisung Internet
- Dienstvereinbarung Internet

DA-IT Landratsamt Waldshut

Inhaltsverzeichnis:

Aktuelle Meldungen im Intranet



Tipp: Suchfunktion nutzen

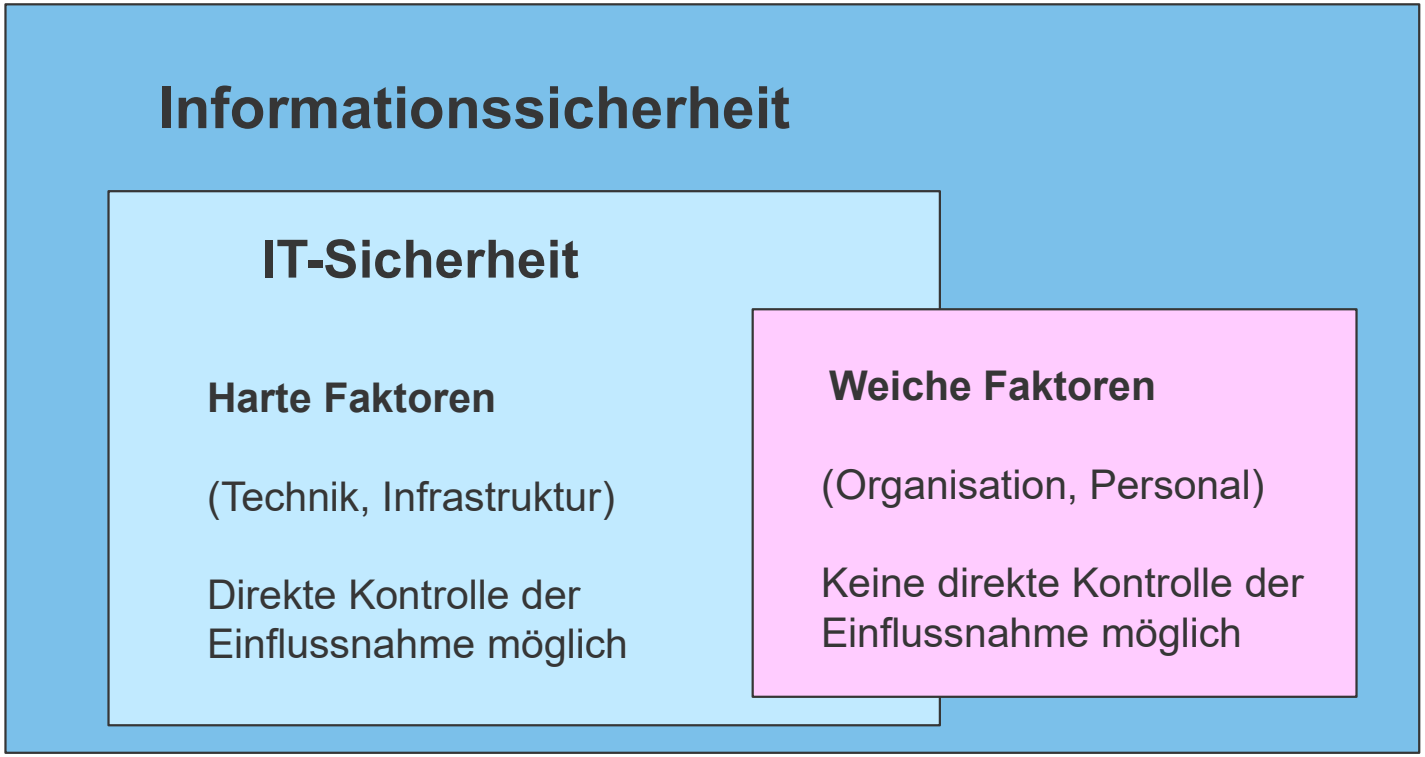
Automatische Maßnahmen

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

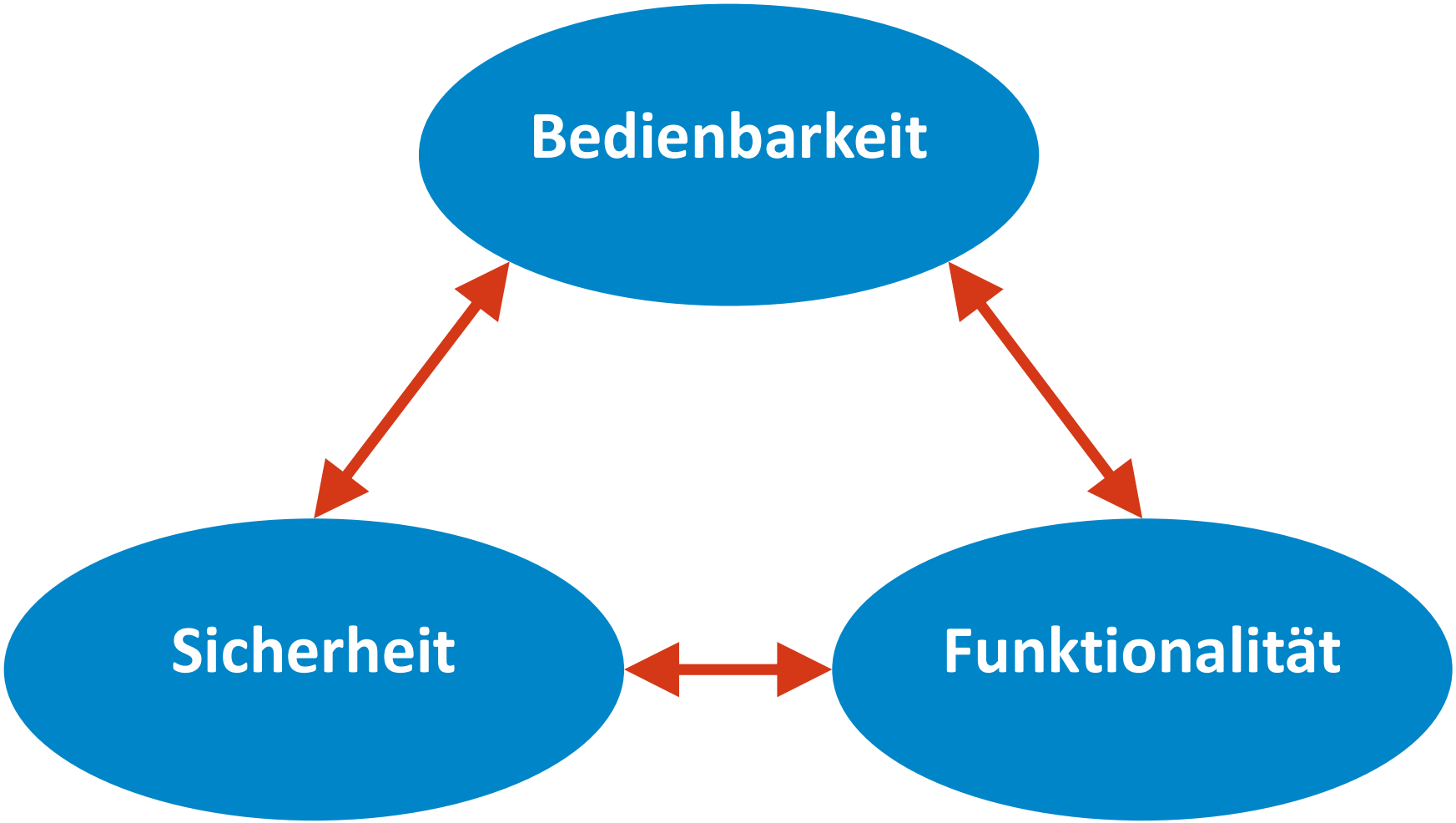
Integrität

Grundwerte der Informationssicherheit

Welche Daten sind besonderes 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

Motivation / Bedrohungslage

Bedrohungslage

Immer professionellere Internetkriminalität

Zunahme von Sicherheitslücken → Zero Day Angriffe

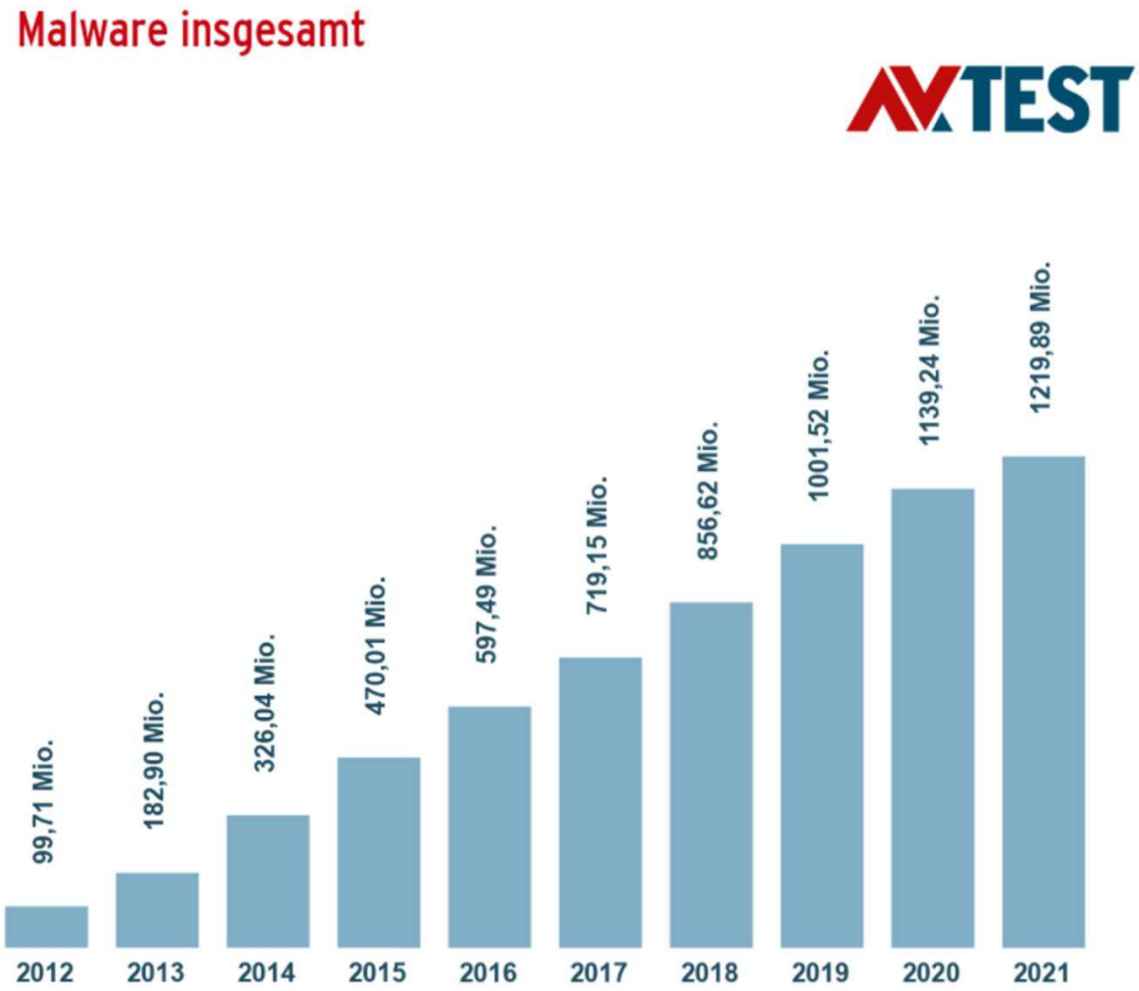
Download Attacken auch auf seriösen Webseiten

Schadprogramme werden immer komplexer

…oder immer einfacher einsetzbar → z.B. Turkojan

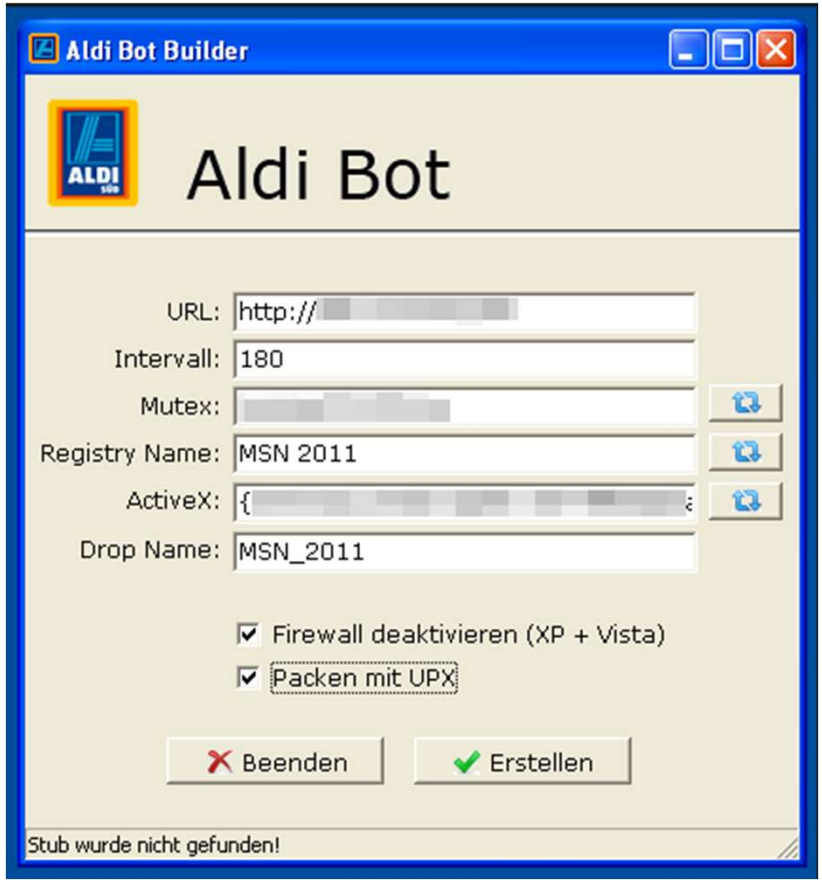
Umgang mit persönlichen Daten, z.B. in sozialen Netzwerken

Social Engineering



Quelle: AV-Test.org

Motivation / Bedrohungslage



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!

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

heise Security 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

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

Internet / WWW
Bin ich auf der richtigen Seite?

Internet / WWW

Verlinkungen prüfen

Bookmarks

Verschlüsselte Verbindungen nutzen

Firewall nicht ausschalten bei Netzzugang

Email

E-Mail – hausgemachte Probleme

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

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

…

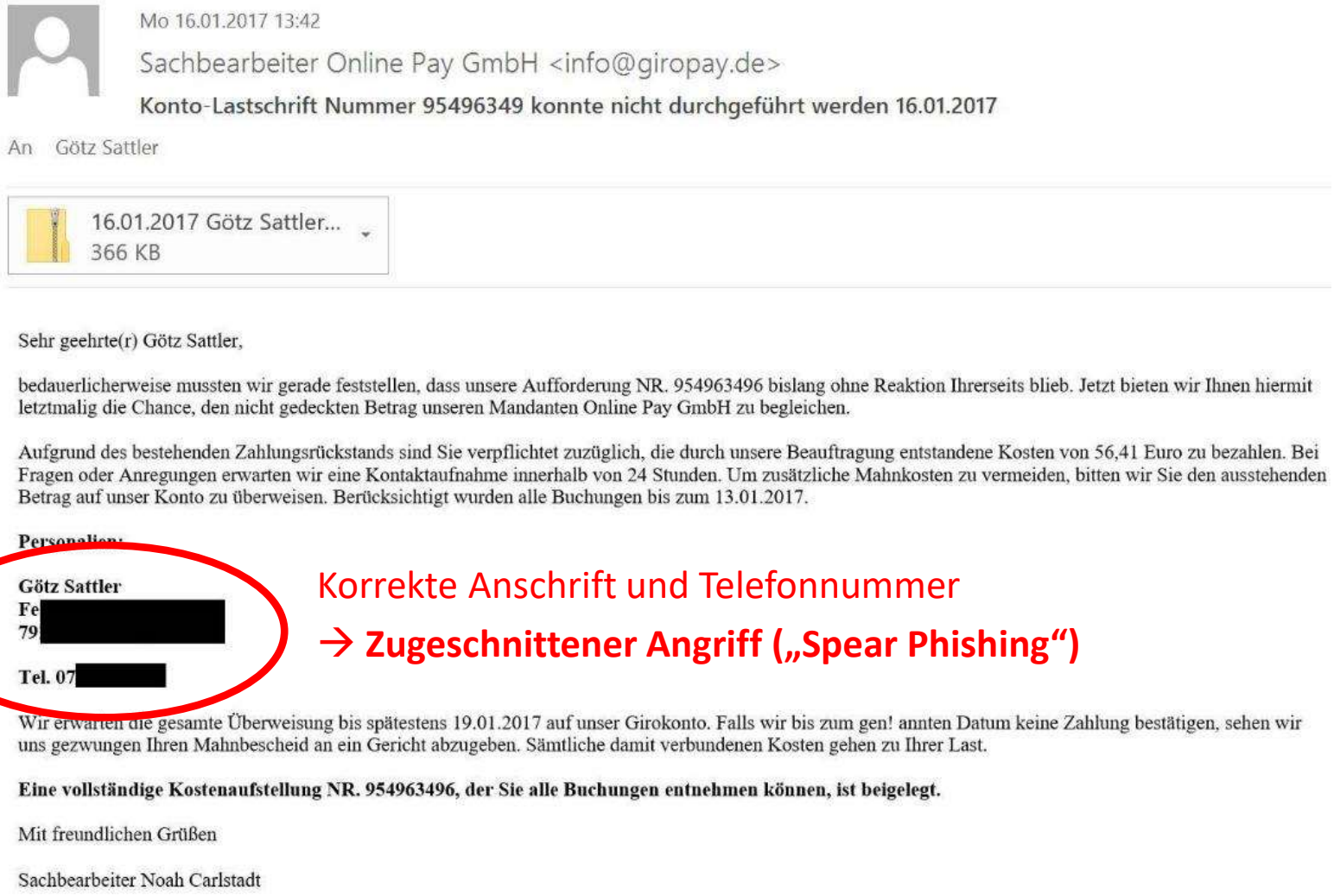
E-Mail - Beispiel Phishing

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 njrat infiziert wurden.
Wenn Sie damit nicht vertraut sind, erkläre ich es Ihnen.
Njrat 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 <info@giropay.de>

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.

Personalien:

Götz Sattler
Fe[redacted]
79[redacted]

Tel. 07[redacted]

Wir erwarten die gesamte Überweisung bis spätestens 19.01.2017 auf unser Girokonto. Falls wir bis zum gen! annten 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

Korrekte Anschrift und Telefonnummer

→ **Zugeschnittener Angriff („Spear Phishing“)**

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

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


Final Exam
Solutions
Confidential

mobile Datenträger

SPIEGEL ONLINE DER SPIEGEL SPIEGEL TV Anmelden

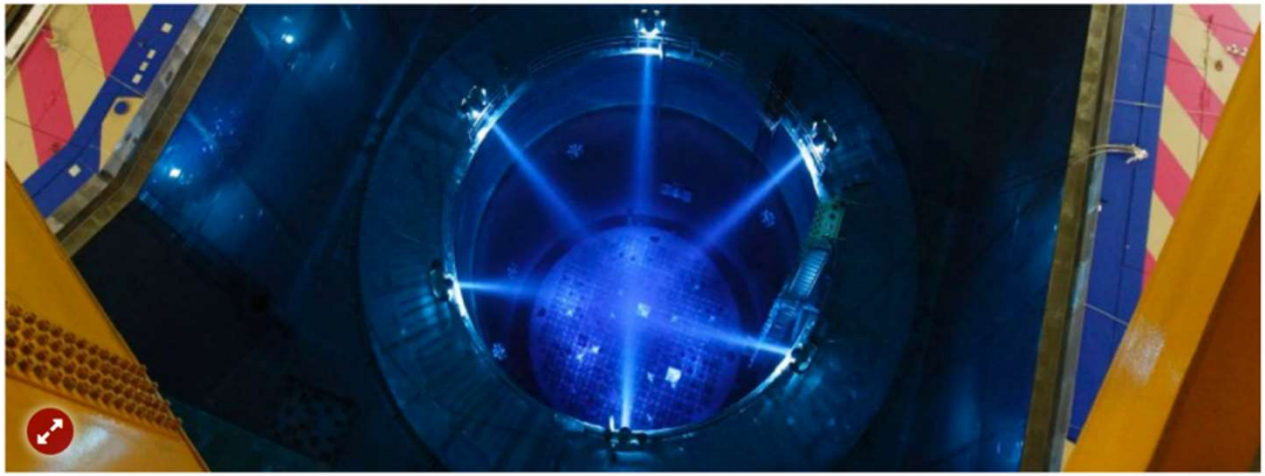
NETZWELT Schlagzeilen | Wetter | DAX 12.409,36 | TV-Programm | Abo

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

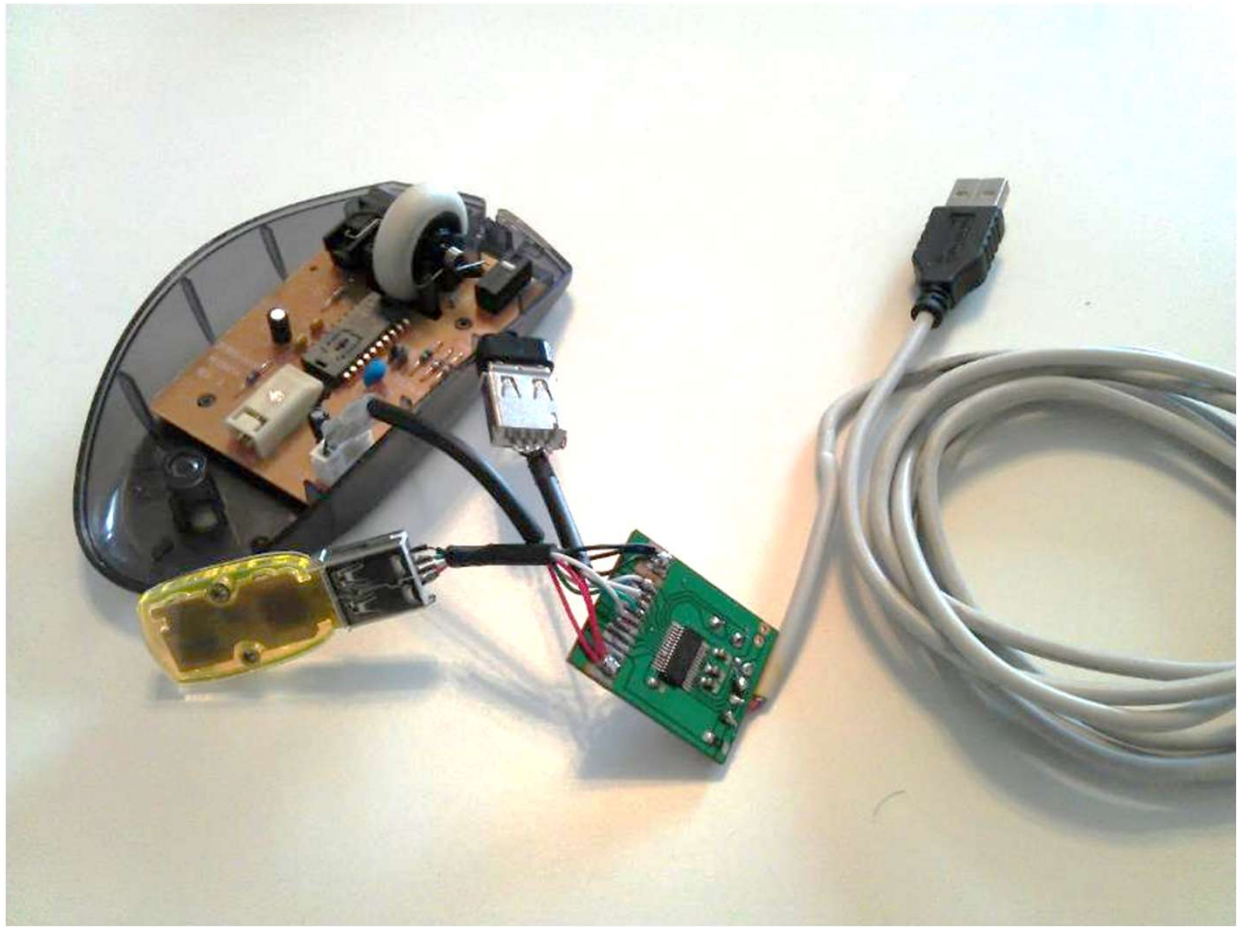
Gundremmingen

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

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

Social Engineering

heise Security

Goldeneye nutzt Informationen vom Arbeitsamt für äußerst gezielte Angriffe

07.12.2016 14:54 Uhr – Fabian A. Scherschel vorles

(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

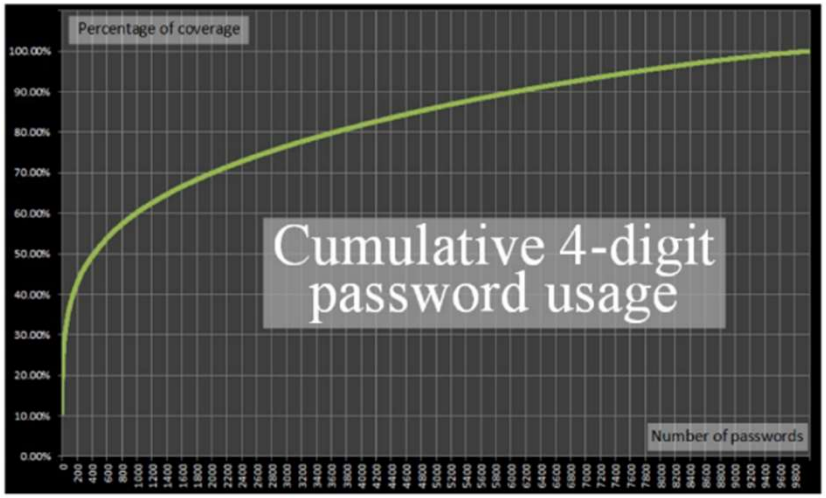
Vorab: PINs

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 ;-)

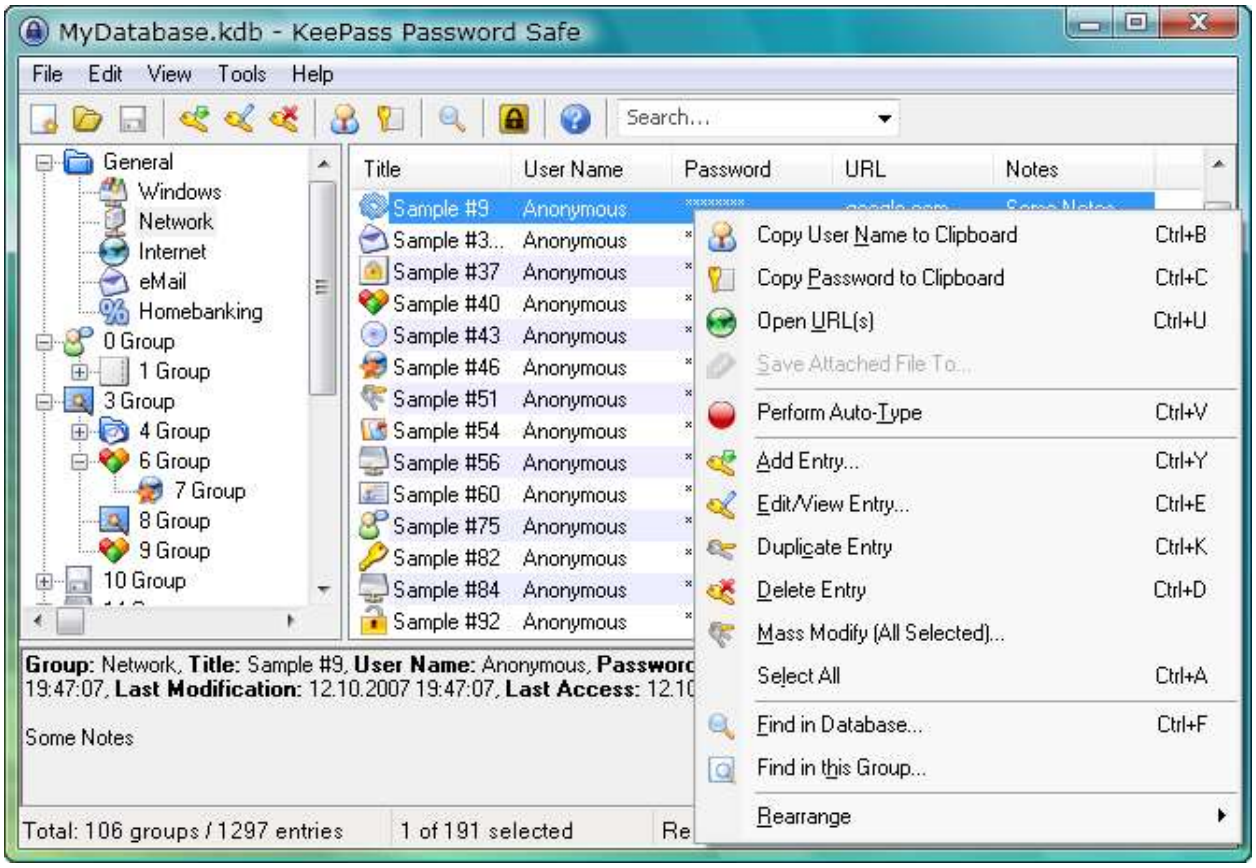
PL:2*3m86,wwW&3m89e

Kleiner Tipp:

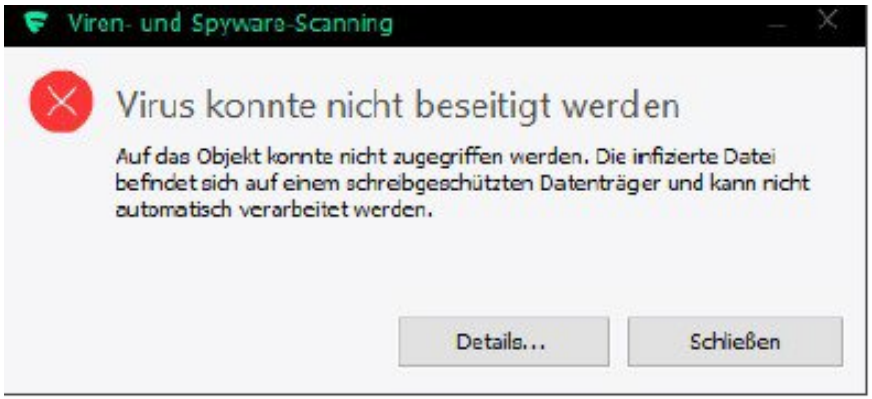
Zeiten zum Knacken eines Passwortes

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

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
- Fachamtsbetreuung

Haben Sie Fragen?

Weitere Informationsquellen

Cyberfibel	www.cyberfibel.de
Secupedia	www.secupedia.info
Heise Security	www.heise.de/security
Statistiken zu Malware	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://spoofmail.de/