

Tobias Scheible, M.Eng.

Cyber Security Vortrag

Internetkriminalität / Cybercrime

- 2009 bis 2012: Softwareingenieur im Bereich Web Development
- Seit 2012: Wissenschaftlicher Mitarbeiter an der Hochschule Albstadt-Sigmaringen
 - Forschungsprojekt SEKT (IT Security & Smart Textiles)
 - Aktuelle & ehemalige Lehrmodule (Auswahl):
 - Grundlagen der digitalen Forensik Masterstudiengang IT GRC Management
 - Digitale Forensik Bachelorstudiengang IT Security
 - Internet Grundlagen Masterstudiengang Digitale Forensik
 - Betriebssystemforensik Masterstudiengang Digitale Forensik
 - IT Security 2 Bachelorstudiengang IT Security
 - Informationssicherheit Bachelorstudiengang Wirtschaftsinformatik
 - Internettechnologien Hochschulzertifikatsprogramm
 - Cloud Technologies and Cloud Security Architectures Masterstudiengang IT GRC

Agenda

■ Cybercrime

■ Gestern

- Pin-Code Beispiel
- Geschichte der Schadsoftware
- Ransomware
- Versteckte Kommunikation

■ Heute

- Cybercrime as a Service
- Passwortsicherheit
- Faktor Mensch
- Fallbeispiel Locky

■ Morgen

- Hacking Hardware
- Internet of Things
- Spionage
- Künstliche Intelligenz



Cyber Crime - Gestern

00000000



Gestern

Pin-Code Beispiel

Schadsoftware

Ransomware

Versteckte Kommunikation

Heute

Morgen

00000000

Launch-Code für die in den USA stationierten Atomraketen

(1962 bis 1977)

Gestern

- Pin-Code Beispiel
- Schadsoftware
- Ransomware
- Versteckte Kommunikation

Heute

Morgen

Pin Code Beispiel - Steuerungstechnik

Cyber Security Vortrag
Internetkriminalität / Cybercrime



Quelle: zeit.de (2)

Gestern

Pin-Code Beispiel
Schadsoftware
Ransomware
Versteckte Kommunikation

Heute

Morgen

20.11.2019 | NKM Noell

Tobias Scheible, M.Eng.

Geschichte der Schadsoftware

■ Nutzung von Standardfunktionen

- 80er Jahre: Der Begriff Computervirus wird zum ersten Mal verwendet
- 1985: Über Computerviren wird in Deutschland berichtet
- 1988: Zum ersten Mal wird das Konzept „Würmer“ bekannt

Gestern

Pin-Code Beispiel
Schadsoftware
Ransomware
Versteckte Kommunikation

Heute

Morgen

11.2019 Gefährliche Standardfunktion

Kontakt | Best of Swiss Web | Best of Swiss Apps | E-Paper | Abo | Shop | Mediadaten

netzwoche

NEWS STORYS DOSSIERS VIDEO SPECIALS EVENTS NETZWITZIG PARTNERZONE

NEWS

Malware per NFC

Android Beam hat gefährliche Sicherheitslücke – so schützt man sich

Di 05.11.2019 - 10:22 Uhr
von avr, Watson

Mit Android Beam können Handy-Nutzer bequem Daten auf andere Geräte laden. Doch das Programm kommt mit einer gefährlichen Sicherheitslücke.

Quelle: [netzwoche.ch](https://www.netzwoche.ch) (4)

PARTNER

watson

ZUM THEMA

"Calls" von Microsoft

Geschichte der Schadsoftware

■ Nutzung von Standardfunktionen

- 80er Jahre: Der Begriff Computervirus wird zum ersten Mal verwendet
- 1985: Über Computerviren wird in Deutschland berichtet
- 1988: Zum ersten Mal wird das Konzept „Würmer“ bekannt

■ Ausnutzung von Schwachstellen

- 1997: Schadsoftware nutzt nun gezielt Schwachstellen aus
- 2000: „I love you“ Virus findet in Deutschland große Verbreitung
- 2000: Erster Trojaner für mobile Endgeräte (PDAs)

■ Krimineller Hintergrund

- 2004: Schadsoftware wird von organisierten Kriminellen eingesetzt
- 2005: „Wurm“ verbreitet sich automatisch auf Symbian Smartphones per MMS

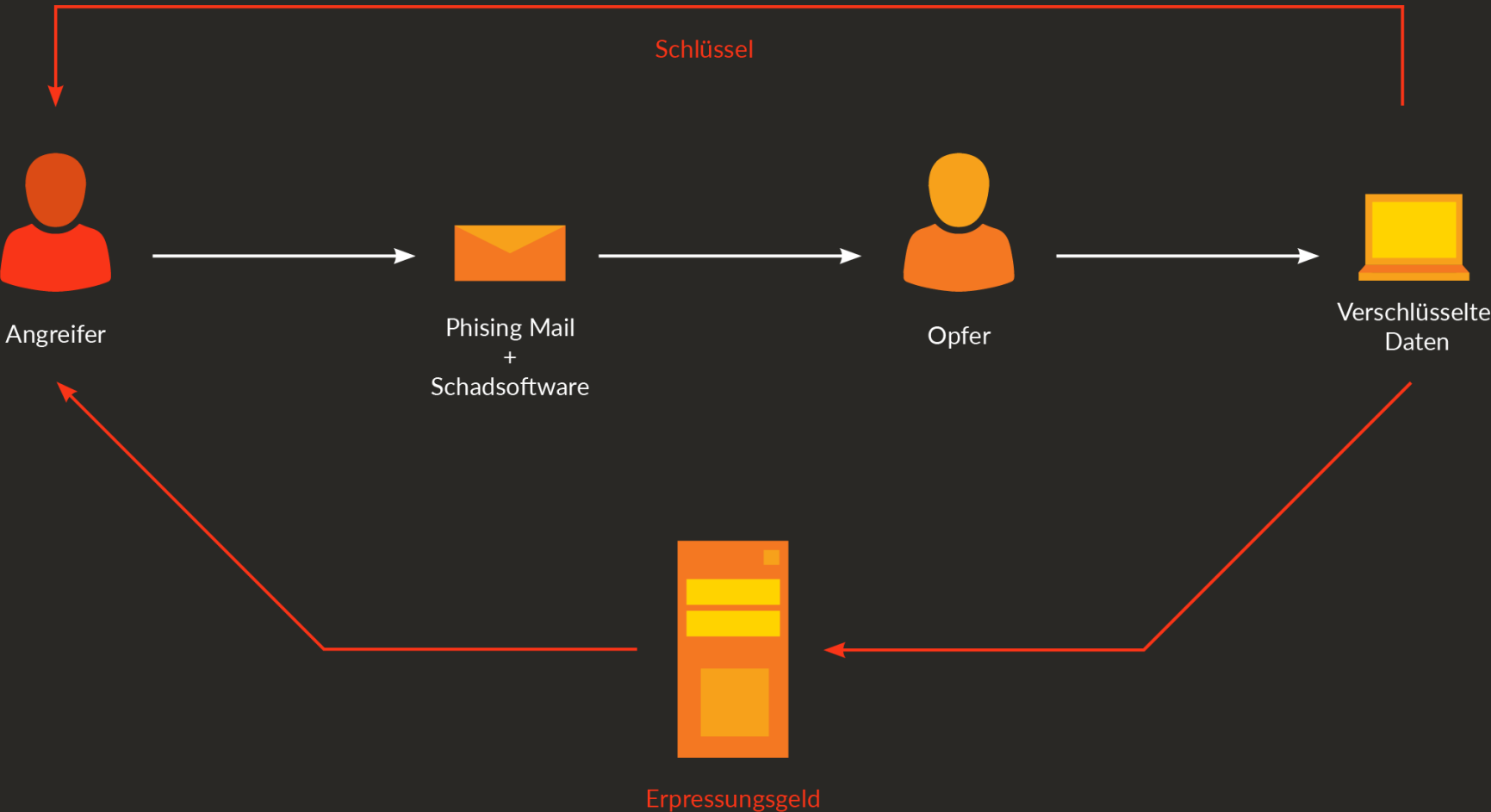
Gestern

Pin-Code Beispiel
Schadsoftware
Ransomware
Versteckte Kommunikation

Heute

Morgen

Ransomware



Gestern

- Pin-Code Beispiel
- Schadsoftware
- Ransomware
- Versteckte Kommunikation

Heute

Morgen

Ransomware - AIDS

- Erste Angriffe mit Ransomware bereits 1989
- Schadsoftware wurde per 5,25“ Diskette mit der Post verschickt
- Nach 90 Starts wurden die Dateien verschlüsselt
 - Eine italienische AIDS Organisation verlor Forschungsergebnisse aus 10 Jahren
 - Ersteller der Ransomware wurde 1990 verhaftet

```
Dear Customer:

It is time to pay for your software lease from PC Cyborg Corporation.
Complete the INVOICE and attach payment for the lease option of your choice.
If you don't use the printed INVOICE, then be sure to refer to the important
reference numbers below in all correspondence. In return you will receive:

- a renewal software package with easy-to-follow, complete instructions;
- an automatic, self-installing diskette that anyone can apply in minutes.

Important reference numbers: A5599796-2695577-

The price of 365 user applications is US$189. The price of a lease for the
lifetime of your hard disk is US$378. You must enclose a bankers draft,
cashier's check or international money order payable to PC CYBORG CORPORATION
for the full amount of $189 or $378 with your order. Include your name,
company, address, city, state, country, zip or postal code. Mail your order
to PC Cyborg Corporation, P.O. Box 87-17-44, Panama 7, Panama.

Press ENTER to continue
```

Quelle: [wikipedia.org](https://de.wikipedia.org/wiki/AIDS_(Ransomware)) (5)

Gestern

Pin-Code Beispiel
Schadsoftware
Ransomware
Versteckte Kommunikation

Heute

Morgen

LIVE Versteckte Kommunikation

The screenshot shows the website 'ledermode.tv' with a navigation bar at the top containing 'Startseite', 'Warenkorb', 'Login', and 'Kontakt'. A search bar is also present. The main content area is divided into several sections:

- Kategorien:** Startseite (10), Ledermode (10), Trachtenmode (5), Motorradbekleidung (41), Accessoires (3), Kontakt.
- Kundeninfos:** Habe ich Rückgaberecht?, Ist Umtausch möglich?, Was kostet der Versand?, Wie kann ich bezahlen?, Wie lange ist die Lieferzeit?
- Impressum:** WebApp.net, Max Muster, Hauptstrasse 123, 12345 Berlin, Tel: 0177-123456.
- Horzlich Willkommen:** Ledermode.TV steht zum Verkauf! Bei Ledermode.TV finden Sie ein ausgewähltes Sortiment hochwertiger Ledermode, Motorradbekleidung und Trachtenmode. Wir führen Ledermode für Damen und Herren, Lederjacks, Lederhosen und Lederjacken, Reithosen, sowie Lederbekleidung für Beruf und Freizeit. Unsere Artikel sind aus ausschliesslich aus hochwertigem Leder, schonend gegerbt und in bester Qualität.
Achtung: Dies ist ein DEMO-SHOP! Bestellungen werden derzeit nicht angenommen.
- Warenkorb:** Keine Artikel im Warenkorb.
- Kundenlogin:** Login fields for 'Istname' and 'Passwort', with 'einloggen' and 'neue anmeldung' buttons.
- Suchbegriffe:** Lederhose, Zimmerriderslederhose, Doppel-Zip Lederjacke, Glazed Used-Optik, Pilotenjacke hellbraun dunkelbraun, Ledermantel van Heising Gothic stark lang, Trachtenhose Hintenhose, Kniebundlederhose, Motorradjacke, Motorradlederjacke, Retro-Look schwarz blau rot gelb grau Textil, Motorradjacke, Camouflage Tarnfarbe grün, Motorradhose, Motorradhose, Motorradschulter, Motorradhose beige, Motorradlederhose 2-teilig, Motorradhandschuh, Motorrad, Winterhandschuh, Motorrad, Satteltaschen, Satteltaschen, Akten-Ledertasche, Akten-Ledertasche, Rückenpanzer Protektor, Schildkröte, Brustpanzer.
- Neue Produkte:** A grid of 12 product cards, each with an image, title, price, and a 'Artikel anschauen' button.
 - Racing Motorradlederkombi 2tlg. in 4 FARBEN:** 2-teiliger Racing-Motorradkombi aus robustem Voll-Blindleder, schmutzabweisend in 4 Farben-Mix-Verbindungen. Preis: 362,00 € (inkl. 19% MwSt, zzgl. Versand).
 - Brust- und Rückenpanzer Safety Jacket - blau:** Safety Jacket mit Protektoren-Elementen aus Spezial-Kunststoff. Preis: 89,00 € (inkl. 19% MwSt, zzgl. Versand).
 - Brust- und Rückenpanzer Safety Jacket - gelb:** Safety Jacket mit Protektoren-Elementen aus Spezial-Kunststoff. Preis: 89,00 € (inkl. 19% MwSt, zzgl. Versand).
 - Brust- und Rückenpanzer Safety Jacket - rot:** Safety Jacket mit Protektoren-Elementen aus Spezial-Kunststoff. Preis: 89,00 € (inkl. 19% MwSt, zzgl. Versand).
 - Rückenpanzer Schildkröte - gelb:** Flexibler Rückenprotektor für wirksamen Schutz aus Spezial-Kunststoff. Preis: 49,00 € (inkl. 19% MwSt, zzgl. Versand).
 - Rückenpanzer Schildkröte - rot:** Flexibler Rückenprotektor für wirksamen Schutz aus Spezial-Kunststoff. Preis: 49,00 € (inkl. 19% MwSt, zzgl. Versand).
 - Rückenpanzer Schildkröte - blau:** Flexibler Rückenprotektor für wirksamen Schutz aus Spezial-Kunststoff. Preis: 49,00 € (inkl. 19% MwSt, zzgl. Versand).
 - Edle Akten tasche aus feinem Rindsleder:** Edler Aktenkoffer mit wahliger weicher Naht aus feinem Rindsleder. Die Tasche hat ich ge... Preis: 49,00 € (inkl. 19% MwSt, zzgl. Versand).
 - Motorrad Satteltaschen:** Microsatteltaschen aus starkem Probe-Sattelleder mit Nylon... Preis: 49,00 € (inkl. 19% MwSt, zzgl. Versand).

Gestern

- Pin-Code Beispiel
- Schadsoftware
- Ransomware
- Versteckte Kommunikation

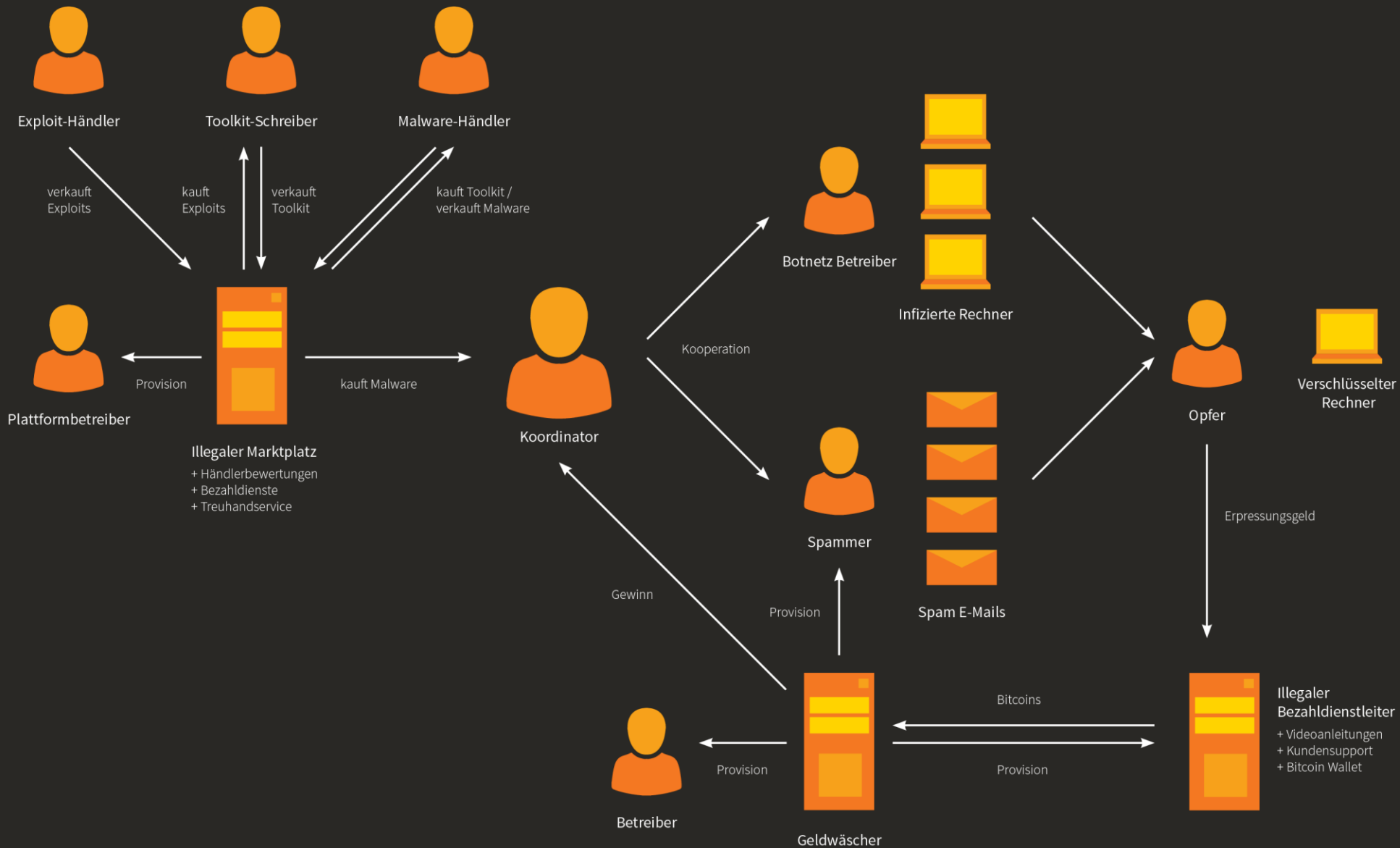
Heute

Morgen



Cyber Crime - Heute

Cybercrime as a Service - CaaS



Gestern

Heute

Cybercrime as a Service
Passwortsicherheit
Faktor Mensch
Fallbeispiel Locky

Morgen

CaaS - Werbevideo



Quelle: [youtube.com](https://www.youtube.com/watch?v=7...) (7)

Gestern

Heute

Cybercrime as a Service
Passwortsicherheit
Faktor Mensch
Fallbeispiel Locky

Morgen

CaaS - Vorgehensweise



The image shows a screenshot of the Google Germany homepage. At the top center is the Google logo in its multi-colored font, with the word 'Deutschland' in a smaller, grey font directly below it. Below the logo is a large, empty search bar with a blue border and a microphone icon on the right side. Underneath the search bar are two buttons: 'Google-Suche' on the left and 'Auf gut Glück!' on the right.

Gestern

Heute

Cybercrime as a Service
Passwortsicherheit
Faktor Mensch
Fallbeispiel Locky

Morgen

CaaS – Suchmaschinen Parameter

Parameter	Beschreibung
site:	Eine Suche mit dem Suchparameter "site" in Verbindung mit einer Domain oder URL liefert alle Seiten dieser Domain, die verfügbar sind. Beispiel: <i>it security site:hs-albsig.de</i>
intitle:	Eine Suche mit dem Suchparameter "intitle" in Verbindung mit einem Suchbegriff liefert Ergebnisse von Webseiten, deren Titel diesen Suchbegriff enthalten. Beispiel: <i>intitle:"it security"</i>
inurl:	Eine Suche mit dem Suchparameter "inurl:" in Verbindung mit einem Suchbegriff liefert Ergebnisse von Webseiten, deren URL den Suchbegriff enthalten. Beispiel: <i>inurl:"it-security"</i>
intext:	Mit dem Suchparameter "intext" in Verbindung mit einem Suchbegriff werden Webseiten angezeigt, in denen der Begriff im Text der Seite vorkommt. Beispiel: <i>intext:"it security bachelor"</i>

Gestern

Heute

Cybercrime as a Service
Passwortsicherheit
Faktor Mensch
Fallbeispiel Locky

Morgen

LIVE CaaS – Webcams finden

- Beispiel Suchanfragen nach Webcams:
 - intitle:webcam 7 inurl:8080 -intext:8080
 - intext:"powered by webcamXP 5"
 - inurl:"viewerframe?mode=motion"
 - intitle:"Live View / - AXIS"
 - inurl:indexFrame.shtml
 - intitle:"EvoCam" inurl:"webcam.html"

Gestern

Heute

Cybercrime as a Service
Passwortsicherheit
Faktor Mensch
Fallbeispiel Locky

Morgen

CaaS – Google Hacking Database

EXPLOIT DATABASE

GET CERTIFIED

Google Hacking Database

Filters Reset All

Show 15

Quick Search

Date Added	Dork	Category	Author
2019-11-12	intitle:index.of "access.conf"	Files Containing Juicy Info	Ismail Tasdelen
2019-11-12	intitle:"index of" "ssh.yml"	Files Containing Juicy Info	Ismail Tasdelen
2019-11-11	intitle:index.of "htaccess.txt"	Sensitive Directories	Ismail Tasdelen
2019-11-11	intitle:"index of" "ws_ftp.log"	Sensitive Directories	Reza Abasi
2019-11-11	inurl:"/index.php?title=Special:Userlogin"	Pages Containing Login Portals	Reza Abasi
2019-11-11	inurl:"/index.php?content=login"	Pages Containing Login Portals	Reza Abasi
2019-11-11	inurl:"/index.php?p=login"	Pages Containing Login Portals	Reza Abasi
2019-11-11	inurl:"/index.php?pageID=login"	Pages Containing Login Portals	Reza Abasi
2019-11-11	inurl:"/index.php/main/login"	Pages Containing Login Portals	Reza Abasi
2019-11-11	intitle:"index of" "databases.yml"	Files Containing Juicy Info	Reza Abasi
2019-11-11	intitle:"index of" "db.conf"	Files Containing Passwords	Reza Abasi
1	inurl:elmah.axd ext:axd	Error Messages	Dhaiwat Mehta
1	intitle:"Error log for /M/"	Error Messages	Dhaiwat Mehta

Quelle: exploit-db.com (9)

Gestern

Heute

Cybercrime as a Service
Passwortsicherheit
Faktor Mensch
Fallbeispiel Locky

Morgen

11.2019 Veraltete Versionen

The screenshot shows the homepage of 'The Hacker News' website. At the top, there is a blue navigation bar with the site's name 'The Hacker News' in white, a 'Click to Subscribe' button, and social media icons for Facebook, Twitter, LinkedIn, YouTube, and RSS. Below this is a white navigation menu with links for Home, Data Breaches, Cyber Attacks, Vulnerabilities, Malware, Deals, and Contact, along with a search icon and a hamburger menu icon. The main content area features a large article titled 'Hackers Breach ZoneAlarm's Forum Site – Outdated vBulletin to Blame' by Swati Khandelwal, dated November 11, 2019. The article's featured image shows a warning icon and the text 'Forum Data Breach Incident' above the ZoneAlarm logo, which includes the text 'ZONEALARM by Check Point'. To the right of the article is a 'Popular This Week' section with four items: 'Amazon's Ring Video Doorbell Lets Attackers Steal Your Wi-Fi Password', 'Gartner Says the Future of Network Security Lies with SASE', 'Rogue TrendMicro Employee Sold Customer Data to Tech Support Scammers', and 'Facebook Reveals New Data Leak Incident Affecting Groups'.

Quelle: thehackernews.com (10)

CaaS – IoT Beispielprodukt

heise online Anmelden Suchen Menü

IT Mobiles Entertainment Wissen Netzpolitik Wirtschaft Journal Newsticker Foren

TOPTHEMEN: CES 2019 DSGVO WINDOWS 10 ANDROID AMAZON KI ANZEIGE: CLOUD SERVICES ZUKUNFTSMACHER

Security 7-Tage-News | 01/2016 | IP-Kameras von Aldi mit massiven Sicherheitslücken

Alert! 15.01.2016 10:49 Uhr | Security

IP-Kameras von Aldi als Sicherheits-GAU

Aldi hatte vergangenes Jahr mehrfach IP-Überwachungskameras mit denkbar schlechten Voreinstellungen verkauft. Die Geräte sind zu Hunderten fast ungeschützt über das Internet erreichbar.

Von Ronald Eikenberg

411



Die bei Aldi verkauften IP-Überwachungskameras der Marke Maginon haben massive Sicherheitsprobleme: Unbefugte könnten über das Internet auf das Kamerabild zugreifen und sogar den Ton anzapfen. Zudem verraten die Geräte unter anderem die Passwörter für WLAN, E-Mail und FTP-Zugang ihres Besitzers. Hunderte Aldi-Kameras sind nahezu ungeschützt über das Internet erreichbar. Darauf hat uns der Zusammenschluss Digitale Gesellschaft aufmerksam gemacht.



Betroffen ist unter anderem die Außenkamera IPC-20 C. (Bild: Hersteller)

Gestern

Heute

Cybercrime as a Service
Passwortsicherheit
Faktor Mensch
Fallbeispiel Locky

Morgen

CaaS – Spezialisierte Suchmaschine

Shodan Developers Monitor View All...

SHODAN [Search Bar] Explore Pricing Enterprise Access New to Shodan? Login or Register

The search engine for **Webcams**

Shodan is the world's first search engine for Internet-connected devices.

Create a Free Account Getting Started

- Explore the Internet of Things**
Use Shodan to discover which of your devices are connected to the Internet, where they are located and who is using them.
- Monitor Network Security**
Keep track of all the computers on your network that are directly accessible from the Internet. Shodan lets you understand your digital footprint.
- See the Big Picture**
Websites are just one part of the Internet. There are power plants, Smart TVs, refrigerators and much more that can be found with Shodan!
- Get a Competitive Advantage**
Who is using your product? Where are they located? Use Shodan to perform empirical market intelligence.

21% of Fortune 100 1,000+ Universities

Quelle: shodan.io (12)

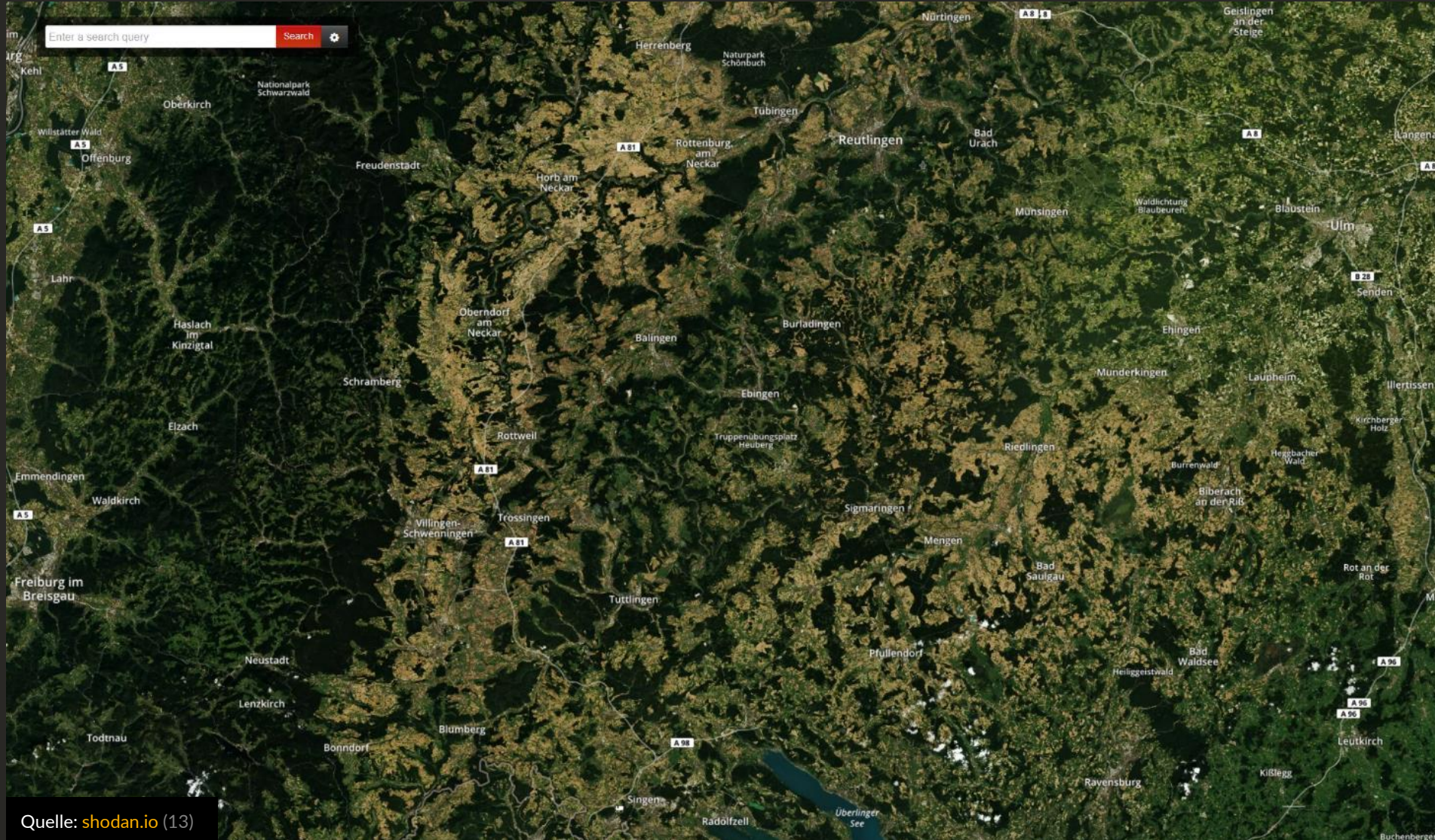
Gestern

Heute

[Cybercrime as a Service](#)
[Passwortsicherheit](#)
[Faktor Mensch](#)
[Fallbeispiel Locky](#)

Morgen

LIVE CaaS - Spezialisierte Suchmaschine



Gestern

Heute

- Cybercrime as a Service
- Passwortsicherheit
- Faktor Mensch
- Fallbeispiel Locky

Morgen

Passwortsicherheit

Top 100 Adobe Passwords with Count

We do not (yet) have the keys Adobe used to encrypt the passwords of 130,324,429 users affected by their most recent breach. However, thanks to Adobe choosing symmetric key encryption over hashing, selecting ECB mode, and using the same key for every password, combined with a large number of known plaintexts and the generosity of users who flat-out gave us their password in their password hint, this is not preventing us from presenting you with this list of the top 100 passwords selected by Adobe users.

While we are fairly confident in the accuracy of this list, we have no way to actually verify it right now. We don't have the keys, and Adobe is not letting any of the affected accounts log in until the owners reset their passwords. So, it is possible there is an error or two in here. Caveat emptor and such.

#	Count	Ciphertext	Plaintext
1.			
2.			
3.			
4.			
5.			
6.			
7.			
8.			
9.			
10.			
11.			
12.			
13.			
14.			

Quelle: github.com (14)

Gestern

Heute

- Cybercrime as a Service
- [Passwortsicherheit](#)
- Faktor Mensch
- Fallbeispiel Locky

Morgen

LIVE Passwortsicherheit

The screenshot shows the homepage of haveibeenpwned.com. At the top, there is a navigation bar with links: Home, Notify me, Domain search, Who's been pwned, Passwords, API, About, and Donate. The main heading is a large white rounded rectangle containing the text "';--have i been pwned?". Below this is a sub-heading: "Check if you have an account that has been compromised in a data breach". A search form is present with a text input field labeled "email address" and a button labeled "pwned?". Below the search form, there is a promotional banner for 1Password: "Generate secure, unique passwords for every account" with a link to "Learn more at 1Password.com" and the text "Why 1Password?".

Statistics section:

- 340 pwned websites
- 6,474,028,664 pwned accounts
- 87,569 pastes
- 96,065,928 paste accounts

Two columns of breach lists are shown:

- Largest breaches:**
 - 772,904,991 Collection #1 accounts
 - 711,477,622 Onliner Spambot accounts
 - 593,427,119 Exploit.In accounts
 - 457,962,538 Anti Public Combo List accounts
 - 393,430,309 River City Media Spam List accounts
 - 359,420,698 MySpace accounts
 - 234,842,089 NetFase accounts
- Recently added breaches:**
 - 772,904,991 Collection #1 accounts
 - 87,633 FaceUP accounts
 - 4,848,734 Dangdang accounts
 - 213,415 BannerBit accounts
 - 7,633,234 BlankMediaGames accounts
 - 242,715 GoldSilver accounts
 - 205,242 Mappery accounts

Quelle: haveibeenpwned.com (15)

Gestern

Heute

- Cybercrime as a Service
- Passwortsicherheit
- Faktor Mensch
- Fallbeispiel Locky

Morgen

Passwortsicherheit

Cyber Security Vortrag
Internetkriminalität / Cybercrime



Quelle: [youtube.com](https://www.youtube.com/watch?v=16) (16)

Gestern

Heute

Cybercrime as a Service
Passwortsicherheit
Faktor Mensch
Fallbeispiel Locky

Morgen

20.11.2019 | NKM Noell

Tobias Scheible, M.Eng.

Passwörter erraten

- Angreifer analysieren das Umfeld eines Opfers, um auf potentielle Passwörter schließen zu können und so diese zu erraten.
 - Alle Seiten bzw. Profile von einem Opfer werden gesucht und analysiert.
 - Dabei werden bevorzugt Inhalte von Social Media Seiten automatisch gescannt.
 - Auch Fotos werden ausgewertet und Texte automatisch erkannt – z.B. Autokennzeichen.
 - Typische Informationen wie Namen von Verwandten, Adressen, Geburtsdaten oder Haustiere werden gezielt gesucht.
 - Aus diesen Informationen werden individuelle Listen generiert.
- Bei Unternehmen werden die Website und Dokumente gescannt.

Gestern

Heute

Cybercrime as a Service
Passwortsicherheit
Faktor Mensch
Fallbeispiel Locky

Morgen

LIVE Passwörter & Flugtickets



Gestern

Heute

Cybercrime as a Service
Passwortsicherheit
Faktor Mensch
Fallbeispiel Locky

Morgen

Brute-Force Methode

- Mit Brute-Force-Angriffen wird versucht, ein Passwort zu knacken, indem in schneller Abfolge verschiedene Zeichenkombinationen ausprobiert werden.
- Der Algorithmus ist sehr einfach und beschränkt sich auf das Ausprobieren möglichst vieler Zeichenkombinationen, weshalb auch von "erschöpfender Suche" gesprochen wird.
- Dabei hängt es von der verfügbaren Rechenleistung ab, wie viele Berechnungen pro Sekunde durchgeführt und entsprechend eine hohe Anzahl an Kombinationen ausprobiert werden können.
- Die Methode wird in der Praxis häufig erfolgreich eingesetzt, da viele Benutzer kurze Passwörter verwenden, die darüber hinaus oft nur aus Zeichen des Alphabets bestehen, womit die Anzahl der möglichen Kombinationen drastisch reduziert wird.

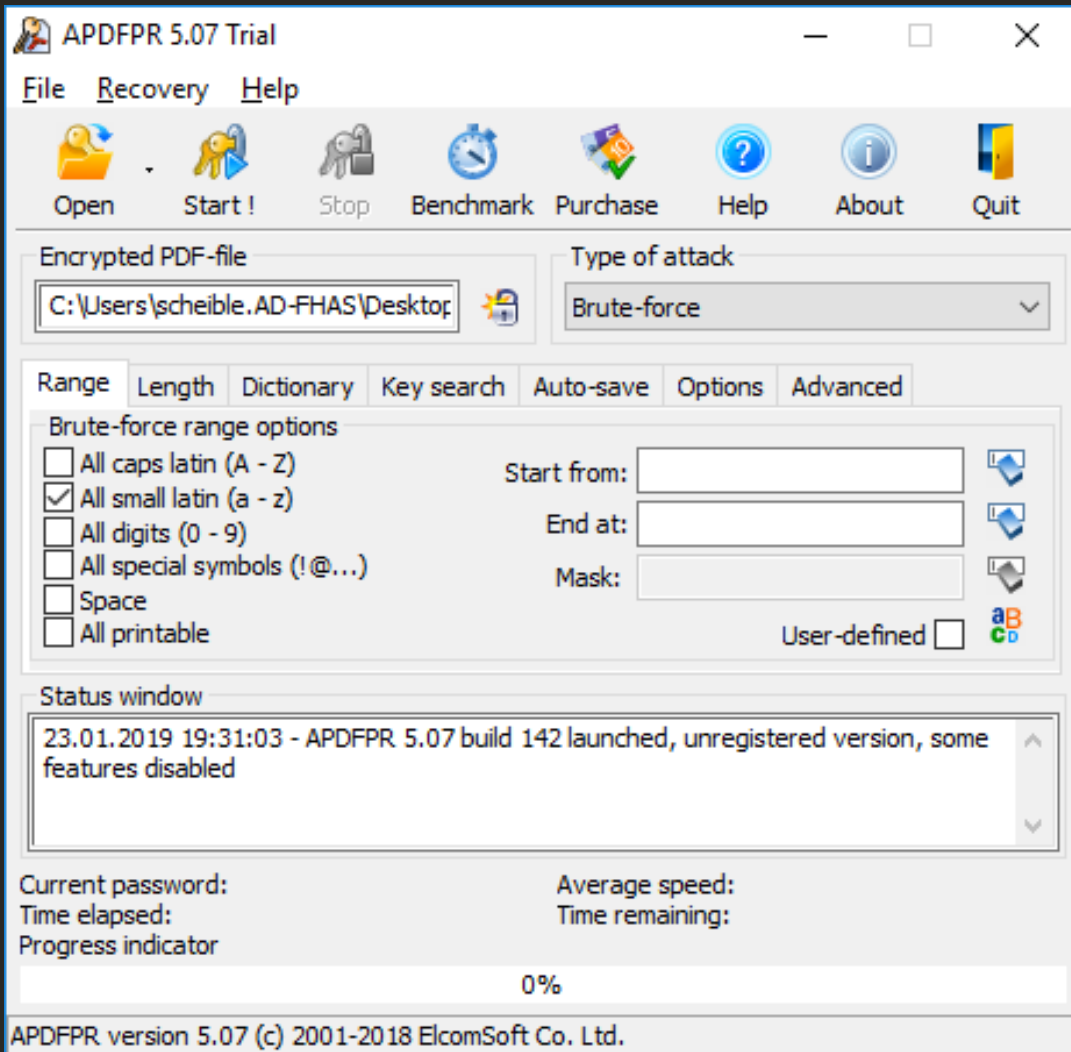
Gestern

Heute

Cybercrime as a Service
Passwortsicherheit
Faktor Mensch
Fallbeispiel Locky

Morgen

DEMO Brute-Force Methode



Gestern

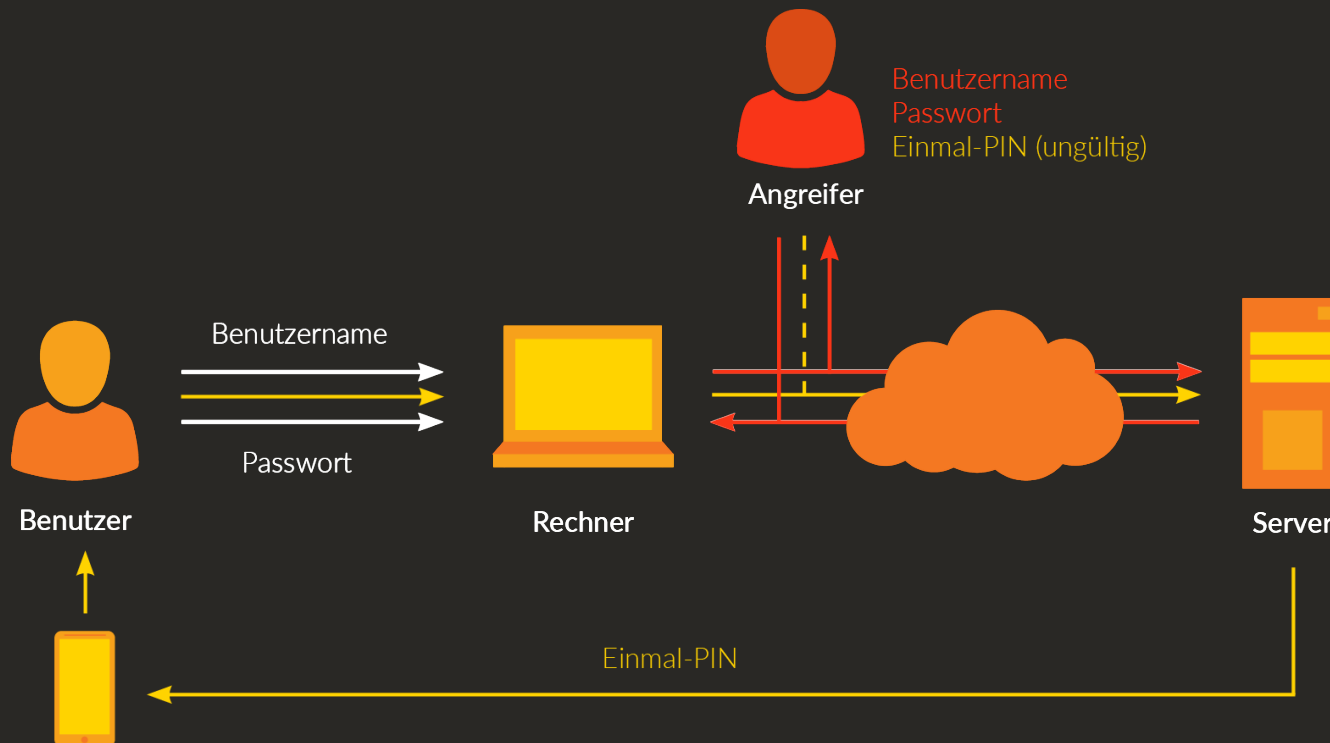
Heute

Cybercrime as a Service
Passwortsicherheit
Faktor Mensch
Fallbeispiel Locky

Morgen

Sichere Passwörter

- Zwei-Faktor-Authentisierung
 - Login mit zwei Faktoren (Passwort + Code per SMS oder APP)
 - Bei geklauten Login-Daten ist trotzdem keine Anmeldung möglich
 - Bekannt von der Bezahlung per EC-Karte (Pin + Karte)



Gestern

Heute

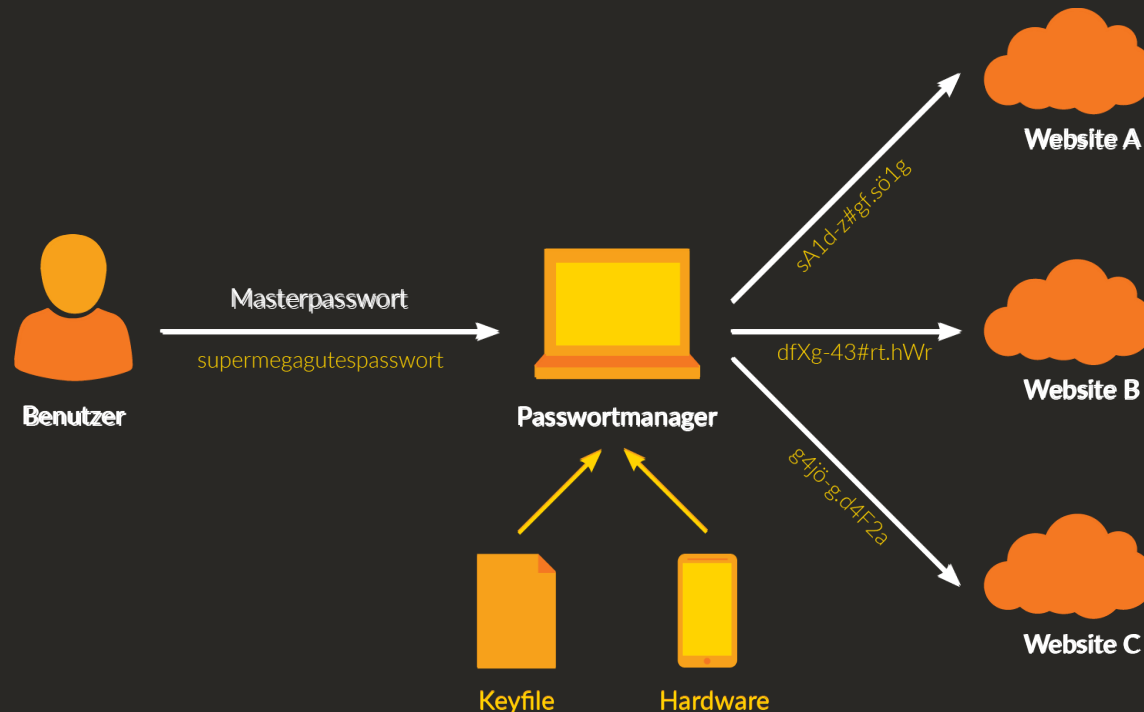
Cybercrime as a Service
Passwortsicherheit
Faktor Mensch
Fallbeispiel Locky

Morgen

Sichere Passwörter

■ Passwortmanager

- Speichert Passwörter in einem verschlüsselten Container mit einem Masterpasswort und Unterstützt bei der Generierung von Passwörtern
- Verschiedene Lösungen sind vorhanden – z.B. KeePassXC
 - Viele Möglichkeiten zur Erweiterung (Firefox / Chrome Plugin, ...)



Gestern

Heute

Cybercrime as a Service
Passwortsicherheit
Faktor Mensch
Fallbeispiel Locky

Morgen

Fazit Passwortsicherheit

- Die Länge eines Passwortes ist ein entscheidender Faktor. Lange Passwörter sind, pauschal gesagt, sicherer als kurze.
- Das Passwort darf nicht mit Ihrem persönlichen Umfeld in Verbindung stehen.
- Nutzen Sie für jeden Dienst verschiedene Passwörter, damit nach einem Angriff nicht auch andere Accounts von Ihnen betroffen sind.
- Nutzen Sie einen Passwortmanager, um die unterschiedlichen Passwörter sicher zu speichern.
- Nutzen Sie überall, wo es geht, eine Zwei-Faktor-Authentisierung.

Was ist die häufigste Angriffsmethode?

Ausnutzung von Schwachstellen

A

Physische Attacken

B

Manipulation von Personen

C

Ausnutzung von Fehlern

D

Faktor Mensch



Gestern

Heute

- Cybercrime as a Service
- Passwortsicherheit
- Faktor Mensch
- Fallbeispiel Locky

Morgen

Faktor Mensch - Angriff auf TV5 Monde

Cyber Security Vortrag
Internetkriminalität / Cybercrime



Quelle: [heise.de](https://www.heise.de) (19)

Gestern

Heute

Cybercrime as a Service
Passwortsicherheit
Faktor Mensch
Fallbeispiel Locky

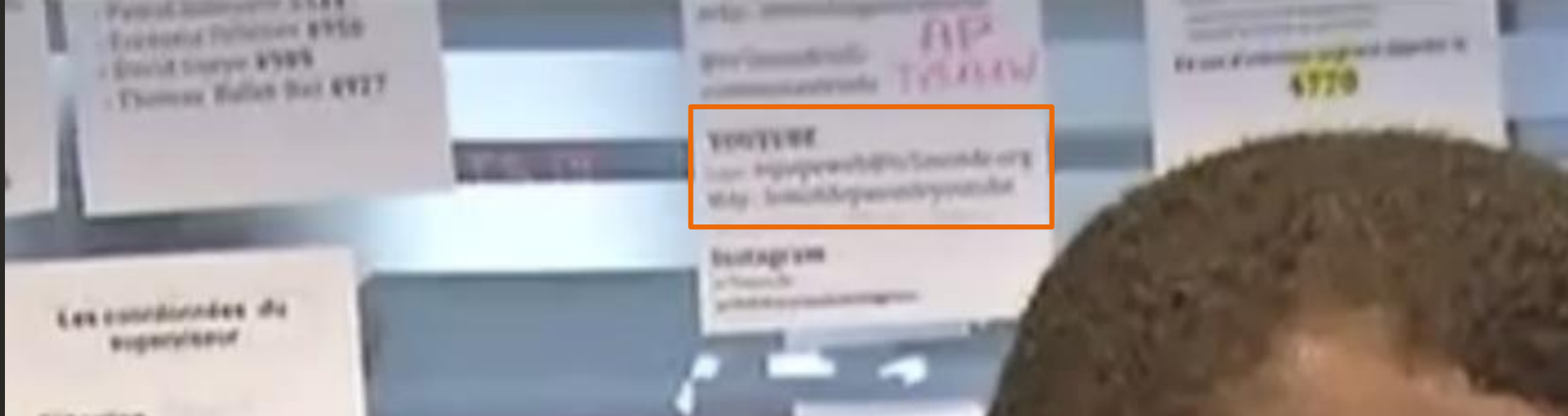
Morgen

20.11.2019 | NKM Noell

Tobias Scheible, M.Eng.

39

Faktor Mensch - Angriff auf TV5 Monde



YouTube Passwort:
"lemotdepasseyoutube"
(etwa "dasyoutubepasswort")

Gestern

Heute

Cybercrime as a Service
Passwortsicherheit
Faktor Mensch
Fallbeispiel Locky

Morgen

Faktor Mensch



Quelle: [vice.com](https://www.vice.com) (20)

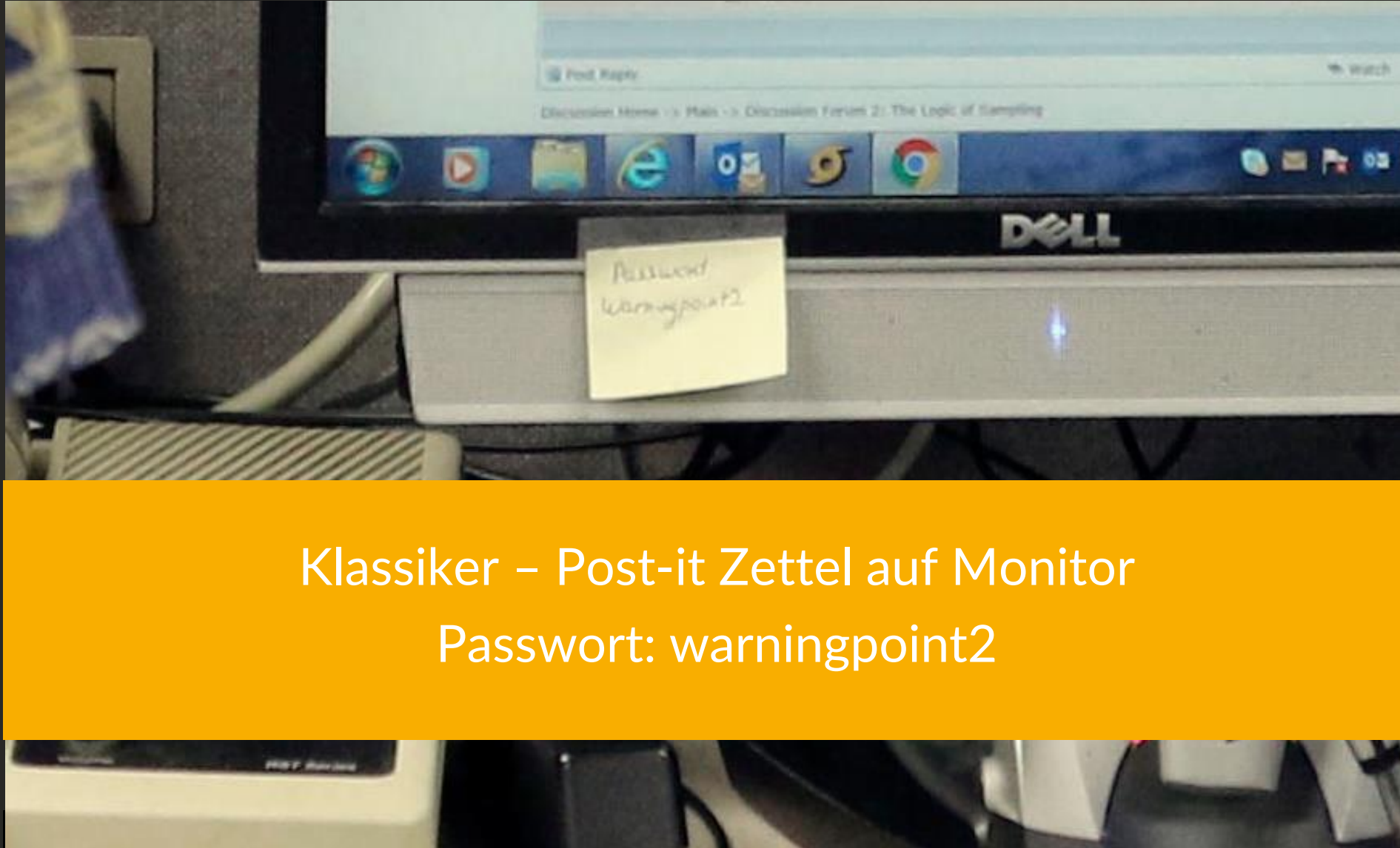
Gestern

Heute

Cybercrime as a Service
Passwortsicherheit
Faktor Mensch
Fallbeispiel Locky

Morgen

Faktor Mensch



Klassiker – Post-it Zettel auf Monitor
Passwort: warningpoint2

Gestern

Heute

Cybercrime as a Service
Passwortsicherheit
Faktor Mensch
Fallbeispiel Locky

Morgen

Faktor Mensch

- Moderner Ausbruch aus einem britischen Gefängnis (März 2015)
- SocialEngineering Angriff auf das Gefängnis
 - Smartphone eingeschmuggelt
 - Domain reserviert, die dem zuständigen Gericht ähnelt
 - E-Mail Adresse mit dieser Domain eingerichtet
 - Hat sich als leitender Beamter ausgegeben
 - Anweisungen zu seiner Entlassung gegeben
- Gefangener kam frei

Gestern

Heute

Cybercrime as a Service
Passwortsicherheit
Faktor Mensch
Fallbeispiel Locky

Morgen

Faktor Mensch - CEO Fraud

Freitag, 12. Februar 2016

Service | Abo | Shop | Newsletter | Login | Registrieren | Suchbegriff, WKN, ISIN

WirtschaftsWoche | UNTERNEHMEN | FINANZEN | POLITIK | ERFOLG | TECHNOLOGIE

Trends | Management | Gründer | Beruf | Jobsuche | Campus & MBA | Karriere | Jobturbo

DAX®	E-STOXX 50®	MDAX®	Dow Jones	Gold (USD)	EUR/USD	Börsenkurse
8.752,87 -2,93%	2.680,35 -3,90%	17.594,68 -2,83%	15.660,18 -1,60%	1.242,83 -0,30%	1,1315 -0,00%	citi Indikatoren

Die WirtschaftsWoche > Erfolg > Management > Falsche Chefs zocken Firmen ab: Den Enkeltrick gibt's auch bei Unternehmen


Falsche Chefs zocken Firmen ab

18. August 2015

Den Enkeltrick gibt's auch bei Unternehmen

★★★★☆
0
Kommentare

Versenden
Drucken
Merken
Startseite



Nicht nur gutgläubige Senioren werden Opfer von Trickbetrü gern.

Bild: dpa

Während sich manche Betrüger als vermisste Enkel ausgeben, um ans Ersparte von Senioren zu kommen, probieren es andere eine Nummer größer. Sie geben sich als Chef aus und erleichtern Unternehmen um Millionenbeträge.

"Hallo, ich bin's, der Chef. Bitte überweisen Sie folgenden Betrag auf folgendes Konto..." So oder so ähnlich funktioniert die Betrugsmasche "CEO Fraud", die derzeit nach Deutschland schwappt. Dabei kontaktieren die mutmaßlichen Betrüger per Telefon und E-Mail Mitarbeiter von Unternehmen und geben sich als Vertreter der Geschäftsführung aus. Dann fordern sie bestimmte Beträge auf

Quelle: wiwo.de (22)

Gestern

Heute

Cybercrime as a Service
Passwortsicherheit
Faktor Mensch
Fallbeispiel Locky

Morgen

Faktor Mensch - CEO Fraud

Von: Gustav.Geschäftsführer@firma.de
<Gustav.Geschäftsführer@firma-gmbh.de>

An: Otto Opfer

Sehr geehrter Herr Opfer!

Sind Sie im Moment verfügbar?

Hochachtungsvoll

Gustav Geschäftsführer

Gestern

Heute

Cybercrime as a Service
Passwortsicherheit
Faktor Mensch
Fallbeispiel Locky

Morgen

Faktor Mensch - CEO Fraud

..wir führen momentan eine finanzielle Transaktion durch, bei der es um eine Unternehmensübernahme in Asien geht.

Diese Übernahme **muss streng vertraulich behandelt werden**. Sie sind als einziger Ansprechpartner damit betraut worden, diesen Vorgang auszuführen und Zahlungen vorzunehmen (Alle Informationslecks oder die Nichteinhaltung des unten genannten Verfahrens können zu **Vertragsstrafen und Sanktionen** gegen unsere Firmen führen).

Die öffentliche Bekanntgabe der Übernahme wird am 15.09.2015 in unseren Räumlichkeiten in Anwesenheit des gesamten Managements stattfinden.

Sie finden diesbezüglich einen von der BaFin (Bundesanstalt für Finanzdienstleistungsaufsicht) erteilten Zahlungsauftrag.

Bitte nehmen Sie zur Einreichung der Bankdaten zur sofortigen Ausführung der Zahlung umgehend Kontakt mit unserem französischen **Berater B. Berater** auf (Dieser interveniert zwischen BaFin und AMF, um unsere Interessen zu verteidigen).

Gestern

Heute

Cybercrime as a Service
Passwortsicherheit
Faktor Mensch
Fallbeispiel Locky

Morgen

Faktor Mensch - CEO Fraud

Bitte vermeiden Sie in persönlichen wie in telefonischen Gesprächen jegliche Anspielung auf diesen Vorgang. Nutzen Sie ausschließlich den E-Mail-Verkehr mit Herrn B. (Berater), der Ihr einziger Ansprechpartner für diesen Vorgang sein wird.

Kontaktdaten von Herrn B. Berater.: B.Berater@berater-firma.com

Sobald Sie die Bankdaten erhalten, führen Sie bitte die Zahlung gemäß der beigefügten Zahlungsanweisung auf eine Weise aus, die Sie alleine vornehmen können.

Ich bitte Sie auch, Herrn B. einen Zahlungsbeleg zuzusenden, sobald er zur Verfügung steht.

Ich möchte, dass Sie bei diesem Vorgang der einzige Gesprächspartner und Ausführende innerhalb unseres Unternehmens sind.

Vielen Dank für Ihr zügiges Vorgehen. Die Finanztransaktion läuft.

Gestern

Heute

Cybercrime as a Service
Passwortsicherheit
Faktor Mensch
Fallbeispiel Locky

Morgen

Faktor Mensch - CEO Fraud

Von: Gustav.Geschäftsführer@firma.de
<Gustav.Geschäftsführer@firma-gmbh.de>

An: Otto Opfer

Konnten Sie das Nötige erledigen?

Hochachtungsvoll
Gustav Geschäftsführer

Gestern

Heute

Cybercrime as a Service
Passwortsicherheit
Faktor Mensch
Fallbeispiel Locky

Morgen

Faktor Mensch - CEO Fraud

Dear Mr Opfer,

Mr G. (Geschäftsführer) just sent me the document signed by him and Mr Z. (2. Genehmiger).

Unfortunately I need to provide to BaFin a Specimen of signature (for security reason) from them, can you please send to me an example of signature of Mr G. and Mr Z. on a document older than today ?

Thank you.

Best regards

B. Berater

BaFin /AMF Consultant

Gestern

Heute

Cybercrime as a Service
Passwortsicherheit
Faktor Mensch
Fallbeispiel Locky

Morgen

LIVE E-Mails fälschen



Tobias Scheible
Cyber Security & IT Forensics Lab

Fake Mail Sender

Example to show how an Mail sender can be faked.

Sender Mail	
Sender Name	
Receiver Mail	
Subject	

send mail

Gestern

Heute

Cybercrime as a Service
Passwortsicherheit
Faktor Mensch
Fallbeispiel Locky

Morgen

LIVE E-Mails fälschen



Tobias Scheible
Cyber Security & IT Forensics Lab

Fake SMS Sender

Example to show how an SMS sender can be faked.

Receiver Number

Sender Number

send sms

Gestern

Heute

Cybercrime as a Service
Passwortsicherheit
Faktor Mensch
Fallbeispiel Locky

Morgen

The screenshot shows the top navigation bar of the heise.de website. It includes the logo 'heise online' and 'heise+', a search bar with the text 'Suchen', and a 'Menü' dropdown. Below the navigation bar are category links: 'IT', 'Mobiles', 'Entertainment', 'Wissen', 'Netzpolitik', 'Wirtschaft', and 'Journal'. There are also links for 'Newsticker' and 'Foren'. A 'TOPTHEMEN:' section features tags for 'EMOTET', 'QUANTENCOMPUTER', 'E-AUTO', 'WINDOWS 10', and 'RASPI 4'. The main headline reads 'Mitarbeiter von IT-Sicherheitsfirma Trend Micro verkaufte Kundendaten an Scammer'. A sub-headline states: 'Ein ehemaliger Trend-Micro-Mitarbeiter hat die Seiten gewechselt und Privatkundendaten an Telefonbetrüger verkauft. Auch deutsche Kunden sollten wachsam sein.' Below the text, there is a 'Lesezeit: 1 Min.' indicator, a 'In Pocket speichern' button, and social sharing icons for audio, print, and comments (19). The bottom of the article is partially obscured by a blurred image.

heise online heise+ Anmelden Suchen Menü

IT Mobiles Entertainment Wissen Netzpolitik Wirtschaft Journal Newsticker Foren

TOPTHEMEN: EMOTET QUANTENCOMPUTER E-AUTO WINDOWS 10 RASPI 4

Mitarbeiter von IT-Sicherheitsfirma Trend Micro verkaufte Kundendaten an Scammer

Ein ehemaliger Trend-Micro-Mitarbeiter hat die Seiten gewechselt und Privatkundendaten an Telefonbetrüger verkauft. Auch deutsche Kunden sollten wachsam sein.

Lesezeit: 1 Min. In Pocket speichern 19

Quelle: [heise.de](https://www.heise.de) (23)

Fallbeispiel Locky

- Effektive Methode, um Geld zu ergaunern
- Auf deutsche Benutzer ausgerichtete Varianten
- Verschlüsselt alle Benutzerdateien, auch auf Netzwerklaufwerke

- Zeitlicher Ablauf:
 - **15.02.2016** Locky wird als Schläfer aktiviert (Makros)
 - **22.02.2016** Gefälschte Unternehmensrechnung (JScript)
 - **24.02.2016** Gefälschtes Sipgate Fax (JScript)
 - **26.02.2016** Neue Infektionstechnik mit Batch-Dateien
 - **02.03.2016** Gefälschte BKA E-Mail (EXE-Datei)

Gestern

Heute

Cybercrime as a Service
Passwortsicherheit
Faktor Mensch
Fallbeispiel Locky

Morgen

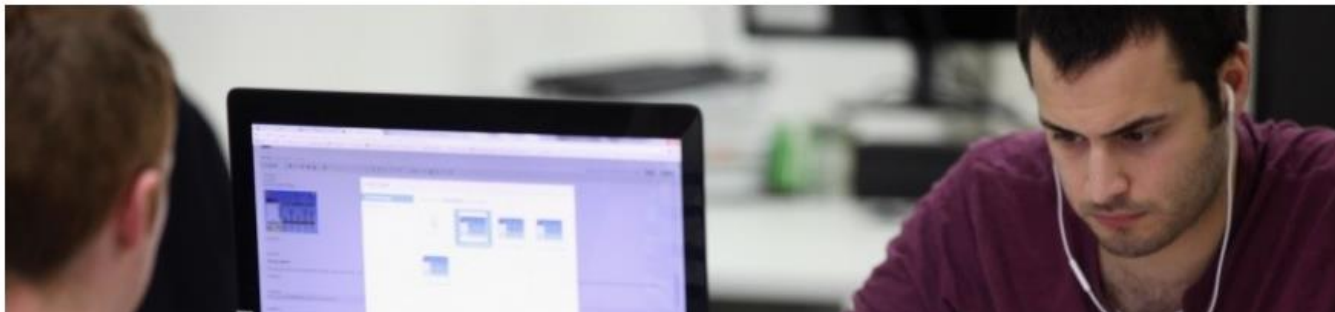
SOCIAL ENGINEERING

"Die Mitarbeiter sind unsere Verteidigung"

Prävention reicht nicht gegen [Social Engineering](#) und die derzeitigen Trainings sind nutzlos, sagt der Sophos-Sicherheitsexperte Chester Wisniewski. Seine Lösung: Mitarbeiter je nach Bedrohungslevel schulen - und so schneller sein als die Kriminellen.

Ein Interview von Moritz Tremmel

14. November 2019, 9:12 Uhr



(Bild: Oli Scarff/Getty Images)

FAZIT Faktor Mensch / Social Engineering

- Informationen im Internet, aber auch SMS und Telefonnummern, können sehr einfach gefälscht werden.
- E-Mails können sehr einfach manipuliert werden und vorhandene Konversationen können von Angreifern aufgegriffen werden.
- Sensibilisieren der Mitarbeiter mit Schulungen über Social Engineering-Strategien und –Methoden. Einbinden bei der Erkennung von Angriffen.
- Definierte Prozesse für alle Abteilungen mit Schnittstellen nach außen.
- Tipp: Auf einem anderen Kanal nachfragen, ob es wirklich stimmt.

A glowing globe with digital data points and lines, symbolizing global connectivity and cybercrime. The globe is composed of numerous small, bright orange and yellow dots connected by thin lines, creating a network-like structure. The background is dark, making the glowing globe stand out prominently. The overall aesthetic is futuristic and technological.

Cyber Crime - Morgen

Hardware Tools



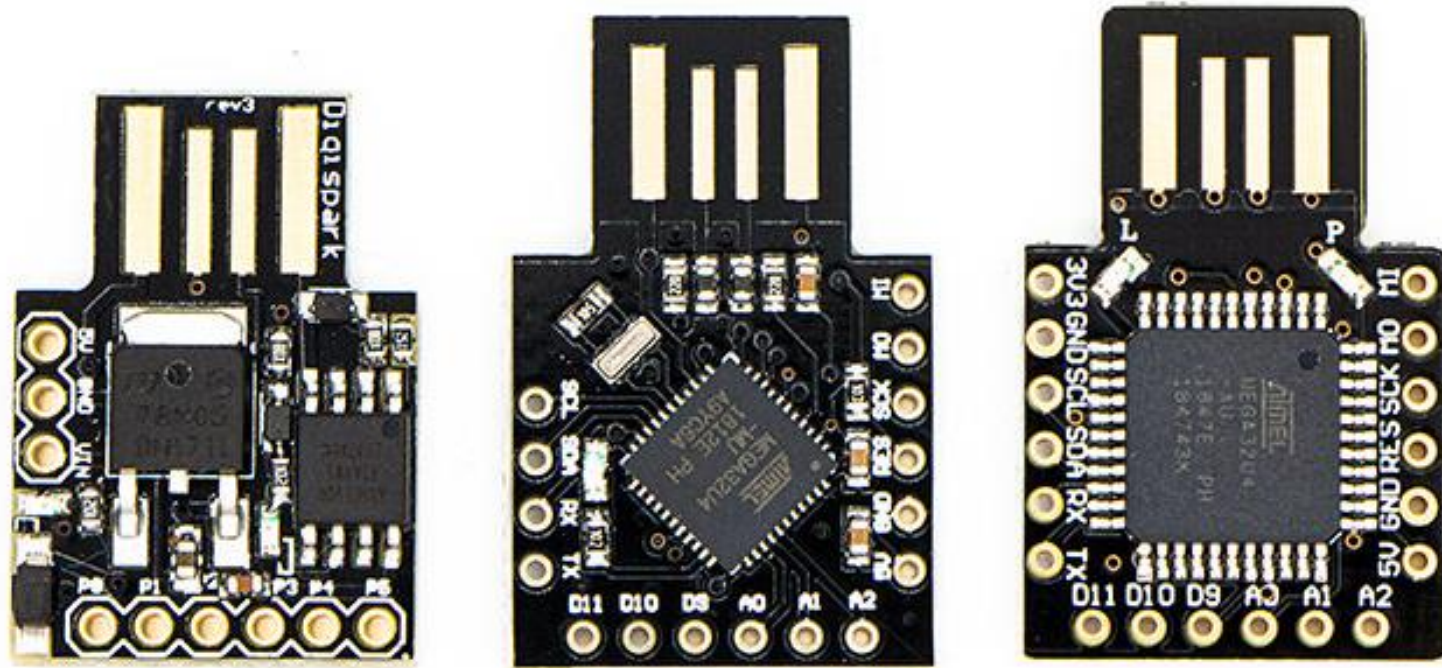
Gestern

Heute

Morgen

Hacking Hardware
Internet of Things
Spionage
Künstliche Intelligenz

LIVE Hardware Tools



Gestern

Heute

Morgen

- Hacking Hardware
- Internet of Things
- Spionage
- Künstliche Intelligenz

FAZIT Hardware Hacks

- Rechner, die sich in einem frei zugänglichen Bereich befinden, sollten durch bauliche Maßnahmen vor Manipulationen geschützt werden.
- Jede Hardware sollte kontinuierlich auf Veränderungen automatisch überprüft und Vorkommnisse gemeldet werden.
- Mitarbeiter müssen sensibilisiert werden, damit unbekannte Geräte oder abweichende Verhaltensweisen sofort gemeldet werden.
- Ein Ausfall einer Sicherheitskomponente soll gleichgesetzt werden wie ein Alarm.

IoT – Internet of Things

- Ein Bot-Netz, das sich aus IoT-Geräten zusammensetzt
- Es wurde genutzt, um DDOS-Angriffe auszuführen
 - Konnte auch gemietet werden
- Seiteneffekte:
 - Es wurde versucht, Router über eine Schnittstelle zur Fernwartung zu übernehmen
 - Durch eine fehlerhafte Umsetzung „stürzten“ die Router ab
 - 900.000 Router der Deutschen Telekom waren nicht mehr erreichbar



Gestern

Heute

Morgen

Hacking Hardware
Internet of Things
Spionage
Künstliche Intelligenz

IoT – Ransomware



Quelle: [computerworld.com](https://www.computerworld.com) (32)

Gestern

Heute

Morgen

Hacking Hardware

Internet of Things

Spionage

Künstliche Intelligenz

FAZIT Internet of Things

- Geräte oder Anwendungen, die im Internet sind, können nicht durch komplizierte Links oder weil die Adresse nirgendwo steht, geschützt werden.
- Die Standard-Passwörter von Geräten, die mit dem Internet verbunden sind, müssen immer geändert werden.
- Komponenten können sich auch selbstständig mit dem Internet verbinden, daher muss die Konfiguration immer geprüft werden.

Spionage – gezielte Angriffe

- Netzwerk
 - Abhören von WiFi-Verbindungen z.B. in Hotels
 - => ausschließlich VPN-Verbindungen benutzen
- Rechner
 - Gezielter Diebstahl oder Manipulationen, um an die Daten zu kommen
 - => Komplette Verschlüsselung, leere Geräte – Daten nachladen
- Datenträger
 - Die äußere Abwehr wird umgangen – häufig harte Schale, weicher Kern
 - => Abwehr in Schichten aufbauen – Bereiche trennen

Gestern

Heute

Morgen

Hacking Hardware
Internet of Things
Spionage
Künstliche Intelligenz

Künstliche Intelligenz

- Beide Seiten entwickeln Lösungen im Bereich künstlicher Intelligenz
- Verteidigung
 - Überwachung von Netzwerkverbindungen und Identifizierung von Anomalien
 - Erkennung von Anomalien im Verhalten von Benutzern
- Angreifer
 - Automatisierung hoch individualisierter Angriffe
- Nachteile
 - Mehr Komplexität und schwierig zu kontrollieren => große Abhängigkeit

Gestern

Heute

Morgen

Hacking Hardware
Internet of Things
Spionage
Künstliche Intelligenz



Fragen?

Präsentation online unter: <https://scheible.it>

Quellen

- (1) 00000000: Passwort für US-Atomraketen, <http://www.heise.de/security/meldung/00000000-Passwort-fuer-US-Atomraketen-2060077.html>, abgerufen am 19.11.2019
- (2) Mit Floppy Disks Atombomben überwachen, <http://www.zeit.de/politik/ausland/2016-05/us-militaer-pcs-technologie-veraltet-rechnungshof>, abgerufen am 19.11.2019
- (3) Was ist eigentlich die Geschichte der Malware?, <https://www.gdata.de/ratgeber/was-ist-eigentlich-die-geschichte-der-malware>, abgerufen am 19.11.2019
- (4) Android Beam hat gefährliche Sicherheitslücke – so schützt man sich, <https://www.netzwoche.ch/news/2019-11-05/android-beam-hat-gefaehrliche-sicherheitsluecke-so-schuetzt-man-sich>, abgerufen am 19.11.2019
- (5) AIDS (Schadprogramm), [https://de.wikipedia.org/wiki/AIDS_\(Schadprogramm\)](https://de.wikipedia.org/wiki/AIDS_(Schadprogramm)), abgerufen am 19.11.2019
- (6) Online-Shop, <http://www.shop.ledermode.tv>, abgerufen am 19.11.2019
- (7) Anuncio - gwapo's, <https://www.youtube.com/watch?v=5M9k7wfiWil>, abgerufen am 19.11.2019
- (8) Google Deutschland, <https://www.google.de>, abgerufen am 19.11.2019
- (9) Exploit Database, <https://www.exploit-db.com/google-hacking-database>, abgerufen am 19.11.2019
- (10) Hackers Breach ZoneAlarm's Forum Site – Outdated vBulletin to Blame, <https://thehackernews.com/2019/11/zonealarm-forum-data-breach.html>, abgerufen am 19.11.2019
- (11) IP-Kameras von Aldi als Sicherheits-GAU , <http://www.heise.de/security/meldung/IP-Kameras-von-Aldi-als-Sicherheits-GAU-3069735.html>, abgerufen am 19.11.2019
- (12) Shodan, <https://shodan.io/>, abgerufen am 19.11.2019
- (13) Shodan Maps, <https://maps.shodan.io>, abgerufen am 19.11.2019
- (14) Have I Been Pwned, <https://haveibeenpwned.com>, abgerufen am 19.11.2019

Quellen

- (15) What is Your Password?, <https://www.youtube.com/watch?v=opRMrEfAlil>, abgerufen am 19.11.2019
- (16) Top 100 Adobe Passwords with Count, <https://github.com/morontt/symfobroute/blob/master/adobe-top100.txt>, abgerufen am 19.11.2019
- (17) Code, <http://pics-for-fun.com/wonder-what-the-code-could-be/>, abgerufen am 19.11.2019
- (18) And the valuables are in the closet on the top shelf in a box marked, <https://de.pinterest.com/pin/3025924727584002/>, abgerufen am 19.11.2019
- (19) Passwörter im TV-Bild: Spekulationen zu TV5-Attacke, <http://www.heise.de/newsticker/meldung/Passwoerter-im-TV-Bild-Spekulationen-zu-TV5-Attacke-2598298.html>, abgerufen am 19.11.2019
- (20) The Agency That Messed Up Hawaii's Nuclear Alert Keeps Passwords on Post-Its, https://www.vice.com/en_us/article/qvwmx5/the-agency-that-messed-up-hawaiis-nuclear-alert-keeps-passwords-on-post-its-vgtrn, abgerufen am 19.11.2019
- (21) Gefängnisausbruch mittels E-Mail-Betrug, <http://www.heise.de/newsticker/meldung/Gefaengnisausbruch-mittels-E-Mail-Betrug-2587303.html>, abgerufen am 19.11.2019
- (22) Den Einzeltrick gibt's auch bei Unternehmen , <https://www.wiwo.de/erfolg/management/falsche-chefs-zocken-firmen-ab-den-einzeltrick-gibts-auch-bei-unternehmen/12201572.html>, abgerufen am 19.11.2019
- (23) Mitarbeiter von IT-Sicherheitsfirma Trend Micro verkaufte Kundendaten an Scammer , <https://www.heise.de/security/meldung/Mitarbeiter-von-IT-Sicherheitsfirma-Trend-Micro-verkaufte-Kundendaten-an-Scammer-4582172.html>, abgerufen am 19.11.2019
- (24) Locky, <https://de.wikipedia.org/wiki/Locky>, abgerufen am 19.11.2019
- (25) Die Mitarbeiter sind unsere Verteidigung, <https://www.golem.de/news/social-engineering-die-mitarbeiter-sind-unsere-verteidigung-1911-144940.html>, abgerufen am 19.11.2019

Quellen

- (26) The Original USB KeyLogger 8MB Black, <http://www.amazon.com/KeyGrabber-USB-KeyLogger-8MB-Black/dp/B004TUBOKW>, abgerufen am 24.04.2018
- (27) Pocket Jammer, <http://www.pki-electronic.com/products/jamming-systems/pocket-jammer/>, abgerufen am 24.04.2018
- (28) Mobile Mini GSM Alarmanlage Quadband mit Rückruffunktion, <https://www.amazon.de/Mobile-Alarmanlage-Quadband-Rückruffunktion-Geräuschaktivierungs-Lautstärke-Schwarz/dp/B00RC7SF8S>, abgerufen am 24.04.2018
- (29) USB Rubber Ducky, <https://hakshop.com/products/usb-rubber-ducky-deluxe>, abgerufen am 24.04.2018
- (30) How do USB killers work?, <https://www.quora.com/How-do-USB-killers-work>, abgerufen am 24.04.2018
- (31) UK police arrested the alleged mastermind of the MIRAI attack on Deutsche Telekom, <http://securityaffairs.co/wordpress/56604/cyber-crime/mirai-attack-deutsche-telekom.html>, abgerufen am 24.04.2018
- (32) Hackers demonstrated first ransomware for IoT thermostats at DEF CON, <https://www.computerworld.com/article/3105001/security/hackers-demonstrated-first-ransomware-for-iot-thermostats-at-def-con.html>, abgerufen am 24.04.2018