



Live Hacking Demo

KBZ St. Gallen

Donnerstag, 26. Oktober 2017

damian.pfammatter@compass-security.com

Cyber-Angriffe
Kriminelle erpressen Schweizer Online-Shops
 Mehr Stunden Zeitung
 Die Gruppe hatte auch die SBB attackiert.

L'HEBDO
 Politique Société Économie & Finance Culture
 BLOGS
 LE MAGAZINE
 RENCONTRES
 CONCOURS
 FORUM DES 100
 Schweizer-
 ilie.ch
 für

HEZZ AM SONNTAG | von Marco Metzler / 27.3.2016, 18:02 Uhr
 Digitec hat nach Cyber-Angriffen mittlerweile Lösegeld-Forderungen erhalten. Die Firma ist kein Einzelfall. Die Schweiz ist schlecht geschützt.
 Noch nie gab es eine so grosse koordinierte Cyber-Attacke auf Schweizer Firmen wie letzte Woche. Der Web-Shop Digitec/Galaxus hat mehrere Erpresserschreiben mit unklarem Absender erhalten, wie CEO Florian Teutheberg der «NGZ» am Sonntag bestätigt. «Wir haben umgehend Polizei und Staatsanwaltschaft eingeschaltet.» Mehr sagt er aus ermittlungstaktischen Gründen nicht. Lösegeld will man nicht bezahlen.
 In der Nacht vom 18. März auf den 19. März starteten bei Digitec die Angriffe, die zeitweise die interne IT und das Telefonsystem lahmlegten. Bei längeren Ausfällen wird die Schadenssumme schnell sechsstellig. Hinzu kommen Imageschaden und Vertrauensverluste.

Hacker knacken Zahlungs-Software
Bei Berner Firma verschwanden 1,2 Millionen Franken
 BERN - Hacker haben über Nacht 1,2 Millionen Franken von den Konten der Berner Künig Holding abgezweigt. Firma, Banken und Software-Vetreiberin streiten darum, wer schuld ist.

Hacker kapern Telefone
M-Budget-Kunden
 Angriff bei Telefondienst M-Budget: Unbekanntes ist es über die Festnetzanschlüsse von M-Budget-Kunden zu

Phishing
Post-Kunden
 Donnerstag, 9. Juni 2016, 17:10 Uhr, aktualisiert um 22:32 Uhr
 Vasilije Mustur



Kunden von Post und Postfinance haben in eine E-Mail von einem gefälschten Absender. Im Anhang wird zur Abholung eines Pakets. Dahinter verbirgt sich ein raffiniertes Virus.
 Jetzt sind Kurve Cyber-Kriminelle zeigen Kunden haben in der erhalten. Die Pakets auf
 Der Anhang versprochene Abholung beim Öffnen des Anhangs Malware installiert. Der Computer ist alsdann teilweise oder ganz ausser Gefecht.

Massangriff auf Schweizer
 Betroffen
 Mehrere Online-Shops wurden heute Opfer einer Cyber-Attacke. Es könnte ein berühmtestes Hacker-Kollektiv dahinter stecken.
 Roman Rey
 HEADLINE NEWS
 14.06.2016, aktualisiert um 11:25 Uhr, 90:00 News, 0:00 Update



450'000'000'000 \$US / Jahr



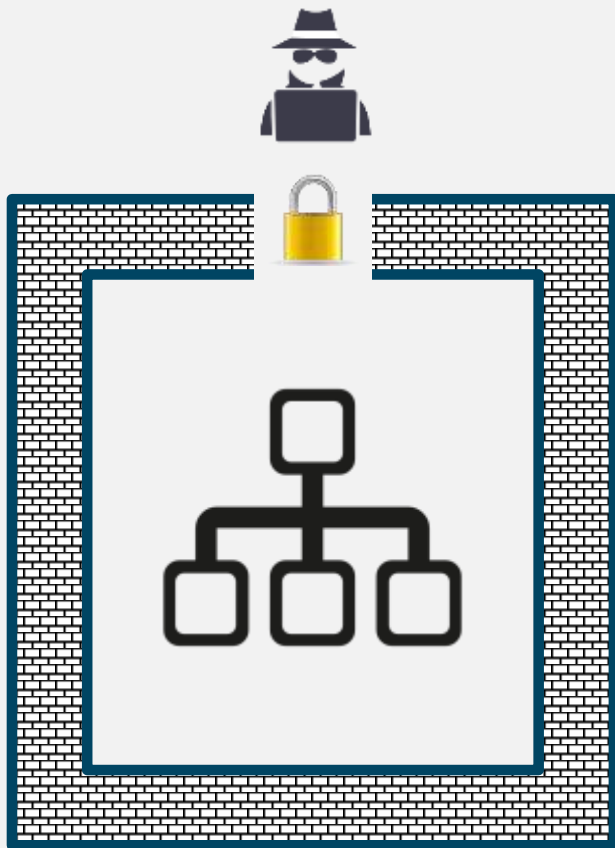
PROFIT
— HACKERS —

374'000'000 CHF / Jahr

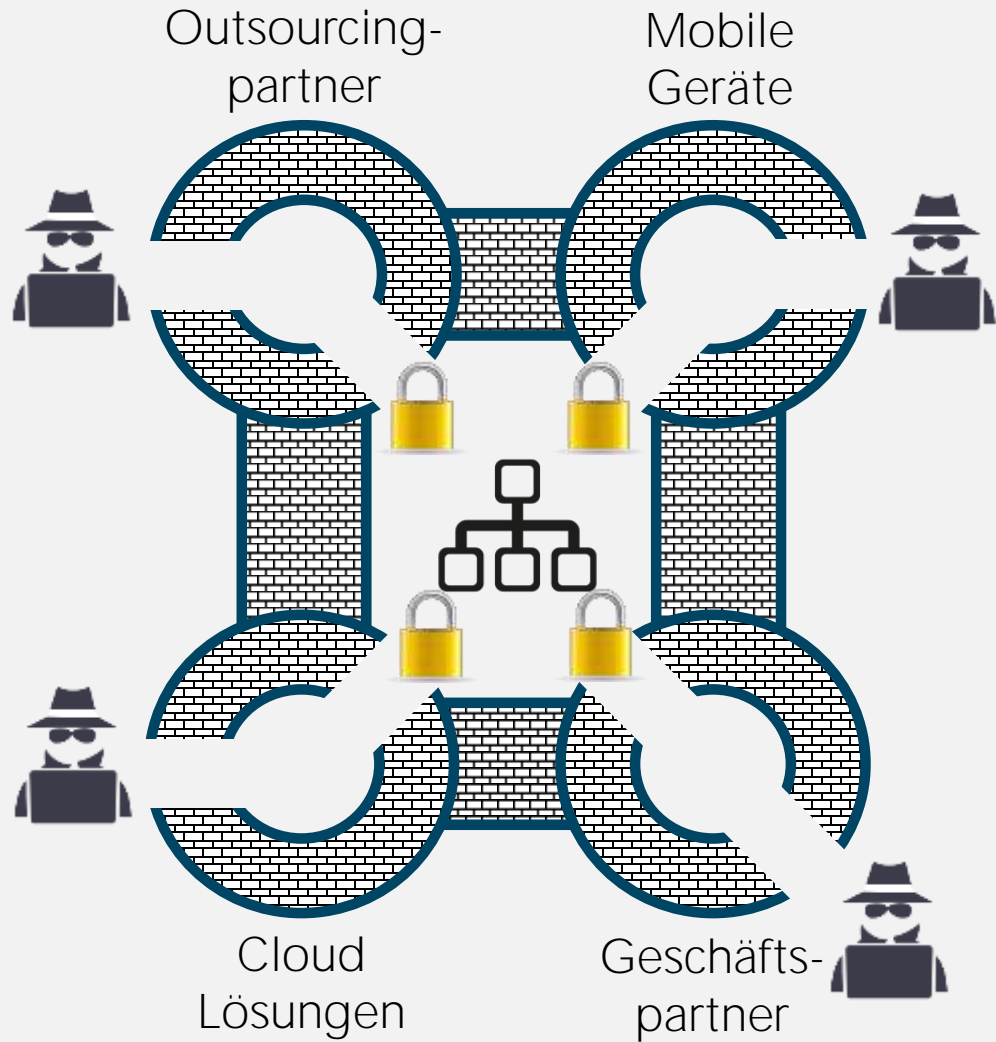


Die Welt verändert sich...

"Alte Welt"



"Neue Welt"





Wer sind
diese Hacker?

Script-Kiddies / Verärgerte Mitarbeiter

Alter

- 9 – 18 Jahre

Ziel

- Endbenutzer
- Kleine- und mittelgrosse Unternehmungen

Schaden

- Tief

Motivation / Zweck

- Um cool zu sein und anzugeben
- Seinem Ärger freien Lauf zu lassen
- Medien Aufmerksamkeit erlangen



Black Hat / White Hat

Alter

- 15 – 50 Jahre

Ziel

- Grosse Unternehmungen
- Hardware / Software / Technologie Lieferanten

Schaden

- Mittel

Motivation / Zweck

- Macht demonstrieren
- Medien Aufmerksamkeit Erlangen
- Aus Neugier und uneigennützigem Zweck
- Aus Neugier und eigennützigem Zweck



Organisierte Kriminalität / Staaten

Alter

- 18 – 50 Jahre

Ziel

- Grosse oder strategische Unternehmungen
- Regierungen, Terrorverdächtige, Individuen

Schaden

- Hoch

Motivation / Zweck

- Für Profit
- Spionage / Gegenspionage
- Überwachung, Kontrolle
- Abstürzen von feindlichen Systemen



WHY ME?

Angriffsarten

Nicht-Zielgerichtete Massen-Angriffe

- Zufällige Ziele
- Schwächstes Opfer (z.B. einfaches Passwort)
- Spam, Phishing, etc.
- Unpatched Systeme

Zielgerichtete Angriffe

- Effizient
- Typischerweise kombiniert mit Social Engineering
- Hohe Erfolgsrate

Dazwischenliegende Ziele

- Im Kreuzfeuer zwischen Angreifer und eigentlichem Ziel



Organisierte
Cyber-
Kriminalität

Cybercrime Versorgungskette



Organisation Leader

Stellt das Team zusammen und definiert die Ziele



Programmierer

Programmieren die Schadprogramme (Malware)



Hacker

Suchen und nutzen Schwachstellen in Anwenderprogrammen und Netzwerken aus



Geldüberbringer

Führen elektronische Bankkontoüberweisungen durch



Verteiler

Kaufen und verkaufen gestohlene Daten



Betrüger

Umwerben potenzielle Opfer mit "sozialen Manipulationen" wie Phishing und Spam



Geldwäscher

Waschen illegale Einnahmen mittels Überweisung an digitalen Finanzdienstleister



Tech. Experten

Pflegen und unterhalten die Infrastruktur der kriminellen Unternehmen



Kassier

Überwachen geknackte Konten und liefern gegen Gebühr Kontenangaben an andere Kriminelle



Hosted System Provider

Bieten illegale Server an

The image features a person wearing a dark hoodie, positioned centrally. The background is a dark blue-green gradient with vertical columns of white and light blue binary code (0s and 1s) falling from the top, reminiscent of the 'Matrix' digital rain effect. A solid green horizontal band is overlaid across the middle of the image, containing the text 'Live Hacking Demos' in white. The overall aesthetic is technical and digital.

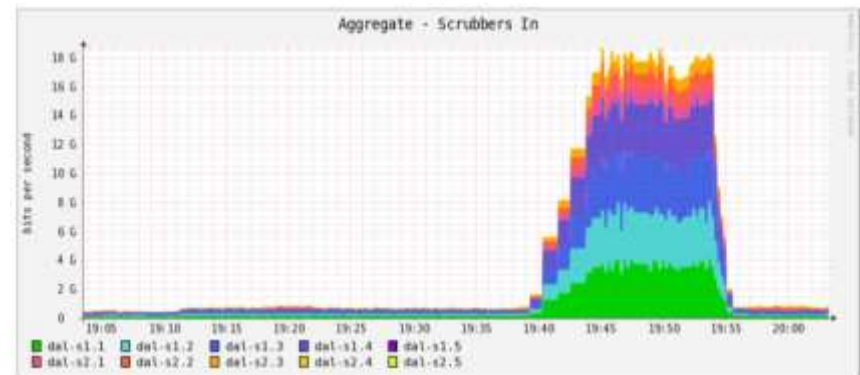
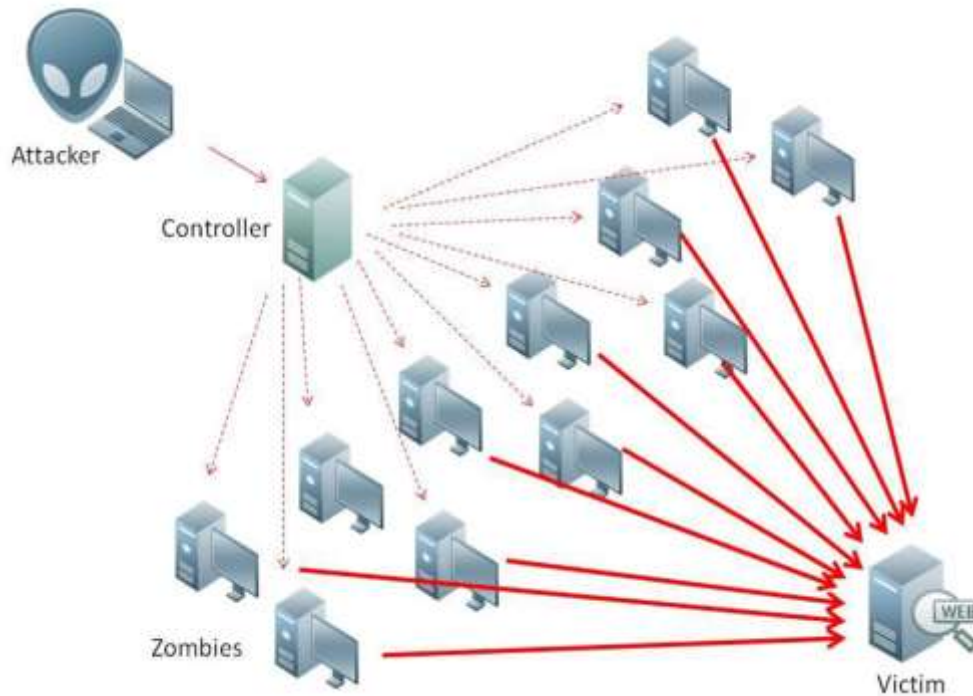
Live Hacking Demos



DDoS

Eine riesige Armee
kleiner Geräte

Distributed Denial of Service (DDoS)



"Network Stressers"

The image shows a screenshot of a website's pricing and features page. On the left, a pricing card for a '1 Month Bronze' plan is partially visible, showing a price of '\$10.00 /month' and an 'Order Now' button. The main content area is titled 'Our Pricing' and 'FEATURES'. The 'FEATURES' section is divided into three columns: a list of features on the left, 'Excellent Stress Testing Services!' in the middle, and 'Instant Attacks!' on the right. The bottom of the page features a silhouette of a city skyline.

Our Pricing

FEATURES

1 Month Bronze

\$10.00
/month

1 Concurrent +

300 seconds boot time

250Gbps total network capa

Resolvers & Tools

24/7 Dedicated Support

[Order Now](#)

- Unlimited Testing
- Great User Experience
- 24/7 Live Support
- Easy Customizable
- Flexible Pricing
- VIP Support
- Affordable Plans

Excellent Stress Testing Services!

With Rage Booter, you never have to worry about power! We monitor our servers 24/7 to provide you a pure and strong attack to any target.

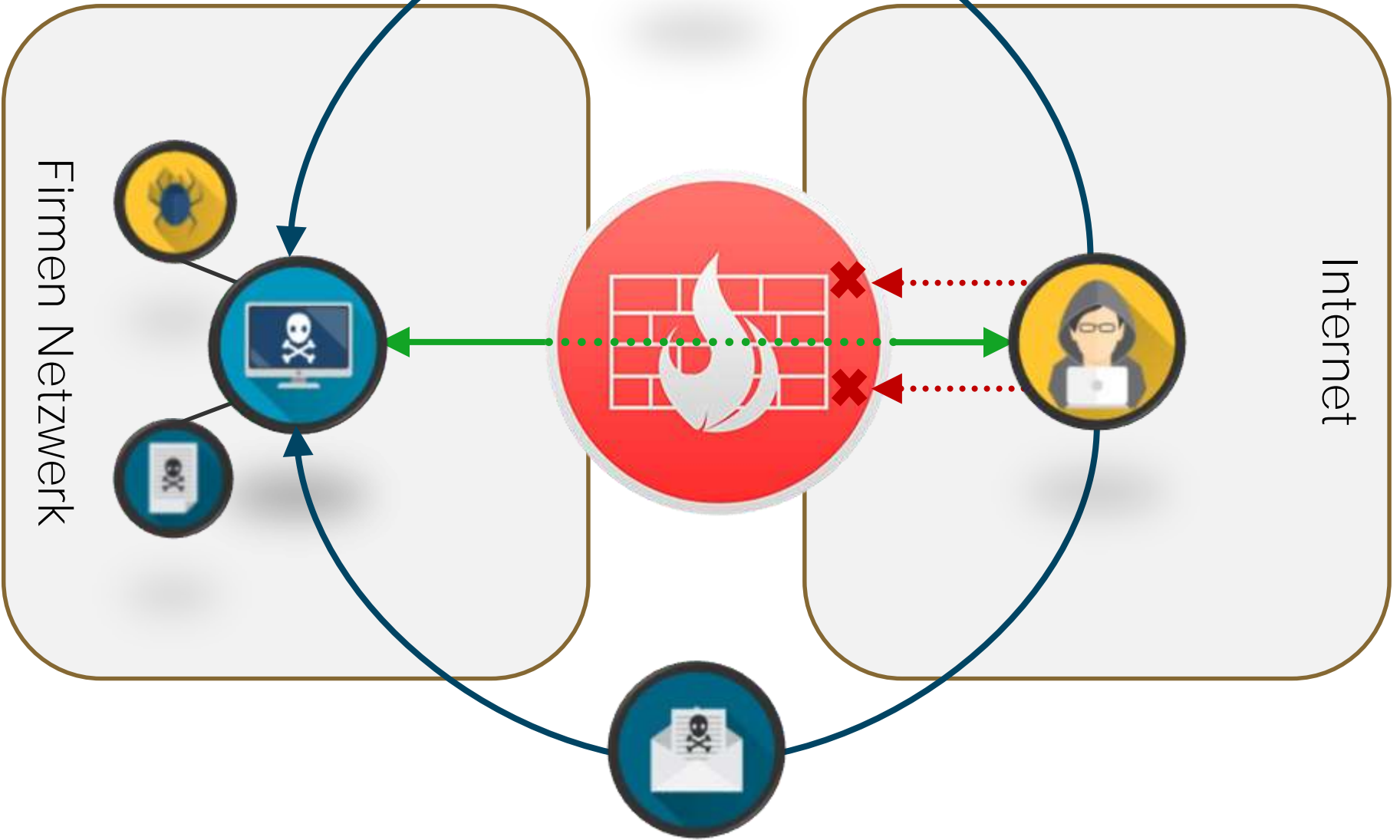
- ✓ Fast and Secure Stress Testing!
- ✓ Ticket & Live Support!
- ✓ A Variety of revolvers from Cloudflare to Skype, we have it all!
- ✓ We have been open since 2010 so you can feel peace at mind that we are not going anywhere!

Instant Attacks!

Unlike other stressers who use SSH2, We utilize IRC (Internet Relay chat) to send all attacks. Attacks are instant and sent fast using this.



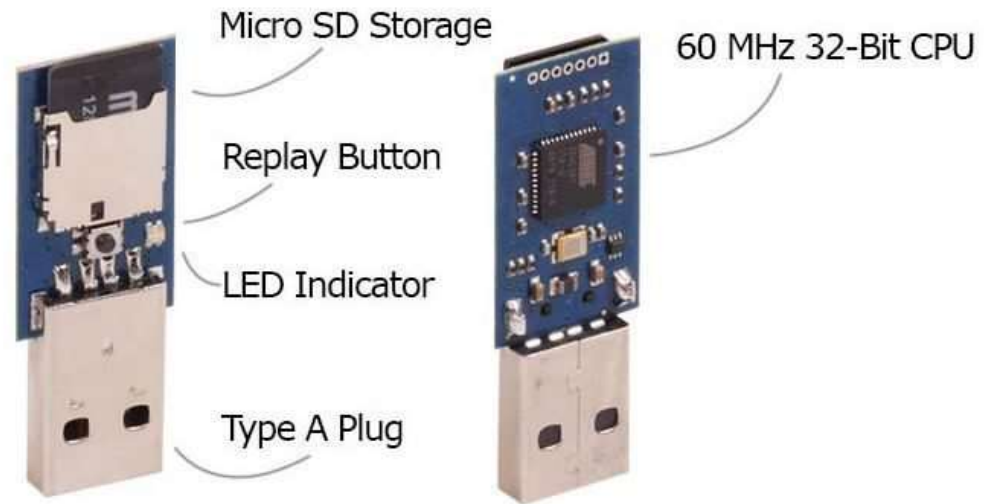
“Verlorener”
USB Stick



Firmen Netzwerk

Internet

“Wenn es wie eine Tastatur quakt...
...muss es eine Tastatur sein.”





SMShing &
Vishing



Gegenmassnahmen

Schutzmassnahmen für Unternehmungen

- Bewusstsein zu Sicherheitsproblemen und Bedrohungen erhöhen
- Mitarbeitende in Ausbildungsprogrammen schulen
- Klare Richtlinien für soziale Medien etablieren
- Sensible Daten verschlüsseln
- Schutzsysteme für Hard- und Software aktuell halten
- Gute Passwort-Richtlinien durchsetzen



Schutzmassnahmen für Privatpersonen

- Verschiedene Passwörter für unterschiedliche Online-Dienste
- Passwort-Manager gebrauchen
- Software regelmässig aktualisieren (OS, Browser, Java, Flash, ...)
- Aktuelles Anti-Virus Programm verwenden
- Eingehende Email kritisch hinterfragen (Phishing)
- Absender von Emails, SMS, etc. nicht blind vertrauen



CONCLUSIONS

A.

B.

C.



The background of the slide is a dense, monochromatic pattern of interlocking gears of various sizes and orientations, creating a complex, mechanical texture. The gears are rendered in shades of gray and black, with highlights and shadows that emphasize their three-dimensional form.

Cyberkriminalität ist hoch organisiert

und

Profit orientiert

Einfache und profitable Ziele werden attackiert



Sei nicht die "Low-Hanging Fruit"!



Danke für die Aufmerksamkeit



Damian Pfammatter
IT Security Analyst
damian.pfammatter@compass-security.com

Compass Security Schweiz AG
Werkstrasse 20, Postfach 2038, CH-8645 Jona
T +41 55 214 41 75, F +41 55 214 41 61