Unveiling the Inner Workings of a Cybercriminal in Your IT-System

Perspektive eines „White-Hat-Hackers“

vodafone enterprise plenum

VITA, STORY & STATIONEN

ProSec
Security redefined.

2016 | #START #SONNENSTUDIO

PROSEC_STORY

B0104 Wirtschaft_k, 14.01.2016 11:56:26 - Benutzer: luit - PROOF

„Gute“ Hacker wollen Betriebe beschützen

Netzwelten Koblenzer setzen Geschäftsidee um

Von unserem Mitarbeiter
Reinhard Kallenbach

Lahnstein/Koblenz. Als Kinder träumten sie davon, Hacker zu werden. Doch dann setzte sich die Vernunft durch. Tim Schughart (24) und Immanuel Bär (34) wollten zu den Guten gehören und Unternehmen dabei helfen, Schwachstellen im Netz aufzuspüren. Und dazu bedarf es besonderer Kenntnisse und Software. Beides vermarkten die beiden Existenzgründer über ihr Koblenzer Unternehmen ProSec Networks. Obwohl es den Betrieb erst seit vier Jahren gibt, ist die Liste der Referenzen bereitsbeachtlich.

„Niemand schickt seine Briefe ohne Umschlag um die Welt“, sagt Tim Schughart und ergänzt, dass das, was für die klassische Post gilt, noch lange nicht in der virtuellen Welt angekommen ist. Das heißt: Viele Unternehmen machen es Unbefugten leicht, die hauseigenen Systeme oder internetbasierte Dienstleistungen zu „entern“, Daten und Passwörter abzusaugen – oder ein zerstörerisches Werk anzurichten. Schon die finanziellen Folgen sind verheerend. Beide verweisen auf Unter-

> „Wir sind angetreten, um IT-Sicherheit neu zu definieren.“
>
> Tim Schughart und Immanuel Bär von der jungen Koblenzer Firma ProSec networks.

einen Hintergrund: menschliches Versagen, wobei das Verhalten der jeweils zuständigen Sachbearbeiter keinesfalls fahrlässig sein muss. „E-Mails mit Schadsoftware sehen heute so aus, dass sie sich kaum von normalen E-Mails unterscheiden“, erklärt Immanuel Bär, der fast zehn Jahre lang bei der Hack AG in Kurtscheid Systemadministrator war. Der gelernte Informatikkaufmann ist heute der Generalist bei ProSec Networks, während der Gründer Tim Schughart, ein gelernter Fachinformatiker, sich um die ganz speziellen Herausforderungen kümmert. Arbeit gibt es für beide genug. Jeden Tag gelangen 350 000 neue Schädlinge ins Netz. „Das ist für die Hersteller von Antivirensoftware ein Katz-und-Maus-Spiel – auch wenn sie sich untereinander austauschen“, meint Tim Schughart. Das heißt: Programmierer mit bösen Absichten haben immer einen leichten Vorsprung – auch wenn die Hersteller von Antivirensoftware in der Regel schnell reagieren, bleibt immer eine Zeitspanne, in der Schadsoftware ihre Wirkung entfalten kann.

Für Unternehmen mit sensiblen Daten bedeutet das: Sie müssen

Tim Schughart (vorne) und Immanuel Bär haben sich dem Kampf gegen „böse“ Hacker verschrieben. Sie selbst wollen die „Guten“ sein. Foto: Kallenbach

der, die im Rahmen eines Expertennetzwerks agieren, bedeutet Unternehmen geradezu rosige Wachstumsperspektiven. Und die Auch wenn sich die beiden Unternehmer in erster Linie an mittlere Daten, die ein Kunde hinterlässt, „nach Stand der Technik“ zu ver-

2022

TODAY_PROSEC

2023

ProSec Heute - international

Durch mittlerweile weltweites Engagement in der Bekämpfung von Hackergruppierungen an der Seite von Regierungen, westlichen Nachrichtendiensten, staatlichen Strukturen und Konzernen gelingt der internationale Durchbruch. Teilaspekt hiervon ist auch der globale Ukraine Konflikt.

t3n digital pioneers

Über t3n Jobs bei t3n

Feature

Targeted by Killnet: This early warning system protec from DDoS attacks

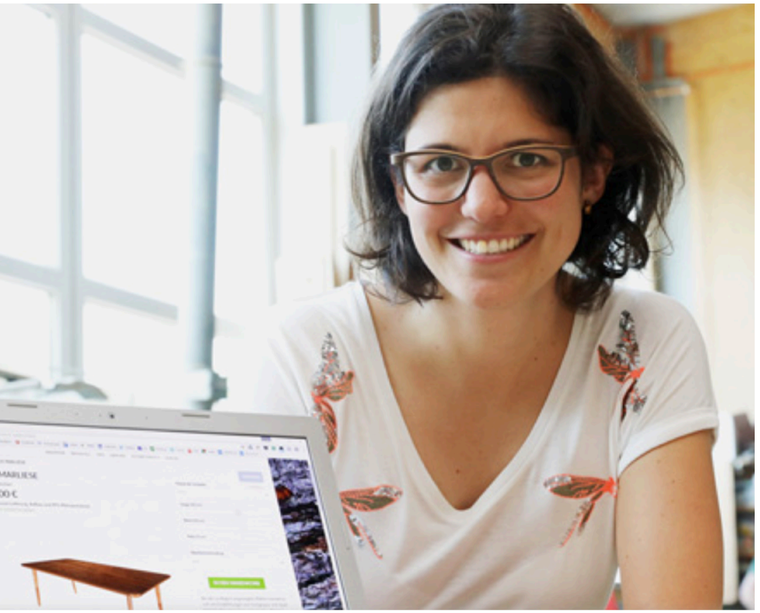
In the Ukraine conflict, German web servers are also being targeted A new early warning system is now intended to protect website ope

Von **Kim Rixecker**

07.06.2022, 14:00 Uhr • 3 Min. Lesezeit

Killnet and Co: How coordinated DDoS attacks can be detected i

2020 | #KMU #MITTELSTAND #KRITIS



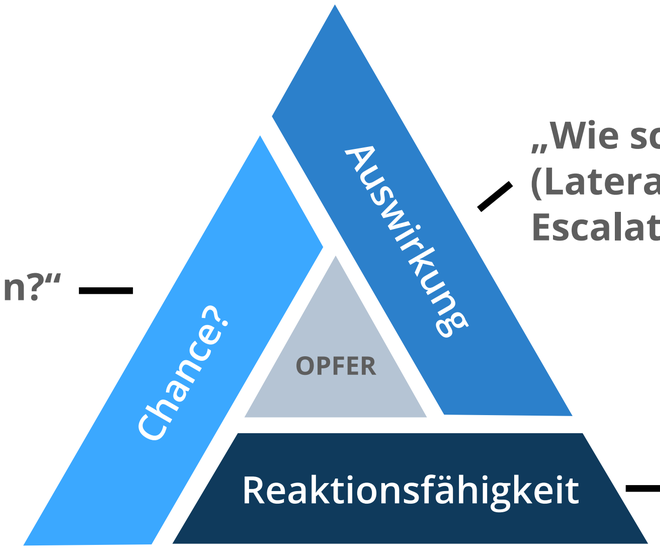
ProSec
Security redefined.

ANGRIFF | THEORIE „HIGH LEVEL“

ProSec
Security redefined.

HACKEN - HANDELN - RESILIENZ!

(EINTRITTSRISIKO | AUSWIRKUNG | REAKTIONSFÄHIGKEIT)



„Wie schnell komme ich da rein?“

„Wie schnell kann ich „eskalieren“? (Lateral Movement, Privilege Escalation, Exploitation etc.)

Detektionsfähigkeit, Reaktionsfähigkeit, Mensch, Prozesse?

Denkweise des Angreifers..

ANGRIFF **FELDER?**

#IT_SICHERHEIT

ANGRIFF_FELDER

Merke FELDER!

PHYSICAL SECURITY

TECHNICAL SECURITY

„FAKTOR MENSCH“

ProSec
Security redefined.

ANGRIFF_ZIELE

Merke ZIELE!

Die Lage der IT-Sicherheit in Deutschland 2022 im Überblick

Top 3-Bedrohungen je Zielgruppe:

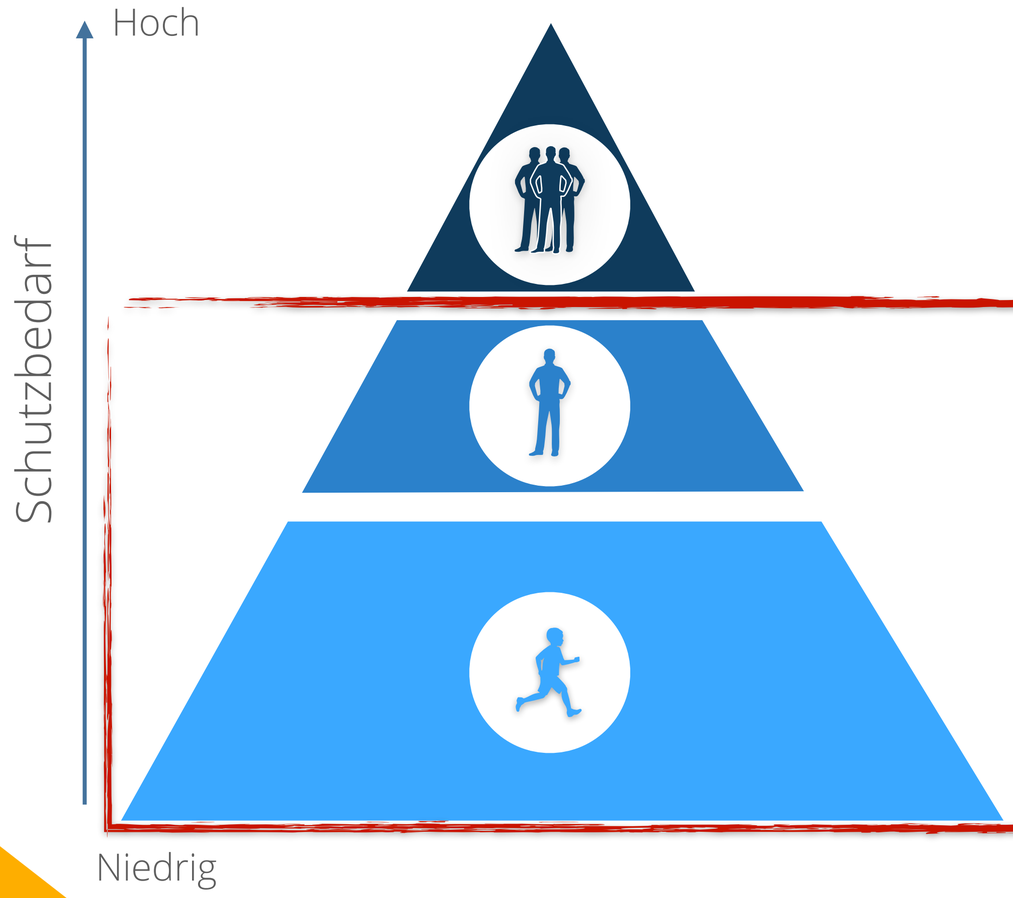
Gesellschaft	Wirtschaft	Staat und Verwaltung
		
Identitätsdiebstahl Sextortion Fake-Shops im Internet	Ransomware Schwachstellen IT-Supply-Chain: Abhängig	Ransomware APT Schwachstellen, offene oder falsch konfigurierte Online-Server

ProSec
Security redefined.

ANGREIFER_GRUPPEN

Govermental Layer

...



Industry Intelligence (APT´s)

Schleusen Mitarbeiter ein und attackieren Zulieferketten

Technical Attacker

Nutzen Social Engineering (Faktor Mensch) + X

Script-Kiddie

Nutzen Fertige Scripts und Frameworks

Merke GRUPPEN!

ProSec
Security redefined.

ANGRIFF | THEORIE & PRAXIS

ProSec
Security redefined.

PHYSICAL „WLAN“

PHYSICAL
SECURITY

ProSec
Security redefined.

PHYSICAL „DUMPSTER DIVING“

PHYSICAL
SECURITY

ProSec
Security redefined.

ANGRIFF | KILLCHAIN „CLASSIC“

ProSec
Security redefined.

ABLAUF EINES ANGRIFFS

Informationsbeschaffung

- Sammeln von relevanten Informationen
- Betrachtung des Unternehmens aus Angreifersicht

Schwachstellen Analyse

- Bestimmung von potenziellen Schwachstellen in Netzwerken, Komponenten, mobilen Endgeräten und Anwendungen
- Researching Exploitcode

- Entry Point Analyse & Social Engineering Analyse
- Einstufung von Cyber-Bedrohungen

Threat modeling

ABLAUF EINES ANGRIFFS

Exploitation

- Schwachstellen kontrolliert ausnutzen, um Zugr
  Systeme zu erhalten oder diese beeinträchtig
- Schutzmaßnahmen aushebeln

Monetarisierung

- Bewertung der Daten z.B. zur Wertermittlung & Höhe Lösegeldforderung
- Kontaktaufnahme mit Opfer oder Interaktion
- Einleitung weiterer krimineller Folgeszenarien

- Prüfung der Festsetzungsmöglichkeiten
- Verschleierung der Angriffe und Spuren
- Prüfung der Ausbreitungsmöglichkeiten

Post exploitation

Technical Attacker | **Technik & MENSCH**

CASE APOTHEKE | ERGEBNIS

vodafone enterprise plenum

ProSec
Security redefined.

Dr. Wolfgang Schlags

Apotheker| Modell*

In 4. Generation

Jahresumsatz **2022 | ca. 45Mio €**

Alle Filialen des Familien Verbundes gesamt!

ProSec
Security redefined.

Business KPI´s

Reichskronen-Apotheke in Mayen | **2004**

Hauptapotheke, Leitung Dr. Wolfgang Schlags

Dr. Schlags-Apotheke in Koblenz | **2007**

Filiale der Reichskronen-Apotheke

Adler-Apotheke in Mendig | **2011**

Hauptapotheke, Leitung Dr. Irina Schlags

Marien-Apotheke in Ochtendung | **2011**

Filiale der Reichskronen-Apotheke

Marien-Apotheke in Ochtendung | **2011**

Filiale der Reichskronen-Apotheke

St. Barbara-Apotheke Dr. Schlags | **2019**

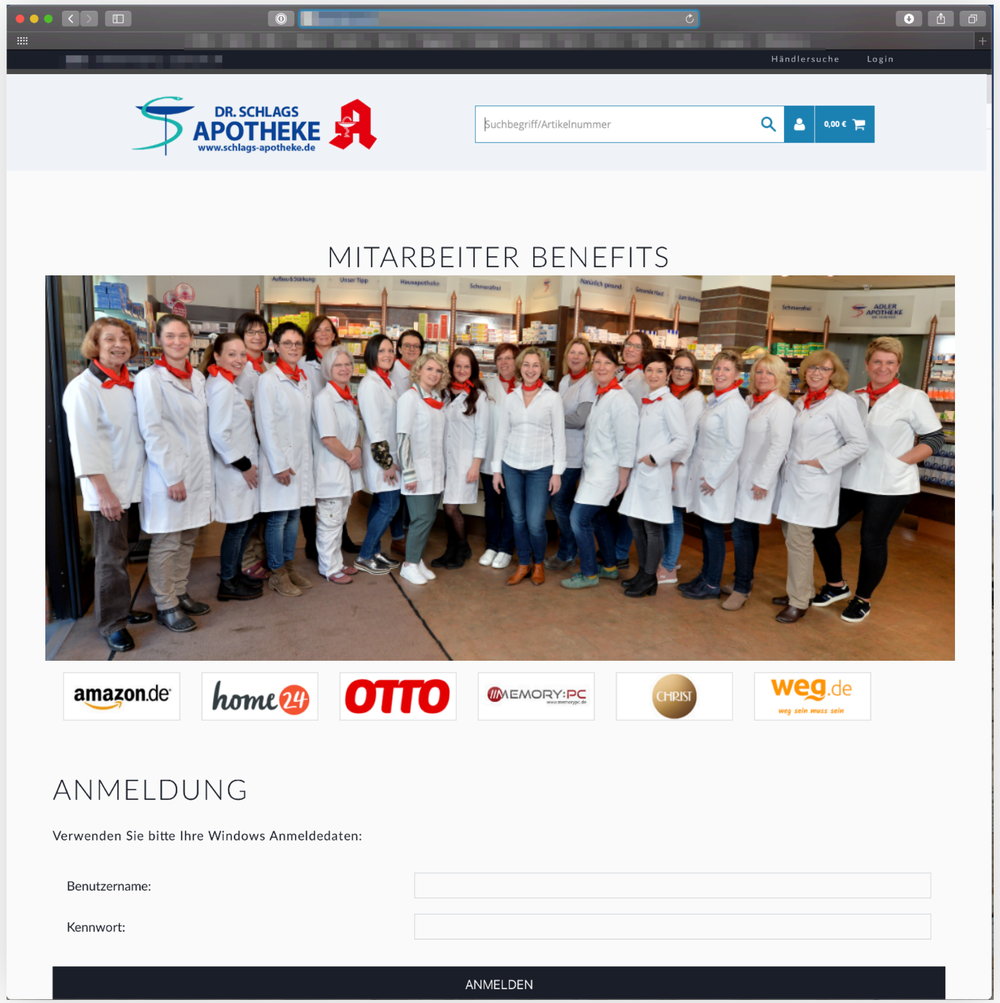
Filiale der Adler-Apotheke

Schwanen-Apotheke Dr. Schlags | **2021**

Filiale der Adler-Apotheke

Exemplarisch!

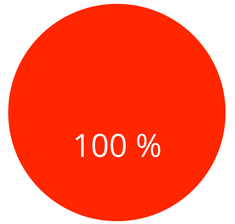
FAKTOR MENSCH - BEISPIEL EVENT & BONUS



REALISMUS NAH..!

Alle Teilnehmer erhalten eine Mail zur Einführung eines Benefit Portals mit der Aussicht auf Gutscheine und Rabattierungen. Das Potential dieser Attacke ist aufgrund eines Sachwerts und dem meist persönlichen Interesse sehr hoch. Ziel ist die Eingabe der Benutzeraccounts im Browser.

Die Erfolgswahrscheinlichkeit bei bisherigen Tests liegt derzeit bei:



Legende

Erfolgreich in Prozent

Nicht Erfolgreich in Prozent

ProSec
Security redefined.

BM

Burgfestspiele Mayen <info@tickets-burgfestispiele-mayen.de>

Gestern um 09:07

An: Christian Horn

Wir freuen uns Ihnen mitteilen zu können, dass wir aufgrund der positiven Resonanz und der aktuellen Situation für kurze Zeit Rabattcoupons zur Verfügung stellen. Diese Coupons können Sie entweder bei der Bestellung von Tickets oder aber beim Einlass zu den Verantstaltungen vorzeigen um bis zu 15€ zu sparen. Besuchen Sie einfach unsere Seite um die Coupons zu erhalten.

https://tickets-burgfestspiele-mayen.de

Wir freuen uns, Sie bei den Vorstellungen begrüßen zu dürfen.

Mit freundlichen Grüßen

Ihr Team der Bugfestspiele Mayen

Mail: info@tickets-burgfestspiele-mayen.de
www.burgfestspiele-mayen.de
www.facebook.com/BurgfestspieleMayen

Senden

CC/BCC

Optionen

Sehr Böse Hackerin

PHISHING MAIL
Faktor Mensch

APOTHEKE

ProSec
Security redefined.

Startseite – Burgfestspiele Maye

https://tickets-burgfestspiele-mayen.de

BURGFESTSPIELE mayen

HOME | ÜBER UNS | TEAM | SPIELPLAN 2021 | SPIELZEIT 2021 | TICKETS | SERVICE | CORONA INFO | KONTAKT

NUR FÜR KURZE ZEIT HABEN SIE DIE MÖGLICHKEIT ZU SPAREN!

Laden Sie den Rabatt-Coupon auf Ihr Smartphone herunter, drucken den Rabatt-Coupon aus und zeigen Sie ihn beim Einlass vor oder lösen Sie den Coupon-Code während der Ticket-Bestellung ein.

Je nach Ticket können Sie bis zu 15€ sparen.

Suchen …

Sehr Böse Hackerin

PHISHING MAIL
Faktor Mensch

APOTHEKE

ProSec
Security redefined.

SPEXBOX Konfiguration | fax_20210705_142307_(002655

10.41.66.117

SPEXBOX

Administrator
Sie sind angemeldet.

Abmelden

SPEXBOX Konfiguration

Start | Anrufliste | Faxversand | Telefonbuch | Nebenstellen | Accounts | Zugangsdaten | Konfiguration

Rezeptanforderung

Medikamentenbedarf für den Zeitraum bis 25.07.2021

[redacted]

Einrichtung: Caritaszentrum St. Johannes, Station 2

Medikament	Dosierung	letzte Pack.	Kommentar
KALINOR RETARD P (HKP)	Täglich 0-1-0-1-0 St	100 St	
XARELTO 15MG (FTA)	Täglich 0-1-0-0-0 St	98 St	

[redacted]

Einrichtung: Caritaszentrum St. Johannes, Station 3

Medikament	Dosierung	letzte Pack.	Kommentar
TORASEMID AL 10MG TABL (TAB)	Täglich 0-1-0-0-0 St	100 St	

[redacted]

Einrichtung: Caritaszentrum St. Johannes, Station 2

Medikament	Dosierung	letzte Pack.	Kommentar
FLECAINID 1A PHARMA 100MG (TAB)	Täglich 0-1-0-1-0 St	100 St	
RAMIPRIL HEXAL 1.25MG (TAB)	Täglich 0-1-0-0-0 St	100 St	

Sehr Böse Hackerin

VS.

APOTHEKE

ProSec
Security redefined.

HACKING & **KRIEG?**

ProSec
Security redefined.

Ethical Hacking.....

ProSec
Security redefined.

Mögt Ihr Schokolade..?

ProSec
Security redefined.

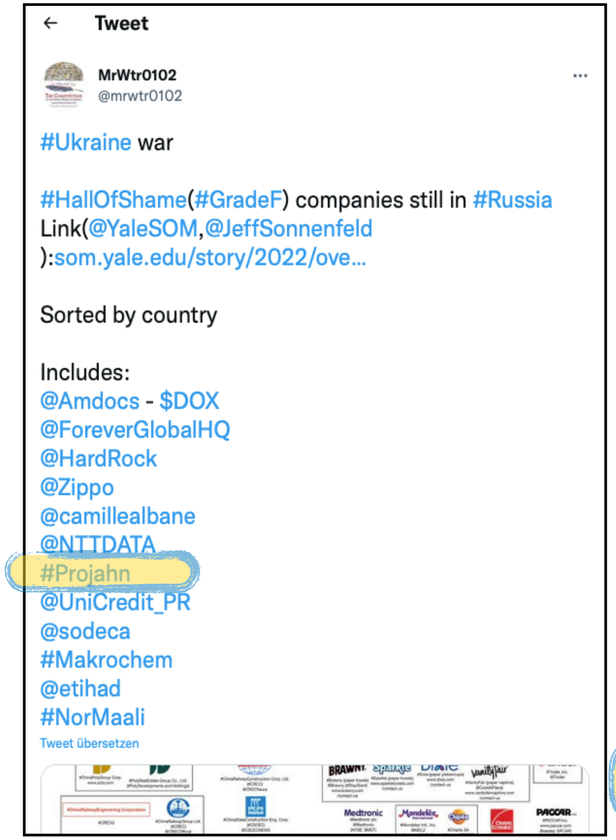
Kunde bei ner Raiffeisen BANK..?

ProSec
Security redefined.

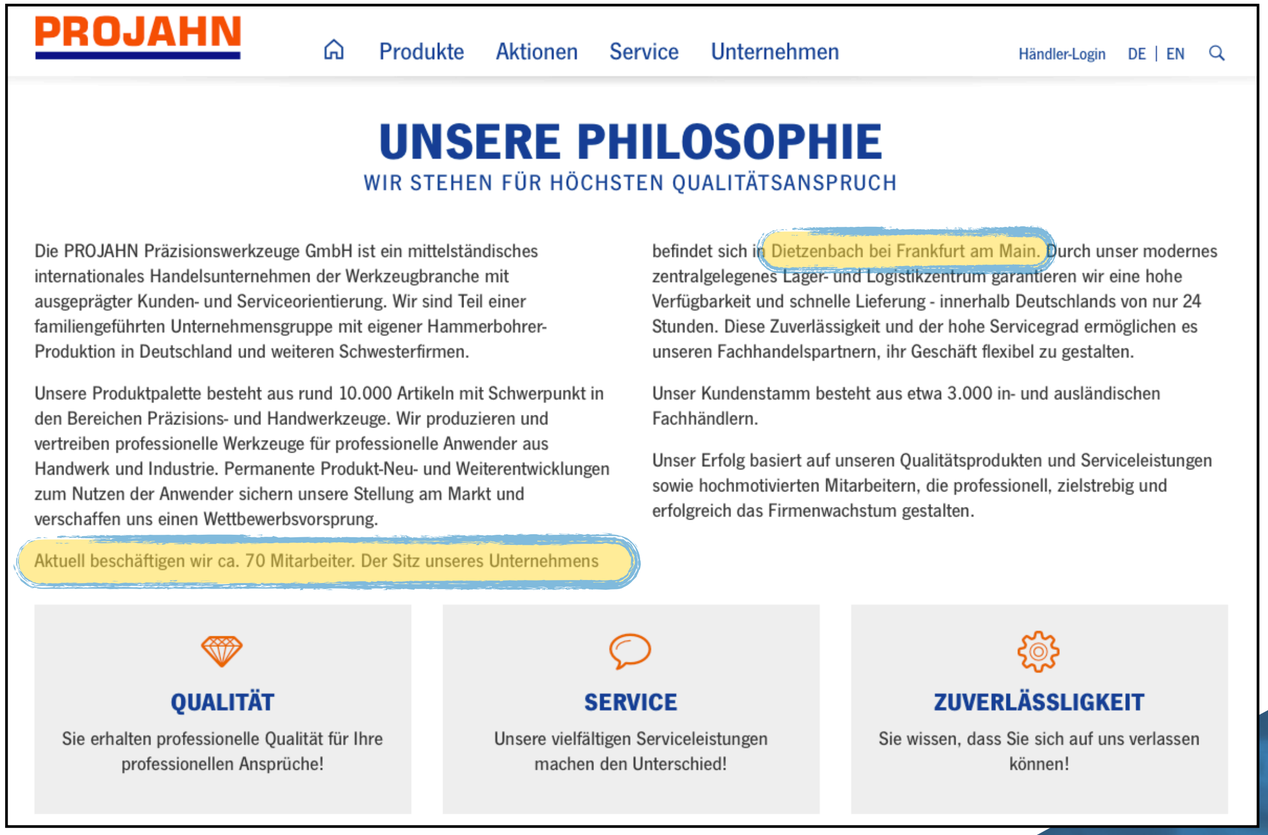
Was mit IT „zu tun“..?

ProSec
Security redefined.

Tweet unter „#bloodytrade & #projahn“



Webseite & Unternehmen „dahinter“



#KMU | #Projahn | 70 Mitarbeiter

ProSec
Security redefined.

- „Hack and Publish“
- „Hack and Leak“

- **„Publish and HACK!“**

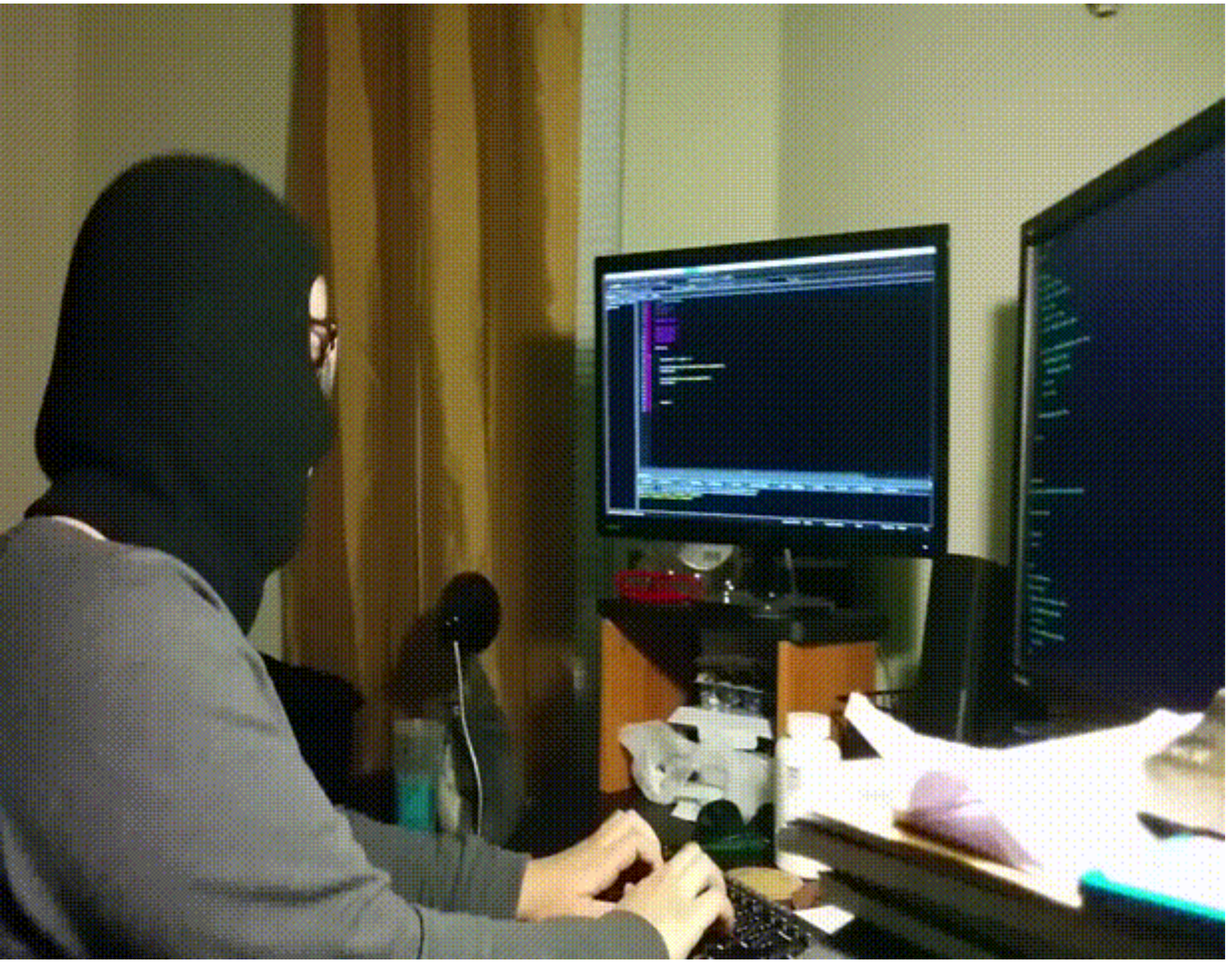
#RECAP_MAIN

vodafone
enterprise
plenum

ProSec
Security redefined.

RE_CAP_PART

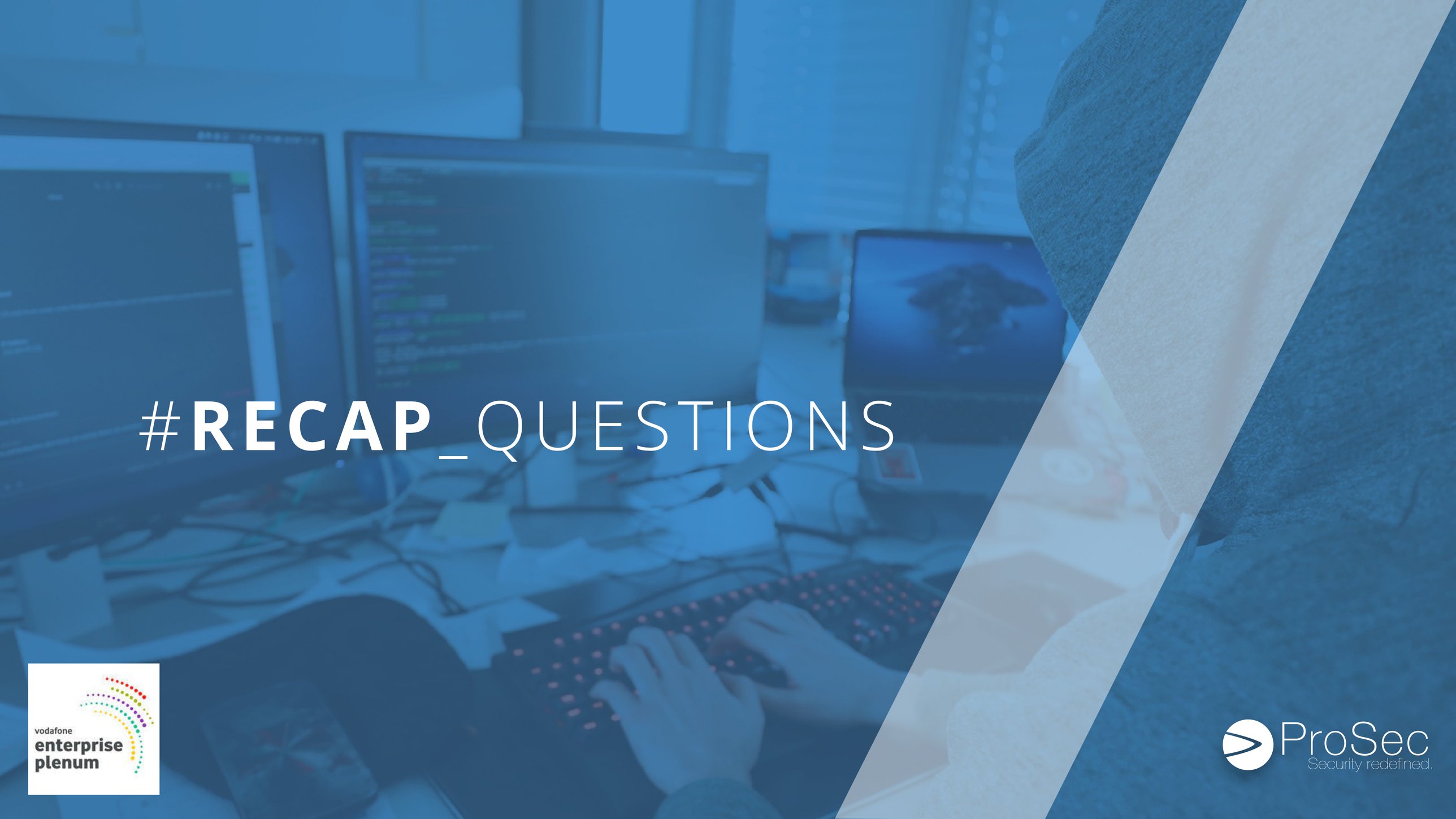
CHANCE MINSET | ..WER SOLL MICH DENN HACKEN??



#SecByDesign

4 REAL!

ProSec
Security redefined.



#**RECAP**_QUESTIONS

vodafone
enterprise
plenum

ProSec
Security redefined.

#**RECAP**_QUESTIONS

„Bottom Up“ & **echter Angriff** auf Mensch_Tec?

.....

Kommunikations- & Fehlerkultur transparent -
„vom Azubi bis Aussendienst“?!

.....

RED BUTTON - habt Ihr einen Knopf „überall & mobil“?

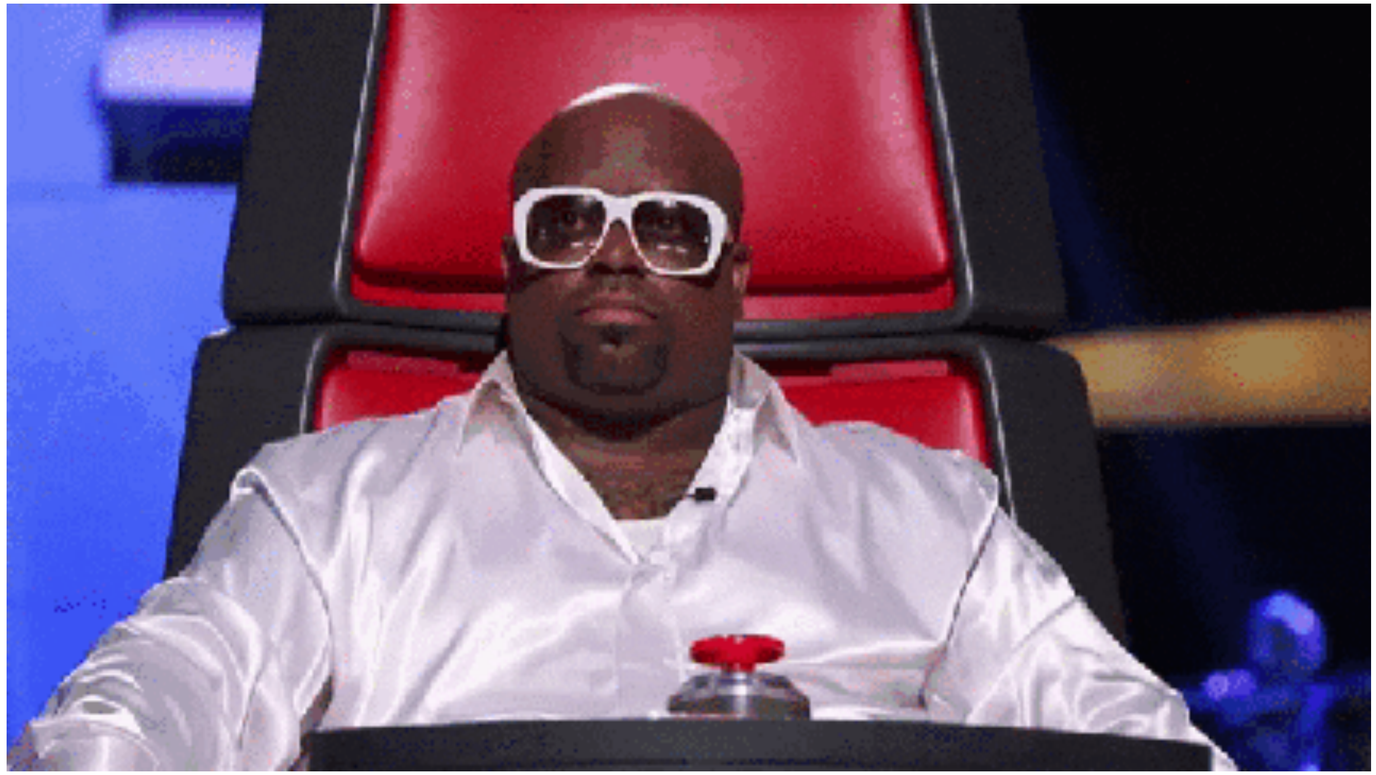
#**RECAP**_4_ADVISORIES

vodafone
enterprise
plenum

ProSec
Security redefined.

RE_CAP_PART

#ADVISORIES | **MYTHOS SCHUTZ DURCH LÖSUNG**



#Red_Button

#Spezialist

ProSec
Security redefined.

RE_CAP_PART

#ADVISORIES| SECURITY_BY_DESIGN VS. „BILLIG“

#Cheap_Security

COST

#High_Cost

ProSec
Security redefined.

„2023 MUSS NIEMAND MEHR EINEN **FATALEN CYBERANGRIFF** ERLEIDEN..!“

#RECAP STATEMENT

vodafone enterprise plenum

ProSec
Security redefined.

GERNE **„ASK MY ANYTHING..!“**

n alle Cyberangriffe existiert ein Gegengift“

de • Lesedauer: 2 Min.

weitere Personen 6 Kommentare • 3 direkt geteilte Beiträge

Angebot für Teilnehmer!

Immanuel Bär | Ethical-Hacker | **KONTAKT** & LinkedIN Code!

linkedin

WWW

ProSec
Security redefined.