

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

Perspektive eines „White-Hat-Hackers“



brennw

VITA, STORY & STATIONEN

A blurred background image of a person working at a computer in what appears to be a control room or security station. The person is seen from the side, wearing a dark hoodie. In front of them are several computer monitors displaying various data and code. The overall atmosphere is professional and tech-oriented.



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 bereits beachtlich.

„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 Unternehmen, die in einem Schad-

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 Kürscheid Systemadministrator war. Der gelernte Informationskaufmann 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 alle Angriffe abwehren. Schad-

der, die im Rahmen eines Expertennetzwerks agieren, bedeutet Unternehmen geradezu rosige Wachstumsperspektiven. Und die Kölner wollen die entsprechenden Unternehmen anmitteln.

Auch wenn sich die beiden Unternehmen, die ein Kunde hinterlässt, „nach Stand der Technik“ zu verhalten scheinen, kann es doch vorkommen, dass sie Fehler machen. Und



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

Foto: Kallenbach



ProSec
Security redefined.

TODAY_PROSEC

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.

2022

2023

t3n digital
pioneers



Über t3n ▾ Jobs bei t3n



Feature

Targeted by Killnet: This early warning system protects 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

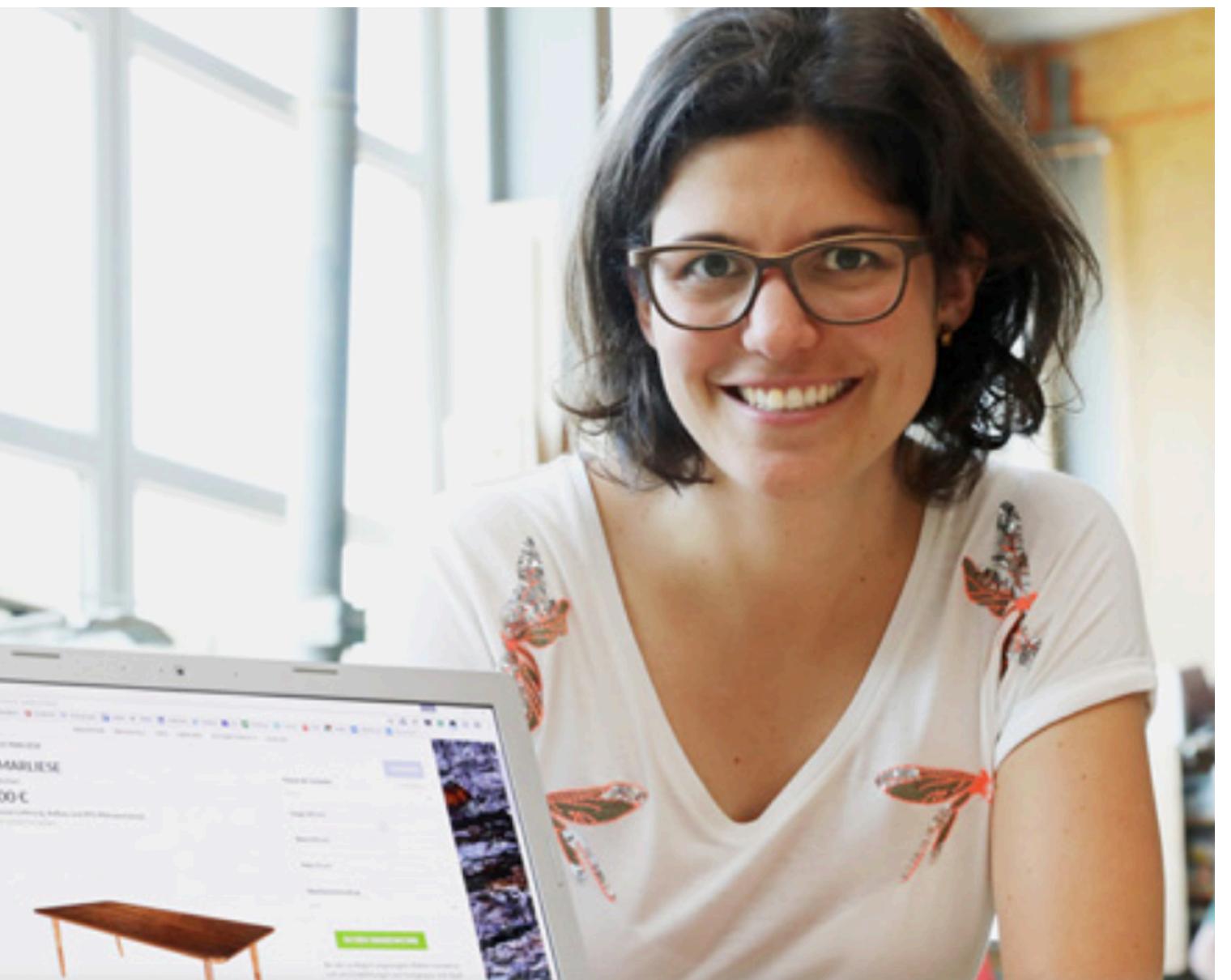
Von Kim Rixecker

07.06.2022, 14:00 Uhr • 3 Min. Lesezeit



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

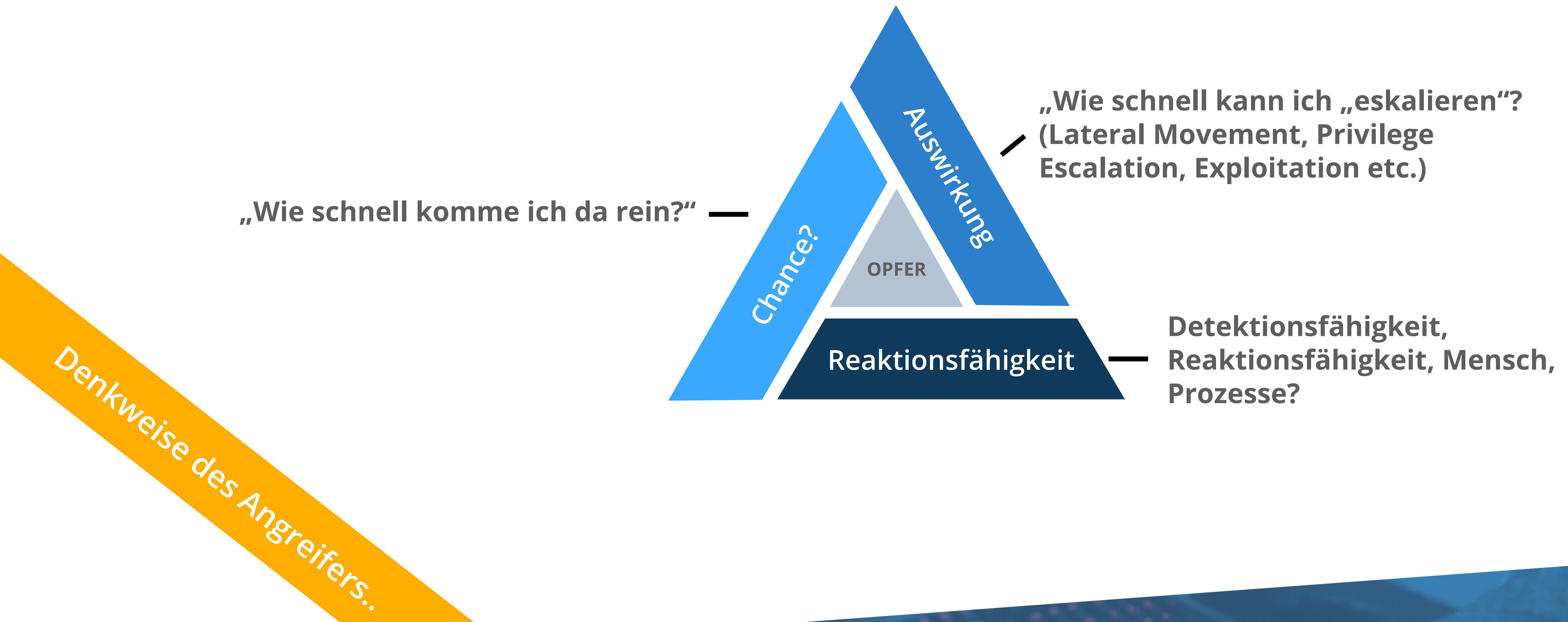
2020 | #KMU #MITTELSTAND #KRITIS



ANGRIFF | THEORIE „HIGH LEVEL“

HACKEN - HANDELN - RESILIENZ!

(EINTRITTSRISIKO | AUSWIRKUNG | REAKTIONSFÄHIGKEIT)





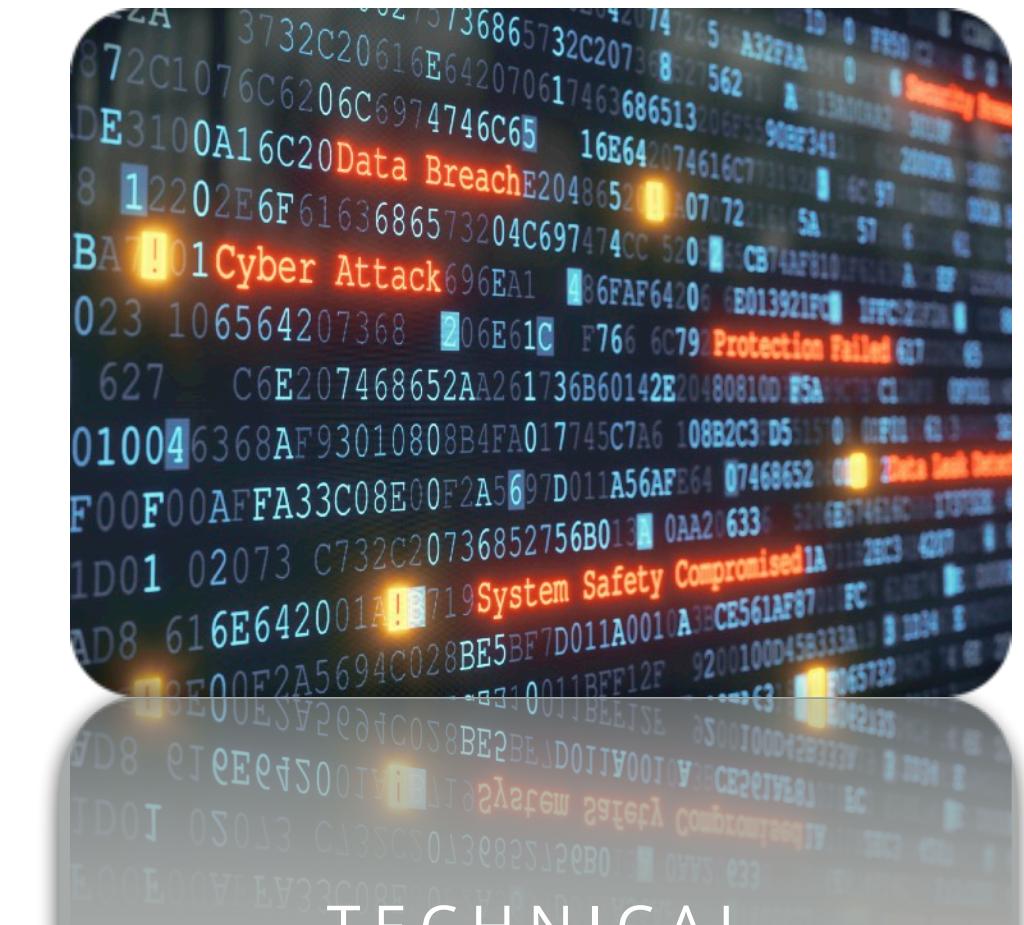
ANGRIFF FELDER?
#IT_SICHERHEIT

ANGRIFF_FELDER

Merke FELDER!



PHYSICAL
SECURITY



TECHNICAL
SECURITY



„FAKTOR
MENSCH“



ANGRIFF_ZIELE

Merke ZIELE!

Die Lage der IT-Sicherheit in Deutschland 2022 im Überblick

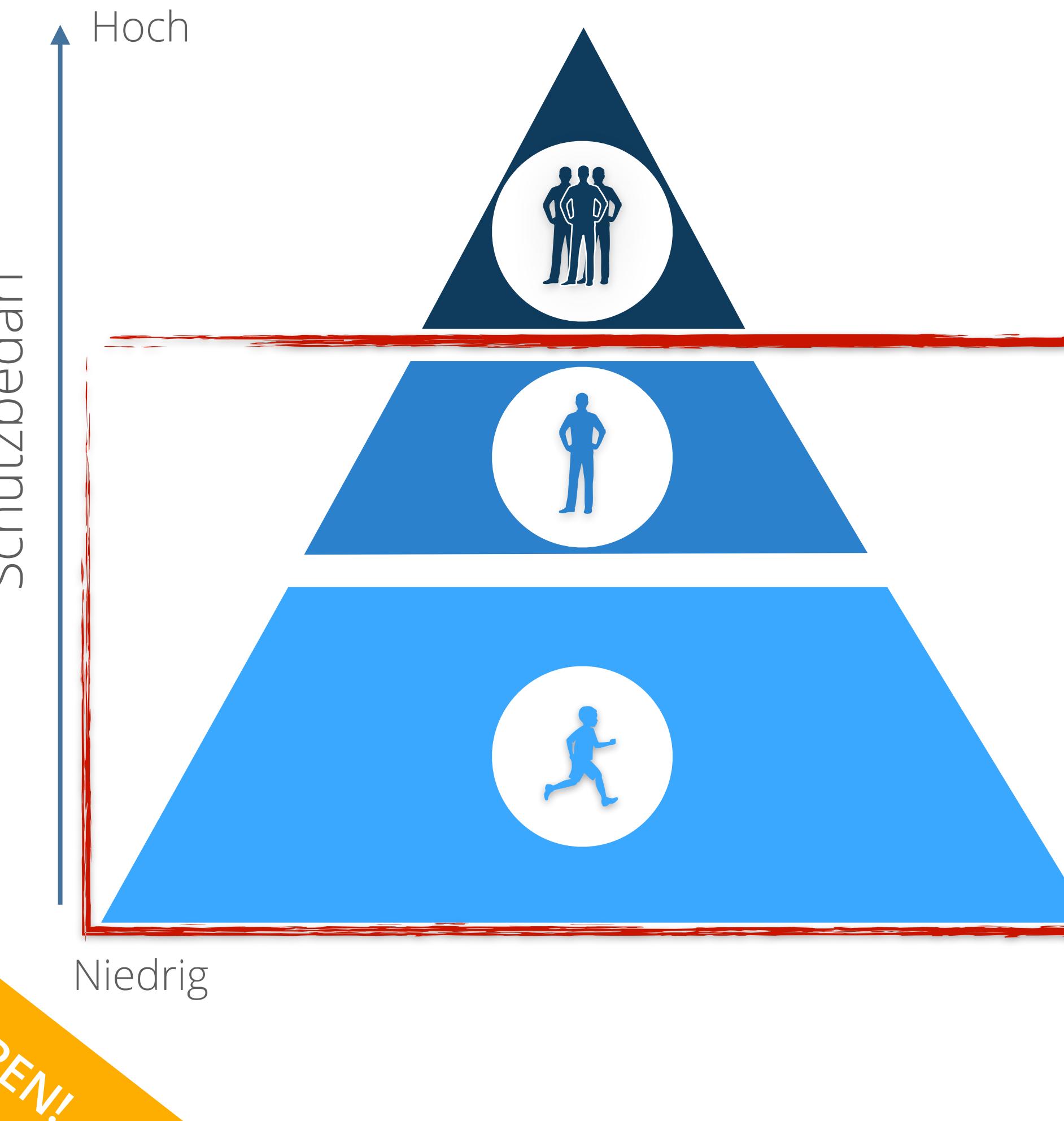
Top 3-Bedrohungen je Zielgruppe:



ANGREIFER_GRUPPEN

Govermental Layer

...



Industry Intelligence (APT's)
Schleusen Mitarbeiter ein und attackieren Zulieferketten

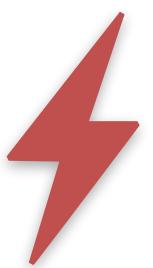
Technical Attacker
Nutzen Social Engineering (Faktor Mensch) + X

Script-Kiddie
Nutzen Fertige Scripts und Frameworks

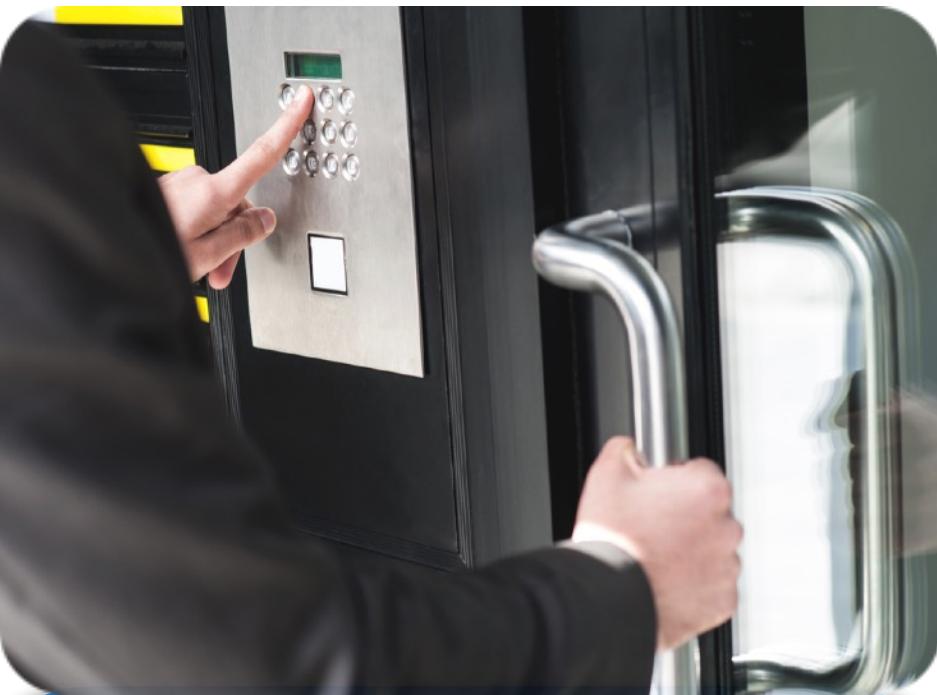
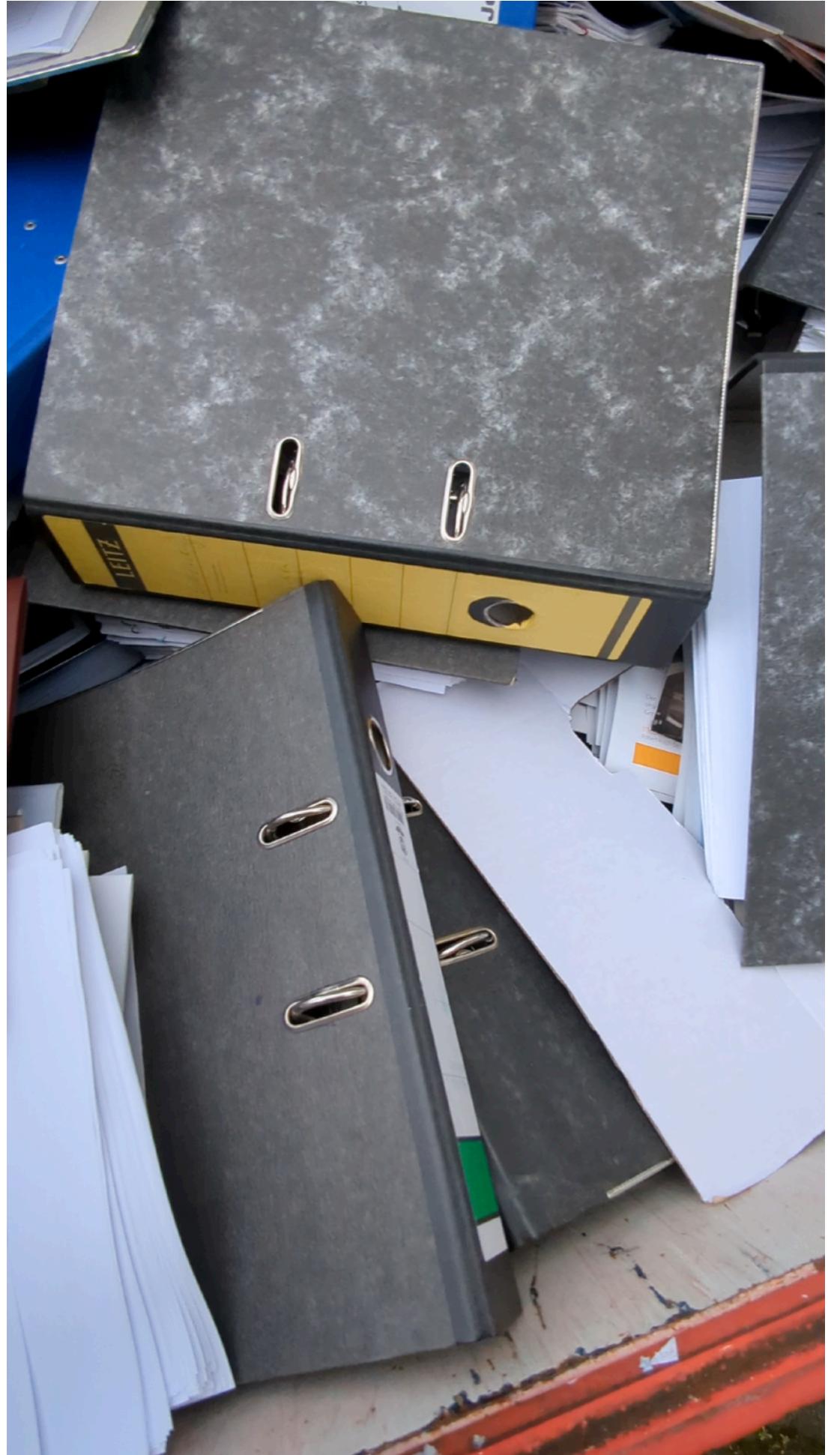
The background of the slide features a blurred photograph of a person sitting at a desk in a dimly lit room. They are facing away from the camera, looking at two computer monitors. The screens show what appears to be terminal windows or code editors. The person's hands are visible on a keyboard in the foreground. The overall atmosphere is professional and focused on technology.

ANGRIFF | THEORIE & PRAXIS

PHYSICAL „WLAN“



PHYSICAL „DUMPSTER DIVING“



PHYSICAL
SECURITY

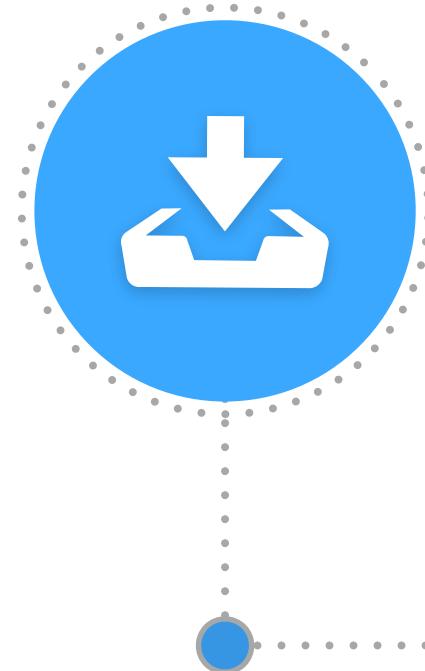


A blurred background image of a person sitting at a desk with multiple computer monitors. One monitor shows a terminal window with code, another shows a map or geographical data, and a third shows some graphical interface. The person's hands are visible on a keyboard in the foreground.

ANGRIFF | KILLCHAIN „CLASSIC“

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



Threat modeling

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

ABLAUF EINES ANGRIFFS

Exploitation



- Schwachstellen kontrolliert ausnutzen, um Zugriff auf Systeme zu erhalten oder diese beeinträchtigen
- Schutzmaßnahmen aushebeln

Monetarisierung

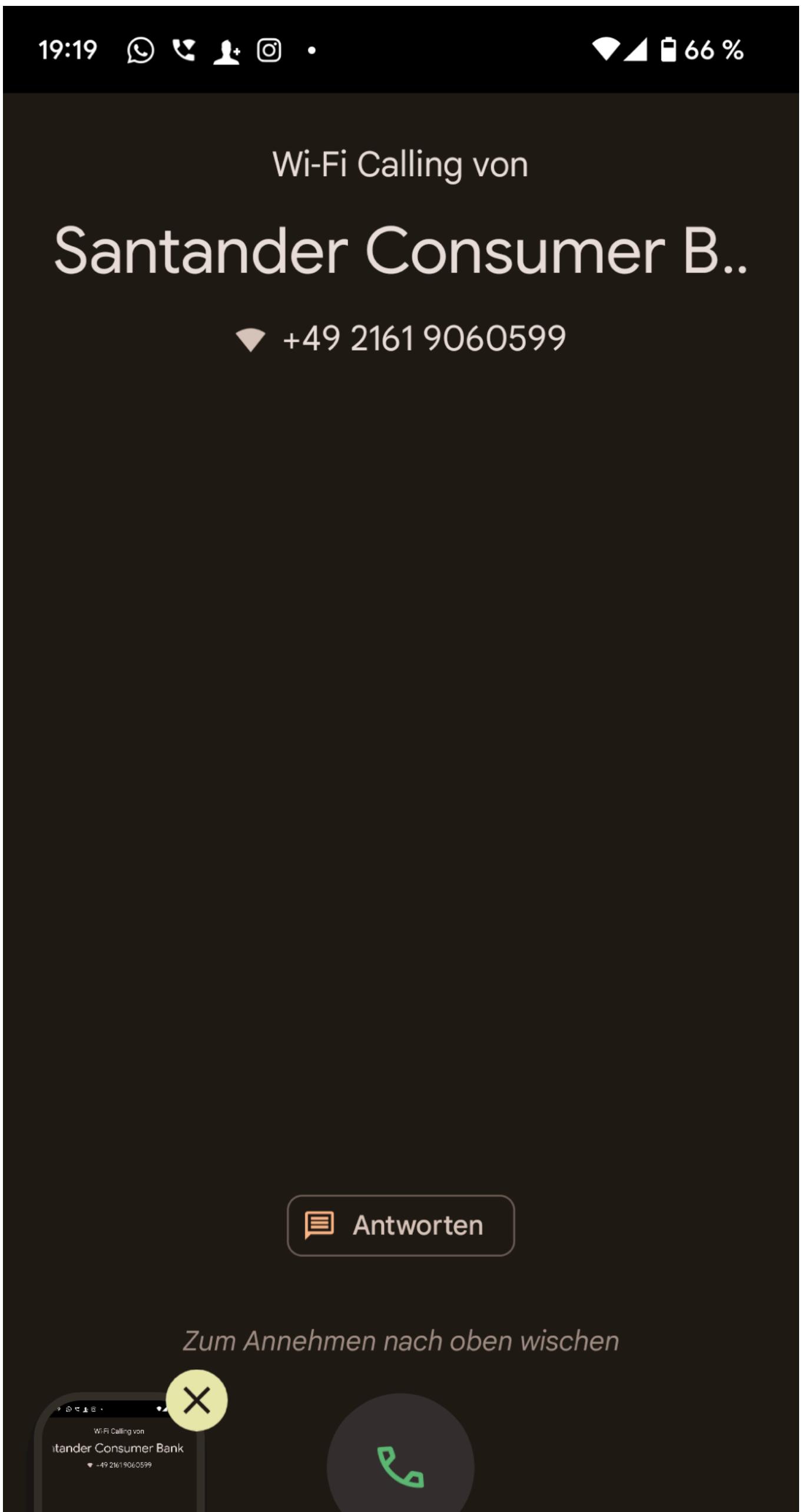


- Bewertung der Daten z.B. zur Wertermittlung & Höhe der Lösegeldforderung
- Kontakt aufnahme mit Opfer oder Interaktion
- Einleitung weiterer krimineller Folgeszenarien



Post exploitation

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



Technical Attacker | **Technik & MENSCH**

CASE APOTHEKE | ERGEBNIS





Business KPI's



Dr. Wolfgang Schlags
Apotheker | Modell*
In 4. Generation

Jahresumsatz **2022** | **ca. 45Mio €**

Alle Filialen des Familien Verbundes gesamt!



ProSec
Security redefined.

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

FAKTOR MENSCH - BEISPIEL EVENT & BONUS

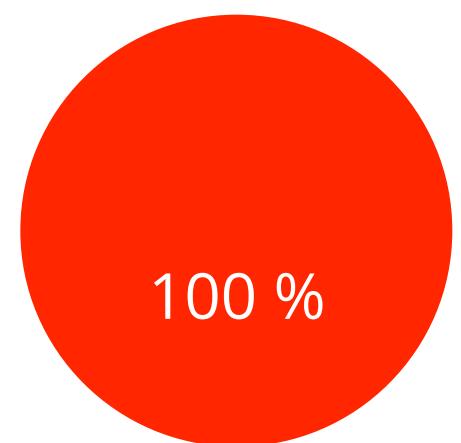
The screenshot shows a web browser window with the following elements:

- Header:** A dark header bar with standard OS controls (red, green, blue buttons) and a search bar.
- Logo:** DR. SCHLAGS APOTHEKE logo with the website address www.schlags-apotheke.de.
- Search Bar:** A search bar containing "Suchbegriff/Artikelnummer" with a magnifying glass icon, a user icon, and a cart icon showing "0,00 €".
- Section:** "MITARBEITER BENEFITS" above a group photo of approximately 18 pharmacists in white coats standing in a row.
- Photo:** A photograph of the pharmacists in a pharmacy setting with shelves of products in the background.
- Logos:** Logos for various partners at the bottom: **amazon.de**, **home24**, **OTTO**, **MEMORY:PC**, **CHRIST**, and **weg.de**.
- Section:** "ANMELDUNG" (Login).
- Text:** "Verwenden Sie bitte Ihre Windows Anmeldedaten:" (Please use your Windows login data:).
- Form:** Two input fields for "Benutzername" (Username) and "Kennwort" (Password).
- Button:** A large black "ANMELDEN" (Login) button at the bottom.

REALISMUS NAH..!

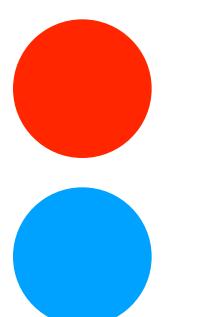
Alle Teilnehmer erhalten eine Mail zur Einführung eines Benefit Portals mit der Aussicht auf Gutscheine und Rabattierungen. Das Potential dieser Attacke ist aufgrund eines Sachwerts und dem meist persönlichen Interesse sehr hoch. Ziel ist die Eingabe der Benutzeraccounts im Browser.

Die Erfolgswahrscheinlichkeit bei bisherigen Tests liegt derzeit bei:



Legende

Erfolgreich in Prozent



Nicht Erfolgreich in Prozent





○ Burgfestspiele Mayen <info@tickets-burgfestspiele-mayen.de>

An: Ⓜ Christian Horn

Gestern um 09:07

Senden

CC/BCC

✉ Optionen ↗

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 Veranstaltungen 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 Burgfestspiele Mayen

Mail: info@tickets-burgfestspiele-mayen.de

www.burgfestspiele-mayen.de

www.facebook.com/BurgfestspieleMayen



Sehr Böse Hackerin



APOTHEKE



ProSec
Security redefined.

The screenshot shows the official website for the Burgfestspiele Mayen. At the top, there are social media icons for Facebook, Instagram, and Email. The main navigation menu includes links for HOME, ÜBER UNS, TEAM, SPIELPLAN 2021, SPIELZEIT 2021, TICKETS, SERVICE, CORONA INFO, and KONTAKT. Below the menu is a large image of two performers on stage. A banner at the bottom left reads "NUR FÜR KURZE ZEIT HABEN SIE DIE MÖGLICHKEIT ZU SPAREN!" (Only for a short time do you have the opportunity to save!).



Sehr Böse Hackerin



APOTHEKE



ProSec
Security redefined.

The screenshot shows the SPEXBOX Konfiguration software interface. At the top, there are two tabs: "SPEXBOX Konfiguration" and "fax_20210705_142307_(002656)". The address bar shows the URL "10.41.66.117". On the left, there's a sidebar with a woman's profile picture and the text "SPEX BOX" and "Administrator Sie sind angemeldet." Below the sidebar is a navigation menu with tabs: Start, Anrufliste, Faxversand, Telefonbuch, Nebenstellen, Accounts, Zugangsdaten, Konfiguration. The "Konfiguration" tab is selected. The main content area displays three sections for "Rezeptanforderung" (Medication Order) under "Medikamentenbedarf für den Zeitraum bis 25.07.2021".

Section 1: 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	

Section 2: 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	

Section 3: 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



A blurred background image of a person sitting at a desk, working on a computer. There are multiple monitors displaying what appears to be code or data. The overall color tone is blue.

HACKING & KRIEG?



Ethical Hacking.....



Mögt Ihr Schokolade..?

**STOP
FUNDING
PUTIN'S
WAR**

#bloodytrade



Kunde bei ner Raiffeisen BANK..?



Was mit IT „zu tun“..?

Tweet unter „#bloodytrade & #projahn“

← Tweet

 MrWtr0102
@mrwtr0102

...

#Ukraine war

#HallOfShame (#GradeF) companies still in #Russia
Link(@YaleSOM, @JeffSonnenfeld
): som.yale.edu/story/2022/ove...

Sorted by country

Includes:

@Amdocs - \$DOX
@ForeverGlobalHQ
@HardRock
@Zippo
@camillealbane
@NTTDATA
#Projahn

@UniCredit_PR

@sodeca
#Makrochem
@etihad
#NorMaali

Tweet übersetzen



#FreedomForUkraine

#HallOfShame companies that haven't left #Russia. (Category Five: #DiggingIn / #GradeF)

Link (@YaleSOM, @JeffSonnenfeld): <https://som.yale.edu/story/2022/over-750-companies-have-withdrawn-russia-some-remain>

ADITYA BIRLA GROUP
#AdityaBirla Group
@AdityaBirlaGrp

HINDALCO
#Hindalco Industries Ltd.
@Hindalco_World
(NSE: #HINDALCO)

bajaj group
#BajajGroup
www.bajajgroup.company

BAJAJ
#Bajaj_Auto_Ltd.
@bajaj_auto_ltd
(NSE: #BAJAJAUTO)

Bharat Petroleum Co.
(#BPCL)
@BPCLLimited
(NSE: #BPCL)

#CoalIndia Ltd.
(#CIL)
@CoalIndiaHQ
(NSE: #COALINDIA)

Dr. Reddy's
#DrReddy's Laboratories Ltd.
@drreddys
(NSE: #DRREDDY)
(NYSE: SRDY)

IndianOil
#IndianOil Corp. Ltd.
(#IOC) (#HOCL)
@IndianOilCoL
(NSE: #IOC)

JSW Steel
#JSWGroup
@jswsteel

LARSEN & TOUBRO
It's all about Imagineering
#LarsenAndToubro Ltd.
(#LAndT)
@larsentoubro
(NSE: #LT)

#MahindraGroup
@MahindraRise

#MAndM
(#MahindraAutomotive)
(#MahindraAuto)
@Mahindra_Auto
(NSE: M&M)

ONGC
#OilAndNaturalGasCorp. Ltd.
(#ONGC)
@ONGC_
(NSE: #ONGC)

Pidilite Industries Ltd.
@PidiliteInd
(NSE: #PIDILITIND)
#ONGC

SUN PHARMA
#SunPharmaceutic
Industries Ltd.
(#SunPharma)
@SunPharma_Liv
(NSE: #SUNPHARMA)

#TitanCompany Ltd.
@TitanCompanyLimited
(NSE: #TITAN)

#AgranaGroup
(#Agrana)
www.agrana.com

ANDRITZ
#Andritz AG
(WBAG: #ANDR)
www.andritz.com

AVL
#AVL
@AVL_List

EGGER Group
www.egger.com

KOTÁNYI
#Kotanyi GbmH
www.kotanyi.com

Kronospan
#Kronospan
www.kronospan
-worldwide.com

#Lisec Group
@lisecgroup

#Raiffeisen Bankengruppe
(#RBG)
@raiffeisen_at

Raiffeisen Bank Intl. AG
(#RBI)
@RBI_Presse
(WBAG: #RBI)

#RussiaFachspedition
#DrLassmann GmbH
(#RussiaLassmann)
www.russia.at
(@Theme_Fusion)

Schoeller Bleckmann
Oilfield Equipment AG
(#SBO)
www.sbo.at

wienerberger A
@wienerberger
(WBAG: #WIE)

#Alumil SA
@AlumilSA

Frigoglass
www.frigoglass.com
(ATHEX: #FRIGO)

Kleemann
#Kleemann
https://kleemannlifts.com

PLASTIKA KRITISSA SARANTIS
#PlastikaKritis SA
www.plastikaritiss.com
#SarantisGroup
(#Sarantis)
www.sarantisgroup.c

#Itochu Corp.
www.itochu.co.jp

Mitsui & Co.
@mitsuiandico

Mizuho
Financial Group, Inc.
(@MizuhoAmericas)
(NYSE: SMFG)

NTT NTT DATA
#NipponTelegraph
and
Telephone Corp.
(#NTT)
@NTTPR

Tokyo Electric Power Company Holdings, Inc.
#TokyoElectricPower
Company Holdings, Inc.
(#TEPCO)
(@TEPCO_English)

#GEA Group AG
(#GEA)
@thegeagroup
(FWB: #G1A)

GLOBUS
#Globus Hypermarket
Holding
www.globus.de

#Liebherr Int'l. AG
@Liebherr

METRO AG
@METRO_News
(FWB: #B4B)

NewYorker Group Services Inc.
GmbH & Co.KG
@NewYorkerOnline

Part of Your World
Storck
www.storck.com

Siemens AG
@Siemens
FWB: #SIE

Siemens EDA
#SiemensEDA
@siemenssoftware
(I/f/a #MentorGraphics, @mentor_graphics)

Subject to updates, corrections and revisions.

Webseite & Unternehmen „dahinter“

PROJAHN

Produkte Aktionen Service Unternehmen Händler-Login DE | EN 

UNSERE PHILOSOPHIE

WIR STEHEN FÜR HÖCHSTEN QUALITÄTSANSPRUCH

Die PROJAHN Präzisionswerkzeuge GmbH ist ein mittelständisches internationales Handelsunternehmen der Werkzeugbranche mit ausgeprägter Kunden- und Serviceorientierung. Wir sind Teil einer familiengeführten Unternehmensgruppe mit eigener Hammerbohrer-Produktion in Deutschland und weiteren Schwesterfirmen.

Unsere Produktpalette besteht aus rund 10.000 Artikeln mit Schwerpunkt in den Bereichen Präzisions- und Handwerkzeuge. Wir produzieren und vertreiben professionelle Werkzeuge für professionelle Anwender aus Handwerk und Industrie. Permanente Produkt-Neu- und Weiterentwicklungen zum Nutzen der Anwender sichern unsere Stellung am Markt und verschaffen uns einen Wettbewerbsvorsprung.

Aktuell beschäftigen wir ca. 70 Mitarbeiter. Der Sitz unseres Unternehmens befindet sich in Dietzenbach bei Frankfurt am Main. Durch unser modernes zentralgelegenes Lager- und Logistikzentrum garantieren wir eine hohe Verfügbarkeit und schnelle Lieferung - innerhalb Deutschlands von nur 24 Stunden. Diese Zuverlässigkeit und der hohe Servicegrad ermöglichen es unseren Fachhandelspartnern, ihr Geschäft flexibel zu gestalten.

Unser Kundenstamm besteht aus etwa 3.000 in- und ausländischen Fachhändlern.

Unser Erfolg basiert auf unseren Qualitätsprodukten und Serviceleistungen sowie hochmotivierten Mitarbeitern, die professionell, zielstrebig und erfolgreich das Firmenwachstum gestalten.

 **QUALITÄT**
Sie erhalten professionelle Qualität für Ihre professionellen Ansprüche!

 **SERVICE**
Unsere vielfältigen Serviceleistungen machen den Unterschied!

 **ZUVERLÄSSIGKEIT**
Sie wissen, dass Sie sich auf uns verlassen können!

#KMU | #Projahn | 70 Mitarbeiter





ProSec
Security redefined.



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



- „Publish and HACK!“



A blurred background image of a person sitting at a desk, working on a computer. There are four monitors visible, all displaying what appears to be lines of code or terminal output. The person's hands are on a keyboard in the foreground.

#RECAP_MAIN



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



#SecByDesign

4 REAL!

#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



#ADVISORIES | MYTHOS SCHUTZ DURCH LÖSUNG



#Red_Button



#Spezialist

#ADVISORIES | SECURITY_BY_DESIGN VS. „BILLIG“



That's actually a very low price.



#Cheap_Security



#High_Cost

A blurred background image of a person sitting at a desk, working on a computer. There are multiple monitors displaying what appears to be code or technical data. The overall color palette is blue and grey.

“2023 MUSS NIEMAND MEHR EINEN
#RECAP STATEMENT
FATALEN CYBERANGRIFF ERLEIDEN...!”



GERNE „ASK MY ANYTHING..!“



Immanuel
Bär

„In allen Cyberangriffe existiert ein Gegengift“

von Immanuel Bär · Lesedauer: 2 Min.

Teilen mit weiteren Personen

6 Kommentare · 3 direkt geteilte Beiträge

Angebot für Teilnehmer!

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



linkedin

