

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

Perspektive eines „White-Hat-Hackers“



vodafone
**enterprise
plenum**

brennw



VITA, STORY & STATIONEN

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 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-



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



Über t3n Jobs bei t3n



Feature

Targeted by Killnet: This early warning system protected 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 operators.

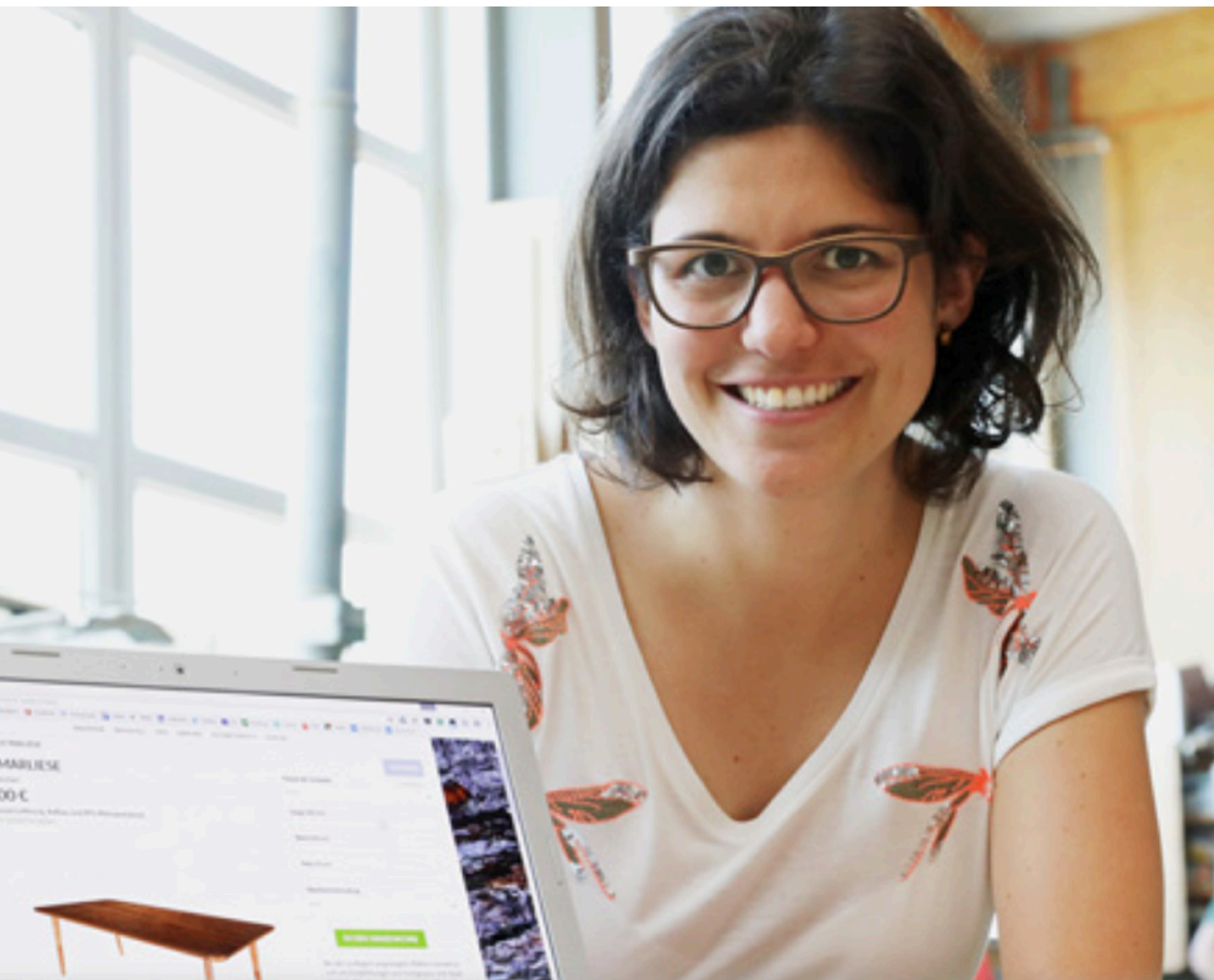
Von Kim Rixecker

07.06.2022, 14:00 Uhr • 3 Min. Lesezeit



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

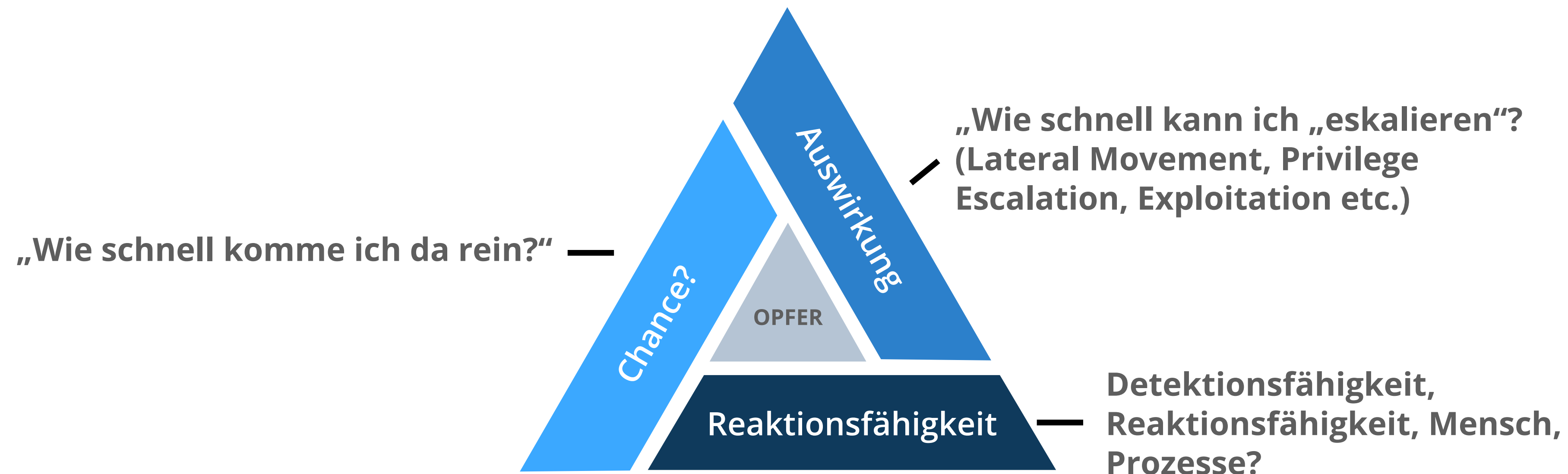
2020 | #KMU #MITTELSTAND #KRITIS



ANGRIFF | THEORIE „HIGH LEVEL“

HACKEN - HANDELN - RESILIENZ!

(EINTRITTSRISIKO | AUSWIRKUNG | REAKTIONSFÄHIGKEIT)



Denkweise des Angreifers..

A woman with dark hair, wearing a grey business suit, is standing in a modern office environment. She is holding a large, inflated orange balloon in front of her face. The word "TROJAN" is written in white, bold, capital letters across the balloon. The background shows office cubicles and a bright window on the left.

TROJAN

ANGRIFF **FELDER?**

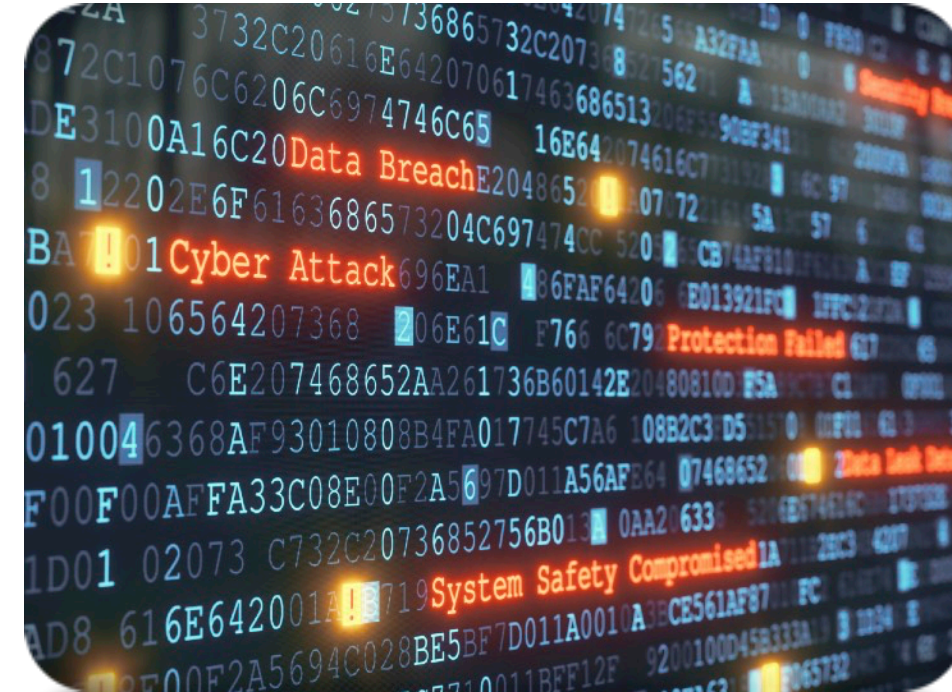
#IT_SICHERHEIT

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

Governmental Layer

...



Industry Intelligence (APT's)

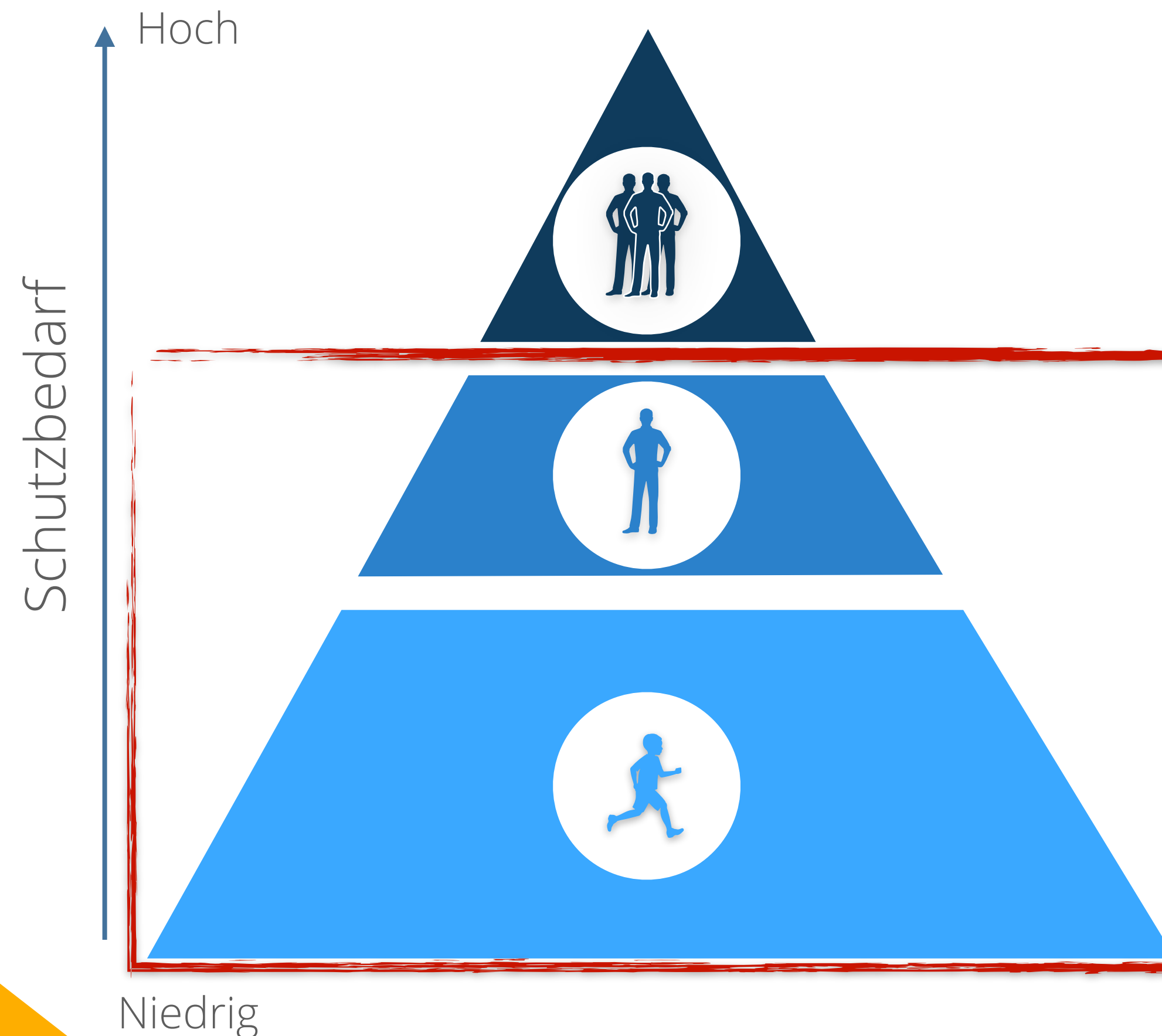
Schleusen Mitarbeiter ein und attackieren Zulieferketten

Technical Attacker

Nutzen Social Engineering (Faktor Mensch) + X

Script-Kiddie

Nutzen Fertige Scripts und Frameworks



Merke GRUPPEN!

ANGRIFF | THEORIE & PRAXIS

PHYSICAL „WLAN“



PHYSICAL
SECURITY



PHYSICAL „DUMPSTER DIVING“



PHYSICAL
SECURITY



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

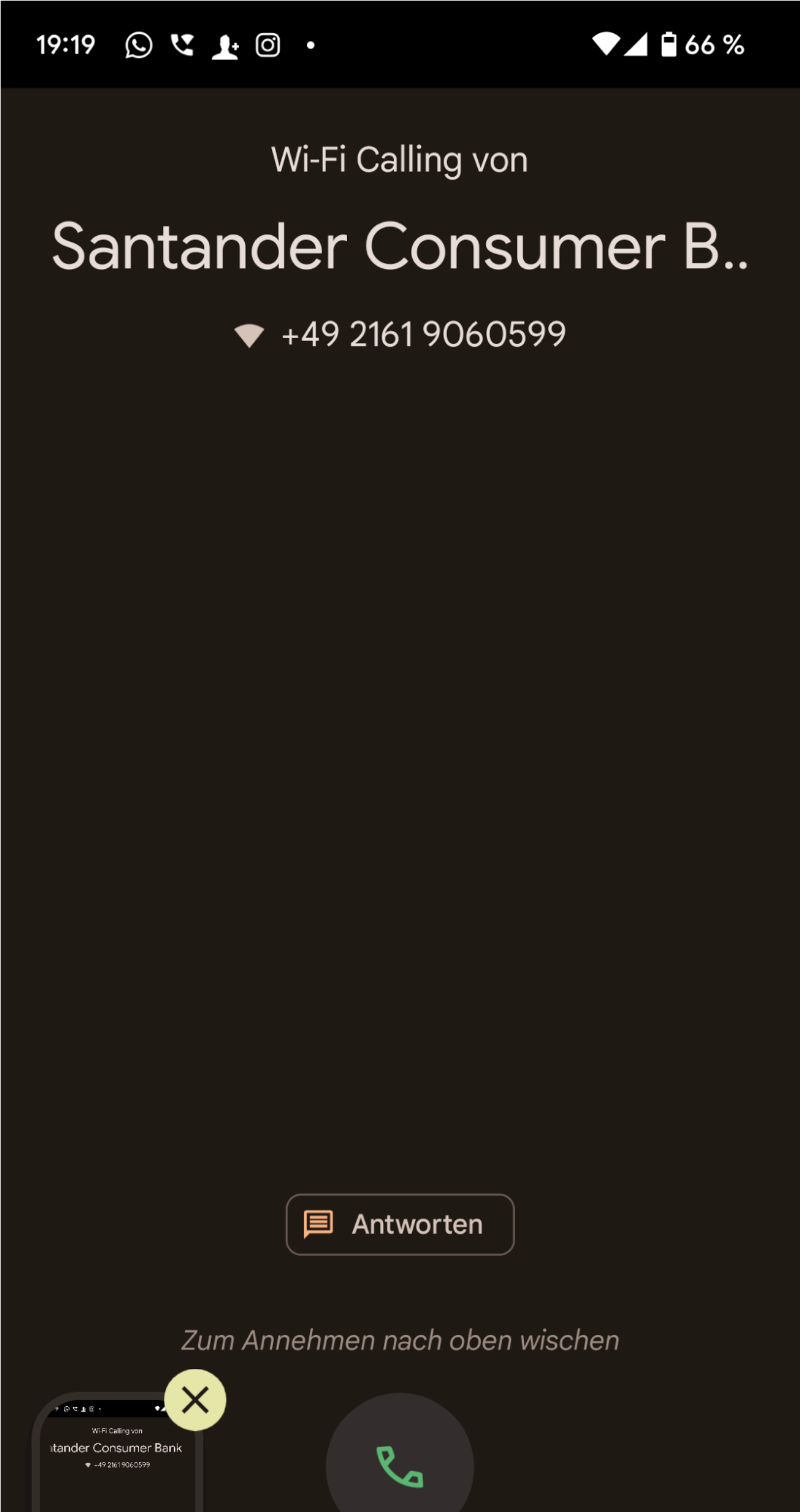


- Bewertung der Daten z.B. zur Wertermittlung & Höhe Lösegeldforderung
- Kontaktaufnahme mit Opfer oder Interaktion
- Einleitung weiterer krimineller Folgeszenarien



Post exploitation

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



Technical Attacker | **Technik & MENSCH**



CASE APOTHEKE | ERGEBNIS





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

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

Alle Filialen des Familien Verbundes gesamt!

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**

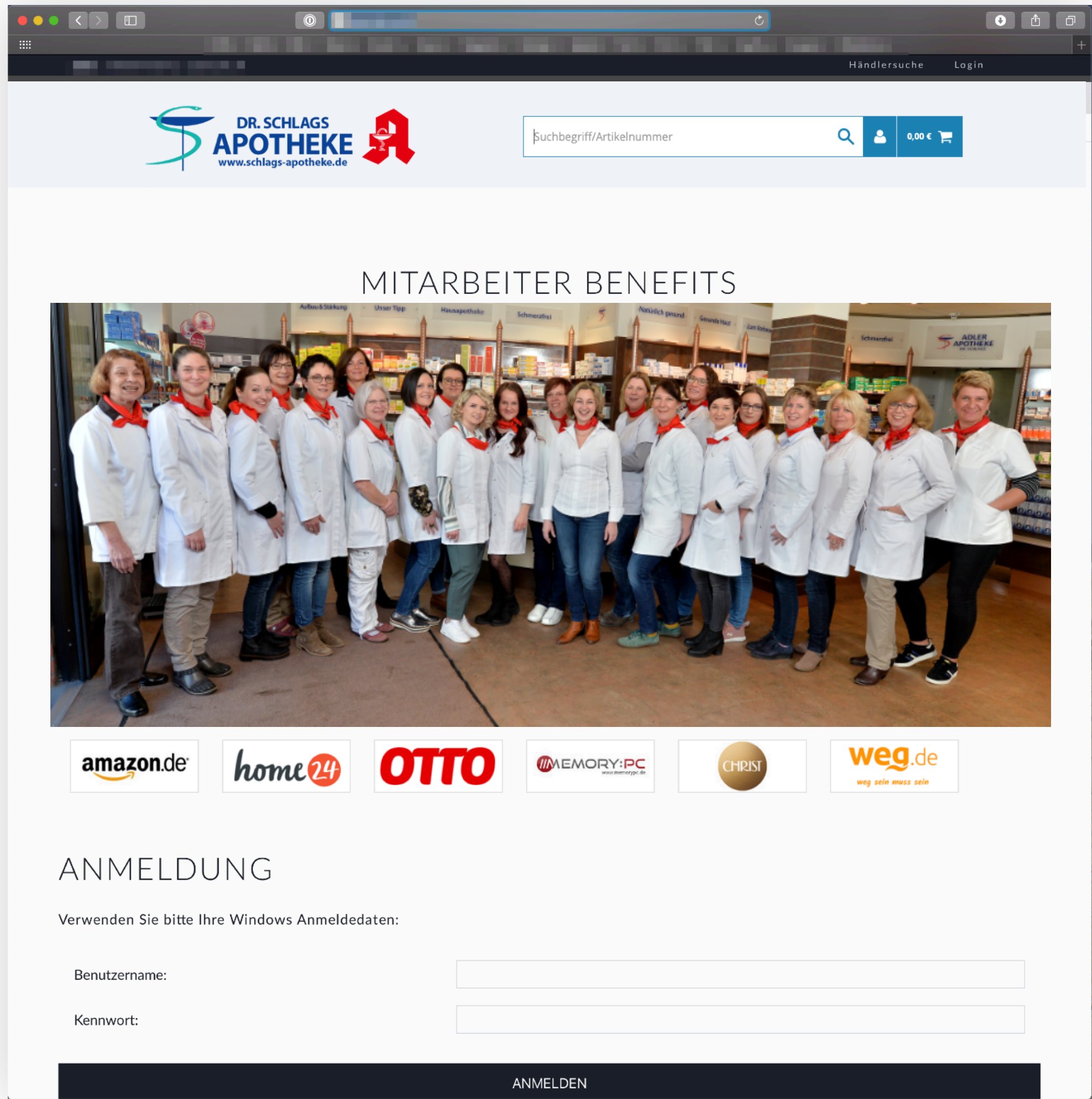
Filiale der Adler-Apotheke

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

Filiale der Adler-Apotheke

FAKTOR MENSCH - BEISPIEL EVENT & BONUS

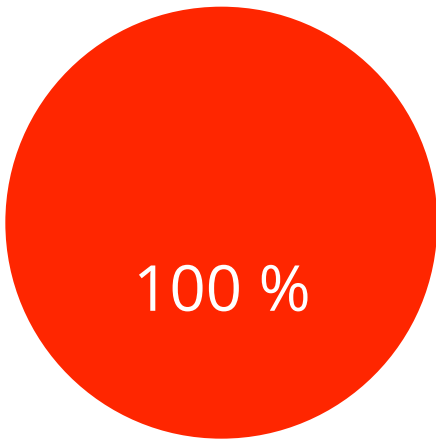
Exemplarisch!



REALISMUS NAH..!

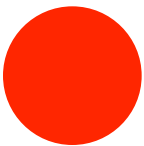
Alle Teilnehmer erhalten eine Mail zur Einführung eines Benefit Portals mit der Aussicht auf Gutscheine und Rabattierungen. Das Potential dieser Attacke ist aufgrund eines Sachwerts und dem meist persönlichen Interesse sehr hoch. Ziel ist die Eingabe der Benutzeraccounts im Browser.

Die Erfolgswahrscheinlichkeit bei bisherigen Tests liegt derzeit bei:




Legende

Erfolgreich in Prozent




Nicht Erfolgreich in Prozent







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

Gestern um 09:07

An:  Christian Horn

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 Bugfestspiele Mayen

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



Sehr Böse Hackerin



PHISHING MAIL
Faktor Mensch

APOTHEKE




Startseite – Burgfestspiele Maye X

https://tickets-burgfestspiele-mayen.de

f Instagram Email

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_(00265E

← → ↺ 🏠

🔒 🔑 10.41.66.117


☆

📧 ⬇️ 📄 📌 📱 1337 🟡 ☰

 **Administrator**
Sie sind angemeldet.

Abmelden

SPEXBOX Konfiguration



Start

Anrufliste

Faxversand

Telefonbuch

Nebenstellen

Accounts

Zugangsdaten

Konfiguration

Rezeptanforderung

Medikamentenbedarf für den Zeitraum bis 25.07.2021

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	

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	

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



HACKING & **KRIEG**?



Ethical Hacking.....



Mögt Ihr Schokolade..?

**STOP
FUNDING
PUTIN'S
WAR**
#bloodytrade



Kunde bei ner Raiffeisen BANK..?

RITTAL

Stop suplly Russia



Was mit IT „zu tun“..?

Tweet unter „#bloodytrade & #projahn“

Tweet

MrWtr0102
@mrwtr0102

#Ukraine war

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

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>

INDIA

ADITYA BIRLA GROUP
AdityaBirlaGrp
@AdityaBirlaGrp
(NSE: #HINDALCO)

Dr.Reddy's
Dr.Reddy's Laboratories Ltd.
@DrReddys
(NYSE: #DRREDDY)

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

MAHINDRA
MahindraGroup
@MahindraRise

AUSTRIA

AGRA
AgranaGroup
@Agrana
www.agrana.com

ANDRITZ
Andritz AG
@Andritz
www.andritz.com

AVL
AVL List
@AVL_List

EGGER
EGGER Group
@EGGER.com

KOTANYI
Kotanyi GmbH
www.kotanyi.com

KRONOSPAN
Kronospan
@Kronospan
www.kronospan-worldwide.com

GREECE

ALUMIL
Alumil SA
@AlumilSA

ELVALHALLOR
Elvalhacor SA
@elvalhacor

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

JAPAN

ITOCHU
Itochu Corp.
www.itochu.co.jp

MITSUBISHI & CO.
Mitsui & Co.
@mitsuandco

MIZUHO
Mizuho Financial Group, Inc.
@MizuhoAmerica
(NYSE: #MFC)

NTT
Nippon Telegraph and Telephone Corp.
@NTT
NTT

TEPCO
Tokyo Electric Power Company Holdings
@TEPCO
@TEPCO_English

GERMANY

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

GLOBUS
Globus Hypermarket Holding
www.globus.de

LIEBHERR
Liebherr Int. AG
@Liebherr

METRO
Metro AG
@METRO_News
(FWB: #B4B)

NEWYORKER
NewYorker Group Services Intl., GmbH & Co. KG
@NewYorkerOnline

PROJAHN
www.projahn.de

STORCK
Storck
www.storck.com

SIEMENS
Siemens AG
@Siemens
FWB: #SIE

Siemens EDA
SiemensEDA
@SiemensEDA
(f/k/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



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



- „Publish and HACK!“

**ANONYMOUS
FOR UKRAINE**

#RECAP_MAIN



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

RE_CAP_PART



#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

RE_CAP_PART



#Red_Button



#Spezialist

#ADVISORIES | SECURITY_BY_DESIGN VS. „BILLIG“

RE_CAP_PART



#Cheap_Security



#High_Cost

"2023 MUSS NIEMAND MEHR EINEN
#**RECAP** STATEMENT
FATALEN CYBERANGRIFF ERLEIDEN..!"

GERNE „ASK MY ANYTHING..!“



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



linkedin



Angebot für Teilnehmer!