



Accenture Case Study

RWTH Aachen, 19.01.2022



Ann-Kathrin Strutzenberger

Cyber Defense Analyst
a.strutzenberger@accenture.com



Jan Schwinghammer

Industry X Security Analyst
Jan.schwinghammer
@accenture.com



Julia Fabian

Recruiting Senior Analyst
julia.fabian@accenture.com

Let there be change

Accenture Unternehmensübersicht

Let there be change

Wir helfen unseren Kunden, diese enormen Veränderungen als Chance zu begreifen, Innovation in der DNA des Unternehmens zu verankern und die sich daraus ergebenden individuellen Möglichkeiten zu erkennen.

Wir begleiten den gesamten Prozess der Entwicklung und Integration - von Anfang bis Ende.



Wir sind

624,000

Mitarbeitende

Wir operieren in über

120

Ländern

Wir beraten über

6,000

Kunden

In

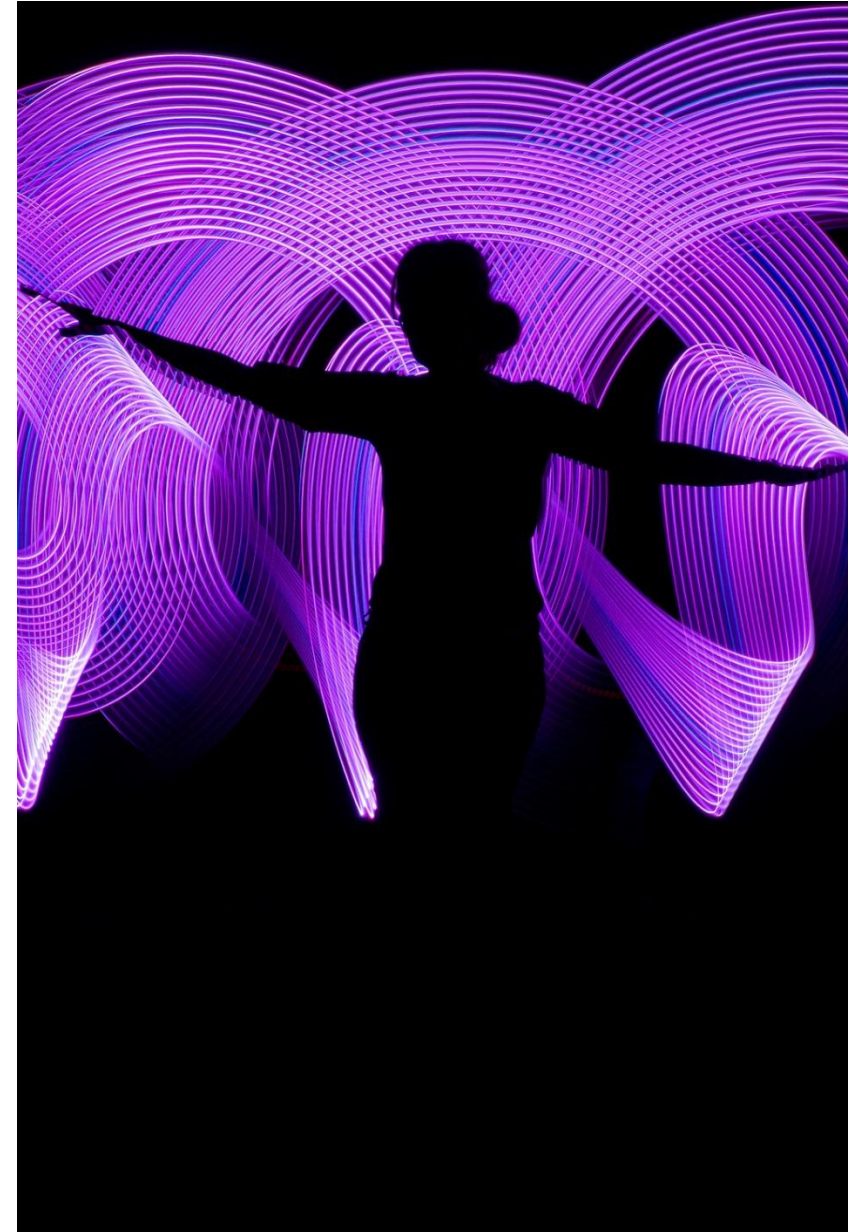
39

Sprachen

Wir arbeiten in über

40

Industrien



Wir bieten eine breite Palette von Dienstleistungen in großem Stil – von der Strategie bis zum Betrieb.

Strategy & Consulting

- Strategien zur Beschleunigung der digitalen Transformation
- Verbesserung von Wachstum / Rentabilität zur Schaffung von nachhaltigem Wert
- Tiefes Branchen-/ Funktions-Know-how
- Angewandte Intelligenz
- Innovationszentren
- Vernetzte Produkte/Plattformen

Interactive

- Sinnvolle Erlebnisse zur Steigerung von Wachstum und Wert
- Wachstum, Produkt- und Kulturdesign
- Technologie & Erlebnisplattformen
- Kreativ-, Medien- und Marketingstrategie
- Orchestrierung von Kampagnen, Inhalten und Kanälen

Technology

- Cloud
- Systemintegration / Application Management
- **Security**
- Intelligent Platform Services
- Infrastruktur
- Software-Entwicklung
- Labs / Ventures
- Ökosystem-Allianzen

Operations

- Geschäftsprozess-Services
- Funktionsspezifisch
- Finanz- und Rechnungswesen / Beschaffung / Supply Chain / Marketing
- Branchenspezifisch
- Banken / Versicherungen / Gesundheitswesen



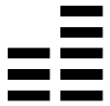
INDUSTRY-SPECIFIC SOLUTIONS





Security

FINANCIAL SERVICES



Banking
Insurance

PRODUCTS



Life sciences
Retail
Manufacturing / Auto

HEALTH & PUBLIC SERVICE



Health
Government

RESOURCES



Energy
Utilities

COMMUNICATIONS MEDIA & TECH



Media
Communications
Software & platforms
Aerospace & defense

PAIN POINTS

- Cyber-Risikomanagement
- Anti-Money Laundry
- Know Your Customer
- Krypto-Währungen
- Blockchain

- Betrug im Einzelhandel
- Connected Car

- Digitale Gesundheit
- Schutz von Patientendaten
- Digitaler Bürger
- eBorders
- Cyber-Intelligenz

- Security und Analytics für industrielle Kontrollsysteme
- Sicherung kritischer Infrastrukturen

- Sichere Produktentwicklung
- Diebstahl von geistigem Eigentum



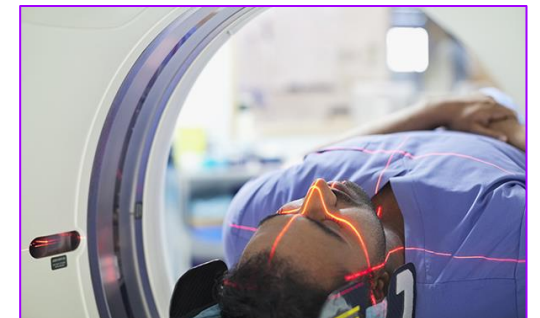
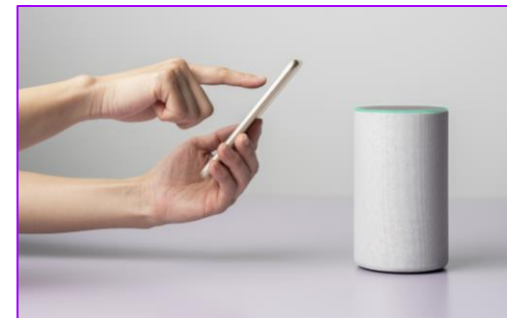
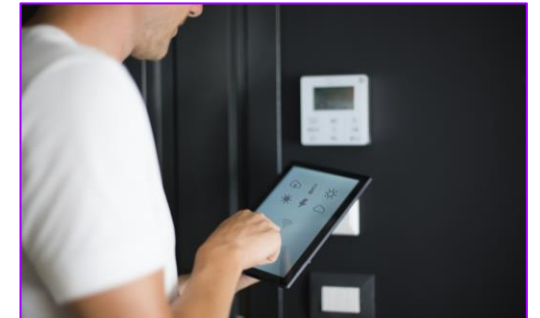
Industry X Security – Überblick

Industry X greift die Herausforderungen und Innovationen der Industrie im Rahmen von Industrie 4.0 (z.B. Digitalisierung und Konnektivität) auf und erweitert diese um den Bereich „Intelligenz“. Dies wird die Art und Weise, wie Unternehmen, Technologie und Menschen arbeiten, **neu definieren**. Industry X Security lässt sich in **zwei Bereiche** einteilen:

Produktionssicherheit



Produktsicherheit

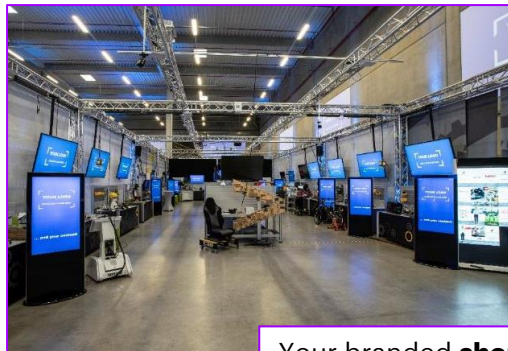


Industry X Innovation Center Essen und Garching

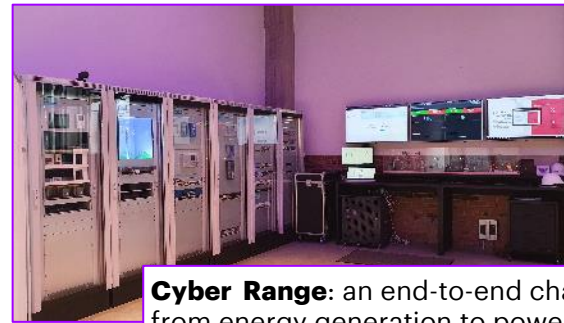
Essen



Experience 80+ IIoT use cases



Your branded **shop floor**



Cyber Range: an end-to-end chain from energy generation to power consumption in households



Smart home Building automation



Power Generation: wind turbine



Demo city: households



Experience digital fun stations

Garching



Vielen Dank

**Heute schaut ihr durch
die Beraterbrille!**

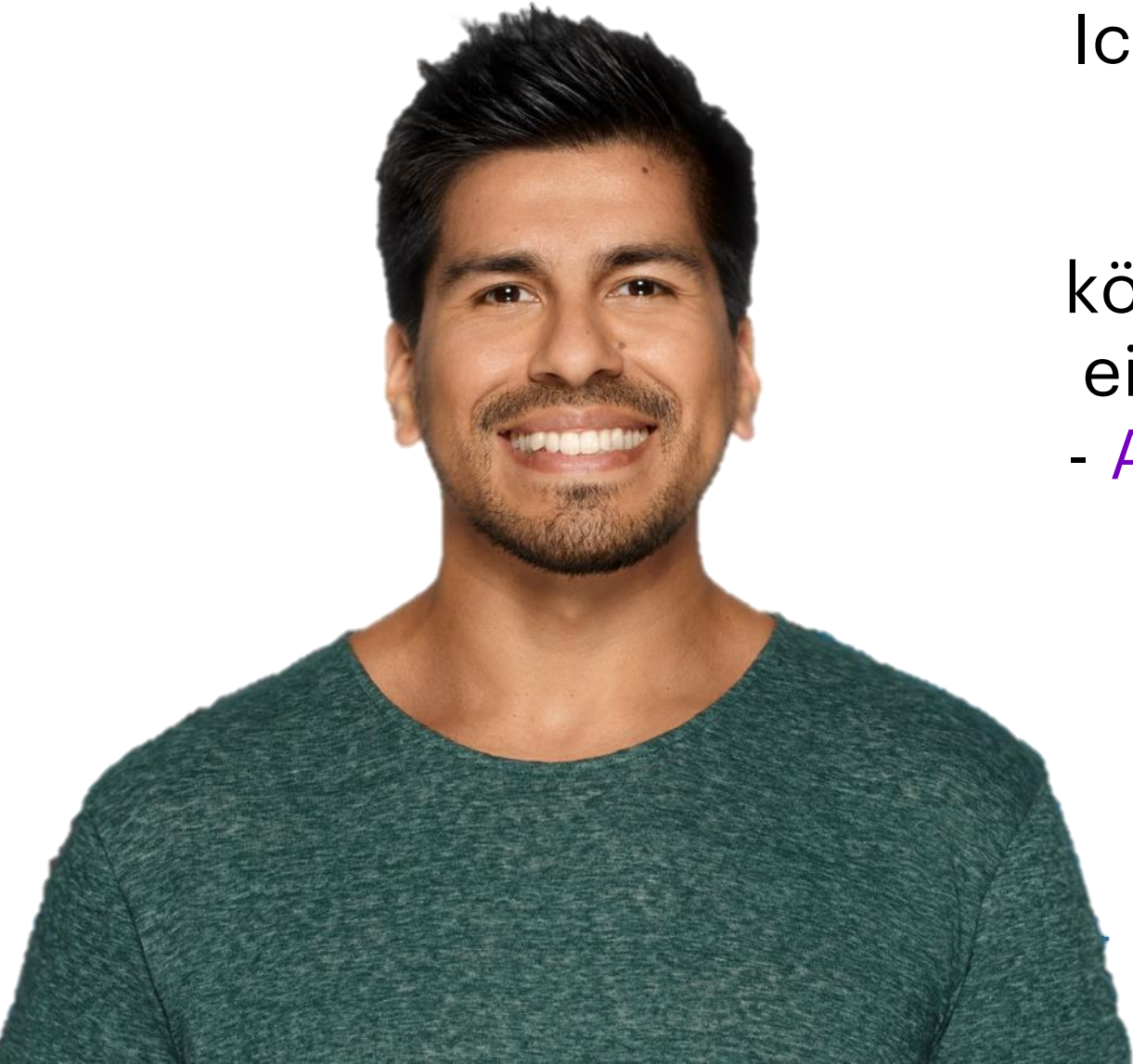


- Vegelicious ist ein Veganer Süßwarenhersteller aus Deutschland
- Ihr bekanntestes Produkt sind die „Sweet Bears“
 - Sie haben Vegelicious bekannt gemacht und erzeugten 79% des Umsatzes 2020
- Vegelicious Jahresumsatz lag 2020 bei 230 Millionen Euro
- Sie bedienen die Märkte in Deutschland, Österreich, der Schweiz und Italien
- Der Wachstumsmarkt der veganen Süßigkeiten ist derzeit hart umkämpft
- Vegelicious Strategie-Ziel lautet die Vorreiterstellung im Mitteleuropäischen Markt zu verteidigen und langfristig weiter international zu expandieren
- Ihre CEO will die Sicherheit des Unternehmens verbessern, da diese während des rasanten Wachstums der letzten Jahre vernachlässigt wurde



- **Confidentiality**
- **Integrity**
- **Availability**





Ich habe Bedenken, dass unsere Mitarbeiter leicht Opfer von **Phishing Attacken** werden könnten. Unsere Mitarbeiter sind einfach unzureichend geschult.

- Alex Kumari, Human Resources Manager Vegelicious



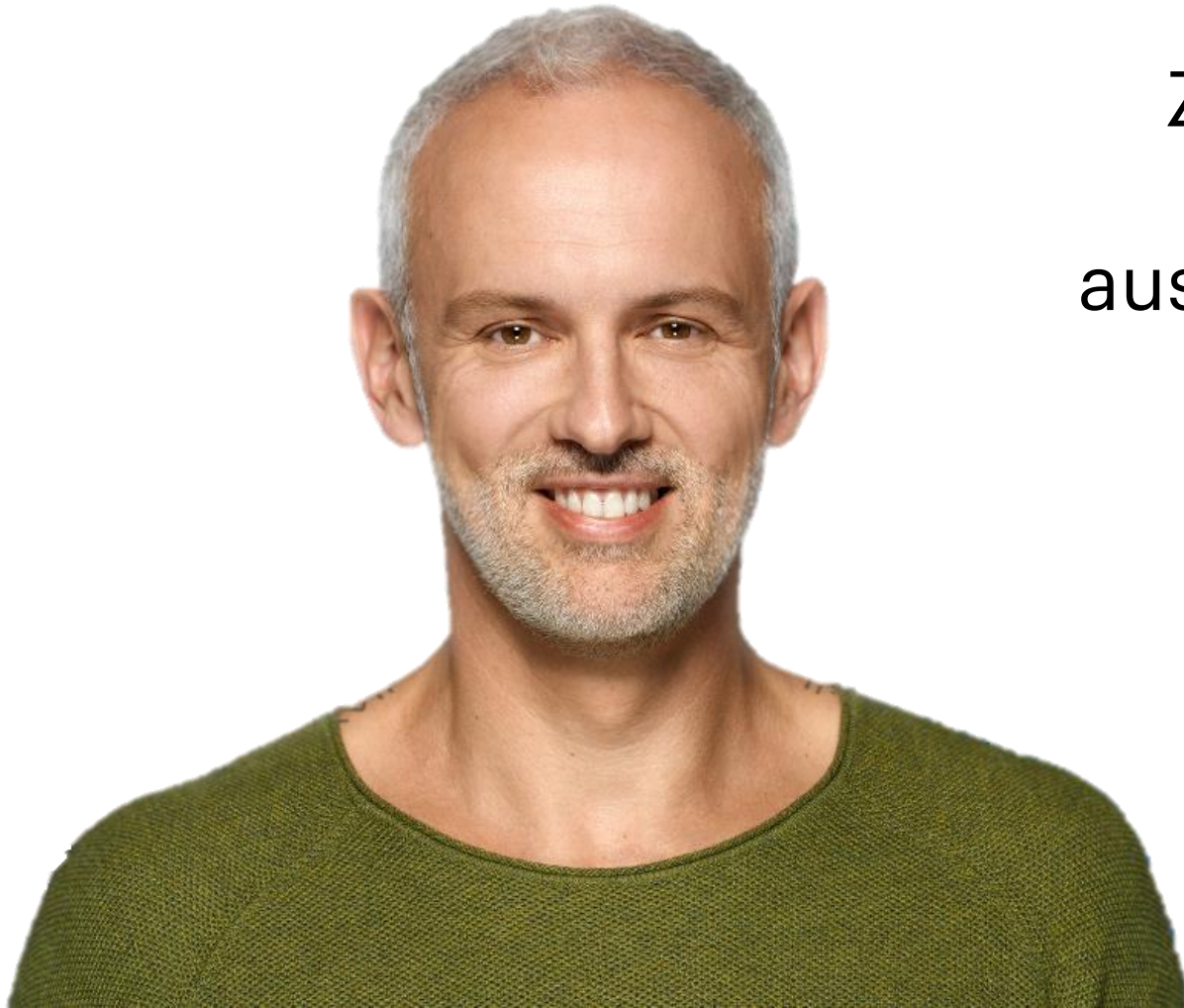
Unsere Sicherheits-
toollandschaft ist zu diffus! Wir
haben derzeit kaum eine Chance
zu erkennen, wann **Hacker** uns
angreifen, was sie im System
machen und wie wir darauf
reagieren können.

- Sarah Mieks, CISO Vegelicious



Wir müssen unsere Server besser schützen! Man hört immer wieder, dass Hacker unbemerkt Server kapern, um sie für **illegales Kryptomining** zweckzuentfremden ...

- Julia West, Infrastructure Managerin Vegelicious



Das Thema **Tailgating** macht mir Sorgen. Die Zugangsbeschränkungen auf unserem Campus sind nicht ausreichend, jeder der will könnte einfach reinspazieren. Wir müssen das angehen!

- Philipp Müller, Facility Management Vegelicious

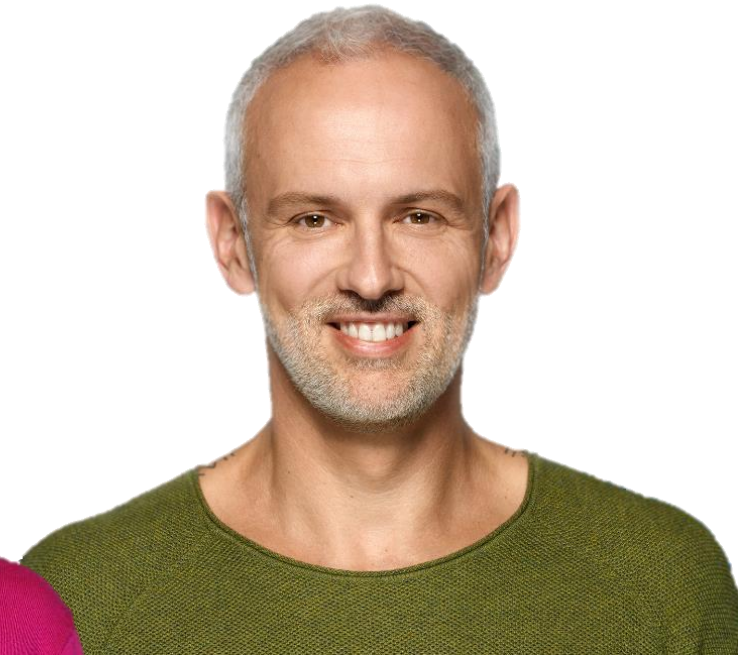
ABER WAS GEHEN WIR ALS ERSTES AN?

Ich habe Bedenken, dass unsere Mitarbeiter leicht Opfer von **Phishing Attacken** werden könnten. Unsere Mitarbeiter sind einfach unzureichend geschult.
- Alex

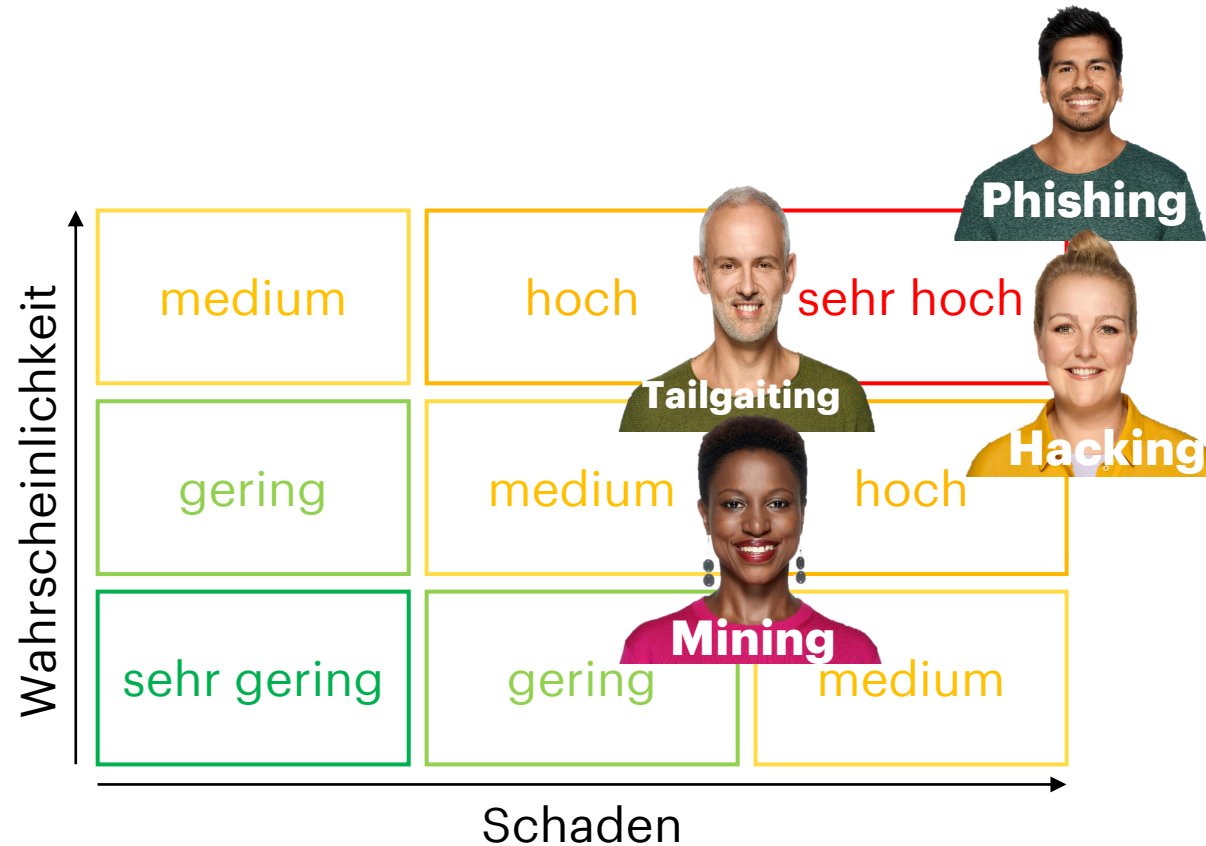
Unsere Sicherheits-toollandschaft ist zu diffus! Wir haben derzeit kaum eine Chance zu erkennen, wann **Hacker** uns angreifen, was sie im System machen und wie wir darauf reagieren können.
- Sarah

Wir müssen unsere Server besser schützen! Man hört immer wieder, dass Hacker unbemerkt Server kapern, um sie für **illegales Kryptomining** zweckzuentfremden.
- Julia

Das Thema **Tailgating** macht mir Sorgen. Die Zugangsbeschränkungen auf unserem Campus sind nicht ausreichend, jeder der will könnte einfach reinspazieren. Wir müssen das angehen!
- Philipp



ABER WAS GEHEN WIR ALS ERSTES AN?



Detaillierte Ausarbeitung der Bedrohungen

Beispiellösung

#1

Phishing

- Persönliche Informationen in betrügerischer Absicht erlangen
- Bösartige Software (Malware) verbreiten

#2

Hacking

- Kredit ruinieren
- Benutzernamen und Passwörter entführen
- Käufe tätigen
- Sozialversicherungsnummer verwenden und missbrauchen

#3

Crypto-Mining

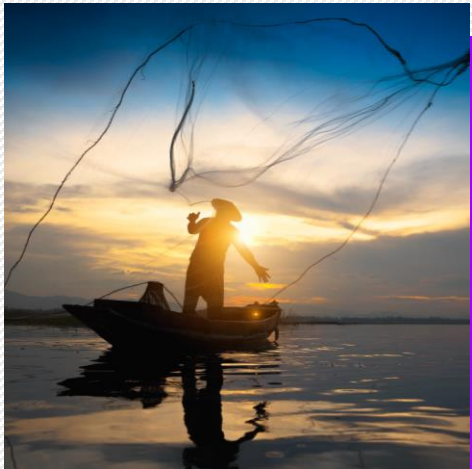
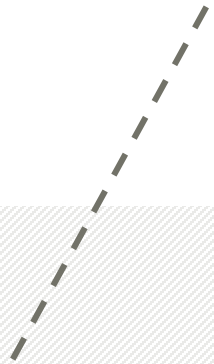
- Physischer Schaden und Stress für infizierte Endgeräte
- Negative Auswirkungen auf Geschäftsabläufe und Produktivität

#4

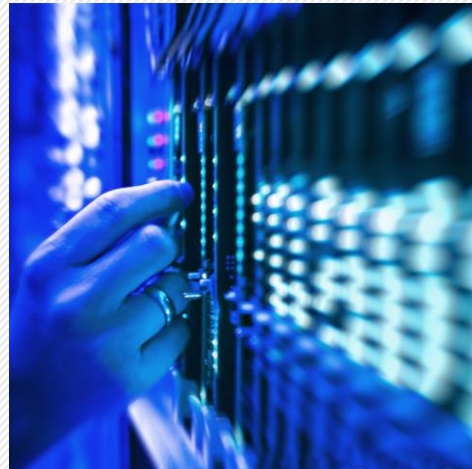
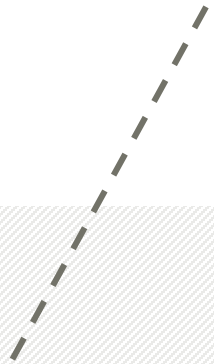
Tailgating

- Sachschäden
- Diebstahl von Informationen und Eigentum
- Das Leben von Mitarbeitern in Gefahr bringen

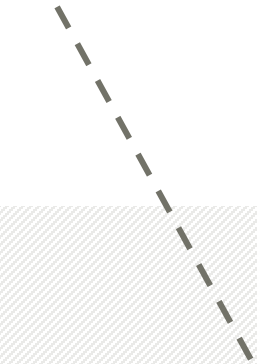
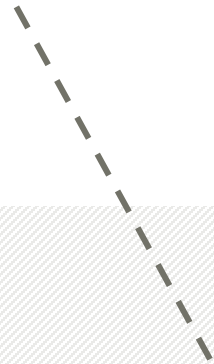
Operative Maßnahmen



Technische Maßnahmen



Physische Maßnahmen



Maßnahmen

#1

Operativ

- Schulungsprogramme
- Awareness-Maßnahmen
- Zertifizierungen
- Sicherheitsorientierte Governance

#2

Technisch

- Event-Monitoring (SOC)
- Restriktive Konfiguration (Eingeschränkte Benutzerkonten, Need-to-know-Prinzip)
- Two-Factor Authentikation
- Regelmäßige Software-Updates
- Einrichtung von Firewalls
- Verschlüsselung von Daten
- Protokollierung

#3

Physisch

- Einsatz von Sicherheitspersonal
- Zutrittskontrollsysteme (Zutrittscodes, Magnetkarten, biometrische Daten)
- Physische Schutzmaßnahmen gegen Feuer, Rauch, Einbruch und Wasser
- Mitarbeiterausweise
- Verwendung von Laptopschlössern



Hallo?

Hier spricht Philipp vom Empfang!
Ich hatte gerade einen Anruf von
einer Person, die mir mit verzerrter
Stimme erklärt hat, dass Sie uns und
alle unsere Server gehackt hat!

Er hat wohl eine **Ransomware**
installiert und wenn wir in den
nächsten **15 Minuten** nicht **10**
Bitcoin an seine Wallet überweisen,
wird er alle Daten auf unseren
Servern unwiederbringlich
verschlüsseln!

Was sollen wir jetzt machen?!

Search

File Home Send / Receive View Help

New Email Delete Reply Reply All Forward

Report Phishing Share to Teams Insights Reply with Meeting Poll

Cancel

23.7 GB Free All folders are up to date. Connected to: Microsoft Exchange 14:15 29.10.2021

Favorites
Inbox
Sent Items
Deleted Items

Online Archive -

2021

Die Zeit läuft!
@ByeVegeIicious

Wed 10/20/2021 3:35 PM

To: CISO.Team.All

Hallo zusammen,


mir wurde soeben

Best regards

Miriam Weigand
CEO

Vegelicious Tweet.png

@VegeIicious: eure Daten sind bei mir sicher. 10BTC oder Ihr werdet sie nie wieder sehen. Ihr habt 15min. Die Zeit läuft.



Was ist da dran? Rufen Sie mich sofort an!

12:49 PM · Oct 21, 2021

571 Retweets 26 Quote Tweets 5.7K Likes

The screenshot shows a Microsoft Outlook interface. The top ribbon includes 'File', 'Home', 'Send / Receive', 'View', and 'Help'. The 'Home' ribbon is active, showing options like 'New Email', 'Delete', 'Reply', 'Reply All', 'Forward', 'Unread/Read', 'Search People', 'Report Phishing', 'Share to Teams', 'Insights', and 'Reply with Meeting Poll'. On the left, the 'Favorites' pane shows 'Inbox', 'Sent Items', and 'Deleted Items'. The main content area displays an email from 'Mieks, Sarah' dated 'Wed 10/27/2021 3:04 PM' sent to 'CISO.Team.All'. The email body contains the following text:

Sehr geehrte Damen und Herren,

diese Nachricht geht an alle Mitglieder des Security-Consulting Teams. Ich habe innerhalb der letzten Minuten eine immense Anzahl direkter Anrufe von Kollegen erhalten, die keinen Zugriff mehr auf die gesamte Serverlandschaft haben. Eine geplante Downtime war zu keinem Zeitpunkt vorgesehen. Was ist hier los? Bitte geben Sie mir sofort einen Überblick über die Lage.

Best regards,

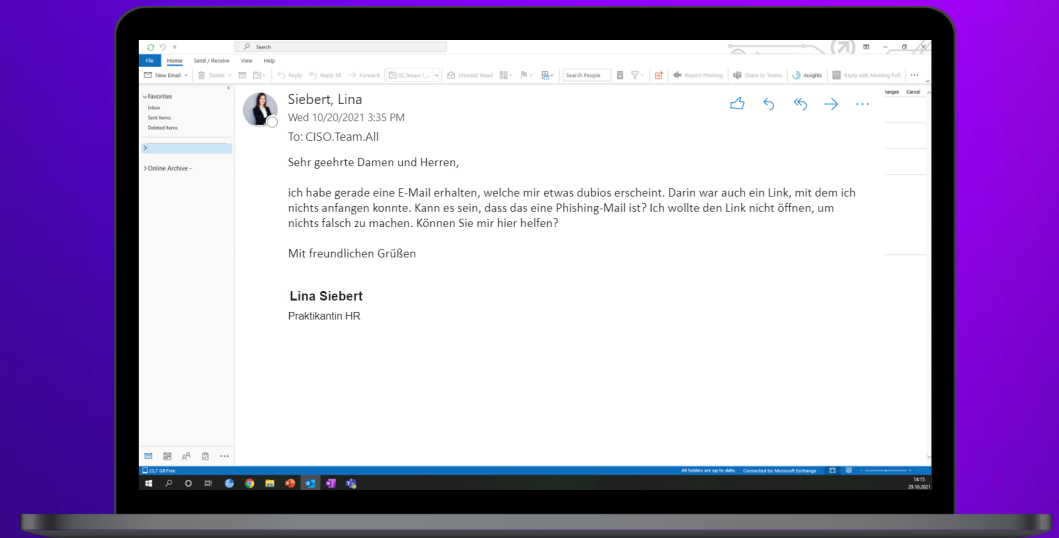
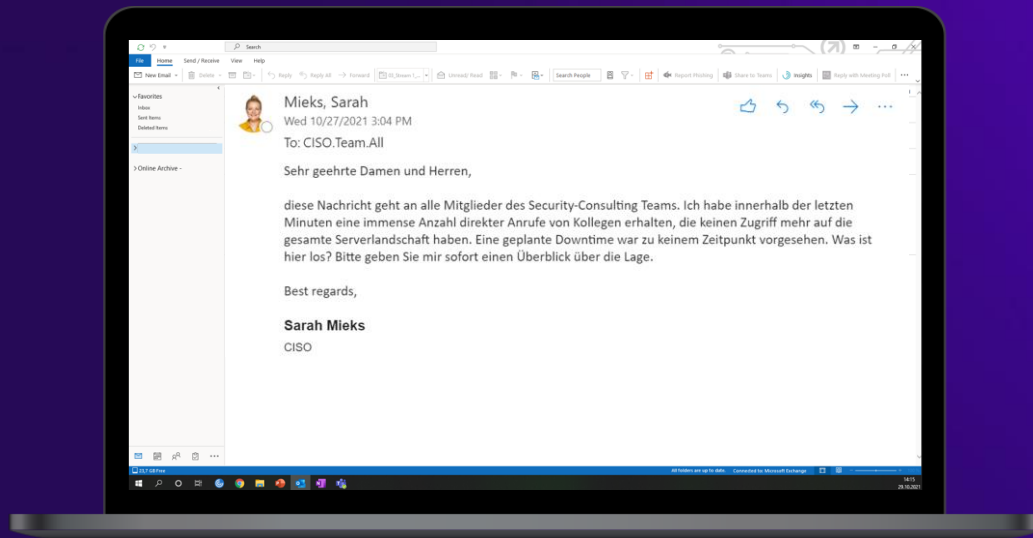
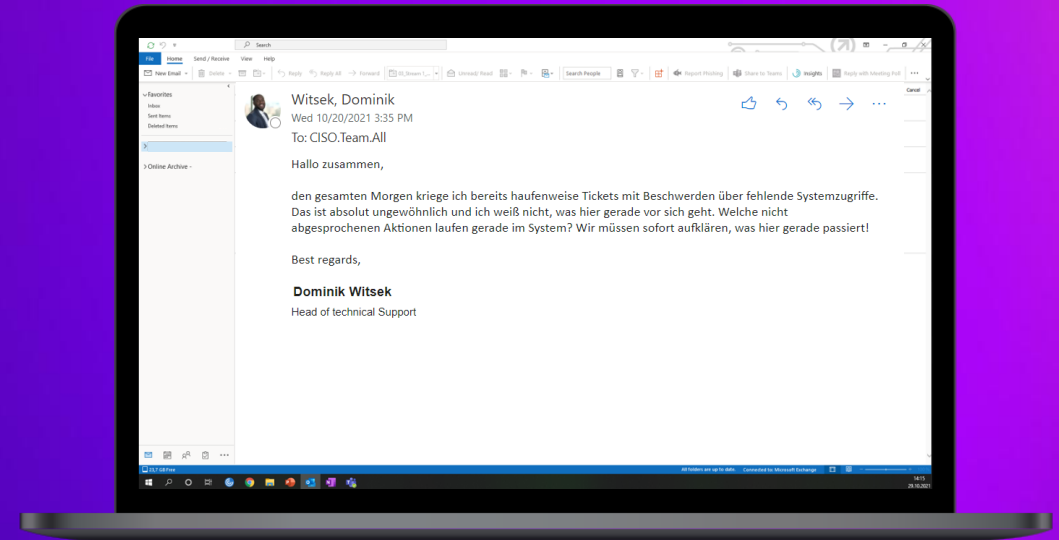
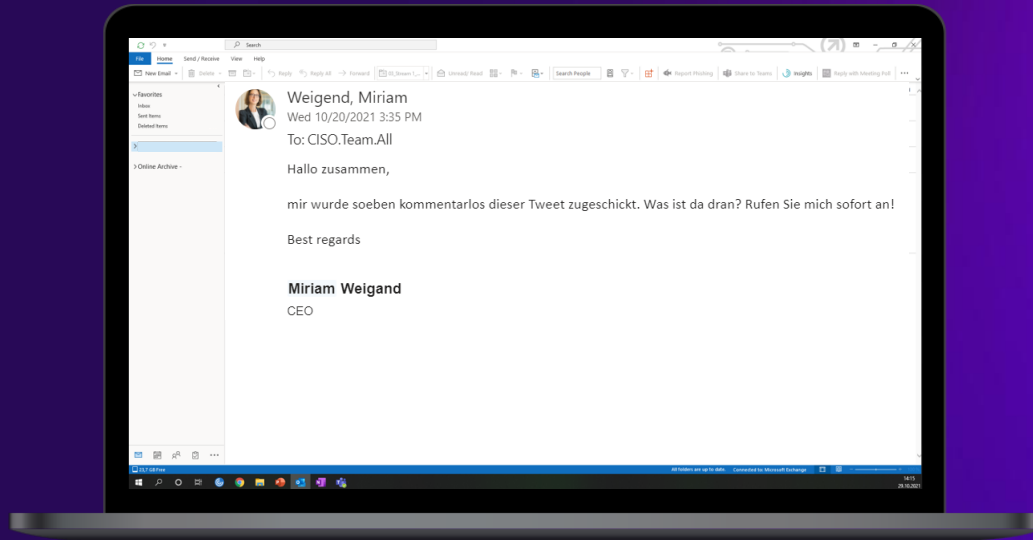
Sarah Mieks
CISO

At the bottom of the Outlook window, a status bar shows '23,7 GB Free', 'All folders are up to date.', 'Connected to: Microsoft Exchange', and the time '14:15' on '29.10.2021'. The Windows taskbar is visible at the very bottom of the screen.

The screenshot shows the Outlook web interface. At the top, there is a search bar and a ribbon with tabs for File, Home, Send / Receive, View, and Help. Below the ribbon are various action buttons like New Email, Delete, Reply, Reply All, Forward, and Search People. On the left side, there is a navigation pane with 'Favorites' (Inbox, Sent Items, Deleted Items) and 'Online Archive'. The main content area displays an email from 'Witsek, Dominik' sent on 'Wed 10/20/2021 3:35 PM' to 'To: CISO.Team.All'. The email body contains the following text: 'Hallo zusammen, den gesamten Morgen kriege ich bereits haufenweise Tickets mit Beschwerden über fehlende Systemzugriffe. Das ist absolut ungewöhnlich und ich weiß nicht, was hier gerade vor sich geht. Welche nicht abgesprochenen Aktionen laufen gerade im System? Wir müssen sofort aufklären, was hier gerade passiert! Best regards, Dominik Witsek Head of technical Support'. At the bottom of the email, there is a status bar showing '23,7 GB Free', 'All folders are up to date.', and 'Connected to: Microsoft Exchange'. The Windows taskbar is visible at the very bottom of the screen.

The screenshot shows a Microsoft Outlook window. The top ribbon includes 'File', 'Home', 'Send / Receive', 'View', and 'Help'. The 'Home' ribbon is active, showing options like 'New Email', 'Delete', 'Reply', 'Reply All', 'Forward', 'Unread/Read', 'Search People', 'Report Phishing', 'Share to Teams', 'Insights', and 'Reply with Meeting Poll'. On the left, the 'Favorites' pane shows 'Inbox', 'Sent Items', and 'Deleted Items'. The main content area displays an email from 'Siebert, Lina' dated 'Wed 10/20/2021 3:35 PM' with the recipient 'To: CISO.Team.All'. The email body contains the following text: 'Sehr geehrte Damen und Herren, ich habe gerade eine E-Mail erhalten, welche mir etwas dubios erscheint. Darin war auch ein Link, mit dem ich nichts anfangen konnte. Kann es sein, dass das eine Phishing-Mail ist? Ich wollte den Link nicht öffnen, um nichts falsch zu machen. Können Sie mir hier helfen? Mit freundlichen Grüßen'. The sender's name 'Lina Siebert' and title 'Praktikantin HR' are listed at the bottom of the email content. The bottom status bar shows '23,7 GB Free', 'All folders are up to date.', 'Connected to: Microsoft Exchange', and the time '14:15' on '29.10.2021'. The Windows taskbar is visible at the very bottom.

Vier Emails, aber wen kontaktieren wir als erstes?



1. CISO

Klären was genau passiert ist

2. CEO

Details weitergeben & weiteres Vorgehen abstimmen

3. UHD

Über Vorfall informieren

4. Praktikantin

Verdachtsfall aufklären

Vermeidet uninformiert bei der CEO aufzutauchen!

Wie hoch wäre der Schaden, sollte die Attacke durchgeführt werden?

Sollten tatsächlich alle unsere Daten verloren gehen, weiß ich nicht, ob wir uns davon jemals erholen würden.

Könnten wir notfalls alle Server ausstecken um eine Ausbreitung zu verhindern?

Ja, allerdings haben wir kein Backup, sprich die gesamte Firma wäre solange lahmgelegt, wie wir daran arbeiten das Problem zu lösen. Der Schaden wäre immens.

Wissen wir, wie der Hacker reingekommen ist?

Wir vermuten, dass einer unserer Mitarbeiter auf eine Phishing Mail reingefallen ist...

Könnten wir die Attacke irgendwie blocken?

Nein, sollte die Drohnung wahr sein, können wir nichts dagegen tun.

Wissen wir, ob die Drohnung ernst ist? Könnte es sich um eine leere Drohnung handeln?

Tatsächlich haben wir Hinweise darauf, dass es sich um einen Fake handeln könnte! Wir prüfen das gerade!





Hi, hier ist Miriam.
Ich habe gute Neuigkeiten!
Wir haben festgestellt, dass wir zwar den
Zugriff auf die Server verloren haben,
dies aber nicht an einer
Ransomwareattacke liegt!
Anscheinend handelt es sich nur um
einen **DDOS-Angriff**, durch welchen der
Zugriff auf die Server blockiert wurde.
Ransomware wurde dabei nicht
eingeschleust.
**Wir werden die Hacker also nicht
bezahlen!**
Gute Arbeit, Team!

Time to Recap!

1

Risiken

- Welche Risiken gibt es?
- Wie bewerte ich Risiken?

2

Sicherheitsmaßnahmen

- Welche Maßnahmen zur Risikominderung kann ich ergreifen?

3

Sicherheitsvorfall

- Wie gehe ich optimalerweise vor?
- Was muss als erstes geklärt werden?

Risiken - Welche Risiken gibt es?

1

Phishing

- Persönliche Informationen in betrügerischer Absicht erlangen

2

Hacking

- Benutzernamen und Passwörter entführen

3

Crypto-Mining

- Physischer Schaden und Stress für infizierte Endgeräte

4

Tailgating

- Sachschäden
- Diebstahl von Informationen und Eigentum



Um Risiken zu bewerten, wird die Schwere potentieller Schäden mit der Wahrscheinlichkeit eines Angriffs multipliziert. Die Darstellung kann zum Beispiel in einer Risikomatrix erfolgen.

Sicherheitsvorfall - Wie sollte ein Unternehmen optimaler Weise vorgehen?

1. Vorbereitung

Mitarbeiterschulungen, Guidelines, Awareness schaffen

2. Vorfall erkennen und melden

Je früher ein Vorfall gemeldet wird, desto schneller kann reagiert werden und Schaden vermieden werden

3. Analysieren

Über Vorfall informieren, Details sammeln, Risikoanalyse

4. Schadensbegrenzung

Beschädigte Systeme abschalten, Sicherheitslücken schließen

5. Maßnahmen nach einem Sicherheitsvorfall

Vorfall dokumentieren, Lessons learned dokumentieren

A large white arrow pointing to the right, centered on a purple gradient background. The arrow is outlined in white and contains the text 'Einstiegsmöglichkeiten' in a bold, white, sans-serif font.

Einstiegsmöglichkeiten

Einstiegsmöglichkeiten

STUDIERENDE

- Praktika
- Werkstudierendentätigkeiten

ABSOLVENT*INNEN

- Direkteinstieg

BERUFSERFAHRENE

- Direkteinstieg

Wir suchen dich!





Wen wir suchen



WIR SUCHEN **DICH**

- **ABSOLVENT*INNEN (BACHELOR/MASTER/DIPLOM) IN:**

- IT-Security, Cybersecurity, ...
- Wirtschaftswissenschaften
- Rechtswissenschaften
- (Wirtschafts-)Informatik
- (Wirtschafts-)Ingenieurwesen
- Naturwissenschaften (Physik, Mathe, ...)

- **ABSOLVENT*INNEN (AUSBILDUNG)**

- Fachinformatiker*in
- IT-Kaufmann/-frau

+ idealerweise erste praktische Erfahrungen



MAKE ACCENTURE MORE **YOU**

Dein Bewerbungs- prozess

01.

Online-
Bewerbung
über unsere
Webseite oder
unser
Talentnetzwerk
Bewerbung
über uns direkt

02.

Qualifikations-
bezogenes
Vorstellungsgespräch
(Telefoninterview)

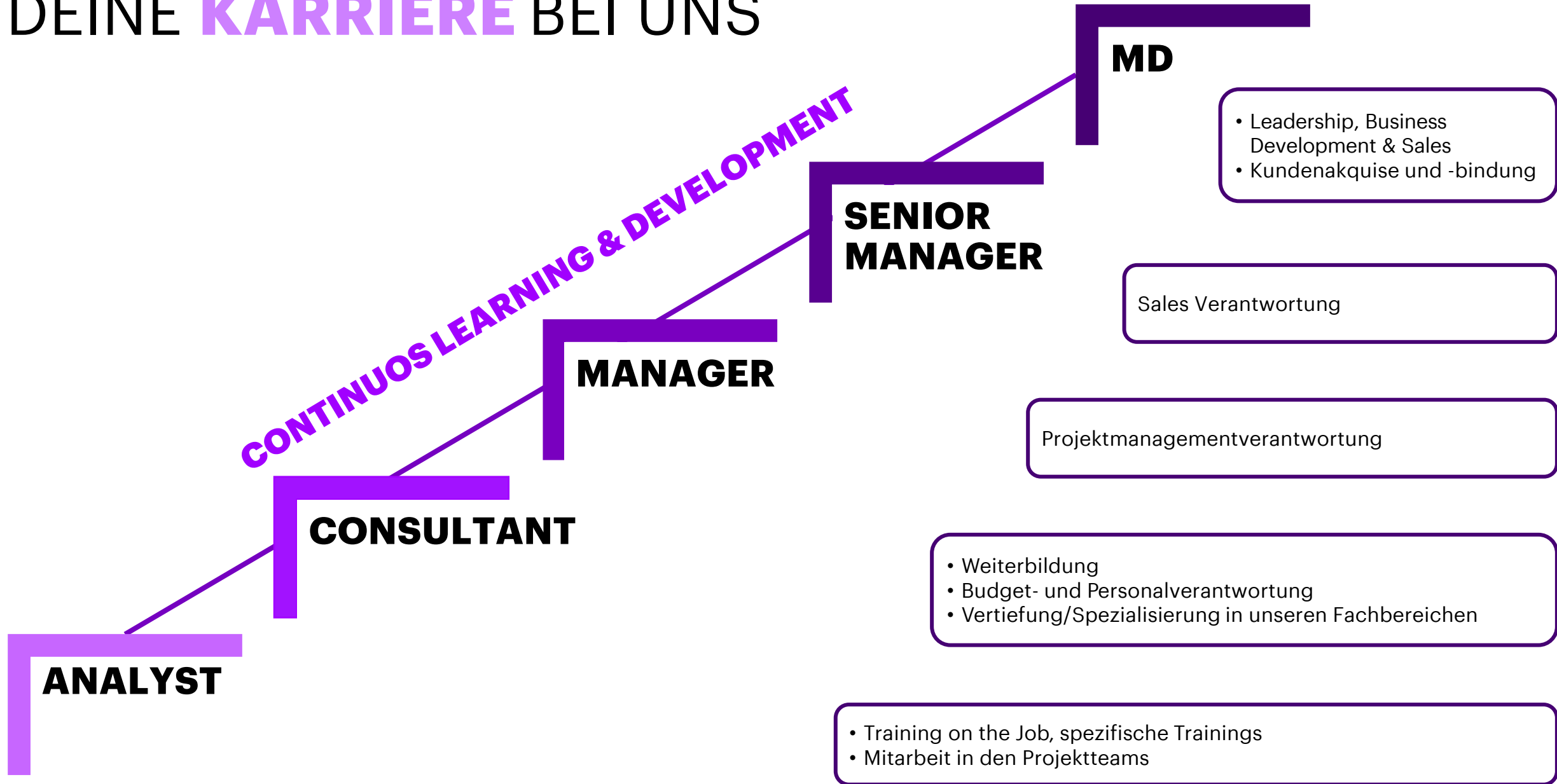
03.

Interview via
Teams

(Auswahltag
oder
persönliches
Gespräch)



DEINE **KARRIERE** BEI UNS



Du möchtest Junior Berater/Beraterin bei uns werden?



Einfach Code scannen und
direkt bewerben!
Wir freuen uns auf Dich

Oder doch lieber im Praktikum durchstarten und unser Arbeitsumfeld kennenlernen ?



Einfach Code scannen und
direkt bewerben!
Wir freuen uns auf Dich

Vielen Dank!