Wege ins Berufsfeld Cybersecurity

DAS KANNST DU MACHEN, SO KOMMST DU REIN!

Isabelle Ewald

Ich bin Isa

- Sen. Consultant Technology Strategy & Governance
- Tech-Kolumnistin
- Dozentin für digitale Kommunikation
- Verheiratet, 1 Kind (13)
- Dog Mummy
- Gerne in der Natur unterwegs

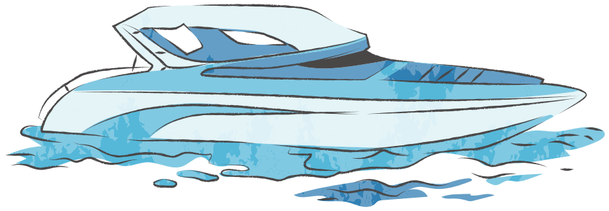
Lebensmotto:
Verrate ich später :-)

Mein Podcast :-)

Überall wo's Podcasts gibt :-)


MIND
THE
TECH
CYBER
CRIME
GESELLSCHAFT


KAFFEEFAHRT
INS DARKNET
mindthetech.de

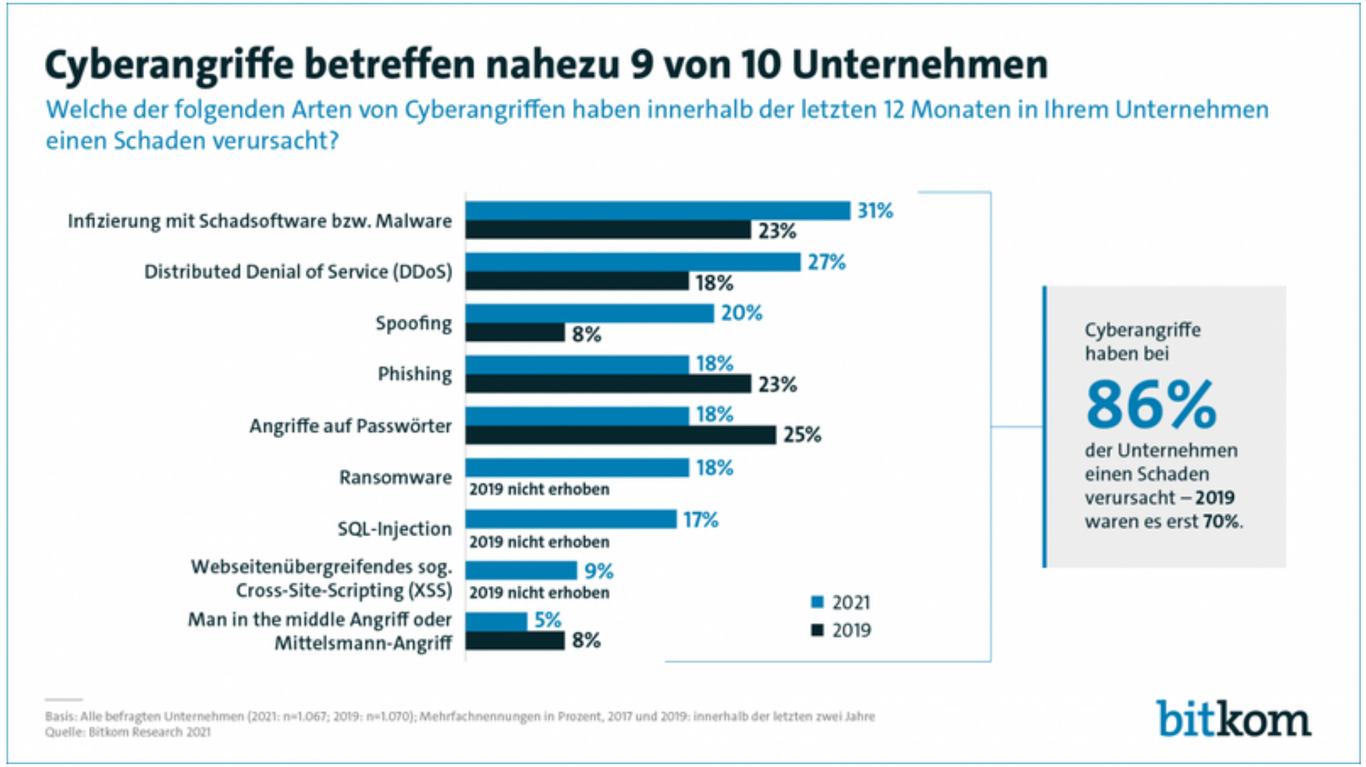


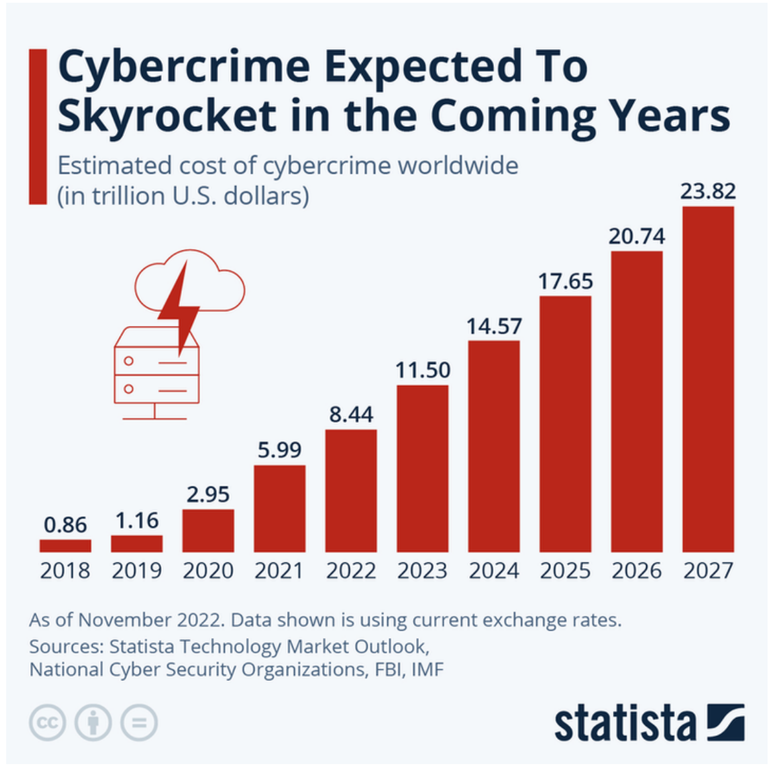
First things first:
Was ist Cybersecurity?

Cybersecurity befasst sich mit dem Schutz von Computersystemen, Netzwerken und Daten vor Bedrohungen wie Hacking, Datenlecks und Malware. Expert*innen entwickeln und implementieren Sicherheitsmaßnahmen, führen Risikoanalysen durch und reagieren auf Sicherheitsvorfälle, um die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen zu gewährleisten.

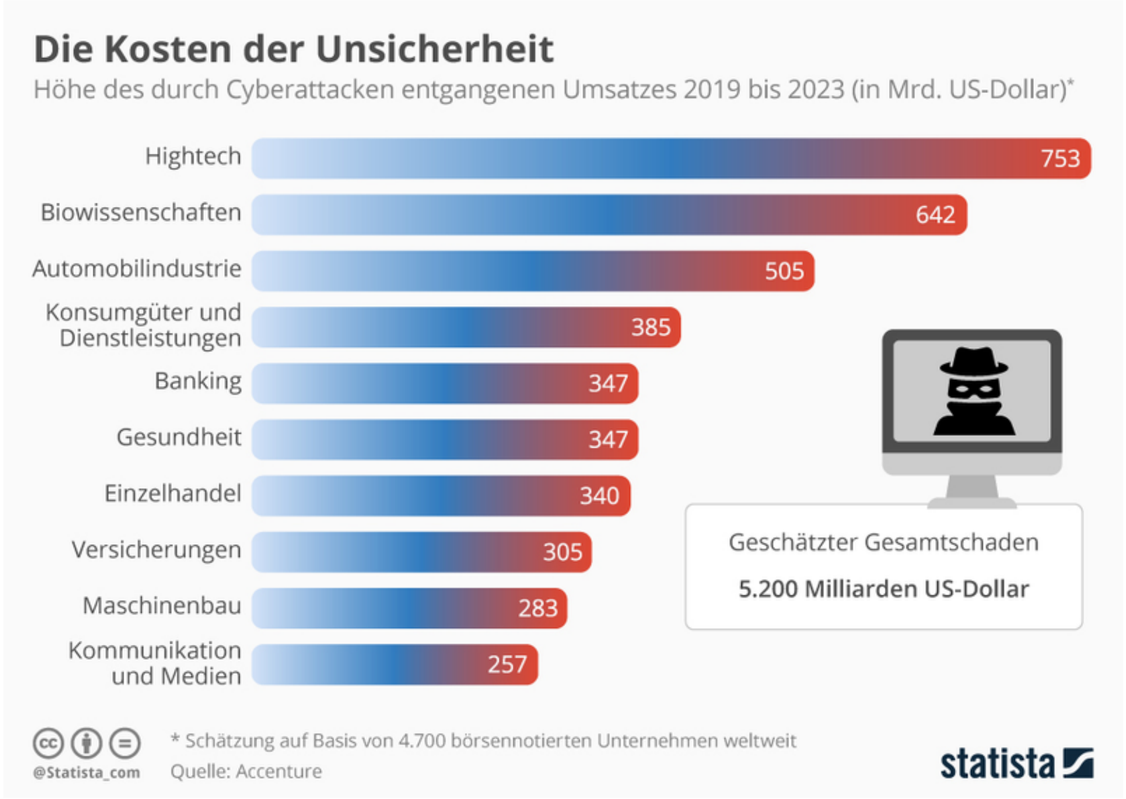
- **Hacktivism**
- **Threat Hunting**
- **Cyberwarfare**
- **Ethical Hacking**
- **Social Engineering**

Cybercrime ist keine Nische...





... sondern längst ein Wirtschaftsfaktor

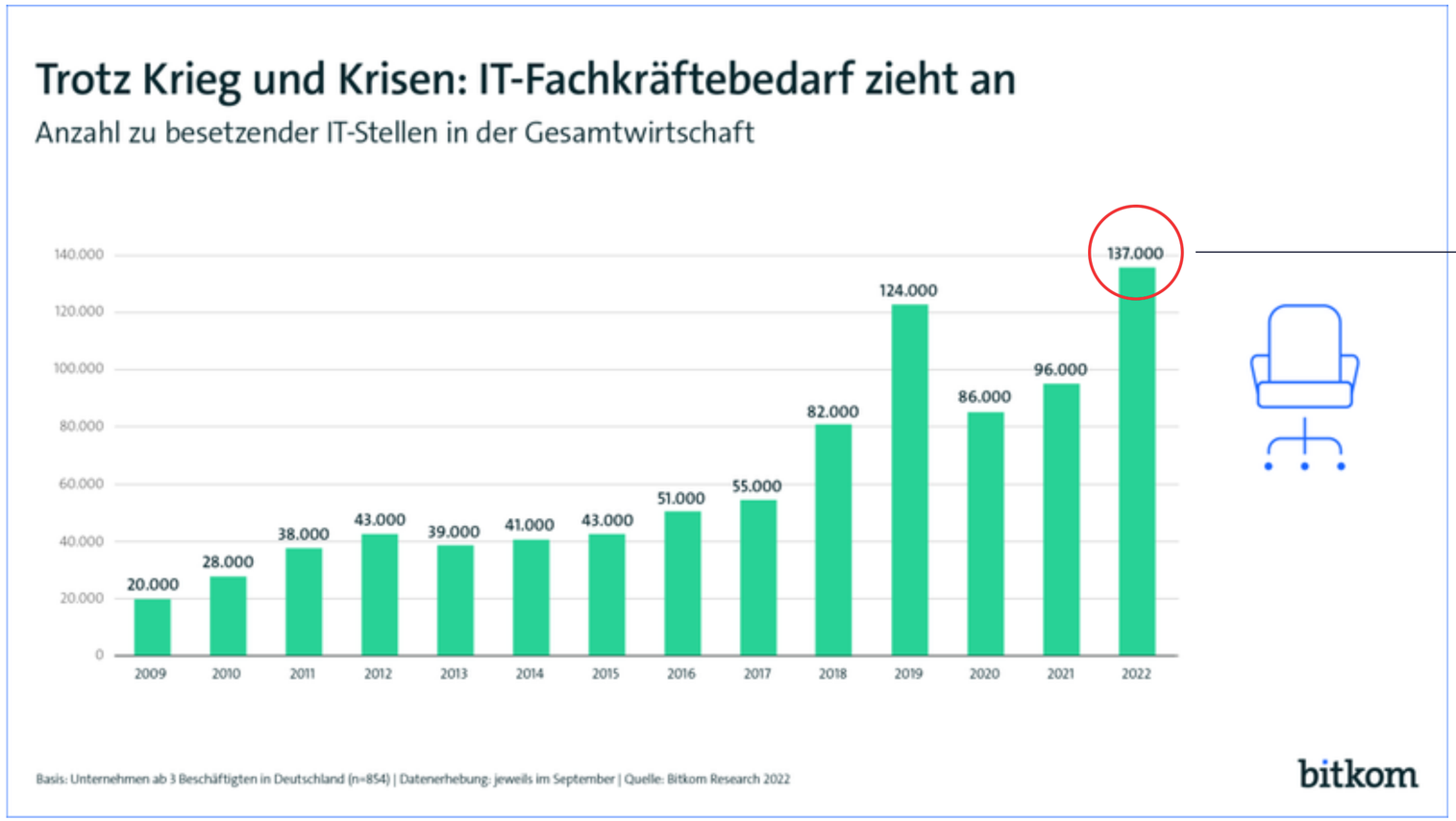


Cyberkriminalität kostete deutsche Unternehmen im Schnitt 13 Millionen US-Dollar pro Jahr (Stand 2019).

https://www.esg-global.com/hubfs/ESG-ISSA-Research-Report-Life-of-Cybersecurity-Professionals-Jul-2021.pdf

Eine Studie aus dem Jahr 2021 ergab, dass 95 Prozent der Befragten angaben, dass sich der Fachkräftemangel im Bereich der Cybersicherheit und die damit verbundenen Auswirkungen in den letzten Jahren nicht verbessert haben, während 44 Prozent sagten, dass sich die Situation nur verschlimmert habe.

Bedarf an IT-Sicherheitsexpert*innen ist e-n-o-r-m



Top-5 der gesuchten Profile:

- Anwendungsentwickler*in
- Systemadministrator*innen
- Netzwerkadministrator*innen
- Softwareentwickler*innen
- IT-Sicherheitsexpert*innen

https://www.staufenbiel.de/magazin/jobsuche/die-fuenf-gefragtesten-it-jobs.html

Aber... was ist eigentlich ein/e CyberSec-Experte/Expertin?

https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-role-profiles

Die Penetration Testerin

- **Informationsbeschaffung:** Die Penetration Testerin sammelt Informationen über das Zielsystem oder die Zielanwendung, einschließlich Netzwerkarchitektur, IP-Adressen, Betriebssysteme, verwendete Software und andere relevante Details.
- **Schwachstellenermittlung:** Die Penetration Testerin verwendet verschiedene Methoden und Tools, um Schwachstellen im Zielsystem zu identifizieren. Dies kann beispielsweise die Durchführung von Schwachstellenscans, das Ausnutzen bekannter Schwachstellen oder die Analyse des Quellcodes umfassen.
- **Exploit-Ausführung:** Sobald Schwachstellen identifiziert wurden, versucht die Penetration Testerin, diese auszunutzen, um Zugriff auf das System zu erlangen oder unerlaubte Aktionen durchzuführen. Dabei wird in der Regel versucht, so weit wie möglich in das System einzudringen, um die Auswirkungen eines tatsächlichen Angriffs zu simulieren.
- **Dokumentation und Berichterstattung:** Die Penetration Testerin dokumentiert alle durchgeführten Tests, die gefundenen Schwachstellen und die verwendeten Exploits. Ein abschließender Bericht wird erstellt, der eine Zusammenfassung der Ergebnisse, Empfehlungen zur Behebung der Schwachstellen und möglicherweise auch Beweise für erfolgreiche Angriffe enthält.
- **Nachtesten und Überprüfung:** Nachdem die Schwachstellen behoben wurden, kann eine Penetration Testerin erneut Tests durchführen, um sicherzustellen, dass die getroffenen Sicherheitsmaßnahmen effektiv waren und keine neuen Schwachstellen entstanden sind.

Die Chief Security Officerin

- **Strategie und Planung:** Die CISO entwickelt eine umfassende Sicherheitsstrategie, die auf die spezifischen Bedürfnisse und Risiken des Unternehmens zugeschnitten ist. Sie identifiziert potenzielle Bedrohungen und entwickelt Pläne zur Risikominderung und Sicherheitsverbesserung.
- **Richtlinien und Standards:** Die CISO erstellt Sicherheitsrichtlinien und -standards, die als Leitlinien für das Unternehmen dienen. Diese umfassen Richtlinien zur Zugriffskontrolle, zum Schutz vertraulicher Informationen, zur Datensicherung, zum Umgang mit Sicherheitsvorfällen und anderen Sicherheitsaspekten.
- **Sicherheitsinfrastruktur:** Die CISO ist für die Planung, Implementierung und Verwaltung der Sicherheitsinfrastruktur verantwortlich. Dazu gehören Firewalls, Intrusion Detection/Prevention Systeme, Verschlüsselungstechnologien, Authentifizierungsmechanismen und andere Sicherheitstools.
- **Sicherheitsüberwachung:** Die CISO überwacht kontinuierlich die Sicherheitslage des Unternehmens, indem er Sicherheitsereignisse und -vorfälle erkennt, analysiert und darauf reagiert. Dazu gehört auch die Durchführung von Sicherheitsaudits, Penetrationstests und anderen Sicherheitsprüfungen, um potenzielle Schwachstellen zu identifizieren.
- **Mitarbeiter- und Awareness-Training:** Die CISO sorgt dafür, dass die Mitarbeiter des Unternehmens über Sicherheitsrichtlinien und -praktiken informiert sind und angemessen geschult werden. Sier fördert die Sicherheitsbewusstsein in der gesamten Organisation und sensibilisiert die Mitarbeiter für die Bedeutung der Informationssicherheit.
- **Zusammenarbeit und Compliance:** Die CISO arbeitet eng mit anderen Abteilungen und Stakeholdern zusammen, um sicherzustellen, dass die Sicherheitsmaßnahmen mit den geschäftlichen Anforderungen und regulatorischen Vorgaben in Einklang stehen. Sie stellt sicher, dass das Unternehmen die geltenden Datenschutzbestimmungen und Sicherheitsstandards einhält.

Gehaltsstruktur

blog.whitelistrecruiting.de/it-security-gehalt

Alles so schön überschaubar...

... eigentlich könnten wir jetzt alle nach Hause gehen, oder?

Denn das ist alles nur die halbe Wahrheit!

Der ewige Eisberg

Nahezu alle Jobs entlang der digitalen Wertschöpfungskette

u.a. Produkt- und Projektmanager*in, Systemarchitekt*in, Softwareentwickler*in, Geschäftsführer*in, Risikoanalyst*in, Ingenieur*in, Online-Marketer*in, Datenanalyst*in

Der ewige Eisberg

Nahezu alle Jobs entlang der digitalen Wertschöpfungskette

u.a. Produkt- und Projektmanager*in, Systemarchitekt*in, Softwareentwickler*in, Geschäftsprozessanalyst*in, Ingenieur*in, Online-Marketer*in, Datenanalyst*in

SECURITY BY DESIGN

Security by Design meint...

Security by Design ist ein Konzept, das darauf abzielt, Sicherheitsaspekte bereits **in den Design- und Entwicklungsprozess** von Systemen, Produkten und Anwendungen zu integrieren.

Anstatt die Sicherheit als **nachträgliche Maßnahme** hinzuzufügen, wird sie von Anfang an in den gesamten Entwicklungsprozess eingebunden.

Das Konzept des Security by Design basiert auf der Erkenntnis, dass es effektiver und kostengünstiger ist, Sicherheitsmaßnahmen **frühzeitig zu planen und zu implementieren**, anstatt sie später zu korrigieren oder zu ergänzen, wenn Sicherheitslücken bereits vorhanden sind.

Meet Lucy

- Online-Marketerin bei einem großen Online-Shop
- Plant eine Kampagne zum Black Friday
- 360 Grad: Social Media, Influencer, Online-Ads, Newsletter...
- Ziel für den ROI erreicht, Kampagne erfolgreich beendet?

- **DDoS-Attacken**

  Mit einer enormen Menge an künstlichem Traffic werden Webserver überlastet und fallen unter Umständen komplett aus.

- **Ransomware-Angriffe**

  Wichtige Daten und/oder Systeme werden verschlüsselt und erste gegen Zahlung eines Lösegeldes wieder freigegeben.

- **Phishing**

  Versand gefälschter E-Mails, die Menschen dazu verleiten sollen, auf einen Betrug hereinzufallen (i.d.R. Abgreifen sensibler Informationen).

https://www.tuvit.de/de/aktuelles/newsroom/news/news-detail/article/fraud-liche-weihnachten-wie-cyberkriminelle-die-vorweihnachtszeit-fuer-ihre-zwecke-nutzen/

In welchem Team willst du spielen?

Team "Security by Design"

(generalistisches CyberSec-Wissen)

Team "Cyberdefender"

(spezialisiertes CyberSec-Wissen)

Up-Skilling: Eine Quellenauswahl

Podcast

Newsletter

Studium

YouTube

Weiterbildung

Mentoring

Bootcamps

Onlinekurse

Up-Skilling: Eine Quellenauswahl

Podcast

Newsletter

Studium

YouTube

Weiterbildung

Mentoring

Bootcamps

Onlinekurse

- Cyberbotschafterin
- Cyberstaatsanwältin
- Netzpolitikerin
- Consultant für Cybersecurity Awareness
- Dozentin für Datensicherheit
- Polizeicoachin/Profilerin
- Pentesterin
- Leiterin Beratungsstelle für Cybersicherheit
- Referentin für Cybersicherheit (BMI)

mindthetech.de/cyberfrauen/

Up-Skilling: Eine Quellenauswahl

Podcast

Newsletter

Studium

YouTube

Weiterbildung

Mentoring

Bootcamps

Onlinekurse

SECURITY INSIDER

ALGORITHM WATCH

digital pioneers

Ergänzend aus dem Plenum:

- Golem
- heise online

Up-Skilling: Eine Quellenauswahl

Podcast

Newsletter

Studium

YouTube

Weiterbildung

Mentoring

Bootcamps

Onlinekurse

- 129 Studiengänge (inkl. Privatschulen)
- Bachelor & Master
- Generalistisch und spezialisiert*
- *zum Beispiel IT-Forensik, IT-Recht oder Digital Investigations

Ergänzend aus dem Plenum:

- HS Offenburg
- HS Albstadt-Sigmaringen
- Ruhr-Universität Bochum
- HS Aalen
- Women's Cyber Academy von SANS

Up-Skilling: Eine Quellenauswahl

Sophie sagt:

*Ich möchte nur alle (nicht nur) studieninteressierte Menschen ermutigen, **nicht von Mathe abgeschreckt zu sein.** Ich war in der Schule eine komplette Niete und fuchse mich gerade rein (und es macht tatsächlich mega Spaß), weil ich Cyber Security studieren möchte (als Zweitstudium).*

Podcast

Newsletter

Studium

YouTube

Weiterbildung

Mentoring

Bootcamps

Onlinekurse

Semester	Fächer					
1	Mathematik 1 *[6 ECTS]*	Grundlagen der Programmierung 1 *[7 ECTS]*	Einführung in die Informatik 1 *[5 ECTS]*	Grundlagen der IT-Sicherheit *[5 ECTS]*	Einführungsprojekt *[2 ECTS]*	Gesellschaftliche Verantwortung sowie Innere und Äußere Sicherheit *[5 ECTS]*
2	Mathematik 2 *[6 ECTS]*	Grundlagen der Programmierung 2 *[7 ECTS]*	Einführung in die Informatik 2 *[7 ECTS]*	Software- Entwicklungsmethodik *[5 ECTS]*	Sichere Systeme *[5 ECTS]*	
3	Angewandte Mathematik für IT-Sicherheit *[6 ECTS]*	Web-Technologien *[5 ECTS]*	Netzwerke *[7 ECTS]*	Software-Design / SW-Architektur und Datenbanken *[7 ECTS]*	Softwaresicherheit & Security Testing *[5 ECTS]*	
4	Cloud-Architekturen und -Dienste *[5 ECTS]*	Projekt-, Qualitäts- und Risikomanagement *[5 ECTS]*	Protokolle der Netzsicherheit *[5 ECTS]*	Security Architectures & Security Engineering *[7 ECTS]*	Ethical Hacking-Praktikum *[5 ECTS]*	Fachwissenschaftliches Seminar *[3 ECTS]*
5	Kommunikations- und Teamkompetenz *[2 ECTS]*	Praktikum (18 Wochen) *[26 ECTS]*				Nachbereitendes Praxisseminar *[2 ECTS]*
6	Recht für IT-Sicherheit und Datenschutz *[3 ECTS]*	Grundlagen Künstliche Intelligenz und deren Anwendung in der IT-Sicherheit *[7 ECTS]*	Incidence Response & Netzwerkmonitoring *[5 ECTS]*	Sichere Netzwerkarchitekturen und Sicherheit vernetzter Anwendungen *[5 ECTS]*	Projekt *[5 ECTS]*	Grundlagen der Betriebswirtschaft und des Gründertums *[5 ECTS]*
7	Fachwissenschaftliche Wahlpflichtmodule 1 *[5 ECTS]*	Fachwissenschaftliche Wahlpflichtmodule 2 *[5 ECTS]*	Fachwissenschaftliche Wahlpflichtmodule 3 *[5 ECTS]*	Seminar Bachelorarbeit *[3 ECTS]*	Bachelorarbeit *[12 ECTS]*	

Grundlagen der Informatik und Mathematik | Cybersicherheit | Softskills und Zusammenarbeitsfähigkeit

Lehrplan für dualen Studiengang Cybersicherheit

Up-Skilling: Eine Quellenauswahl

Podcast

Newsletter

Studium

YouTube

Weiterbildung

Mentoring

Bootcamps

Onlinekurse

1. Semester	2. Semester	3. Semester	4. Semester	5. Semester	6. Semester	7. Semester	8. Semester
Grundlagen der IT Forensik	Betriebssysteme und Digitale Spuren I	Betriebssysteme und Digitale Spuren II	Algorithmen und Datenstrukturen	Grundlagen der Kryptologie	Kryptoanalyse	Malware Analysis	Projekt-management/ Wissenschaftliches Oberseminar 6 Wochen (10 Credits)
Einführung IT-Sicherheit	Allgemeine Forensik II	Computerforensische Methoden	Grundlagen Mobilfunkforensik	Forensische Bild- und Videoanalyse	Netzwerkforensik/ Abwehr von IT-Angriffen	Embedded Systems Forensics und Speichertechnologien	
Allgemeine Forensik I	Cybercrime II	Forensik in DBMS	Grundlagen der Datenanalyse und -visualisierung	Grundlagen des maschinellen Lernens	Datenkompression/ Multimediaformate	Der Sachverständige vor Gericht	Bachelorprojekt (Bachelorarbeit 12 Credits/ Kolloquium 3 Credits) 18 Wochen
Cybercrime I	Programmierung I	Programmierung II	Entwicklung und Design sicherer Systeme	Datennetze/ Cloud-Forensik	Predictive Policing/ Dunkelfeld	Social Engineering und OSINT	
			Krisenmanagement	Text Retrival und Textmining	Softwareprojekt		
20	20	20	25	25	25	20	25

Fundamente der Informatik
Programmierung
Forensik
Kryptologie
Praxismodule

Lehrplan für Bachelor IT-Forensik
Hochschule Mittweida

Up-Skilling: Eine Quellenauswahl

Podcast

Newsletter

Studium

YouTube

Weiterbildung

Mentoring

Bootcamps

Onlinekurse

The Morpheus Tutorials

Ein Kanal rund um das Thema Informatik und Programmieren mit über 2000 Videos! Ob Python, Java oder Webdev oder doch Hacken u...

YouTube

youtube.com/@TheMorpheusTutorials

Up-Skilling: Eine Quellenauswahl

Podcast

Newsletter

Studium

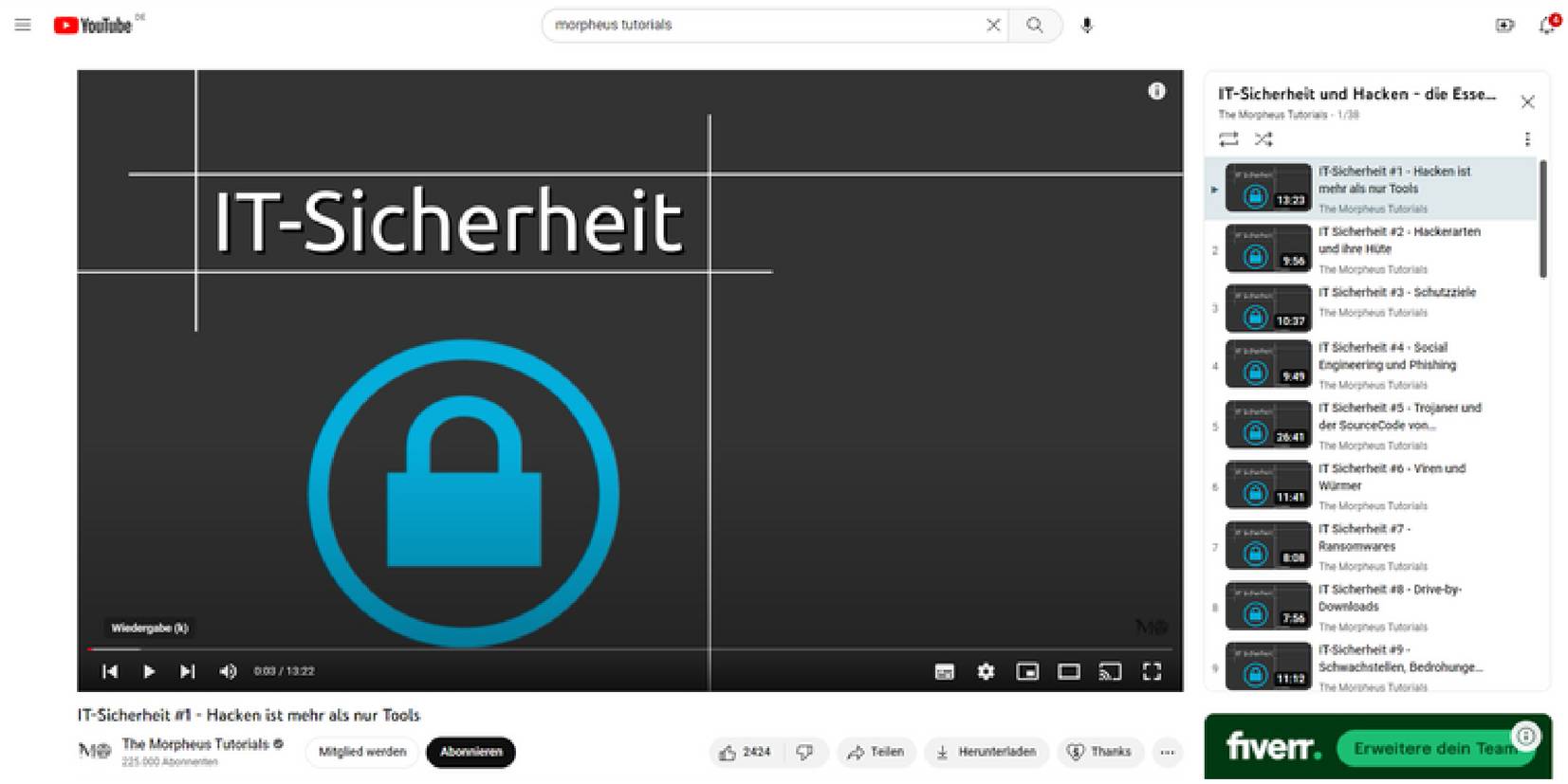
YouTube

Weiterbildung

Mentoring

Bootcamps

Onlinekurse



Up-Skilling: Eine Quellenauswahl

Podcast

Newsletter

Studium

YouTube

Weiterbildung

Mentoring

Bootcamps

Onlinekurse

bitkom akademie

Seminare Inhouse Studie 2022 Bitkom Management Club News Kontakt

Seminar	Format	Datum	Ort	Verfügbar	Preis
IT-Sicherheit IT-Sicherheitsbeauftragter (ITSiBe) / Chief Information Security Officer (CISO)	Zertifikatslehrgang	12.06.23	Online		2.200 €
IT-Sicherheit BSI IT-Grundschutz-Berater – Aufbauschulung	Workshop	15.06.23	Online		1.600 €
IT-Sicherheit IT-Security Club	Live-Online	16.06.23	Online		kostenfrei
IT-Sicherheit Digitaltag 2023: Passwörter sicher und einfach – das geht!	Live-Online	16.06.23	Online		kostenfrei
IT-Sicherheit BSI IT-Grundschutz-Praktiker – Zertifikatslehrgang	Zertifikatslehrgang	19.06.23	Online		2.200 €
IT-Sicherheit Angreifern mit dem Zero Trust IT-Sicherheitsmodell keine Chance bieten	Live-Online	27.06.23	Online		kostenfrei
IT-Sicherheit DNS-Protokoll basierte Security Operation	Live-Online	04.07.23	Online		kostenfrei
IT-Sicherheit Wie gelingt ein erfolgreicher Projektstart?	Live-Online	05.07.23	Online		kostenfrei
IT-Sicherheit Crashkurs IT-Fortgeschrittenenwissen	Workshop	06.07.23	Online		1.300 €
IT-Sicherheit Crashkurs IT-Hintergrundwissen	Workshop	10.07.23	Online		1.300 €
IT-Sicherheit Security Awareness für Administratoren und Entwickler schaffen	Live-Online	12.07.23	Online		kostenfrei
IT-Sicherheit IT-Sicherheitsbeauftragter (ITSiBe) / Chief Information Security Officer (CISO)	Zertifikatslehrgang	13.07.23	Online		2.200 €
IT-Sicherheit IT-Notfallmanagement: Business Continuity Manager (BCM)	Zertifikatslehrgang	20.07.23	Online		2.100 €
IT-Sicherheit ISMS in der Praxis – Zertifikatslehrgang	Zertifikatslehrgang	31.07.23	Online		2.200 €
IT-Sicherheit BSI IT-Grundschutz-Praktiker – Zertifikatslehrgang	Zertifikatslehrgang	03.08.23	Online		2.200 €
IT-Sicherheit IT-Notfallmanagement: Business Continuity Manager (BCM)	Zertifikatslehrgang	10.08.23	Online		2.100 €
IT-Sicherheit IT-Sicherheitsbeauftragter (ITSiBe) / Chief Information Security Officer (CISO)	Zertifikatslehrgang	17.08.23	Online		2.200 €

Up-Skilling: Eine Quellenauswahl

Podcast

Newsletter

Studium

YouTube

Weiterbildung

Mentoring

Bootcamps

Onlinekurse

WOMEN 4CYBER
EUROPEAN CYBER SECURITY ORGANISATION

Up-Skilling: Eine Quellenauswahl

Podcast

Newsletter

Studium

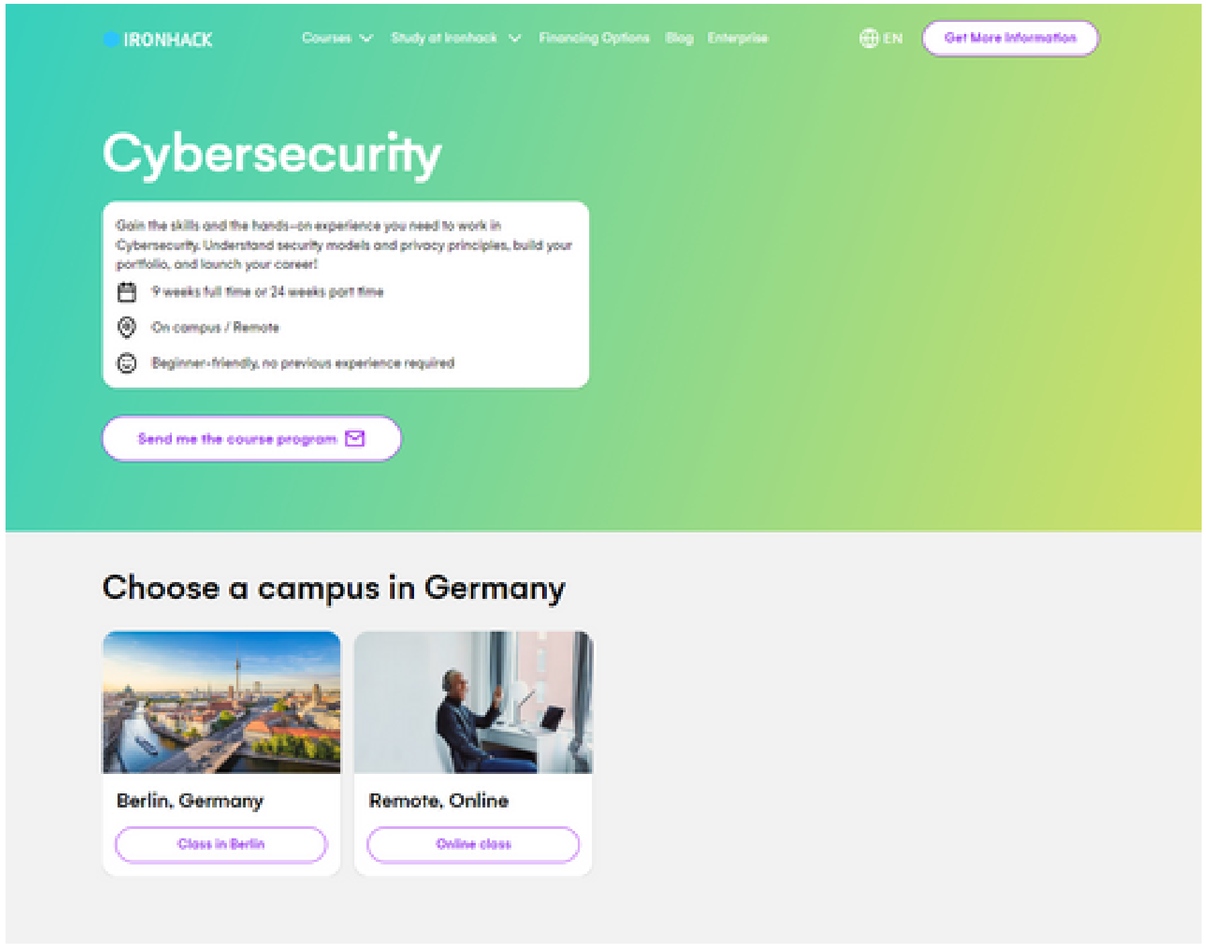
YouTube

Weiterbildung

Mentoring

Bootcamps

Onlinekurse



Up-Skilling: Eine Quellenauswahl

Podcast

Newsletter

Studium

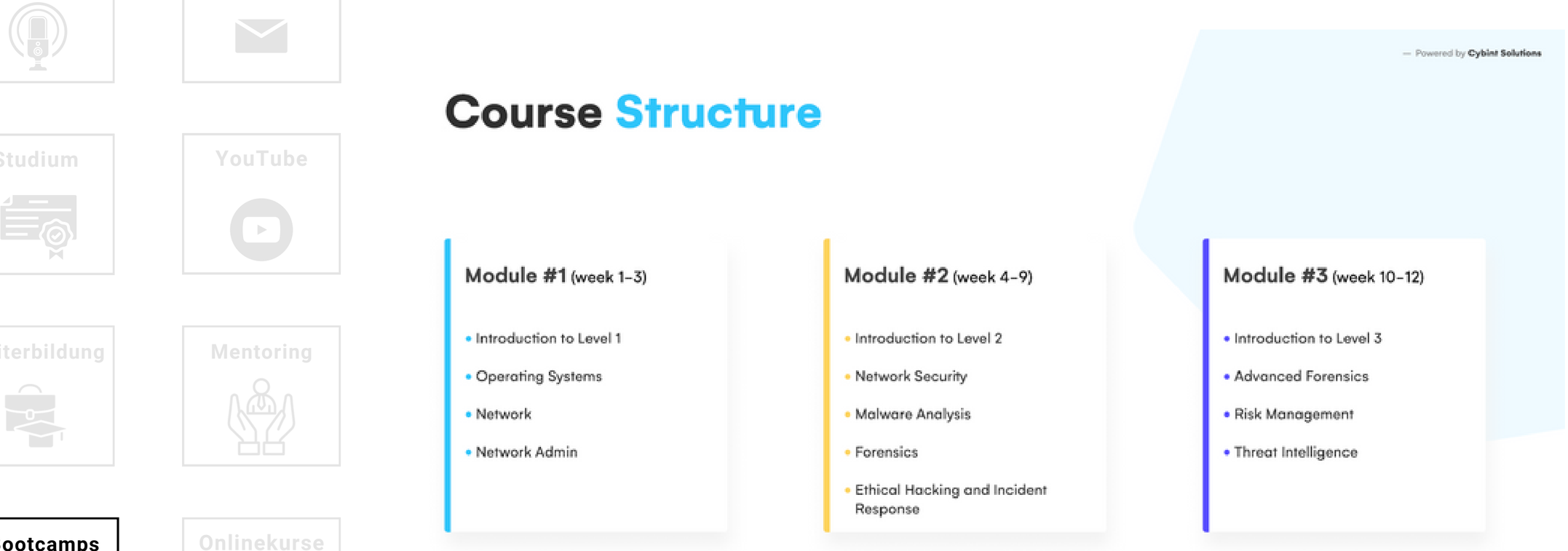
YouTube

Weiterbildung

Mentoring

Bootcamps

Onlinekurse



Up-Skilling: Eine Quellenauswahl

Podcast

Newsletter

Studium

YouTube

Weiterbildung

Mentoring

Bootcamps

Onlinekurse

coursera

UDACITY

OPEN HPI

udemy

Fraunhofer ACADEMY

Ergänzend aus dem Plenum:

- tryhackme.com/
- edx.org
- netacad.com/courses/cybersecurity

Up-Skilling: Eine Quellenauswahl

Podcast

Newsletter

Studium

YouTube

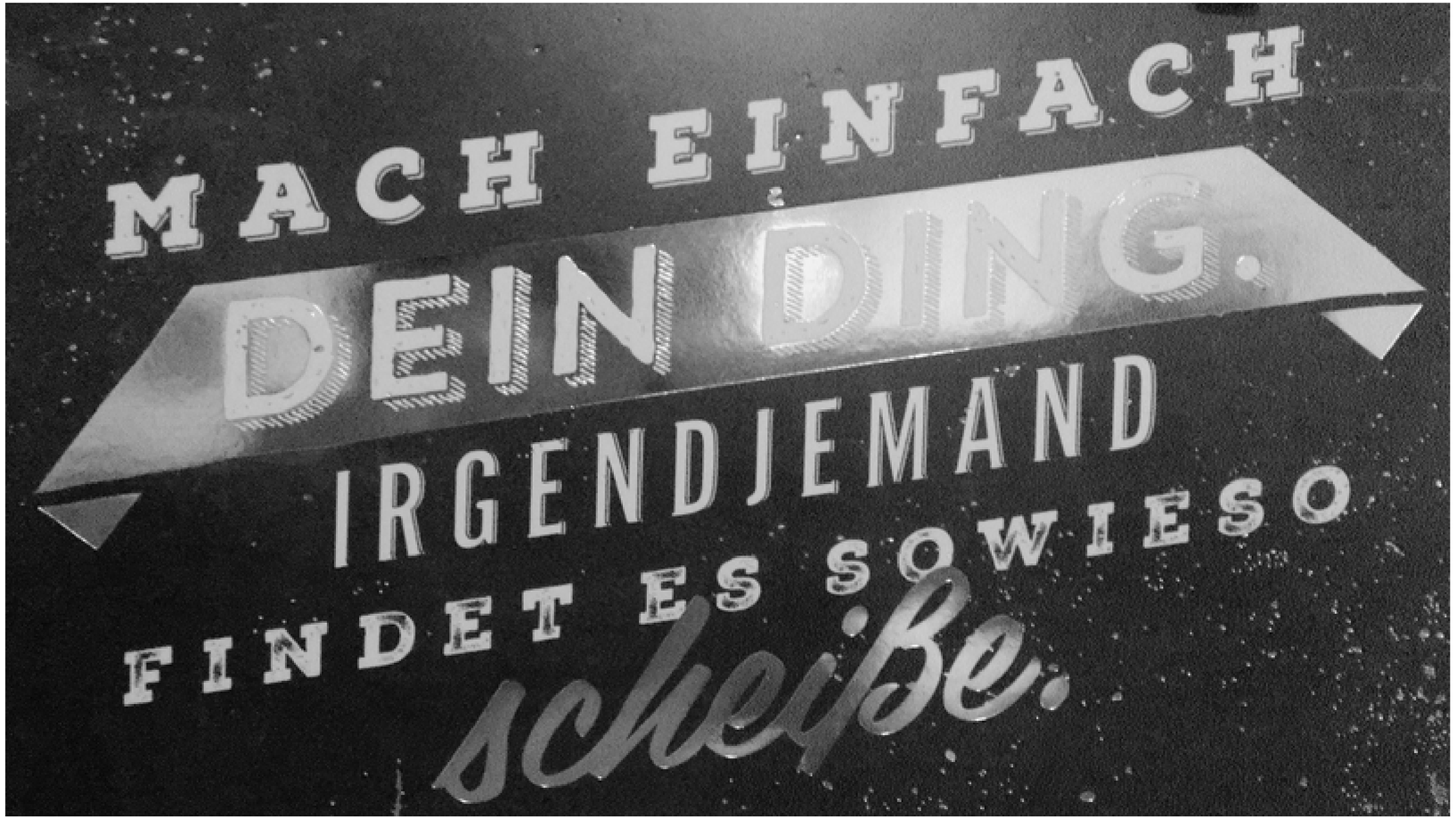
Weiterbildung

Mentoring

Bootcamps

Onlinekurse

Mein Motto


MACH EINFACH
DEIN DING.
IRGENDJEMAND
FINDET ES SOWIESO
scheiße.

Und denkt dran:


Vielen Dank