Wer von euch wurde schon ~~einmal~~ gehackt?

«There are two types of companies: those who have been hacked, and those who don’t yet know they have been hacked.»

Dmitri Alperovitch, McAfee Vice President of Threat Research

Gemeinsam ist sicherer

«Cybersecurity Framework» bestehend aus Standards, Richtlinien und Best Practices

admin
.digital

Verein OneGov.ch
12.11.2024

Themen

1. **Über uns**
2. **Relevanz von Cybersicherheit**
3. **Was muss ich schützen?**
4. **Was ist die Bedrohung?**
5. **Risiko-Management**
6. **Standards ISO-27001 (NIST CSF)**
7. **Best Practices**

seantis
data. web. applications.

Über uns

1/7

Geschäftsleitung

seantis gmbh entwickelt seit 2005 Webapplikationen für die öffentliche Verwaltung, die medizinische Forschung sowie für die Aviatik. Wir sind ein agiles Team vom 10 Personen und bilden einen Lehrling sowie einen Praktikanten aus.

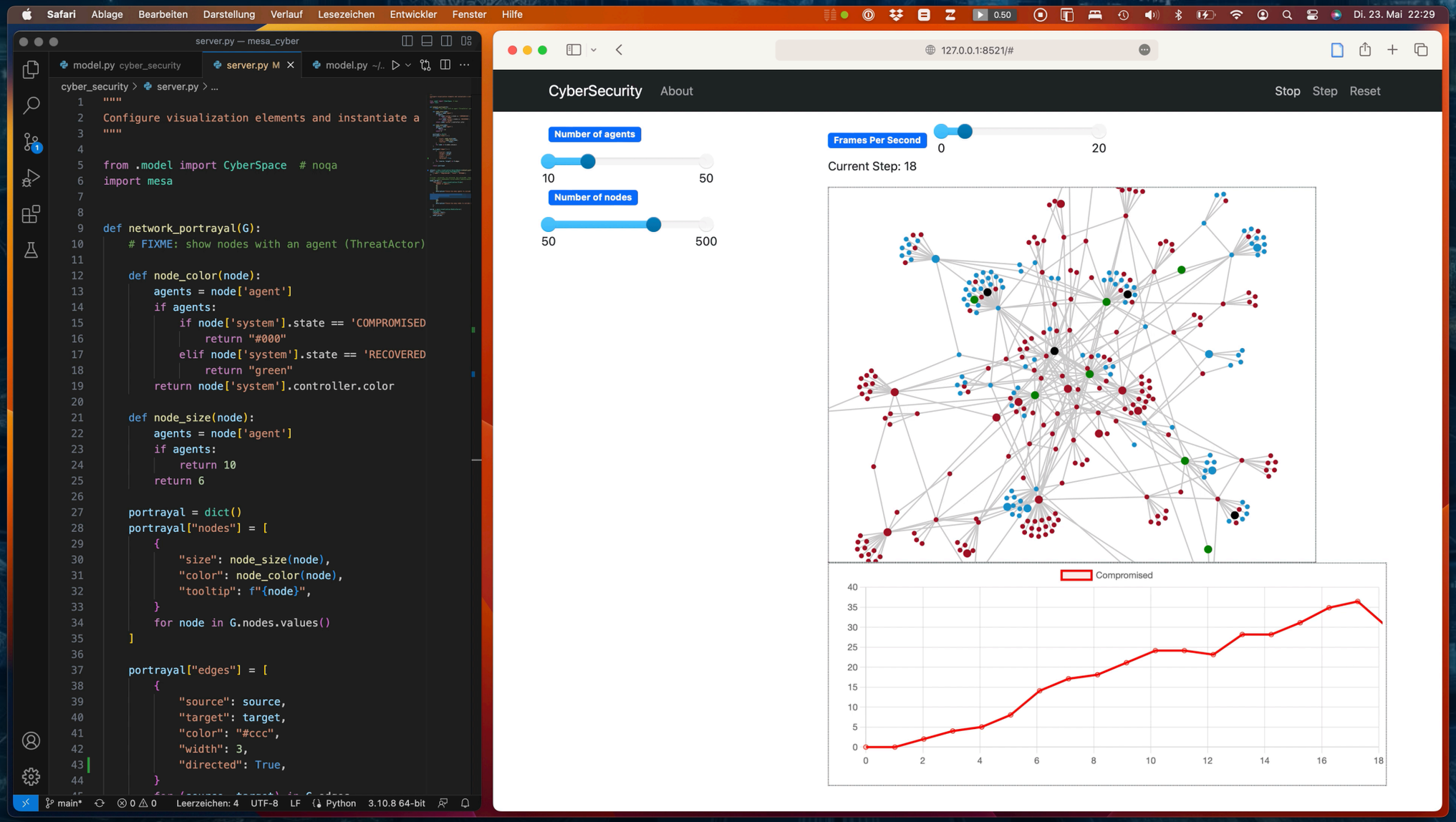
Fabian Reinhard (M A UZH)
Managing Partner, Business Analyst

Fabian studierte Politikwissenschaften, VWL und Allgemeines Staatsrecht. Er forscht aktuell als freier Doktorand an der Universität Zürich zum Thema Cybersecurity.

Dr. Tobias Reinhard (dipl. inform. UZH)
Partner, Software Engineer

Tobias studierte Informatik an der Universität Zürich und promovierte ebenda im Bereich Requirements Engineering.

Cyber Conflict Simulation



DALL-E

seantis
data. web. applications.

Relevanz von Cybersicherheit

2/7

Die Bedrohung nimmt zu

1. Alle **8.5 Minuten** wurde beim National Cyber Security Centre (NCSC) ein Cyber-Vorfall gemeldet.

2. Mit 34’789 gemeldeten Cyber-Vorfällen an das NCSC in der ersten Hälfte des Jahres 2024 haben sich die **Zahlen im Vergleich zum gleichen Zeitraum des Vorjahres fast verdoppelt**.

https://www.ncsc.admin.ch/ncsc/en/home/aktuell/im-fokus/2024/ncsc-hjb-2024-1.html

seantis
data. web. applications.

Was muss ich schützen?

3/7

DALL-E

Inventar der digitalen Vermögenswerte

CIA Triad

1. Vertraulichkeit
2. Integrität
3. Verfügbarkeit

- Medical Research Database
- DNS Server
- Backup Server

C + I + A = CIA Score

seantis
data. web. applications.

Was ist die Bedrohung?

4/7

Schwachstelle, Bedrohung, Risiko

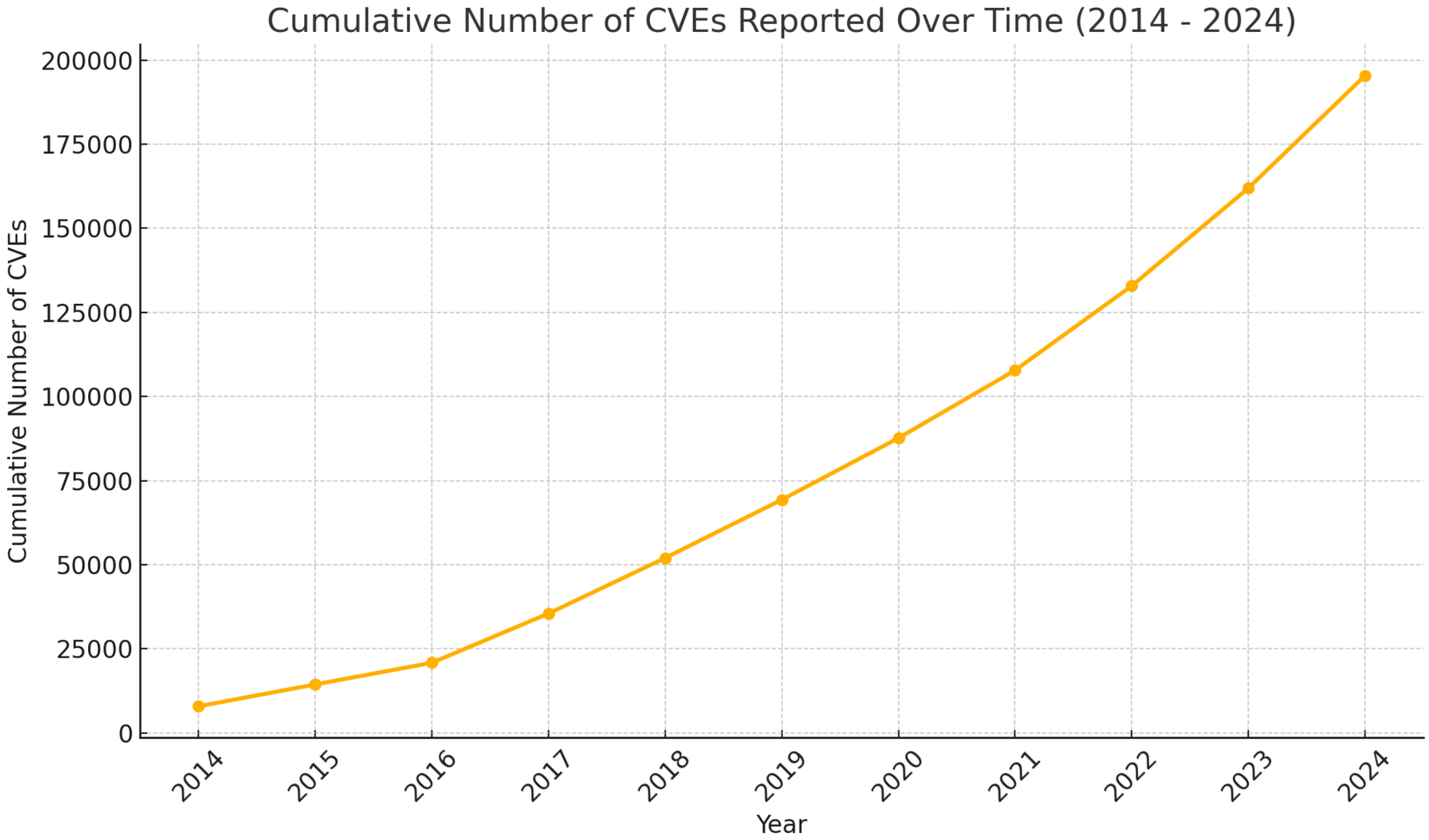
1. Eine **Schwachstelle** setzt deine Organisation Bedrohungen aus.

2. Eine **Bedrohung** ist ein böswilliges oder negatives Ereignis, das eine Schwachstelle ausnutzt.

3. Ein **Risiko** ist das Potenzial für Verlust und Schaden, wenn die Bedrohung tatsächlich eintritt.

https://www.splunk.com/en_us/blog/learn/vulnerability-vs-threat-vs-risk.html

Schwachstellen (CVE)



https://www.cve.org/About/Metrics, eigene Darstellung

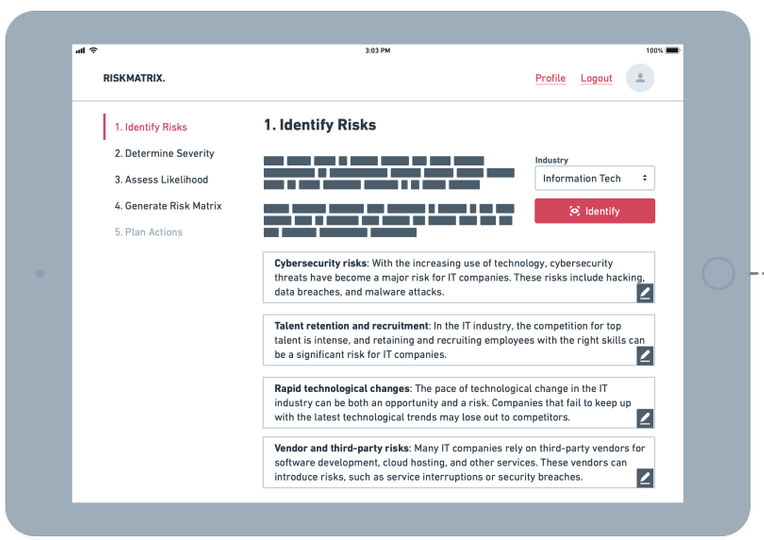
seantis
data. web. applications.

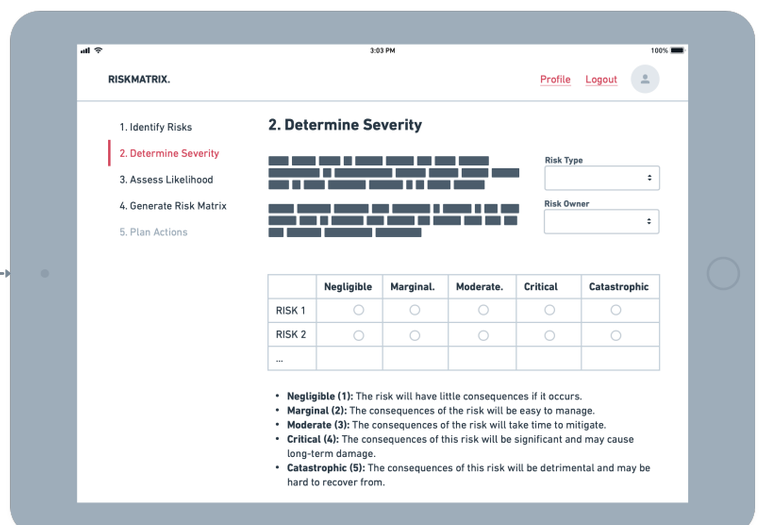
Risiko-Management

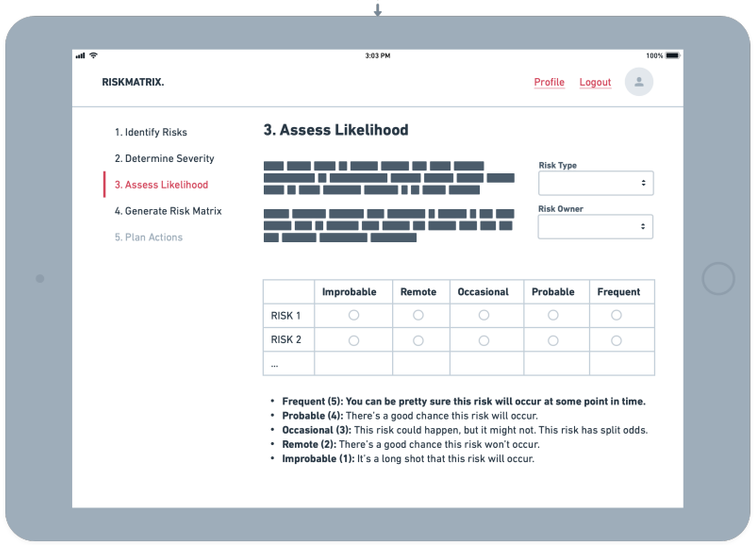
5/7

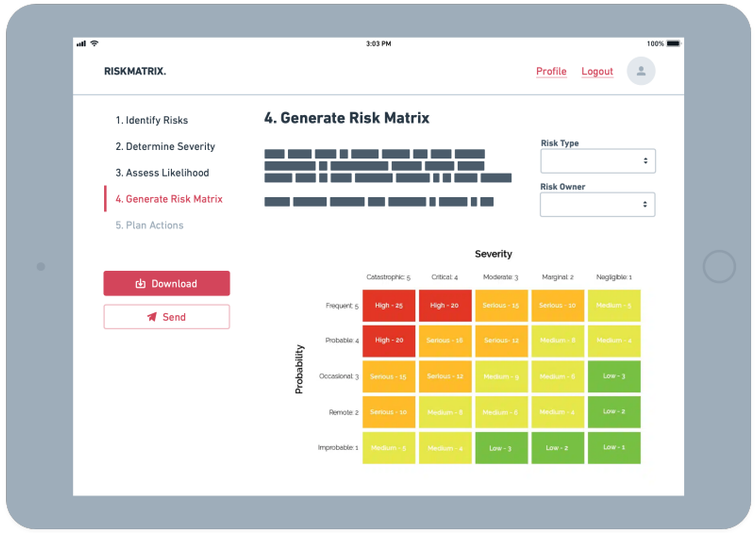
RiskMatrix

http://seantis.ch/riskmatrix









Risikoerkennung

Risikobewertung

Risikosteuerung

seantis
data. web. applications.

ISO 27001 / NIST CSF

6/7

NIST CSF (Core Functions)

National Institute of Standards and Technology (NIST):
Cybersecurity Framework (CSF)

1. **Identifizieren**: Entwicklung eines Verständnisses für Risiken gegenüber Systemen, Personen, Vermögenswerten, Daten und Fähigkeiten.

2. **Schützen**: Umsetzung von Schutzmassnahmen, um die Bereitstellung kritischer Dienste sicherzustellen.

3. **Erkennen**: Ermöglichung der rechtzeitigen Erkennung von Cybersecurity-Vorfällen.

4. **Reagieren**: Massnahmen ergreifen, um erkannte Vorfälle zu minimieren und den Schaden zu begrenzen.

5. **Wiederherstellen**: Wiederherstellung von Fähigkeiten und Diensten, die durch einen Cybersecurity-Vorfall beeinträchtigt wurden.

Zentrale Elemente ISO 27001

1. Risikomanagement ⚠️
2. Sicherheitsmaßnahmen (93 Controls) 🔒
   - Organisatorische Kontrollen: 37
   - Personenbezogene Kontrollen: 8
   - Physische Kontrollen: 14
   - Technologische Kontrollen: 34
3. Managementverantwortung 👔
4. Kontinuierliche Verbesserung 🏋️
5. Dokumentation und Nachweisführung 📝
6. Schulung und Sensibilisierung 👩‍🏫

ZERTIFIKAT CERTIFICAT

ATTESTA

SCHWEIZER ZERTIFIZIERUNGSGESELLSCHAFT AG

ZERTIFIKAT

Die ATTESTA Schweizer Zertifizierungsgesellschaft AG in CH-8806 Bäch
UID: CHE-357.699.924 - bescheinigt, dass die Firma:

Seantis GmbH
Pilatusstrasse 3
6003 Luzern

Für den Geltungsbereich:
Entwicklung und Betrieb von digitalen Plattformen für die medizinische Forschung, die öffentliche Verwaltung sowie für die Aviatik

ein Managementsystem eingeführt hat und anwendet nach:
ISO 27001 : 2022 Informationssicherheit

Registriernummer	224-03-080.Q
Erstzertifizierung:	08. März 2024
Überwachungsaudit:	
Nächstes Überwachungsaudit	März 2025
Gültig bis:	07. März 2027

Kay Baumgartner
Mitglied des Zertifizierungsrates
Bäch 15.03.2024

IRQAO
ATTESTA ISO 27001 ZERTIFIZIERT
ISO CASCO 17021 anerkannt überwacht unabhängig

Ziele und KPIs (Praxis)

1. Die Services, welche wir für unsere Kunden entwickeln und betreiben, sind hochverfügbar. [Z1]
2. Wir legen grossen Wert auf Benutzerfreundlichkeit unserer Services und streben darum eine gute Performance und schnelle Antwortzeiten an. [Z2]
3. Wir schützen die Vertraulichkeit der Daten mit geeigneten Massnahmen der Verschlüsselung; die eingesetzten Verfahren werden regelmässig überprüft und auf dem modernsten Stand der Technik gehalten. [Z3]
4. Unsere Mitarbeiter sind gut ausgebildet, verfügen über ein breites Knowhow und bilden sich regelmässig weiter. [Z4]
5. Wir treiben die kontinuierliche Verbesserung der Informationssicherheit voran. [Z5]
6. Unsere Webapplikationen sind sicher und werden regelmässig auf bekannte Sicherheitslücken geprüft. [Z6]
7. Wir vermeiden potentiellen Datenverlust indem wir funktionsfähige Backup- und Restore-Prozesse betreiben und überwachen. [Z7]
8. Wir entwickeln und betreiben State-of-the-Art Webapplikation und lösen veraltete Legacy-Software ab. [Z8]
9. Unser testgetriebener Entwicklungsansatz beinhaltet automatisierte und transparente Build- und Test-Prozeduren. [Z9]
10. Wir überwachen unsere Services und erkennen Fehler proaktiv. [Z10]
11. Mit unseren Kunden bleiben wir im Austausch und informieren sie regelmässig über relevante Neuigkeiten rund um unsere Firma und Services. [Z11]
12. Wir führen einen Prozess mit den geeigneten Tools um Ereignisse, welche die Informationssicherheit gefährden können, schnellstmöglich zu erkennen und so zeitnah wie möglich Massnahmen zu ergreifen. [Z12]

https://www.seantis.ch/portrait/informationssicherheit-iso-27001/

seantis
data. web. applications.

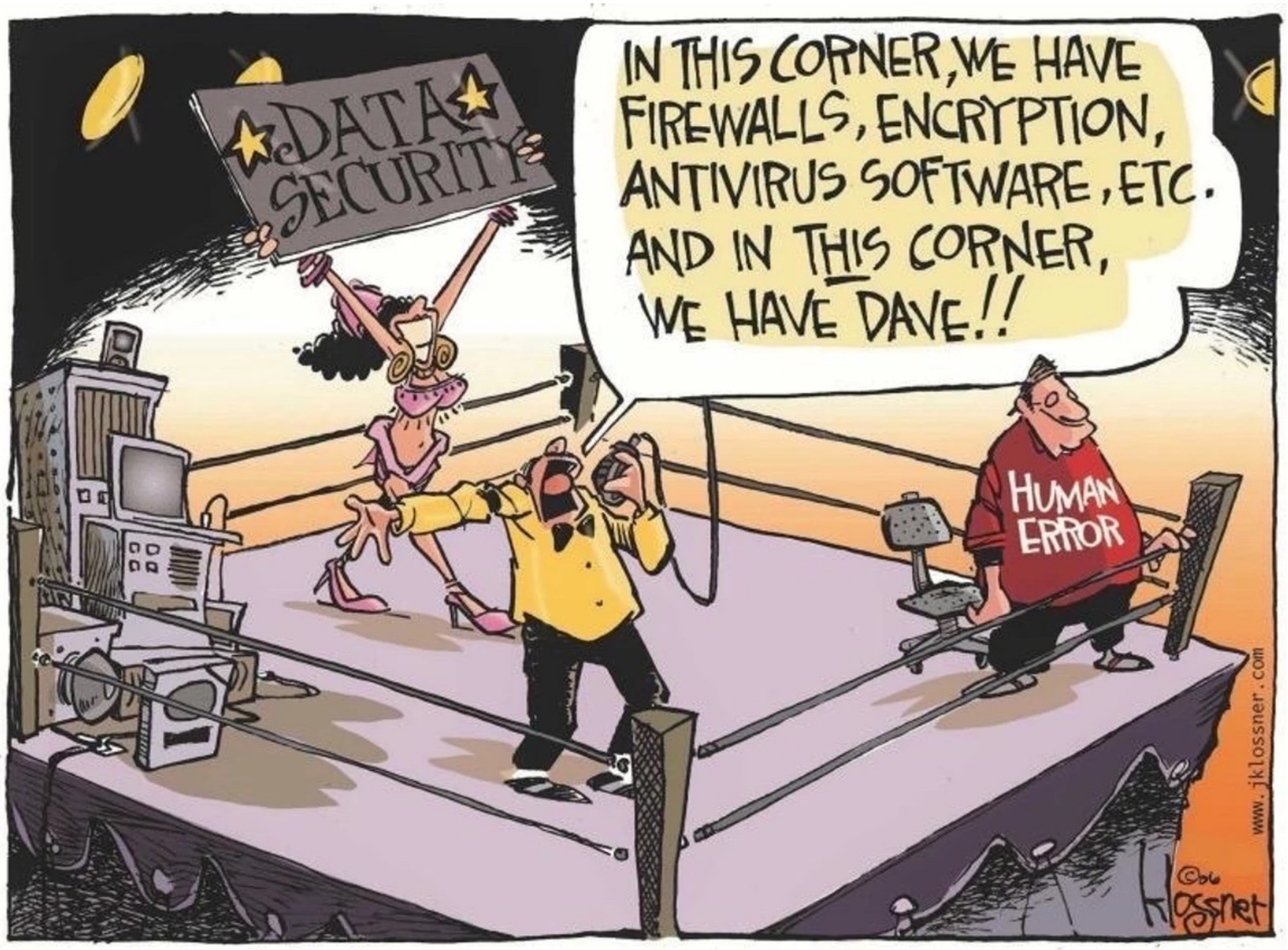
Best Practices

7/7

Cyber Hygiene 🪥✅

1. Starke Passwörter und Passwort-Management
2. Multi-Faktor-Authentifizierung (MFA)
3. Aktualisierungen und Patches installieren
4. Regelmässige Datensicherungen (Backups)

Human Factor



«While cybersecurity is usually treated as a technology problem, more than 80% of data breaches are the result of human error.»

IBM Cyber Security Intelligence Index

- **Awareness training**
- **Access rights and privileges**
- **Encourage cyber hygiene**

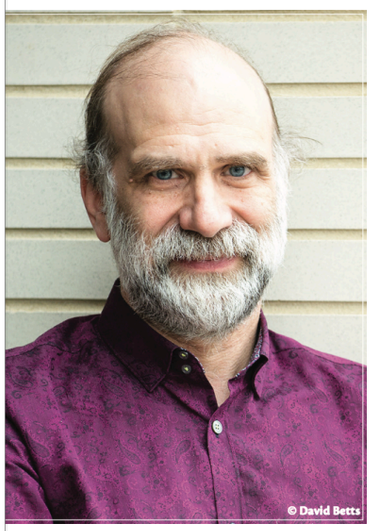
Stop Trying to Fix the User

«The problem isn't the users: it's that we've designed our computer systems' security so badly that we demand the user do all of these counterintuitive things.»

Bruce Schneier, Harvard University

https://csdl-downloads.ieeecomputer.org/mags/sp/2016/05/msp2016050096.pdf

LAST WORD



Bruce Schneier
Harvard University

Stop Trying to Fix the User

Every few years, a researcher replicates a security study by littering USB sticks around an organization's grounds and waiting to see how many people pick them up and plug them in, causing the autorun function to install innocuous malware on their computers. These studies are great for making security professionals feel superior. The researchers get to demonstrate their security expertise and use the results as "teachable moments" for others. "If only everyone was more security aware and had more security training," they say, "the Internet would be a much safer place."

Enough of that. The problem isn't the users: it's that we've designed our computer systems' security so badly that we demand the user do all of these counterintuitive things. Why can't users choose easy-to-remember passwords? Why can't they click on links in emails with wild abandon? Why can't they plug a USB stick into a computer without facing a myriad of viruses? Why are we trying to fix the user instead of solving the underlying security problem?

Traditionally, we've thought about security and usability as a tradeoff: a more secure system is less functional and more annoying, and a more capable, flexible, and powerful system is less secure. This "either/or" thinking results in systems that are neither usable nor secure.

Our industry is littered with examples. First: security warnings. Despite researchers' good intentions, these warnings just inure people to them. I've read dozens of studies about how to get people to pay attention to security warnings. We can tweak their wording, highlight them in red, and jiggle them on the screen, but nothing works because users know the warnings are invariably meaningless. They don't see "the certificate has expired; are you sure you want to go to this webpage?" They see "I'm an annoying message preventing me from read

as a way to bypass the system completely—effectively falling back on the security of their email account.

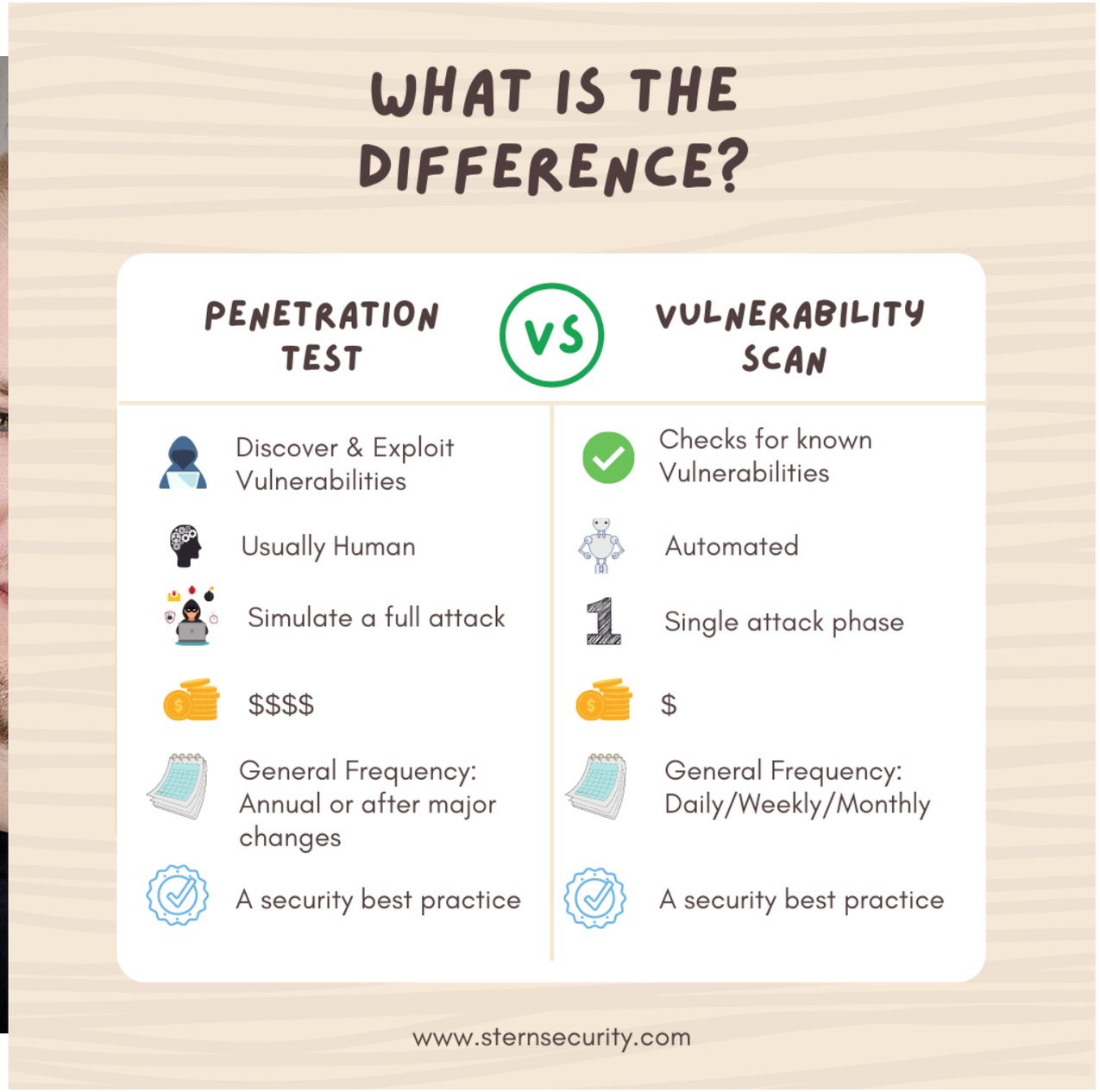
And finally: phishing links. Users are free to click around the Web until they encounter a link to a phishing website. Then everyone wants to know how to train the user not to click on suspicious links. But you can't train users not to click on links when you've spent the past two decades teaching them that links are there to be clicked.

We must stop trying to fix the user to achieve security. We'll never get there, and research toward those goals just obscures the real problems. Usable security doesn't mean "getting people to do what we want." It means creating security that works, given (or despite) what people do. It means security solutions that deliver on users' security goals without—as the 19th-century Dutch cryptographer Auguste Kerckhoffs aptly put it—"stress of mind, or knowledge of a long series of rules."

I've been saying this for years. Security usablity guru (and one of this issue's guest editors) M. Angela Sasse has been saying it even longer. People—and developers—are finally starting to listen. Many security updates happen automatically so users don't have to remember to manually update their systems. Opening a Word or Excel document inside Google Docs isolates it from the user's system so there's little risk of embedded malware. And programs can run in sandboxes that don't compromise the entire computer. We've come a long way, but we have a lot further to go.

Blame-the-victim thinking is older than the Internet, of course. But that doesn't make it right. We owe it to our users to make the Information Age a safe place for everyone—

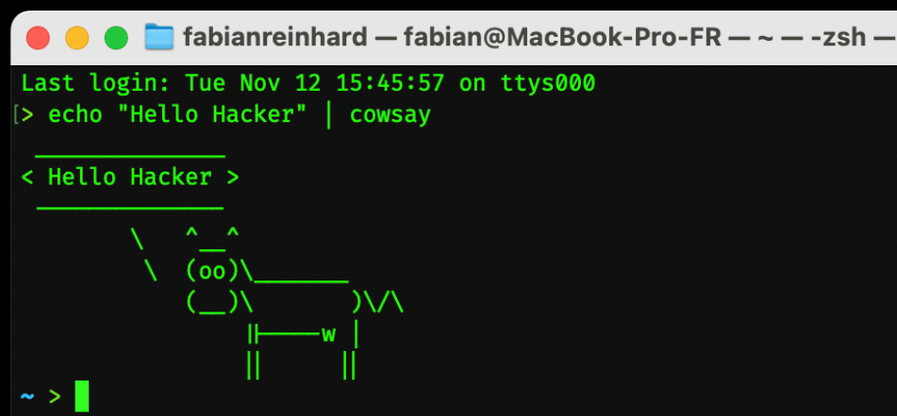
Penetration Tests



Eine Einladung für Hacker?

Hey ~~Hacker~~ Security Researcher, irgendwo da draussen in der weiten Welt:

- Komm und ~~hacke~~ teste die Sicherheit unserer System!
- Wir werden dich nicht verklagen!
  Versprochen, solange du dich an die Regeln hältst.
- Wir verpflichten uns, die Schwachstelle schnellstmöglich zu beheben (Innerhalb einer nützlichen Frist).
- Wir zahlen dir eine ~~Bug Bounty~~ Belohnung. Aber nur vielleicht …



VDP: eine Einladung für Hacker?

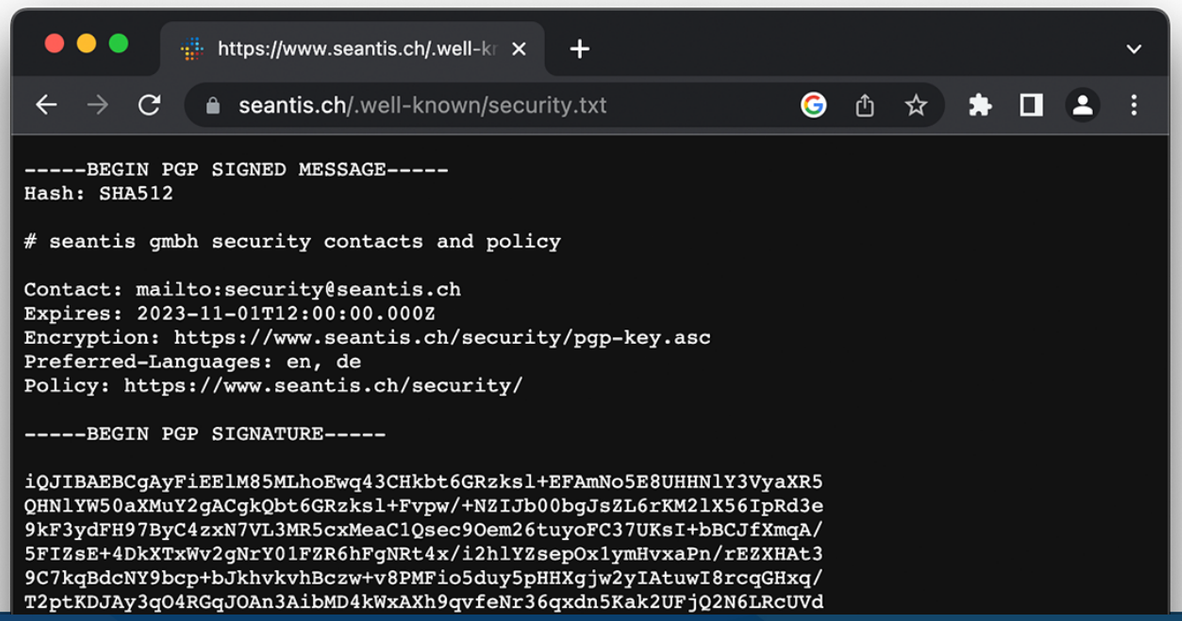
https://www.seantis.ch/blog/vulnerability-disclosure-policy/

Eine Vulnerability Disclosure Policy (kurz: VDP) regelt, wie ethische Hacker Systeme untersuchen dürfen und wie sie allfällige Schwachstellen an das betroffene Unternehmen melden können.

Eine Vulnerability Disclosure Policy viele Vorteile. Sie etabliert klare Regeln für beide Seiten - Hacker und Unternehmen - im Umgang mit Schwachstellen und kann verhindern, dass Schwachstellen ungemeldet ihren Weg in falsche Hände finden.

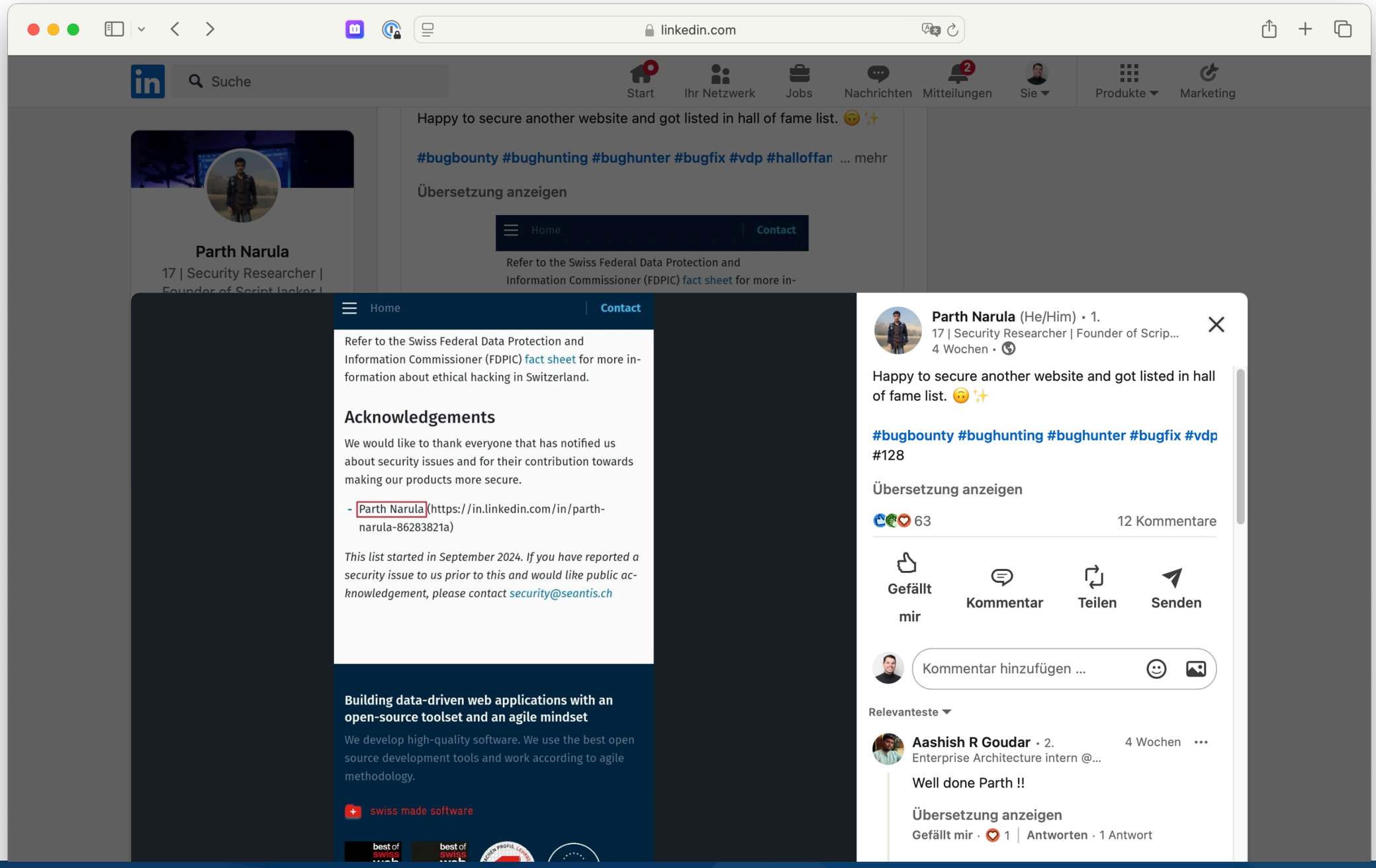
	Uptime OGC staatskalender.bs.ch [Z1] (until 07/23)	-	-	-	-
	Response Time OCQM app.scqm.ch [Z2]	362	465	428	3
	Response Time staatskalender.bs.ch [Z2]	166	163	151	1
	SSL Check app.scqm.ch [Z3]	A+	A+	A+	A
	Sentry [Z10]	1	1	1	1
	Information (Newsletter, Blog, News Website, Vorträge) [Z11]	0	0	0	
	Anzahl Safety DB [Z4] 1	1	1	1	1
	Anzahl VDP Meldungen	9	1	1	

Seite



Hacker on LinkedIn

https://www.linkedin.com/in/parth-narula-86283821a/recent-activity/all/




HEY, TOM, I JUST REALIZED THAT I DON'T NEED TO OUTRUN THE BEAR; I ONLY NEED TO OUTRUN YOU.

admin
.digital

Herzlichen Dank

Diskussion 🙋

Fabian Reinhard | M A UZH | Managing Partner
fabian.reinhard@seantis.ch | +41 41 511 22 50

www.admin.digital