Herausforderungen und Chancen für Schwachstellenmeldungen in Deutschland

envia TEL Community-Treffen Cybersecurity - 23.04.2026 - Markkleeberg

Sebastian Neef

Security in Telecommunications
TU Berlin, Germany

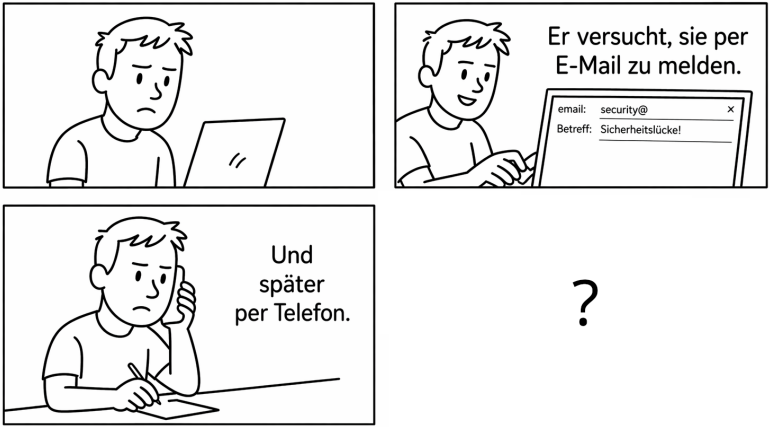
Kurz über mich

- 2010, während des Abiturs: Interesse an IT-Sicherheit
- 2012, während des Informatikstudiums: Freiberuflicher IT-Sicherheitsberater, Pentester & Whitehat
- Seit 2021 Doktorand mit Schwerpunkt Web-, Netzwerk-, Softwaresicherheit an der TU Berlin (FG SecT)

- Weiteres: AG Rechnersicherheit e.V., Capture-the-Flag Wettbewerbe, Bugbounty-Programme (Detectify #2, ehem. Bugcrowd Top 10)

Motivation

Sebastian findet eine Sicherheitslücke auf der Website eines groβen Automobilherstellers.



Motivation


Sebastian findet eine Sicherheitslücke auf der Website eines großen Automobilherstellers.
Er versucht, sie per E-Mail zu melden.
email: security@
Betreff: Sicherheitslücke!
Und später per Telefon.
Wir wissen nicht, wer für die Website verantwortlich ist.
Wir können nichts tun.

Eine kurze Vorgeschichte aus dem Jahr ~2010...

„Ist Hacken wirklich so einfach, oder sind Webseiten einfach sehr unsicher?“

Im Jahr 2026 ist klar: Kein System ist 100% sicher.

Faktor ”Mensch”

- SPAM, Phishing, Social Engineering, Fehlkonfigurationen, Softwareupdates, usw.

⇒ CEO Fraud: Zulieferer um 40M€ betrogen.[1]

Faktor ”Software”

- Klassische Schwachstellen, bspw. Buffer Overflows, SQL Injection, Remote Command Execution, usw.

⇒ Heartbleed leakt SSL/TLS Daten und Zertifikate[2]

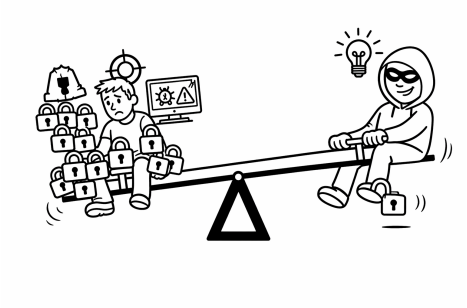
Faktor ”Hardware”

- Spekulative Ausführung, Side-Channels, Fault Injections, usw.

⇒ Voltage-Fault-Injection erlaubt Tesla-Premiumfeatures freizuschalten[3]

[1] https://www.golem.de/news/ceo-fraud-autozulieferer-leoni-um-40-millionen-euro-betrogen-1608-122741.html
[2] https://www.heartbleed.com/
[3] https://www.heise.de/news/Tesla-Jailbreak-AMD-Prozessor-verhilft-zu-kostenlosen-Premium-Features-9235296.html

Die Asymmetrie zwischen Verteidiger und Angreifer



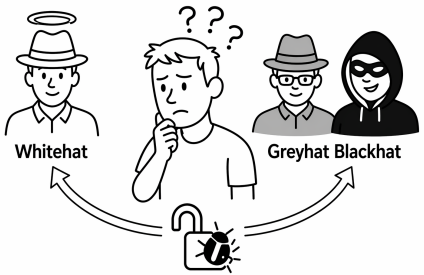
- Verteidiger muss **alle** Sicherheitsgefahren **immer** abwehren
- Verteidiger hat begrenzte Ressourcen
  (Personal, Arbeitszeit, Geld, usw.)

- Angreifer müssen **nur eine** Schwachstelle
  irgendwann finden und ausnutzen
- Angreifer haben potentiell **beliebig viele** Ressourcen

Aber: Es gibt auch ”gute” Hacker

- ”Wie mit einer gefundenen Schwachstelle umgehen?”
  - **Whitehat**: Verantwortlich melden
  - **Greyhat**: Direkt veröffentlichen
  - **Blackhat**: Ausnutzen oder verkaufen

- Laut einer Befragung von Algarni et al.[1] sind die Gründe von Sicherheitsforschenden, Schwachstellen zu melden:
  - Entwicklern zu helfen, einen Patch zu veröffentlichen
  - Reputation oder Eigenwerbung
  - Belohnungen (bspw. Geld) zu erhalten (bei entsprechenden Meldeprogrammen)
  - ...



[1] ”Most Successful Vulnerability Discoverers: Motivation and Methods” by Algarni et al. in SAM, 2013

Der Elefant im Raum: Die Politik und der ”Hackerparagraph”

- **”Problem”:** Hackerparagraph[1] (§ 202a/b/c StGB)
  - Vorbereitung des Ausspähens und Abfangens von Daten ist illegal
  - Datenveränderung oder Computersabotage[2] (§ 303b/c)
  - ”Never decompile” $\rightarrow$ Urheberrechtsverletzungen

  $\Rightarrow$ Rechtlich unklar, welche Intention vorlag.

[1] https://www.gesetze-im-internet.de/stgb/__202c.html
[2] https://www.gesetze-im-internet.de/stgb/__303b.html

Der Elefant im Raum: Der ”Hackerparagraph” und die Politik

- **Medienwirksame Fälle**:
  - ”Modern Solution”[1]:
    - Zugangsdaten zur Datenbank in Kundenanwendung im Klartext
    - Responsible Disclosure führt zu Anklage und Verurteilung, weil die (Zugangs-)Daten geschützt und nicht ”nicht für Jedermann” zugreifbar waren.
    - Verfassungsbeschwerde für mehr Klarheit beim Hackerparagraphen abgelehnt

[1] https://www.heise.de/news/Bundesverfassungsgericht-lehnt-Beschwerde-im-Fall-Modern-Solution-ab-10663649.html
[2] https://www.heise.de/news/Verfahren-gegen-Lilith-Wittmann-eingestellt-weil-CDU-connect-ungeschuetzt-war-6194222.html

Der Elefant im Raum: Der ”Hackerparagraph” und die Politik

- **Medienwirksame Fälle**:
  - ”CDU-Wahlkampf-App”[2]:
    - Ungeschützte Server-API exponierte Datensätze der Wahlunterstützer
    - Responsible Disclosure führt zur Anzeige; Ermittlungen werden eingestellt, weil die Daten ungeschützt waren.

[1] https://www.heise.de/news/Bundesverfassungsgericht-lehnt-Beschwerde-im-Fall-Modern-Solution-ab-10663649.html
[2] https://www.heise.de/news/Verfahren-gegen-Lilith-Wittmann-eingestellt-weil-CDU-connect-ungeschuetzt-war-6194222.html

Der Elefant im Raum: Der ”Hackerparagraph” und die Politik

- **Medienwirksame Fälle**:
  - ”CDU-Wahlkampf-App”[2]:
    - Ungeschützte Server-API exponierte Datensätze der Wahlunterstützer
    - Responsible Disclosure führt zur Anzeige; Ermittlungen werden eingestellt, weil die Daten ungeschützt waren.

- $\Rightarrow$ In beiden Fällen rechtliche Schritte gegen verantwortliche Melder :-/

[1] https://www.heise.de/news/Bundesverfassungsgericht-lehnt-Beschwerde-im-Fall-Modern-Solution-ab-10663649.html
[2] https://www.heise.de/news/Verfahren-gegen-Lilith-Wittmann-eingestellt-weil-CDU-connect-ungeschuetzt-war-6194222.html

Politische Entwicklungen in die richtige Richtung

- **DSGVO**
  - Artikel 33/34 schreiben vor, dass bei Verletzung des Schutzes der pers. Daten durch die Verantwortlichen eine Meldung bei der Aufsichtsbehörde abzugeben ist.
  - $\rightarrow$ Meldung von Sicherheitslücken sollte im Interesse der Verantwortlichen sein

[1] https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/national-implementation/cvd-policy

Politische Entwicklungen in die richtige Richtung

- **DSGVO**
- **NIS2**
  - Artikel 12 setzt voraus, dass Schwachstellen in EU-Mitgliedsstaaten gemeldet werden können
  - Belgien setzt bspw. Coordinated Vulnerability Disclosure Programme für NIS2-Betroffene voraus[1]

[1] https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/national-implementation/cvd-policy

Politische Entwicklungen in die richtige Richtung

- **DSGVO**
- **NIS2**
- **CRA**
  - Artikel 13 besagt, dass Hersteller Anlaufstellen für Schwachstellenmeldungen benennen sollen

[1] https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/national-implementation/cvd-policy

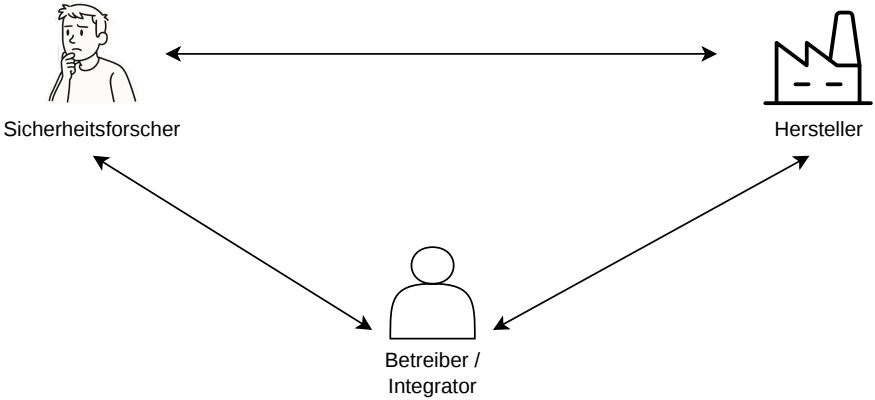
Politische Entwicklungen in die richtige Richtung

- **DSGVO**
- **NIS2**
- **CRA**
  - Artikel 13 besagt, dass Hersteller Anlaufstellen für Schwachstellenmeldungen benennen sollen

- $\Rightarrow$ Wie sieht es in der Praxis aus?

[1] https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/national-implementation/cvd-policy

Sicherheitsforscher vs. Hersteller vs. Betreiber



- Nicht immer ist der Hersteller auch der Betreiber
- Frage: Wie oder an wen die Schwachstelle melden?

security@-Postfach (RFC 2142)

- Eins von vielen Standard-Postfächern seit 1997
- **Leider kaum Verbreitung**
  - 46% Bounce-Rate in unserer Studie
  - 85% in anderen Studien (Stock et al., 2018)[1]
  - $\leq$15% der Top 1M haben diese Postfächer eingerichtet (Soussi et al., 2020)[2]

4. NETWORK OPERATIONS MAILBOX NAMES

Operations addresses are intended to provide recourse for customers, providers and others who are experiencing difficulties with the organization's Internet service.

MAILBOX	AREA	USAGE
ABUSE	Customer Relations	Inappropriate public behaviour
NOC	Network Operations	Network infrastructure
SECURITY	Network Security	Security bulletins or queries

3

[1] https://swag.cispa.saarland/papers/stock2018notification.pdf
[2] https://ieeexplore.ieee.org/document/9229722
[3] https://datatracker.ietf.org/doc/html/rfc2142

Security.txt (RFC 9116) - Der einfache Weg zu sicherheitsrelevanten Kontaktinformationen

2.6. Example of an Unsigned "security.txt" File

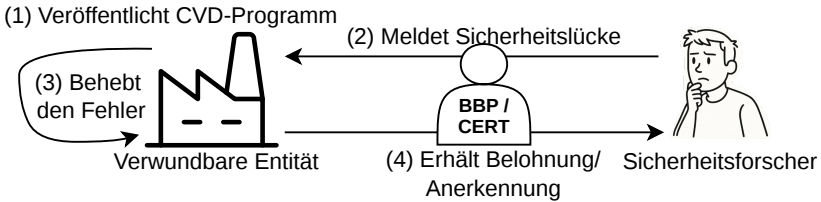
```
# Our security address
Contact: mailto:security@example.com

# Our OpenPGP key
Encryption: https://example.com/pgp-key.txt

# Our security policy
Policy: https://example.com/security-policy.html

# Our security acknowledgments page
Acknowledgments: https://example.com/hall-of-fame.html

Expires: 2021-12-31T18:37:07z
```

[1]

- Relativ neuer Standard (2022)
- Kanonischer Ort für sicherheitsrelevante Kontaktinformationen
- Textdatei unter `/security.txt` oder `/.well-known/security.txt`
- Bisher noch geringe Verbreitung laut Poteat et al.[2] oder Findlay et al.[3] (15.6%)

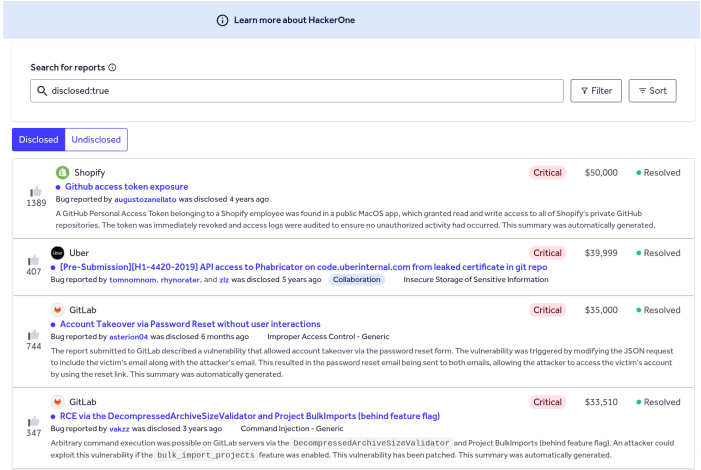
[1] https://datatracker.ietf.org/doc/html/rfc9116
[2] https://dl.acm.org/doi/10.1145/3487552.3487841
[3] https://www.ndss-symposium.org/wp-content/uploads/madweb2022_23014_paper.pdf

Coordinated Vulnerability Disclosure (CVD)-Programme: Ein Lösungsansatz mit Vorteilen



- Coordinated Vulnerability Disclosure (CVD)-Programme:
  - **Scope**: Was darf (nicht) getestet werden? Was ist (nicht) erlaubt?
  - **Kommunikation**: Wo und wie sollen die Funde gemeldet werden?
  - **Belohnung**: Wie wird sich für valide Funde bedankt?
- CVD-Plattformen können als Vermittler fungieren
- Sicherheitsforscher erhalten rechtlichen Rahmen

CVD-Plattformen als Vermittler und Filter



[1]

- CVD-Plattformen agieren als Vermittler
- Hackerone, Bugcrowd, Intigriti, YesWeHack, uvm.
- Entlastung durch Vorfilterung der Meldungen. Mediator bei Unstimmigkeiten.

[1] https://hackerone.com/hacktivity/overview

CVD-Programme: Beispiel Google

Security.txt

www.google.com/.well-known/security.txt

```
Contact: https://g.co/vulnz
Contact: mailto:security@google.com
Encryption: https://services.google.com/corporate/publickey.txt
Acknowledgments: https://bughunters.google.com/
Policy: https://g.co/vrp
Hiring: https://g.co/SecurityPrivacyEngJobs
Expires: 2030-04-01T00:00:00z
```

[1]

CVD-Programm

Category	Examples	Google applications on Tier 0 domains [0], or global impact [1] (T0)	Google applications on Tier 1 domains [2] (T1)	Normal Google Applications (T2) Examples include: *.google.com, *.youtube.com, *.blogger.com, *.admob.com	Applications on acquisition Tier 0, Tier 1 domains [3] [4] (T3a)	Other acquisitions, other sandboxed or lower priority applications [4] (T3b) Examples include: *.withgoogle.com, *.withyoutube.com
Vulnerabilities giving direct access to Google servers						
Remote code execution (S0)	Command injection, deserialization bugs, sandbox escapes	$101,010	$101,010	$75,000	$10,000	$1,337 - $5,000
Unrestricted file system or database access (S1)	Unsandboxed XXE, SQL injection	$75,000	$75,000	$50,000	$10,000	$1,337 - $5,000
Logic flaw bugs leaking or bypassing significant security controls impacting **Information Tier 0** or **Critical Actions** (S2a)	Direct object reference, remote user impersonation	$50,000	$50,000	$31,337	$5,000	$500

[2]

[1] https://www.google.com/.well-known/security.txt
[2] https://g.co/vrp

CVD-Programme: Beispiel Telekom

Security.txt

```
# Contact for misuse of Deutsche Telekom AG services (Abuse)
Contact: abuse@telekom.de
Website: https://www.telekom.com/en/company/data-privacy-and-security/governance-security/abuse

# Contact for Deutsche Telekom AG related Security Issues (Incident Response)
Contact: cert@telekom.de
Website: https://www.telekom.com/en/company/data-privacy-and-security/news/rfc-2350-deutsche-telekom-cert-358280

# Contact for coordinated vulnerability disclosure (Bug Bounty)
Contact: bugbounty@telekom.de
Policy: https://www.telekom.com/bugbounty

# Deutsche Telekom AG security acknowledgments page (Hall of fame)
Acknowledgments: https://www.telekom.com/en/company/data-privacy-and-security/news/acknowledgements-358300
Expires: 2026-12-31T22:59:00.000Z
Preferred-Languages: de, en
Canonical: https://www.telekom.com/.well-known/security.txt
Hiring: https://careers.telekom.com
```

[1]

CVD-Programm

Scope

Folgende Systeme gehören zum Bug Bounty Programm der Deutschen Telekom (T Mobile US betreibt ein separates Bug Bounty Programm auf Bugcrowd)

Domains

Privates Bug-Bounty-Programm

Critical / P1	High / P2	Medium / P3
5.000 Euro	2.000 Euro	1.000 Euro

- *.telekom.de
- *.telekom.net
- *.telekom.com
- *.t-systems.com
- *.open-telekom-cloud.com
- auth.otc.t-systems.com
- *.otc-service.com

Out of Scope:

- *.reverse.open-telekom-cloud.com
- *.lila.dih.telekom.com

Out of Scope: Alle Kundensysteme, die nicht der Deutschen Telekom AG gehören

Du hast eine Schwachstelle gefunden? Dann sende uns!

Für Deine Meldung sind insbesondere die folgenden Informationen aus Deiner Analyse für uns wichtig:

[2]

[1] https://www.telekom.com/security.txt

[2] https://www.telekom.com/bugbountycas

Wie steht es um CVD-Programme in Deutschland am Beispiel der 40 DAX Unternehmen?

Do (Not) Tell Me About My Insecurities: Assessing the Status Quo of Coordinated Vulnerability Disclosure in Germany Amid New EU Cybersecurity Regulations

Sebastian Neef
Technische Universität Berlin
Berlin, Germany
0000-0003-3055-0823

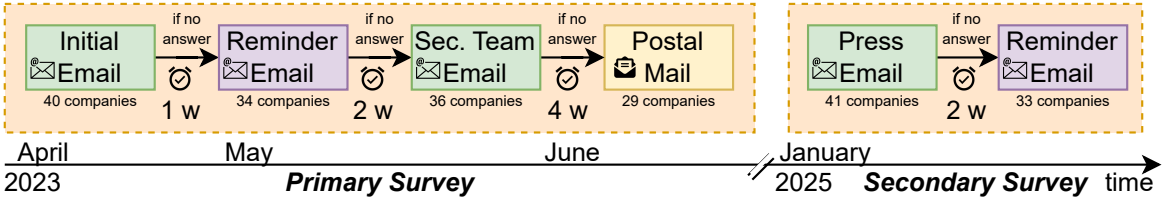
Cenk Schlunke
Technische Universität Berlin
Berlin, Germany
0009-0002-3142-5776

Anne Hennig
Karlsruhe Institute of Technology
Karlsruhe, Germany
0000-0002-6964-589X

1

[1] https://ieeexplore.ieee.org/document/11300384, 2025 European Symposium on Usable Security (EuroUSEC)

CVD-Papier: Methodik



2023

- Öffentliche CVD-Informationen gesammelt
- Kontakt per E-Mail (Impressum) oder per Kontaktformular
- E-Mails an sicherheitsbezogene Kontakte (security.txt, Webseite, `security@`)
- Postversand mit frankiertem Rücksendeumschlag an die ”Hauptquartiere” in Deutschland

2025

- Öffentliche CVD-Informationen gesammelt
- E-Mails an Pressekontakte oder -kontaktformulare

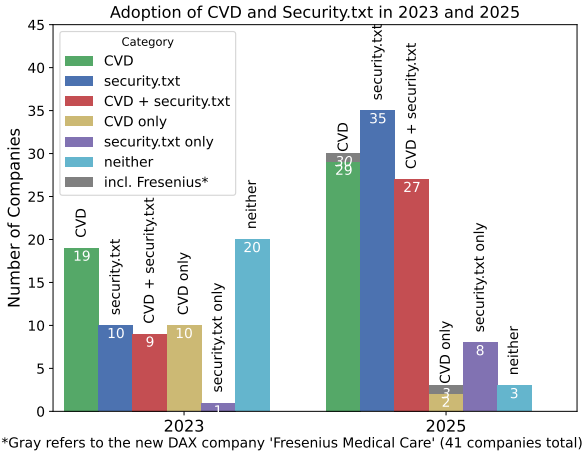
CVD-Papier: Auswertung der CVD-Programme

2023

- Nur 50% (20) hatten Meldemöglichkeiten
  - 19x CVD-Programm und 10x security.txt
  - 9x beides
  - 10x nur CVD, 1x nur security.txt

2025

- Substanzielle Steigerung auf 92.5% (37)
  - 29x CVD (+10) und 35x security.txt (+15)
  - 27x beides
  - 2x nur CVD, 8x nur security.txt
- Trotzdem: 3x weder CVD noch security.txt



CVD-Papier: Auswertung der Umfrage

- **Rückmeldungen**
  - Insgesamt: 31, 8 Antworten (20%)
  - Am meisten Antworten von den Sicherheitsteams und durch die Presse-Erinnerung
  - 46% Bounce-rate für security@-Postfächer

CVD-Papier: Auswertung der Umfrage

- **CVD-Programme**
  - Meldungs-Validität: 3x 80-100%, 1x 60-80%, 1x 20-40%
  - Meldungs-Qualität: 1x sehr gut, 2x gut, 1x *gemischt*
  - Budget: 1x 10k - 100k, 1x $\geq$ 1m EUR

CVD-Papier: Auswertung der Umfrage

- **Vorteile**
  - Erhöhung der IT-Sicherheit (6x), Vertrauen und Reputation (3x), Einhaltung der Gesetze (2x), Vermeidung von Angriffen (1x)
  - Strukturierte Kanäle (1x), bessere Fehlerkultur (1x), und Gewinn von Kompetenz (1x)

CVD-Papier: Auswertung der Umfrage

- **Herausforderungen**
  - Fehlende menschliche/finanzielle Ressourcen (2x), fehlendes Sicherheitsbewusstsein (1x), Aufmerksamkeit der Hacker (1x)
  - Fehlende Verantwortlichkeiten (1x), qualifiziertes Personal (1x), Identifizierung relevanter Akteure (1x), Arbeitslast (1x)
  - Zwei sehen keine größeren Hürden: Ähnlich zu anderen Business-Prozessen
  - Eins hat noch kein CVD-Programm wegen interner Hürden.

CVD-Papier: Auswertung der Umfrage

- **Herausforderungen**
  - Fehlende menschliche/finanzielle Ressourcen (2x), fehlendes Sicherheitsbewusstsein (1x), Aufmerksamkeit der Hacker (1x)
  - Fehlende Verantwortlichkeiten (1x), qualifiziertes Personal (1x), Identifizierung relevanter Akteure (1x), Arbeitslast (1x)
  - Zwei sehen keine größeren Hürden: Ähnlich zu anderen Business-Prozessen
  - Eins hat noch kein CVD-Programm wegen interner Hürden.

- $\Rightarrow$ Kann das nicht KI machen?

Chancen und Herausforderungen durch KI

- **Vorteil: Aufdecken von Schwachstellen**
  - Automatisierte Schwachstellenanalyse[1]
    - Bspw. Code-Reviews
  - Agentisches Pentesting[2]
    - Iterativ und interaktiv

[1] https://www.anthropic.com/glasswing
[2] https://arxiv.org/abs/2510.03610
[3] https://daniel.haxx.se/blog/2025/07/14/death-by-a-thousand-slops/

Chancen und Herausforderungen durch KI

- **Nachteil: "AI-Slop"** am Beispiel vom curl-Projekt[3]
  - Erhöhte Meldungsmenge: +20% AI-slop in 2025
  - Ungültige Meldungen: Plausibel, aber nicht valide
  - Validitätsrate ist gesunken: Nur 5% tatsächlich korrekt

- $\Rightarrow$ KI ist ein Werkzeug, das richtig eingesetzt werden muss.
- $\Rightarrow$ Validierung der Funde vor dem Einreichen bleibt notwendig.

[1] https://www.anthropic.com/glasswing
[2] https://arxiv.org/abs/2510.03610
[3] https://daniel.haxx.se/blog/2025/07/14/death-by-a-thousand-slops/

Wie können wir das Melden von Schwachstellen verbessern?

- **Hersteller und Betreiber**
  - Mehr und bessere Meldewege
    - Eingerichtetes **security@**-Postfach
    - Kontaktinformationen in einer **security.txt**
    - Rechtlicher Rahmen mittels eines **CVD-Programms**
  - ”Mindset”-Änderung
    - Offen und konstruktiv mit Meldungen umgehen
    - Transparent über Vorfälle und (Software-)Updates informieren

- **Sicherheitsforscher**
  - Verantwortliches Melden von Schwachstellen
  - Einhalten der CVD-Regeln
  - Nutzung von KI als Werkzeug

- **Politiker**
  - Mehr Rechtssicherheit für Whitehat-Sicherheitsforschung

Fazit

- Die DAX-Unternehmen legen vor, ziehen die KMUs nach?
- Mehr Kommunikation und Austausch zwischen allen Beteiligten
- Mit Sicherheit zu besserer IT-Sicherheit durch mehr Meldewege :)

Folien

Kontakt

Sebastian Neef
neef@tu-berlin.de
https://sebastian-neef.de

Fazit

- Die DAX-Unternehmen legen vor, ziehen die KMUs nach?
- Mehr Kommunikation und Austausch zwischen allen Beteiligten
- Mit Sicherheit zu besserer IT-Sicherheit durch mehr Meldewege :)

Diskussion

- Welche CVD-Maßnahmen haben Sie bereits umgesetzt? (security@, security.txt, CVD-Programm, ...)
- Welche Hürden gibt bzw. gab es?
- Welche Erfahrungen haben Sie bisher gemacht?

Folien

Kontakt

Sebastian Neef
neef@tu-berlin.de
https://sebastian-neef.de