Neulich
auf Twitter

Folien: https://dhgo.to/selbstbestimmt23

SELBSTBESTIMMT UNSICHER?

Herausforderungen an Datensicherheit und Datenschutz im digitalen Alltag

Prof. Dr. **Dominik Herrmann**
Universität Bamberg, @herdom

Smartwatch.de – die ganze Sma

https://www.smartwatch.de

120%

Huawei Watch GT3 Pro

46mm | Silber | Titanband

ab 439,49 €

Lieferzeit 1 bis 5 Tage

Michael Kors Access Gen 6 Bradshaw

Gold mit Schmucksteinchen

ab 369,50 €

Lieferzeit 1 bis 5 Tage

Samsung Galaxy Watch 5

LTE | 45mm | Silver

ab 289,50 €

Lieferzeit 1 bis 5 Tage

Fossil Gen 6 Smartwatch

44mm | Lederarmband | Schwarz/Braun

ab 215,50 €

Lieferzeit 1 bis 5 Tage

https://www.smartwatch.de/smartwatch/michael-kors-access-gen-6-bradshaw/#variation-7108

Sicherheit und Datenschutz sind mir wichtig. Welche Uhr soll ich kaufen?

Ich bin schlecht informiert.

https://www.youtube.com/watch?v=Ql5_6Nc4Pv8

Smartwatch.de – die ganze Sma

https://www.smartwatch.de

120%

Huawei Watch GT3 Pro

46mm | Silber | Titanband

ab 439,49 €

Lieferzeit 1 bis 5 Tage

Michael Kors Access Gen 6 Bradshaw

Gold mit Schmucksteinchen

ab 369,50 €

Lieferzeit 1 bis 5 Tage

Samsung Galaxy Watch 5

LTE | 45mm | Silver

ab 289,50 €

Lieferzeit 1 bis 5 Tage

Fossil Gen 6 Smartwatch

44mm | Lederarmband | Schwarz/Braun

ab 215,50 €

Lieferzeit 1 bis 5 Tage

https://www.smartwatch.de/smartwatch/michael-kors-access-gen-6-bradshaw/#variation-7108

GEFÖRDERT VOM

GESELLSCHAFT FÜR INFORMATIK

InviDas

Bundesministerium für Bildung und Forschung

CONSUMER EMPOWERMENT

Wir müssen die VuV besser informieren!

Ist das so?

Machen die das absichtlich?

Wohl kaum.

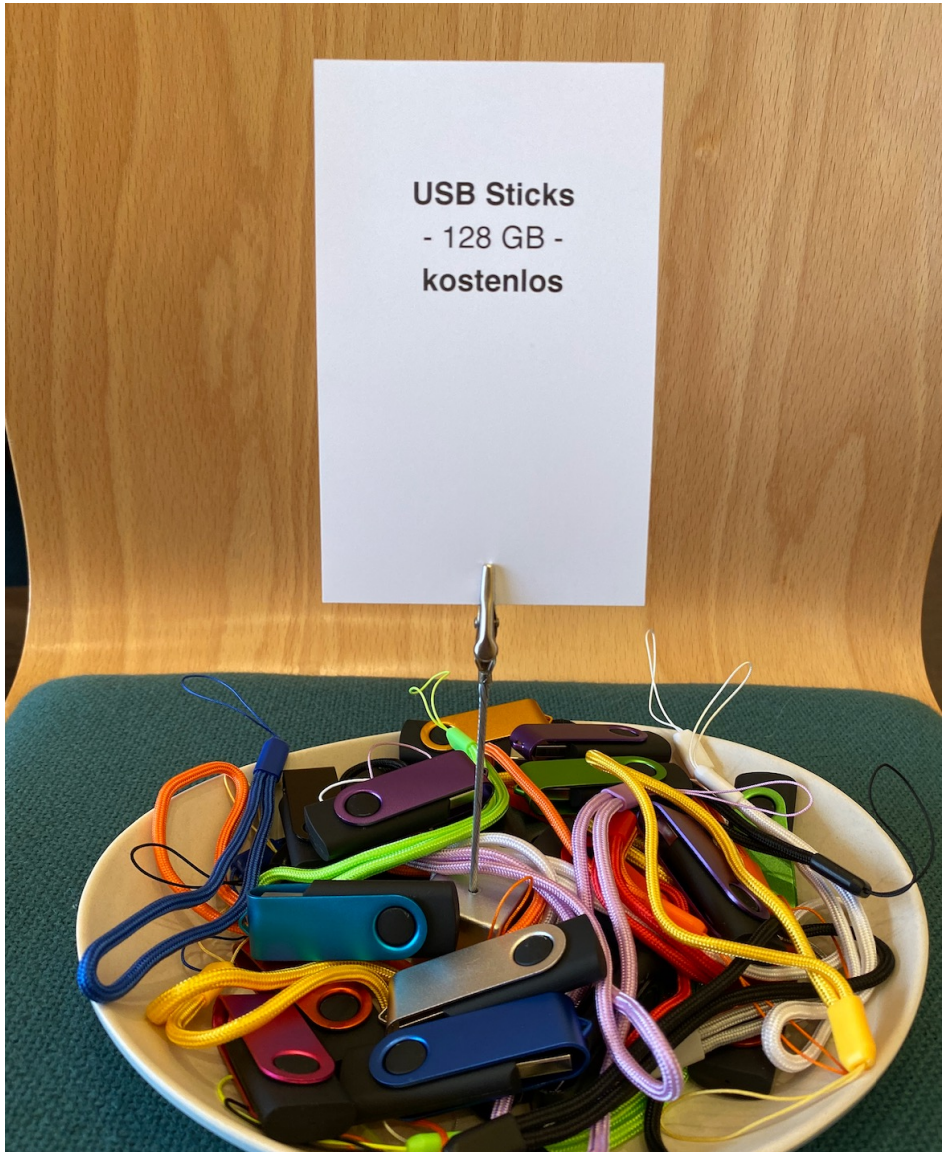
SELBSTBESTIMMT UNSICHER?

Herausforderungen an Datensicherheit und Datenschutz im digitalen Alltag

Prof. Dr. **Dominik Herrmann**
Universität Bamberg, @herdom

Verhaltensökonomische Umstände als Ursache

- Menschen entscheiden bei Security und Privacy **nicht rational** (u.a. A. Acquisti)
  - hyperbolic discounting
  - immediate gratification
  - availability heuristic
  - probability neglect
- Häufig **externalisierte Kosten**, Beispiel: Mirai-Botnet



Schnell zugreifen bevor sie weg sind!

Fehlendes Wissen
als Ursache?

Natürlich!

Weil wir es ihnen schlecht erklärt haben.

Was ist ein gutes Passwort?

„Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen“
„Passwort regelmäßig ändern“

hallo123

passwort

Hallo123!

Passwort.4

master

2010-Auggust

12345

123456

lbi=zEd4

schlechter als

mehlbalkontisch

Warum?


Warum?

Wie viele Rate-Versuche?

(alle Möglichkeiten durchprobieren)

```
 ! " # $ % & ' ( ) * + , - . /
0 1 2 3 4 5 6 7 8 9 : ; < = > ?
@ A B C D E F G H I J K L M N O
P Q R S T U V W X Y Z [ \ ] ^ _
` a b c d e f g h i j k l m n o
p q r s t u v w x y z
```

90 Zeichen

lbi=zEd4 (8 Stellen)

4.304.672.100.000.000

Versuche (höchstens)

lbi=zEd4 (8 Stellen)

4.304.672.100.000.000

Versuche (höchstens)

mehlbalkontisch (15 Stellen)

1.677.259.342.285.725.925.376

Versuche (nur Kleinbuchstaben)


Angreifer
sind schlau.

aaaaaaaaaaaaaaaa … aaaaaaaaaaaaaaaab …

mehlbalkontisch … zzzzzzzzzzzzzzz

1.677.259.342.285.725.925.376 Versuche

aachenaachenaachen … aachenaachenaal …

mehlbalkontisch … zuziehenzuziehenzuziehen

125.000.000.000.000.000 Versuche

lbi=zEd4 4.304.672.100.000.000 Versuche

Fehlendes Wissen
als Ursache?

Natürlich!

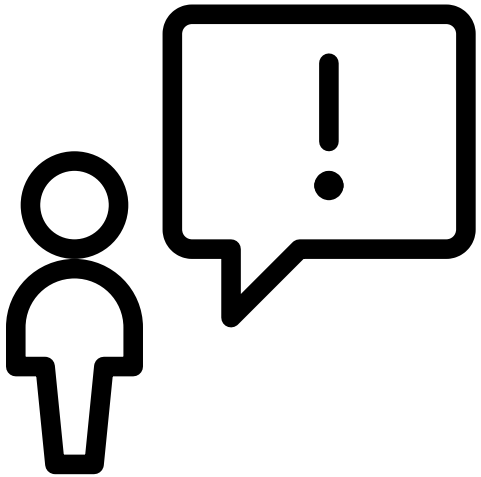
Weil wir es ihnen schlecht erklärt haben.

231 Sicherheitsexperten wurden befragt:

Was sind die 3 wichtigsten Ratschläge, die Sie einem technisch nicht versierten Benutzer geben würden?

Ergebnis

152 verschiedene Ratschläge…



https://ai.google/research/pubs/pub46306/

https://www.usenix.org/system/files/conference/soups2015/soups15-paper-ion.pdf

Moral Hazards: Wissen kann auch Schaden anrichten!

Anwender mit Antiviren-Software, Thunderbird und Passwort-Manager häufiger infiziert als andere!

DeKoven et al. Measuring Security Practices and How They Impact Security, IMC 2019.

Handeln Verbraucherinnen und Verbraucher am Ende vielleicht doch rational?

So Long, And No Thanks for the Externalities: The Rational Rejection of Security Advice by Users
Cormac Herley (Microsoft), NSPW, April 2009.

„Es wird oft behauptet, dass die Benutzer hoffnungslos faul und unmotiviert sind, wenn es um Sicherheitsfragen geht.

Wir argumentieren, dass **die Ablehnung der Sicherheitshinweise**, die die Nutzer erhalten, **aus wirtschaftlicher Sicht** völlig rational ist.

Die Hinweise schützen vor den **direkten Kosten der Angriffe**, belasten sie aber mit indirekten Kosten, den **externen Effekten**.

… zeigt sich, dass der Aufwand für die Befolgung der Sicherheitsempfehlungen tatsächlich **größer ist als die direkten Verluste**, die durch den Angriff verursacht werden.“

Schätzungen: US-Bürgern entsteht nur 20–30 USD Schaden durch Cybercrime (Breen et al.: A Large-Scale Measurement of Cybercrime Against Individuals, CHI 22)

CONSUMER EMPOWERMENT

Wir müssen die VuV besser informieren!

Ist das so?

Produkte werden zu Diensten und Plattformen

Aus Sicherheitssicht häufig vorteilhaft, aber
bisher oft auf Kosten der Privatsphäre.

Grundlagenwissen reicht nicht mehr, wir müssen Handlungskompetenz vermitteln.

***politisch**

Also eigentlich Produktempfehlungen aussprechen.*

foundation.mozilla.org/en/privacynotincluded/

Facebook
WhatsApp

Google
Fitbit Charge 5

Happify, Inc.
Happify

Huawei
Huawei Band 6

Amazon
Amazon Echo Buds

Google
Fitbit Sense 2

Onyx International Inc.
Onyx Boox

Flo Health Inc.
Flo Ovulation & Period Tracker

Extrem unheimlich!

Open "https://foundation.mozilla.org/en/privacynotincluded/google-nest-cams/" in a new tab

MOBILSICHER

Das Infoportal für sichere Handynutzung

Check deine A

Welche Apps sind sauber und welche heir
Das kannst du jetzt selbst checken. Unser
Testergebnisse für rund 30.000 Android-A

ZUR DATENBANK

tagesschau – Aktuelle Nachrichten

ARD Online

de.tagesschau

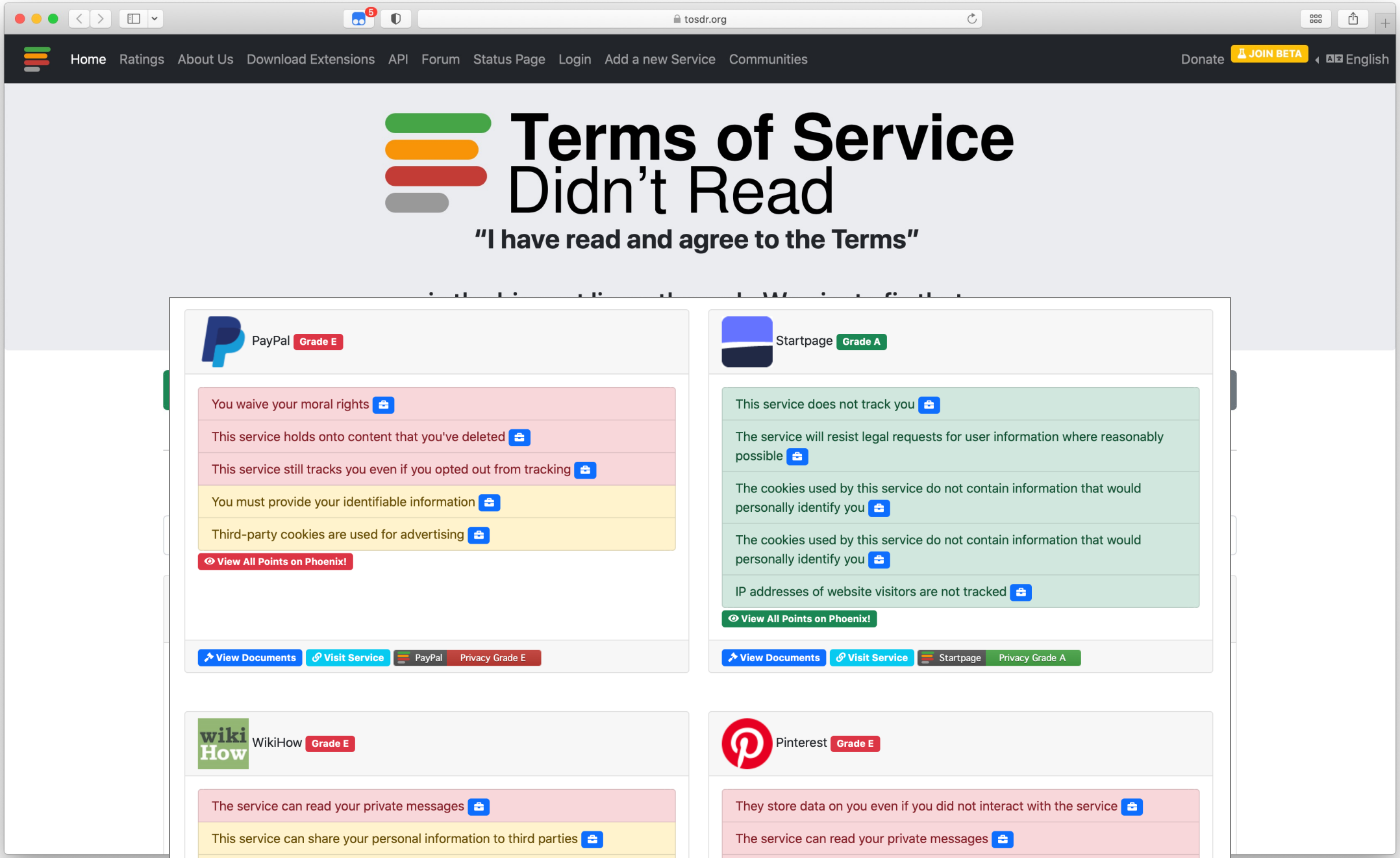
Downloads:	Kategorie:	Werbung:	In-App-Käufe:	Tracker:
1.000.000+	N	nein	nein	5

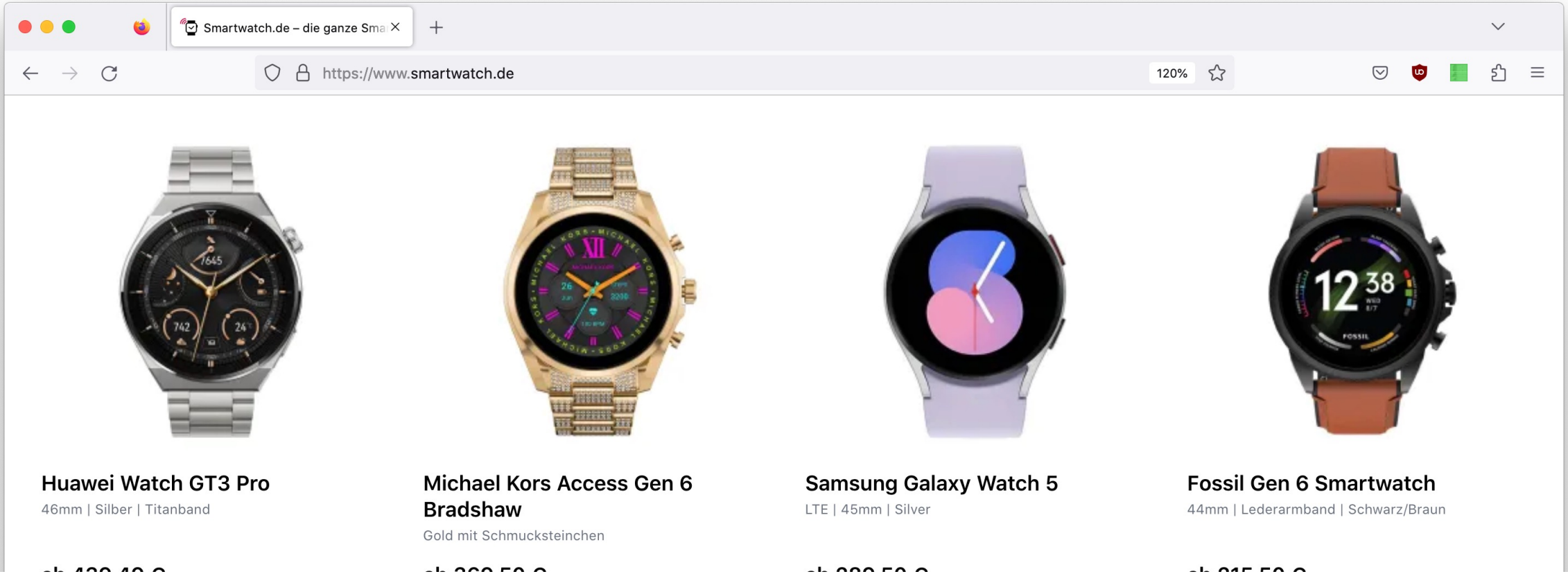
Testbericht, Version 3.3.3 vom 22.07.2022

Mit dieser App gehen Sie ein Risiko für Ihre Privatsphäre ein. Diese Punkte sehen wir kritisch:

Die App baute eine Internetverbindung zu fünf bekannten Drittanbietern auf, die alle im Bereich Werbung, Marketing oder Nutzeranalyse tätig sind. Aufgrund der Dienstleistungen, die diese Unternehmen anbieten, gehen wir davon aus, dass dabei Informationen über Ihr Gerät, Ihren ungefähren Standort und Ihr Online-Verhalten gesammelt werden. Die App kontaktiert im Vergleich überdurchschnittlich viele dieser Tracker, was einen Überblick über die eigenen Daten besonders erschwert. Daher vergeben wir hier Score vier.

Alle relevanten, im Test übermittelten Informationen, sowie die Besitzer aller kontaktierten Internetadressen, sind in der Tabelle weiter unten aufgeführt.

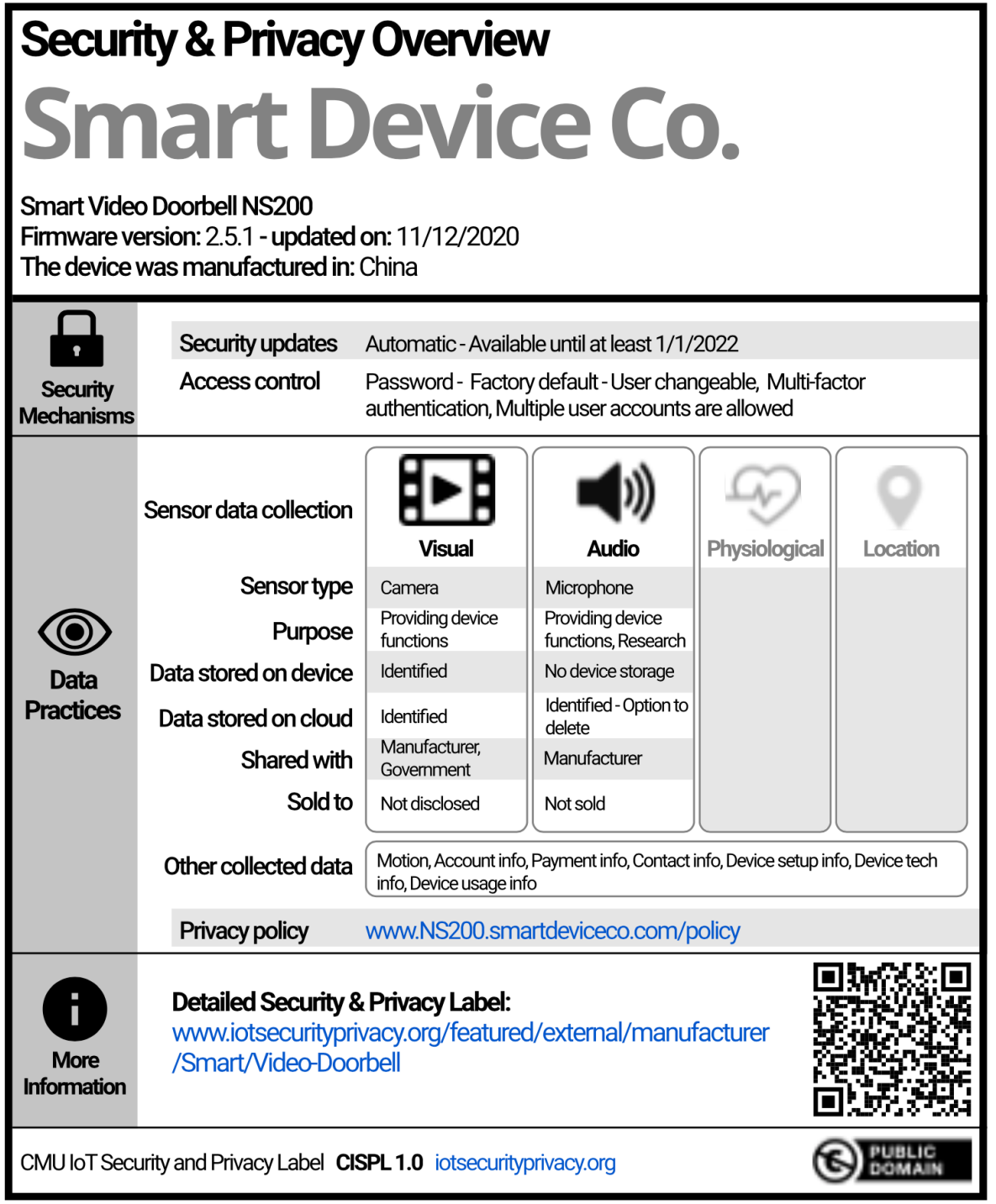

tosdr.org
Home Ratings About Us Download Extensions API Forum Status Page Login Add a new Service Communities
Donate JOIN BETA English
Terms of Service Didn't Read
"I have read and agree to the Terms"
PayPal Grade E
You waive your moral rights
This service holds onto content that you've deleted
This service still tracks you even if you opted out from tracking
You must provide your identifiable information
Third-party cookies are used for advertising
View All Points on Phoenix!
View Documents
Visit Service
PayPal Privacy Grade E
Startpage Grade A
This service does not track you
The service will resist legal requests for user information where reasonably possible
The cookies used by this service do not contain information that would personally identify you
The cookies used by this service do not contain information that would personally identify you
IP addresses of website visitors are not tracked
View All Points on Phoenix!
View Documents
Visit Service
Startpage Privacy Grade A
WikiHow Grade E
The service can read your private messages
This service can share your personal information to third parties
The service can delete your account without prior notice and without a reason
Pinterest Grade E
They store data on you even if you did not interact with the service
The service can read your private messages
The service can delete specific content without reason and may do it without prior notice



Samsung	Fitbit	Apple	Xiaomi	Huawei	Diesel
kampyle	optimizely	metrics.icloud	firebaselogging	optimizely	onesignal
googleapis	m.stripe	xp.apple			
eum-appdynamics					
onesignal					

Security und Privacy Label für bessere Transparenz?

Erste Ergebnisse sehen gut aus!



https://iotsecurityprivacy.org/downloads/Emami-Naeni_USENIX23_ConsumerWillingnesstoPay.pdf
https://doi.org/10.1145/3290605.3300764

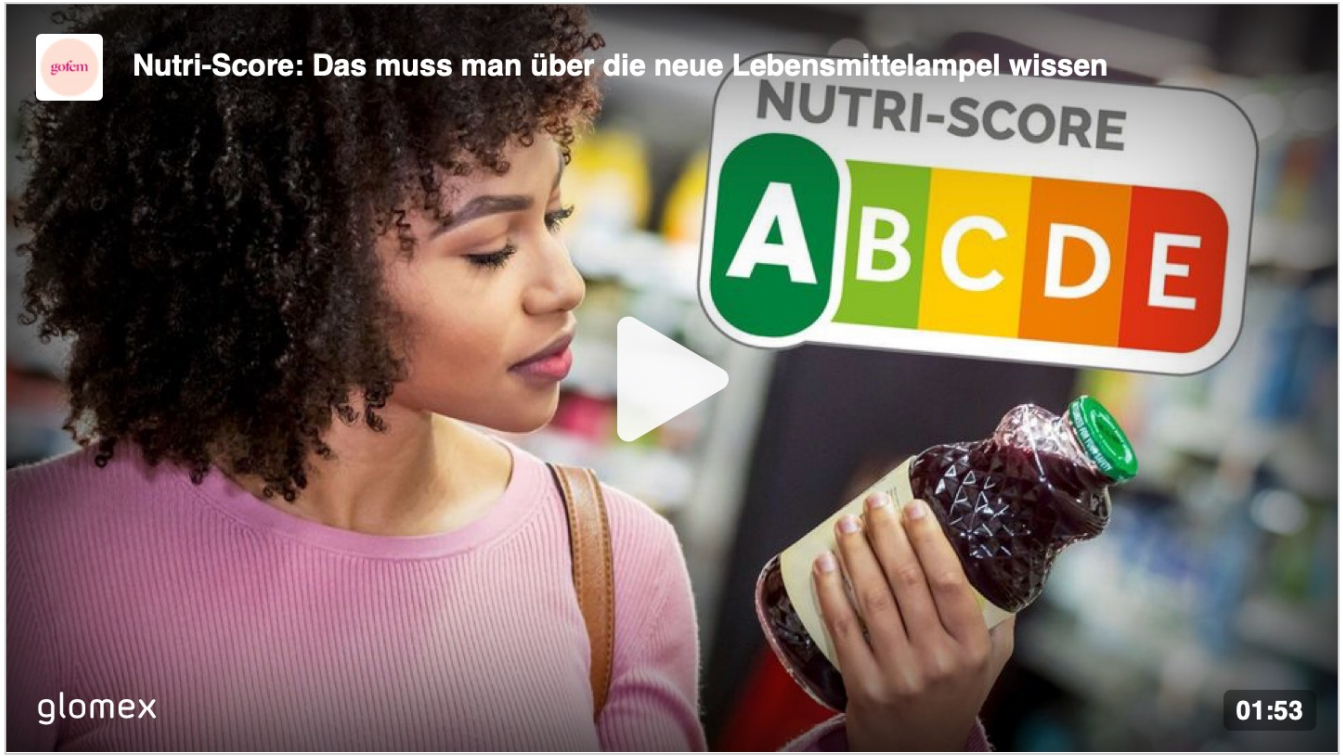
Security und Privacy Label für bessere Transparenz?

Nutri-Score bei Lebensmitteln

Verwirrender Nutri-Score

Nestlé-Kakao ist „gesund“: Verbraucherzentrale warnt vor Schönrechnerei

13.05.2021 - 20:45



Ein Kakao von Nestlé besteht zu 70 Prozent aus Zucker und ist laut Nutri-Score dennoch „gesund“. Wie kann das sein, hat sich die Verbraucherzentrale gefragt. Hier die Antwort.

https://www.ruhr24.de/service/nestle-nesquik-kakao-gesund-trinkschokolade-kaba-verbraucherzentrale-nutriscore-deutschland-90575275.html

Betreiben wir Bike Shedding?

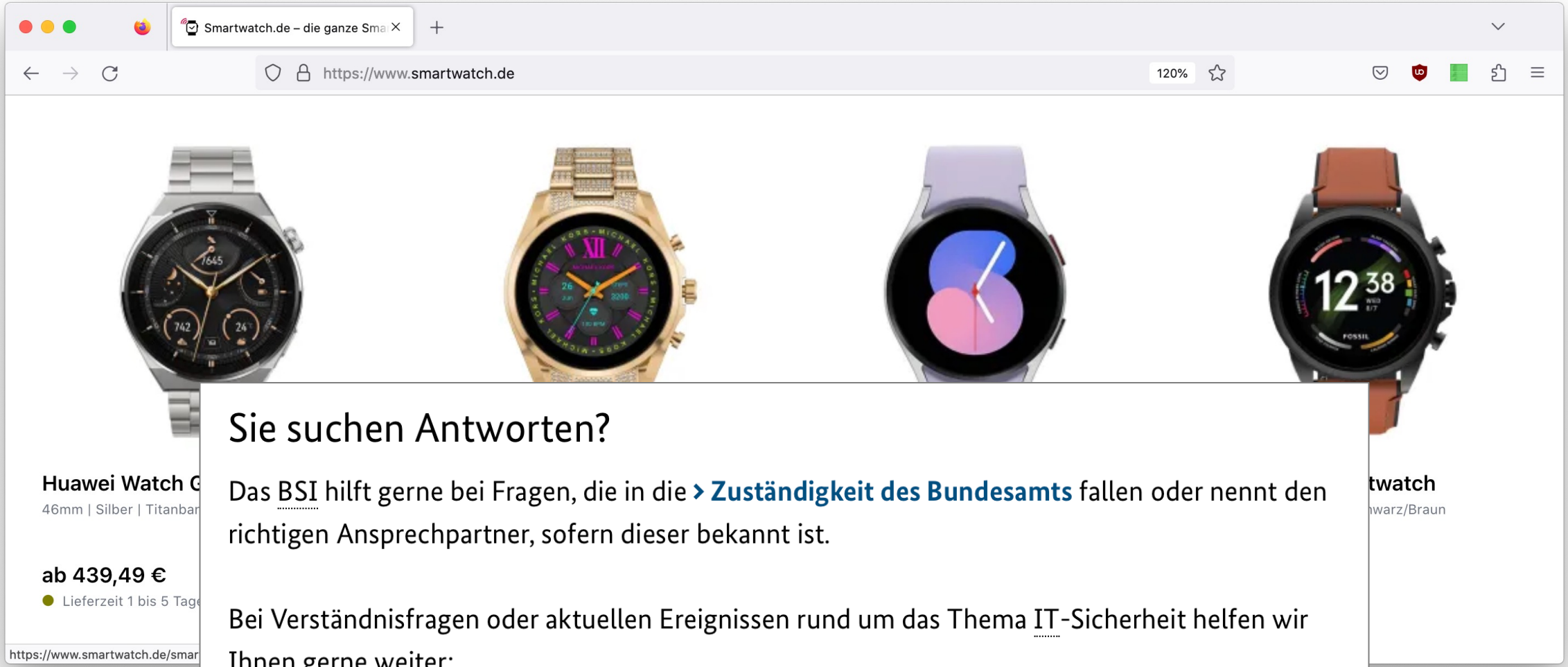
Wir sollten die Ursache des Problems nicht aus den Augen verlieren.

(Viele?) VuV vertrauen auf die Expertise von Fachleuten

z.B. bei Anlageprodukten (finanztest, finanztip.de, …)

***Eingriff in den Markt**

Wer kann neutral Empfehlungen* aussprechen?



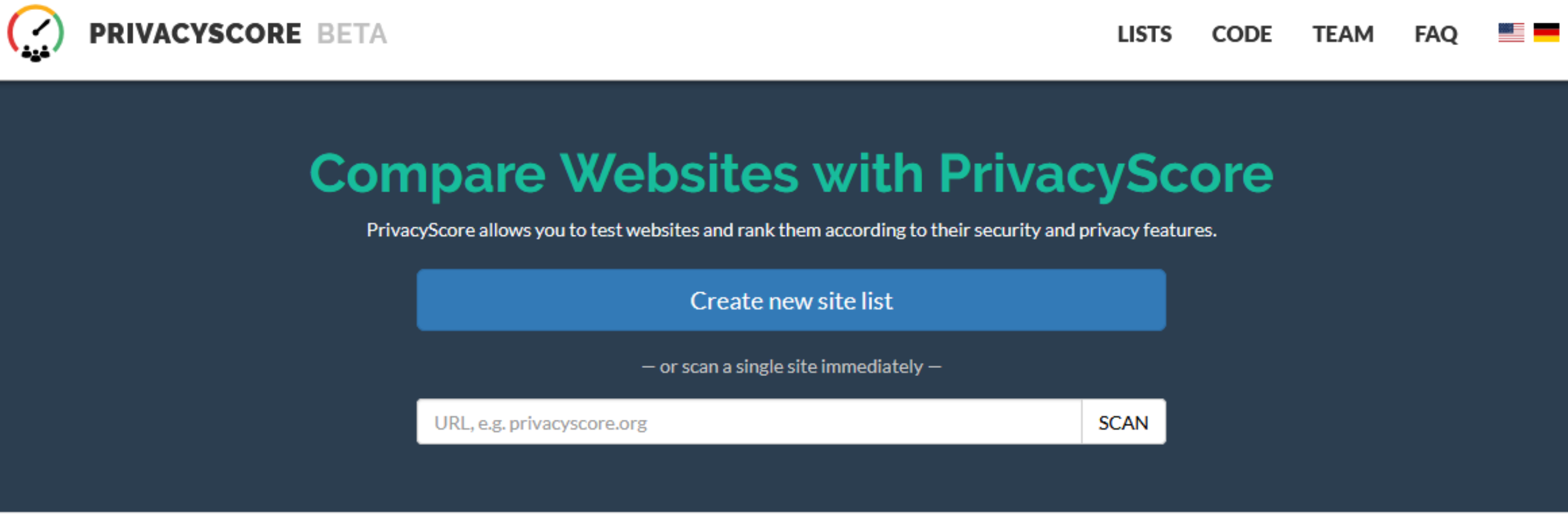
Sie suchen Antworten?

Das BSI hilft gerne bei Fragen, die in die **› Zuständigkeit des Bundesamts** fallen oder nennt den richtigen Ansprechpartner, sofern dieser bekannt ist.

Bei Verständnisfragen oder aktuellen Ereignissen rund um das Thema IT-Sicherheit helfen wir Ihnen gerne weiter:

Erreichbarkeit: ***Montag bis Freitag von 08:00-18:00 Uhr***
Telefon: ***0800 274 1000***
(kostenlos aus dem deutschen Fest- und Mobilfunknetz)
Oder schicken Sie eine E-Mail an: ***service-center@bsi.bund.de***

Die Wissenschaft?



Webseiten deutscher Krankenkassen und -versicherungen

Ranking

#	URL	Name	Versicherte	Typ	Kategorie	NoTrack	EncWeb	Attacks	EncMail	Rating
1	http://www.ikkbb.de/ / 2019-12-08 @ 18:59:22	Innungskrankenkasse Brandenburg und Berlin	212.807	gesetzl	IKK	✓	✓	!	?	!
2	http://www.bkk-bpw.de/ / 2019-12-08 @ 19:02:21	Betriebskrankenkasse BPW Bergische Achsen KG – betriebsbezogen	6.550	gesetzl	BKK	✓	!	!	?	!
3	http://www.atlasbkkahlmann.de/ / 2019-12-08 @ 18:59:22	Atlas BKK ahlmann	55.000	gesetzl	BKK	✓	!	!	?	!
4	http://www.bkkgs.de/ / 2019-12-08 @ 19:01:25	BKK Gildemeister Seidensticker	183.297	gesetzl	BKK	✓	!	!	!	!
5	http://www.bkk-pfaff.de/ / 2019-12-08 @ 19:01:17	Betriebskrankenkasse der G. M. Pfaff AG Kaiserslautern	29.391	gesetzl	BKK	✓	!	!	!	!
5	http://www.bkk-linde.de/ / 2019-12-08 @ 19:02:59	BKK Linde	89.540	gesetzl	BKK	✓	!	!	!	!
6	http://www.bkk-da.de/ / 2019-12-08 @ 19:02:45	BKK Dürkopp Adler	23.622	gesetzl	BKK	✓	!	!	!	!
7	http://www.bkk-grillo.de/ / 2019-12-08 @ 19:01:25	BKK Grillo-Werke AG – betriebsbezogen	1.150	gesetzl	BKK	✓	✗	!	!	✗

Wie reagieren Anbieter, wenn sie auf das Ranking hingewiesen werden?

M. Maass et al., **On the Difficulties of Incentivizing Online Privacy through Transparency: A Qualitative Survey of the German Health Insurance Market**, WI 2019, https://arxiv.org/abs/1811.12775 (2019).

Von weiteren Scans ausgenommen

Die Betreiber der hier aufgeführten Seiten haben uns gebeten, keine weiteren Scans durchzuführen. Aus Gründen der Transparenz archivieren wir das Ergebnis des letzten erfolgreichen Scans in der folgenden Tabelle. Beachten Sie, dass es möglich ist, dass Seitenbetreiber in der Zwischenzeit Änderungen an ihrer Website vorgenommen haben, die sich nicht in diesen veralteten Ergebnissen widerspiegeln.

#	Adresse (URL)	Name	Versicherte	Typ	Kategorie	NoTrack	EncWeb	Attacks	EncMail	Rating
1	http://www.meine-krankenkasse.de/ / 2018-01-12 @ 06:51:56	BKK Verkehrsbau Union	498.000	gesetzl	BKK	!	!	!	?	!
2	http://www.novitas-bkk.de/ (1 Fehler) / 2018-01-16 @ 13:18:50	Novitas BKK	410.216	gesetzl	BKK	!	!	!	?	!
3	http://www.bmwbkk.de/ / 2017-12-18 @ 13:53:50	Betriebskrankenkasse der BMW AG – betriebsbezogen	157.839	gesetzl	BKK	!	!	!	!	!
4	http://www.big-direkt.de/ / 2017-12-13 @ 14:46:08	Bundesinnungskrankenkasse Gesundheit	409.000	gesetzl	IKK	!	!	!	!	!
5	http://www.ikk-nord.de/ / 2017-12-14 @ 13:40:04	Innungskrankenkasse Nord	230.005	gesetzl	IKK	!	!	!	!	!
6	http://www.die-bergische-kk.de/ / 2017-12-18 @ 09:48:17	Die Bergische Krankenkasse	71.889	gesetzl	BKK	!	!	⚠	!	⚠
7	http://www.bkkdb.de/ / 2018-01-11 @ 06:27:53	BKK Deutsche Bank AG – betriebsbezogen	80.998	gesetzl	BKK	!	✖	!	?	✖
8	http://www.bkk-pwc.de/ / 2017-12-18 @ 10:08:47	Betriebskrankenkasse PricewaterhouseCoopers – betriebsbezogen	19.001	gesetzl	BKK	!	✖	!	!	✖

Betrieb in Deutschland rechtlich zulässig, *arxiv.org/abs/1705.08889* (GI INFORMATIK 2017)

Anbieter haben wenig Anreize, Produkte sicherer zu machen.

- Buchbinder (2020): kein Bußgeld verhängt
- Quickticket (Feb 2023): Sicherheitslücke monatelang offen
- Godaddy: “4 breaches in 4 years”

Auch Habeck und BSI-Chef betroffen Kundendaten von Autovermieter Buchbinder standen offen im Netz

Ein IT-Sicherheitsexperte entdeckt ein großes Datenleck. Mietverträge und Unfallberichte waren einsehbar. Die Firma habe nicht auf Hinweise reagiert.

Wie ein Datenleck in einem Arzt-Terminservice monatelang offen bleiben konnte

Das erfolgreiche Melden von Sicherheitslücken ist nicht immer so einfach. Ein Beispiel aus dem Umfeld von Arztpraxen zeigt, wo Stolpersteine liegen.

Lesezeit: **8 Min.** speichern 37

https://www.heise.de/hintergrund/Wie-ein-Datenleck-in-einem-Arzt-Terminservice-monatelang-offen-bleiben-konnte-7526518.html

Warum sind Privacy by Disaster und Security by Disaster so verbreitet?

- Allgemeiner Übergang zu **reaktiver Sicherheit**.
- Sicherheitslücken suchen wird nicht angemessen honoriert – und birgt persönliche Risiken.
- Unzureichende Durchsetzung des Rechts.

heise online heise+

Offenlegung von Softwarelücken: Rechtsstreit endet mit Vergleich

Forscher mit der Urheberrechtskeule an der Veröffentlichung von Softwarelücken zu hindern, widerspreche gesundem Menschenverstand, befand ein Landgericht.

Lesezeit: **4 Min.** speichern 126

Dritte Zivilkammer des Landgerichts Nürnberg-Fürth unter dem Vorsitz von Ulrich Dettenhofer (Bild: heise online/Ermert)

06.09.2018 12:36 Uhr

Von Monika Ermert

Fear, Uncertainty, Doubt (FUD) wurden ggü. Anbietern noch nicht ausgeschöpft.*

- Vermehrte anlasslose Kontrollen (vgl. Gastro-Hygienechecks)**
- Bußgelder und Untersagungen
- Herstellerhaftung bei nicht behobenen Schwachstellen

* unsere Studien zur Google-Analytics-Nutzung und Art. 15 DSGVO zeigen: Anbieter handeln dann eher

** für Wissenschaftler schwierig wegen forschungsethischer Schwierigkeiten

Max Maass, Alina Stöver, Henning Pridöhl, Sebastian Bretthauer, Dominik Herrmann, Matthias Hollick, Indra Spiecker: Effective Notification Campaigns on the Web: A Matter of Trust, Framing, and Support. USENIX Security Symposium 2021: 2489-2506
Jacob Leon Kröger, Jens Lindemann, Dominik Herrmann: How do app vendors respond to subject access requests?: a longitudinal privacy study on iOS and Android Apps. ARES 2020: 10:1-10:10

Konstruktive Handlungsfelder

- Bug-Bounty-Programm oder Kompensationsmöglichkeiten für die Schwachstellensuche
- Definition des Stands der Technik
- Kriterien für sichere Produkte

CONSUMER EMPOWERMENT

„Unser Produkt kann im Prinzip schon sicher betrieben werden – man muss sich halt auskennen!“

Geht das wirklich nicht besser?

SELBSTBESTIMMT UNSICHER?

Herausforderungen an Datensicherheit und Datenschutz im digitalen Alltag

Prof. Dr. **Dominik Herrmann**
Otto-Friedrich-Universität Bamberg

https://herdom.net Folien: https://dhgo.to/selbstbestimmt23