

Digital Sovereignty through Self-Hosting?

A Human-Centered View on Security Challenges

Lea Gröber - Doctoral Researcher @CISPA, Germany

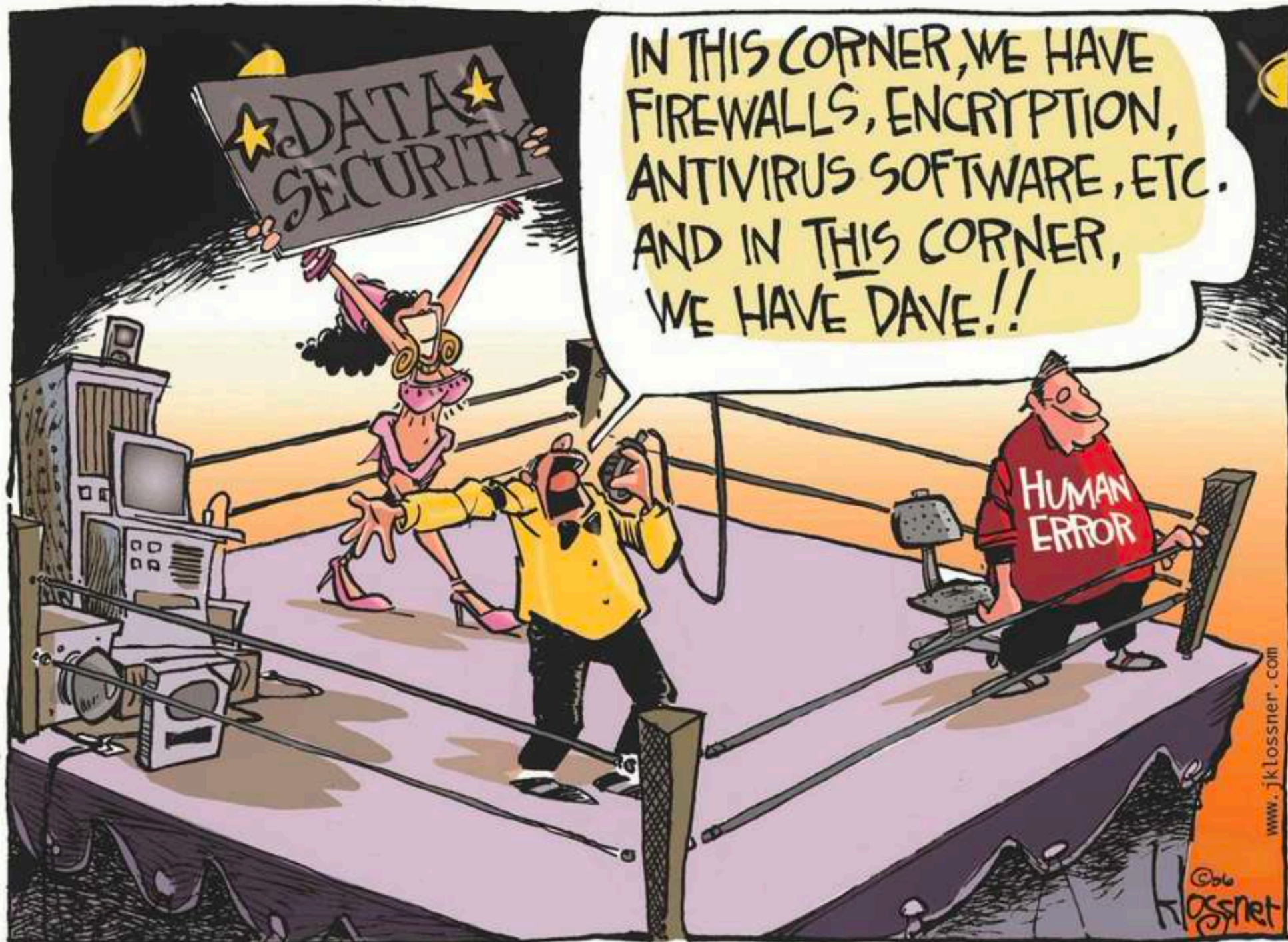




Lea Gröber



- M.Sc. in Compute Science, Saarland University
- Doctoral Researcher in the Usable Security group of Katharina Krombholz
- Research interests in empowering users and making the Internet a safer and more inclusive space





A Brief Excursion: What is Usable Security?

Three seminal papers from the 90s

Common message:

- Users should not merely be seen as a problem to be dealt with
- Security professionals need to communicate more with users and adopt user-centred design approaches

USERS ARE NOT THE ENEMY

Why users compromise computer security mechanisms and how to take remedial measures.

Confidentiality is an important aspect of computer security. It depends on authentication mechanisms, such as passwords, to safeguard access to infor-

**Why Johnny Can't Encrypt:
A Usability Evaluation of PGP 5.0**

Alma Whitten
*School of Computer Science
Carnegie Mellon University
Pittsburgh, PA 15213
alma@cs.cmu.edu*

J. D. Tygar¹
*EECS and SIMS
University of California, Berkeley*

User-Centered Security

Mary Ellen Zurko
zurko@opengroup.org
The Open Group Research Institute
Eleven Cambridge Center
Cambridge, MA 02142

Richard T. Simon
rsimon@opengroup.org
The Open Group Research Institute
Eleven Cambridge Center
Cambridge, MA 02142

tract— We introduce the term user-centered security to We evaluate the pros and cons of this effort, as a p



In this Talk

1. Digital Sovereignty

Human-centered view of self-hosting through two papers:

2. Exploring Self-Hosting Dimensions

Motivation, Operation, Security Challenges

3. Measuring Self-Hosting on a Large-Scale

Prevalence, Population Analysis



My Awesome Collaborators



**Simon
Lenau**



**Rebecca
Weil**



**Elena
Groben**



**Michael
Schilling**



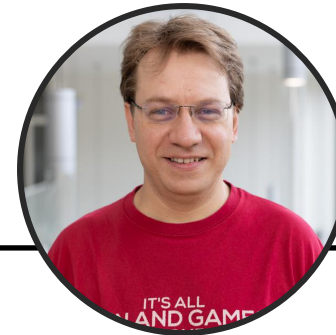
**Nimisha
Vijay**



**Daphne
Muller**



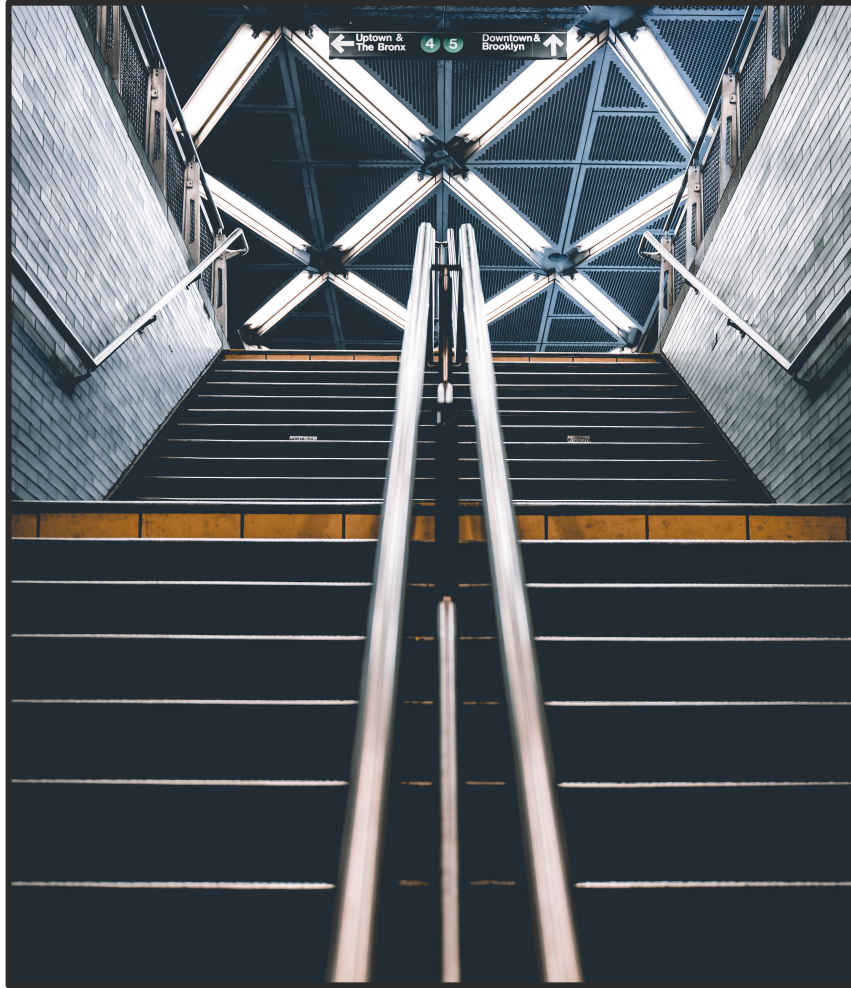
**Rafael
Mrowczynski**



**Adrian
Dabrowski**



**Katharina
Krombholz**



Digital Sovereignty

What is it and how can it be achieved?



A Definition of Digital Sovereignty

“Digital sovereignty is the sum of all **abilities** and **options** of **individuals** and **institutions** to be able to exercise their role(s) in the digital world in an **independent**, **self-determined** and **secure manner.**”

- German Competence Center for Public IT



Abilities

- Expertise
 - Education
 - Specialized Background (e.g. It, Security)
- Skills
 - related to specific domain (e.g. hosting, Web browsing)





A Definition of Digital Sovereignty

“Digital sovereignty *is the sum of all abilities and options of individuals and institutions to be able to exercise their role(s) in the digital world in an independent, self-determined and secure manner.”*

- German Competence Center for Public IT



Technological Options

- Privacy violating or preserving
- Security Mechanisms
- Usability





The FTC's New Report Reaffirms Big Tech's Personal Data Overreach – What's New?

The report confirms that privacy advocates have been



WORK & ECONOMY

High tech is watching you

John Laidler | Harvard Correspondent

March 4, 2019 • 8 min read

In new book, Business School professor emerita says surveillance capitalism undermines autonomy – and democracy

...l revolution can be dazzling. But at Harvard Business School, warns that ...ade us blind and deaf to the ways high- ...for their own ends.



404

SIGN IN SUBSCRIBE

FEATURES

Inside the U.S. Government-Bought Tool That Can Track Phones at Abortion Clinics

Privacy advocates gained access to a powerful tool bought by U.S. law enforcement agencies that can track smartphone locations around the world. Abortion clinics, places of worship, and individual people can all be monitored without a warrant.

JOSEPH COX · OCT 23, 2024 AT 6:00 AM



WORK & ECONOMY

...ch is watching you

John Laidler | Harvard Correspondent

March 4, 2019 · 8 min read

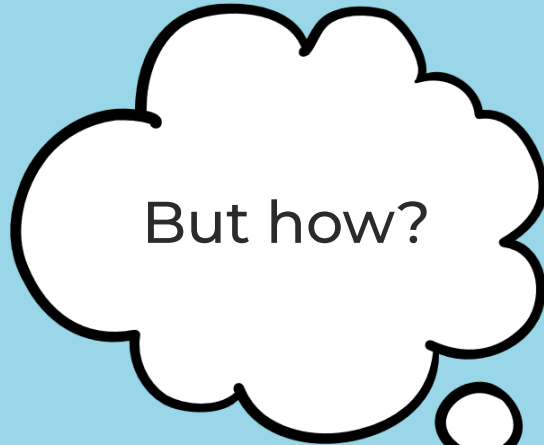
... Business School professor ... surveillance capitalism ... autonomy – and

SUBSCRIBE

... revolution can be dazzling. But
... at Harvard Business School, warns that
... made us blind and deaf to the ways high-
... for their own ends.

Bought Tool That Can Track Phones at Abortion Clinics

... access to a
powerful tool bought by U.S. law
enforcement agencies that can track
smartphone locations around the
world. Abortion clinics, places of
worship, and individual people can all
be monitored without a warrant.



WORK & ECONOMY

ch is watching you

John Laidler | Harvard Correspondent

March 4, 2019 · 8 min read

Business School professor s surveillance capitalism s autonomy – and

SUBSCRIBE

l revolution can be dazzling. But
t Harvard Business School, warns that
ade us blind and deaf to the ways high-
for their own ends.

Bought Tool That Can Track Phones at Abortion Clinics

access to a
powerful tool bought by U.S. law
enforcement agencies that can track
smartphone locations around the
world. Abortion clinics, places of
worship, and individual people can all
be monitored without a warrant.



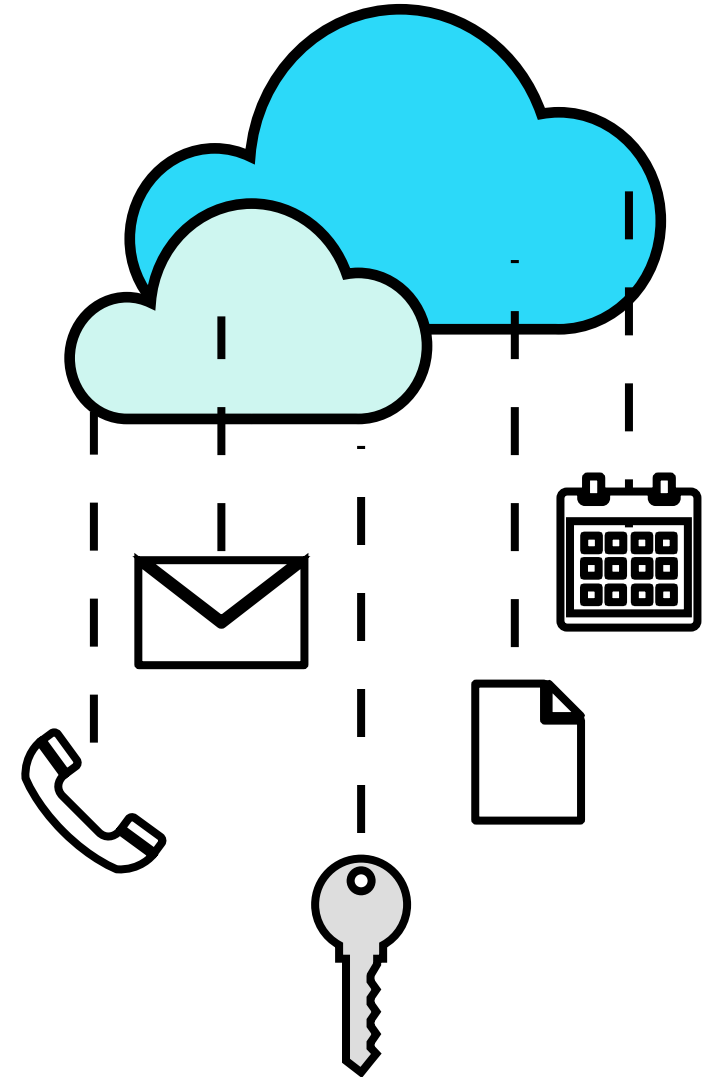
Self-Hosting

as a practice that enables the largest degree of digital sovereignty.



What is “Self-Hosting”?

- A. Control over hardware
- B. Control over software
- C. Dedicated installation for the usage of that user or organisation





Gepostet von u/muchTasty vor 1 Jahr 7 2 2

925

Beginner guide: How to secure your self-hosted services



Self Help

Hi guys,

I decided to write this little guide following a bunch of posts about people having their things published without any form of protection on the web.

I hope this helps many gain a little insight in to what they're actually doing.

Note: This will be a work-in-progress at first. Any feedback is welcome!

Important: This guide is aimed at *beginners*, so I won't go too much in-depth and mostly rely on common sense and (fairly) easy to implement solutions. I will make a more advanced guide later on.

READ ME FIRST:

Über diese Community



r/selfhosted

A place to share alternatives to popular online services that can be self-hosted without giving up privacy or locking you into a service you don't control.



Erstellt am 8. Juli 2014

232k

Mitglieder

● 1.2k

Online

Oberste 1%

Sortiert nach Größe

Beitreten

Ähnlich wie dieser Beitrag



r/rust

redact: tool for building decentralized,





To Cloud or not to Cloud: A Qualitative Study on Self-Hosters' Motivation, Operation, and Security Mindset

Lea Gröber, *CISPA Helmholtz Center for Information Security and Saarland University*;
Rafael Mrowczynski, *CISPA Helmholtz Center for Information Security*;
Nimisha Vijay and Daphne A. Muller, *Nextcloud*; Adrian Dabrowski and
Katharina Krombholz, *CISPA Helmholtz Center for Information Security*
<https://www.usenix.org/conference/usenixsecurity23/presentation/grober>

This paper is included in the Proceedings of the
32nd USENIX Security Symposium.

August 9–11, 2023 • Anaheim, CA, USA
978-1-939133-37-3

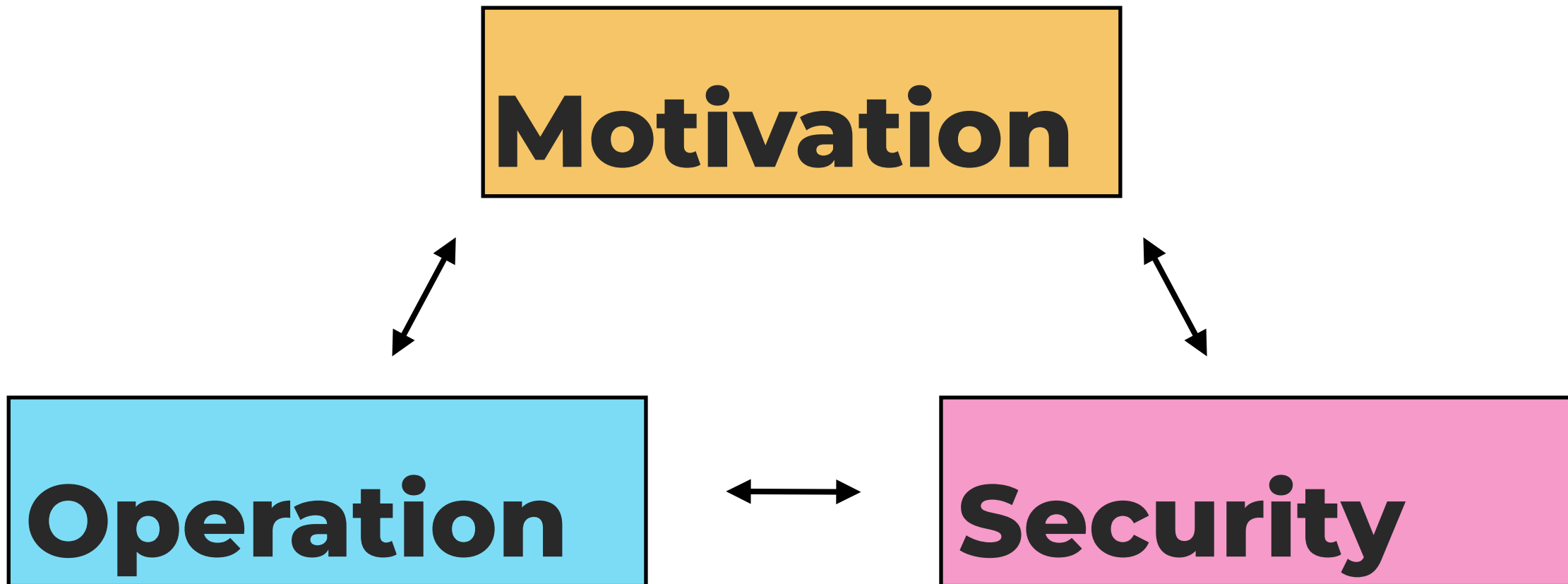
Open access to the Proceedings of the
32nd USENIX Security Symposium
is sponsored by USENIX.

Research Questions

1. What motivates people to self-host?
2. How do self-hosters operate?
3. What are perceived threats and how do self-hosters manage them?
4. How do self-hosters maintain their set-up?



Goal: Exploring Self-Hosting Dimensions





Case Study on Nextcloud





Methodology

Combining broad high-level data with individual in-depth insights.

- I. **Nextcloud Community Survey (N=994)**
qualitative and quantitative data

User groups:

private, commercial, non-profit, government

- II. **Semi-structured Interviews (N=41)**
qualitative data

User groups:

private, commercial, non-profit



Participant Overview

- I. **16 Countries** across Europe, North America, and Oceania
- II. **Professional background** is broad (teachers, journalists, lawyers, developers, system administrators, ...)
- III. **Commercial users:** Architectural offices, law firms, journalists, travel agencies, ...
- IV. **Non-profit users:** research institutes, universities, schools, political parties, art collectives, different clubs, and a data protection community,
- V. **Diverse set-ups:** Raspberry pis, repurposed, or upcycled hardware, private data centers, hosting on third-party clouds



Participant Overview

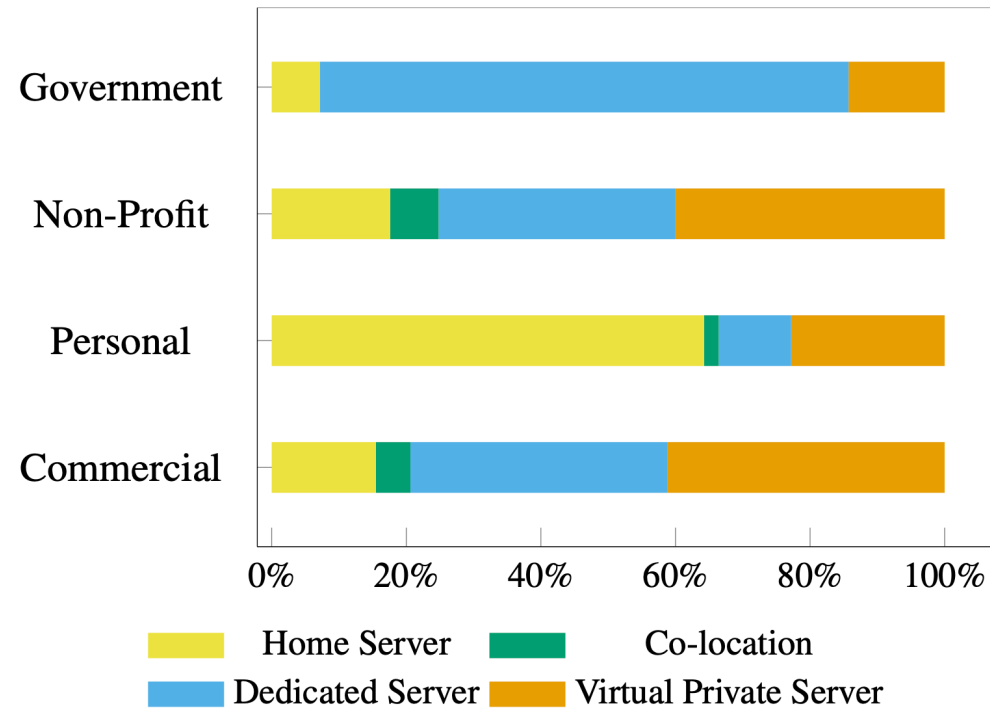


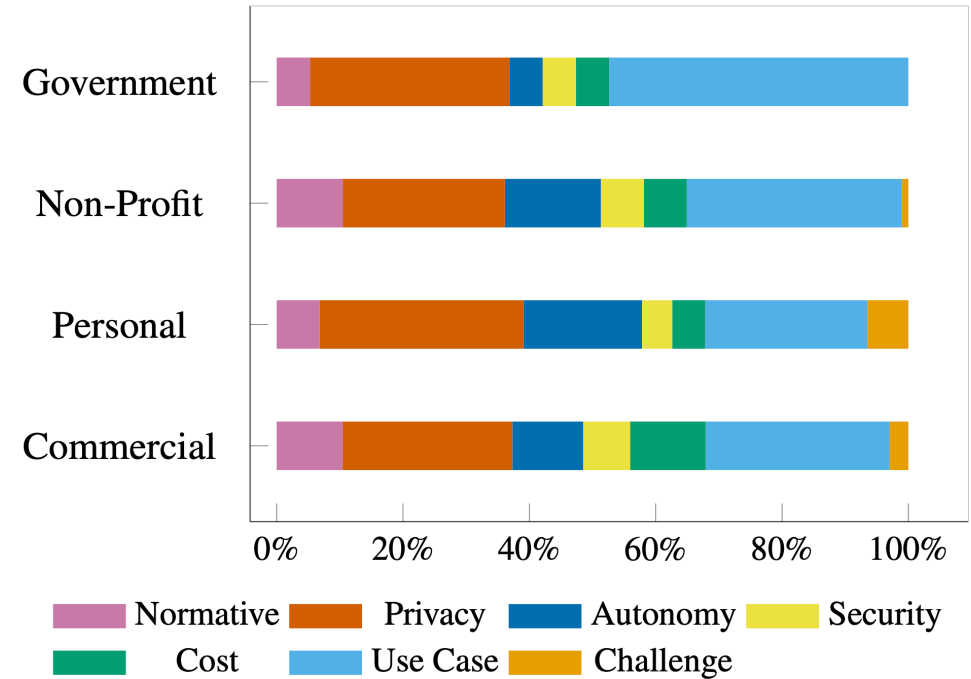
Figure 4: *[survey data]* Relative frequencies of reported server types across user groups.



RESULTS

Motivation

- Normative Driven
- Privacy Driven
- Autonomy Driven
- Security Driven
- Cost Saving
- Use-Case Driven
- Personal Challenge





RESULTS

Operator Constellations

Self-hosting as a socially-embedded activity

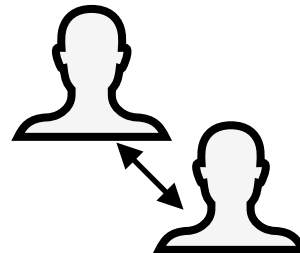
- ♥ private
- non-profit
- commercial



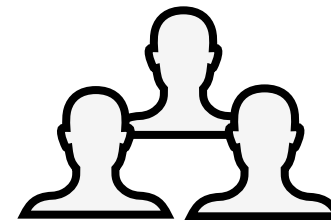
Sole Operator



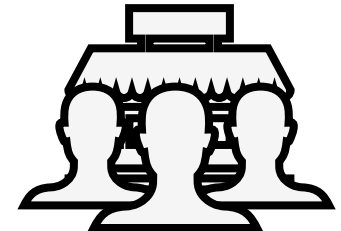
Organisational
Embedded Sole
Operators



Knowledge
Bartering



Collaborative
Networks



Team Members
Within Organ-
isations



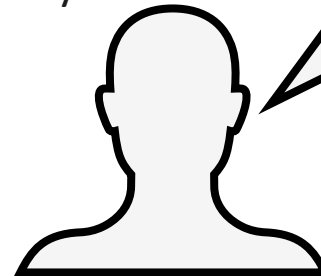


RESULTS

Security Mindsets + Practices

- Attacker Models
- Perceived Risks
- Trust Anchors
- Defensive Mechanisms
- Maintenance

78%
of survey



The security of my Nextcloud instance is a concern to me.



Perspectives on Security

“Security is [a] prerequisite for everything else”

”
survey 957
government

- no software or system can ever be 100% secure [i17-np, i20-np]

Fatalistic Mindset

- skilled attacker can break into any system
- “so i wouldn’t even try [defending]” [i44-c]

Pragmatic Mindset

- acknowledge threats
- security is achievable when following state-of-the-art security recommendations [i2-c]



Attacker Models

- **Targeted State Actor**

- biggest threat to lawyer and investigative journalist
- public knowledge on how institutions legally are allowed to operate + experiences (own and colleagues')
- threat: gaining access through search warrants
- believe self-hosting is only way to protect data, thus knowledge bartering



Attacker Models

- Targeted State Actor

pragmatic

"[the operator] is a former client of mine. And no law enforcement agency in the world had managed to penetrate [their] systems"^{l-14c}.



fatalistic

"it would be game over against a national security service. I don't think someone at my level can defend against that, so I wouldn't even try"^{l-44c}



Attacker Models

- **Targeted External Attacker**
 - only companies identified this threat
 - business competitors, opponents to their cause, personal enemies
 - rivaling artists use hacking as a form of dialogue [i21-np]
 - globally operating energy corporations seek to spy on and sabotage climate activists [i17-np]

“Any kind of attacker that can spend on one person that is skilled/motivated for some months would be able to access data. So this is my rough estimation, which is based on nothing.”



interview 17
non-profit



Attacker Models

- **Internal Attacker**
- mentioned rarely
- malicious admins
- hosting provider (case of off-premise instances)
- broad understanding that users are not trustworthy
- it is their incompetence that makes them a risk, not malicious intent
- personal self-hosters do not report users as potential threats

“ [I know my users], so it’s unlikely that there would be malicious intent

”

interview 44
commercial



Attacker Models

- **Untargeted External Attacker**
- most prominent across groups; participants rank this as top threat
- bots, “Script Kiddies” who “poke around the internet fro the fun of it” [i5-p]
- most had pragmatic mindset
- low-expertise hosters have issues to identify adequate means of protection
- problems when mindset is borrowed from the end-user domain

“*My security is probably woeful*”

”

interview 5
private

“*Ransomware usually targets Microsoft, not Linux*”

”

interview 5
private



RESULTS

Gaps in Security Mindsets

1. Attacker Model

“ *Everything is a threat.*

”

interview 40
non-profit



RESULTS

Gaps in Security Mindsets

1. Attacker Model
2. Prioritising Risk

“*I learn what I can [...], but server security feels like a bottomless pit.*”

”

survey 118
private



RESULTS

Gaps in Security Mindsets

1. Attacker Model
2. Prioritising Risk
3. Identifying Defensive Mechanisms

“ *I don't have to pay attention to what services are running and what ports they have open.* **”**

interview 35
commercial

Challenges for Digital Sovereignty

- The security of the operations poses a major challenge to individuals and institutions.
- Without robust security, however, the privacy guarantees that self-hosting offers do not hold in practice.



Towards Privacy and Security in Private Clouds: A Representative Survey on the Prevalence of Private Hosting and Administrator Characteristics

Lea Gröber, *CISPA Helmholtz Center for Information Security and Saarland University*;
Simon Lenau and Rebecca Weil, *CISPA Helmholtz Center for Information Security*;
Elena Groben, *Saarland University*; Michael Schilling and Katharina Krombholz,
CISPA Helmholtz Center for Information Security

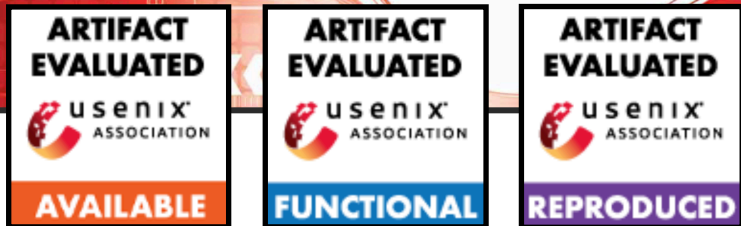
<https://www.usenix.org/conference/usenixsecurity24/presentation/gröber-private-clouds>

This paper is included in the Proceedings of the
33rd USENIX Security Symposium.

August 14–16, 2024 • Philadelphia, PA, USA

978-1-939133-44-1

Open access to the Proceedings of the
33rd USENIX Security Symposium
is sponsored by USENIX.

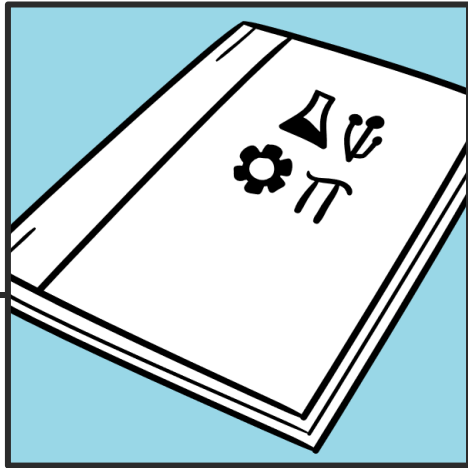


Research Questions:

- How widespread is self-hosting for private use cases?
- Which tools are self-hosted and how?
- What kind of people are self-hosting?
- In which characteristics do self-hosters differ from the average U.S. population?

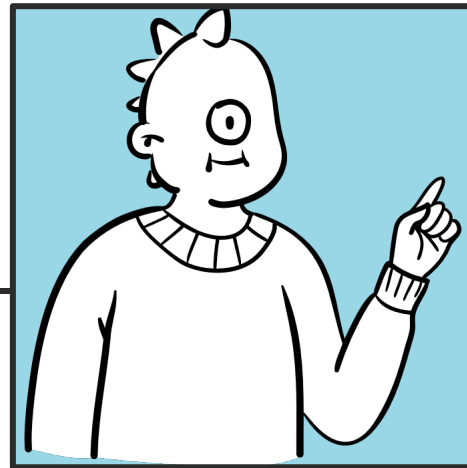


Study Procedure



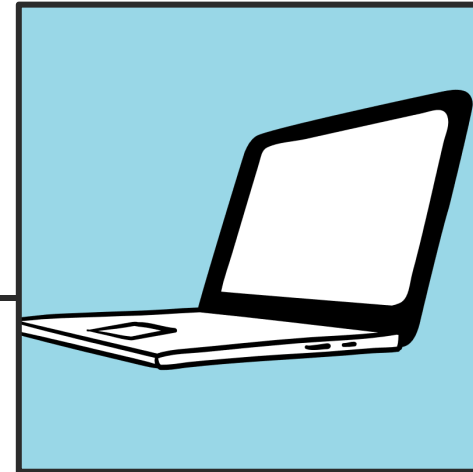
Literature Review

Define scope and form hypotheses



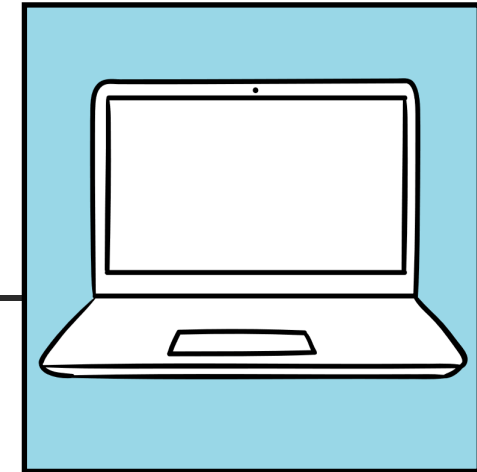
Focus Groups

(non) technical participants to explore scope and solidify hypotheses



Survey 1 (n=1505)

Online (Prolific) focusing on prevalence and technical perspective



Survey 2 (n=589)

Online (Prolific) focusing on individual characteristics



Survey 1 (n=1505)

Goal:

Estimate the prevalence of private Self-Hosting






Method:

Identification of Self-Hosters in a representative sample of the U.S. population (age, sex, ethnicity)

Framing:

Survey on Software and Application Use

Use cases:

-  **File storage** - synchronization, transfer
-  **Web sites** - CMS, blogging
-  **Communication** - messaging, voice/video telephony
-  **Synchronized Password Managing**
-  **Smart Home**



Survey 1 (n=1505)

Goal:












Estimate the prevalence of private Self-Hosting

Method:

Identification of Self-Hosters in a representative sample of the U.S. population (age, sex, ethnicity)

Framing:

Survey on Software and Application Use

	private context	work context (resp. studies)
 ownCloud	<input type="checkbox"/>	<input type="checkbox"/>
 Seafile	<input type="checkbox"/>	<input type="checkbox"/>
 MEGA	<input type="checkbox"/>	<input type="checkbox"/>
 SparkleShare	<input type="checkbox"/>	<input type="checkbox"/>
 Microsoft OneDrive	<input type="checkbox"/>	<input type="checkbox"/>
 Dropbox	<input type="checkbox"/>	<input type="checkbox"/>
 Box	<input type="checkbox"/>	<input type="checkbox"/>
 Google Drive	<input type="checkbox"/>	<input type="checkbox"/>
 Synthing	<input type="checkbox"/>	<input type="checkbox"/>
 Nextcloud	<input type="checkbox"/>	<input type="checkbox"/>
 iCloud	<input type="checkbox"/>	<input type="checkbox"/>
I do not use any of these tools	<input type="checkbox"/>	<input type="checkbox"/>



Findings S1: Prevalence

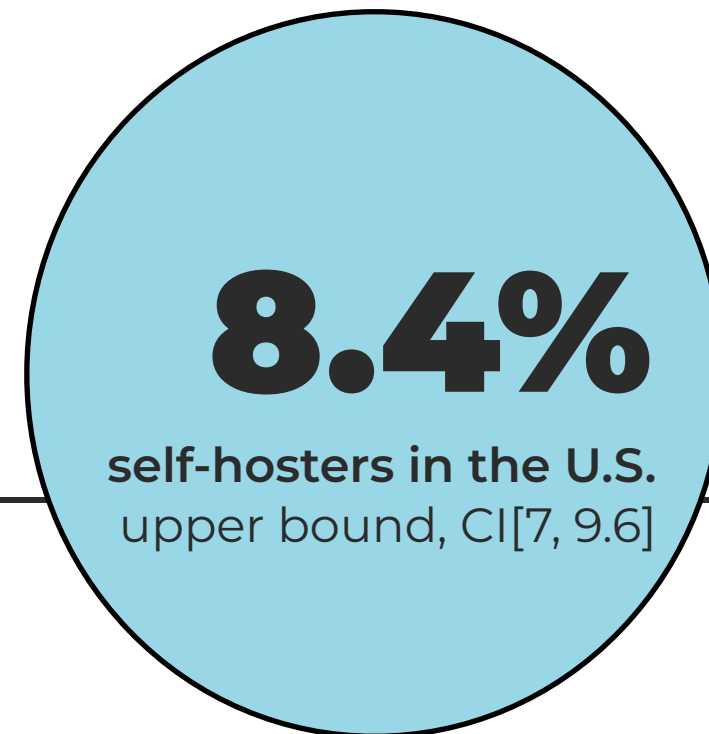
- Selected or added at least 1 self-hostable tool in one of the use case categories
- Indicated that they had set it up themselves on a server
- Confirmed they had come into contact with self-hosting prior to survey

Self-hosters are statistically more likely to

- fall in the age group 48 - 58
- be men

Self-hosters are statistically less likely to

- be older than 58 years
- be woman or non-binary





Findings S1: Usage Patterns



- Web site Hosting is the most frequent use case (51.4%)
- 46% host Wordpress; out of which 47.9% run on home servers



- Use cases Communication, File Storage, Synchronized PW Managing and Smart Home were equally frequent
- S-Hers used more (non-sh) tools in general



- For Smart Home Home Assistant is the most frequent tool (21.5%)
- 25.3% have it accessible via the Internet



Survey 2 (n=589)

Goal:

Understand enabling and constraining individual characteristics relevant to system administration work.

Method:

Compare self-hosters to a demographically matched control group.

Core themes captured by scale measures:

- **Security**
- **Privacy**
- **Technology interest and skills**
- **Openness to new things**
- **Tinkering and DIY**
- **Money**
- **Work effort**
- **Control**



Findings S2: Individual Characteristics

Security

Security concerns with respect to the protection of personal information

Privacy

Concerns regarding the availability of private information on the Internet

Technology interest and skills

Affinity for technology interaction (ATI)
Computer self-efficacy
Hosting skills
IT background

Tinkering and DIY

“Maker” activities

Money

Frugality

Work effort

Grit

Control

Autonomy

Openness to new thing

Personal innovativeness in the domain of information technology (PIIT)



Findings S2: Individual Characteristics

Security

Security concerns with respect to the protection of personal information

Privacy

Concerns regarding the availability of private information on the Internet

Technology interest and skills (+)

Affinity for technology interaction (ATI)

Computer self-efficacy

Hosting skills

IT background

Tinkering and DIY (+)

“Maker” activities

Money

Frugality

Work effort (-)

Grit

Control

Autonomy

Openness to new thing

Personal innovativeness in the domain of information technology (PII)



Challenges for Digital Sovereignty

- While software options exist that enable individuals to be fully digitally sovereign, they are not widely used.
- This might hint at severe usability issues that span the hosting ecosystem including self-hostable software options.

The good news? There is lots to do!



- The problems are human-made. People can solve them.
- It has never been easier to access data than it is today.
- We need to break down existing barriers.

Lea Gröber - lea.groeber@cispa.de - lea418@infosec.exchange