Innovationsverbund
Öffentliche Gesundheit

GEFÖRDERT VOM
Bundesministerium
für Bildung
und Forschung

The CRA - An Activists silver bullet

helping open source and legalizing security research

09.11.2024 - Freedom not Fear

https://inoeg.de gregor.bransky@inoeg.dee https://github.com/InOG-projects

Agenda

- The CRA - What is it about?
- Good news: Open Source Stewards
- Silver Bullets:
  - Mandatory CVD Process mandate legalizing security research
  - Open Source Stewards are a candidate for charitable causes

The CRA What is it about?

- Reducing vulnerabilities in digital products
- Cyber Security maintenance throughout a product’s life cycle
- Empower users to make informed decisions

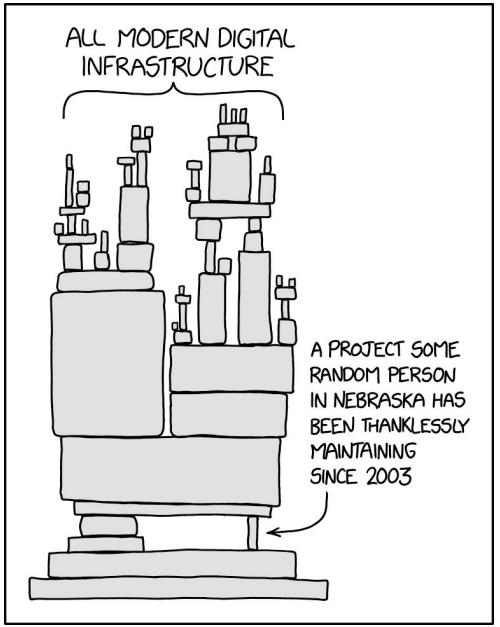
The CRA What is it about? Practically speaking

- Reducing vulnerabilities in digital products
- Cyber Security maintenance throughout a product's life cycle
- Empower users to make informed decisions

It introduces the concept of product liability for all products that include software and the corresponding supply chains.

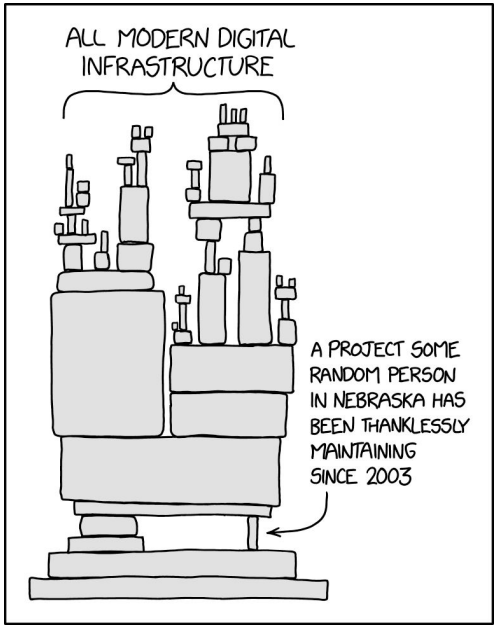
Good news: Open Source stewards

- Product liability along supply chains scared Open Source



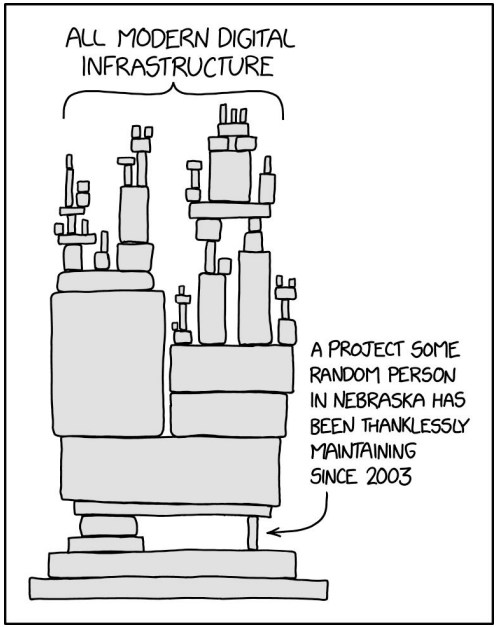
Good news: Open Source stewards

- Product liability along supply chains scared Open Source



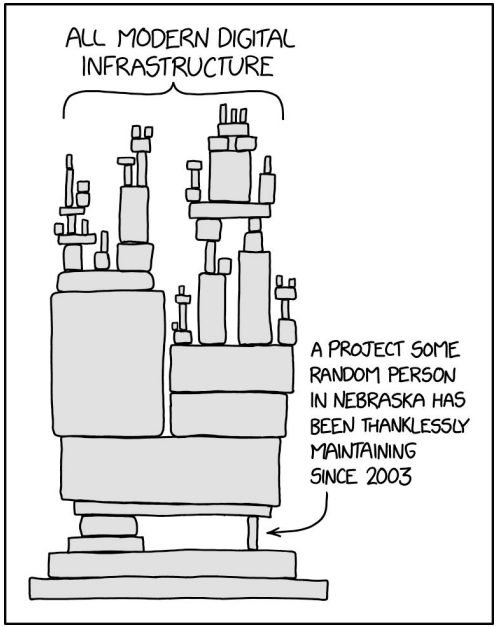
Good news: Open Source stewards

- Product liability along supply chains scared Open Source
- The challenge:
  Regulating Chrome, Safari and Firefox
  without hurting open source.



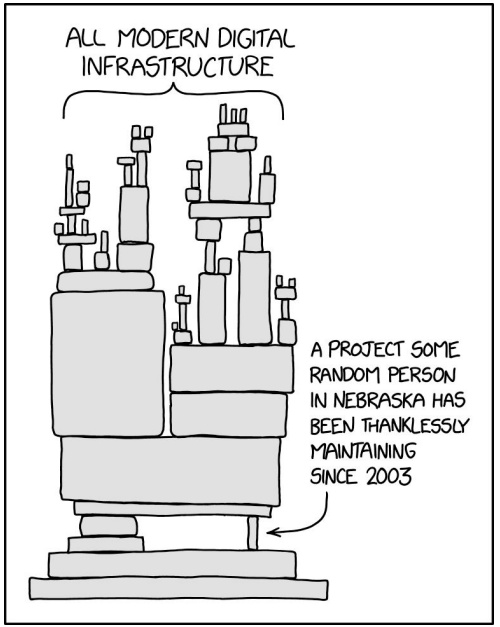
Good news: Open Source stewards

- Product liability along supply chains scared Open Source
- The challenge:
  Regulating Chrome, Safari and Firefox
  without hurting open source.
- The solution:
  Follow the money.



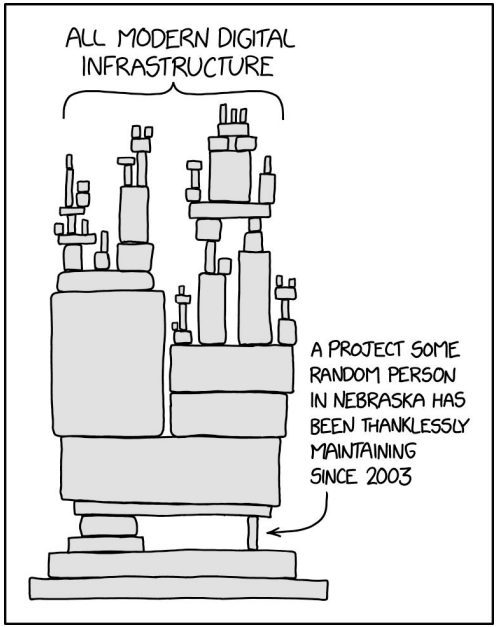
Good news: Open Source stewards

- Product liability along supply chains scared Open Source
- The challenge:
  Regulating Chrome, Safari and Firefox
  without hurting open source.
- The solution:
  Follow the money.

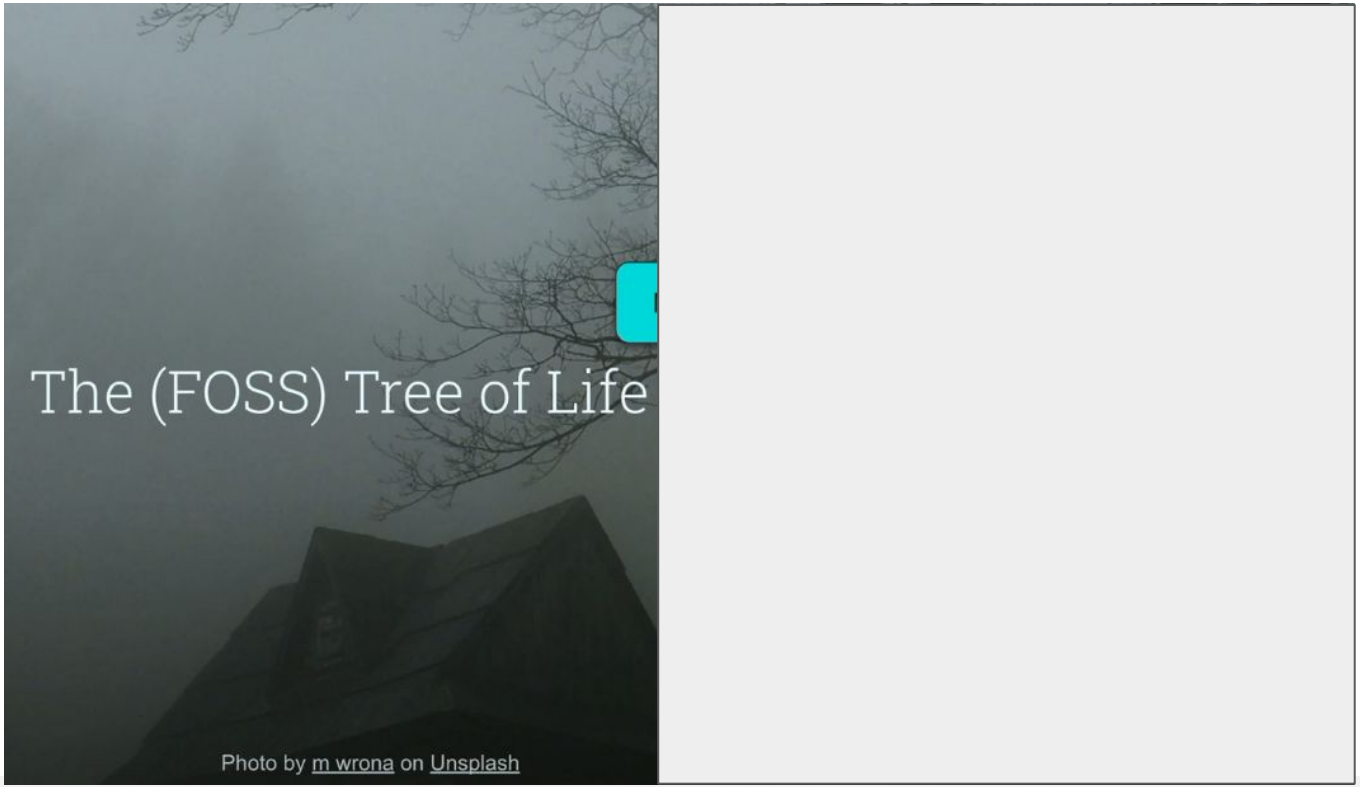


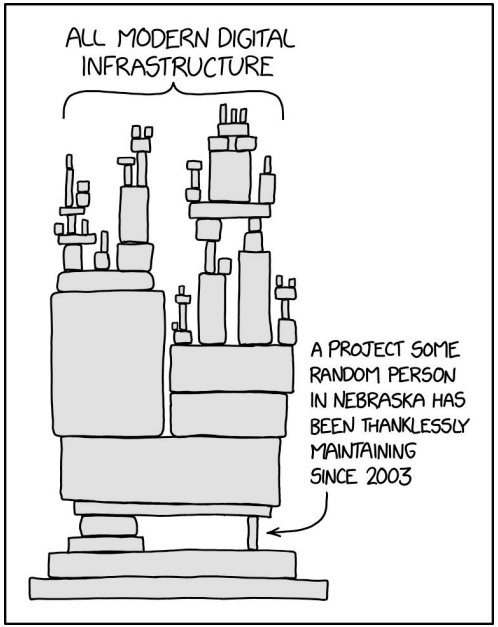
Good news: Open Source stewards

- Product liability along supply chains scared Open Source
- The challenge:
  Regulating Chrome, Safari and Firefox
  without hurting open source.
- The solution:
  Follow the money.
- The fix
  The FOSS Tree of live
  from an organisation perspective

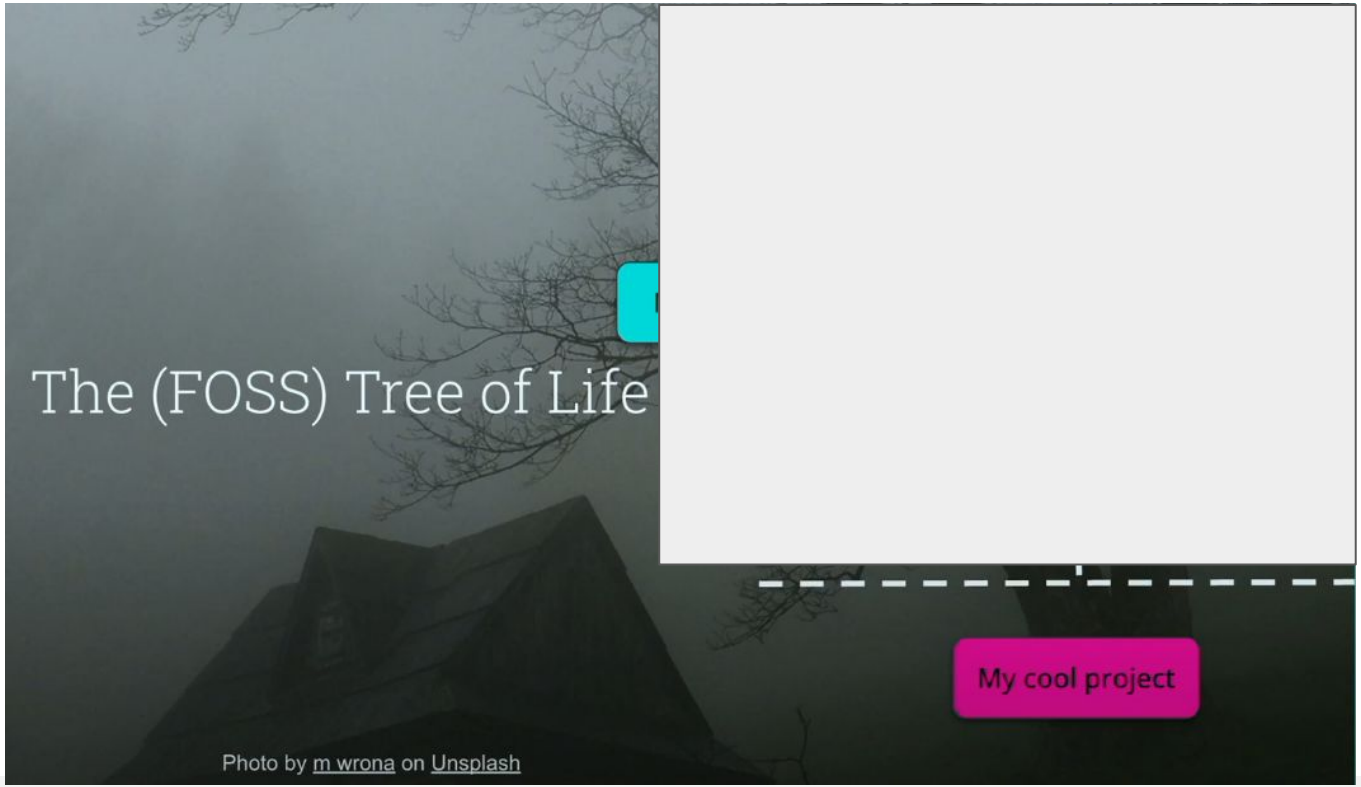


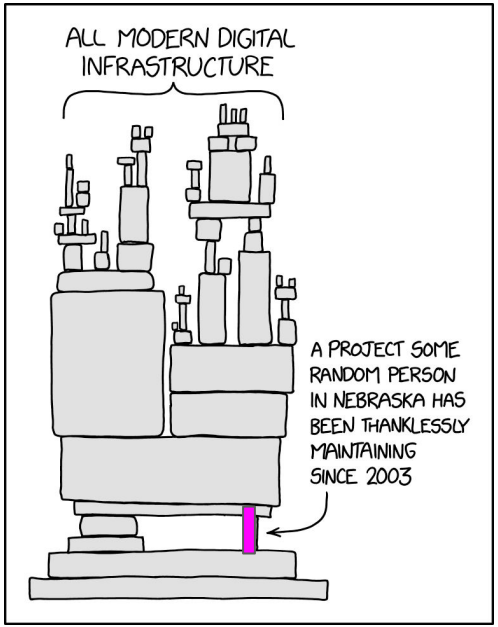
Good news: Open Source stewards - The FOSS Tree of live



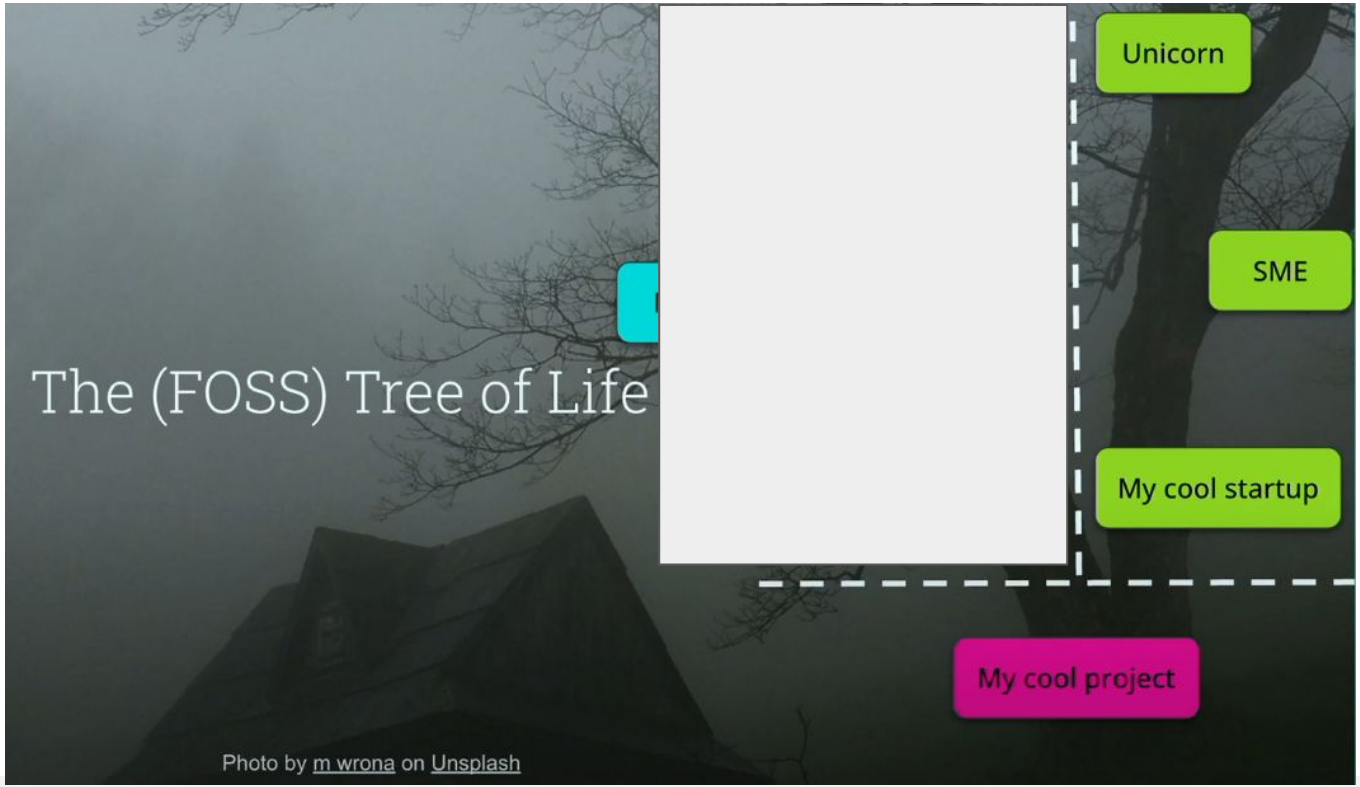


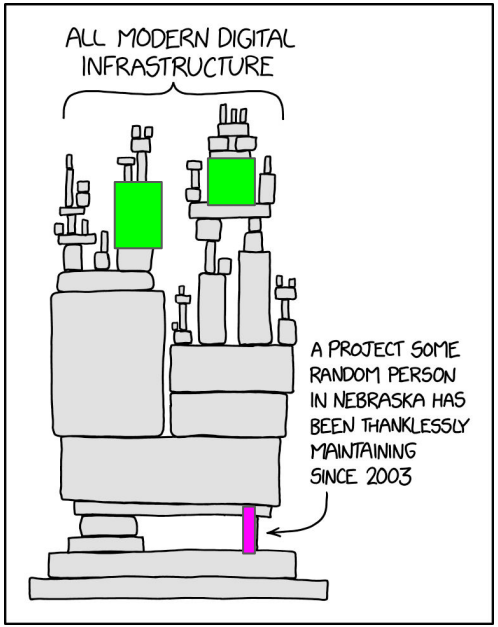
Good news: Open Source stewards - The FOSS Tree of live



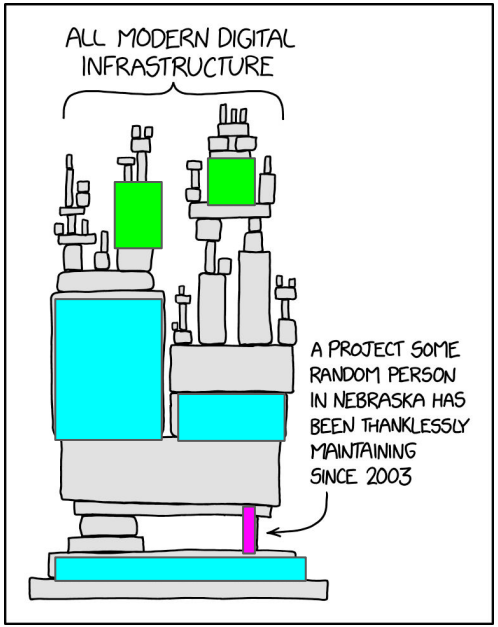


Good news: Open Source stewards - The FOSS Tree of live





Good news: Open Source stewards - The FOSS Tree of live



The CRA defines market actors (12):

Manufacturers (13)

Open Source Stewards (14)

The CRA defines market actors (12):

Manufacturers (13)

- Natural or legal persons
- Develops or manufacture Products with digital elements
- Markets them for:
  - Payment
  - Monetisation
  - Free of charge

Open Source Stewards (14)

The CRA defines market actors (12):

Manufacturers (13)

- Natural or legal persons
- Develops or manufacture
  Products with digital elements
- Markets them for:
  - Payment
  - Monetisation
  - Free of charge

Open Source Stewards (14)

The CRA defines market actors:

Manufacturers (13)

- Natural or legal persons
- Develops or manufacture
  Products with digital elements
- Markets them for:
  - Payment
  - Monetisation
  - Free of charge

Open Source Stewards (14)

The CRA defines market actors:

Manufacturers (13)

- Natural or legal persons
- Develops or manufacture
  Products with digital elements
- Markets them for:
  - Payment
  - Monetisation
  - Free of charge

Open Source Stewards (14)

- Natural or legal persons
  Other than a manufacturer
- Systematically provide support
  Free and open source software
- Markets them for:
  - Payment
  - Monetisation
  - Free of charge

The CRA defines market actors:

Manufacturers (13)

- Natural or legal persons
- Develops or manufacture
  Products with digital elements
- Markets them for:
  - Payment
  - Monetisation
  - Free of charge

Open Source Stewards (14)

- Natural or legal persons
  Other than a manufacturer
- Systematically provide support
  Free and open source software
- Markets them for:
  - Payment
  - Monetisation
  - Free of charge

The CRA defines market actors:

Manufacturers (13)

- Natural or legal persons
- Develops or manufacture
  Products with digital elements
- Markets them for:
  - Payment
  - Monetisation
  - Free of charge

Open Source Stewards (14)

- Natural or legal persons
  Other than a manufacturer
- Systematically provide support
  Free and open source software
- Markets them for:
  - ~~Payment~~
  - ~~Monetisation~~
  - Free of charge

The CRA defines market actors: Obligations

Manufacturers (13)

Open Source Stewards (14)

The CRA defines market actors: Obligations

Manufacturers (13)

- All of the CRA

- Offer a CVD Process (77)
- Check the FOSS used in your product
- Collaborate with stewards

Open Source Stewards (14)

- place and document in a verifiable manner a cybersecurity policy
- cooperate with the market surveillance authorities
- Report vulnerabilities they become aware of to CSIRT & ENISA (Cyber Security Agencys)

The CRA defines market actors: Obligations

Manufacturers (13)

- All of the CRA

- Offer a CVD Process (77)
- Check the FOSS used in your product
- Collaborate with stewards

Open Source Stewards (14)

The CRA defines market actors: Obligations

Manufacturers (13)

- All of the CRA

- Offer a CVD Process (77)
- Check the FOSS used in your product
- Collaborate with stewards

Open Source Stewards (14)

- place and document in a verifiable manner a cybersecurity policy
- cooperate with the market surveillance authorities
- Report vulnerabilities they become aware of to CSIRT & ENISA (Cyber Security Agencys)

Good news: Open Source stewards

The EUC squared the circle:

They basically modeled an exemption for the liability of organisations based on the business model of open source foundations.

Silver Bullets - Legalizing Security Research

- Given that every digital product is mandated to have a CVD process security research will have to be legalized to a certain extend in the EU

Silver Bullets - Legalizing Security Research

- Given that every digital product is mandated to have a CVD process security research will have to be legalized to a certain extend in the EU

I hacked the dutch government and all I got was this lousy shirt …

Silver Bullets - Legalizing Security Research

- Given that every digital product is mandated to have a CVD process security research will have to be legalized to a certain extend in the EU

I hacked the dutch government and all I got was this lousy shirt …

Silver Bullets - Legalizing Security Research

- Given that every digital product is mandated to have a CVD process security research will have to be legalized to a certain extend in the EU

- Questions regarding legal standing of security researchers
  - will lead to less reporting,
    - this becomes a problem for the manufacturer,
      every reported vulnerability is potentially a not exploited vulnerability [3]

Silver Bullets - Legalizing Security Research

- Given that every digital product is mandated to have a CVD process security research will have to be legalized to a certain extend in the EU

- Questions regarding legal standing of security researchers
  - will lead to less reporting,
    - this becomes a problem for the manufacturer,
      every reported vulnerability is potentially a not exploited vulnerability [3]

- There is a ton of other arguments but **EU law > national law**

Silver Bullets - FOSS for good

- So far most FOSS Projects have either:

Silver Bullets - FOSS for good

- So far most FOSS Projects have either:
  - No legal entity

Silver Bullets - FOSS for good

- So far most FOSS Projects have either:
  - No legal entity
  - Are 501 (c) 3´s [4][5] - Mozilla, Ruby, Haskel, Python, …

Silver Bullets - FOSS for good

- So far most FOSS Projects have either:
  - No legal entity
  - Are 501 (c) 3´s [4][5] - Mozilla, Ruby, Haskel, Python, …
  - Are 501 (c) 6´s [4][5] - Linux Foundation, Open Source Collective, etc.

Silver Bullets - FOSS for good

- So far most FOSS Projects have either:
  - No legal entity
  - Are 501 (c) 3´s [4][5] - Mozilla, Ruby, Haskel, Python, …
  - Are 501 (c) 6´s [4][5] - Linux Foundation, Open Source Collective, etc.
- Open Source stewards have to set-up cybersecurity policies
  The implementation costs money

Silver Bullets - FOSS for good

- So far most FOSS Projects have either:
  - No legal entity
  - Are 501 (c) 3´s [4][5] - Mozilla, Ruby, Haskel, Python, …
  - Are 501 (c) 6´s [4][5] - Linux Foundation, Open Source Collective, etc.
- Open Source stewards have to set-up cybersecurity policies
  The implementation costs money
- Manufacturers have to collaborate with them but can not have business relations

Silver Bullets - FOSS for good

- So far most FOSS Projects have either:
  - No legal entity
  - Are 501 (c) 3´s [4][5] - Mozilla, Ruby, Haskel, Python, …
  - Are 501 (c) 6´s [4][5] - Linux Foundation, Open Source Collective, etc.
- Open Source stewards have to set-up cybersecurity policies:
  The implementation costs money
- Manufacturers have to collaborate with them but can not have business relations, so what to do?

Silver Bullets - FOSS for good - tax code to the rescue?

- Manufacturers can not just give money out for free, they need assurances

Silver Bullets - FOSS for good - tax code to the rescue?

- Manufacturers can not just give money out for free, they need assurances
  - Normal way: Have a contract
    -> Not possible under CRA with stewards
  - Donate money:
    -> possible for charitable causes

Silver Bullets - FOSS for good - tax code to the rescue?

- Manufacturers can not just give money out for free, they need assurances
  - Normal way: Have a contract
    -> Not possible under CRA with stewards
  - Donate money:
    -> possible for charitable causes
    -> allows to report to the tax authority

Silver Bullets - FOSS for good - tax code to the rescue?

- Manufacturers can not just give money out for free, they need assurances
  - Normal way: Have a contract
    -> Not possible under CRA with stewards
  - Donate money:
    -> possible for charitable causes
    -> allows to report to the tax authority
- US tax code more favourable than EU tax code
  - The CRA might become an Open Source tax payed to the 501 (c)s in the US

Silver Bullets - FOSS for good - tax code to the rescue?!

- If we do not want the EU Economy to pay a:
    - Digital Infrastructure tax next to the
    - Microsoft tex
    - Hyperscaler tay

    Maybe allow open-source stewardship to become recognized as a charitable cause.

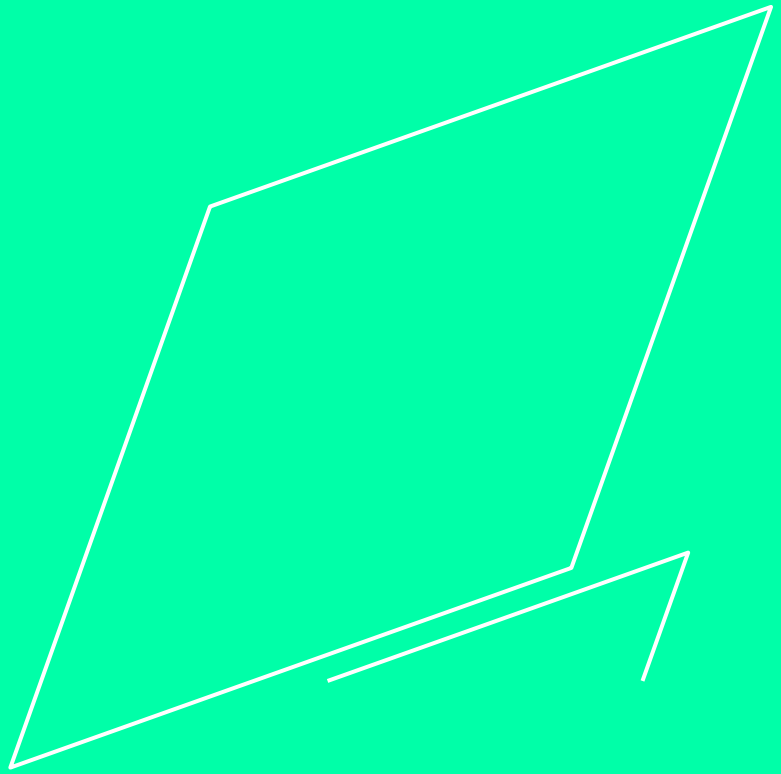
I would love to hear from you:

- Survey: Cyber security research
  Is cyber security research legal in your country?
  - If so, to which degree?
  - If not, what is the punishment?
- Survey: Is FOSS recognized to contribute to the greater good?
  Is the development and maintenance of FOSS recognized as a charitable cause in your tax-code?

Sources

[1] https://program.foss-backstage.de/fossback24/talk/SVRP9E/
[2] https://av.tib.eu/media/67124
[3] https://program.foss-backstage.de/fossback23/talk/KEMRGG/
[4] https://program.foss-backstage.de/fossback24/talk/WNHFDT/
[5] https://shaneslides.com/fossbackstage/WhoFundsFOSSFoundations-FOSSBackstage2024#1

Ich freue mich auf die Diskussion.



Wtf … is the InÖG? A child of the pandemic

- March 2020
  Part of the #wirvsvirus Hackathon of the german government

Wtf … is the InÖG? A child of the pandemic

#WIRVSVIRUS
DER HACKATHON DER BUNDESREGIERUNG

- March 2020
  Part of the #wirvsvirus Hackathon of the german government
  - digitales Wartezimmer - DataDump for public health centers

Wtf … is the InÖG? A child of the pandemic

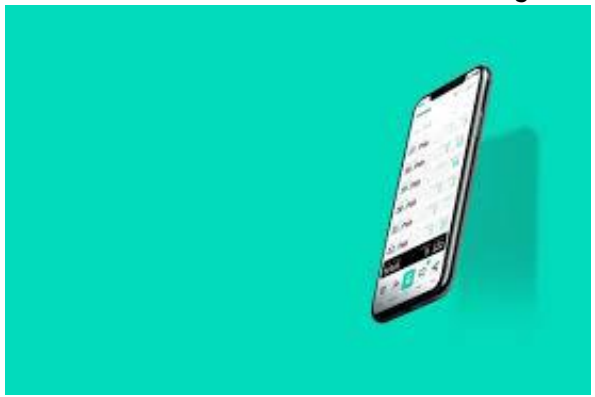
#WIRVSVIRUS
DER HACKATHON DER BUNDESREGIERUNG

- March 2020
  Part of the #wirvsvirus Hackathon of the german government
  - digitales Wartezimmer - DataDump for public health centers
  - LabHive - Resource sharing platform for lab equipment

Wtf … is the InÖG? A child of the pandemic

#WIRVSVIRUS
DER HACKATHON DER BUNDESREGIERUNG

- March 2020
  Part of the #wirvsvirus Hackathon of the german government
  - digitales Wartezimmer - DataDump for public health centers
  - LabHive - Resource sharing platform for lab equipment
  - Coronika - a contact diary



Wtf … ist der InÖG? A child of the pandemic

#WIRVSVIRUS
DER HACKATHON DER BUNDESREGIERUNG

- März 2020
  Part of the #wirvsvirus Hackathon of the german government

- September 2020
  Innovationsverbund Öffentliche Gesundheit
  #wivsvirus becomes #wirvsbleistift (us vs. pencils)

Innovationsverbund
Öffentliche Gesundheit

Wtf … ist der InÖG? A child of the pandemic

- März 2020
  Part of the #wirvsvirus Hackathon of the german government

- September 2020
  Start
  Innovationsverbund Öffentliche Gesundheit

- März 2021 - IRIS connect
  IRIS-connect, a civil society response to the luca app

IRIS connect

initiiert von

gefördert durch

Wtf … ist der InÖG? A child of the pandemic

- März 2020
  Part of the #wirvsvirus Hackathon of the german government

- September 2020
  Start
  Innovationsverbund Öffentliche Gesundheit

- März 2021 - IRIS connect
  IRIS-connect, a civil society response to the luca app

- October 2021 - Impftermin
  When the vaccination looks for you!

Wtf … ist der InÖG? A child of the pandemic

#WIRVSVIRUS
DER HACKATHON DER BUNDESREGIERUNG

- März 2020
  Ursprung ist der #wirvsvirus Hackathon der Bundesregierung

- September 2020
  Zusammenschluss
  Innovationsverbund Öffentliche Gesundheit

Innovationsverbund Öffentliche Gesundheit

- März 2021
  IRIS-connect, die
  Zivilgesellschaftliche Antwort auf die Luca-App

IRIS connect

initiiert von Innovationsverbund Öffentliche Gesundheit

gefördert durch Björn Steiger Stiftung
WIR HELFEN LEBEN RETTEN

- Oktober 2021 - Impftermin
  Dein Impftermin bucht dich!

What does the InÖG do? NGO, Tech & Forschung

- NGO Founding - 24.02.2022

Was macht der InÖG? Vereinsmeierei, Tech & Forschung

- Vereinsgründung - 24.02.2022
- Gemeinnützigkeit - demnächst_TM
- Forschung mit der TU München
  - Bachelorarbeit
    "Wie kann am Beispiel des ÖGDs das Konzept des Crowdsou
    in der öffentlichen Verwaltung etabliert werden?"
  - Masterarbeit
    "Prozessanalyse der deutschen Gesundheitsämter"

Was macht der InÖG? Vereinsmeierei, Forschung & Tech

- Vereinsgründung - 24.02.2022
- Gemeinnützigkeit - demnächst_TM
- Forschung mit der TU München
- Signierte Container - Sommer 2023

Wie arbeitet der InÖG?

Innovationsverbund Öffentliche Gesundheit

Initiiert vom Innovationsverbund Öffentliche Gesundheit (InÖG) e.V.

- Impuls aus der Zivilgesellschaft
- Menschen stellen ihre Fachexpertise zur Verfügung
- arbeitet ehrenamtlich als Verein mit ähnlichem Verständnis wie THW, Samariter, DRK oder Malteser

Björn Steiger Stiftung
WIR HELFEN LEBEN RETTEN

Finanziert und gefördert durch u.a. die Björn Steiger Stiftung

- stellt Produktstruktur zur Verfügung, koordiniert Dienstleister für
- geregelten Verfahrensbetrieb und
- ist direkter Vertragspartner für die Öffentliche Hand

Kostenlos nutzbar für die Öffentliche Hand

- Softwareprodukte sind Open Source und werden der Öffentlichen Hand unentgeltlich bereitgestellt
- Digitalisierung wird vorangetrieben

digitale Agilität

Struktur