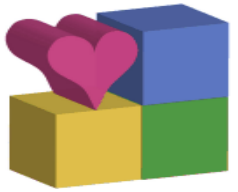


Ohjelmistohaavoittuvuudet käytännössä

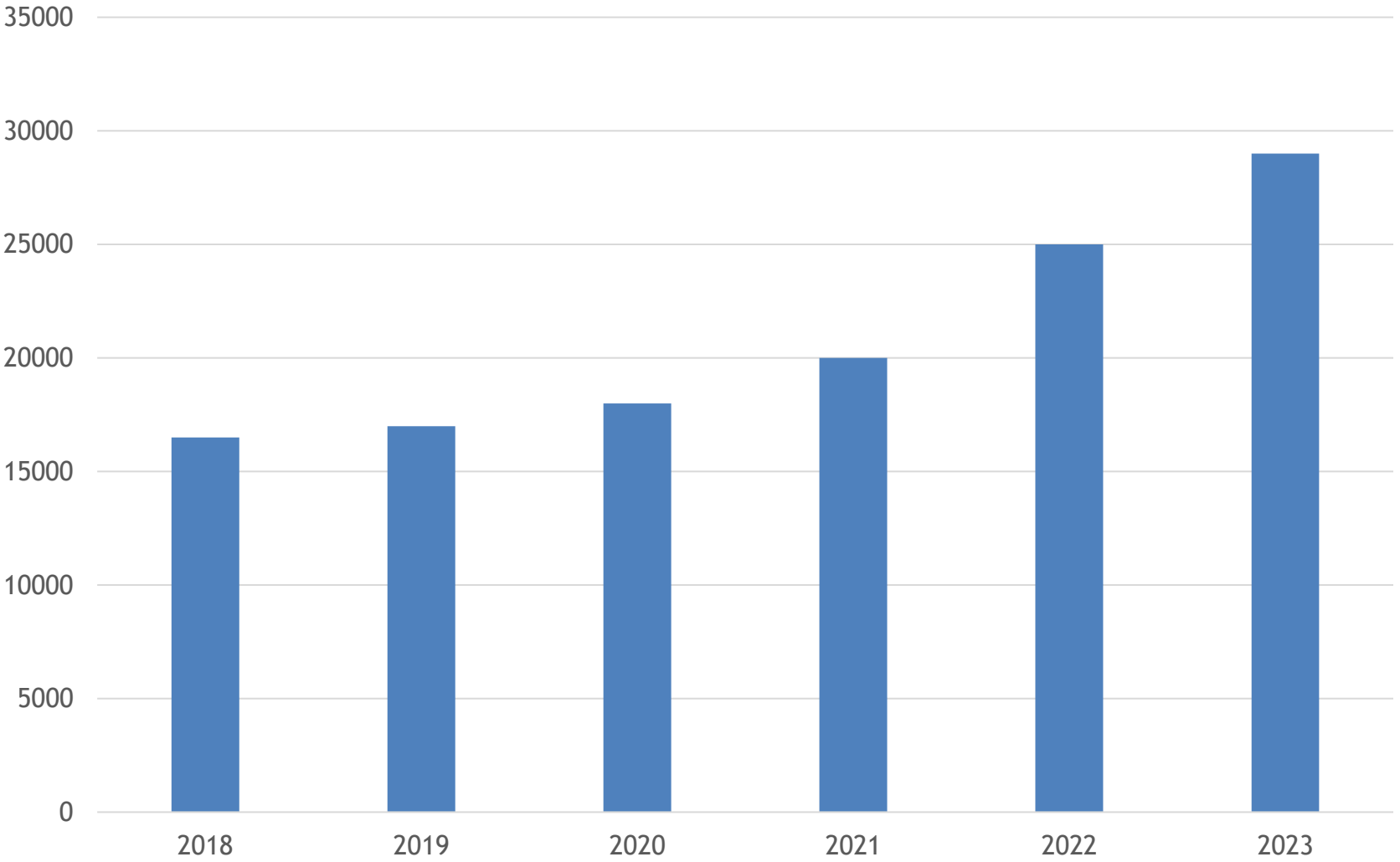
Lea Viljanen
LAV Security Oy / Hackrfi Oy
23.1.2024



Credits: Runa Sandvik & Michael Auger

Hack credits: Werling, Kuhnapfel, Jacob, Drokin / TU Berlin, Photo credits: Tesla

Credits: Nozomi Networks


NIST haavoittuvuustilasto
35000
30000
25000
20000
15000
10000
5000
0
2018
2019
2020
2021
2022
2023

5 Years of Microsoft Bounty Programs

July 01,2018 to June 30, 2023

$58.9M

in bounty rewards

22

Bounty programs

5,446

Eligible vulnerability reports

1,117

Researchers awarded

$200K

Biggest reward

"Since 2019, Zoom has worked with 900 hackers, of which 300 have submitted vulnerabilities that we have had to quickly move on. We've paid out over $7 million. It's a substantial investment but the returns are worth it: we find world-class talent to find real-world solutions before it's a real-world problem."

Michael Adams, CISO, Zoom

zoom

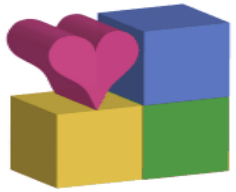
Here are some highlights from February 2022 to February 2023:

- Awarded $1,576,364 in bounties for 364 vulnerabilities, bringing us to $3,839,287 in total rewards via HackerOne since 2016.

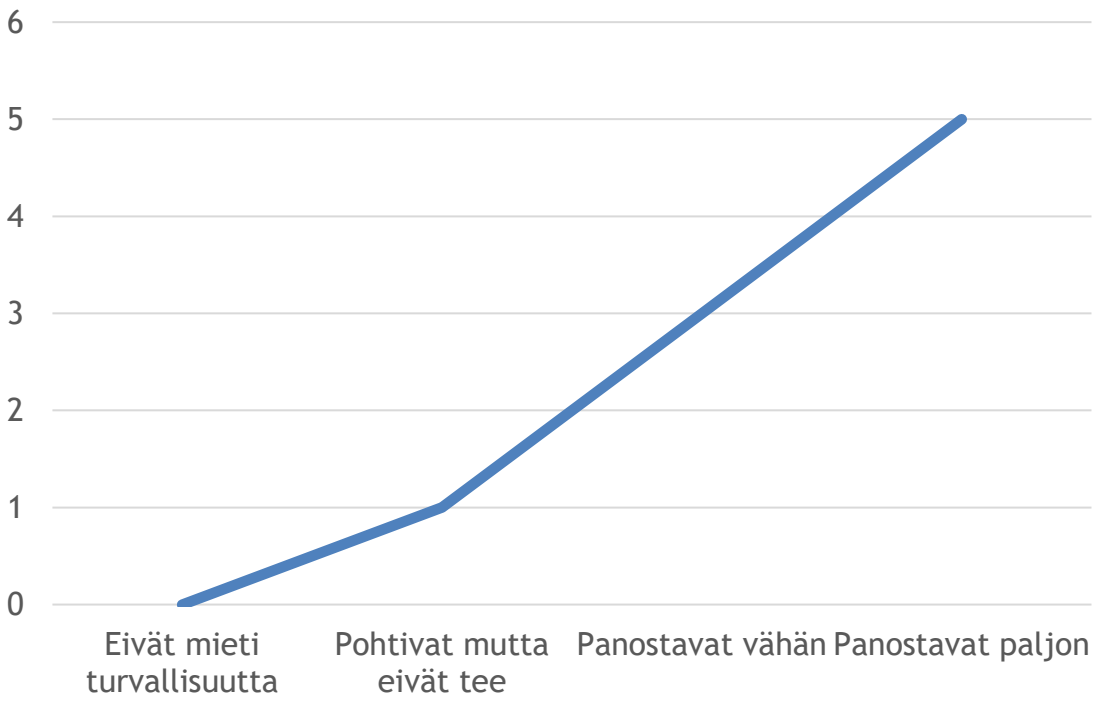
HACKRFI **palkkioita maksettu 170 000 €**

Credits: KC Green -- https://gunshowcomic.com/648

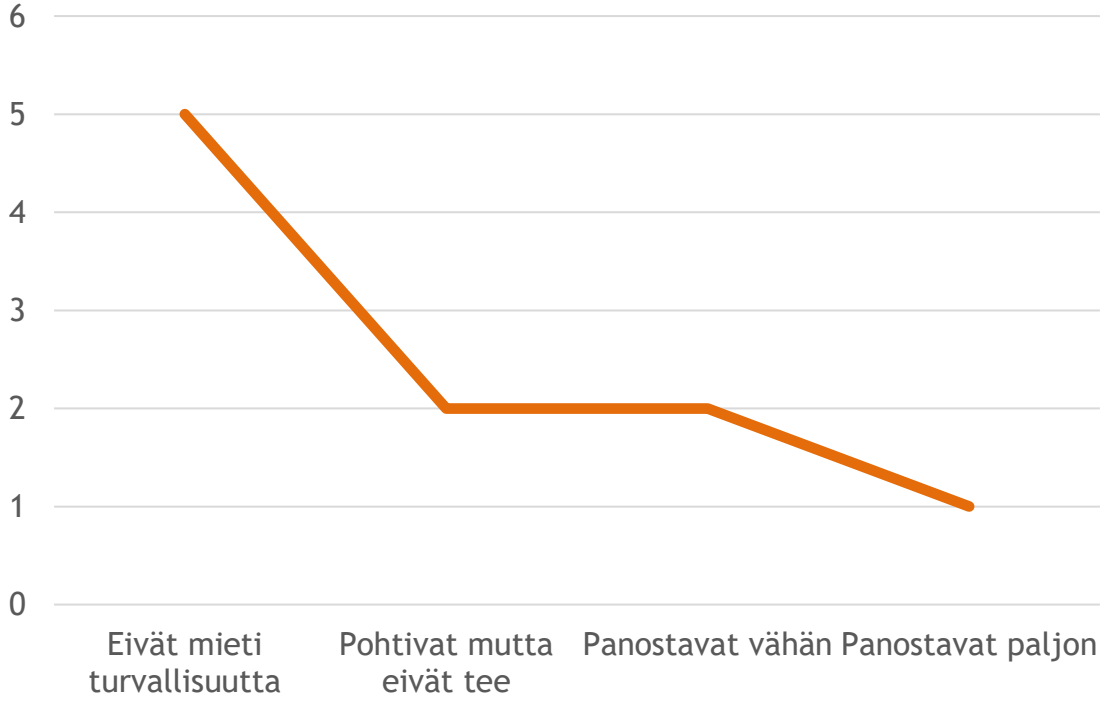
Organisaatioiden tietoturvakypsyys?



Minun kuplani

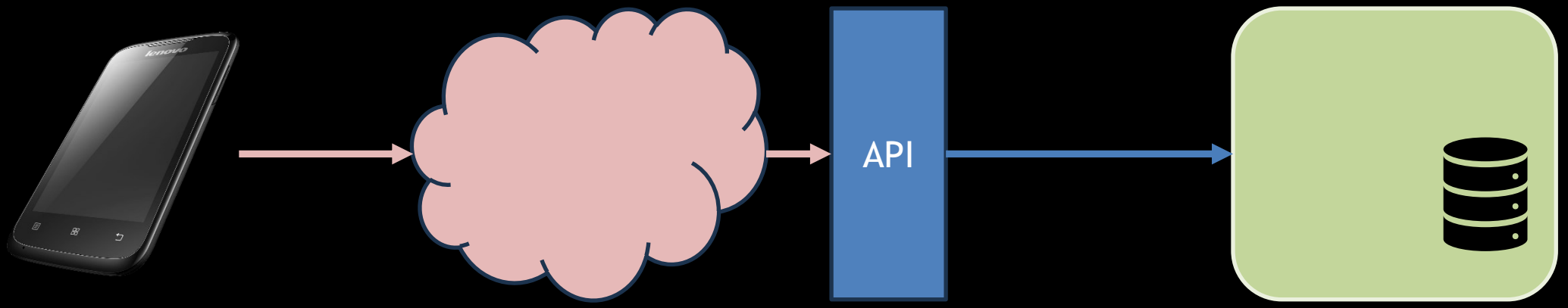


Todellisuus?



Jos se on saavutettavissa, sitä hakkeroidaan.

Rajapinnat!



GET /api/users/123456

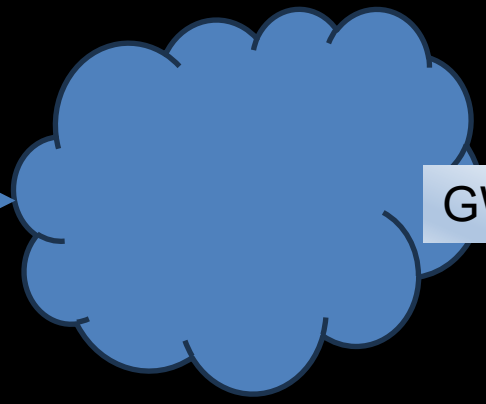
Tietojen keräys!

Suorituskyky!

HTTP/2 200 OK

{“etunimi”: “Lea”, … }

Integraatiot!



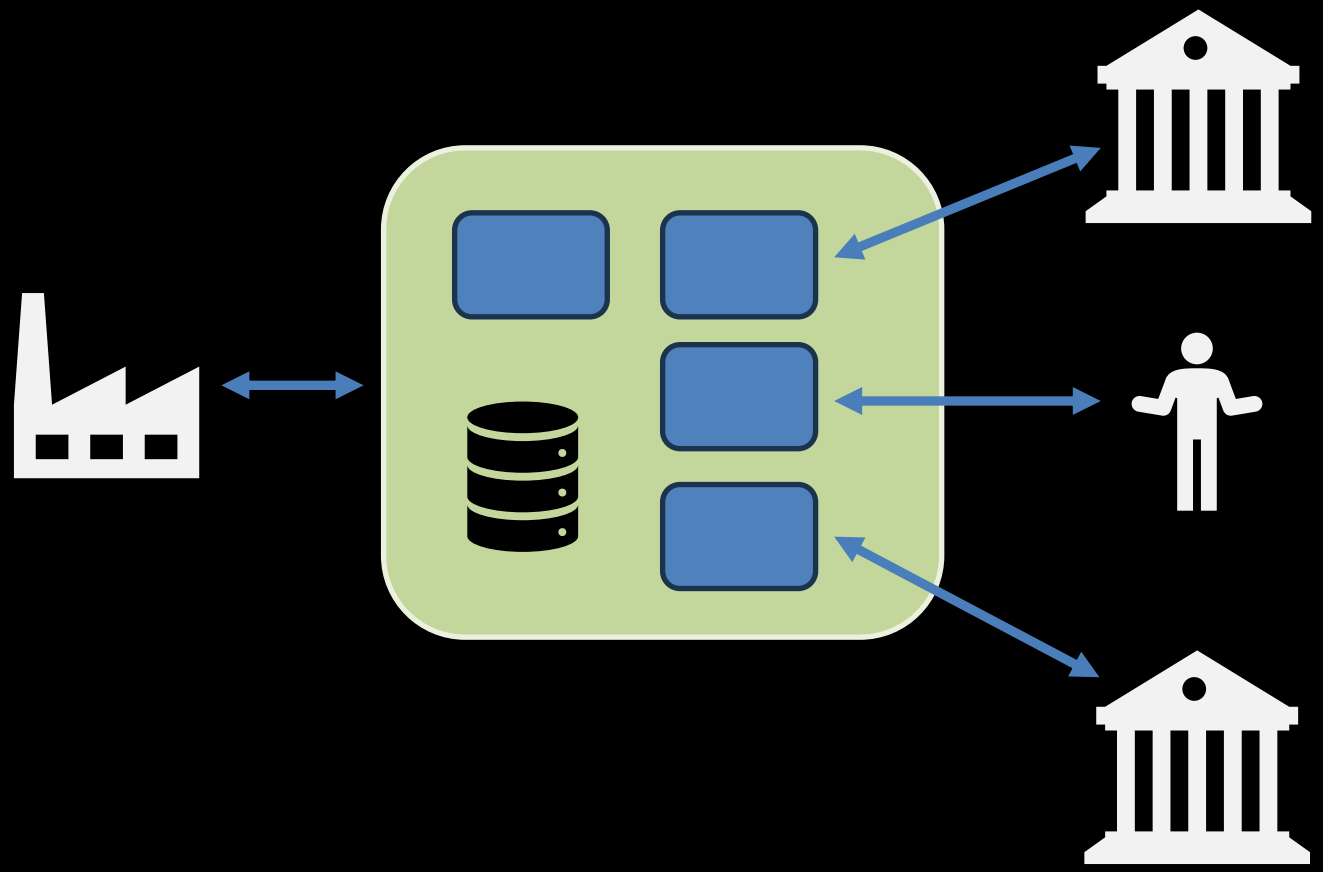
GW

HTTP

POST …
X-From: +358123123
X-From: +358777777
kenelle=999999&min=123

Kenelle: 999999
Minuutteja: 123
\nX-From: +358777777

Alihankintaketjut!



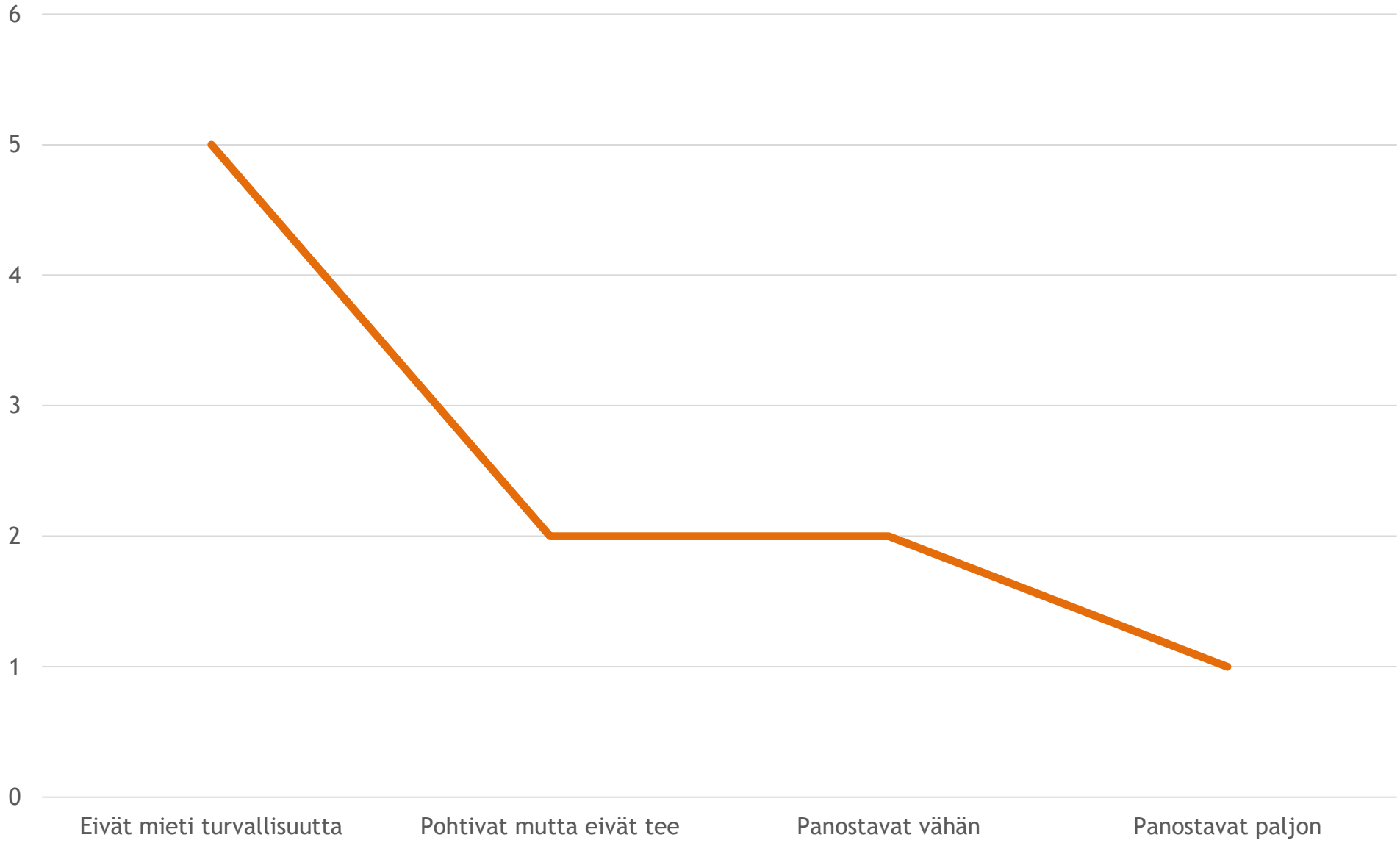
Ohjelmistokomponentit

Tietojen kalastelu
Kotikoneen haavat

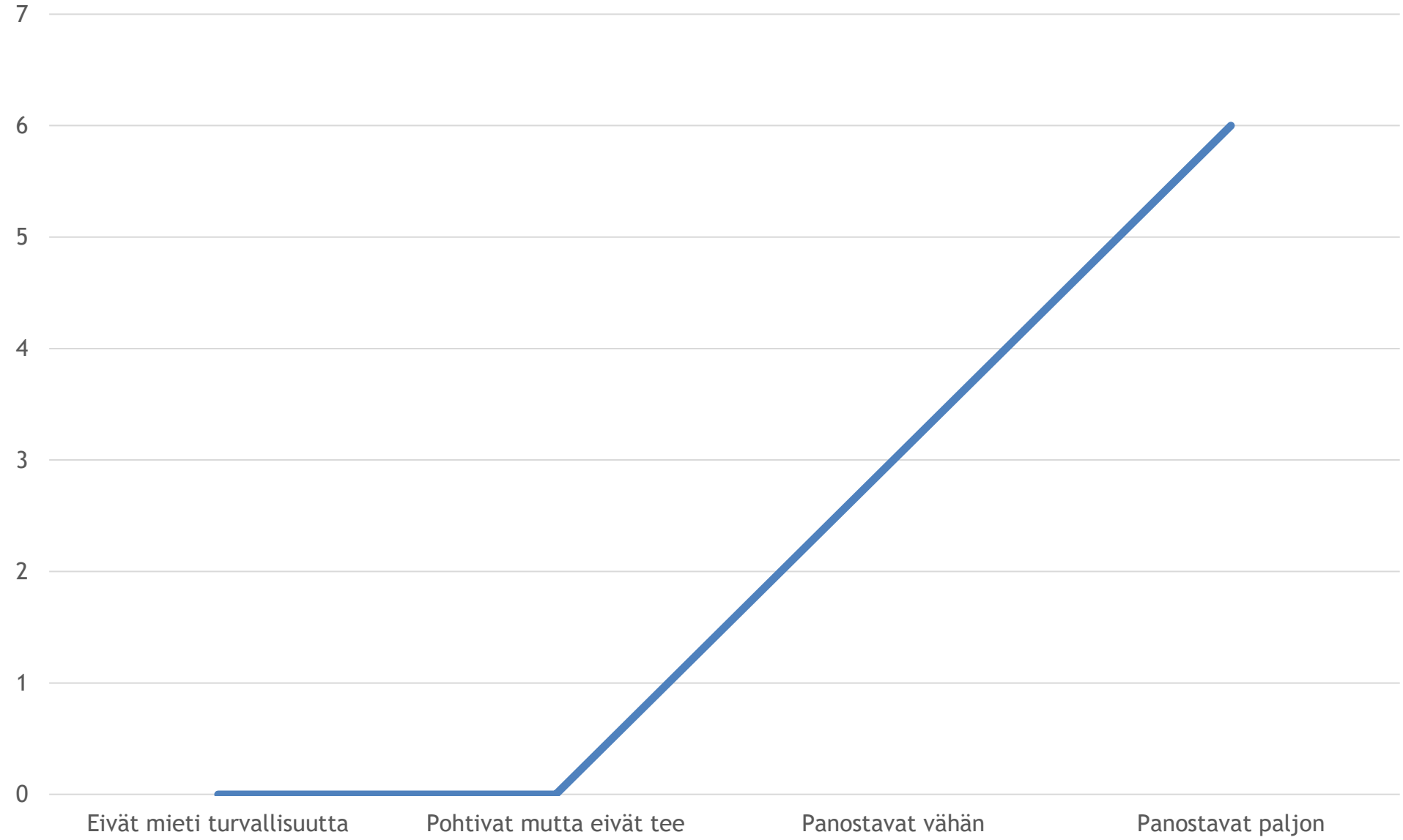
Etäyhteysohjelmat
Palvelutoimittajat

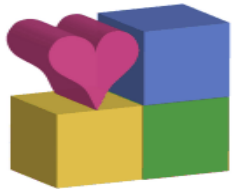
Organisaatio on niin turvallinen kuin alihankintaketjun heikoin lenkki.

Regulaation lähtötila

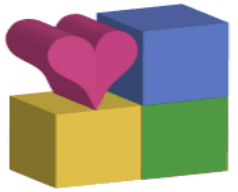


Regulaation tavoite





Älä ole ketjun heikoin lenkki!



Kiitos!