GOPAS

Proč ransomware funguje neboli proč antivirus nefunguje

Ing. Ondřej Ševeček | GOPAS a.s. |
ondrej@sevecek.com | www.sevecek.com |

O čem to je?

GOPAS

Co je ransomware?

- vnitřní infekce (malware) počítačové sítě
- která se sama po síti šíří
- a ničí to data

Supr byznys

- vývar XY 000 000 alespoň od některých zákazníků
- příprava malware - dny
- část poloautomaticky - 0 práce
- zbytek ručně - dny

GOPAS

Šíření

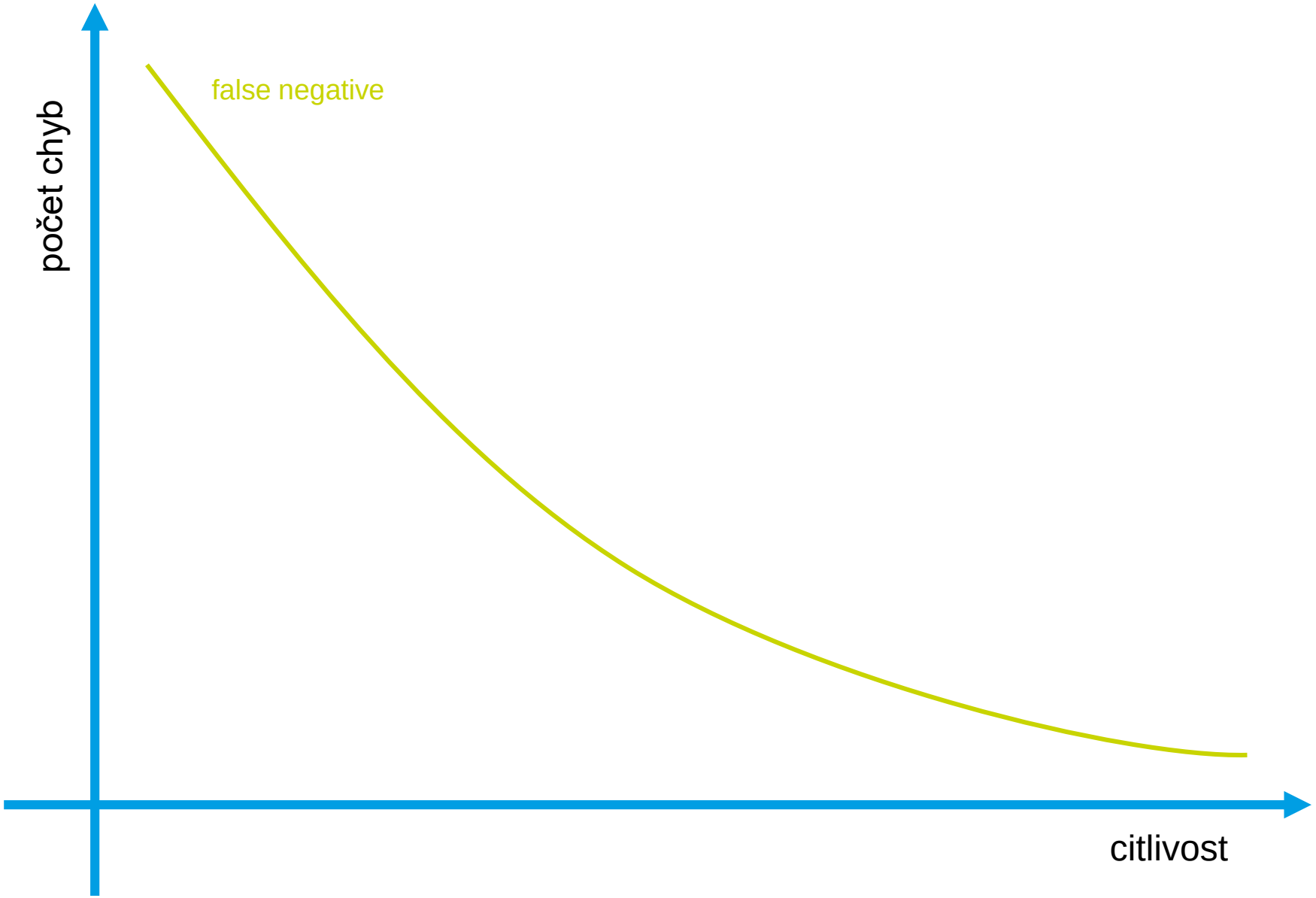
- z internetu do RDP
  - zkoušení hesel
- z internetu do VPN s heslem
  - zkoušení hesel
- z internetu přes exploit?
- social engineeringem rovnou na stanici
  - spam, SEO
  - idiot si to chce stáhnout
  - omylem kliknete
  - exploit v prohlížeči nebo emailovém klientovi

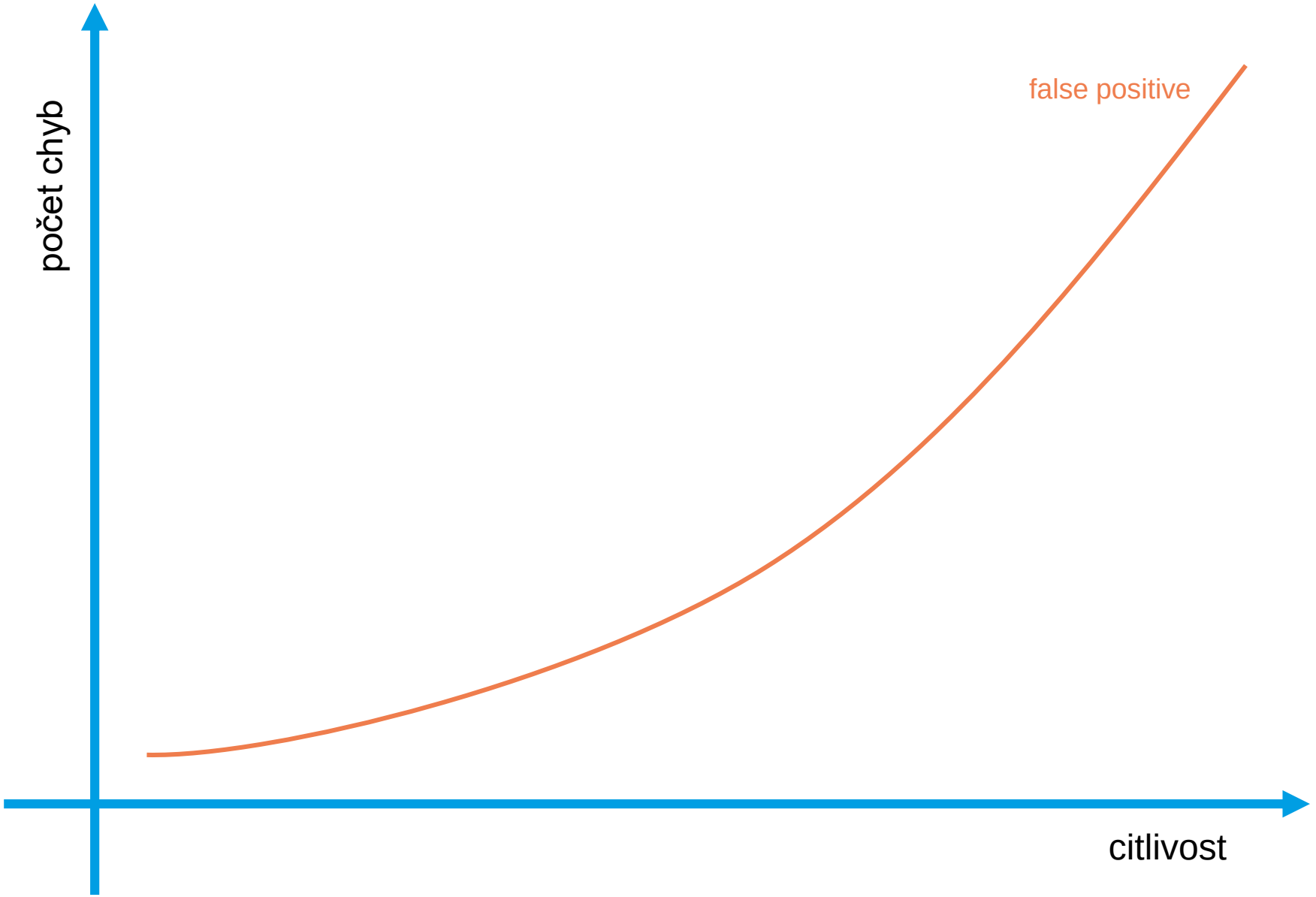
Ochrání mě antivirus?

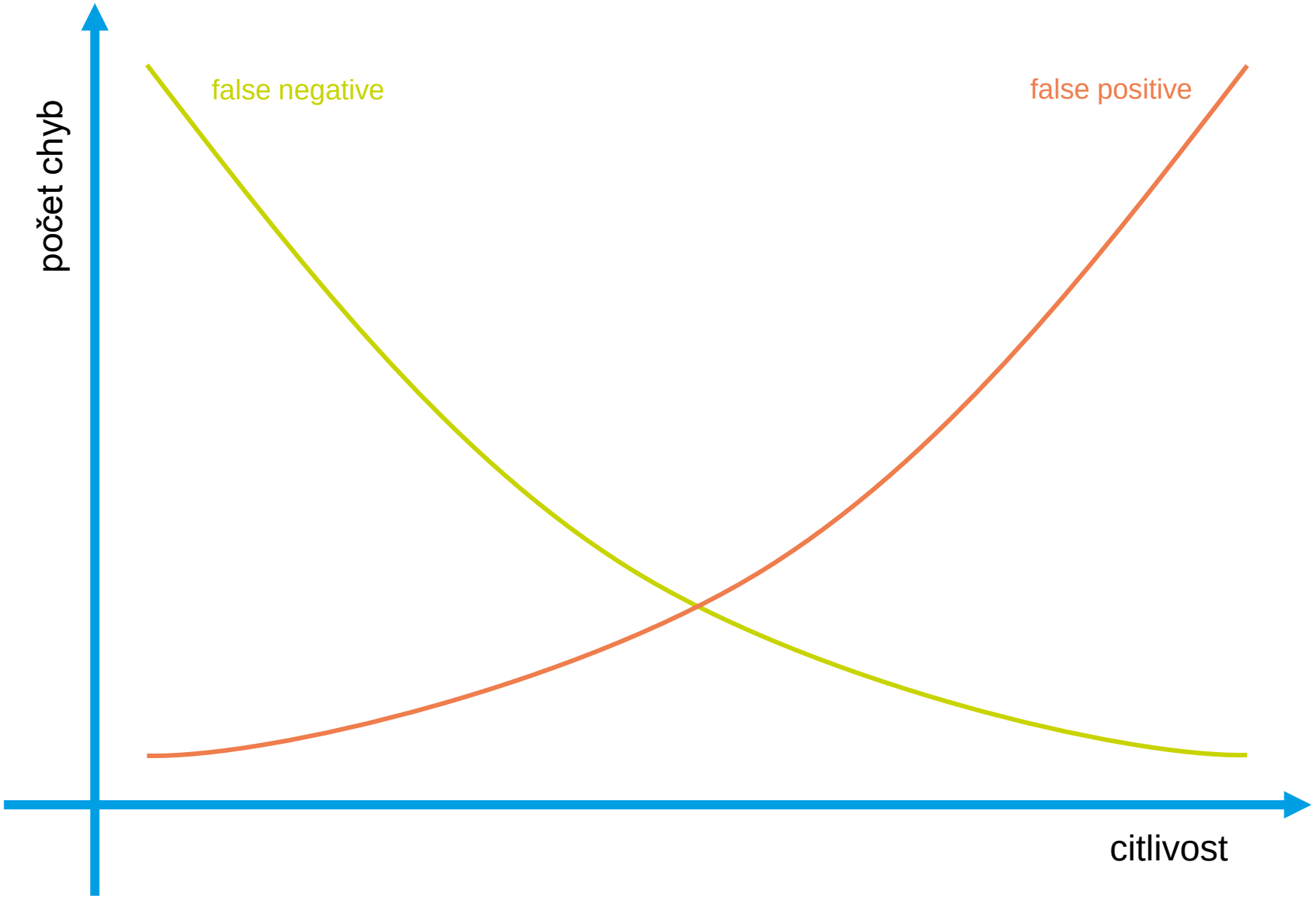
- známé infekce
  - prostá signatura
- vektor průniku
- masivní výskyt
  - cloudové služby

- je to vždycky jen detekční systém
  - false positive
  - false negative

GOPAS


počet chyb
false negative
citlivost


počet chyb
false positive
citlivost



GOPAS

Jak se opravdu chránit?

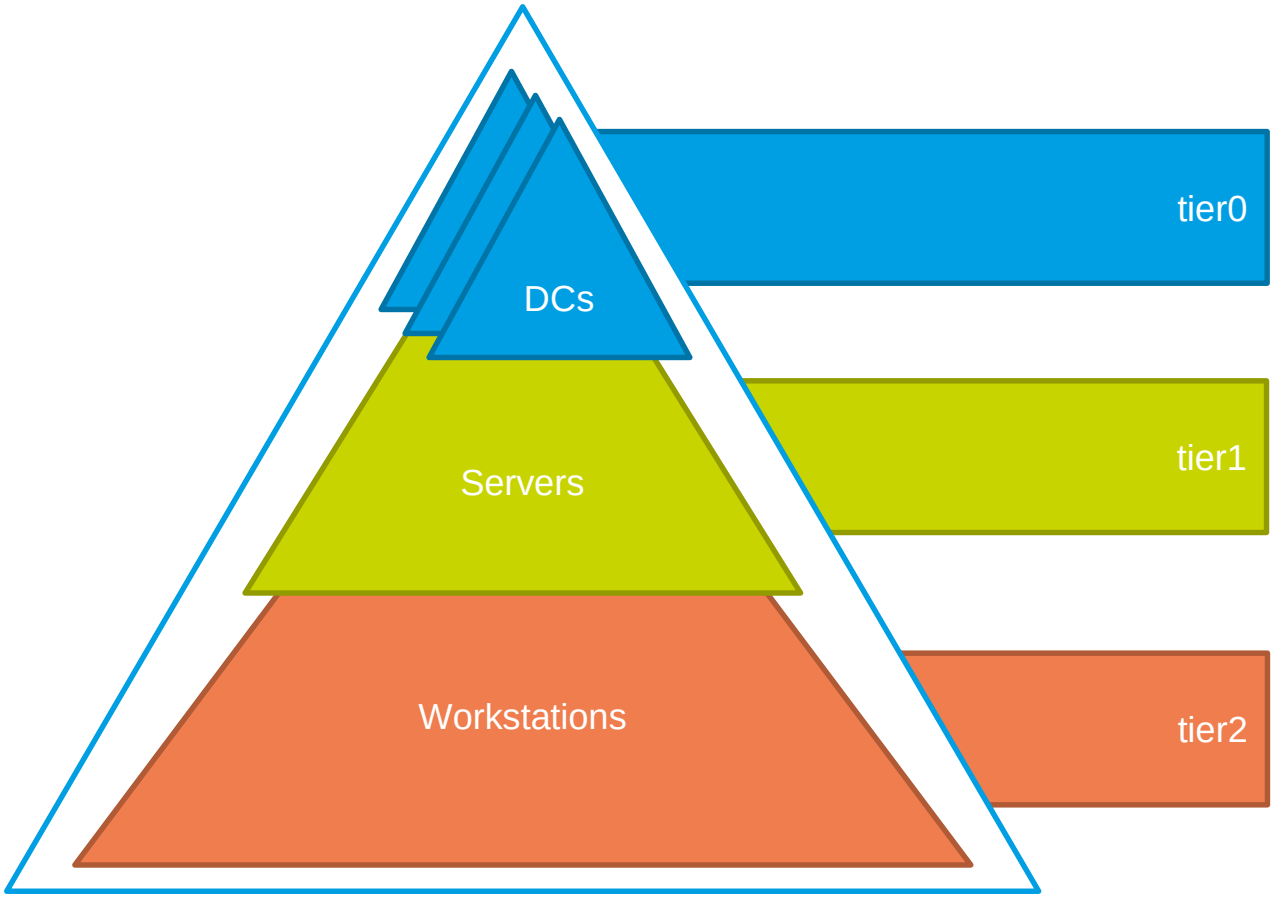
GOPAS

SAE a tiering

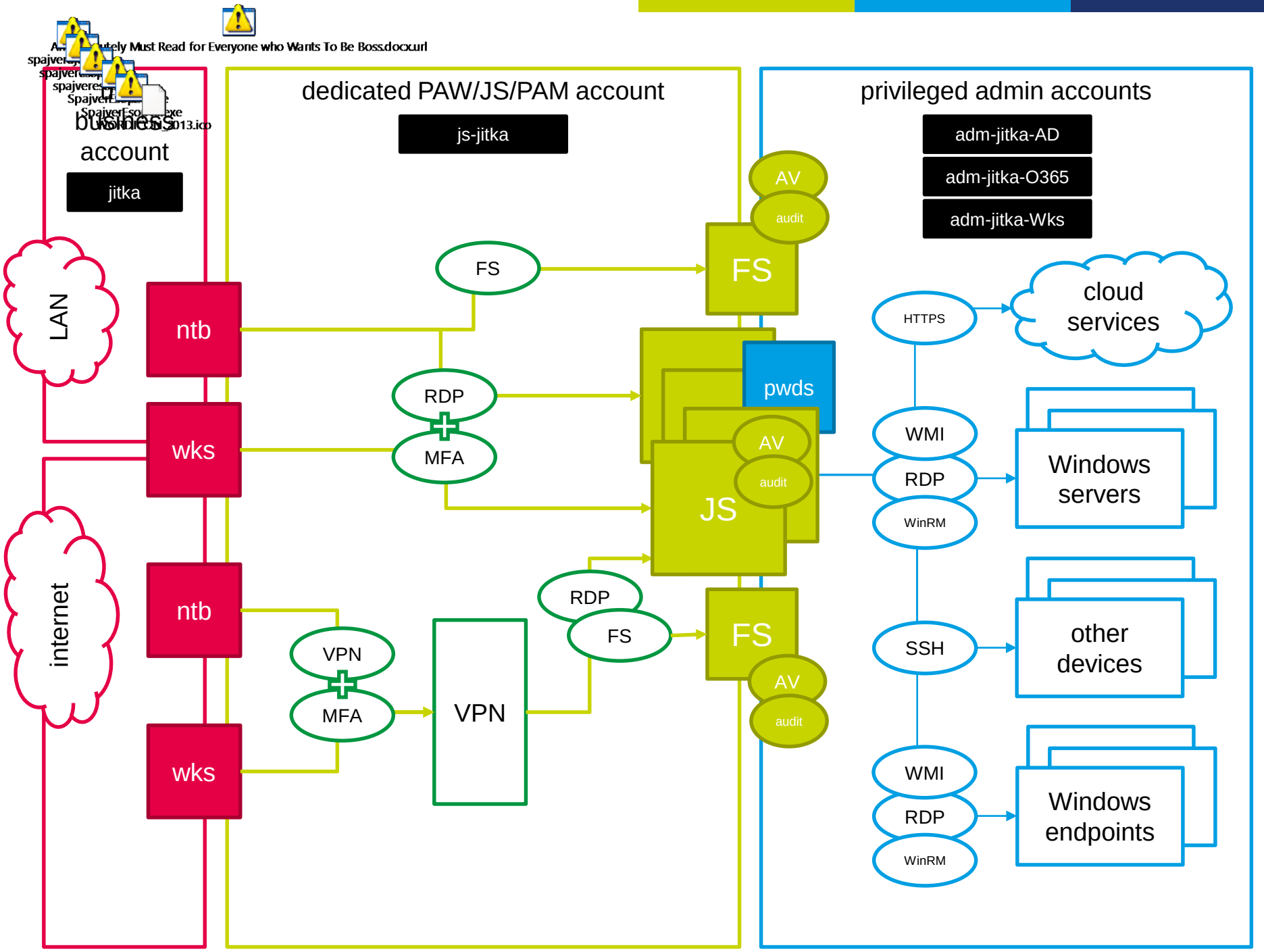
- SAE
  - secure administration environment
  - bezpečné metody přihlašování a používání účtů
  - bezpečné ukládání a použití hesel
  - více-faktorové ověřování kde je to možné
- tiering
  - opravdu separátní účty na správu různých částí sítě
  - opravdová izolace proti lateral movementu

GOPAS

Tiering



GOPAS


business account
jitka
dedicated PAW/JS/PAM account
js-jitka
privileged admin accounts
adm-jitka-AD
adm-jitka-O365
adm-jitka-Wks
LAN
internet
ntb
wks
ntb
wks
FS
RDP
MFA
VPN
MFA
VPN
RDP
FS
AV
audit
FS
pwds
AV
audit
JS
AV
audit
FS
HTTPS
cloud services
WMI
RDP
WinRM
Windows servers
SSH
other devices
WMI
RDP
WinRM
Windows endpoints

Děkuji za pozornost!

ondrej@sevecek.com (pořád)

GOPAS kurz GOC159 (pořád)

konference WUG Days 2020 (říjen 2020)

konference HackerFest 2020 online (do 24.9.2020)