Martin Haller

⟨ Krizové řízení při ransomware útoku ⟩

PATRON ⟨IT⟩ OCHRANA A SPRÁVA SÍTÍ

Kybernetický incident si nenaplánujete.

Martin Haller

- PATRON-IT s.r.o. (MSP / MSSP)
- Etický hacker
- Blog MartinHaller.cz

O jakých situacích se budeme bavit

- Úplné zastavení firmy při ransomware útoku
- Střední firmy (100-1000 PC)

Co děláme?

Šetříme peníze

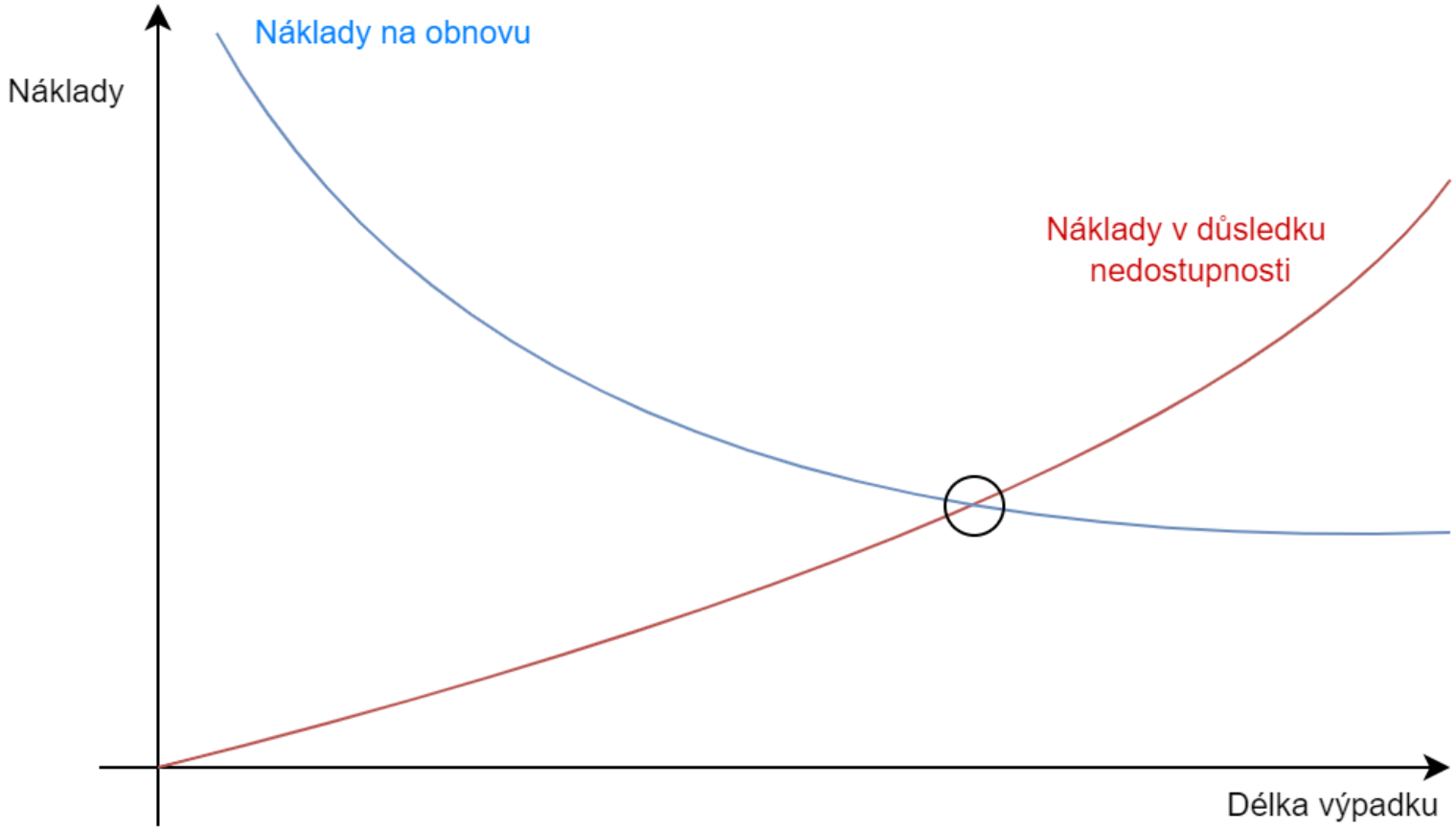
Co potřebujeme před zahájením prací?

Kompetence
Důvěru

⟨ Co se děje na místě ⟩

Co se děje na místě

1. Stanovení priorit s managementem



Co se děje na místě

1. Stanovení priorit s managementem
2. Vyjednávání s útočníky

Co se děje na místě

1. Stanovení priorit s managementem
2. Vyjednávání s útočníky
3. Zjišťování rozsahu kompromitace

Co se děje na místě

1. Stanovení priorit s managementem
2. Vyjednávání s útočníky
3. Zjišťování rozsahu kompromitace
4. Zjišťování vektoru průniku (zajišťování stop)

Co se děje na místě

1. Stanovení priorit s managementem
2. Vyjednávání s útočníky
3. Zjišťování rozsahu kompromitace
4. Zjišťování vektoru průniku (zajišťování stop)
5. Návrh procesu obnovy
   - Časově nejnáročnější
   - Nutné dokázat ohodnotit reálné hrozby
   - Umět pracovat v cizím prostředí
   - Role interního IT
   - Sestavit a ubránit

Nejčastější chyby

Podcenění délky výpadku

Rozložení sil

Učení se na bojišti

Prostoje

Děkuji za ⟨pozornost⟩