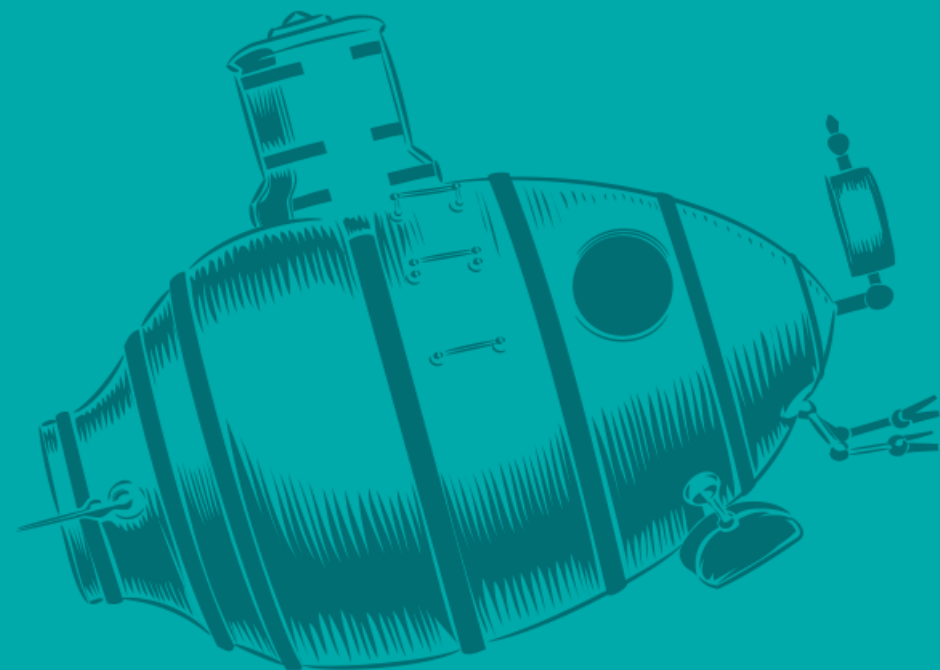


# Jak incident (snad) spustí krizové řízení

Michal Zedníček

ALEF NULA



# T0 – cca 8 měsíců

1. ALEF podává budoucí oběti nabídku na bezpečnostní audit Windows Infrastructure
2. Budoucí oběť odmítá nabídku ALEF
3. Mohli jsme se pouze domnívat, jak vypadá AD tiering, hardening endpointů a AD, autentizační mechanismy aj.

# Pátek večer, čas T0 ...

1. **Neznámý útočník (X1)**  
využívá přístup k firemnímu  
PC korporátního uživatele  
přes zneužitý domácí WIFI  
router
2. **X1 plně ovládá firemní PC**  
korporátního uživatele jako  
lokální admin

**Fidelis XDR hlásí ALERT**  
– vznik nového lokálního  
admina na firemním PC  
KU1 a posílá ho na  
adresu řešitelského týmu

# Sobota ráno, čas T0 + cca 12h ...

1. X1 vytáčí VPN do podnikové sítě, vyhledává MSFT AD a skenuje jeho zranitelnosti
2. X1 získává skrze kritické zranitelnosti doménového admina DA1, zakládá nového doménového admina DA2 a skryje ho, odhlašuje se z DA1

Fidelis XDR hlásí  
**CRITICAL ALERT** –  
skenování portů a vznik  
doménového admina a  
posílá ho na adresu  
řešitelského týmu

# Pondělí ráno, čas T0 + cca 2,5 dne ...

1. Člen řešitelského týmu čte email obsahující ALERTy Fidelis XDR
2. Řešitelský tým začíná řešit, co se stalo a reviduje domain admin účty
3. Co dělá X1 se můžeme pouze domýšlet. Reinkarnační schránky v ICT prostředí? Ovládnutí aplikačních systémů?

# Úterý, čas T0 + cca 3,5 dny ...

1. Řešitelský tým si začíná uvědomovat tíhu situace a zve si první externí experty Security Operation (CSIRT1) na konzultaci
2. CSIRT1 po posouzení situace, kdy ke kompromitovanému AD byly trustovány oboustranně důvěryhodnou komunikací další AD (vč. AD třetích stran), oznamuje poprvé calamitní stav a nastiňuje realitu katastrofy
3. Řešitelský tým začíná propadat panice a jímá ho hrůza, co by se mohlo stát

# Pátek, čas T0 + cca 7 dnů ...

1. Řešitelský tým si pozval experty ALEF CSIRT na konzultaci
2. ALEF CSIRT na sdílených informacích potvrdil závěry CSIRT1.
3. Řešitelský tým začíná přemýšlet, koho a jak informovat (NUKIB, 3.strany v důvěryhodném trustu ...).

# Pondělí, čas T0 + cca 10 dnů ...

**Neznámý útočník (X1)  
nezpůsobuje v prostředí žádné  
škody, nevyhrožuje jimi a  
nepokouší se obět' kontaktovat**

**CSIRT1 i ALEF CSIRT se  
kloní k závěru, že:  
X1 = APT aktér**



Úterý, čas T0 + cca 11 dnů ...

ALEF CSIRT podává nabídku  
na služby „Incident response“  
řešitelskému týmu

**Pátek, čas T0 + cca 14 dnů ...**

**Řešitelský tým odmítá nabídku  
ALEF CSIRT**

## čas T0 + cca 30 dnů ...

1. CSIRT 3. strany (CSIRT3rd)  
v důvěryhodném trustu AD  
žádá o pomoc ALEF CSIRT
2. ALEF CSIRT obratem  
podává nabídku na služby  
„Incident response“  
CSIRT3rd

3. CSIRT3rd přijímá  
nabídku ALEF CSIRT  
a začíná služba  
Incident response

## čas T0 + cca 35 dnů ...

1. ALEF CSIRT vypracoval závěr Incident response a vysvětlil situaci managementu organizace (MAN3rd)
2. MAN3rd vyhlašuje stav katastrofy a zahajuje krizové řízení

**X1 nepůsobí ani u 3rd organizace žádné škody**

# čas T0 + cca 36 dnů ...

ALEF CSIRT představil MAN3rd  
2 možnosti řešení

1. Všechno smazat a postavit znovu = 12 – 18 měsíců plně mimo kontinuitu, další roky až desetiletí návrat současnému SLA
2. Vystavět sadu bezpečnostních opatření a modlit se, že X1 chytíme, až začne přístupy využívat = obrovské investice a neošetřitelná rizika

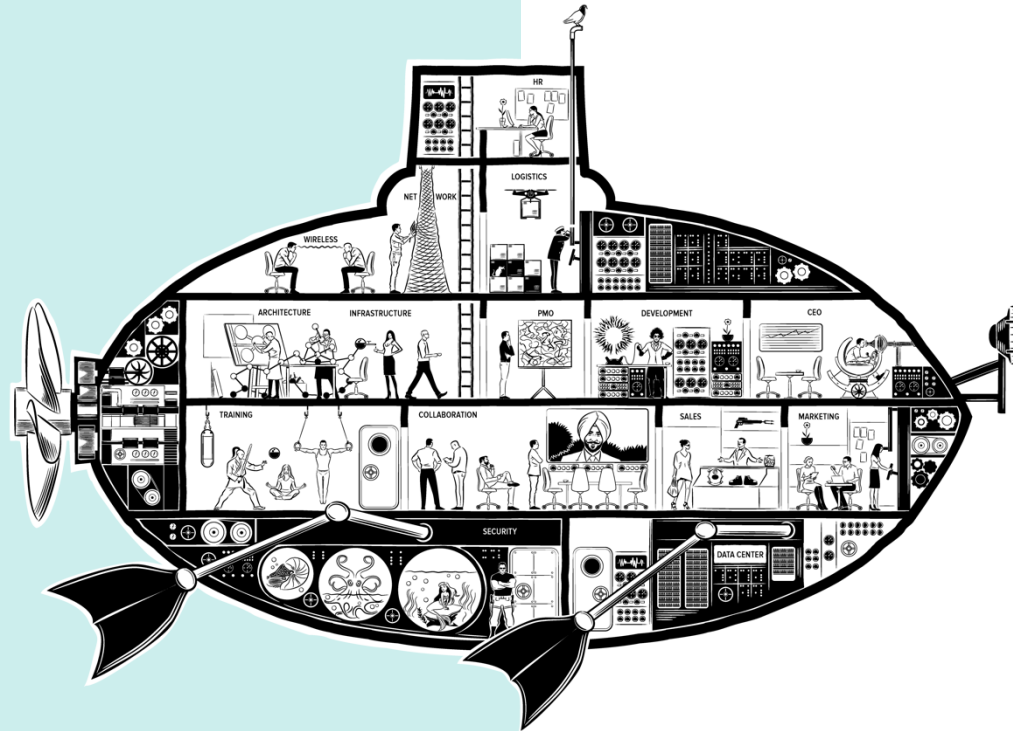
**čas T0 + cca 36 dnů ...**

**MAN3rd se rozhoduje pro  
druhou možnost se vším, co to  
znamená**

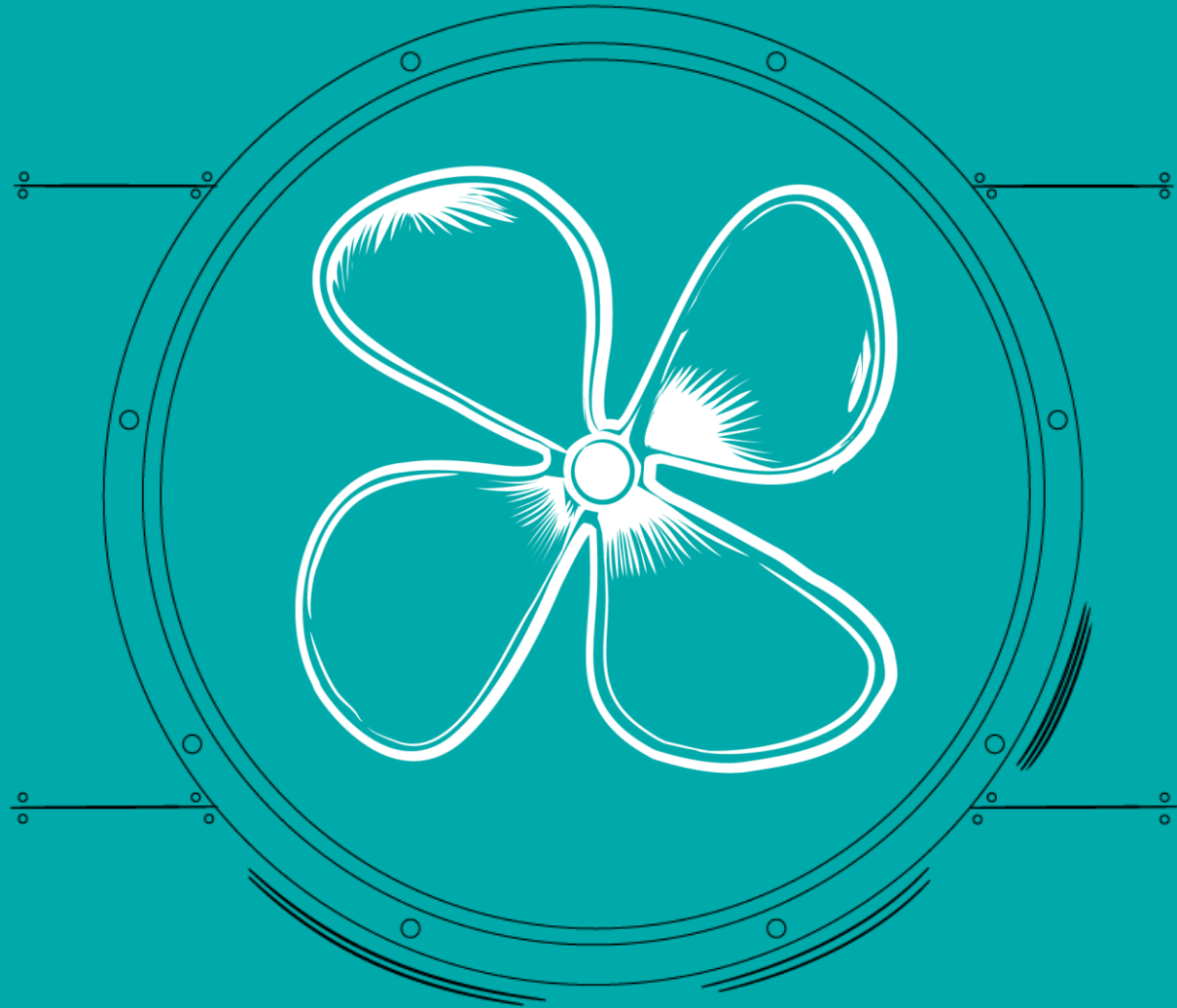
# Poučení

1. **Prevence je většinou levnější než reakce (a to i když stojí hodně!)**
2. **Min. 95% klientů, kteří objednali audit Windows Infrastructure, BYLO snadno hacknutelných. U 5% nebylo jasné, jaké úsilí by to stálo.**
3. **Krizové řízení nastává většinou po souhře banálních příhod. Kybernetická bezpečnost je bohužel o detailu.**

# OUR KNOWLEDGE IS YOUR FUTURE







**Thank you for your attention!**