

# Ransomware

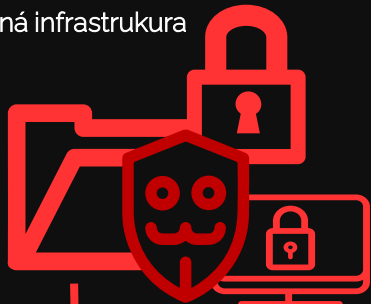
.....a kdy dojde na vás?



Tomas Hlavsa

# 100% ochrana neexistuje

Infikovaná infrastruktura



Koupíte si klíč?

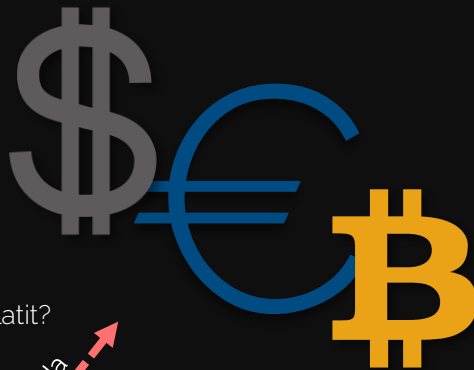
**Vydírání**  
(zdvořile formulováno)

výkupné  
V jaké měně preferujete zaplatit?

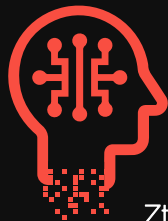
Hrozba zveřejnění dat



Krádež dat



škoda



Ztráta intelektuálního vlastnictví

Škody  
vícenaklady



Výpadky produkce

Škody



Ztráta citlivých dat

Náklady



Obnova infrastruktury

škoda



Ztráta důvěry  
a  
poškození reputace

# Díky o day exploitům jde jen o otázku motivace útočníků

Motivovaný útočník



Ransomware



....v příloze posíláme fakturu

...stáhněte si.....

...je libo reklamni USB?



UŽIVATEL  
ochotný pomoci



ZAŘÍZENÍ

KAŽDÉ ZAŘÍZENÍ JE ZRANITELNÉ



#3  
cíl

Infekce  
Enkrypcce  
Extrakce

Network

Servery

Storage/  
Backup

síť

Databases

EndPoint

síť

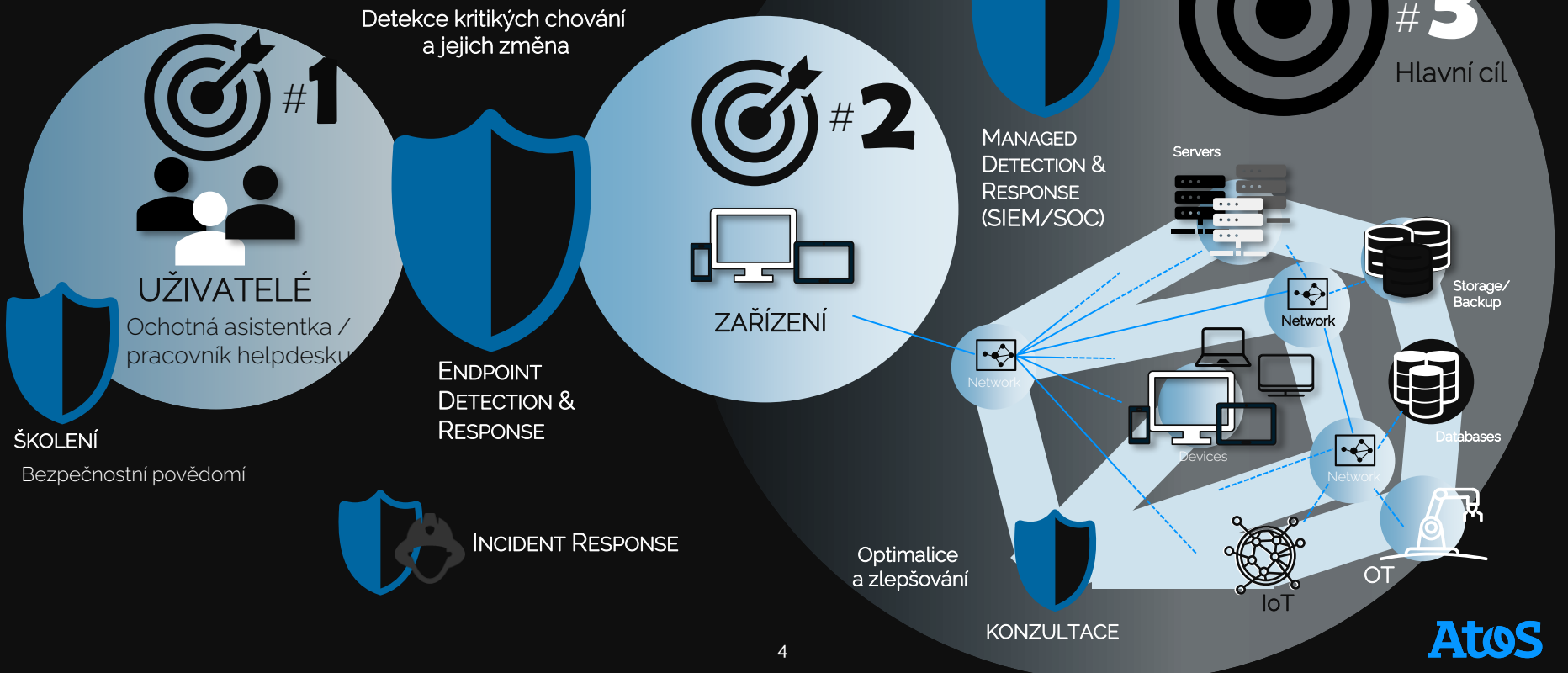
IoT

OT

Zaplatíte?

# Ne ochrana, ale ...PROTIOPATŘENÍ

.....zkuste myslet jinak, aktivně bojujte



# Kdo za to může?

X

## Jak zvýšit naše šance?

# Snižování rizika konkrétně

## CO

ZVYŠOVÁNÍ  
BEZPEČNOSTNÍHO  
POVĚDOMÍ



Bezpečnostní povědomí a  
SCHOPNOST REAGOVAT

HODNOCENÍ  
/ KONZULTACE



Přehled a revize priorit  
prostředí a jeho  
optimalizace

ENDPOINT  
DETECTION &  
RESPONSE



Detekce kritického chování  
Machine learning a regulace

MANAGED  
DETECTION &  
RESPONSE  
(SIEM/SOC)



Zvyšování transparentnosti a  
Nasazování preventivních  
mechanismů

INCIDENT  
RESPONSE



Cílené akce v případě  
bezpečnostního ohrožení

## PROČ

Lidé jsou slabý článek

....

A vždycky budou

Nemonitorujete = nevíte

Nevíte = neřídíte

Neřídíte = ☹️

Detekce, monitoring  
REAKCE

Kupujete si čas pro  
PODPORU ROZHODOVÁNÍ

Udržovat si SCHOPNOST REAGOVAT

X

Mít tuto schopnost jako službu?

## KDY

# HNEDE

# Metodika Atosu

ZVYŠOVÁNÍ  
BEZPEČNOSTNÍHO  
POVĚDOMÍ



Školení si můžete koupit leckde.

Atos má metodiku pro jaké role mají mít lidé jaké předpoklady a teprve poté jaká školení

HODNOCENÍ  
/ KONZULTACE



Když ne permanentní, tak alespoň pravidelné vyhodnocování prostředí.

Pokud Vás nezajímá co se ve Vašem prostředí děje (nová síť, nová pobočka, nový software) .....tak Vám moc gratulujeme

ENDPOINT  
DETECTION &  
RESPONSE



Antivirus, DLP, Antimalware, DRM, CloudProtection

I EndPointy by měly být schopny RESPONSE

MANAGED  
DETECTION &  
RESPONSE  
(SIEM/SOC)



Koncepce, Implementace a SPRÁVA ŘÍZENÍ BEZPEČNOSTI (.....SOC)

Preventivní bezpečnost namísto pasivní detkce bez adekvátní reakce.

Bez RESPONSE jsou to jen vyhozené peníze a ztracený čas.

INCIDENT  
RESPONSE



A když už se stane.....

# .....a když už se stane.....máte komu ZAVOLAT!!!

Stali jste se obětí RANSOMWARE útoku?

Jistě, bylo by lepší, kdyby k úspěšnému útoku nedošlo. Umíme nabídnout i preventivní kontroly a penetrační testy vč. metodik sociálního inženýrství. Tím odhalujeme slabiny a navrhujeme způsob jejich odstranění.

Atos emergency hotline

Provozujeme 24 x 7 linku na které Vám pomůžeme i během probíhajícího útoku. Náš „Rapid Response Team“ je připraven dorazit v co nejkratší době. Bezpečnostní profici na „incident response“, „forenzní zkoumání“ a „bezpečnost informací“ na místě/na dálku spolu s Vámi provedou urgentní zásahy. Dále se budou pokoušet o limitaci škod, prevenci dalších vln útoku a obnovu původního stavu. Samozřejmostí je zajištění forenzních stop pro následné vyšetřování.

Budeme od Vás potřebovat informace:

- KDY incident nastal
- CO (popis) se stalo?
- KDO incident zaznamenal?
- Jak se na incident přišlo?
- Jaké kroky od té doby KDO podniknul?



# Chcete vědět více?:

[tomas.hlavska@atos.net](mailto:tomas.hlavska@atos.net)

+420 604 290 196



Atos, the Atos logo, Atos|Syntel are registered trademarks of the Atos group.  
June 2021. © 2021 Atos. Confidential information owned by Atos, to be used by the recipient only. This document, or any part of it, may not be reproduced, copied, circulated and/or distributed nor quoted without prior written approval from Atos.