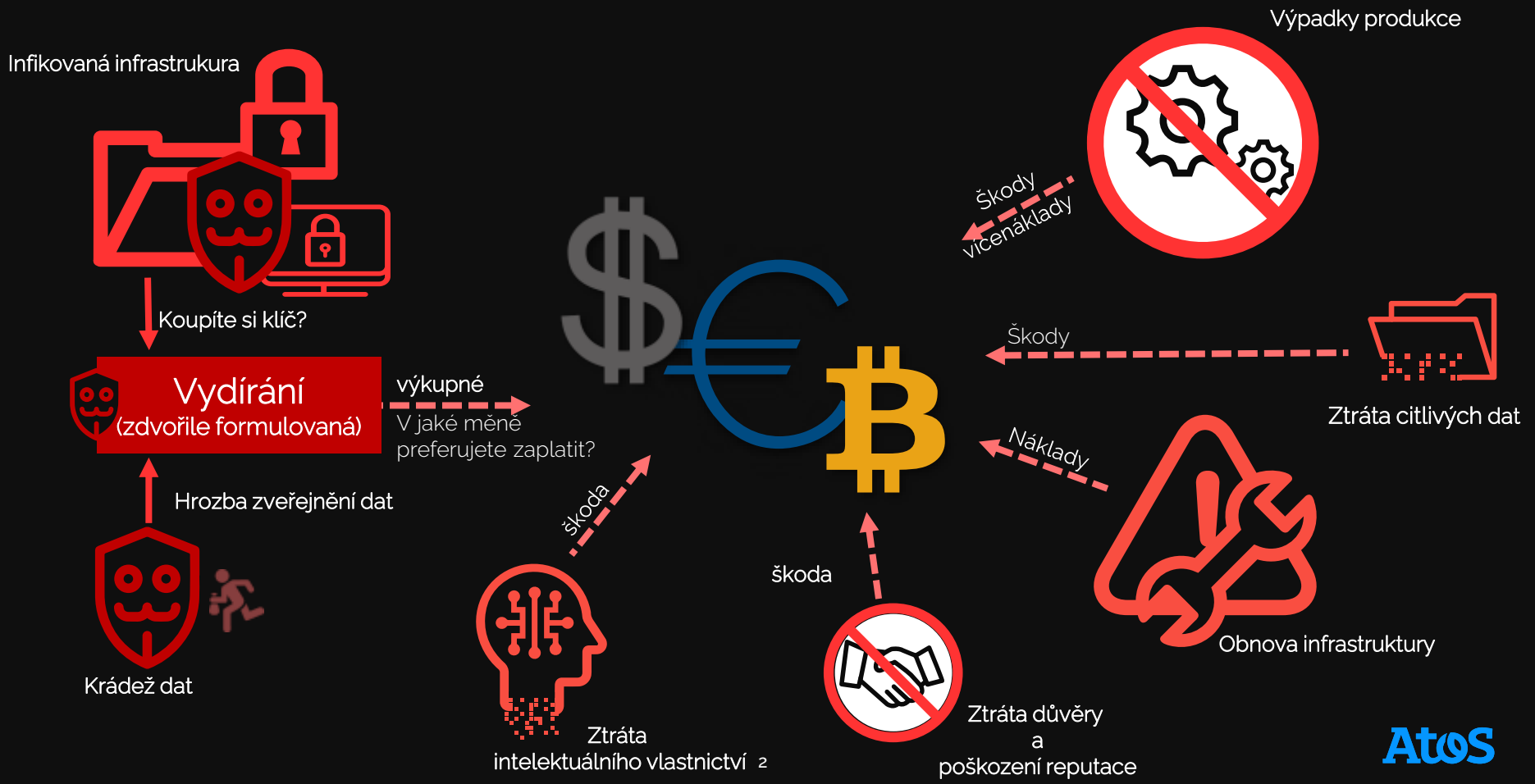
Ransomware

.....a kdy dojde na vás?

Tomas Hlavsa

100% ochrana neexistuje



Díky 0 day exploitům jde jen o otázku motivace útočníků

Motivovaný útočník

Ransomware

#1

.....v příloze posíláme fakturu

...stáhněte si.....

....je libo reklamni USB?

UŽIVATEL
ochotný pomoci

#2

ZAŘÍZENÍ
KAŽDÉ ZAŘÍZENÍ JE ZRANITELNÉ

Infekce
Enkrypce
Extrakce

Network

#3
cíl

Servery

Storage/
Backup

síť

Databases

EndPoint

síť

IoT

OT

Zaplatíte?

Ne ochrana, ale ....PROTIOPATŘENÍ

.....zkuste myslet jinak, aktivně bojujte

Každé nápravné opatření / zlepšení se počítá

#1

UŽIVATELÉ

Ochotná asistentka / pracovník helpdesku

ŠKOLENÍ

Bezpečnostní povědomí

Detekce kritických chování a jejich změna

ENDPOINT DETECTION & RESPONSE

#2

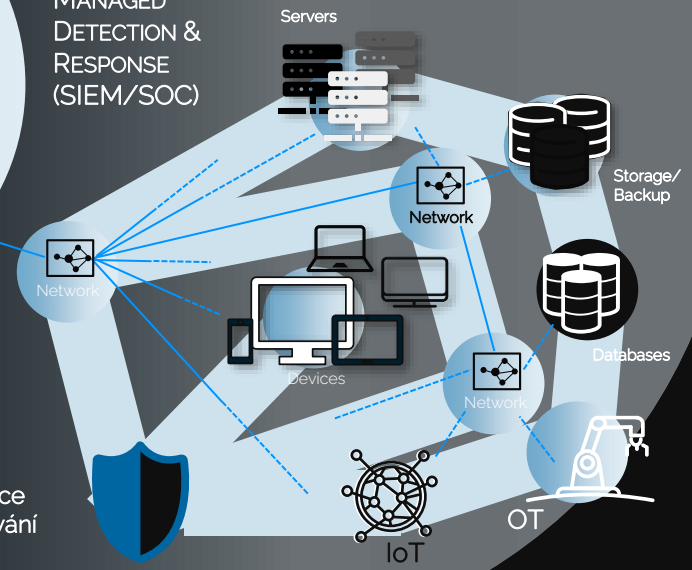
ZAŘÍZENÍ

INCIDENT RESPONSE

MANAGED DETECTION & RESPONSE (SIEM/SOC)

#3

Hlavní cíl



Optimalice a zlepšování

KONZULTACE

Kdo za to může?

X

Jak zvýšit naše šance?

Snižování rizika konkrétně

	CO	PROČ	KDY
Zvyšování bezpečnostního povědomí 	Bezpečnostní povědomí a SCHOPNOST REAGOVAT	Lidé jsou slabý článek .... A vždycky budou	
Hodnocení / konzultace 	Přehled a revize priorit prostředí a jeho optimalizace	Nemonitorujete = nevíte Nevíte = neřídíte Neřídíte = ☺	
Endpoint Detection & Response 	Detekce kritického chování Machine learning a regulace	Detekce, monitoring REAKCE	HNED
Managed Detection & Response (SIEM/SOC) 	Zvyšování transparentnosti a Nasazování preventivních mechanismů	Kupujete si čas pro PODPORU ROZHODOVÁNÍ	
Incident Response 	Cílené akce v případě bezpečnostního ohrožení	Udržovat si SCHOPNOST REAGOVAT X Mít tuto schopnost jako službu?	

Atos

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.....

Atos

.....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 preventovní 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 profíci 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.hlavsa@atos.net

+420 604 290 196

Atos