



BaltoGrid – případová studie analýzy datového provozu
pro odhalování škodlivého provozu v energetice

Vladimír Sedláček, CTO

NA ÚVOD

Kdysi, když lidé viděli automobil, si říkali "ejhle, automobil."

V době rozmachu automobilizmu se pak naučili rozpoznávat jednotlivé značky a poznali, k čemu je osobní a nákladní vůz a co je autobus.

Nedávno, když lidé viděli počítač, si říkali "ejhle, počítač."

Dnes sebou denně nosíme tablety a mobily,

víme, k čemu je dobrý notebook a server,

tušíme, co je cloud,

a hádáme se, jestli je lepší iPhone 7 nebo Samsung Galaxy.

GREYCORTEX

ALE KDYŽ ŘEKNU „BEZPEČNOST?“

Co se vám vybaví, když někdo mluví o bezpečnosti?

Firewall?

Antivirus?

Bezpečnosti v síti?

Bezpečnosti v síťových odvětvích?



[Tato fotka](#) od autora Neznámý autor s licencí [CC BY-SA](#)

GREYCORTEX

CO JE GREYCORTEx?

Společnost: GREYCORTEx s.r.o., Brno

- 100% český kapitál, profesionálové v IT a veteráni kyberbezpečnosti (C|EH, CISSP, ...)

Cíl: **Dělat svět bezpečnějším.**

Napomáhat ochraně podniků, úřadů, kritické infrastruktury, přenosových sítí

- Prostřednictvím sledování a analýzy provozu IT a OT (SCADA, ICS, Smart Buildings / Cities / Grids)

Produkt: **GREYCORTEx MENDEL**

- kombinace BI, ML a AI

Historie: 2009 výzkum (bezpečnostní analýza videomonitoringu - 3x cena NIST)

2013 produkt pro NTA (MENDEL)

2016 založen GREYCORTEx

2019 jediný dodavatel NTA v kontinentální Evropě podle
Gartner Market Guide for Network Traffic Analysis

GREYCORTEx

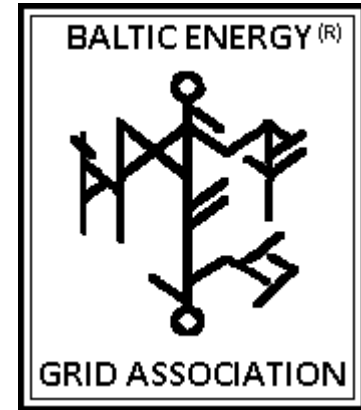
Naši severští sousedé

Podobnost se skutečnými firmami, žijícími nebo mrtvými, je čistě fiktivní.

BALTOGRID – PŘEDSTAVENÍ

Zájmové sdružení právnických osob (spolek)

- Výrobci energií
- Operátoři přenosových soustav
- Operátoři distribučních soustav
- Obchodníci



Společný postup při plnění regulovaných činností a zajišťování spolehlivých dodávek v požadované kvalitě – nikoliv cenový kartel!

GREYCORTEX

BALTOGRID – ETAPY PROPOJOVÁNÍ

Technické propojení

- provozních systémů s informačními
 - Samostatné, ještě před vznikem sdružení
- informačních systémů navzájem
 - Nahodilé, ještě před vznikem sdružení
 - Systematické v rámci sdružení, standardizace rozhraní
- obchodních systémů do centralizovaného obchodování
 - Centrální místo obchodování a předávání dispečerských informací, jednotné rozhraní
- call centra, zákaznická samoobsluha
 - Sdílené služby, externí dodavatelé služeb

BALTOGRID – DŮSLEDKY PROPOJOVÁNÍ

Propojení zodpovědnosti

- za provozní bezpečnost
- za informační bezpečnost
- za reporting, vyšetření, nápravu a prevenci bezpečnostních incidentů

Ale jak zaručíte něco, do čeho nevidíte?

Jaká jsou rizika?

VNITŘNÍ RIZIKA

Individuální

- technologie
- údržba
- dodavatelé, aktualizace

Společná

- vzájemná komunikace a integrace systémů řízení
- společné administrativní systémy

VNĚJŠÍ RIZIKA

- konkurence
- zájmové agentury
- soused s velmocenskými ambicemi
- cílený průnik
- přírodní vlivy
- nahodilý průnik

VRSTVY OCHRANNÝCH OPATŘENÍ

- provozní
- technická
- organizační, vzdělávací
- **kontrolní - NTA**

MENDEL: Posvit' na síť!

Plná síťová viditelnost pro síťovou bezpečnost

Jak se zapojujeme do sítě

Jak analyzujeme, co jsme našli

PROČ CHYTAT HROZBY V SÍTI?

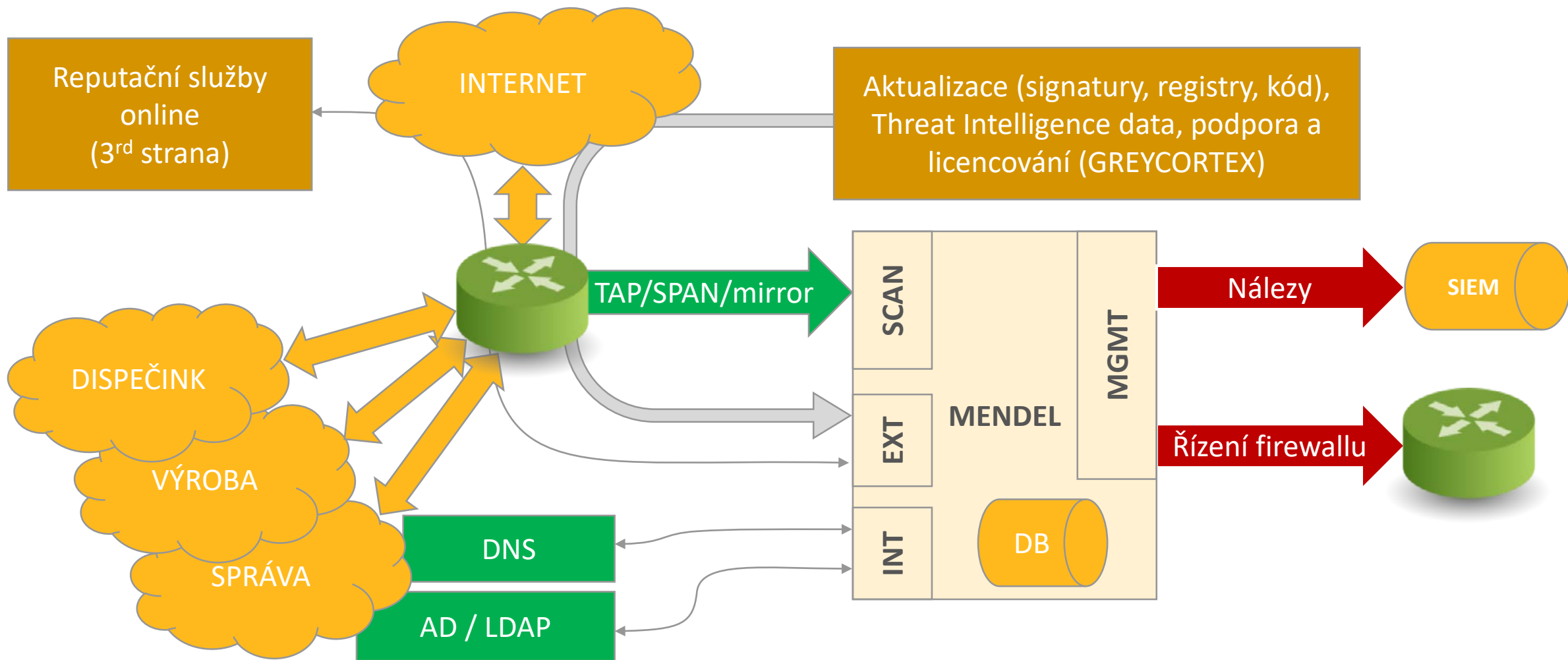
- Vše je dnes propojené do jediné „Sítě věcí“
 - Všechna zařízení nějak komunikují přes síť, nejčastěji IP protokoly (IPv4, IPv6)
 - Malá zařízení s omezeným výkonem obětují bezpečnost za funkčnost
 - Zastaralá, neudržovaná zařízení (akt. webové rádio)
- Komunikace je vždy potřeba
 - Malware do svého Command and Control Centra
 - Malware pro rozšíření (Laterální pohyb)
 - Insider, vetřelec nebo malware exfiltruje (uploaduje) data
 - Přitom síťové firewally často neomezují komunikaci směrem do internetu, nebo se dají snadno proděravět. Pračky obsahu lze obejít pokročilými technikami

**PRODUKTY NTA, JAKO NÁŠ
GREYCORTEx MENDEL,
UMÍ ODHALIT NEŽÁDOUCÍ PROVOZ
VČETNĚ KOMUNIKUJÍCÍCH APT**

Pokročilý persistentní malware (Advanced Persistent Threat, APT) vždy po síti komunikuje. Jeho komunikace vždy vykazuje specifické nebo neobvyklé známky chování.

GREYCORTEx

ZDROJE DAT A INTEGRACE



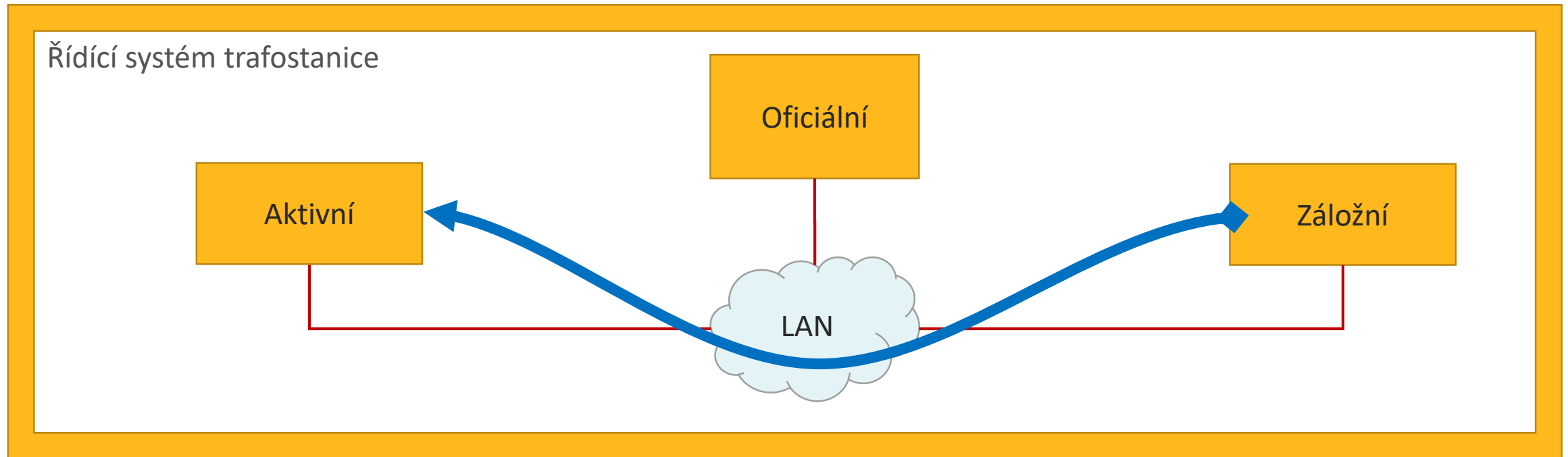
GREYCORTEX

Dosažené úspěchy

- prověrka zařízení u výrobce/dodavatele
- analýza provozu

CHYBNÁ KONFIGURACE TRAFOSTANICE

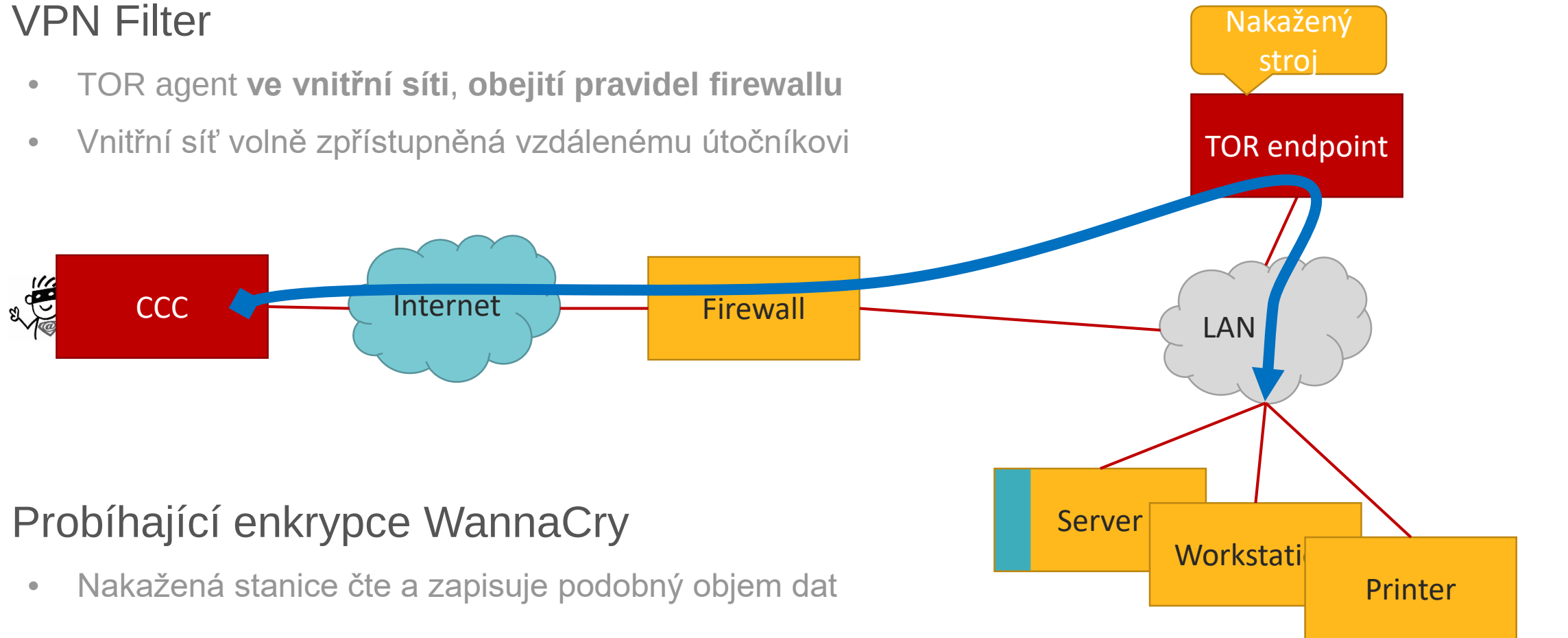
- Aktivní a záložní systém si vzájemně poskytovaly služby namísto komunikace s určeným systémem. Vzniklo riziko nesprávné funkce a ohrožení dodávky energie. Zjištěno ještě u výrobce.



REZIDENTNÍ MALWARE V AKCI

- VPN Filter

- TOR agent **ve vnitřní síti**, obejití pravidel firewallu
- Vnitřní síť volně zpřístupněná vzdálenému útočníkovi

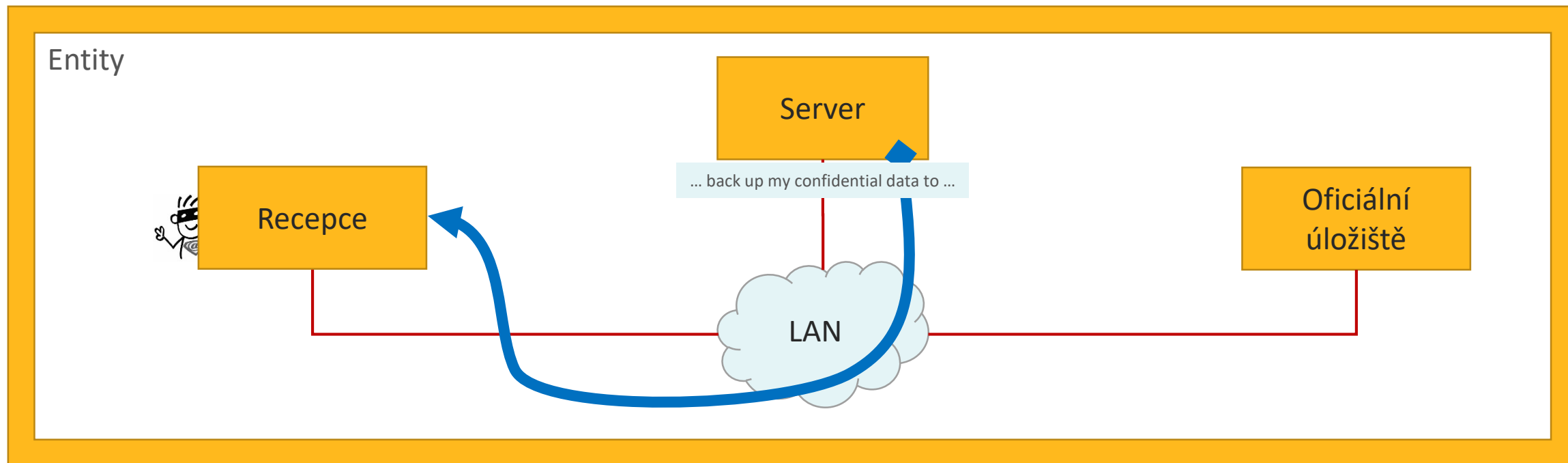


- Probíhající enkrypcce WannaCry

- Nakažená stanice čte a zapisuje podobný objem dat

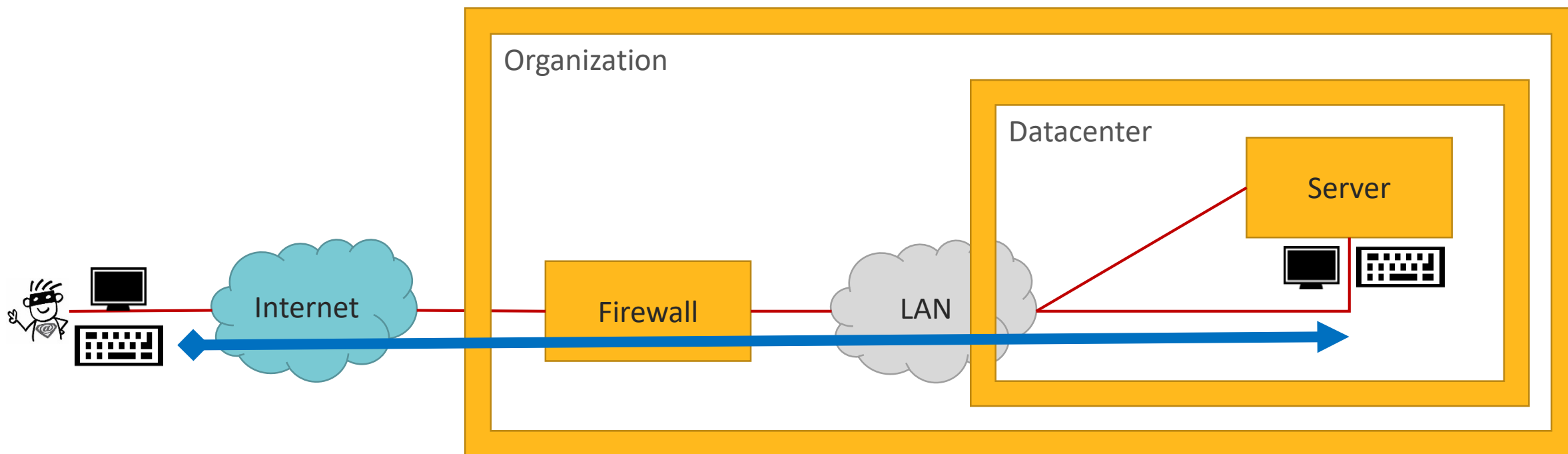
ZÁLOHOVÁNÍ DAT NA NESPRÁVNÝ CÍL

- Konfigurace zálohování použitá při testování nebyla následně opravena a citlivá data o zákaznících končila na pracovní stanici recepce.



VZDÁLENÁ KONZOLA NA INTERNETU

- Firewall nakonfigurovaný pro předávání portů na adresu serverového IPMI
- Vznikl tak neomezený přístup s možností instalovat software na produkční server, navíc nebylo změněno výchozí heslo dodavatele



A jak to máte vy?

MĚLO BY VÁS TO ZAJÍMAT?

Je vaše provozní infrastruktura dobře izolovaná od okolí? A můžu ji vidět?

Dokážete si představit všechny možné útoky a jejich vektory? A zkusili jste si je?

Máte certifikáty a ujištění dodavatelů a zaměstnanců, že všechno je nastavené a zabezpečené dle ustanovených politik? A ví o nich útočníci?

Víte, co u vás komunikuje s čím, jak a o čem? A můžeme si to zobrazit v reálu?

Zjistíte, že se připojilo nepovolené zařízení nebo proběhla podivná komunikace, která by mohla znamenat kompletní odstávku dodávek během desítek minut?
A dostanete o tom varování?

A dokážete na takové varování reagovat včas?

POLEMIKA

Nepotřebujeme přece vidět do sítě! Máme ujištění a certifikáty od dodavatelů a konzultantů. To nám stačí.

BEZPEČNÝ STANDARD ZABEZPEČENÍ?

Recent Exploitable Flaw in IEEE 802.11: **KRACK (CVE-2017-13082)**

Existing since 2008, introduced into 802.11r by support for fast BSS Transition (envisioning SIP IP roaming)

From Wikipedia, the free encyclopedia [2017-11-05, <https://en.wikipedia.org/wiki/KRACK>]:

*“KRACK (Key Reinstallation AttaCK) is a severe replay attack (a type of exploitable flaw) on the Wi-Fi Protected Access protocol that secures Wi-Fi connections. ... discovered in 2016 by the Belgian researchers ... published details of the attack in October 2017. By repeatedly resetting the **nonce** transmitted in the **third step of the WPA2** handshake, an attacker can gradually match encrypted packets seen before and learn the full keychain used to encrypt the traffic.”*

The **weakness is in** the Wi-Fi **standard itself**, ... any **correct implementation** of WPA2 is likely to be **vulnerable** ... all major software platforms ...

The widely used **open-source** ... wpa_supplicant, ... Linux and Android, is especially susceptible as it can be manipulated to install an all-zeros encryption key, effectively nullifying WPA2 protection in a man-in-the-middle attack.

Final ...

Questions?

KDO JE NÁŠ ZÁKAZNÍK (TYPOVĚ)

- Výzkumná a výrobní organizace
- Banka, finanční instituce
- Informační společnost
- Zdravotnické zařízení
- Právní kancelář
- Úřad, ministerstvo, prefektura
- Státní agentura, silový odbor
- Městský podnik služeb
- Operátor přenosové soustavy
- SoC poskytovatel
- VY?

VYZKOUŠEJTE SI NÁS



GREYCORTEX

ZNÁME JEN DVA DRUHY UŽIVATELŮ ICT

- ti, které už hackli
- ti, které to teprve čeká

Jste na řadě?

Jak se vám spí?



[Sleeping Positions](#), unknown author, 2019-09-16 20:09

GREYCORTEX

Používejte GREYCORTEx Mendel, budete spát lépe!

www.greycortex.com – whitepapers, use cases, and more
info@greycortex.com – komunikace
www.youtube.com/greycortex – videa a další

Memes courtesy of: <http://weknowmemes.com/generator/generator/>
Logo based on <https://cochese-tattoo.com/tatouage-symbole-magie/>

GREYCORTEx