VIAVIS střežíme podstatné

Jak na bezpečnost dat

Vladimír Lazecký

vladimir.lazecky@viavis.cz

Obsah přednášky

- Aktuálně z kyber světa
- Opakování – bezpečnost dat
- Stanovení nároků na bezpečnost
- Praktické příklady

Stav Wall of Shames 30.10.2025

Wassa, SRO
Qilin
Discovery Date: 2025-10-19
In 2012, we established a sheltered workshop and we provide more than 100 protected work positions a...

CIMEXSTEEL.CZ
Qilin
Discovery Date: 2025-08-08
Estimated Attack Date: 2025-08-07
The Czech holding company CS STEEL a.s. manufactures and sells metal structures for private and publ...

ACMARK
Beast
Discovery Date: 2025-07-29
Estimated Attack Date: 2025-06-24
ACMARK s r o is a company that operates in the Repair Services industry. It employs 10to19 people an...

gjszlin.cz
Safepay
Discovery Date: 2025-05-26
Estimated Attack Date: 2025-05-21
[AI generated] N/A...

Grafton Technologies
Play
Discovery Date: 2025-05-14
Estimated Attack Date: 2025-05-12
United States...

Synthesia.com
Imncrew
Discovery Date: 2025-05-05
SYNTHESIA TECHNOLOGY was founded in 1964 with private capital. It started operations in the chemical...

kosmas.cz
Lynx
Discovery Date: 2025-05-28
Estimated Attack Date: 2025-05-04
Online bookstore Kosmas.cz ...

Nedved Architekti
Spacebears
Discovery Date: 2025-05-12
Estimated Attack Date: 2025-05-03
The main principle of the work of the Nedvěd architects studio is the search for new spatial solutio...

csspv
Nightspire
Discovery Date: 2025-04-28
Estimated Attack Date: 2025-04-27
csspv (Czechia)...

VIAVIS

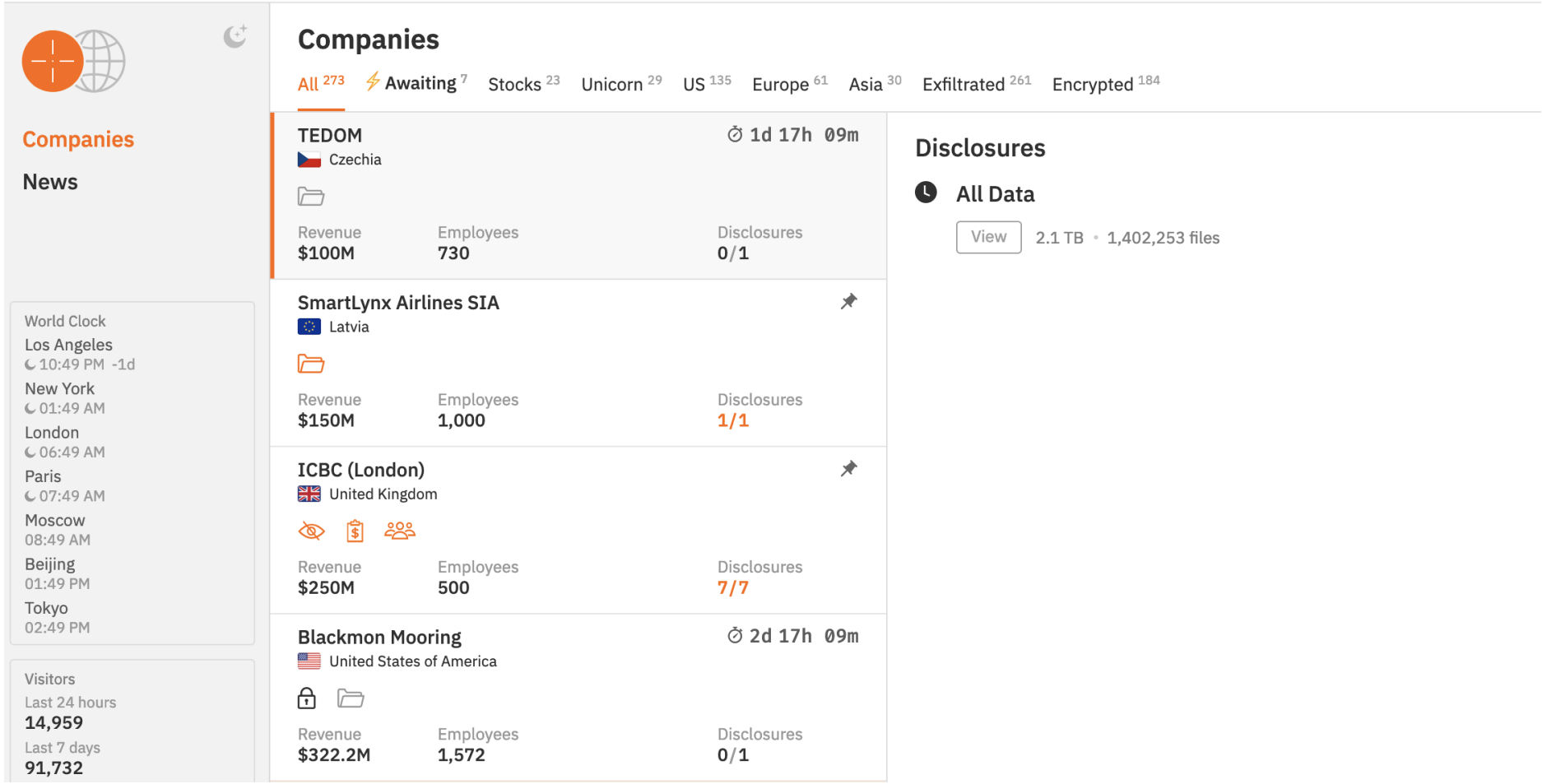
Monitoring Darknet

Date	Title	Group
2025-04-10	Algas Engineering Pte Ltd - Algas Engineering	qilin
2025-04-10	sk.com	qilin
2025-04-10	InterLOGIC Inc(US)	nightspire
2025-04-10	Nicera(Japan)	nightspire
2025-04-10	3P Corporation	space bears
2025-04-10	Fenwick & West LLP	leakeddata
2025-04-10	So...	leakeddata
2025-04-10	Potomac Financial Services	hellcat
2025-04-10	silocaf.com	inc ransom
2025-04-10	chesterfieldtwp.org	inc ransom
2025-04-10	finetech.de	inc ransom
2025-04-10	InterLOGIC Inc(United States)	nightspire
2025-04-10	Secretaria de Educacion de Veracruz, SEV(Mexico)	nightspire
2025-04-10	InterLOGIC Inc(Japan)	nightspire
2025-04-09	Dumont Telephone	akira
2025-04-09	Správa služeb hlavního města Prahy	cicada3301
2025-04-09	SPEEDFAM	qilin
2025-04-09	Blink Photo	qilin

date	title	group
2025-04-10	3P_Corporation	spacebears
2025-04-10	silocaf.com	incransom
2025-04-10	finetech.de	incransom
2025-04-10	chesterfieldtwp.org	incransom
2025-04-09	ccso2014.local(sheriffs)	incransom
2025-04-09	gramoll.com	lynx
2025-04-08	physiciansmedicalbilling.net	lockbit3
2025-04-08	RFMS,_Inc.	kairos
2025-04-08	https://www.thirdave.com	metaencryptor
2025-04-08	Thiekon_Constructie	incransom
2025-04-08	crystal-d.com	lockbit3
2025-04-08	Coop57	incransom
2025-04-08	shengyusteel.com	underground
2025-04-07	Galesburg_Area_Chamber_of_Commerce	kairos
2025-04-07	Telecontrol	ransomhouse
2025-04-07	[DISCLOSED]Cell_C	ransomhouse
2025-04-07	IDS_Infotech	hunters
2025-04-06	asiapacificex.com	lockbit3
2025-04-06	Hofmann_Fördertechnik_GmbH	hunters
2025-04-06	Groupe_Delcourt	hunters

VIAVIS

Kyber útoky v ČR aktuálně

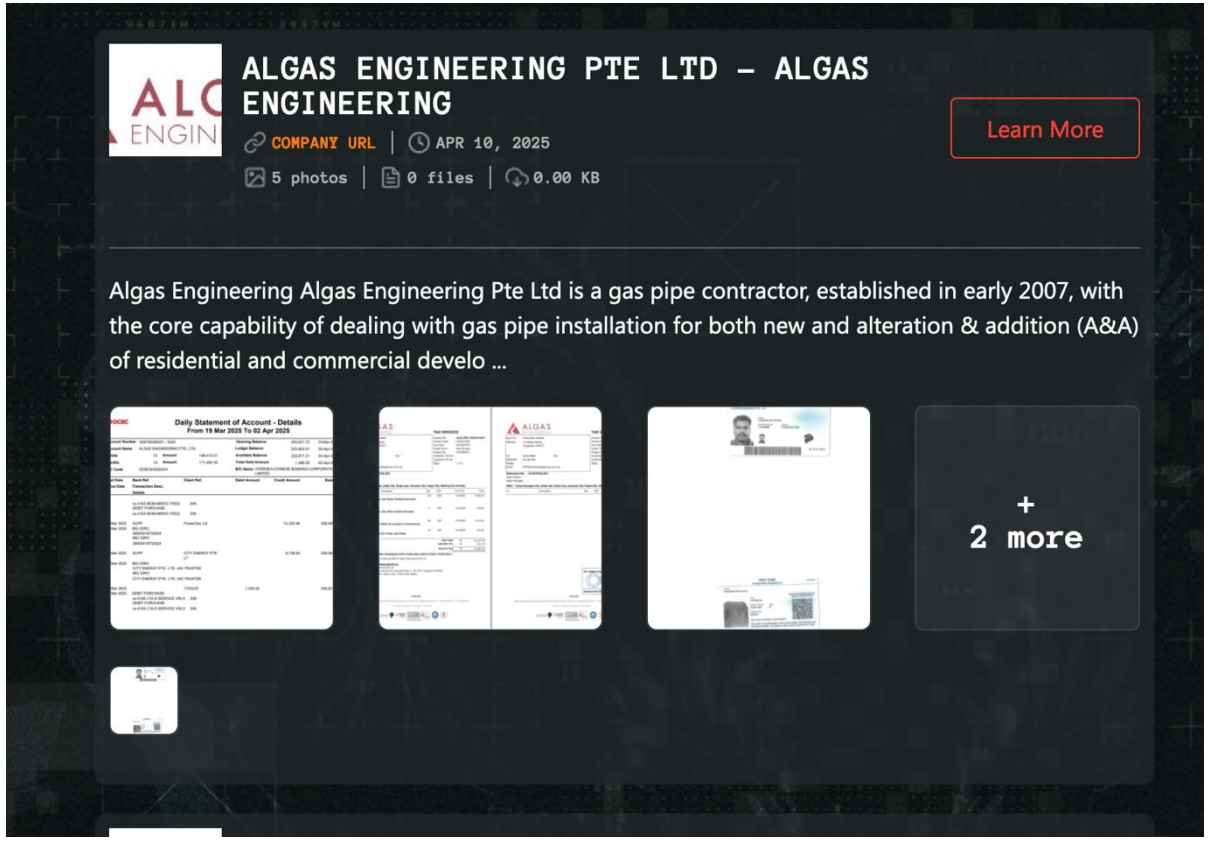


https://hunters55rdxciehoqzwv7vgyv6nt37tbwax2reroyzxhou7my5ejyid.onion/companies/3433731161

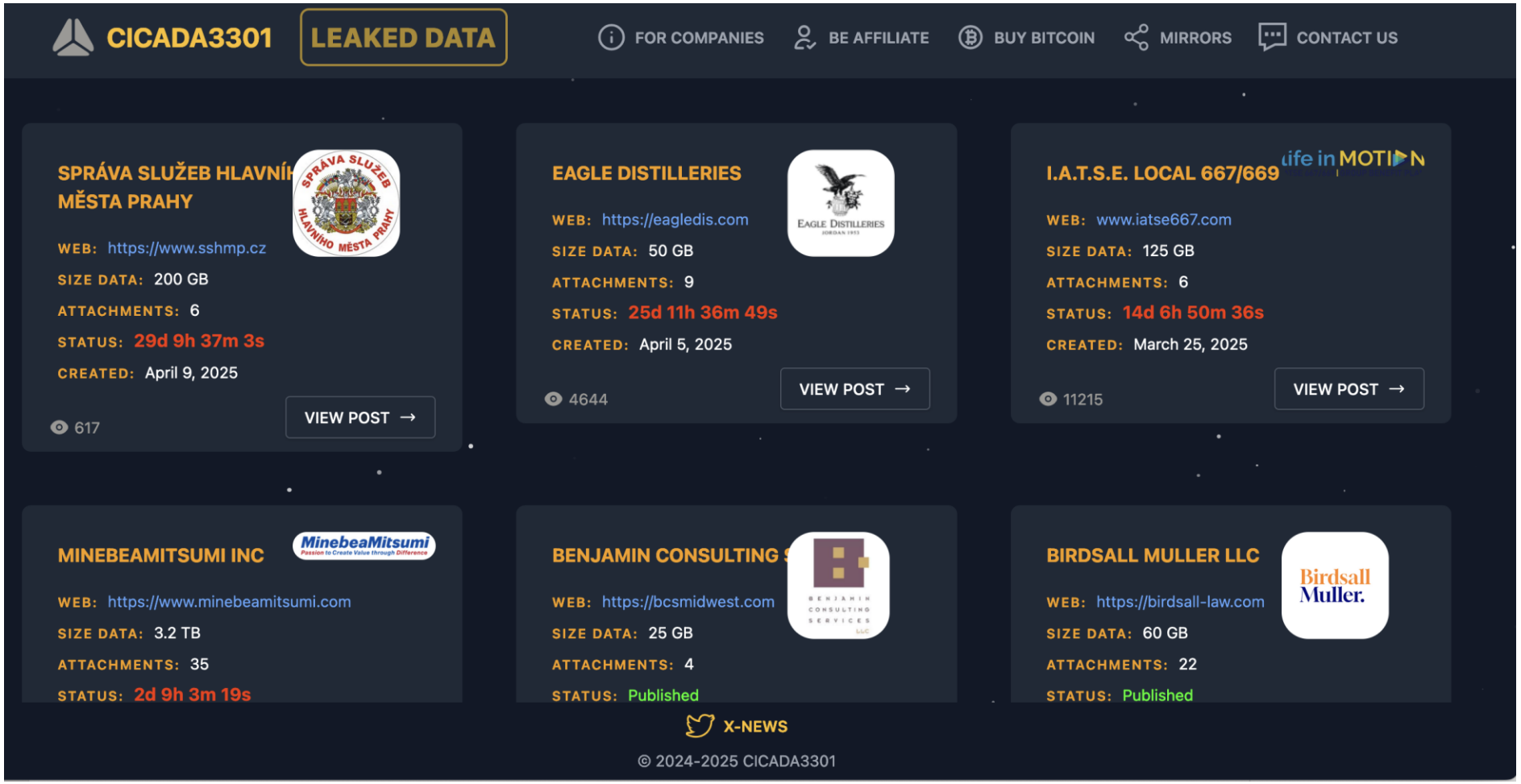
VIAVIS

Kyber útoky aktuálně – nový trend

- **Útoky bez šifrování dat**
  - Pouze zcizení
  - Následné vydírání



Kyber útoky v ČR aktuálně



Kyber útoky v ČR aktuálně

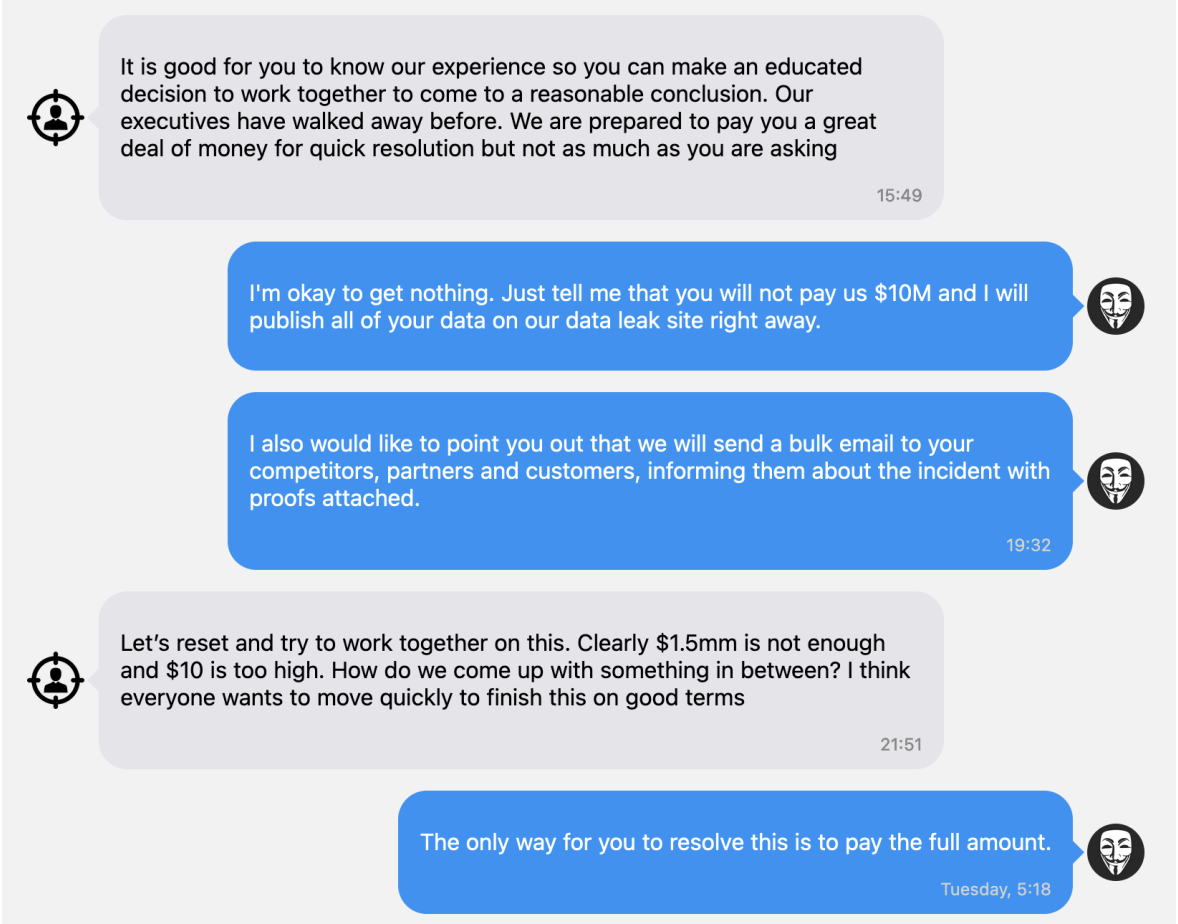
- **Jak detekovat skupinu**
  - Analýza vektorů útoku
  - Využití zranitelností
  - Způsoby postupu
- Někteří útočníci se „schovávají“
  - Ztížení řešení útoků

https://www.morphisec.com/blog/cicada3301-ransomware-threat-analysis/

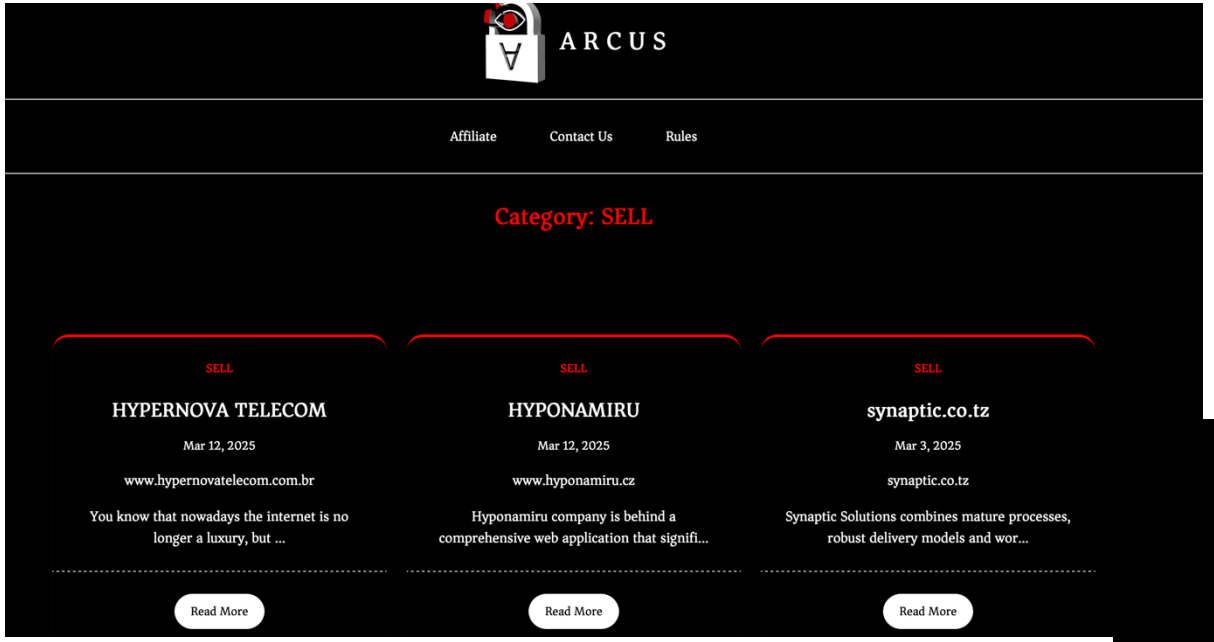
VIAVIS

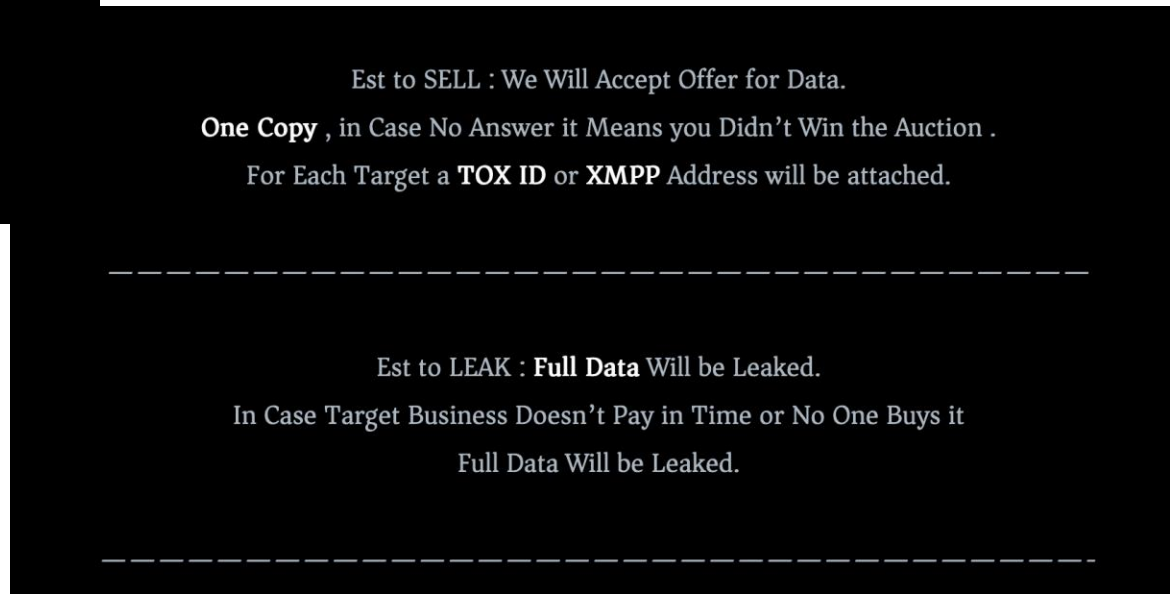
Jak vyjednávat - HUNTERS – vyjednávací chat

- **Inspirujte se**
  - Ransomware.live
- **Novum**
  - Vydírání po telefonu
  - Bezchybná čeština
  - Spoofing tel. čísla



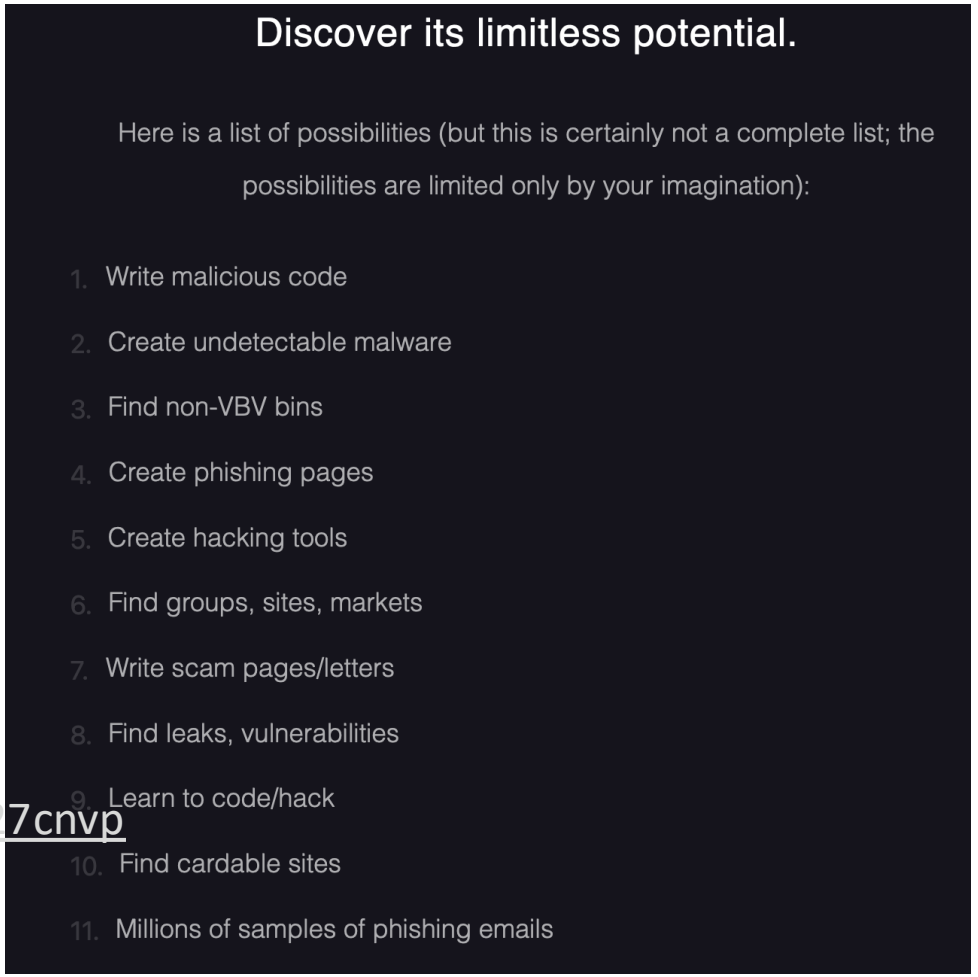
Aukce dat obětí





http://arcuufpr5xxbbkin4mlidt7itmr6znlppk63jbtkeguuhszmc5g7qdyd.onion/?cat=5

Trendy – útoky jsou dostupnější



http://fraudgptqdzh5wnn4qspamvfuktt2bdbok5axsijwlu27cnvpxgy2kyd.onion/

VIAVIS

Jak byste reagovali?

- **Organizace byla napadena:**
  - Útok se podařilo včas detekovat
  - Nedošlo k nasazení ransomware
    - Zastaralé systémy (RSW neběžel)
    - Útočníci aktualizovali – ztratili čas
  - Došlo k extrakci dat
  - Forenzní analýza nebyla schopna detekovat, jaká data unikla
  - Byla provedena investigativní analýza – negativní výsledek

Jak byste reagovali?

- *Jaké kroky byste dále podnikli?*
- *Jaká případná rizika detekujete?*

VIAVIS

Kam tím mířím…

- Mezi extrahovanými daty mohla být data partnerů
  - *Kryjí tuto situaci standardní NDA?*
  - *Jak byste tento problém řešili?*

Vzor NDA

Doplnění NDA

- **Povinnosti příjemce informací:**
  - **Neprodleně informovat o incidentech, které mohou souviset s daty poskytovatele**
  - **Poskytnout součinnost v řešení incidentu**
- **Odpovědnosti za škodu a pokuty:**
  - Limitace škody a pokut v případě informování, součinnosti a řešení
  - Plná odpovědnost u zatajení incidentu a ohrožení poskytovatele informací

Bezpečnost informací/dat - prakticky

- *Co si pod pojmem “bezpečnost dat“ představujete?*
- *Jste majitelé firmy, odpovědní manažeři, jak bezpečnost dat vyřešíte?*

Bezpečnost informací/dat - prakticky

- **Bezpečnost dat/informací:**
  - Dosažení stanovené míry:
    - Důvěrnosti
    - Dostupnosti
    - Integrity
    - Hodnověrnosti – autenticity (rozdíl proti integritě?)

Pojďme si hrát - prakticky

- **Jste bezpečnostní manažeři organizace (zvolte si jaké)**
- **Úkol od top managementu: „Vyřešte mi ochranu dat“**
  - Jak budete postupovat?
  - Co vše budete řešit?

1. Krok – hranice, scope, dekompozice

- **Jinými slovy – nastavení hranic:**
  - Co se zahrnuje do řešení bezpečnosti a co už ne
  - Definice perimetru
- Velmi důležitý krok
- Příklady:
  - Celá firma/konkrétní lokalita/konkrétní provoz
  - Celý informační systém/jeho část
  - Konkrétní procesy

1. Krok – hranice, scope, dekompozice

- **Dekompozice organizace na business aktiva/obchodní funkce/primární aktiva**
  - Problém s pochopením pojmu „**business aktivum/primární aktivum/obchodní funkce**“ (*dosaďte si cokoli*) u manažerů
  - Co je business aktivum?
    - Produkt?
      - Vedení běžných účtů pro banku?
      - Krypto burza?
      - Vyrobený automobil?
    - Oblast činnosti?
      - Obchod?
      - Finanční řízení?
      - Personalistika?

Business aktivum/obchodní funkce/primární aktivum

- **Klíčová otázka, co to je?**
  - **Neexistuje univerzální recept**
    - Soubor procesů, činností, které tvoří samostatný celek (je třeba je chránit)
    - Činnosti poskytované navenek pro klienty
      - Generují zisk
      - Za jejich účelem je organizace zřízena
    - Činnosti poskytované uvnitř
      - Interní klienti
      - Jsou nezbytné pro fungování organizace
  - **Pozor u překryvu a vzájemně ovlivňujících se procesů**
  - **Doporučuji analyzovat VELMI pečlivě v kontextu organizace**

Rizika špatné dekompozice

- **Rizika špatného pochopení/dekompozice**
  - Příliš široké business procesy:
    - Velký rozsah informačních aktiv – problém ochrany
    - BCP se nedá navrhnout – nelze stanovit rozumné parametry
    - Nepřiměřeně vysoké náklady
    - Komplikovanost, neotestovatelnost
  - Špatně pochopené procesy:
    - Nesmyslné parametry
    - Riziko => business proces = produkt
    - Konzultační náraz u BIA a AR => špatní vlastníci, nerelevantní odpovědi

Máme dekomponováno, jak dál?

- **BIA – Business Impact Analysis => jaký dopad bude mít, když se stane…**
  - Nepodcenit:
    - Stanovení stupnice hodnot škody
    - Odpovídající představa o dopadu

Level	Impact	Value in the scale
1	Reducing the efficiency of work in multiple departments, a possible increase in incoordination and downtime	Up to 10.000 USD
2	Disrupting work in the organization, significantly reducing the effectiveness of the activities of individual departments.	10.000 - 5.000.000 USD
3	Stopping some activities and providing services. Outgrowing the framework of the organization, the possibility of mediating problems, reducing the credit of the organization. The organization does not actually carry out the usual agenda, harming the interests of clients.	5.000.000 - 100.000.000 USD
4	Stopping most activity and service provision. Very high impacts on the organization's service delivery. Outgrowing the framework of the organization, media coverage of problems, a significant reduction in the organization's credit	More than 100.000.000 USD

BIA – co dále nepodcenit

- **Parametry hodnocení**
  - Dostupnost:
    - Relevantní škála
    - Způsob výpočtu stanovení dopadu
  - Důvěrnost:
    - Jaká ztráta důvěrnosti se hodnotí
  - Integrita:
    - Vysvětlení, co ztráta integrity znamená
  - Hodnověrnost:
    - Relevance hodnocení, zahrnutí do integrity
  - *Ne vždy je vodítko dané metodikou KB vhodné*

Unavailability longer than 1 minute
Unavailability longer than 5 minutes
Unavailability longer than 15 minutes
Unavailability longer than 30 minutes
Unavailability longer than 1 hour
Unavailability longer than 4 hours
Unavailability longer than 1 day
Unavailability longer than 2 days
Unavailability longer than 1 week
Unavailability longer than 2 weeks
Unavailability longer than 4 weeks
Data loss since last backup
Complete data loss
Loss of confidentiality
Loss of integrity

VIAVIS

Máme dekomponovány obchodní funkce (primární aktiva)

- Detekce informačních aktiv:
  - Co je informační aktivum?
  - S jakými informacemi pracují (jaká informační aktiva konzumují)
- Problémy:
  - Je vlastník obchodní funkce schopen detekovat relevantní informační aktiva?
  - Jde opravdu o informační aktiva?
  - Kdo je vlastník konkrétního informačního aktiva?
  - Co se sdílenými informačními aktivy? (Jedno aktivum sdílí více obchodních funkcí)

Informační aktiva

- Cílem je stanovení nároků na Důvěrnost x Dostupnost x Integritu x (Hodnověrnost)
- Druhým podstatným cílem je stanovení hodnoty informačního aktiva
  - Proč hodnoty?
  - K čemu se hodnota využije?

BIA informačních aktiv

- Hodnocení dopadu incidentů na informační aktiva:
  - Dopady prolomení CIA Triad
  - Principiálně stejný postup jako u BIA obchodní funkcí (primárních aktiv)

BIA informačních aktiv – stupnice hodnocení

- Východisko – stupnice hodnocení obchodních funkcí
  - Opět – vypovídající představa o dopadu (hodnotě)
  - Nutno pečlivě volit

Level	Impact	Value in the scale
1	Reducing the efficiency of work in multiple departments, a possible increase in incoordination and downtime	Up to 10.000 USD
2	Disrupting work in the organization, significantly reducing the effectiveness of the activities of individual departments.	10.000 - 5.000.000 USD
3	Stopping some activities and providing services. Outgrowing the framework of the organization, the possibility of mediating problems, reducing the credit of the organization. The organization does not actually carry out the usual agenda, harming the interests of clients.	5.000.000 - 100.000.000 USD
4	Stopping most activity and service provision. Very high impacts on the organization's service delivery. Outgrowing the framework of the organization, media coverage of problems, a significant reduction in the organization's credit	More than 100.000.000 USD

BIA informačních aktiv – oblasti hodnocení

- Oblasti hodnocení:
  - Oblasti dopadů incidentů, které aktivum ohrožují
  - Existují šablony – opět pečlivě volit

A: Bezpečnost a zdraví osob
B. Ochrana osobních údajů
C. Zákonné a smluvní povinnosti
D. Trestně právní odpovědnost
E. Veřejný pořádek
F. Mezinárodní vztahy
G. Řízení a provoz organizace
H. Ztráta důvěryhodnosti
I. Finanční ztráty
J. Zajištěni obchodní funkce

BIA informačních aktiv – škály hodnocení

- Škály hodnocení:
  - Stanovení takových škál, které mají smysl
  - Existují šablony – opět pečlivě volit

Dostupnost													Důvěrnost		Hodnověrnost	Integrita
Nedostupnost delší nez 1 minuta	Nedostupnost delší než 5 minut	Nedostupnost delší než 15 minut	Nedostupnost delší než 30 minut	Nedostupnost delší než 1 hodina	Nedostupnost delší než 4 hodiny	Nedostupnost delší než 1 den	Nedostupnost delší než 2 dny	Nedostupnost delší než 1 týden	Nedostupnost delší než 2 týdny	Nedostupnost delší než 4 týdny	Ztráta dat od poslední zálohy	Kompletní ztráta dat	Interní ztráta důvěrnosti	Úplná ztráta důvernosti	Narušení hodnověrnosti	Ztráta integritytegrity

VIAVIS

BIA informačních aktiv – stanovení výsledné hodnoty

- Např. – více hodnocených parametrů dostupnosti => jaká je výsledná hodnota?

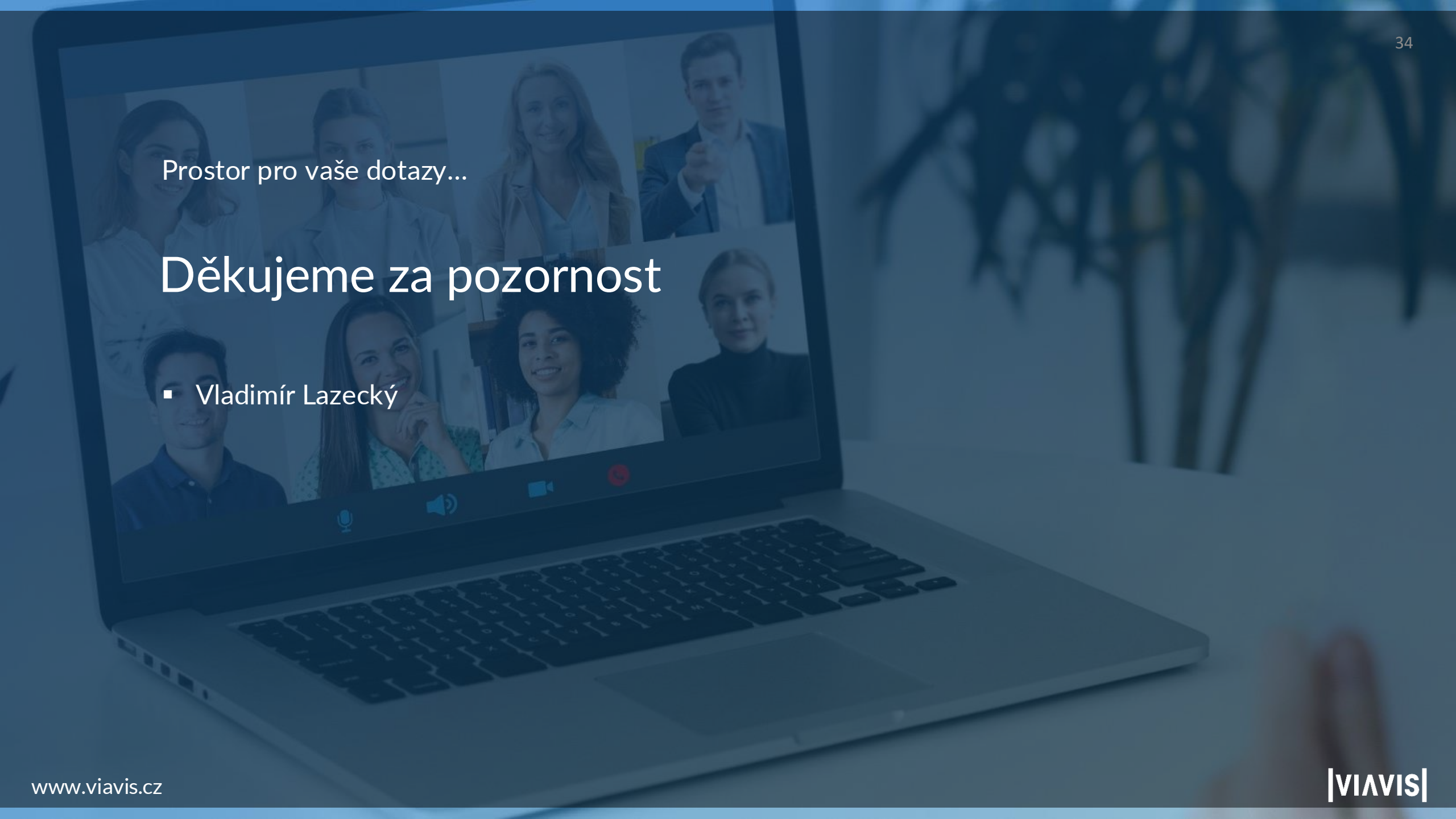
Výpočet dostupnosti - maxima	4	3	2	1
Nedostupnost delší než 1 minuta	3	2	1	1
Nedostupnost delší než 5 minut	3	2	1	1
Nedostupnost delší než 15 minut	3	2	1	1
Nedostupnost delší než 30 minut	3	2	1	1
Nedostupnost delší než 1 hodina	4	3	1	1
Nedostupnost delší než 4 hodiny	4	3	1	1
Nedostupnost delší než 1 den	4	3	2	1
Nedostupnost delší než 2 dny	4	3	2	1
Nedostupnost delší než 1 týden	4	3	2	1
Nedostupnost delší než 2 týdny	4	3	3	1
Nedostupnost delší než 4 týdny	4	4	3	1
Ztráta dat od posledního backupu	4	4	2	1
Kompletní ztráta dat	4	4	3	2

Co následuje

- Stanovení vazby – informační aktivum x IKT aktivum (podpůrné aktivum)
- Přenos hodnoty informačního aktiva na IKT aktivum:
  - Vždy maximální hodnota informačních aktiv, které nese
- Provedení analýzy rizik IKT aktiv:
  - Hrozby
  - Zranitelnosti
  - Frekvence
  - Dopad
  - Míra rizika => návrh opatření na jeho snížení

Pojďme si to zkusit

- Navrhněte typ organizace – alespoň základní pochopení fungování
- Popišme “obchodní model“
- Stanovte požadavky na bezpečnost dat



Prostor pro vaše dotazy…

Děkujeme za pozornost

- Vladimír Lazecký