

|VIAVIS| střežíme podstatné

Jak na bezpečnost dat

Vladimír Lazecký


vladimir.lazecky@viavis.cz


- ✓ 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
📄 **Discovery Date:** 2025-10-19
🚩 **Estimated Attack 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)...

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	Secretaría 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

Kyber útoky v ČR aktuálně

The screenshot shows a web application interface with a sidebar on the left and a main content area. The sidebar includes a 'World Clock' section with times for Los Angeles, New York, London, Paris, Moscow, Beijing, and Tokyo, and a 'Visitors' section showing 14,959 visitors in the last 24 hours and 91,732 in the last 7 days. The main content area is titled 'Companies' and features a navigation bar with filters: 'All 273', 'Awaiting 7', 'Stocks 23', 'Unicorn 29', 'US 135', 'Europe 61', 'Asia 30', 'Exfiltrated 261', and 'Encrypted 184'. Below this, there are four company entries: TEDOM (Czechia, 1d 17h 09m), SmartLynx Airlines SIA (Latvia, 1/1 disclosures), ICBC (London) (United Kingdom, 7/7 disclosures), and Blackmon Mooring (United States of America, 2d 17h 09m). Each entry shows revenue, employee count, and disclosure status. To the right, a 'Disclosures' section shows 'All Data' with a 'View' button and '2.1 TB · 1,402,253 files'.

Companies

All 273 ⚡ Awaiting 7 Stocks 23 Unicorn 29 US 135 Europe 61 Asia 30 Exfiltrated 261 Encrypted 184

Companies

News

World Clock
Los Angeles 10:49 PM -1d
New York 01:49 AM
London 06:49 AM
Paris 07:49 AM
Moscow 08:49 AM
Beijing 01:49 PM
Tokyo 02:49 PM

Visitors
Last 24 hours
14,959
Last 7 days
91,732

TEDOM 1d 17h 09m
Czechia
Revenue \$100M Employees 730 Disclosures 0/1

SmartLynx Airlines SIA
Latvia
Revenue \$150M Employees 1,000 Disclosures 1/1

ICBC (London)
United Kingdom
Revenue \$250M Employees 500 Disclosures 7/7

Blackmon Mooring 2d 17h 09m
United States of America
Revenue \$322.2M Employees 1,572 Disclosures 0/1

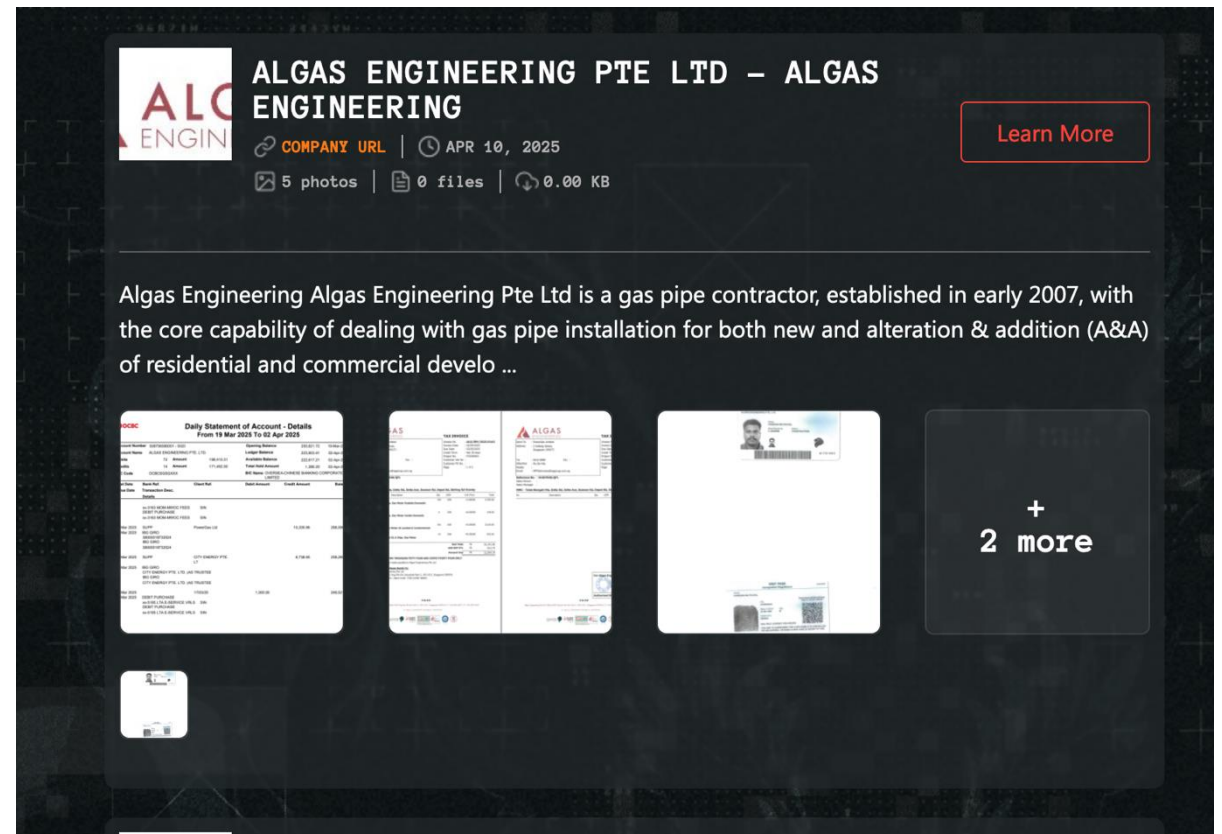
Disclosures

All Data
View 2.1 TB · 1,402,253 files

Kyber útoky aktuálně – nový trend

✓ Útoky bez šifrování dat

- ✓ Pouze zcizení
- ✓ Následné vydírání



Kyber útoky v ČR aktuálně

CICADA3301 **LEAKED DATA** [FOR COMPANIES](#) [BE AFFILIATE](#) [BUY BITCOIN](#) [MIRRORS](#) [CONTACT US](#)

- SPRÁVA SLUŽEB HLAVNÍHO MĚSTA PRAHY**
WEB: <https://www.sshmp.cz>
SIZE DATA: 200 GB
ATTACHMENTS: 6
STATUS: 29d 9h 37m 3s
CREATED: April 9, 2025
617 views
[VIEW POST →](#)
- EAGLE DISTILLERIES**
WEB: <https://eagledis.com>
SIZE DATA: 50 GB
ATTACHMENTS: 9
STATUS: 25d 11h 36m 49s
CREATED: April 5, 2025
4644 views
[VIEW POST →](#)
- I.A.T.S.E. LOCAL 667/669**
WEB: www.iatse667.com
SIZE DATA: 125 GB
ATTACHMENTS: 6
STATUS: 14d 6h 50m 36s
CREATED: March 25, 2025
11215 views
[VIEW POST →](#)
- MINEBEAMITSUMI INC**
WEB: <https://www.minebeamitsumi.com>
SIZE DATA: 3.2 TB
ATTACHMENTS: 35
STATUS: 2d 9h 3m 19s
- BENJAMIN CONSULTING SERVICES**
WEB: <https://bcsmidwest.com>
SIZE DATA: 25 GB
ATTACHMENTS: 4
STATUS: Published
- BIRDSALL MULLER LLC**
WEB: <https://birdsall-law.com>
SIZE DATA: 60 GB
ATTACHMENTS: 22
STATUS: Published

X-NEWS
© 2024-2025 CICADA3301

✓ Jak detekovat skupinu

- ✓ Analýza vektorů útoku
- ✓ Využití zranitelností
- ✓ Způsoby postupu

✓ Někteří útočníci se „schovávají“

- ✓ Ztížení řešení útoků

Decoding the Puzzle: Cicada3301 Ransomware Threat Analysis



Michael Gorelik · 03 Sep 2024 · 3 min read

[Morphisec Labs](#)



In the rapidly evolving landscape of cybersecurity threats, a new adversary has emerged, drawing inspiration from one of the internet's most enigmatic puzzles—Cicada3301. This new threat, dubbed Cicada3301 ransomware, was identified in a Morphisec customer environment just a week ago after bypassing a leading endpoint and detection and response (EDR) provider

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

Jak vyjednávat - HUNTERS – vyjednávací chat

✓ Inspirujte se

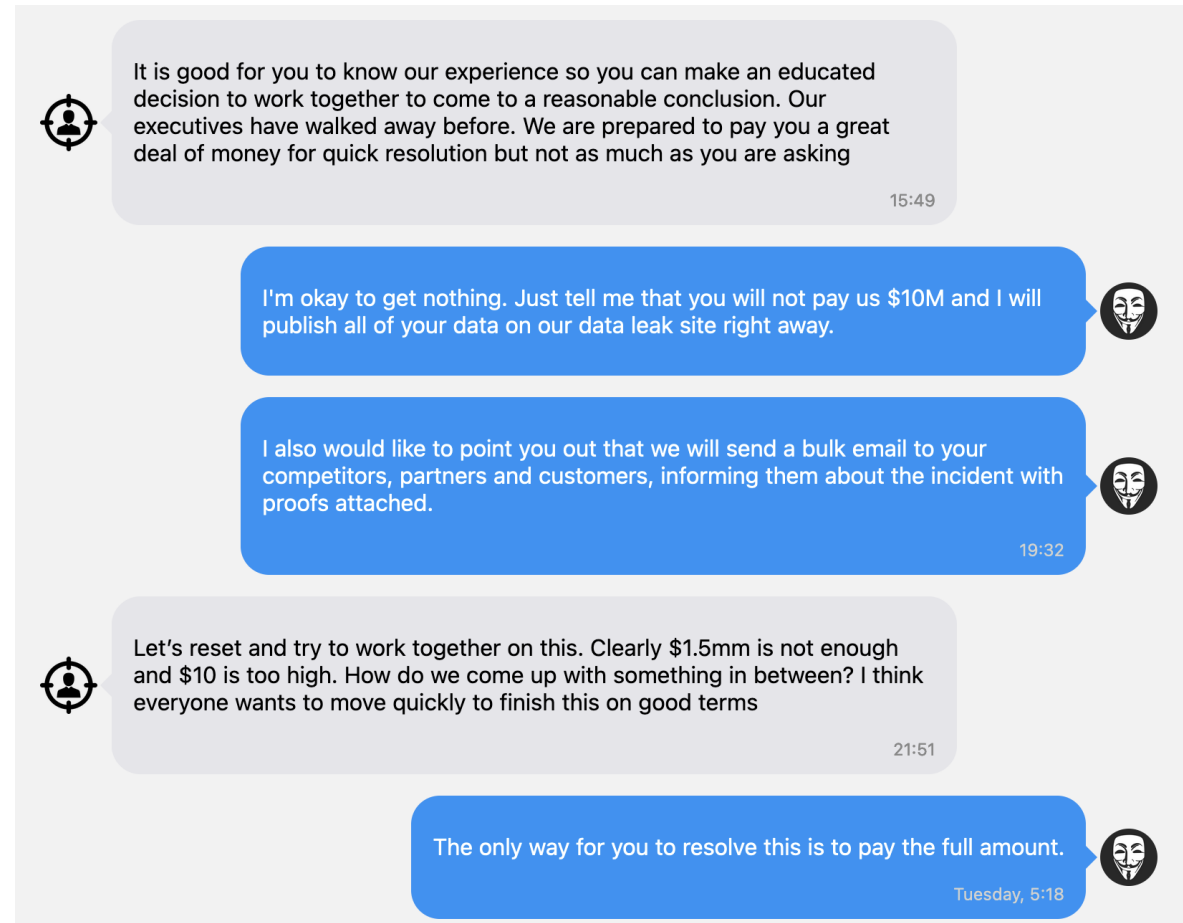
✓ Ransomware.live

✓ Novum

✓ Vydírání po telefonu

✓ Bezchybná čeština

✓ Spoofing tel. čísla



Aukce dat obětí

The screenshot shows the ARCUS website interface. At the top, there is a logo for ARCUS and navigation links for 'Affiliate', 'Contact Us', and 'Rules'. Below this, the category 'Category: SELL' is displayed in red. Three auction listings are shown in a grid:

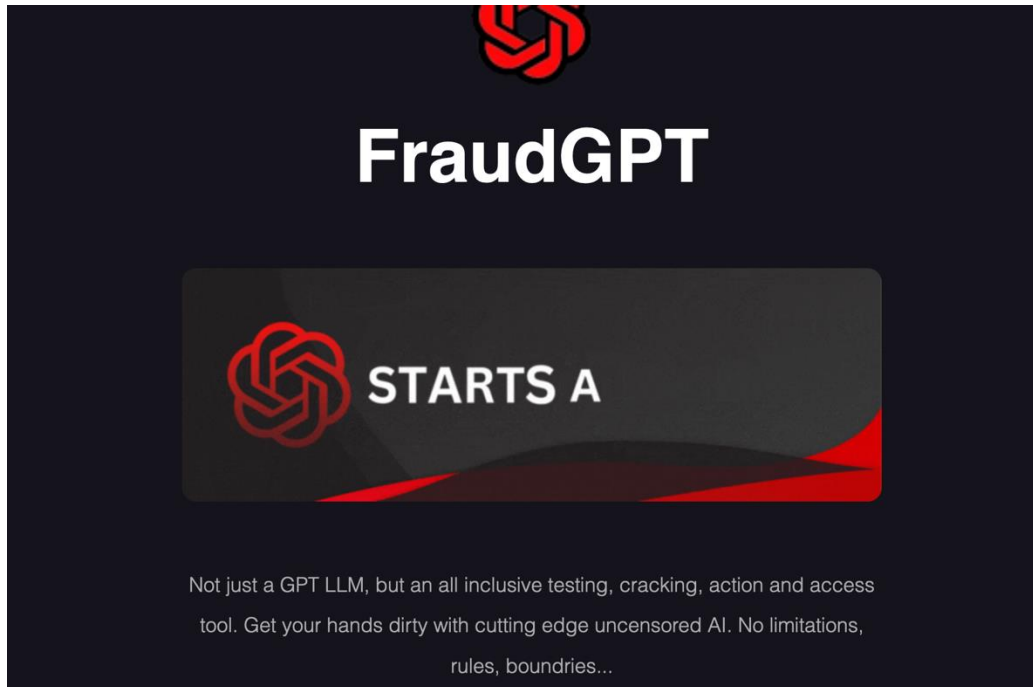
- HYPERNOVA TELECOM**: Mar 12, 2025, www.hypernovatelecom.com.br. Description: "You know that nowadays the internet is no longer a luxury, but ..."
- HYPONAMIRU**: Mar 12, 2025, www.hyponamiru.cz. Description: "Hyponamiru company is behind a comprehensive web application that signifi..."
- synaptic.co.tz**: Mar 3, 2025, synaptic.co.tz. Description: "Synaptic Solutions combines mature processes, robust delivery models and wor..."

Each listing has a 'Read More' button at the bottom.

Est to SELL : We Will Accept Offer for Data.
One Copy , in Case No Answer it Means you Didn't Win the Auction .
For Each Target a **TOX ID** or **XMPP** Address will be attached.

Est to LEAK : **Full Data** Will be Leaked.
In Case Target Business Doesn't Pay in Time or No One Buys it
Full Data Will be Leaked.

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



FraudGPT

STARTS A

Not just a GPT LLM, but an all inclusive testing, cracking, action and access tool. Get your hands dirty with cutting edge uncensored AI. No limitations, rules, boundaries...

[http://fraudgptqdzh5wnn4qspamvfuktt2bdbok5axsijwlu27cnvp
xgy2kyd.onion/](http://fraudgptqdzh5wnn4qspamvfuktt2bdbok5axsijwlu27cnvp
xgy2kyd.onion/)

Discover its limitless potential.

Here is a list of possibilities (but this is certainly not a complete list; the possibilities are limited only by your imagination):

1. Write malicious code
2. Create undetectable malware
3. Find non-VBV bins
4. Create phishing pages
5. Create hacking tools
6. Find groups, sites, markets
7. Write scam pages/letters
8. Find leaks, vulnerabilities
9. Learn to code/hack
10. Find cardable sites
11. Millions of samples of phishing emails

✓ 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?*

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

Vzor 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

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

✓ Bezpečnost dat/informací:

✓ Dosažení stanovené míry:

- ✓ Důvěrnosti
- ✓ Dostupnosti
- ✓ Integrity
- ✓ Hodnověrnosti – autenticity (rozdíl proti integritě?)

- ✓ 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**“
(*dosadte si cokoli*) u manažerů

✓ Co je business aktivum?

✓ Produkt?

✓ Vedení běžných účtů pro banku?

✓ Krypto burza?

✓ Vyrobený automobil?

✓ Oblast činnosti?

✓ Obchod?

✓ Finanční řízení?

✓ Personalistika?

✓ 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 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

✓ 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

✓ 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)

- ✓ 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?

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

✓ 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

✓ 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. Zajištění obchodní funkce

✓ Škály hodnocení:

- ✓ Stanovení takových škál, které mají smysl
- ✓ Existují šablony – opět pečlivě volit

Dostupnost											Důvěrnost		Hodnověrnost	Integrita		
Nedostupnost delší než 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 důvěrnosti	Narušení hodnověrnosti	Ztráta integrity

✓ 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

- ✓ 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

- ✓ Navrhňte typ organizace – alespoň základní pochopení fungování
- ✓ Popište “obchodní model“
- ✓ Stanovte požadavky na bezpečnost dat

Prostor pro vaše dotazy...

Děkujeme za pozornost

- Vladimír Lazecký