



Analýza rizik

Vladimír Lazecký

vladimir.lazecky@viavis.cz

✓ Aktuálně z kyber světa

✓ Analýza rizik

✓ Praktický příklad

Stav Wall of Shames 27.11.2025

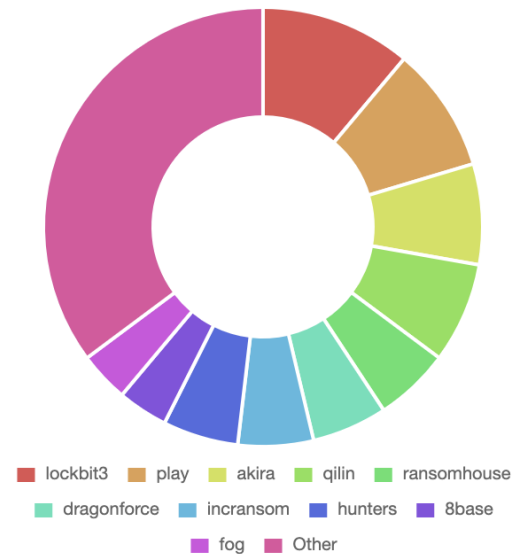
3

54 victims for Czechia

 [83 CISRTs/CERTs](#) listed

 [Country statistics](#)


Top 10 Groups



Oběti – útoky na zranitelnosti










4

Znojma Czechia
Incransom




Discovery Date: 2025-11-12

Subject of activity Main activity comprehensive administration in the area of housing owned by...












atg.cz
Warlock




Discovery Date: 2025-11-06

No description provided....












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 ...



EU schválila mírnější podobu Chat Control. Česko hlasovalo proti, přesto přijdeme o část soukromí



Martin Chroust

26. listopadu 2025

Rada EU dnes překvapivě schválila kontroverzní zákon **Chat Control 2.0**, který je hlavní zbraní eurozóny v boji proti dětské pornografii. Kontroverzní zákon známý pod zkratkou CSAM měl velké množství kritiků a dlouhodobě mu chyběla potřebná podpora, přičemž mezi ty nejhlasitější patřilo Španělsko a Německo. Právě Německo nakonec dalo celému projektu zelenou, což je smutný den pro všechny, kteří si váží svého soukromí. Česko bylo dlouhodobě proti jeho přijetí, to však na celé věci nic nemění. Poskytovatelé messengerů v Evropě budou moci plošně monitorovat soukromé konverzace, byť je to v kompromisní verzi návrhu popsáno jako **povinně „dobrovolná“ činnost**.

<https://mobilmania.zive.cz/clanky/eu-schvalila-mirnejsi-podobu-chat-control-cesko-hlasovalo-proti-presto-prijdeme-o-cast-soukromi/sc-3-a-1363811/default.aspx>

✓ Zákon o zadávání veřejných zakázek

✓ Vylučuje diskriminaci

✓ Zákon o kybernetické bezpečnosti

✓ Varování NÚKIB

✓ Co s tím?

VAROVÁNÍ

Národní úřad pro kybernetickou a informační bezpečnost, se sídlem Mučednická 1125/31, 616 00 Brno (dále jen „Úřad“), podle § 12 odst. 1 zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, ve znění pozdějších předpisů (dále jen „zákon o kybernetické bezpečnosti“) vydává toto

varování

před hrozbou v oblasti kybernetické bezpečnosti spočívající

1. v předávání systémových a uživatelských dat do Čínské lidové republiky, na území zvláštních administrativních oblastí či subjektům usídleným na území Čínské lidové republiky nebo zvláštních administrativních oblastí, a
2. ve vzdálené správě technických aktiv vykonávané z území Čínské lidové republiky, zvláštních administrativních oblastí či ze strany subjektů usídlených na území Čínské lidové republiky nebo zvláštních administrativních oblastí.

- ✓ *Co si pod tímto pojmem představíte?*
- ✓ *Jak chápete pojem riziko?*
- ✓ *Proč v oblasti bezpečnosti mluvíme o analýze rizik?*

- ✓ Většina systémů managementu informační/kybernetické a regulativů bezpečnosti je postavena na principu řízení rizik
 - ✓ ISMS, DORA, NIS2, GDPR...
- ✓ Proč?
- ✓ Co je bezpečnost?

Nudné základní pojmy – bez nich se nepohneme

9

✓ Bezpečnost => schopnost odolávat hrozbám

- ✓ Bezpečnost není absolutní stav
- ✓ Bezpečnost je daná mírou schopnosti odolávat
- ✓ Celková míra bezpečnosti => daná nejnižší mírou

✓ Podmínka nutná:

- ✓ Detekce hrozeb
- ✓ Stanovení míry „odolnosti“

✓ Bezpečnost dat/informací => zajištění stanovené míry Dostupnosti x Důvěrnosti x Integrity

✓ DORA přidává Hodnověrnost (Autenticitu)

✓ Klíčové otázky:

✓ Jak stanovit míru, která dává smysl?

✓ Jak jí dosáhnout, když informace/data mají nehmotnou podstatu?

Odpovědí je analýza rizik

11

✓ Definicí je mnoho => záleží na pohledu

✓ Pro pochopení jde o identifikaci:

- ✓ Hodnot (Aktiv)
- ✓ Co je může poškodit (Hrozby)
- ✓ Jaké je riziko, že k poškození dojde
- ✓ Jak dané riziko mitigovat

✓ Neformální přístup

- ✓ Jednoduchá neformální úvaha

- ✓ *Kdy je vhodná?*

- ✓ *Jaké má výhody?*

- ✓ *Jaké má nevýhody?*

- ✓ Zkusme si – analýza rizik pro váš mobilní telefon

✓ Formální přístup

- ✓ Analýza rizik celého systému a každého jeho prvku
- ✓ Postup přesně dokumentovaným a metodickým přístupem
 - ✓ Metodiky CRAMM, RAMSES, RANIT...
- ✓ *Kdy je vhodná?*
- ✓ *Jaké má výhody?*
- ✓ *Jaké má nevýhody?*

✓ Kombinovaný přístup

- ✓ Nastavení rozsahu a hranic analýzy
- ✓ Stanovení částí systému pro neformální/formální přístup
- ✓ Nejvyužívanější přístup

✓ Spojuje výhody obou předchozích přístupů

Zpět k základním pojmům - Aktivum

15

- ✓ **Aktivum => vše, co má hodnotu**

- ✓ Má smysl chránit aktiva bez hodnoty?

- ✓ **Babylónská věž aktiv => zmatení pojmů různých regulativů (NIS2/ZKB, ISMS, DORA...)**

- ✓ **Co si představíte pod pojmy:**

- ✓ Primární aktivum

- ✓ Informační aktivum

- ✓ Technické aktivum

- ✓ Podpůrné aktivum

✓ Primární Aktivum (ZKB/NIS2):

- ✓ Je informace nebo služba, která je pro organizaci zásadní a bez které by nemohla plnit své poslání nebo hlavní činnosti
- ✓ Je to zdroj hodnoty, který přímo souvisí s hlavní činností organizace
- ✓ Zahrnují např. data, know-how nebo klíčové obchodní procesy

✓ Primární Aktivum (ZKB/NIS2)

- ✓ Primární aktivum představuje informaci nebo službu, kterou zpracovává nebo poskytuje informační a komunikační systém
- ✓ Tato primární aktiva jsou současně často hodnototvorná pro fungování dané organizace. Jako příklady primárních aktiv lze uvést data, informace nebo poskytované služby

✓ *Přemýšlejte, je takový pohled dostatečný?*

✓ *V čem je výhodný a kde má slabiny?*

✓ Obchodní funkce/Business Asset

- ✓ Služba, která představuje ucelenou soustavu procesů je možné ji posoudit jako celek
- ✓ Obchodní funkce směřující vně:
 - ✓ Vedení běžných účtů
 - ✓ Poskytování úvěrů
- ✓ Obchodní funkce dovnitř:
 - ✓ Finanční řízení
 - ✓ Řízení HR

V čem se liší od ZKB? V čem má výhodu/nevýhodu?

✓ Výhoda „DORA pohledu“

- ✓ Hodnocení rizik nezužuje pouze na IKT systémy
 - ✓ Vrcholový pohled přes obchodní funkci je objektivnější
 - ✓ Lepší pochopitelnost pro vlastníky
 - ✓ Lepší východisko pro hledání míry bezpečnosti

✓ Potřeba vrcholového pohledu => BIA

- ✓ Nastavení hranic (scope) pro AR
- ✓ Volba přístupu (formální/neformální)
- ✓ Stanovení základních bezpečnostních parametrů
- ✓ Získání metrik => finanční pohled
 - ✓ Hledání optima nákladů na bezpečnost x výše škody
- ✓ Stanovení vlastníků a odpovědnosti
- ✓ Identifikace obchodních funkcí závislých na IKT systémech

- ✓ Informační aktivum => data nebo informace, kterou je třeba chránit
 - ✓ *Co tím rozumíte?*
- ✓ Informační aktivum je konzumováno obchodní funkcí
 - ✓ Obchodní funkce potřebuje informační aktiva, jinak není funkční
 - ✓ Jedno informační aktivum může vstupovat do více obchodních funkcí

Podpůrné aktivum (NIS2/ZKB)

22

✓ Podpůrné aktivum:

- ✓ Technické aktivum
- ✓ Zaměstnanci
- ✓ Dodavatele

✓ *Proč se zavádí podpůrné aktivum?*

Podpůrné aktivum (NIS2/ZKB)

23

- ✓ **Podpůrné aktivum nese Primární aktivum**
 - ✓ Mírná nelogičnost
 - ✓ Informace/data nemohou reálně existovat samy o sobě
- ✓ *Přeběhneme – analýza rizik se provádí na Podpůrná aktiva*

✓ Aktivum v oblasti IKT / IKT aktivum => Podpůrné aktivum

✓ HW, SW

✓ IKT funkce/služby

✓ IKT dodavatelé

✓ Lidské zdroje

✓ Lze je stromově strukturovat => vytvářet závislosti

✓ Hodnota

✓ *Jak stanovíme hodnotu aktiva?*

✓ Nároky na:

✓ Dostupnost

✓ Důvěrnost

✓ Integritu

✓ Autenticitu (DORA)

✓ Hrozba:

- ✓ Potenciální událost která může způsobit škodu
- ✓ Využití katalogu hrozeb => NÚKIB, veřejně dostupné katalogy
 - ✓ *Gefährdungskataloge* vydaný Bundesamt für Sicherheit in der Informationstechnik
- ✓ Příklady hrozeb:
 - ✓ Požár
 - ✓ Selhání uživatele
 - ✓ Ransomware útok
 - ✓ Výpadek energie...

- ✓ Zranitelnost => vlastnost aktiva
 - ✓ Slabé místo, které může být využito hrozbou
 - ✓ Příklady zranitelností:
 - ✓ Chyba v SW
 - ✓ Latentní slabiny v procesech...
 - ✓ Citlivost na kolísání napětí
 - ✓ ...

✓ Zranitelnost je daná svou úrovní – analytik nastavuje

Úroveň		Popis
1	Nízká	Zranitelnost neexistuje nebo je zneužití zranitelnosti málo pravděpodobné. Jsou zavedena bezpečnostní opatření, která jsou schopna včas detekovat možné zranitelnosti nebo případné pokusy o jejich zneužití.
2	Střední	Zneužití zranitelnosti je málo pravděpodobné až pravděpodobné. Jsou zavedena bezpečnostní opatření, jejichž účinnost je pravidelně kontrolována. Schopnost bezpečnostních opatření včas detekovat možné zranitelnosti nebo případné pokusy o překonání opatření je omezena. Nejsou známy žádné úspěšné pokusy o překonání bezpečnostních opatření.
3	Vysoká	Zneužití zranitelnosti je pravděpodobné až velmi pravděpodobné. Bezpečnostní opatření jsou zavedena, ale jejich účinnost nepokrývá všechny potřebné aspekty a není pravidelně kontrolována. Jsou známy dílčí úspěšné pokusy o překonání bezpečnostních opatření.
4	Kritická	Zneužití zranitelnosti je velmi pravděpodobné až víceméně jisté. Bezpečnostní opatření nejsou realizována nebo je jejich účinnost značně omezena. Neprobíhá kontrola účinnosti bezpečnostních opatření. Jsou známy úspěšné pokusy překonání bezpečnostních opatření.

✓ Frekvence => jak často se hrozba uplatní

✓ Zkušenost, statistiky

Úroveň		Četnost výskytu hrozby
1	Nízká	Hrozba neexistuje nebo je málo pravděpodobná. Předpokládaná realizace hrozby není častější než jednou za 5 let.
2	Střední	Hrozba je málo pravděpodobná až pravděpodobná. Předpokládaná realizace hrozby je v rozpětí od 1 roku do 5 let.
3	Vysoká	Hrozba je pravděpodobná až velmi pravděpodobná. Předpokládaná realizace hrozby je v rozpětí od 1 měsíce do 1 roku.
4	Kritická	Hrozba je velmi pravděpodobná až víceméně jistá. Předpokládaná realizace hrozby je častější než jednou za měsíc.

Dopad hrozby

Úroveň		Dopad hrozby z hlediska:			
		provozního	poškození aktiva	výpadku služby	finančního
1	Nízká	Snížení efektivity práce ve více odděleních, možný nárůst nekoordinovanosti a prostojů.	do 1%	do 1 hodiny	do 1 000 000 CZK
2	Střední	Narušení činnosti ve Společnosti, výrazné snižování efektivity činnosti jednotlivých oddělení.	do 10%	do 1 dne	1 000 000 CZK-10 000 000 CZK
3	Vysoká	Zastavení některých činností a poskytování služeb. Dopad přerůstá rámec Společnosti. Možnost zprostředkování problémů, snižování kreditu Společnosti. Společnost fakticky nevykonává běžnou agendu, poškozuje zájmy klientů.	do 50%	do 1 týdne	10 000 000 CZK - 100 000 000 CZK
4	Kritická	Zastavení většiny činností a poskytování služeb. Velmi vysoké dopady na poskytování služeb Společnosti. Přerůstání rámce Společnosti, medializace problémů, výrazné snížení kreditu Společnosti.	> 50%	> 1 týden	> 100 000 000 CZK

Výpočet míry rizika

31

✓ $RX = SA * ZX * HC * HD$

- ✓ RX míra rizika;
- ✓ SA hodnota aktiva;
- ✓ ZX hodnota zranitelnosti;
- ✓ HC hodnota četnosti hrozby;
- ✓ HD hodnota dopadu hrozby.

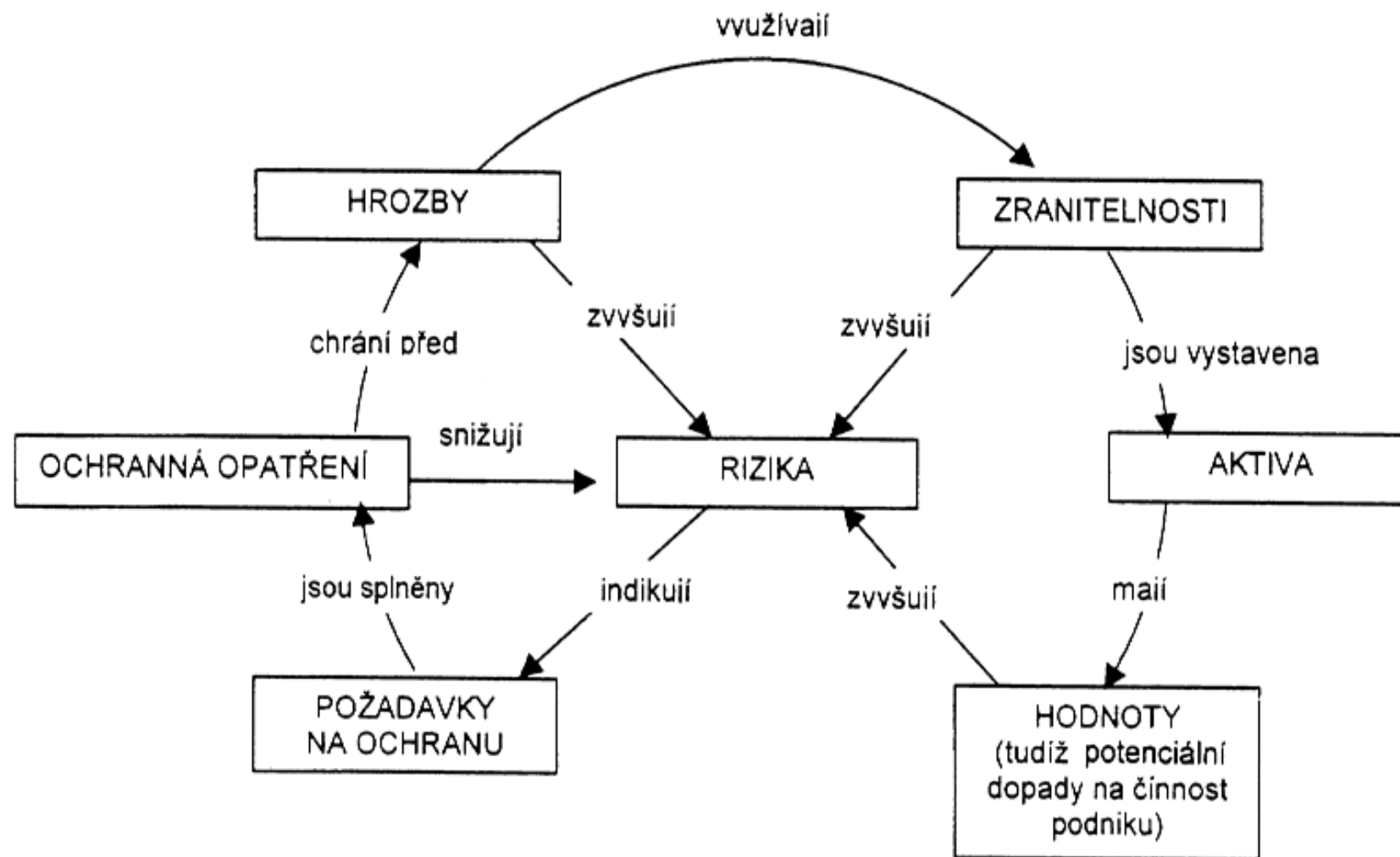
- ✓ **Konkrétní opatření snižující míru rizika**
 - ✓ Školení uživatelů
 - ✓ Antivir, firewall
 - ✓ Popsaný proces
 - ✓ Zálohování znalostí...

- ✓ Každé protiopatření má svou účinnost
 - ✓ Téměř žádné není účinné na 100%...

- ✓ **Riziko, které není pokryto protiopatření**
 - ✓ Vlastník obchodní funkce/primárního aktiva ho akceptuje
 - ✓ Náklady na protiopatření snižující toto riziko jsou neadekvátní
 - ✓ Tolerované riziko musí být zdůvodněno

Základní vztahy – nic složitého 😊

34



- ✓ Nastavení hranic posuzování
- ✓ Volba přístupu
- ✓ Identifikace aktiv
- ✓ BIA – Business Impact Analysis => analýza dopadů
- ✓ Hodnocení rizik
- ✓ Návrh protiopatření
- ✓ Akceptace tolerovaných rizik
 - ✓ Prohlášení o aplikovatelnosti
 - ✓ Plán digitální provozní odolnosti
- ✓ A vše znovu => management rizik

- ✓ **Jinými slovy – nastavení hranic:**
 - ✓ Co se zahrnuje do řešení bezpečnosti a co už ne
 - ✓ Východisko pro definice perimetrů
 - ✓ *Co je perimetr*
- ✓ Velmi důležitý krok
- ✓ Příklady:
 - ✓ Celá firma/konkrétní lokalita/konkrétní provoz
 - ✓ Celý informační systém/jeho část
 - ✓ Konkrétní obchodní funkce

✓ Dekompozice organizace na business assets/obchodní funkce/primární aktiva

✓ Problém s pochopením pojmu „**business aktivum/primární aktivum/obchodní funkce**“
(*dosad'te 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
- ✓ Bezpečnost se téměř 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

- ✓ **Dekompozice obchodních funkcí na smysluplné procesní kroky**

- ✓ Identifikace Informačních aktiv

- ✓ Procesní kroky je konzumují (potřebují je)

- ✓ Identifikace vlastníků Informačních aktiv

- ✓ Identifikace IKT aktiv (podpůrných aktiv)

- ✓ Informační aktiva jsou na IKT aktivech závislá

- ✓ Nutná dokumentace vzájemných vazeb

Identifikace aktiv – logičtější přístup DORA

41

Skupinové aktivum	Id	Informační aktivum	Vlastník IA	Typ IA
	1.1.1.	Osobní data, scan dokladů, email, telefon	XY	PD
	1.1.1.	Osobní data, scan dokladů, email, telefon	XY	PD

Id IKT aktiva	IKT aktivum	Vlastník	Hodnota IKT aktiva	Lokalita
1,1	IKTA1	qq		
3,8	IKTA2	qq		

Máme dekomponováno, jak dál?

42

✓ 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

BIA obchodních funkcí

44 / 36

Obchodní funkce	OF1	OF2		
Hodnota obchodní funkce	3	3	0	0
Kategorizace	Z/D	Z/D		
Hodnocení dopadů				
Nedostupnost delší než 1 minuta	1	1		
Nedostupnost delší než 5 minut	1	1		
Nedostupnost delší než 15 minut	1	1		
Nedostupnost delší než 30 minut	1	1		
Nedostupnost delší než 1 hodina	2	2		
Nedostupnost delší než 4 hodiny	2	2		
Nedostupnost delší než 1 den	2	2		
Nedostupnost delší než 2 dny	2	2		
Nedostupnost delší než 1 týden	3	3		
Nedostupnost delší než 2 týdny	3	3		
Nedostupnost delší než 4 týdny	4	4		
Ztráta dat od posledního backupu	2	2		
Kompletní ztráta dat	4	4		
Hodnota dostupnosti	3	3		
Ztráta důvěrnosti - interní	3	3		
Ztráta důvěrnosti - úplná	4	4		
Hodnota důvěrnosti	3	3		
Ztráta integrity	3	3		
RTO - maximální doba přípustného výpadku	2h	2h		
RPO - maximální přípustná ztráta dat	1h	1h		

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
Výpočet důvěrnosti - maxima	4	3	2	1
Ztráta důvěrnosti - interní	4	3	2	1
Ztráta důvěrnosti- úplná	4	4	3	1

- ✓ Validace škody – dopadu na obchodní funkci jako celek
- ✓ Stanovení parametrů RTO/RPO
- ✓ Dopad na řešení bezpečnosti => náklady, smluvní vztahy, personální zajištění...

✓ Proč?

- ✓ Stanovení nároků na CIA
- ✓ Stanovení hodnoty informačních aktiv => hodnotu přebírají IKT aktiva

✓ 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)

- ✓ 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	

BIA informačních aktiv – stanovení výsledné hodnoty

51 / 36

✓ 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

BIA informačních aktiv – stanovení výsledné hodnoty

52 / 36

Hodnoty Informačního aktiva					
	Dostupnost	Důvěrnost	Hodnověrnost	Integrita	Celková hodnota
Hodnota	1	4	1	4	4
Typ Inf. aktiva	PD,FD				
Klasifikace	Citlivé s vysokými nároky na integritu a standardními požadavky na hodnověrnost				
Vlastník	ccc				
Hodnoceno	10.06.2025				

Analýza rizik nad IKT aktivy

53 / 36

IKT aktivum	Hrozba	Hodnota	Zranitelnost	Četnost	Dopad	Míra rizika	Protiopatření	Efektivita	Zbytkové riziko
Server	Výpadek energie	3	2	3	1	18	P1	0,9	1,8
	Chyba administrátora	3	1	3	2	18	P2	0,9	1,8
	Krádež	3	3	1	3	27	P3	0,8	5,4
	Požár serverovny	3	3	1	2	18	P4	0,8	3,6
	Chyba dodavatele	3	4	1	2	24		0,9	2,4
		3	2	1	2	12		0,9	1,2
		3	2	1	2	12		0,9	1,2

Pojďme si to zkusit

54 / 36

- ✓ Navrhněte typ organizace – alespoň základní pochopení fungování
- ✓ Popište “obchodní model”
- ✓ Proveďte analýzu rizik

Prostor pro vaše dotazy...

Děkujeme za pozornost

- Vladimír Lazecký