GAPP
SYSTEM

NIS2, jeho dopad na organizace z pohledu infrastruktury a návrhy řešení

Jan Dupač

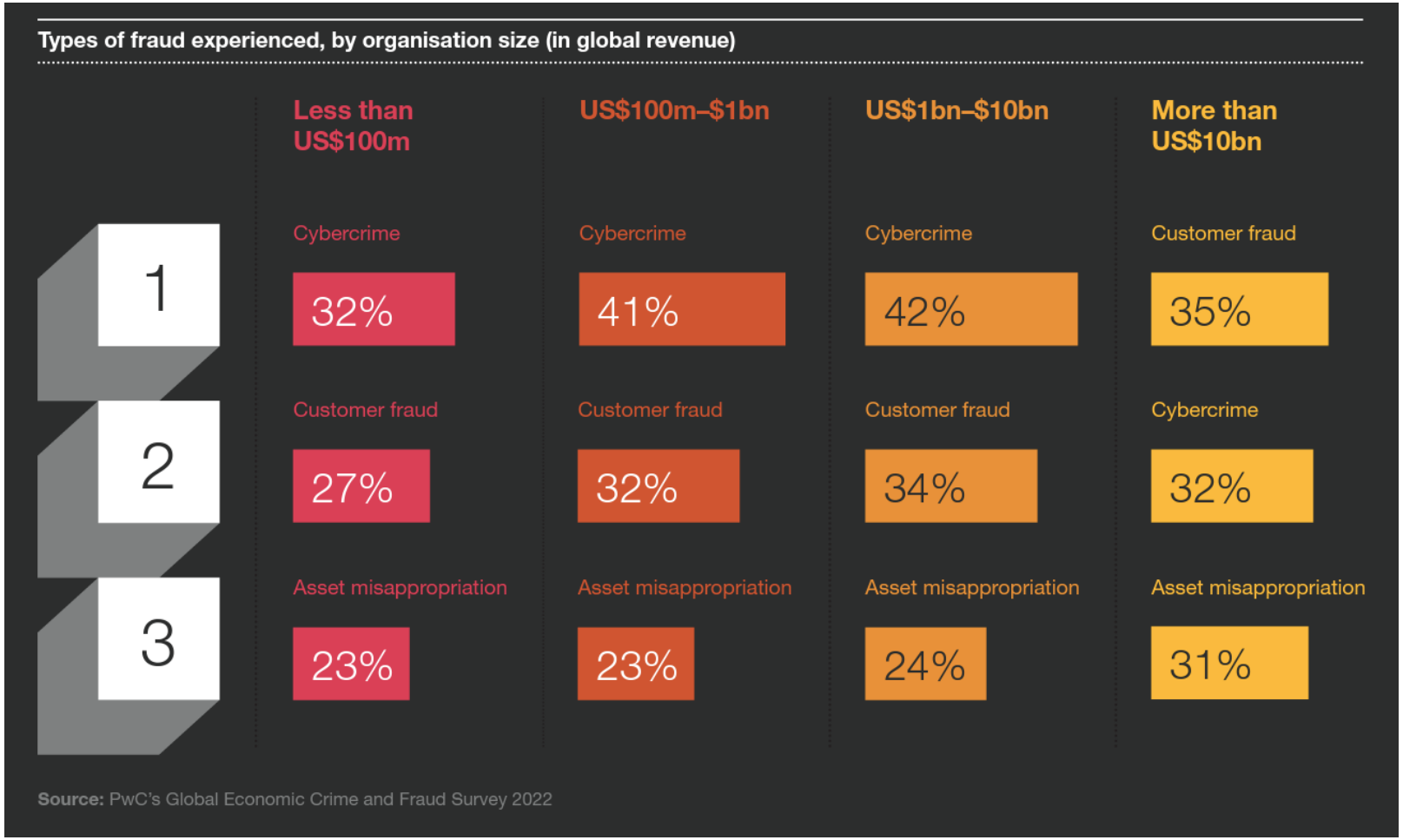
Kybernetické útoky

Ve světovém měřítku neustále roste počet kyberútoků na společnosti.

Studie PwC Global Economic Crime and Fraud 2022 z konce loňského roku poukázala na fakt, že téměř polovina firem v posledních dvou letech zaznamenala nějaký typ hospodářské kriminality. Nejohroženější jsou přitom společnosti podnikající v technologiích, mediálním prostoru či telekomunikacích, vyplývá ze studie mezi 1300 top manažery v 53 zemích světa.

Zkušenost s útokem přiznávají téměř dvě třetiny (64 %) firem, které se zabývají technologiemi, komunikací nebo působí v mediálním prostoru. Všem bez výjimky pak rostou ztráty způsobené takovými útoky.

Studie od společnosti PWC z roku 2022



Nejvíce útoků v posledních dvou letech se týkalo především kyberprostoru.

Jak je na tom ČR

Česko je pátou evropskou zemí, na kterou cílí kyberútoky nejčastěji

„Česká republika se v dubnu dále držela mezi nebezpečnými zeměmi, patřila jí celosvětově 26. pozice a 5. mezi evropskými zeměmi“ podle Check Pointu.

V praxi to znamená, že jedna tuzemská organizace čelila v průměru 1800 kyberútoků za týden, přitom evropský průměr se pohybuje okolo hranice 1100 útoků za týden.

Ještě předloni na jaře se přitom Česko chlubilo 87. pozicí, patřilo tedy spíše mezi ty bezpečnější země.

Co je NIS2?

- Směrnice Evropského parlamentu a Rady (EU) o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii (Network and Information Security).

- NIS2 se nezabývá IS, ale poskytovanými službami a vším, co je podporuje.

- NIS2 je jen směrnice, ne nařízení, tzn., definuje cíle a směr, jak se k nim dobrat, přičemž konkrétní požadavky budou stanoveny příslušnými národními legislativami (nový ZKB, nové vyhlášky o KB a další – od 3Q/2024).

- Implementace všech předpisů se bude dít skokově v jedné novelizační linii.

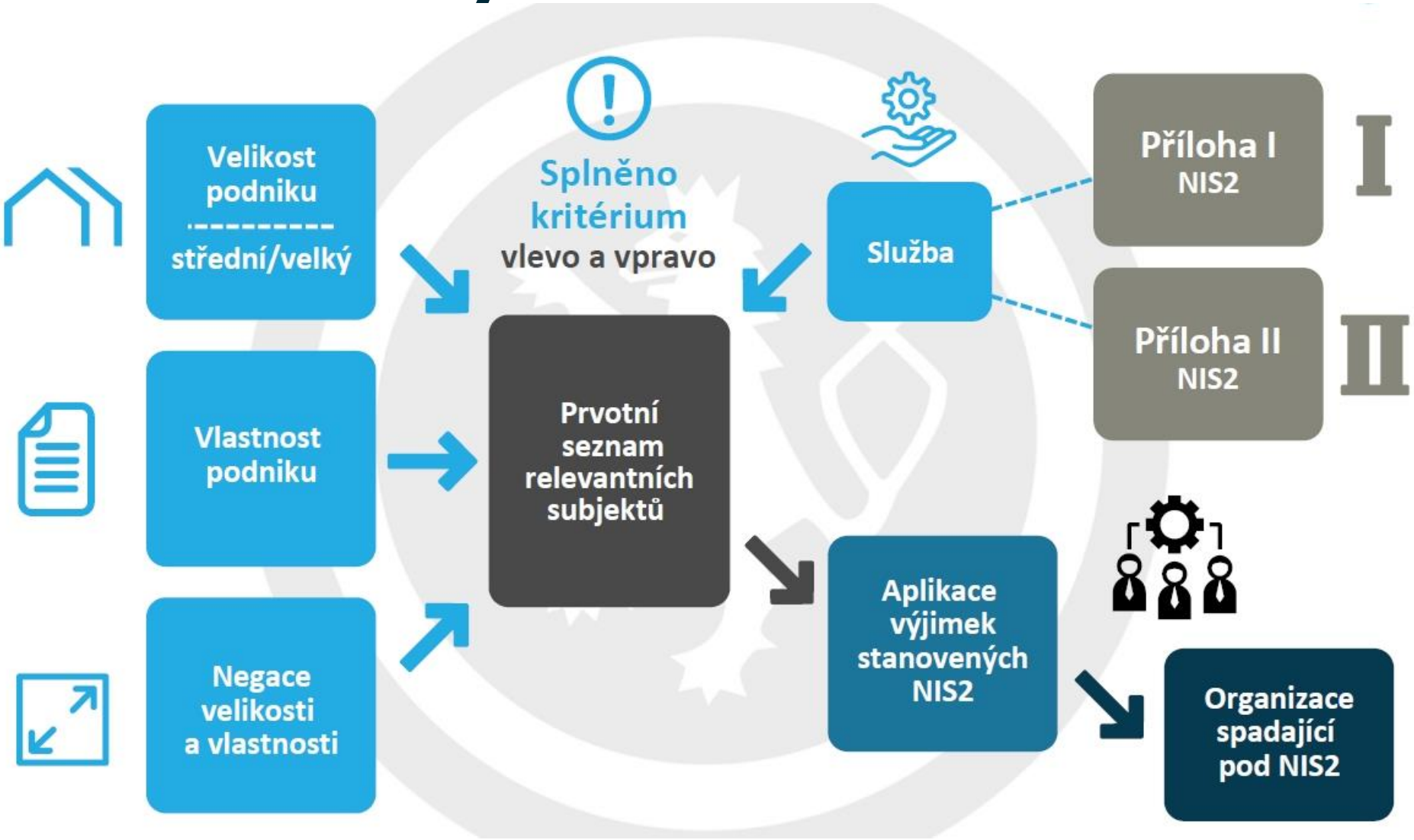
Čím se liší od NIS1?

- Na rozdíl od NIS1 přibydou novinky – kontrola dodavatelských řetězců, certifikace procesů a schémat.
- Povinnosti hlášení bezpečnostních incidentů.
- Povinnosti významného dodavatele poskytovateli regulované služby - jsou prověřováni dle předpisů o rizikovosti dodavatele (Huawei, Kaspersky).
- Míra kontrol dodržování - NÚKIB má kapacity na spravování max. 1000 subjektů, vzniknou soukromí kontroloři.
- Drastické pokuty viz GDPR, navíc je možné i pozastavení licence či certifikace služby, nebo omezení jednacích práv odpovědných osob za KB.
- Aktuálně regulováno cca 400 povinných osob, nově půjde o minimálně 6000.

Koho se NIS2 týká?

- Všech organizací >50 zaměstnanců nebo >10M Eur obrat, zároveň poskytujících regulovanou službu.
- Orgánů veřejné správy (včetně obcí nad 125.000 obyvatel a obcí z rozšířenou působností do 125.000 obyvatel).
- Výlučných poskytovatelů služby, nebo služby s významným dopadem při jejím narušení.
- Kdo je povinný dle směrnice CER (kritická infrastruktura dle krizového zákona), je povinný i dle NIS2.
- Seznam regulovaných služeb bude definován Vyhláškou o regulovaných službách.
- Cloudoví poskytovatelé spadají pod národní legislativu státu, na jehož území jsou umístěna data, nebo dle úrovně dopadu incidentu.
- Poskytovatel regulované služby je jakákoliv povinná osoba, provozující základní službu, kritickou infrastrukturu, významný informační systém, všechny subjekty z NIS2 a nazývá se PRS.

Koho se NIS2 týká?



Koho se NIS2 týká?

SLUŽBY UVEDENÉ V PŘÍLOZE I

Subjekty poskytující služby uvedené v příloze I níže a splňující podmínku „velký podnik" dle doporučení Komise (EU) 2003/361/EC budou regulovány vždy v režimu „essential".

ENERGETIKA

Provozovatelé distribuční a přenosové soustavy, výrobci a prodejci elektrické energie, nominovaní organizátoři trhu s elektřinou, provozovatelé dobíjecích stanic spolu s poskytovateli elektromobility.

Subjekty poskytující službu dálkového vytápění nebo chlazení.

Provozovatelé ropovodů, zařízení na těžbu, rafinaci a zpracování ropy, skladovacích a přenosových zařízení, ústřední správci zásob.

Obchodníci s plynem, distributoři plynu, přepravci plynu, výrobci plynu a poskytovatelé uskladňování plynu.

Provozovatelé výroby, skladování a přepravy vodíku. Doposud však není implementováno do českého právního řádu.

DOPRAVA

Komerční letečtí dopravci, řídicí orgány letišť a subjekty provozující pomocná zařízení v rámci letišť, provozovatelé kontroly řízení provozu.

Provozovatel dráhy celostátní nebo regionální anebo veřejné přístupné vlečky a dopravce provozující na těchto drahách drážní dopravu.

Předmětné předpisy se vztahují na námořní přístavy a pro Českou republiku tedy nejsou relevantní.

Silniční orgány odpovědné za plánování, kontrolu a správu silnic spadajících do jejich územní působnosti, poskytovatelé služeb ITS.

BANKOVNICTVÍ

Sektor bankovnictví je regulován nařízením DORA.

INFRASTRUKTURA FIN. TRHŮ

Sektor infrastruktura finančních trhů je regulován nařízením DORA.

ZDRAVOTNICTVÍ

Poskytovatelé zdravotní péče (nemocnice a další), subjekty provádějící výzkum a vývoj léčivých výrobků a přípravků, výrobci základních farmaceutických přípravků.

PITNÁ VODA

Dodavatelé a distributoři vody určené k lidské spotřebě, avšak kromě těch, pro které je to vedlejší činnost k jejich hlavní činnosti zabývající se distribucí jiných komodit a zboží.

ODPADNÍ VODA

Subjekty shromažďující, vypouštějící nebo upravující městské nebo průmyslové odpadní vody nebo splašky, avšak kromě těch, pro které se jedná pouze o vedlejší činnost k jejich hlavní činnosti.

DIGITÁLNÍ INFRASTRUKTURA

Poskytovatelé: výměnných uzlů internetu (IXP), cloud computingu, datového centra, služeb vytvářejících důvěru, elektronických komunikací, CDN služeb, registrů TLD, služeb systému doménových jmen (DNS), s výjimkou poskytovatelů root name serverů .

POSKYTOVATELÉ ŘÍZENÝCH ICT SLUŽEB

Poskytovatelé řízených ICT služeb a poskytovatelé řízených ICT bezpečnostních služeb. Subjekty, pro zákazníky provozující či spravující ICT služby a nástroje, typicky na základě smlouvy o úrovni služeb (SLA).

VEŘEJNÁ SPRÁVA

Ústřední orgány státní správy, veřejná správa na regionální úrovni, soudy a státní zastupitelství a další instituce významné pro chod státu.

VESMÍR

V České republice nejsou umístěny žádné subjekty pozemní infrastruktury, pro Českou republiku tedy nerelevantní.

SLUŽBY UVEDENÉ V PŘÍLOZE II

Subjekty poskytující služby uvedené v příloze I a splňující podmínku „střední podnik" a subjekty poskytující služby uvedené v příloze II a splňující podmínku „velký podnik" a „střední podnik" dle doporučení Komise (EU) 2003/361/EC budou regulovány v režimu „important" (nižší nároky z hlediska bezpečnostních opatření), pokud nebude stanoveno speciálními kritérii jinak.

POŠTOVNÍ SLUŽBY

Subjekty, poskytující poštovní služby, tzn. výběr, třídění, přepravu a dodání poštovních zásilek, včetně provozovatelů kurýrních služeb.

ODPADNÍ HOSPODÁŘSTVÍ

Subjekty, poskytující službu nakládání s odpady, tzn. zařízení určená pro nakládání s odpady, obchodníci, zprostředkovatelé, dopravci podle zákona č. 541/2020 Sb., kromě těch, pro které nakládání s odpady není jejich hlavní ekonomickou činností.

CHEMICKÝ PRŮMYSL

Subjekty, poskytující služby v chemickém průmyslu, tzn. výrobci, distributoři, včetně maloobchodníka, který skladuje a uvádí na trh chemickou látku nebo předmět.

POTRAVINÁŘSTVÍ

Potravinářské subjekty, které se zabývají velkoobchodní distribucí a průmyslovou výrobou nebo zpracováním.

VÝROBA

Výroba: zdravotnických a diagnostických zdravotnických prostředků, počítačů, elektronických a optických přístrojů, elektrických zařízení, strojů a zařízení, motorových vozidel (kromě motocyklů), přívěsů a návěsů, ostatních dopravních prostředků a zařízení.

POSKYTOVATELÉ DIGI SLUŽEB

Poskytovatelé on-line tržišť, internetových vyhledávačů, platforem služeb sociálních sítí.

VÝZKUM

Výzkumné organizace, s výjimkou vzdělávacích institucí, jejichž hlavním cílem je provádět aplikovaný výzkum nebo experimentální vývoj s ohledem na využití výsledků tohoto výzkumu pro komerční účely.

SUBJEKTY, KTERÝM PLYNOU POVINNOSTI Z NIS2, ALE NESPADAJÍ DO REŽIMU ESSENTIAL, ANI IMPORTANT

Jaké vyplývají povinnosti z NIS2?

- **Dva režimy povinností dle velikosti subjektu a typu služby:**
  - Vyšší (prakticky vylepšená vyhláška o kybernetické bezpečnosti č. 82)
  - Nižší (bude vydán nový právní předpis, prakticky jen kybernetické desatero dle NIS2)

- **Provést evidenci aktiv poskytujících službu, BIA nebo AR.**
- **Hlásit bezpečnostní incidenty.**
- **Provádět kontrolu dodavatelských řetězců.**
- **Po registraci na NÚKIB do roka začít zavádět bezpečnostní opatření.**

- **Organizační opatření:**
  - Definovat bezpečnostní politiku a předpisy, řízení rizik, přístupů a komunikací
  - Provádět školení včetně povinného vzdělávání vrcholového vedení
- **Technická opatření:**
  - FW, EDR, dostupnost, redundance, monitoring, testování, šifrování, ochrana záloh, DR/BCM a logy
  - Mikrosegmentace sítí

- **Vedení je povinno zajistit prostředky na zavedení nutných opatření, stanovit manažery KB a garanty aktiv.**

Jak hlásit bezpečnostní incidenty?

- Hlášení bezpečnostních incidentů
  - S významným dopadem
  - S úmyslným zaviněním

- Organizace ve vyšším režimu hlásí vše.
- Nižší PRS nemusí, jsou-li oba parametry záporné, významnost stanoví sám.
- Vznikne portál pro registraci subjektů, ohlašování incidentů a přístup k databázi zranitelností.
- Portál bude mít API pro Incident management systémy organizací.

- NÚKIB smí zveřejňovat informace o zjištěných kybernetických bezpečnostních incidentech.

Jak bude kontrolováno dodržování NIS2?

- Je možné, že budou existovat komerční auditoři KB pro NIS2, aby se uvolnily kapacity kontrolorů NÚKIB.
- Kontroly zahraničních poskytovatelů budou probíhat ve spolupráci s cizím regulátorem.
- Certifikace ISO 27001 neznamená, že nebude podnik kontrolován.
- KB musí být obsahem zápisů z valných hromad společností.

- Drastické pokuty viz GDPR, navíc je možné i pozastavení licence či certifikace služby, nebo omezení jednacích práv odpovědných osob za KB.
- Statutární orgán se nemůže zbavit zodpovědnosti delegováním povinností a může být zbaven pozice až na 18 měsíců, a to ve všech společnostech, kde je zapsán.

Jak vám GAPP System může pomoci?

- Zpracovat analýzu vašeho stávajícího prostředí.
- Zhodnotit, jakým způsobem vaše organizace plní jednotlivé body směrnice.
- Navrhnout technická a organizační opatření.
- Zpracovat případné návrhy řešení jednotlivých oblasti i s cenovou náročností.
- Realizovat jednotlivá technická opatření.
- Zajistit průběžnou aktualizaci technických opatření a jejich souladu se směrnicí.

Jak vypadá analýza prostředí?

- **Analýza stávajících procesů a relevantní dokumentace**
  - Předpisy, popisy infrastruktury, nastavení jejích prvků
- **Řízené rozhovory – interview**
  - 250 dotazů z 23 oblastí definovaných NIS2
- **Analýza rizik**
  - Evidence aktiv, identifikace hrozeb, zranitelností a dopadů
- **Návrhy opatření**
  - Organizační
  - Technická

Strukturované interview

Dot. č.	§ VoKB	Čl. Př. 5	ISO 27002	Obl.	Název Dotaz Upřesnění	Ano/Ne	Známka	Body
	§21	1.17	12.2	09.4	**Ochrana proti škodlivým kódům**			
58					Jsou zajištěna pravidla a postupy pro ochranu před škodlivým kódem pro:	n/a	n/a	n/a
58 a					Endpointy	Ano		
58 b					Mobilní zařízení	Ano		
58 c					Servery	Ano		
58 d					Datová úložiště	Ano		
58 e					Přenosné nosiče dat	Ne		
58 f					Komunikaci a přenos dat	Ano		
59					Jsou na endpointech s OS Windows zobrazovány přípony souborů?	Ano		
60					Lze detekovat a blokovat škodlivý e-mail před doručením koncovému uživateli?	Ano		
61					Je v přílohách přijatých e-mailů vypnuto automatické spouštění maker?	Ano		
62					Je monitorováno a řízeno používání výměnných zařízení a datových nosičů?	Ne		
63					Je řízeno automatické spouštění obsahu výměnných zařízení a datových nosičů?	Ne		
64					Je řízeno oprávnění ke spouštění kódu?	Ne		
65					Je prováděna pravidelná aktualizace nástroje pro ochranu před škodlivým kódem?	Ano		
		1.9	12.3	09.5	**Zálohování a archivace dat**			
66					Je zajištěno provádění pravidelného zálohování a kontrola použitelnosti provedených záloh?	Ano		
67					Jak vypadá zálohovací infrastruktura a nastavení zálohovacích procesů?	n/a	n/a	n/a
68					Jak jsou zabezpečena přístupová oprávnění a uživatelské účty k systémům zálohovací infrastruktury?	n/a	n/a	n/a
69					Je dostatek místa pro obnovy ze záloh?	Ne		
70					Jsou zálohy šifrovány?	Ne		
71					Kde jsou uloženy zálohy dešifrovacích klíčů k zálohám?	n/a	n/a	n/a
72					Je používán systém záloh 3-2-1 (3 kopie, 2 typy úložišť, 1 mimo lokalitu)?	Ne		
73					Existují zálohy image OS či celých VM pro případ obnovy čistým deploymentem?	Ano		
	§18	1.16	13.0	09.6	**Řízení bezpečnosti sítí**			
74					Je pro ochranu bezpečnosti komunikační sítě zajištěna segmentace sítě?	Ne		
75					Je pro zajištění segmentace sítě a pro řízení komunikace mezi segmenty využíván nějaký nástroj, který zajistí ochranu integrity komunikační sítě?	Ne		
76 a					Izolace portů ve stejné VLAN	Ne		
76 b					Automatické přiřazování do VLAN podle ověření uživatele (např. v RADIUS)	Ne		
76 c					Automatické přiřazování do Guest VLAN podle MAC adresy zařízení	Ano		

Interaktivní tabulka analýzy rizik

ID	Zranitelnost	Potenciální riziko	Vlastník rizika	Provázanost na aktiva	Hledisko bezpečnosti informací	Související hrozby	Hodnota aktiva	Síla zranitelnosti	Pravděpodobnost výskytu hrozby	Míra rizika	Navržené opatření	Přístup k riziku	Síla zranitelnosti po přezkoumání rizika	Míra rizika po realizaci opatření
R1	Nejsou definována pravidla pro bezpečné používání mobilních zařízení	Může vést k neoprávněnému přístupu k mobilnímu zařízení a narušení důvěrnosti, dostupnosti nebo integrity aktiv.		Aktiva uložená na mobilních zařízení	Dů, Do, Int	H8, H9, H10, H11	4	3	3	36				0
R2	Zaměstnanci společnosti a relevantní smluvní strany (např. zaměstnanci ostrahy) neabsolvují školení, které by komplexně pokrývalo oblast bezpečnosti informací.	Zvýšená pravděpodobnost bezpečnostních incidentů způsobených neznalostí bezpečnostních pravidel.		Veškerá aktiva společnosti	Dů, Do, Int	H8, H9, H10, H11, H12, H15, H16, H17, H18, H20	4	3	3	36				0
R3	Nejsou definována pravidla pro přenos informací. Citlivé informace jsou zaměstnanci posílány e-mailem mimo společnost v nezabezpečené podobě. Jsou využívány veřejné portály pro sdílení souborů (např. uloz.to, uschovna.cz) a soukromé e-mailové schránky zaměstnanců	Únik informací a jejich zneužití.		Informační aktiva v elektronické podobě	Dů	H12, H20	4	3	3	36				0
R4	Zpracované plány kontinuity nezahrnují všechny klíčové systémy společnosti.	V případě mimořádných událostí může dojít k větší nedostupnosti systému než je nutné, nebo ke ztrátě dat.		Informační, fyzická, SW aktiva a služby	Do	H1, H2, H3, H4, H5, H6	4	3	3	36				0
R5	Nejsou nastavena pravidla pro manipulaci s médii.	Únik citlivých informací.		Informační aktiva	Dů	H17, H18	4	3	3	36				0
R6	Nespolehlivý zálohovací software.	Ztráta důležitých dat.		Informační a SW aktiva	Do, Int	H7, H8, H20	4	3	3	36				0
R7	Je povoleno připojení uživatelů z neověřených zařízení k firemní síti prostřednictvím vzdáleného přístupu VPN.	Může dojít k úniku informací v důsledku přístupu třetí osoby nebo v důsledku infikace přistupujícího zařízení, případně může také dojít k infikaci sítě společnosti.		Informační a SW aktiva	Dů, Int	H8, H9, H17, H18, H20	4	3	3	36				0
R8	Není defaultně nastaveneno zabezpečení mobilních telefonů nebo jejich vzdálená správa.	Může dojít k neoprávněnému přístupu a úniku důvěrných a citlivých informací při krádeži nebo ztrátě mobilního telefonu.		Informační aktiva	Dů, Int	H12, H15, H17, H20	3	3	3	27				0
R9	Nejsou definována pravidla pro přípustné použití aktiv	Narušení důvěrnosti, dostupnosti nebo integrity aktiv z důvodu špatného zacházení s aktivy.		Veškerá aktiva společnosti	Dů, Do, Int	H8, H9, H10, H11, H12, H15, H16, H17, H18, H20	4	2	3	24				0
R10	Není zavedena klasifikace informací v souladu s jejich důležitostí pro společnost.	Informace nejsou chráněny odpovídajícím způsobem, což může vést k jejich zneužití.		Informační aktiva	Dů	H9, H10, H17, H18	4	2	3	24				0
R11	Není prováděna pravidelná revize přístupových oprávnění.	Neoprávněný přístup k citlivým informacím a jejich zneužití.		Informační aktiva	Dů, Do, Int	H9, H10	4	2	3	24				0
R12	Nejsou dodržovány zásady prázdného stolu a čisté obrazovky.	Neoprávněný přístup k citlivým informacím a jejich zneužití.		Informační aktiva	Dů, Do, Int	H9, H10, H17, H18	4	2	3	24				0
R13	Není zaveden postup pro monitoring kapacit.	Nedostupnost systémů z důvodu nedostatku výkonu nebo kapacit.		SW aktiva	Do	H13, H19	4	2	3	24				0

Co doporučujeme?

- **Patch management**
  - Pravidelné instalace bezpečnostních záplat a jejich testování
- **Bezpečnostní testování**
  - Penetrační testy, social engineering
- **Monitoring činností uživatelů a událostí, správa logů**
  - Včasné odhalení nevhodných procesů a chování uživatelů – DLP, CheckMK, Logmanager
- **Zajištění nezměnitelnosti záloh**
  - Jediná ochrana proti ransomware – Datový trezor, DR lokalita, cloud
- **Plány kontinuity a Disaster recovery procesů**
  - Různé scénáře výpadků provozu a znepřístupnění dat

A dál…?

- Ustanovit role kybernetické bezpečnosti
- Provádět pravidelné školení bezpečnostního povědomí
- Používat segmentaci sítí
- Smluvně ošetřit dodržování bezpečnostních pravidel dodavateli
- Šifrovat disky přenosných počítačů
- Provádět pravidelné Disaster Recovery testy
- Aktivně používat a aktualizovat Evidenční tabulky aktiv
- … a nebát se ničeho.

Děkuji za pozornost

Jan Dupač
jan.dupac@gapp.cz