

Č.J. NEPŘIDĚLENO • BRNO • 21. ÚNORA 2022

VERZE DOKUMENTU: 1.0

HLÁŠENÍ KYBERNETICKÉHO BEZPEČNOSTNÍHO INCIDENTU

základní metodika k upřesnění plnění povinnosti podle
§ 8 zákona č. 181/2014 Sb., o kybernetické bezpečnosti

1 Úvod

V kybernetickém prostoru a fyzickém světě může nastat řada situací, při nichž dojde k narušení dostupnosti, důvěrnosti nebo integrity informací. V praxi se mohou tyto situace velmi lišit ve svém reálném dopadu – od zcela zásadních, až po zcela marginální, nemající žádný dopad na poskytované služby nebo shromážděné údaje.

Zákon č. 181/2014 Sb., o kybernetické bezpečnosti (dále jen „zákon o kybernetické bezpečnosti“), již od svého původního znění ukládá povinnost orgánům a osobám, které pod něj spadají, hlásit kybernetické bezpečnostní incidenty relevantním CERT týmům – vládnímu CERT nebo národnímu CERT.

Dosavadní zkušenosti Národního úřadu pro kybernetickou a informační bezpečnost (dále jen „Úřad“) však vedou k tomu, že počet hlášených kybernetických bezpečnostních incidentů dlouhodobě neodpovídá reálnému počtu incidentů, které by měly být hlášeny.

Vedle celé řady potenciálních problémů v rámci procesu zvládnání kybernetických bezpečnostních incidentů u jednotlivých povinných osob se dále jako jeden z důvodů dlouhodobě jeví především problematická šíře definice kybernetického bezpečnostního incidentu podle § 7 odst. 2 zákona o kybernetické bezpečnosti¹ a srozumitelnost platné právní úpravy.

Úřad měl a má z tohoto důvodu dlouhodobý cíl – stanovit, které případy narušení bezpečnosti informací lze považovat za taková narušení dostupnosti, důvěrnosti a integrity, která není nezbytně nutné hlásit Úřadu a jejichž hlášení nebude Úřad vymáhat, což by mělo mít za cíl přinést větší právní jistotu a zvýšit počet hlášení kybernetických bezpečnostních incidentů, zejména těch nejvýznamnějších.

Tento dokument vznikl jako základ realizace tohoto cíle a odráží

- poznatky Úřadu a jeho zkušenosti,
- princip zasahování veřejné moci do práv osob pouze v nezbytném rozsahu a zásadu hospodárnosti a efektivnosti,
- skutečnost, že mezinárodní diskurs směřuje k hlášení pouze incidentů s významným dopadem, a
- smysl a účel povinnosti hlásit kybernetické bezpečnostní incidenty.

¹ „Kybernetickým bezpečnostním incidentem je narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací v důsledku kybernetické bezpečnostní události.“

V případě dotazů se prosím obraťte na sekretariát Národního úřadu pro kybernetickou a informační bezpečnost:

Národní úřad pro kybernetickou a informační bezpečnost

Mučednická 1125/31

616 00 Brno – Žabovřesky

Tel.: +420 541 110 560

E-mail: regulace@nukib.cz

Upozornění:

Tento dokument slouží jako podpůrné vodítko, nenahrazuje žádný ze zákonů ani prováděcích právních předpisů. Právo změny tohoto dokumentu vyhrazeno.

Informace obsažené v dokumentu se vztahují k právní úpravě účinné ke dni platnosti publikované verze dokumentu.

2 Definice kybernetického bezpečnostního incidentu

Podle § 7 odst. 2 zákona o kybernetické bezpečnosti je **kybernetickým bezpečnostním incidentem** „(...) *narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací v důsledku kybernetické bezpečnostní události*“.²

Z výše uvedeného lze dovodit, že v souladu s aktuálním zněním zákona o kybernetické bezpečnosti je kybernetickým bezpečnostním incidentem v zásadě každé narušení zajištění důvěrnosti, integrity a dostupnosti informací a dat a narušení dostupnosti nebo interoperability služeb a integrity sítí.

Pro praktické použití však tento výklad není zcela přesný, neboť je potřeba správně interpretovat podstatu pojmu „narušení“ v této definici. Norma ISO/IEC 27000, z jejíhož obsahu definice kybernetického bezpečnostního incidentu v zákoně o kybernetické bezpečnosti podstatně vychází, uvádí, že definičními znaky incidentu bezpečnosti informací je také to, že se jedná o skutečnost, která je „*neočekávaná*“.³

V tomto smyslu je nutno rozumět také definici kybernetického bezpečnostního incidentu podle zákona o kybernetické bezpečnosti.

Právě definiční znak „neočekávanosti“ se v rámci definice projeví tím způsobem, že za kybernetický bezpečnostní incident není možné chápat plánované zásahy do informačních systémů.

Plánované a avizované (těm subjektům, na které bude mít plánovaný zásah do systému dopad) servisní zásahy do systému nejsou kybernetickým bezpečnostním incidentem za předpokladu, že rozsah zásahu do informačního systému nepřesáhne plán zásahu, a to i přesto, že z důvodu zásahu dojde (zcela logicky a očekávaně) k nedostupnosti informací a dat a dopadu na službu, kterou systém zajišťuje nebo významně ovlivňuje.

² Tuto definici je možné podrobněji rozdělit následovně. Bezpečnost informací v souladu s § 2 písm. c) zákona o kybernetické bezpečnosti znamená „*zajištění důvěrnosti, integrity a dostupnosti informací a dat*“. Bezpečností sítí a služby se v souladu s § 98 odst. 1 zákona č. 127/2005 Sb., o elektronických komunikacích, rozumí „*jejich schopnost odolávat s dostatečnou spolehlivostí veškerým zásahům, které narušují dostupnost, hodnověrnost, integritu nebo důvěrnost této sítě a služby, uchovávaných, předávaných nebo zpracovávaných dat nebo souvisejících služeb, které tato síť nebo služba elektronických komunikací nabízí nebo které jsou jejich prostřednictvím přístupné.*“ a dále pak se podle § 2 odst. 4 písm. c) téhož zákona interoperabilitou rozumí „*takové nastavení přenosových parametrů služby a rozhraní, které umožňuje komunikaci mezi koncovými uživateli nebo mezi koncovým uživatelem a podnikatelem poskytujícím službu prostřednictvím technologicky různých sítí elektronických komunikací*“ a podle § 2 odst. 4 písm. b) se integritou sítí rozumí „*funkčnost a provozuschopnost propojených sítí elektronických komunikací, ochrana těchto sítí vůči poruchám způsobeným elektromagnetickým rušením nebo provozním zatížením*“. Ustanovení o bezpečnosti informací se analogicky použije i na bezpečnost služeb a bezpečnost a integritu sítí elektronických komunikací. Z toho důvodu se dále hovoří pouze o bezpečnosti informací v informačních systémech.

³ Definice „*3.31 Incident bezpečnosti informací*“ podle normy ISO/IEC 27000.

Na druhou stranu, v případě, že se nejedná o zásah, který by byl plánovaný, nebo narušení překročilo plánem stanovené parametry, nelze takovou situaci nadále označovat za „očekávanou“ a o kybernetický bezpečnostní incident se jednat bude.

Obdobně se jedná též o případy plánovaných zásahů do zajištění konektivity nebo dalších plnění (typicky zajištění elektrické energie) nezbytných pro řádné fungování systémů spadajících pod zákon o kybernetické bezpečnosti, za předpokladu, že povinná osoba je o plánované odstávce informována a rozsah nepřesáhne plán zásahu. Kybernetickým bezpečnostním incidentem pak v tomto případě zůstává ta situace, kdy dojde k narušení dostupnosti daného systému, protože nebude tato plánovaná a oznámená odstávka brána v potaz, nebo nezafungují bezpečnostní opatření či bude přesáhnut plán, který s touto odstávkou souvisel.

3 Obecně o hlášení kybernetického bezpečnostního incidentu

Podle § 8 odst. 1 zákon o kybernetické bezpečnosti je **povinnost hlásit kybernetické bezpečnostní incidenty** stanovena následovně: „Orgány a osoby uvedené v § 3 písm. b) až f) zákona o kybernetické bezpečnosti⁴ jsou povinny hlásit kybernetické bezpečnostní incidenty v jejich významné síti⁵, informačním nebo komunikačním systému kritické informační infrastruktury, informačním systému základní služby nebo významném informačním systému, a to bezodkladně po jejich detekci.“⁶

Z výše uvedeného vyplývá, že povinné osobě zákon ukládá hlásit každou skutečnost, která naplní definici kybernetického bezpečnostního incidentu.

Povinnost hlásit kybernetické bezpečnostní incidenty se tedy týká incidentu realizovaného v určeném informačním systému podle zákona o kybernetické bezpečnosti. Na incidenty, ke kterým dojde v rámci stejné organizace, ale mimo tyto informační systémy určené podle zákona o kybernetické bezpečnosti, nedopadá povinnost je hlásit (je to nicméně možno učinit dobrovolně).

Správci a provozovatelé informačních a komunikačních systémů kritické informační infrastruktury, správci a provozovatelé významných informačních systémů a správci, provozovatelé informačních systémů základní služby a případně provozovatelé základní služby hlásí kybernetické bezpečnostní incidenty Úřadu, resp. vládnímu CERT.⁷

Orgány nebo osoby zajišťující významnou síť a poskytovatelé digitální služby, hlásí kybernetické bezpečnostní incidenty provozovateli národního CERT.⁸

Povinné osoby si nemusejí být vždy zcela jisté, zda se jedná o kybernetický bezpečnostní incident nebo pouhou kybernetickou bezpečnostní událost. **V případě jakékoliv nejistoty Úřad povinné osoby vyzývá, aby se na něj neváhaly obrátit. I pouhé kybernetické bezpečnostní události mohou být zdrojem cenných informací např. o probíhajících útocích.**⁹

⁴ Orgán nebo osoba zajišťující významnou síť, správce a provozovatel informačního systému kritické informační infrastruktury, správce a provozovatel komunikačního systému kritické informační infrastruktury, správce a provozovatel významného informačního systému a správce a provozovatel informačního systému základní služby.

⁵ „Významnou síť (se rozumí) síť elektronických komunikací zajišťující přímé zahraniční propojení do veřejných komunikačních sítí nebo zajišťující přímé připojení ke kritické informační infrastruktuře.“

⁶ V případě hlášení kybernetických bezpečnostních incidentů poskytovatelem digitální služby nebo provozovatelem základní služby podle § 8 odst. 2 a 8 zákona o kybernetické bezpečnosti je součástí definice hlášení „významnost“ dopadu kybernetického bezpečnostního incidentu a tuto metodiku tedy není potřeba v takových případech vůbec aplikovat.

⁷ § 8 odst. 4 zákona o kybernetické bezpečnosti

⁸ § 8 odst. 3 zákona o kybernetické bezpečnosti

⁹ Jako povinné osoby podle zákona o kybernetické bezpečnosti by však měly postupem podle § 24 vyhlášky o kybernetické bezpečnosti dospět k finální identifikaci, zda se jednalo o kybernetickou bezpečnostní událost nebo incident.

Úřad na svých internetových stránkách dlouhodobě deklaruje, že „Včasné nahlášení incidentu primárně nevede k vyslání kontroly do Vaší organizace ani udělení sankce, ale pouze k jeho zaevidování, analýze a případné nabídce pomoci.“¹⁰

Zákon o kybernetické bezpečnosti také nezná přestupek, který by spočíval v tom, že se povinné osobě stal kybernetický bezpečnostní incident.

Přestupkem podle § 25 zákona o kybernetické bezpečnosti však je neohlášení takového kybernetického bezpečnostního incidentu.

¹⁰ Dostupné zde: <https://www.nukib.cz/cs/kyberneticka-bezpecnost/vladni-cert/hlaseni-incidentu/>

4 Úřadem stanovené a uznané výjimky z hlášení kybernetického bezpečnostního incidentu

Úřad měl a má dlouhodobý cíl – stanovit, které případy narušení bezpečnosti informací lze považovat za taková narušení dostupnosti, důvěrnosti a integrity, která není nezbytně nutné hlásit Úřadu a jejichž hlášení nebude Úřad vymáhat.

Definování takových situací, kdy se jedná o univerzálně platné tvrzení, je jisté, že dané narušení bezpečnosti nemůže nikdy mít významné dopady na povinnou osobu nebo poskytované služby, a zároveň daná situace nemůže být důležitým indikátorem, který by mohl pomoci zabránit mnohem výraznějšímu dopadu, je však v praxi velmi obtížné.

Tato kapitola má za cíl uvést takové situace, v rámci kterých dlouholeté zkušenosti Úřadu ukazují, že jejich dopad takové vlastnosti má a z tohoto důvodu není nutné je Úřadu hlásit.

Úřad z těchto důvodů a s ohledem na výše uvedené nepovažuje za nutné v rámci povinnosti hlášení kybernetických bezpečnostních incidentů v souladu s § 8 odst. 1 zákona o kybernetické bezpečnosti hlásit kybernetické bezpečnostní incidenty, které lze definovat takto:

4.1 Redundance aktiv

Kybernetický bezpečnostní incident není potřeba Úřadu hlásit v případě, kdy došlo v důsledku technického selhání k nedostupnosti části aktiv, lze s jistotou vyloučit úmyslné zavinění¹¹ (zejména útočníkem), a zároveň řádné zafungování k nim záložních (redundantních, zdvojených) aktiv zabránilo vzniku nedostupnosti systému jako celku.

4.2 Další výjimky z hlášení kybernetických bezpečnostních incidentů

Další situace, které by splňovaly výše uvedené podmínky a nebylo je tedy jako kybernetické bezpečnostní incidenty nutno Úřadu hlásit do této chvíle Úřad neidentifikoval.

Úřad má za cíl tento dokument dále doplňovat o další univerzálně platné výjimky, jakmile tyto budou dostatečně jistě identifikovány.

Podněty na toto téma můžete zasílat na e-mailovou adresu: regulace@nukib.cz.

¹¹ Protože se bude v těchto situacích jednat vždy minimálně o kybernetickou bezpečnostní událost, je povinností povinné osoby v souladu s § 24 vyhlášky o kybernetické bezpečnosti takové události vyhodnocovat.

5 Podmínky využití informací

Využití poskytnutých informací probíhá v souladu s metodikou Traffic Light Protocol (dostupná na webových stránkách www.nukib.cz/cs/infoservis/doporuceni/1593-doporuceni-k-pouzivani-protokolu-tlp-ke-sdileni-chranenych-informaci/). Informace je označena příznakem, který stanoví podmínky použití informace. Jsou stanoveny následující příznaky s uvedením charakteru informace a podmínkami jejich použití:

Barva	Podmínky použití
Červená TLP: RED	Informace nemůže být poskytnuta jiné osobě než té, které byla informace určena, nebudou-li výslovně stanoveny další osoby, kterým lze takovou informaci poskytnout. V případě, že příjemce považuje za důležité informaci poskytnout dalším subjektům, lze tak učinit pouze se souhlasem původce informace.
Oranžová TLP: AMBER	Informace může být sdílena v rámci organizace, které byla informace poskytnuta. Dále může být poskytnuta pouze těm partnerům, kteří splňují need-to-know a jejichž informování je důležité pro vyřešení problému či hrozby uvedené v informaci. Jiným osobám, než výše uvedeným, nesmí být informace poskytnuta. Původce informace může rozsah sdílení dále omezit.
Zelená TLP: GREEN	Informace může být sdílena v rámci organizace příjemce a případně také s dalšími partnerskými subjekty příjemce, avšak nikoli skrze veřejně dostupné kanály; příjemce musí při předání zajistit důvěrnost komunikace.
Bílá TLP: (WHITE)	Informace může být dále poskytována a šířena bez omezení. Případné omezení na základě práva duševního vlastnictví původce a/nebo příjemce či třetích stran nejsou tímto ustanovením dotčena.

Verze dokumentu			
datum	verze	změněno	popis změny
21. února 2022	1.0	OREG – ORESS	Vznik dokumentu