EVROPSKÁ UNIE
Evropské strukturální a investiční fondy
Operační program Výzkum, vývoj a vzdělávání

MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY

jihomoravský kraj

INFORMAČNÍ BEZPEČNOST

Právní nástroje kybernetické bezpečnosti

Metodický list

Autor: Ing. Vladimír Šulc, Ph.D., Metodik: Mgr. Hana Hrádková

Recenzent: Mgr. Lukáš Podepřel

Rok vydání: 2023

Obsah

Cíle

- Žák definuje stěžejní pramen právní úpravy kybernetické bezpečnosti v ČR.
- Žák rozlišuje rozdíly mezi kybernetickou bezpečností a kybernetickou obranou.
- Žák dokáže odpovědět jaké jsou základní cíle k naplnění zákona o KB.

Dovednosti

- Žák umí detekovat kybernetické bezpečnostní události.
- Žák rozpozná okruh povinných subjektů podle ZKB.
- Žák popíše chyby lidského faktoru, které ohrožují kybernetickou bezpečnost.

Kontrolní otázky

- Co znamená pojem „Bezpečnostní opatření“
- Zamlčení bezpečnostního incidentu dle § 25 odst. 2 písm. b) – vysvětlete.
- Popište a vysvětlete unijní legislativní činnost.
- Vysvětlete a přeložte pojem „Akt kybernetické bezpečnosti“.

Průběh výuky

Otevřete internetový prohlížeč pro vyhledávání informací.

1. Opakování z předchozí hodiny (zákon o KB a vyhláška o KB).
2. Výklad nové látky v rámci tématu Právní nástroje Kybernetické bezpečnosti.
3. Zadání úlohy v rámci cvičení.
4. Prezentace výsledků žáky.
5. Shrnutí nových poznatků.

Úvod

Zajištění kybernetické bezpečnosti je navýsost aktuálním tématem. S rozšířením informačních a komunikačních technologií a očekávatelným rozvojem informační společnosti, který současně umocňují události typu pandemie COVID-19 nebo válečné konflikty, představuje důležitou výzvu v národním i mezinárodním měřítku. Ve vyspělé společnosti se bez působení v kyberprostoru a bez použití moderních technologií neobejdeme, jelikož čím dál více lidské činnosti se stává podmíněné nebo minimálně závislé na použití informační či komunikační infrastruktury, převážně sítě internet. Počet zařízení a uživatelů napojených na infrastrukturu se každým rokem zvyšuje a lze důvodně předpokládat, že požadavek na zabezpečení těchto zařízení a jejich prostřednictvím zpracovávaných dat bude žádoucí, aby nedošlo k jejich zneužití. To jak ze strany státu, správců nebo provozovatelů systémů, služeb či sítí, tak samotných koncových uživatelů, o jejichž bezpečnost je v konečném důsledkuusilováno.3Během posledních asi deseti let vznikla v českém právu legislativa, jejímž předmětem je úprava kybernetické bezpečnosti, založená na ochraně prostředí. Vybraným subjektům jsou ukládány povinnosti tak, aby došlo k prevenci vzniku kyberbezpečnostních incidentů a aby v případě narušení bezpečnosti byly takové události v co největší míře potlačeny s minimalizací následků. Cesta, jak kýženého cíle dosáhnout, je do značné míry ponechána povinným subjektům na uvážení a přináší do tohoto typu právní regulace s prvky veřejnoprávními i soukromoprávními nevídanou míru autonomie vůle.

1 Kybernetická bezpečnost v českém právním řádu

Oblast kybernetické bezpečnosti je relativně nové právní odvětví, které z důvodu snazší dostupnosti moderních technologií a jejich stále silnější roli ve společnosti nabývá na významu. Právní úprava však nemůže a ani by kvůli značnému přesahu do jiných právních odvětví neměla být kodifikována. Kybernetická bezpečnost je tak v porovnání s jinými právními odvětvími tvořena širším spektrem pramenů od základních právních principů a zásad, zákonů či předpisů nižší právní síly, soudní praxe, až po velmi podrobné metodiky, konkrétní doporučení, standardy a jiná nezávazná stanoviska orgánů veřejné moci. Takové rozdělení za použití performativních pravidel v konečném důsledku umožňuje relativní flexibilitu regulace, aniž by při požadavku na její změnu muselo dojít k výraznému nárůstu složitých a časové náročných legislativních změn či užšímu zapojení vlády, příslušných ministerstev nebo zákonodárného sboru.

1.1 Vnitrostátní prameny

Není překvapením, že v informační společnosti zajištění kybernetické bezpečnosti jednoznačně patří mezi nejvyšší priority státu a současně jeho základní povinnosti. Ve smyslu čl . 1 ústavního zákona č. 110/1998Sb.,

o bezpečnosti České republiky, ve znění pozdějších předpisů, je základní povinností státu „zajištění svrchovanosti a územní celistvosti České republiky, ochrana jejích demokratických základů a ochrana životů, zdraví a majetkových hodnot“. Narušení kybernetické bezpečnosti je bezpochyby způsobilé tyto hodnoty velmi výrazně negativně ovlivnit. Dalším pramenem na úrovni ústavního pořádku je samotná Ústava, jež kromě vymezení základních principů pro uplatňování státní moci a chování subjektů v soukromoprávním postavení prosazuje dělbu moci, a tím nepřímo formuje i institucionální zajištění kybernetické bezpečnosti. Listina tvoří katalog práv, do kterých by nemělo být vrchnostensky zasahováno, respektive stanovuje limity toho, v jakých případech a do jaké míry zásah možný je.

Stěžejní pramen právní úpravy kybernetické bezpečnosti v ČR představuje zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, ve znění pozdějších předpisů, jenž nabyl účinnosti dne 1. 1. 2015. ZKB upravuje práva a povinnosti povinných subjektů, působnost a pravomoci orgánů veřejné moci v oblasti kybernetické bezpečnosti a zpracovává příslušné předpisy Evropské unie, tj. směrnice NIS.21Cílem zákona je ochrana existence a funkčnosti prostředí tvořeného informačními systémy a sítěmi a službami elektronických komunikací tak, aby nedošlo „k ohrožení práva subjektů na informační sebeurčení, fungování základních společenských funkcionalit chráněných nedistributivními právy České republiky a národní kybernetická infrastruktura nebyla zneužitelná k útokům mimo Českou republiku“.22 Dle výčtu na oficiálních stránkách NÚKIB je třeba k naplnění cílů ZKB:

- stanovit základní úroveň bezpečnostních opatření,
- zlepšit detekci kybernetických bezpečnostních incidentů,
- zavést hlášení kybernetických bezpečnostních incidentů,
- zavést systém opatření k reakci na kybernetické bezpečnostní incidenty,
- upravit činnost dohledových pracovišť,
- zavést systém opatření k reakci na kybernetické bezpečnostní incidenty,
- upravit činnost dohledových pracovišť.

ZKB doplňují tři prováděcí vyhlášky, na které odkazuje textace ZKB:

- VKB,
- vyhláška VIS,
- vyhláška ZS.

VKB upravuje obsah a strukturu bezpečnostní dokumentace a bezpečnostních opatření, včetně povinnosti jejich aktualizace, typy, kategorie a hodnocení významnosti incidentů, způsob a náležitosti jejich hlášení, náležitosti oznámení o provedení reaktivního opatření a jeho výsledku, vzor a formu oznámení kontaktních údajů a způsob likvidace dat, provozních údajů, informací a jejich kopií.

2 Unijní úprava

Vedle vnitrostátní úpravy s ohledem na přeshraniční povahu kybernetické bezpečnosti postupně začíná nabírat na obrátkách i unijní legislativní činnost. Tuto aktivitu ještě umocnil příchod pandemieCOVID-1930, kdy sítě a informační systémy, především internet, začaly být využívány i tam, kde by to za běžného stavu bylo nemyslitelné nebo by prosazení takto radikální změny přístupu k využití dříve nedostupných technologií trvalo podstatně déle. Procesy na úrovni organizací se změnily natrvalo. Na druhou stranu rozšířením aktivity doonline prostředí zákonitě došlo i k navýšení kyberbezpečnostních rizika incidentů, navzdory uvědomění si jeho důležitosti.

2.1 Směrnice NIS

Sítě a informační systémy mají nezastupitelnou roli při usnadňování přeshraničního pohybu zboží, služeb a osob a sebemenší narušení jejich bezpečnosti se dotýká vedle jednotlivých členských států fungování celého vnitřního trhu Evropské unie. Evropská unie proto v roce 2016 přistoupila k přijetí minimálních požadavků napříč všemi členskými státy a představila závazné harmonizované požadavky ve směrniciNIS.33 Z pohledu právního řádu České republiky se nejednalo o převratnou novinku. Směrnice NIS byla přijata několik let po nabytí účinnosti ZKB. Česká právní úprava v tomto směru „předběhla“ Evropskou unii. Česká republika si dokonce připsala ze všech členských států prvenství, když takto komplexně, a navíc ještě bez povinnosti implementace, přijala rámec kybernetické bezpečnosti

2.1.1 Směrnice NIS II

V současnosti je velmi „živým“ předpisem návrh směrnice NIS II. Jedná se o zamýšleného nástupce prvního harmonizačního předpisu Evropské unie na poli kybernetické bezpečnosti, směrnice NIS z roku 2016. Směrnice NIS II zatím neprošla celým legislativním procesem a v době přípravy tohoto textu bylo poslední zveřejněnou informací o průběhu jejího schvalování jednání Rady ze dne 20. 4. 2022 a předběžná dohoda Rady a evropského parlamentu. Jelikož k transpozici směrnice NIS II budou mít po jejím schválení členské státy 21 měsíců, nelze pravděpodobně očekávat reálný dopad dříve než na začátku roku 2024.

3 Rozdíl mezi kybernetickou bezpečností a kybernetickou obranou

Definice kybernetické obrany není v českém právním prostředí jednotná a vymezení tohoto pojmu, na kterém by co do rozsahu panovala přesná shoda, bychom hledali stěží. Ostatně ani legální definici tohoto pojmuv českém právním řádu nenajdeme. Obecný konsensus panuje na tom, že při širším chápání kybernetické bezpečnosti do ní lze zahrnout také kybernetickou obranu – kybernetická obrana tvoří jednu z jejích „podmnožin". Tento pohled potvrzuje samo Vojenské zpravodajství ČR jako subjekt odpovědný za zajišťování kyberobrany na svých oficiálních webových stránkách a další zdroje, například strategie EU, odborné publikace a v neposlední řadě kvalifikační práce. Uvedené prameny obdobně definují oblast kybernetické obrany jako součást kybernetické bezpečnosti v širším smyslu, jež je zajišťována v rámci aktivit zpravodajských služeb či armády se zaměřením na obranu státu před útoky proti státu jako takovému za pomocí kybernetických zbraní. Zajišťováním „všeobecné" obrany státu, včetně složky kybernetické obrany, se rozumí ve smyslu zákona č. 222/1999 Sb., o zajišťování obrany české republiky, ve znění pozdějších předpisů, „souhrn opatření k zajištění svrchovanosti, územní celistvosti, principů demokracie a právního státu, ochrany života obyvatel a jejich majetku před vnějším napadením". Snahou a cílem kybernetické obrany je v souladu se zákonnou definicí především vybudovat funkční a zároveň efektivní systém, kterým budou zastaveny a odvráceny vnější kybernetické útoky na zmíněné chráněné hodnoty. Oproti kybernetické bezpečnosti v užším významu budou zpravidla využity mnohem invazivnější nástroje, metody a postupy. To je dáno už charakterem oprávněných subjektů k zajišťování obrany, podmínkami jejich zmocnění, jakož i tím, že předpisy upravující jejich činnost dávají silné pravomoci i prostředky k provádění jejich činnosti. Například Vojenské zpravodajství jako jeden z působících orgánů kybernetické obrany provádí tzv. cílenou detekci kybernetických útoků majících původ v zahraničí, směřuje-li takový útok proti důležitým zájmům státu. V krajním případě je Vojenské zpravodajství oprávněno provést tzv. aktivní zásah ve smyslu § 16g zákona o Vojenském zpravodajství. Jinými slovy, zanedbatelné incidenty v kontextu obrany České republiky Vojenské zpravodajství vůbec neřeší ani pravomoc řešit mít nebude, jelikož se nejedná o důležitý zájem státu. Tomu odpovídají i nástroje, které jsou institucionálnímu zajištění kyberobrany k dispozici, spadá-li incident do jejich působnosti. Mezi nejsilnější nástroje, které za splnění podmínek zákona může Vojenské zpravodajství využít, patří odposlechy, kontrola zásilek, sledování osob a věcí, pořizování audiovizuálních záznamů či monitoring provozu na sítích. Mezi „mírnější", méně vstupující do základních práv a svobod zacílených subjektů, bude pravděpodobně patřit krycí dokumentace, respektive krycí prostředky s tím, že i tak se nejedná o běžně svěřený prostředek orgánům veřejné moci pro zajišťování jejích úkolů.

3.1 Struktura povinností a nástroje v kyberbezpečnosti

Kybernetická bezpečnost přesahuje do více oblastí práva a je upravena v mnoha předpisech. V navazujícím textu se plně zaměřuji na povinnosti koncentrované v ZKB.ZKB chrání prostředí a neupravuje práva a povinnosti koncových uživatelů přímo. Se zachováním této koncepce počítá i připravovaná legislativa na úrovni EU v podobě směrnice NIS II, která navazuje na původní a nyní platnou směrnici NIS.

3.1.1 Okruh povinných subjektů podle ZKB

Povinné osoby, na které lze uplatnit instituty podle ZKB jsou definovány v § 3 ZKB. Jedná se o tyto subjekty tříděné do kategorií podle jejich zaměření a významu pro zajištění kybernetické bezpečnosti:

- poskytovatel služby elektronických komunikací59 a subjekt zajišťující síť elektronických komunikací (§ 3 písm. a) ZKB);
- orgán nebo osoba zajišťující významnou síť (§ 3 písm. b) ZKB);
- správce a provozovatel informačního systému kritické informační infrastruktury (§ 3 písm. c) ZKB);
- správce a provozovatel komunikačního systému kritické informační infrastruktury (§ 3 písm. d) ZKB);
- správce a provozovatel významného informačního systému (§ 3 písm. e) ZKB);
- správce a provozovatel informačního systému základní služby (§ 3 písm. f) ZKB);
- provozovatel základní služby (§ 3 písm. g) ZKB);
- poskytovatel digitální služby (§ 3 písm. h) ZKB).
-

3.1.2 Rozdíl mezi kybernetickou bezpečností a kybernetickou obranou

Definice kybernetické obrany není v českém právním prostředí jednotná a vymezení tohoto pojmu, na kterém by co do rozsahu panovala přesná shoda, bychom hledali stěží. Ostatně ani legální definici tohoto pojmuv českém právním řádu nenajdeme.50 Obecný konsensus panuje na tom, že při širším chápání kybernetické bezpečnosti do ní lze zahrnout také kybernetickou obranu – kybernetická obrana tvoří jednu z jejích „podmnožin“. Tento pohled potvrzuje samo Vojenské zpravodajství ČR jako subjekt odpovědný za zajišťování kyberobrany na svých oficiálních webových stránkách a další zdroje, například strategie EU, odborné publikace a v neposlední řadě kvalifikační práce. Uvedené prameny obdobně definují oblast kybernetické obrany jako součást kybernetické bezpečnosti v širším smyslu, jež je zajišťována v rámci aktivit zpravodajských služeb či armády se zaměřením na obranu státu před útoky proti státu jako takovému za pomocí kybernetických zbraní. Zajišťováním „všeobecné“ obrany státu, včetně složky kybernetické obrany, se rozumí ve smyslu zákona č. 222/1999 Sb., o zajišťování obrany České republiky, ve znění pozdějších předpisů, „souhrn opatření

k zajištění svrchovanosti, územní celistvosti, principů demokracie a právního státu, ochrany života obyvatel a jejich majetku před vnějším napadením“. Snahou a cílem kybernetické obrany je v souladu se zákonnou definicí především vybudovat funkční a zároveň efektivní systém, kterým budou zastaveny a odvráceny vnější kybernetické útoky na zmíněné chráněné hodnoty. Oproti kybernetické bezpečnosti v užším významu budou zpravidla využity mnohem invazivnější nástroje, metody a postupy. To je dáno už charakterem oprávněných subjektů k zajišťování obrany, podmínkami jejich zmocnění, jakož i tím, že předpisy upravující jejich činnost dávají silné pravomoci i prostředky k provádění jejich činnosti. Například Vojenské zpravodajství jako jeden z působících orgánů kybernetické obrany provádí tzv. cílenou detekci kybernetických útoků majících původ v zahraničí, směřuje-li takový útok proti důležitým zájmům státu. krajním případě je Vojenské zpravodajství oprávněno provést tzv. aktivní zásah ve smyslu § 16g zákona o Vojenském zpravodajství.

Jinými slovy, zanedbatelné incidenty v kontextu obrany České republiky Vojenské zpravodajství vůbec neřeší ani pravomoc řešit mít nebude, jelikož se nejedná o důležitý zájem státu. Tomu odpovídají i nástroje, které jsou institucionálnímu zajištění kyberobrany k dispozici, spadá-li incident do jejich působnosti. Mezi nejsilnější nástroje, které za splnění podmínek zákona může Vojenské zpravodajství využít, patří odposlechy, kontrola zásilek, sledování osob a věcí, pořizování audiovizuálních záznamů či monitoring provozu na sítích. Mezi „mírnější“, méně stupující do základních práv a svobod zacílených subjektů, bude pravděpodobně patřit krycí dokumentace, respektive krycí prostředky s tím, že i tak se nejedná o běžně svěřený prostředek orgánům veřejné moci pro zajišťování jejích úkolů.

3.1.3 Povinnosti subjektů a nástroje k zajištění bezpečnosti

V závislosti na zařazení do skupiny dle ZKB musí subjekt plnit dané povinnosti a lze vůči němu použít různé nástroje. ZKB stanovuje v zásadě 7 typů povinností, a to:

1. hlášení kontaktních údajů;
2. hlášení kybernetických bezpečnostních incidentů;
3. detekce kybernetických bezpečnostních událostí;
4. implementace a provádění bezpečnostních opatření;
5. provádění reaktivních opatření a oznámení o jejich provedení;
6. provádění ochranných opatření;
7. zohlednění požadavků na dodavatele

3.1.4 Hlášení kontaktních údajů

Hlásit údaje musí každý, na koho dopadá ZKB. V případě jejich změny, nejedná-li se o referenční údaje, je rovněž nutné změnu ihned oznámit příslušnému subjektu, který vede evidenci – to může být vládní nebo národníCERT. Díky tomu je snadné v případě potřeby (například za účelem doručení varování) neprodleně zkontaktovat povinný subjekt. Ke splnění této povinnosti je nutné využít předepsaný formulář na stránkách NÚKIB.

3.1.5 Hlášení kybernetických bezpečnostních incidentů

Podle § 7 odst. 2 ZKB 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“. Dle metodiky NÚKIB je důležité zdůraznit, že plánované servisní zásahy nespadají (nedojde-li k odchýlení od původního záměru) pod tuto definici, přestože v ní není obsažen definiční znak neočekávanosti. Cílem hlášení incidentů je především asistence a pomoc zainteresovaných týmů s vhodným řešením a koordinace společného postupu za předpokladu, že bezpečnostní incident cílí na více subjektů. Jedná se o projev regulatorní techniky tzv. chytrých pravidel.

Zamlčení bezpečnostního incidentu je přestupkem podle § odst. 2 písm. b) s pokutou do 1 000 000 Kč. Hlášení incidentů je jednoduchý a relativně nenákladný způsob, jak přispět ke zvýšení kybernetické bezpečnosti, a které pomáhá vyvažovat „asymetričnost“ vztahu útočníka a obránce (subjektu chránícího infrastrukturu). Přestože to není cílem ZKB, důležitou vedlejší funkcí může být motivace adresátů investovat do kybernetické bezpečnosti.

3.1.6 Detekce kybernetických bezpečnostních událostí

Rozdíl mezi kybernetickým bezpečnostním incidentem a událostí spočívá v tom, že událost má „pouze“ potenciál stát se incidentem, kdežto incident znamená skutečné narušení bezpečnosti.89 Vybrané skupiny povinných subjektů tak mají za úkol nejen hlásit incidenty, ale předcházet jim mimo jiné tím, že budou detekovat jakékoli hrozby vedoucí k možnému bezpečnostnímu incidentu.

3.1.7 Bezpečnostní opatření

Nosným pilířem, na kterém stojí celá systematika ZKB, je ochrana prostředí za pomocí bezpečnostních opatření. Povinnost implementovat a provádět bezpečnostní opatření je vázána na kritickou informační infrastrukturu, významné informační systémy, základní službu a parciálně digitální službu. Jedná se o soubor organizačních opatření, technických opatření, bezpečnostní politiky a bezpečnostní dokumentace, jejich správně volená kombinace může předcházet vzniku kybernetických bezpečnostních incidentů, případně zmírnit jejich reálný dopad. Jinými slovy bezpečnostním opatřením může být jak aplikace vyspělých kryptografických nástrojů, zabezpečení fyzického perimetru a přístupu k hardware i software, tak i triviální metodiky pro zaměstnance.

4 Scénáře

Zadání 1

Národní strategie kybernetické bezpečnosti (NIS) je dokument, který obsahuje směrnice pro ochranu kybernetické bezpečnosti v České republice. Vaším úkolem bude seznámit se s tímto dokumentem a odpovědět na tyto otázky:

1. Co je Národní strategie kybernetické bezpečnosti (NIS) a jaké jsou její cíle?
2. Jaká jsou nejvýznamnější rizika v oblasti kybernetické bezpečnosti v České republice a jak se NIS snaží tato rizika minimalizovat? Jaká rizika se týkají společnosti, ve které pracujete? (sektorové zaměření společnosti si můžete zvolit)
3. Na jaké klíčové prvky musíte myslet v případě, že z Vaší pozice je nutné dodržovat směrnici NIS? Jak tato směrnice definuje spolupráci mezi vládou, společností, ve které pracujete, ale i Vámi samotnými jako jednotlivcem?
4. Jaká jsou důležitá opatření, která by měla být přijata pro zajištění kybernetické bezpečnosti ve Vaší organizaci (opět s přihlédnutím k typu Vámi zvolené společnosti) a jak mohou být tato opatření uplatněna v praxi?

Řešení

1. **Národní strategie kybernetické bezpečnosti (NIS)** je dokument, který byl vytvořen vládou České republiky a obsahuje směrnice pro ochranu kybernetické bezpečnosti v ČR. Hlavním cílem této strategie je

minimalizovat rizika spojená s kybernetickými hrozbami a zajistit bezpečné a spolehlivé fungování digitálních služeb v ČR.

2. **Mezi nejvýznamnější rizika v oblasti kybernetické bezpečnosti** patří například útoky na informační systémy, využití malware, phishing, ransomware a další. NIS se snaží tato rizika minimalizovat pomocí několika opatření, jako jsou například vytváření standardů pro zabezpečení informačních systémů, zajišťování dostatečného školení v oblasti kybernetické bezpečnosti a spolupráce mezi vládou, podniky a jednotlivci.

3. **Klíčovými prvky NIS jsou:**

   - **Identifikace a hodnocení kybernetických rizik:** NIS se snaží identifikovat a hodnotit kybernetická rizika, aby bylo možné přijmout opatření na minimalizaci těchto rizik.
   - **Prevence a ochrana:** NIS stanovuje opatření pro prevenci a ochranu před kybernetickými hrozbami, jako jsou například standardy pro zabezpečení informačních systémů, monitorování síťového provozu a způsobů výměny informací o kybernetických hrozbách.
   - **Odpověď na incidenty:** NIS stanovuje postupy pro řešení kybernetických incidentů, jako jsou například útoky na informační systémy a úniky dat. Tyto postupy mají minimalizovat dopad incidentů a zajistit rychlou obnovu funkcí kritických informačních systémů.
   - **Spolupráce:** NIS podporuje spolupráci mezi vládou, podniky a jednotlivci v oblasti kybernetické bezpečnosti. Spolupráce má za cíl minimalizovat kybernetická rizika a zlepšit reakci na kybernetické hrozby.

4. **Pro zajištění kybernetické bezpečnosti** je důležité přijmout několik opatření. Tato opatření by měla být přizpůsobena konkrétním potřebám a rizikům organizace. Některá z důležitých opatření jsou například:

   - **Zabezpečení informačních systémů:** Organizace by měly mít stanovené standardy pro zabezpečení svých informačních systémů a provádět pravidelné auditování a testování zabezpečení.
   - **Školení zaměstnanců:** Zaměstnanci jsou často slabým místem v kybernetické bezpečnosti. Proto je důležité, aby byli školeni v oblasti kybernetické bezpečnosti a měli povědomí o rizicích spojených s používáním informačních technologií.
   - **Zálohování dat:** Zálohování dat je důležité pro minimalizaci dopadů kybernetických incidentů, jako jsou například útoky ransomware. Organizace by měly mít vytvořené plány pro zálohování dat a pravidelně testovat obnovu dat z těchto záloh.

- **Využití bezpečnostních nástrojů:** Organizace by měly využívat bezpečnostní nástroje, jako jsou například antivirové programy nebo programy pro šifrování komunikace.

Zadání 2

Jste pracovníkem kybernetické bezpečnosti ve střední organizaci s počtem zaměstnanců do 250 osob (zvolte, čím se Vaše organizace bude zabývat – důležité pro následující úkoly). Vaším úkolem je navrhnout možná zabezpečení dle směrnice ISO 27000, která pomohou minimalizovat rizika pro Vaši organizaci. Pro každé navržené zabezpečení uveďte příklad ohrožení, které by se mohlo projevit, kdyby toto zabezpečení nebylo použito.

Řešení

1. **Zavedení politiky pro správu hesel**
   - **Ohrožení:** Neoprávněný přístup k informačním systémům organizace. Pokud zaměstnanci používají slabá hesla, která lze snadno uhodnout, je riziko, že se do informačních systémů dostanou neoprávněné osoby, které mohou způsobit škodu.
   - **Zabezpečení:** Zavedení politiky pro správu hesel, která vyžaduje silná hesla, pravidelnou změnu hesel a omezení počtu neúspěšných pokusů o přihlášení.
2. **Zabezpečení sítě pomocí firewallů**
   - **Ohrožení:** Neoprávněný přístup k informačním systémům organizace přes internet. Pokud organizace nemá zabezpečenou svou síť pomocí firewallu, může se stát, že se útočníci dostanou do sítě organizace a způsobí škodu.
   - **Zabezpečení:** Zabezpečení sítě pomocí firewallu, který monitoruje síťový provoz a blokuje neoprávněné pokusy o přístup.
3. **Školení zaměstnanců v oblasti kybernetické bezpečnosti**
   - **Ohrožení:** Zaměstnanci organizace mohou být cílem phishingových útoků nebo mohou neúmyslně ohrozit bezpečnost informačních systémů organizace.
   - **Zabezpečení:** Školení zaměstnanců v oblasti kybernetické bezpečnosti, které je naučí rozpoznat phishingové e-maily a zajistí, že budou dodržovat stanovené postupy pro zabezpečení informačních systémů.

Zadání 3

Jste na obchodním jednání. Zákazník si přeje pro svou organizaci implementovat vhodnou infrastrukturu IT oddělení. Stručně svého zákazníka seznamte s tím, co jsou IT rámce infrastruktury COBIT a ITIL. Uveďte mezi nimi příklady 3 odlišností a 3 shod. Souvisí COBIT a ITIL také s dalšími existujícími dokumenty či legislativou?

Řešení

Co jsou ITIL a COBIT

ITIL je soubor osmi knihoven, které poskytují osvědčené postupy a doporučení pro správu IT služeb. ITIL se zaměřuje na procesy a postupy, které mají zajistit, že IT služby jsou dodávány s maximální efektivitou a efektivitou.

COBIT je rámec, který poskytuje celkovou kontrolu nad informačními technologiemi a poskytuje různé cíle řízení, kontroly a auditu informačních technologií. COBIT se zaměřuje na procesy a postupy, jež zajistí, že informační technologie jsou spravovány v souladu s podnikovými cíli a strategiemi.

Rozdíly

1. **Zaměření:** ITIL se zaměřuje na procesy správy služeb, zatímco COBIT se zaměřuje na správu a řízení IT jako celku.
2. **Obecnost:** COBIT poskytuje obecný rámec pro řízení IT, zatímco ITIL je specifický pro správu služeb.
3. **Způsob implementace:** ITIL poskytuje návod krok za krokem na implementaci, zatímco COBIT poskytuje spíše obecné směrnice a doporučení.
4. **Měření a hodnocení:** COBIT klade větší důraz na měření a hodnocení, zatímco ITIL se více zaměřuje na procesy a postupy.
5. **Rozsah:** COBIT pokrývá širší oblasti IT, zatímco ITIL se zaměřuje pouze na správu služeb.

Shody

1. **Oba rámce jsou zaměřené na řízení IT a zvyšování hodnoty IT** pro organizaci.
2. **Oba rámce se snaží zajistit kvalitu služeb IT a vylepšit výkon**.

3. **Oba rámce jsou používány k dosažení souladu s normami a regulacemi** v oblasti IT.
4. **Obě infrastruktury se zaměřují na zlepšení výkonu a efektivity** v oblasti IT. ITIL se zaměřuje na poskytování služeb a procesů IT, zatímco COBIT se zaměřuje na řízení a kontrolu IT.
5. **ITIL i COBIT jsou pružné rámcové struktury**, které lze upravit a přizpůsobit konkrétním potřebám a prostředí organizace, v níž jsou aplikovány.

Zadání 4

Porovnejte směrnice NIS a NIS2 (směrnice EU, která vstoupí v platnost roku 2024) a určete jejich hlavní rozdíly a dopady na další vývoj nastavených procesů z pohledu kybernetické bezpečnosti ve Vámi zvolené společnosti.

1. Jaké jsou hlavní rozdíly mezi směrnicí NIS a NIS2?
2. Jaký je rozsah působnosti obou směrnic?
3. Jaké jsou hlavní cíle a principy směrnic NIS a NIS2?
4. Jak se liší požadavky na zabezpečení informačních systémů podle obou směrnic?
5. Jaké jsou hlavní povinnosti organizací podle směrnic NIS a NIS2?

Řešení

1. **Hlavní rozdíly mezi směrnicemi NIS a NIS2 jsou:**
   - **NIS2 rozšiřuje rozsah působnosti** směrnice o služby digitálního hospodářství a digitální platformy.
   - **NIS2 klade větší důraz na spolupráci mezi členskými státy EU** a zahrnuje nová opatření na ochranu kritických digitálních služeb.
   - **NIS2 stanovuje nové požadavky na bezpečnost dodavatelů** digitálních služeb a jejich kontrolu.
2. **Rozsah působnosti směrnic NIS a NIS2** se mírně liší. Zatímco směrnice NIS se zaměřuje na kritické infrastruktury, NIS2 rozšiřuje rozsah působnosti o služby digitálního hospodářství a digitální platformy.
3. **Hlavní cíle a principy směrnic NIS a NIS2** jsou podobné, ale NIS2 klade větší důraz na spolupráci mezi členskými státy EU a ochranu kritických digitálních služeb.

4. **Požadavky na zabezpečení informačních systémů** jsou odlišné dle obou směrnic. NIS se zaměřuje na zabezpečení kritických infrastruktur, zatímco NIS2 klade větší důraz na ochranu digitálních služeb.
5. **Hlavní povinnosti organizací podle směrnic NIS a NIS2** jsou odlišné. NIS stanovuje požadavky na zabezpečení kritických infrastruktur a stanovuje povinnosti pro provozovatele a správce těchto infrastruktur. NIS2 klade větší důraz na spolupráci mezi členskými státy EU a na ochranu digitálních služeb a stanovuje nové požadavky na bezpečnost dodavatelů digitálních služeb.

Shrnutí a závěr

Kybernetická bezpečnost představuje současnou a s narůstajícím počtem uživatelů informačních a komunikačních technologií zejména budoucí výzvu, jak přistoupit k regulaci prostředí a zajištění dostatečné bezpečnostní úrovně. Česká republika má slibně nakročeno k tomu, aby udávala trendy ve vývoji této oblasti a regulatorním přístupu. Kybernetická bezpečnost je nejen v České republice, ale také na úrovni Evropské unie klíčovou prioritou. Státní instituce i jiné organizace si uvědomují svoji závislost na moderních technologiích a nezbytnost zajištění bezpečnosti kyberprostoru jako podmínky pro uspokojivý globální vývoj. Cílem vyvíjené snahy je optimálně nastavit právní rámec pro klíčové subjekty a odvětví na úrovni státu i celé Evropské unie.

Seznam použitých zdrojů

[1] Hathaway, M. E., Klimburg, K. *Preliminary Considerations: On National Cybersecurity*. In: National Cybersecurity – Framework Manual.Talinn, NATO CCD COE, 2012. Dostupné zde: https://www.belfercenter.org/sites/default/files/legacy/files/hathaway-klimburgnato-manual-ch-1.pdf

[2] Jirásek, P., Novák, L., Požár, J. *Výkladový slovník kybernetické bezpečnosti*. Praha: CZ.NIC, 2019. Dostupné zde: https://cybersecurity.cz/data/slovnik_v310.pdf

[3] Kolouch, J. a kol. *Cybersecurity.* Praha: CZ.NIC, 2019.

[4] Kremling, J., Sharp Parker, M. A. *Cyberspace, Cybersecurity, and Cybercrime*. SAGE Publications, 2018.

[5] Maisner, M., Vlachová, B. *Zákon o kybernetické bezpečnosti: Komentář*. Praha: Wolters Kluwer, 2015.

[6] Polčák, R. a kol. *Právo informačních technologií*. Praha: Wolters Kluwer, 2018.

[7] Polčák, R. *Internet a proměny práva*. Praha: Auditorium, 2012.

[8] Přívora, J. *Právní nástroje národní kybernetické bezpečnosti*. Masarykova univerzita. Brno 2022.

[9] Šulc, V. *Kybernetická bezpečnost*. Plzeň: Aleš Čeněk, 2018. ISBN 978-80-7380-737-5.