Politika informační bezpečnosti, Dodatek

PV 017 ◇ Bezpečnost IT

Jan Staudek
http://www.fi.muni.cz/usr/staudek/vyuka/

Verze : podzim 2019

Obsah dodatku

XXX tipů pro tvorbu politiky informační bezpečnosti

- Bezpečnostní politika je nejefektivnější, když si ji organizace napíše sama
  - ✓ Vypsáním bezpečnostních cílů a plánů se vytváří dokument, který lze využít pro více účelů
    - je návodem kam zaměřovat zabezpečovací úsilí
    - pomáhá měřit úspěšnost a/nebo postup implementace bezpečnosti
    - jestliže dojde k chybnému zaměření nebo se zjistí neúspěšnost postupu, pomůže najít správné zaměření dalšího pracovního úsilí
    - je základem pro budoucí rozvoj a dolaďování bezpečnosti
  - ✓ Napsanou BP mohou autorizovaní jedinci číst a hodnotit.
  - ✓ Napsaná BP se stává společným standardem pro implementaci, řízení a administraci informační bezpečnosti v organizaci
  - ✓ Bez napsané BP úsilí bude zabezpečovací úsilí chaotické, necílevědomé a mnohdy nespolehlivé.
  - ✓ Napsaná BP je pevným základem pro úspěšnost zabezpečovacího úsilí.

XXX tipů pro tvorbu politiky informační bezpečnosti

- Politika informační bezpečnosti by měla být klíčovým faktorem při všech rozhodnutích o činnosti organizace, není pravda, že ovlivňuje činnost pouze IT oddělení
  - ✓ Byly doby, kdy byl problém informační bezpečnosti považovaný za problém počítačových ,,exotů''
  - ✓ Ve světle současné informační ekonomiky je bezpečnost informací bázovým požadavkem napříč všemi aspekty malé i velké organizace.
  - ✓ Bez účelného zajištění informační bezpečnosti je organizace vystavena rizikům útoků jak zvenčí, tak i zevnitř i rizikům náhodných chyb.
  - ✓ Prosazování bezpečnostní politiky v rámci všech významných podnikatelských rozhodnutí je pomáhá především z hlediska dlouhodobého zachování profilu organizace než při řešení okamžitých bezpečnostních problémů

    (řešení takových problémů podporuje Plán zvládnutí rizik)

XXX tipů pro tvorbu politiky informační bezpečnosti

- Zaměstnanci musí být školení pro dodržování bezpečnostní politiky
  - ✓ Je chybou očekávat, že že zaměstnanci budou dodržovat bezpečnostní politiku, pokud si nejsou vědomi její existence a jejího obsahu.
  - ✓ Pro dlouhodobé (trvalé) dodržování bezpečnostní politiky nestačí ani jednorázové informování zaměstnanců.
  - ✓ Organizace musí zavést průběžný trvalý školící systém pro pěstování bezpečnostního uvědomění.
  - ✓ Všichni zaměstnanci mají absolvovat každý půlrok, resp. jednou ročně základní školení zaměřené na udržování minimální úrovně informační bezpečnosti v celé organizaci.
  - ✓ Na této bázi pak lze vyvinout specifická školení zaměřená na konkrétní pracovní role, cílená na dosažení maximální produktivity práce při používání bezpečnostního systému.

XXX tipů pro tvorbu politiky informační bezpečnosti

- ✓ Všechna bezpečnostní školení musí být revidována tak často, jak je aktualizována bezpečnostní politika.
- ✓ Zaměstnance, kteří opakovaně porušují bezpečnostní pravidla, se nutné proškolit dodatečnými, rozšiřujícími kurzy.
- ✓ Pokud po takových dodatečných školeních zaměstnanec dále porušuje bezpečnost, musí být z pozice, na které bezpečnost porušuje, uvolněný

XXX tipů pro tvorbu politiky informační bezpečnosti

- Bezpečnostní politika nebude organizaci chránit před všemi možnými hrozbami.
  - ✓ Cílem bezpečnostní politiky je snížení rizika na akceptovatelnou úroveň
  - ✓ Její řádné zavedení a prosazování zmaří většinu generických útoků
  - ✓ I při neomezeném rozpočtu, vždy budou existovat neznámá rizika, neznámé hrozby a neočekávané útoky, které bezpečnost informací poruší.
  - ✓ Žádná implementace bezpečnosti nezaručí perfektní bezpečnost, perfektní bezpečnostní opatření neexistuje, neexistují nenapadnutelné infrastruktury
  - ✓ Smyslem zavedení informační bezpečnosti je dát organizaci tu největší šanci odvrátit nebo přežít útoky, nikoli zaručit perfektní bezpečnost

XXX tipů pro tvorbu politiky informační bezpečnosti

- Účinná bezpečnostní politika je bezpečnostní politika, která se trvale aktualizuje a reviduje
  - ✓ Nic netrvá věčně, nic netrvá – *Panta rhei* – všechno plyne pravil pravil Platon, když interpretoval Hérakleitovo *Nelze dvakrát vstoupit do téže řeky*
  - ✓ Bezpečnost není nikdy statický stav, rizika a hrozby, jimž čelí organizace se neustále mění.
  - ✓ Chápání bezpečnosti rychle zastará a bude nedostatečné, pokud není pravidelně revidováno a zlepšováno.
  - ✓ Útočníci rozvíjejí nové útoky každodenně.
  - ✓ Organizace musí své bezpečnostní ochrany zlepšovat alespoň se stejnou frekvencí jako útočníci

XXX tipů pro tvorbu politiky informační bezpečnosti

- Bezpečnostní politika má zahrnovat sledování výkonu.
  - ✓ Je jedním z nejvíce přehlíženým cílů informační bezpečnosti je ochrana dostupnosti.
  - ✓ Výrazně se požaduje ochrana důvěrnosti a integrity, ochrana dostupnosti se často ignoruje.
  - ✓ Jeden aspekt ochrany dostupnosti je sledování výkonu.
  - ✓ Sledování trendů propustnosti, zpoždění, chyb, přenosových toků, frontování zpráv, chyb při komunikaci, včasnosti varování na selhání hardware, nálady zaměstnanců, infekcí škodlivým software nebo penetrací, umožní si všimnou problému dříve, než nastane.
  - ✓ Ochrana před ztrátou energie se má zaměřit na včasnost detekce a prevence, nikoli na rychlou reakci a zotavení.

XXX tipů pro tvorbu politiky informační bezpečnosti

- Co nemůžete obhájit / dokázat u soudu, není ani spolehlivé ani užitečné pro bezpečnost.
  - ✓ Pokud zajištění bezpečnosti organizaci nepomůže vyhrát soudní případ, zabránit placení pokut za porušování regulačních omezení nebo ochránit před ručením či nedbalostmi, tak prostě není dobré.
  - ✓ Aby organizace mohla potrestat potrestat podezřelého, musí mít silné důkazy o tom, co se dělo a kdo to dělal.
  - ✓ Musí existovat konkrétní dokumentované politiky, ty se musí přísně dodržovat, musí existovat chráněné auditní systémy, jasné vymezení autorizace a neobejitelná autentizace.
  - ✓ V týmu vyvíjejícím bezpečnostní politiku by měl participovat technicky orientovaný právník.
  - ✓ Bezpečnost musí být implementovaná tak, aby výsledkem podání žaloby bylo vynesení rozsudku ve prospěch organizace a ne odhalení nedostatků v organizaci.

XXX tipů pro tvorbu politiky informační bezpečnosti

- Všichni musí dodržovat bezpečnostní politiky nebo čelit důsledkům
  - ✓ Žádné výjimky, žádná božská královská práva, žádné předpokládané nároky.
  - ✓ Kdo pracujete v/s/pro organizaci, musí dodržovat její bezpečnostní politiky.
  - ✓ Odpovědnost za bezpečnost má každý v celé personální hierarchii, od vrcholového vedení až po posledního zaměstnance
  - ✓ Každý je fakticky členem bezpečnostní týmu
  - ✓ Pokud někdo aktivně nepodporuje bezpečnost, bezpečnostní úsilí organizace podkopává
  - ✓ Když zaměstnanci vidí, že členové vedení nedodržují pravidla, ignorují nebo aktivně porušují restrikce, vnímají tato omezení jako umělá a bezvýznamná
  - ✓ Co musí dodržovat zaměstnanec, musí dodržovat i vrcholové vedení
  - ✓ Když dojde k narušování bezpečnosti, musí být odpovídající aktivity zastaveny a musí být aplikovány adekvátní reakce a původce musí čelit důsledkům.

XXX tipů pro tvorbu politiky informační bezpečnosti

- Zaměstnanci potřebují uvolnění.
  - ✓ Studie prokázaly, že zaměření na pracovní úkoly po dobu delší než 50 minut v době bez 5 až 10 minutové přestávky způsobuje snížení produktivity.
  - ✓ Pokud se taková možnost relaxace zaměstnancům neposkytne, budou si hledat vlastní skryté cesty k takovému uvolnění
  - ✓ Je důležité usilovat vyváženost mezi lidskou přirozeností a bezpečností a poskytnout zaměstnancům jisté množství nepracovní svobody
  - ✓ To si může vyžádat vytvoření zvláštních síťových cest, virtuálních systémů nebo alternativních ,,hracích/relaxačních prostorů''
  - ✓ Pokud je jistá svoboda poskytnuta v primárním produkčním prostředí musí se zmírnit přísnost Internetových filtrů, zákazů používání některého software.
  - ✓ Zaměstnanci musí být informováni, že toto je jim nabízeno jako privilegium, že jsou zaměstnání proto, aby plnili pracovní úkoly. A jakmile se produktivita sníží, toto privilegium se odebere.

XXX tipů pro tvorbu politiky informační bezpečnosti

- Bezpečnostní politika je předmětem k diskusi.
  - ✓ To, že všichni v organizaci mají dodržovat bezpečnostní politiku, ještě neznamená, že s ní všichni souhlasí.
  - ✓ Všem zaměstnancům na všech úrovních má být dána možnost politiku kritizovat a vznášet návrhy na změny její implementace.
  - ✓ Návrhy nemusí být akceptovány, ale otevření se vnitřní diskusi a debatám o bezpečnosti vede ke zdravější bezpečnosti, k produktivnějším a bezpečnějším infrastrukturám. A zaměstnaci budou zasvětěnější a spokojenejší.

XXX tipů pro tvorbu politiky informační bezpečnosti

- Účinnost a přijatelnost bezpečnosti jsou dva neoddělitelné faktory.
  - ✓ Bezpečnost vyžaduje udržovat rovnováhu mezi účinnými preventivními opatřeními eliminujícími nežádoucí události a únosnou komplikací pracovních činností autorizovaných osob
  - ✓ Obstrukční, těžkopádné, narušující nebo obtěžující opatření budou obcházena, porušována či likvidována.

XXX tipů pro tvorbu politiky informační bezpečnosti

- Bezpečnostní politika musí být jasná, čtivá, srozumitelná
  - ✓ Nepište bezpečnostní politiky v komplikované jazyku právních předpisů nebo pouze pomocí obrázků,
  - ✓ Všechny položky v bezpečnostní politice vyjádřete explicitně a snadno pochopitelnou formou
  - ✓ Každou akci nebo omezení kladené na pracovníka napište, vyjádřete alespoň třemi způsoby, pokud to jde. Vždy použijte jiná slov, jiné pojmy.
  - ✓ Buďte si jistí, že každý čtenář bezpečnostní politiky plně chápe co se od něj očekává.
  - ✓ Neporozumění a možnost odlišných výkladů bezpečnostních návodů vede k porušování bezpečnosti.

XXX tipů pro tvorbu politiky informační bezpečnosti

- Předpisy a dosažení souladu s nimi jsou nutné zla
  - ✓ Každý, kdo pracuje podle předpisů, zákonů nebo příkazů ví, že je nesmírně důležité být s nimi v souladu.
  - ✓ Jejich nedodržení může vést k přísným pokutám, k odebrání autorizace, ke ztrátě klientů/zákazníků, ke zrušení smlouvy, může mít právní důsledky apod.
  - ✓ Při navrhování a psaní bezpečnostní politiky, je nutné začít s předpisy jako se základem, a pak lze expandovat na další bezpečnostní prvky z celé bezpečnostní infrastruktury.
  - ✓ Po dokončení tvorby bezpečnostní politiky, vždy zkontrolujte, že soulad s předpisy zůstal uchován.

XXX tipů pro tvorbu politiky informační bezpečnosti

- Když jste na pochybách, konzultujte standardy
  - ✓ Vytvoření bezpečnostní politiky se stalo standardní podnikatelskou činnosti, ale ne všichni představitelé organizace mají vždy dostatečné znalosti k vytvoření nebo ke zhodnocení bezpečnostní politiky.
  - ✓ Primární zdroje pro získání znalostí, resp. pro porovnání, zda postupujete správně, jsou např.
    - NIST SP 800-100 - Information Security Handbook
    - ISO 27002 - Information technology - Security techniques - Code of practice for information security management
    - Standard of Good Practice (SoGP) - Information Security Forum (ISF)
    - IT GOVERNANCE, A Manager's Guide to Data Security and ISO 27001/ISO 27002, Alan Calder & Steve Watkins, Kogan Page Limited, ISBN 978 0 7494 5271 1

Dodatek, politika dle zákona o kyb. bezpečnosti

- Struktura politiky informační bezpečnosti dle zákona o kybernetické bezpečnosti

Dodatek, politika dle zákona o kyb. bezpečnosti

- Politika systému řízení informační bezpečnosti
  - ✓ Cíle, principy a potřeby řízení informační bezpečnosti
  - ✓ Rozsah a hranice systému řízení informační bezpečnosti
  - ✓ Pravidla a postupy pro řízení dokumentace
  - ✓ Pravidla a postupy pro řízení zdrojů a provozu systému řízení informační bezpečnosti
  - ✓ Pravidla a postupy pro provádění auditů kybernetické bezpečnosti
  - ✓ Pravidla a postupy pro přezkoumání systému řízení informační bezpečnosti
  - ✓ Pravidla a postupy pro nápravná opatření a zlepšování systému řízení informační bezpečnosti

Dodatek, politika dle zákona o kyb. bezpečnosti

- Politika organizační bezpečnosti
  - ✓ Určení bezpečnostních rolí a jejich práv a povinností
    - Práva a povinnosti manažera informační bezpečnosti
    - Práva a povinnosti architekta informační bezpečnosti
    - Práva a povinnosti auditora informační bezpečnosti
    - Práva a povinnosti garanta (vlastníka) aktiv
    - Práva a povinnosti výboru pro řízení informační bezpečnosti
  - ✓ Požadavky na oddělení odpovědností
- Politika řízení dodavatelů
  - ✓ Pravidla a principy pro výběr dodavatelů
  - ✓ Pravidla pro hodnocení rizik dodavatelů
  - ✓ Náležitosti smlouvy o úrovni služeb a způsobů a úrovní realizace bezpečnostních opatření a o určení vzájemné smluvní odpovědnosti
  - ✓ Pravidla pro provádění kontroly zavedení bezpečnostních opatření
  - ✓ Pravidla pro hodnocení dodavatelů

Dodatek, politika dle zákona o kyb. bezpečnosti

- Politika klasifikace aktiv
  - ✓ Identifikace, hodnocení a evidence primárních aktiv
    - – Určení a evidence jednotlivých aktiv včetně určení jejich garanta
    - – Hodnocení důležitosti aktiv z hlediska důvěrnosti, integrity a dostupnosti
  - ✓ Pravidla ochrany jednotlivých úrovní aktiv
    - – Způsoby rozlišování jednotlivých úrovní aktiv
    - – Pravidla pro manipulaci a evidenci aktiv podle úrovní aktiv
    - – Přípustné způsoby používání aktiv
  - ✓ Způsoby spolehlivého smazání nebo ničení paměťových médií

Dodatek, politika dle zákona o kyb. bezpečnosti

- Politika bezpečnosti lidských zdrojů
  - ✓ Pravidla rozvoje bezpečnostního povědomí a způsoby jeho hodnocení
    - – způsoby a formy poučení uživatelů
    - – způsoby a formy poučení garantů aktiv
    - – způsoby a formy poučení administrátorů
    - – způsoby a formy poučení dalších osob v bezpečnostních rolích
  - ✓ Bezpečnostní školení nových zaměstnanců
  - ✓ Pravidla pro řešení případů porušení bezpečnostní politiky systému řízení informační bezpečnosti
  - ✓ Pravidla pro ukončení pracovního vztahu nebo změnu pracovní pozice
    - – vrácení svěřených aktiv a odebrání práv při ukončení pracovního vztahu
    - – změna přístupových oprávnění při změně pracovní pozice

Dodatek, politika dle zákona o kyb. bezpečnosti

- Politika řízení provozu a komunikací
  - ✓ Pravomoci a odpovědnosti spojené s bezpečným provozem
  - ✓ Postupy bezpečného provozu
  - ✓ Požadavky a standardy bezpečného provozu
  - ✓ Řízení technických zranitelností
  - ✓ Pravidla a omezení pro provádění auditů kybernetické bezpečnosti a bezpečnostních testů
- Politika řízení přístupu
  - ✓ Princip minimálních oprávnění/potřeba znát (need to know)
  - ✓ Požadavky na řízení přístupu
  - ✓ Životní cyklus řízení přístupu
  - ✓ Řízení privilegovaných oprávnění
  - ✓ Řízení přístupu pro mimořádné situace
  - ✓ Pravidelná revize přístupových oprávnění včetně adresářových služeb

Dodatek, politika dle zákona o kyb. bezpečnosti

- Politika bezpečného chování uživatelů
  - ✓ Pravidla pro bezpečné nakládání s aktivy
  - ✓ Bezpečné použití přístupového hesla
  - ✓ Bezpečné použití elektronické pošty a přístupu na internet
  - ✓ Bezpečný vzdálený přístup
  - ✓ Bezpečné chování na sociálních sítích
  - ✓ Bezpečnost ve vztahu k mobilním zařízením
- Politika zálohování a obnovy
  - ✓ Požadavky na zálohování a obnovu
  - ✓ Pravidla a postupy zálohování
  - ✓ Pravidla bezpečného uložení záloh
  - ✓ Pravidla a postupy obnovy
  - ✓ Pravidla a postupy testování zálohování a obnovy

Dodatek, politika dle zákona o kyb. bezpečnosti

- Politika bezpečného předávání a výměny informací
  - ✓ Pravidla a postupy pro ochranu předávaných informací
  - ✓ Způsoby ochrany elektronické výměny informací
  - ✓ Pravidla pro využívání kryptografické ochrany
- Politika řízení technických zranitelností
  - ✓ Pravidla pro omezení instalace software
  - ✓ Pravidla a postupy vyhledávání opravných programových balíčků
  - ✓ Pravidla a postupy testování oprav software
  - ✓ Pravidla a postupy nasazení oprav software
- Politika bezpečného používání mobilních zařízení
  - ✓ Pravidla a postupy pro bezpečné používání mobilních zařízení

Dodatek, politika dle zákona o kyb. bezpečnosti

- Politika licencování softwaru a informací
  - ✓ Pravidla a postupy nasazení software a jeho evidence
  - ✓ Pravidla a postupy pro kontrolu dodržování licenčních podmínek
- Politika dlouhodobého ukládání a archivace informací
  - ✓ Pravidla a postupy archivace dokumentů a záznamů
  - ✓ Ochrana archivovaných dokumentů a záznamů
  - ✓ Politika přístupu k archivovaným dokumentům a záznamům
- Politika ochrany osobních údajů
  - ✓ Charakteristika zpracovávaných osobních údajů. Popis přijatých a provedených organizačních opatření pro ochranu osobních údajů
  - ✓ Popis přijatých a provedených technických opatření pro ochranu osobních údajů

Dodatek, politika dle zákona o kyb. bezpečnosti

- Politika fyzické bezpečnosti
  - ✓ Pravidla pro ochranu objektů
  - ✓ Pravidla pro kontrolu vstupu osob
  - ✓ Pravidla pro ochranu zařízení
  - ✓ Detekce narušení fyzické bezpečnosti
- Politika bezpečnosti sítě
  - ✓ Pravidla a postupy pro zajištění bezpečnosti sítě
  - ✓ Určení práv a povinností za bezpečný provoz sítě
  - ✓ Pravidla a postupy pro řízení přístupů v rámci sítě
  - ✓ Pravidla a postupy pro ochranu vzdáleného přístupu k síti
  - ✓ Pravidla a postupy pro monitorování sítě a vyhodnocování provozních záznamů

Dodatek, politika dle zákona o kyb. bezpečnosti

- Politika ochrany před škodlivým kódem
  - ✓ Pravidla a postupy pro ochranu komunikace mezi vnitřní a vnější sítí
  - ✓ Pravidla a postupy pro ochranu serverů a sdílených datových úložišť
  - ✓ Pravidla a postupy pro ochranu pracovních stanic
- Politika nasazení a používání nástroje pro detekci kybernetických bezpečnostních událostí
  - ✓ Pravidla a postupy nasazení nástroje pro detekci kybernetických bezpečnostních událostí
  - ✓ Provozní postupy pro vyhodnocování a reagování na detekované kybernetické bezpečnostní události
  - ✓ Pravidla a postupy pro optimalizaci nastavení nástroje pro detekci kybernetických bezpečnostních událostí

Dodatek, politika dle zákona o kyb. bezpečnosti

- Politika využití a údržby nástroje pro sběr a vyhodnocení kybernetických bezpečnostních událostí
  - ✓ Pravidla a postupy pro evidenci a vyhodnocení kybernetických bezpečnostních událostí
  - ✓ Pravidla a postupy pravidelné aktualizace pravidel pro vyhodnocení kybernetických bezpečnostních událostí
  - ✓ Pravidla a postupy pro optimální nastavení bezpečnostních vlastností nástroje pro sběr a vyhodnocení kybernetických bezpečnostních událostí
- Politika bezpečného používání kryptografické ochrany
  - ✓ úroveň ochrany s ohledem na typ a sílu kryptografického algoritmu
  - ✓ pravidla kryptografické ochrany informací
    - při přenosu po komunikačních sítích
    - při uložení na mobilní zařízení nebo vyměnitelné médium
  - ✓ systém správy klíčů