Portál pre odborné publikovanie ISSN 1338-0087

Informační podpora security managera organizace

Seidl Jaromír · Informačné technológie

25.08.2014

Kvalitní zabezpečení citlivých dat a klíčových aktiv se dnes stává pro firmu jakéhokoliv zaměření a velikosti naprostou nutností. Historie vývoje informační bezpečnosti začala především v prostředí velkých organizací, které zpracovávaly značné množství dat. Je logické, že právě větší a často bohatší firmy měly dostatek prostředků na investice do zabezpečení svých aktiv. Kromě toho, poměrně velké procento malých a středních firem má o svém informačním zabezpečení poněkud mylné informace. Stále více útočníků se zaměřuje na organizace střední velikosti, které jsou nedostatečně chráněny, a je daleko snazší se dostat k jejich citlivým datům.

Malé a střední firmy se často brání zavádění certifikovaných norem. Důvodem je obava z přílišné formální administrativy, která je u certifikací často vyžadována a která je především u malých firem zbytečná a zatěžující. U organizací střední velikosti (50-250 zaměstnanců) je už jistá administrativa spojená s informační bezpečností nutností. Zaměstnanci se podobně jako u malých firem většinou osobně znají, ale již zde existuje určitá míra anonymity, která může být impulsem k tomu, že někteří zaměstnanci se budou snažit bezpečnostní procedury obcházet, zejména když nebudou přesně definovány a jejich dodržování nebude pravidelně kontrolováno. Závisí na více okolnostech, zda je pro danou organizaci vhodnější certifikace nebo zavedení vlastní interní metodiky pro bezpečnost informací.

Úvod

Význam výpočetní techniky a využívání informačních a komunikačních technologií ve všech oblastech života společnosti neustále vzrůstá. Jen velmi těžko bychom našli odvětví nebo činnosti, do kterých tyto technologie ještě nepronikly. Zároveň s tím ale také roste nebezpečí neoprávněného přístupu nebo celkového zneužití důležitých informací. Tato skutečnost pak v činnostech organizací a podniků vyžaduje, aby při zpracování, ukládání, přenosu a využití dat nedocházelo k jejich modifikaci, chybám či dokonce ztrátě. Proto se v posledních letech stále více firem zaměřuje na ochranu svých dat a informací. Disciplína, která se zabývá ochranou citlivých dat v podniku, se nazývá informační bezpečnost.

V dnešní době se stává klíčovou činností v rámci řízení společnosti, která poskytuje strategický směr pro zabezpečení a dosažení plánovaných cílů. Dále zajišťuje, že rizika spojená s bezpečností informací jsou řádně spravována a zdroje podnikových informací jsou používány zodpovědně. Cílem řízení je poskytnout systém, který se soustředí na

všechny aspekty bezpečnosti informací a spravuje všechny související procesy. Termín „informace“ je používán jako obecný pojem a zahrnuje všechna aktiva, která mají pro činnosti organizace nějakou hodnotu.

Cílem informační bezpečnosti je chránit zájmy těch, kteří se spoléhají na informační a komunikační systémy. Jejím prvořadým úkolem je zajistit, aby organizace byla chráněna před škodami způsobenými selháním dostupnosti, důvěrnosti nebo integrity citlivých aktiv. Dosáhnout požadovaného stupně informační bezpečnosti a tedy i ochrany dat a informací lze pomocí stanovení softwarových, hardwarových, personálních, komunikačních a dalších opatření a s nimi souvisejících pravidel, postupů a funkcí. Jestliže ve světě a nyní i v naší republice je informační bezpečnosti věnována významná pozornost ve velkých organizacích, je tato oblast v malých a středně velkých organizacích nedoceněna a také neexistují vhodné nástroje pro zavedení a hodnocení opatření souvisejících s informační bezpečnosti.

1. Základní pojmy

1.1 Bezpečnostní událost

Je to identifikovaný stav informačního systému, služby nebo počítačové sítě, jež může narušit pravidla bezpečnostní politiky nebo selhání některého opatření nebo dříve neznámá nebo nepředpokládaná situace, jež může ovlivnit bezpečnost.

1.2 Bezpečnostní incident

Je to jedna nebo více nechtěných nebo neočekávaných indikovaných bezpečnostních událostí, jimiž může být s vysokou pravděpodobností narušena podpora hlavních procesů organizace nebo díky nimž může dojít k narušení bezpečnosti informačního systému.

1.3 Autentizace

Proces ověřování proklamované identity subjektu. Autentizace znamená ověřování pravosti, autentický znamená původní, pravý, hodnověrný. Autentizace patří k bezpečnostním opatřením a zajišťuje ochranu před falšováním identity, kdy se subjekt vydává za někoho, kým není. Rozlišuje se autentizace entity (osoby, programu, zařízení) a autentizace zprávy.

1.4 Autorizace

Proces zjištění oprávněnosti. Autorizovat znamená povolit, schválit, zmocnit, oprávnit. O autorizaci hovoříme, pokud určitá entita (uživatel, program, zařízení) chce přistupovat k určitým zdrojům (např. serveru, souboru, tiskárně). Aby mohla entita ke zdrojům přistoupit, musí být k tomu autorizována – oprávněna (musí mít přístupová práva). Předpokladem autorizace entity je úspěšná autentizace. [1]

1.5 Aktiva

- informační aktiva
  - databáze a datové soubory, dokumentace, uživatelské manuály, školící materiály,

interní záznamy a jiné archivované informace
- aplikační aktiva
  - aplikační a systémové programové vybavení, vývojové nástroje a utility
- fyzická aktiva
  - počítače, servery, záznamová zařízení, switche, tiskárny, skartovačky a další technická zařízení, prostory, nábytek (např. trezor)
- aktiva služeb
  - servisní služby externí a interní
- personální aktiva
  - lidé přicházející do kontaktu se zpracovávanou informací
- nehmotná aktiva
  - image, důvěryhodnost, beztrestnost/bezúhonnost

2. Řešení informační bezpečnosti

Úroveň bezpečnosti, která je v organizaci vyžadována, je možné dosáhnout pouze komplexním přístupem a podrobnou identifikací hrozeb a detailním plánováním. Výše uvedené oblasti informační bezpečnosti spolu často bezprostředně souvisí a v některých případech se dokonce vzájemně prolínají. ISO/IEC 27001 popisuje nejlepší praktiky pro zajištění bezpečnosti informací, které by organizace měla vzít v úvahu pro zajištění kontrolních cílů. 133 "základních" opatření se ale ve skutečnosti dále rozpadají na stovky specifických bezpečnostních opatření. Norma nepřikazuje, která opatření musí být bezpodmínečně aplikována, ale ponechává rozhodnutí na organizaci. Vhodná opatření jsou vybírána na základě hodnocení rizik a jejich implementace je závislá na konkrétní situaci.

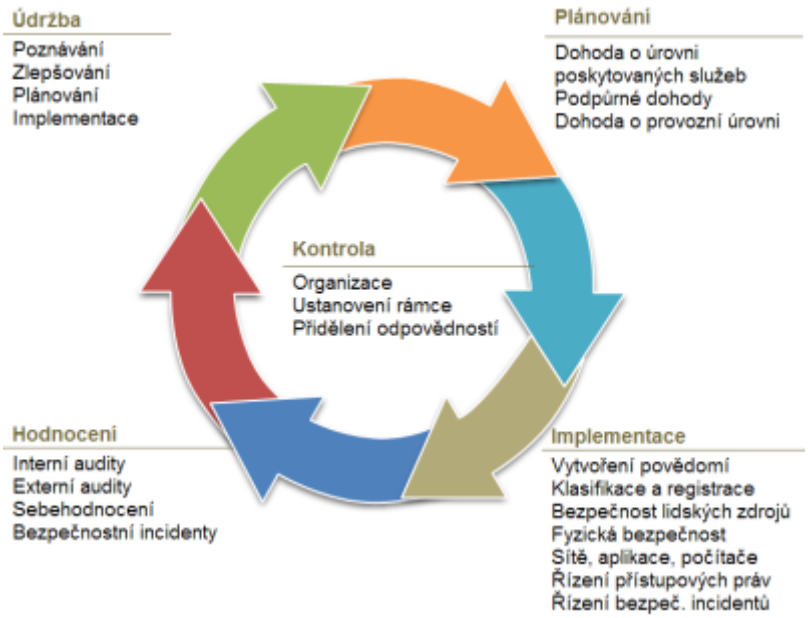
Cílem není implementovat vše, co norma popisuje, ale spíše naplnit všechny aplikovatelné cíle opatření. Tento přístup zajišťuje, že norma je široce aplikovatelná a dává uživatelům velkou flexibilitu při implementaci. Nicméně toto přináší obtíže při ne certifikaci, kdy může být složité posoudit, zda jsou aktuální bezpečnostní opatření plně v souladu s normou. V dalším textu jsou popsány základní principy všech 11 oblastí této normy včetně doporučených opatření k nim náležejícím. ISO/IEC 27001 je skupina standardů pro systém řízení informační bezpečnosti (ISMS). Tato série norem vychází od roku 2005, kdy se objevila ISO/IEC 27001, pomocí které se celý systém certifikuje. Tvůrcem těchto norem je Mezinárodní organizace pro normalizaci logické a fyzické bezpečnosti (International Organization for Standardization). [1]

3. Řízení informačních systémů

Aby byla dosažena odpovídající úroveň informační bezpečnosti, je nutné zajistit, aby všechny prostředky automatizovaného zpracování v podniku byly používány pouze oprávněnými osobami / systémy pro obchodní účely. Zapotřebí je dodržovat následující podmínky. Implementovat pravidla pro řízení přístupu ke službám na základě individuálních potřeb zobrazit, přidat, změnit nebo odstranit informace a transakce; především je nutné správně nastavit práva přístupu poskytovatelům služeb, dodavatelům a zákazníkům. Ujistit se, že jsou přiděleny odpovídající odpovědnosti pro správu všech uživatelských účtů a prostředků zabezpečení (např. hesel, karet a dalších zařízení) a kontrolu všech těchto zařízení, která mají nějakou finanční hodnotu. Pravidelně kontrolovat / potvrzovat jednání a oprávněnost těch, kteří spravují

uživatelské účty, zajistit, aby tyto odpovědnosti nebyly přiděleny jedné osobě. Zaznamenávat důležitá porušení bezpečnostní (např. systému a přístupu k síti, virů, zneužití a nelegálního software).

Zajistit, aby byly neprodleně hlášeny a včas se vyřešili k zajištění důvěryhodnosti smluvních stran a k jistotě, že při použití elektronických transakčních systémů jsou obchodní ujednání platná nastavit bezpečnostní pokyny tak, aby byly přiměřené a v souladu se smluvními závazky. Prosazovat používání antivirové ochrany v rámci celé podnikové infrastruktury a zajistit pravidelnou aktualizaci používaného software na všech stanicích. Používat pouze legální software. Definovat politiku, která určuje, jaké informace mohou opustit systém organizace a které naopak mohou do systému vstoupit, v souvislosti s tím konfigurovat systémy síťové bezpečnosti (firewally), monitorovat výjimky a sledovat závažné incidenty. Zvážit, jak chránit mobilní výpočetní prostředky a zařízení. [2]



Obr.1 Bezpečnostní politika organizace

4. Role bezpečnostního managera

4.1 Zvládání bezpečnostních incidentů

Součástí života manažera bezpečnosti IS/ICT jsou bezpečnostní incidenty a jejich řešení. Zavedením libovolné bezpečnostní politiky není garantována absolutní bezpečnost IS. Pro zajištění bezpečnosti je implementováno mnoho různých bezpečnostních funkcí a opatření, přesto v IS vždy zůstávají zranitelná místa a ta představují někdy významná rizika. Právě existence slabých míst představuje hrozbu vzniku bezpečnostního incidentu a s negativními vlivy na chod organizace. [3]

4.2 Fáze oblasti bezpečnostních incidentů v organizaci

Nasazení a provoz systému zvládání bezpečnostních incidentů se stává zpravidla z fází detekce události, identifikace a rozhodnutí, jak situaci řešit a řešení incidentu.

4.3 Bezpečnostní incidenty

Popsané bezpečnostní incidenty je povinen kterýkoliv pracovník neprodleně hlásit CISO. Takovéto incidenty jsou zaznamenány v záznamu Kniha neshod a bezpečnostních incidentů, a to včetně řešení (odpovídá CISO) a pokud CISO rozhodne, je vystaveno nápravné opatření. Bezpečnostní incident lze zaznamenávat z pohledu uživatele anebo administrátora. Za bezpečnostní incident z pohledu uživatele lze považovat za pohyb návštěvy bez doprovodu, vstup dvou osob do prostorů společnosti bez identifikace v přístupovém systému, neohlášení návštěvy na recepci, nestandartní chování PC stanice. Mezi další incidenty spadá i manipulace jinými osobami s přidělenými stanicemi nebo nezdařené tři pokusy logování do stanice či serveru.

Další incidenty spadají mezi nepřítomnost uložených dat v domovském adresáři. Z pohledu antivirového programu lze naleznou virus při automatické analýzy systému. Z hlediska správce nebo v praxi využíván taky pojem administrátor je bezpečnostní incident považován za nestandartní zápisy v inventory logu, Security logu a config logu příslušného serveru nebo v zápise systémových logu konkrétní pracovní stanice. Administrátor detekuje incident při pozitivní intruze Firewallu či serveru nebo nahlášení viru při manuální analýze stanic či serveru. [4]

5. Preventivní opatření

Smyslem preventivních opatření (PO) je předcházet neshodám / incidentům. Při vypracování návrhu preventivního opatření je doporučeno postupovat dle určitých kritériích, které jsou v organizaci zavedeny. Provádět analýzu údajů jako zdroj pro stanovení preventivních opatření, lze na základě informací od zákazníků, podmětů pracovníků zainteresovaných stran, analýzy z testovacích protokolů, analýzy rizik, analýzy incidentů a penetračních testů, analýzy výsledky auditů, analýzy změn relevantních právních předpisů, analýzy změn relevantních právních předpisů. Preventivní opatření spořívá i na základě analýzy výsledku SW nebo HW auditu, které vyhodnotí zranitelnosti v systému. Informovat ostatní odpovědné pracovníky organizace o výsledcích přijatého PO Preventivní opatření se zaznamenávají do stejného protokolu jako nápravná opatření. Za evidenci odpovídá Chief Information Security Officer CISO. [5]

Závěr

Zmíněné důsledné dodržování pravidel pro hesla a omezení uživatelských práv na potřebné minimum automaticky také implikuje centralizování správy klientských stanic do rukou administrátora iT, což je další z požadavků navržené bezpečnostní politiky, takže tato dvě opatření jdou spolu ruku v ruce. Jakmile může administrátor iT efektivně řídit obsah instalovaného softwaru na jednotlivých počítačích, může také mnohem účinněji dohlížet nad jeho integritou. i toto opatření vede k usnadnění či dokonce zásadnímu umožnění naplňování jeho zodpovědnosti za funkčnost a bezpečnost celé iT infrastruktury.

Literatura

1. POŽÁR, J. Informační bezpečnost. Vydavatelství a nakladatelství Aleš Čeněk. Plzeň 2005. ISBN 80-86898-38-5
2. ČSN ISO/IEC 27002:2005. Informační technologie – Bezpečnostní techniky – Soubor

postupů pro řízení bezpečnosti informací. ČNI 2008
3. ISO/IEC TR 18044 – Information technology – Security techniques – Information security incident management
4. HÖNIGOVÁ, A., MATYÁŠ, V., ml. Anglicko-česká terminologie bezpečnosti informačních technologií, Computer Press, 1996. ISBN 80-85896-44-3
5. ISO/IEC 13335-1:2004 Informační technologie – Bezpečnostní techniky – Management informací a bezpečnost technologie komunikací – Část 1: Pojetí a modely informací a management bezpečnosti technologie komunikaci