Audit bezpečnosti informačních systémů: Klíčový krok k eliminaci zranitelností

itbiz.cz/clanky/audit-bezpecnosti-informacnich-systemu-klicovy-krok-k-eliminaci-zranitelnosti

8. dubna 2016

V původním významu pojmu audit se dostáváme k latinskému auditus – trpný rod minulý slova audio (slyšet) – volně interpretováno „slyšení, naslouchání“. Pojem audit se mnohdy zužuje na audit finanční, neboli nezávislé ověření správnosti účetních dokladů. V současné době je však definována celá řada specifických auditních činností podle oblasti na kterou je audit zaměřen. Obecně je předmětem auditu ověření a popis stávajícího stavu, jeho porovnání s požadovanou úrovní dle zákonných a normativních požadavků a tzv. nejlepší praxí v dané oblasti, s cílem poskytnout vedení organizace podklady k rozhodování o zlepšení nebo nápravě dané situace.

Audit informačních systémů

Významnou a v současné době velmi sledovanou oblastí je audit informačních systémů. Informační systém (IS) můžeme pro naše potřeby definovat jako celek složený z počítačových technologií a

souvisejícího programového vybavení, včetně lidí, kteří je využívají a procesů (činností), které přitom vykonávají za účelem sběru, zpracování a šíření informací potřebných k plánování, rozhodování a řízení určité organizace. Audit informačních systémů má řadu dílčích částí, z nichž se v tomto článku zaměříme na audit bezpečnosti informačních systémů.

Metodiky a postupy auditu IS

Pro vypracování auditu bezpečnosti IS existuje celá skupina metodik a postupů a na jejich základě bylo vyvinuto i mnoho automatizovaných nástrojů, Mezi známé a rozšířené metodiky a nástroje patří například ASSET (Automated Security Self-Evaluation Tool), COBIT (Control Objectives for Information and related Technology) a metodika ITIL (IT Infrastructure Library).

COBIT je komplexní otevřený standard, určený pro hodnocení IS jako celku a bezpečnost IS je jeho podmnožinou.

ASSET je zase nástroj publikovaný a distribuovaný americkou vládní organizací NIST (National Institute of Standards and Technology), který automatizuje proces sebehodnocení (self-assesment) úrovně zabezpečení IS, založený na dotaznících, které vycházejí ze souvisejících normativů, vymezujících požadavky na zabezpečení IS. Kromě zmíněných norem vydávaných NIST existuje soustava norem a zákonů s evropskou i národní působností a závazností, například ucelená a stále vyvíjená soustava norem ISO/IEC 27000, které je třeba při auditu bezpečnosti IS zohlednit a respektovat.

Úskalí sebehodnocení

Při využití nástrojů self-assesmentu je třeba počítat s určitým rizikem subjektivního nadhodnocení posuzovaného stavu, snahy „vidět se v lepším světle“. Pro objektivní a reálné posouzení stavu zabezpečení IS je proto většinou vhodnější využít nezávislého auditu a nástroje self-assesmentu používat pro následná periodická hodnocení.

Vždy je ale podmínkou úspěchu ochota managementu dané společnosti uvědomovat si hodnotu informací a důležitost zabezpečení IS. Každý bezpečnostní incident je nepříjemný a někdy může ve svých důsledcích vést k významným ztrátám jak finančním, tak i prestiže a pověsti, což může být ještě bolestnější.

Základní atributy bezpečnosti informací

Cílem zabezpečení informačního systému je zajištění bezpečnosti informací, někdy označovaných jako informační aktiva určité organizace, vytvářených, zpracovávaných nebo ukládaných v daném IS.

Základními atributy bezpečnosti informací jsou:

- **integrita dat** – informace jsou chráněny před neautorizovanou úpravou, změnou nebo zničením,
- **důvěrnost dat** – informace jsou chráněny před neautorizovaným přístupem a jejich vyzrazením jak při jejich zpracování, tak i při jejich přenosu,
- **dostupnost dat** – je zajištěna disponibilita dat v okamžiku, kdy je oprávněným uživatelem vyžadována.

Dalšími atributy bezpečnosti informací jsou:

• **autentizace** (ověření jednoznačnosti, pravosti identity subjektu nebo zprávy), autorizace (omezení oprávněnosti přístupu k informacím jen na určené uživatele),

• **nepopiratelnost** (vyloučení možnosti popřít provedení určité operace v informačním systému).

Provedení auditu IS

Vypracování auditu bezpečnosti IS má několik fází. Bez dobré přípravy a naplánování totiž výsledky auditu nebudou dostatečně pokrývat požadované cíle. Další nezbytnou podmínkou je podpora

vedení auditované společnosti a spolupráce zaměstnanců s auditorem.

Prvním úkolem při provádění auditu je stanovení jeho jasného a srozumitelného cíle.
Dalším krokem je stanovení rozsahu auditu – například je požadováno jen orientační posouzení existence bezpečnostních opatření, nebo naopak hloubková kontrola systému bezpečnosti IS včetně provedení potřebných testů. Rozsah auditních prací bývá stanoven na základě potřeb organizace a může zahrnovat buď komplexní audit týkající se všech oblastí bezpečnosti IS, nebo může být zaměřen jen na určitou specifickou část bezpečnostní problematiky.

V průběhu provádění auditu jsou pomocí zvolených metod šetření (interview, získávání a studium relevantní dokumentace, dotazníkové šetření, pozorování, testy, atd.) shromažďovány informace, které jsou třeba k vyhodnocení zadaného předmětu auditu.
Pak následuje etapa zpracování zjištěných informací, jejich detailní analýza, porovnání s požadovaným resp. pro danou organizaci optimalizovaným stavem a případným zpracováním návrhu nápravných opatření, které povedou k dosažení potřebné nebo požadované úrovně zabezpečení IS.

Srozumitelné podání výsledků auditu

Výstupy auditu ve formě auditní zprávy je třeba zpracovat takovou formou, aby byla srozumitelná pro určeného příjemce. V řadě případů je auditní zpráva vyhotovena v několika verzích – stručná souhrnná zpráva pro vrcholový management organizace a podrobná, technicky specializovaná zpráva pro odpovědné pracovníky útvaru IT. Důležitým krokem je projednání návrhu závěrů auditu s příslušnými pracovníky organizace a zapracování akceptovaných připomínek do konečných výsledků auditu. Odsouhlasené výsledky

auditu by měly být promítnuty do závazného plánu činnosti příslušných útvarů společnosti formou odpovídající zvyklostem dané organizace.

Obvyklá struktura výstupů auditu bezpečnosti IS zahrnuje:

• popis zjištěného stavu,

• základní bezpečnostní posouzení systému,

• popis zjištěných nedostatků v oblasti dokumentace,

• popis zjištěných zranitelností a bezpečnostních nedostatků IS,

• identifikace kritických míst,

• návrh protiopatření, včetně doporučení postupu realizace.

Zaměření auditu IS

Audit bezpečnosti IS se zaměřuje na následující oblasti, které jsou systematicky specifikovány a popsány v souboru norem ISO/IEC 27000, vycházející resp. navazující na britský standard BS 7799:

bezpečnostní politika,

organizace bezpečnosti,

klasifikace a řízení aktiv,

bezpečnost lidských zdrojů,

fyzická bezpečnost a bezpečnost prostředí,

řízení komunikací a řízení provozu,

řízení přístupu,

vývoj, údržba a rozvoj informačního systému,

zvládání bezpečnostních incidentů,

řízení kontinuity činností organizace,

soulad s požadavky.

Bezpečnostní politiky organizace

Audit informační bezpečnosti obsahuje fázi posouzení dokumentace týkající se zajištění opatření potřebných k bezpečnému provozu a využívání IS organizace. Tato dokumentace by měla pokrývat všechny procesy, které zpracovávají nebo využívají informační aktiva dané společnosti. Dokumentovaná bezpečnostní opatření jsou většinou v organizaci označována jako bezpečnostní politiky, které je možno dle užívaných metodik členit například na:

celkovou bezpečnostní politiku,

politiku zacházení s informačními aktivy,

politiku kontroly přístupu,

politiku nastavení a kontroly hesel,

politiku elektronické pošty,

politiku využívání internetu,

antivirovou politiku,

politiku klasifikace informací,

politiku klasifikace dokumentů,

politiku vzdáleného přístupu,

politiku vztahu k dodavatelům IT služeb a komponent atd.

Upozornění a opatření vyplývající za auditu

Audit by měl v této fázi identifikovat zranitelnosti IS a hrozby, které vyplývají z nedostatečného nastavení bezpečnostních opatření. Následující fáze auditu by měla porovnat dostatečnost implementace

nastavených bezpečnostních politik, případně posoudit, kde jsou rizika, která stávající bezpečnostní dokumentace nebo nastavení IS organizace nepokrývá.

Pokud zranitelnost IS umožní dané hrozbě, aby se uskutečnila, vzniká bezpečnostní incident. Je úkolem auditu upozornit na zjištěné zranitelnosti, aby bylo možno pomocí následných bezpečnostních opatření tyto hrozby a zranitelnosti eliminovat nebo zmírnit na míru akceptovatelnou pro danou organizaci.

Tato opatření jsou klasifikována jako:

Preventivní – slouží k prevenci výskytu bezpečnostních incidentů. Příkladem je systém přidělování a řízení přístupových práv skupině oprávněných osob, systém autorizace, identifikace a autentizace.

Redukční – opatření, která mohou být přijata v předstihu tak, aby se minimalizovaly případné škody, které mohou nastat. Příkladem je systém zálohování nebo systém řízení kontinuity organizace.

Detekční – pokud dojde k bezpečnostnímu incidentu, je důležité odhalit tuto skutečnost co nejdříve – detekovat. Příkladem je systém monitoringu bezpečnostních incidentů nebo antivirový program.

Represivní – opatření proti pokračování nebo opakování bezpečnostního incidentu. Příkladem je dočasná blokace účtu či síťové adresy po neúspěšných pokusech o přihlášení, nebo zadržení karty po pokusech o přihlášení nesprávným PIN kódem.

Nápravná – opatření sloužící k rychlé nápravě vzniklé škody. Příkladem je obnovení dat ze zálohy nebo návrat systému do poslední stabilní verze.

Uvedená auditní fáze může být uskutečněna různým stupněm detailního posouzení dané situace, od formálnějšího porovnání dokumentace a skutečného stavu zjištěného pomocí interview a

jednoduchých testů, až po podrobné a technicky náročné testování včetně penetračních testů ověřujících odolnost IS proti napadení zevnitř i zvenčí systému.

Lidský faktor

Důležitým efektem pravidelně prováděných auditů bezpečnosti informačního systému je nejenom zjištění a případná náprava nedostatečných bezpečnostních opatření, ale také zvýšení bezpečnostního povědomí zaměstnanců i vedení organizace. Ze statistik výskytu bezpečnostních incidentů vyplývá, že významný podíl na jejich vzniku má vliv nerespektování nebo neznalost bezpečnostních principů při práci s informačními zdroji ze strany zaměstnanců dané organizace.

Významnou částí auditu bezpečnosti IS je tedy ověření stavu bezpečnostního povědomí odpovědných zaměstnanců a systému řízení lidských zdrojů, s ohledem na zajištění bezpečnosti IS. To se týká celého tohoto procesu počínaje, přijímáním a výběrem zaměstnanců na citlivé pozice, přes systém jejich školení a ověřování znalostí až po proces případného ukončení pracovního poměru, včetně odebrání přidělených přístupů, oprávnění a technologického vybavení.

Auditoři vs. vedení organizace

Výsledek a následný efekt auditního šetření je do značné míry závislý jak na zkušenostech a znalostech auditorů a jejich komunikačních dovednostech, tak i na ochotě a vůli vedení i odpovědných zaměstnanců po nastavení a zlepšení zabezpečení informačního systému auditované organizace na požadovanou úroveň.

Pavel Alexander je dlouholetým bezpečnostním auditorem, který tuto činnost prováděl zejména ve velkých organizacích.

Rubriky: Podnikový softwareSecurity