Organizace bezpečnosti, personální politika

Dodržování standardů vývoje programů

aby byly efektivní, musí být standardy důsledně dodržovány za všech okolností
typickými situacemi, kdy vznikají tendence je porušovat jsou okamžiky, kdy projekt nabírá zpoždění proti plánu, po odchodu klíčových pracovníků apod.
dodržování standardů by měli podporovat pravidelné audity bezpečnosti (security audits) prováděné nezávislým bezpečnostním týmem

Rozdělení úkolů

je vhodné práci rozdělit mezi více lidí, kteří se znají co možná nejméně
omezuje se tak nebezpečí vzniku bezpečnost ohrožujících programů, navíc pokud programátor očekává, že jeho kód bude podroben zkoumání nezávislého testovacího týmu, omezí své nekalé aktivity

Charakter přijímaných pracovníků

firmy běžně sestavují profily svých potenciálních pracovníků a přijímané podrobují všestrannému zkoumání, zda nebudou představovat hrozbu pro bezpečnost - obvyklé jsou reference z dřívějších působišť, psychologické testy apod.
po přijetí má pracovník povětšinou velmi omezený přístup k senzitivním informacím, až časem získává důvěru a tím i rozsáhlejší bezpečnostní oprávnění

Sledování pracovníků

je vhodné vést co nejpodrobnější informace o pracovnících, zejména o:
◊ vybraných zálibách (hraní, drogy, sex, jiné finančně náročné koníčky)
◊ neobvyklých změnách chování pracovníka
◊ nenadálých změnách majetkových poměrů

Havarijní plán

určuje, co dělat po odhalení útoku (bezpečnostního incidentu) a jak postupovat, aby se udržela kontinuita činnosti organizace.
určuje

- místa skladování a počty náhradních dílů,
- místa skladování a způsob organizace záloh dat,
- obsah pohotovostního skladu technických a softwarových náhrad,
- metodiku udržování aktuálnosti skladů dat, softwaru, hardwaru a
- metodiku aktualizace a testování hardwaru.

Součástí havarijního plánu jsou

- návody, jak postupovat v poskytování služeb po zjištění útoku – *plán činnosti po útoku*,
- dohody o poskytování náhradních řešení informaticky orientovaných úkolů organizace,
- dohody o uvedení dat IS do původního stavu po havárii (incidentu).
- návod, jak postupovat při obnově činnosti IS po havárii – *plán obnovy*.

Plán činnosti po útoku

soubore scénářů pro situace vzájemně se lišící délkou přerušení činnosti, ztrátou různých typů vybavení, omezením přístupu do areálu organizace, potřebou návratu do původního stavu před útokem apod.

obvykle předepisuje provedení analýzy incidentu, , co se stalo a kdy, zda se řešila reakce podle plánu.

Po vyřešení incidentu je potřeba přijmout závěr, zda byl plán činnosti po útoku řešitelům dostupný,
zda byl efektivní, co příště dělat jinak a zda je potřeba plán modifikovat.

Průběh reakce na incident

1. okamžitě reagují odpovídající *týmy 1. reakce*.
Cílem
- ambulantní zásah,
- zajištění činnosti ve stavu nouze.

k dispozici
- návody pro činnosti po detekci útoku,
- seznamy adres, telefonů, e-mail adres

musí informovat pracovníka odpovědného za vyřešení incidentu

2. Týmy pro řešení incidentu mají
- směrnice definující postupy řešení,
- definice lokalit archivů,
- definice zdrojů náhradních dílů

provádějí posouzení důsledků útoku.

3. *týmy pro obnovu*,
uvádějí IS do standardního stavu

Plán obnovy

musí obsahovat kritéria definující,
- co se chápe havárií,
- odpovědnosti za aktivaci obnovy,
- odpovědnosti za aktivaci dílčích činností podle plánu obnovy a
- návody k provádění činností podle plánu obnovy.

V plánu obnovy je potřeba prosadit obvykle následující zásady:

Je potřeba provést segmentaci informačních zdrojů podle priority obnovy (např.: nejkritičtější zdroje do 30 minut, ostatní kritické zdroje do 2 hodin a zbývající během24 hodin).
Zbývající zdroje lze dále kategorizovat na prioritní zdroje obnovované do 6 hodin, žádoucí obnovované do 12 hodin a zdroje vhodné pro obnovu do 24 hodin.

Důležité je, aby byla zavedena shodná pořadí obnovy ve všech odděleních organizace.

Odpovědného pracovníka za vymezení kritičnosti a priorit stanovuje celková bezpečnostní politika. Stejná pořadí obnovy v plánu obnovy stanovují systémové bezpečnostní politiky.

 Vyhodnocování kritičnosti a priorit multiuživatelských aplikací se provádí alespoň jednou ročně
 Vypracovávají se seznamy kritických aplikací tříděné podle priorit obnovy.
 Existuje plán činnosti organizace ve stavu nouze
 Organizace musí mít vypracován plán udržení činnosti kritických aplikací při přerušení nebo při degradaci služeb.
 Tým 1. reakce je potřeba udržovat v pohotovosti
 Udržuje se přehled o stavu týmu, trénuje se schopnost týmu bezprostředně zahájit svoji činnost – jeho schopnost reagovat na odhalení viru, na odhalení činnosti hackera atd.
 Přirozeným cílem je výchova týmu k minimalizaci publicity útoku.
 Existují definice činností po podezření na průnik do systému
 Obsahují typicky nepominutelné (minimální) úkoly pro správce systému, které jsou často protichůdné vůči požadavkům a tlaku správy uživatelů, postupy při odstavení kompromitovaného počítače od ostatní sítě, postupy pro uschování záznamů o kritických činnostech uživatelů z hlediska bezpečnosti, návody jak dělat identifikace provedených změn, návody pro obnovu softwaru z důvěryhodného zdroje, návody pro re-inicializaci systému řízení přístupu (změna hesel …) atd.
 Je zaveden systém varování o podezření na průnik útočníka či jiné porušení bezpečnosti
 Tento systém musí být nejen zaveden, ale i udržován a testován. Jeho součástí jsou seznamy potřebných čísel telefonů či faxů, e-mailových adres, faxů a osobních kontaktů nutných pro mobilizaci členů týmů 1. reakce, včetně jejich pobytů mimo pracoviště.
 Cílem takového systému je minimalizace šance úspěchu širokého průniku.
 Je zaveden systém sběru informací o podezření na porušení bezpečnosti
 Takový systém podporuje stav bdělosti u zaměstnanců, partnerů a konzultantů. Týká se takových skutečností, jakými jsou oznámení o poruše disku, oznámení o ztrátě souboru nebo oznámení o krádeži.
 Jsou stanoveny povinnosti zaměstnanců při účasti na procesu obnovy po porušení bezpečnosti
 Povinnosti se mohou stanovovat u zaměstnanců, nikoli u partnerů nebo konzultantů. Povinnosti se nemohou křížit se společenskými zájmy vyšší důležitosti, jakými je např. činnost v rámci Červeného kříže při záplavách apod.
 Vyhodnocování pokrytí funkcí předepsaných v celkové bezpečnostní politice se provádí typicky s roční periodou
 Vyhodnocování provádí vrcholový management a jeho součástí je udržování zástupnosti expertů v týmu obnovy pro kritické aplikace.
 Minimalizace automatizace znamená minimalizace ceny
 Co lze udělat manuálně, je vhodné manuálně dělat.
 Je zavedena periodicita archivace dat
 Plán obnovy řeší rotaci použití archivního média (dědeček–otec–syn). Periodicita je pochopitelně aplikačně závislá, může být denní, týdenní nebo třeba i měsíční.
 V současné době nabývá na významu archivace kritických dat na mobilních počítačích
 Přirozenou nutnosti je provádět potřebné archivace před cestou.
 Musí být zaveden systém řízení přístupu k archivním kopiím
 Koncový uživatel nemůže archivační systém využít k obejití autorizace přístupů. To vede k šifrovaným uložením archivních souborů a vyžaduje to periodické prohlížení záznamů o činnostech uživatelů bezpečnostním správcem.
 Je třeba zachovat důvěrnost off–line uschovávaných archivních kopií
 Typickým opatřením je šifrované uložení takových dat i mimo prostory organizace a je tudíž potřebné mít zabezpečenou dostupnost klíčů při jejich obnově. Samozřejmé je ošetření povinnosti zachovávat důvěrnost dat archivačním týmem.
 Násobnost archivních kopií (alespoň duplicita)

 Dříve než se použije archivní kopie pro obnovu, je potřeba mít alespoň jednu její kopii uloženou v archivu. Kritická data se obvykle trvale uchovávají mimo organizaci alespoň ve dvou kopiích.

37

 Nepominutelná je existence inventurní evidence archivních kopií
 Musí se zavést systematizace značení kopií a zajistit on–line udržování přehledů.
 V síťových prostředích je vhodná automatizace archivace na serveru LAN
 Musí se řešit trvalá dostupnost, tj. zapojení připojených koncových počítačů pro automaticky prováděnou archivaci např. „v nočním provozu“, aby bylo možné provádět archivaci automaticky bez zásahu koncového uživatele. Musí se ovšem vyřešit problém přístupových práv ze serveru ke stanicím chráněným heslem.
 Likvidace dále nepotřebných informací je zárukou zachování důvěrnosti
 Existují mnohé legislativní závazky pro stanovení periody uchovávání kopií dat. Za jejich znalost běžně odpovídá právní oddělení organizace.
 Pro úspěšnou obnovu je důležitá volba archivního média
 Určení archivního média obvykle předpisuje systémová bezpečnostní politika, stejně tak předepisuje i periodicitu testování použitelnosti archivního média.
 Plán obnovy musí splňovat požadavky dané kvantitativním cílem dostupnosti zdrojů
 Uživatelé musí mít např. sdílené počítače dostupné po dobu rovnou alespoň 95% pracovní doby ve výrobní organizace, po dobu rovnou alespoň 99,98 % pracovní doby v telefonní společnosti apod. Tyto limity normálně stanovuje vrcholový management v celkové bezpečnostní politice.
 Zálohování kritických zdrojů lze řešit několika způsoby
 Horká záloha představuje dostupnost plně provozuschopného centra obnovy po katastrofě, které je plně vybaveno technickými i logickými prostředky (hardware, software, komunikace) i technickým personálem. Předpokládá se restart provozu řádově do několika hodin a schopnost poskytovat služby i po dobu několika měsíců.
 Mobilní horká záloha může být řešena např. instalací IT v dobře vybaveném „karavanu“.
 Teplá záloha znamená, že lokální koncová pracoviště (displeje, tiskárny) jsou rekonfigurovatelná tak, aby umožnila přístup do vzdáleného centra obnovy po katastrofě.
 Studená záloha požaduje, aby si organizace po katastrofě mohla připravit jiné pracoviště vlastním vybavením, doba reakce je obvykle několik dní.
 Organizace může provozovat duální (záložní) datové centrum umístěné v geograficky vzdálené budově.
 Pro stanovení ekonomické optimálnosti plánu obnovy je potřeba vzít do úvahy, čím je dána cena kopie
 Na cenu kopie má vliv výše možných ztrát (roční ztráty nebo roční náklady) a náklady na pořízení, náklady na skladování kopií. Velký problém je řešení zálohování on-line systémů provozovaných 24 hod., kdy se musí využívat techniky typu kontrolní body, žurnál transakcí, tandemové nebo zrcadlové zpracování.
 Systémová bezpečností politika předepisuje správu záloh dat
 Kde se udržují, což je ovlivněno energetickou závislostí, fyzickou bezpečností, složitostí řízení provozu. V jaké násobnosti se udržují a jak se distribuují.
 Zálohy dokumentace, manuálů
 Opět systémová bezpečnostní politika určuje, kde jsou uloženy a počet jejich kopií. Doporučuje se udržovat „zlatou kopii“, která slouží pouze k reprodukci provozních kopií a normálně se nepoužívá.

38

 Zajištění dostupnosti hardwaru
 Požaduje existenci případně smluvního systému oprav a údržby hardwaru, provozování náhradních zdrojů apod.

Interní (bezpečnostní) audit

Důležitou zásadou je oddělení povinností výkonných a kontrolních.
Audit musí být nezávislý na prosazování provozní bezpečnosti a hlavně musí se skutečně provádět.

Auditní postup:
 fáze detekce – je zjištěna událost, která má vztah k bezpečnosti
 fáze rozlišovací – určuje, zda je nutné zaznamenat událost nebo spustit bezpečnostní poplach
 fáze zpracování bezpečnostního poplachu – je spuštěn bezpečnostní poplach nebo je vydána bezpečnostní auditní zpráva
 fáze analýzy – událost, vztahující se k bezpečnosti je posouzena v kontextu dříve zjištěných zpráv, zaznamenaných v bezpečnostním záznamu a je určen průběh činnosti
 fáze agregační – distribuované záznamy dílčích bezpečnostních auditních záznamů jsou spojeny do jednoho bezpečnostního auditního záznamu
 fáze generování zprávy – z bezpečnostních auditních záznamů jsou vytvořeny auditní zprávy
 fáze archivace – dílčí části bezpečnostního auditního záznamu jsou uloženy do archivu bezpečnostních auditních záznamů.