Bezpečnost aktiv

aktivem rozumíme jakýkoliv zdroj hodnoty – hmotný i nehmotný
relevantní normy:

- Security of Information Act (Kanada)
- GDPR (EU)
- Official secrets Act (GB)
- FIPS 199 (USA)
- Zákon o utajovaných skutečnostech
- Zákon významných IS
- … a nekonečně dalších

Identifikace a klasifikace informací a aktiv

nezbytná pro stanovení důležitosti aktiv a priorit
cílem je inventarizace

- jaká aktiva máme
- kde jsou
- kdo za ně odpovídá

Klasifikace dat

kategorizace dat dle

- senzitivity
- kritičnosti (nepostradatelnosti)
- hodnoty

potřebujeme proto, abychom pro jednotlivé kategorie mohli navrhnout odpovídající bezpečnostní mechanismy

- založená na kontextu – odvozujeme od kontextu / metadat (vlastník, umístění, zdroj, …)
- založená na obsahu – na základě posouzení obsahu identifikujeme / deklarujeme míru senzitivity
- založená na uživateli – tj. ad-hoc přiřazení míry senzitivity

Správné je mít formální politiku hodnocení dat

Kategorizace dat

seskupování typů dat na základě obdobných nároků na zabezpečení
cílem opět minimalizace typů používaných opatření

Klasifikace obecných aktiv

identifikace jednotlivých položek,
hodnocení senzitivity, kritičnosti, hodnoty i v závislosti na zpracovávaných datech
seskupování aktiv dle jejich relativní míry senzitivity
podobně jako v případě dat cílem „inventurní seznam“ aktiv
pro každou třídu se stanoví *minimální sada bezpečnostních opatření*
často se používají hierarchické systémy (tier X, essential …)

Požadavky na nakládání s aktivy a informacemi

třeba vytvořit politiku a procedury pro práci s aktivy

Označování

viditelné etikety na zařízení značící důležitost, bezpečnostní úroveň, senzitivitu
v případě dat vhodné označení v záhlaví, zápatí dokumentu, v názvu souboru, vlastnostech, …
Implicitně byste měli o nových objektů nastavit nejvyšší úroveň a následně dle potřeby reklasifikovat

Zpracování

politika a pravidla a postupy pro přístup, přenos, transport a používání senzitivních dat a kritických aktiv
základem školení a povědomí

Uložení

lokace a zabezpečení uložených dat
třeba promyslet i incidenty typu odcizení nosiče, neoprávněný přístup k úložišti, date ve všech stavech (včetně záloh, …), mobilní platformy
šifrování, použití HW prostředků
důležitá limitace objemu uchovávaných dat

Deklasifikace

proces modifikace přiřazené klasifikace – musí být zdokumentováno, vhodné vícenásobné schválení, účast vlastníka
deklasifikace může zahrnovat vyjmutí, nebo zamlžení senzitivních elementů

- deidentifikace – odstranění údajů identifikujících osoby
- tokenizace – substituce senzitivního elementu bezvýznamovým řetězcem (může být provedena tak, že daný element je vždy nahrazován stejným řetězcem - pseudonymizace)

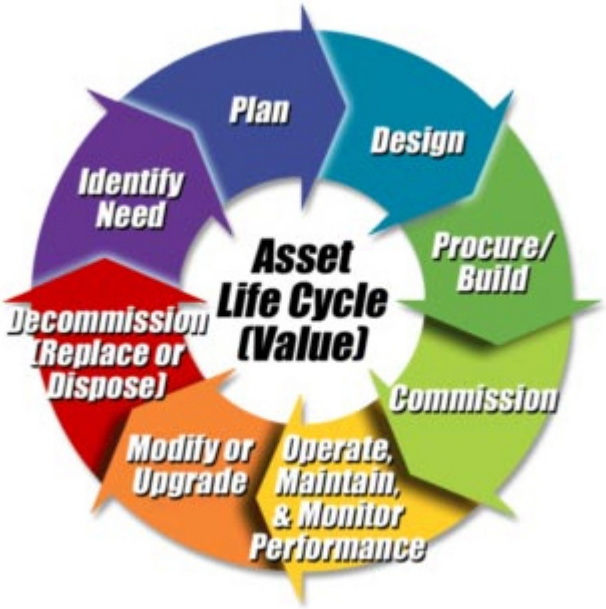
Bezpečné poskytování zdrojů

aktiva chráněná dle zákona, smluvního vztahu či požadavků na shodu musí být vždy řízena
stanoven vlastník, určena odpovědnost za aktivum, jasná definice rolí všech, kdo s aktivem nakládají
statutární orgán deleguje odpovědnost
Požadavky:

- aktuální inventarizace
- správná klasifikace
- odpovídající bezpečnostní opatření
- monitoring a vyhodnocování
- řízení přístupu včetně procesu odnímání přístupu
- hodnocení prostředí

Správa aktiv

aktivum musí být sledováno, řízeno a chráněno ve všech částech životního cyklu

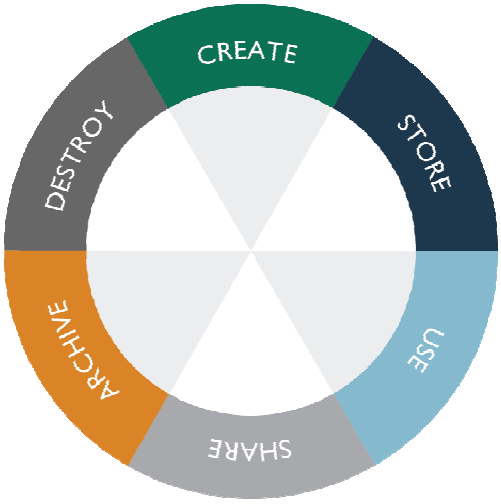


zdroj: readytomanage.com

Správa konfigurací – zajišťuje řízení a dokumentaci, definice základní úrovně (baseline) , minimální bezpečnostní nastavení apod.
Řízení změn – standardizuje proces vytváření, testování a aktivace změn

Správa životního cyklu dat

vzhledem k specifickým nárokům zpravidla řešeno samostatnými předpisy a postupy



zdroj: micsolutions.co.uk

Role spojené se správou dat

vlastník

odpovědný za stanovení, jak a kým budou data používána, rozhoduje o udělení a odebrání přístupu, plně odpovědný za data a zodpovídá za ně v plnéém rozsahu – a to i v případě, že deleguje provádění některých úkonů

definuje pravidla ochrany, použité mechanismy

měl by postupovat dle zásad náležité péče a náležité pečlivosti

regulátor

je osoba, agentura či společnost určující účel a způsoby zpracování dat

odpovědný za dodržování příslušných principů a shody

zajišťuje shodu s legislativou, spravedlnost, transparentnost, správnost dat, minimalizaci užití a držení dat, limity uložení atd.

správce

je odpovědný za údržbu dat na IT infrastruktuře a údržbu technických prostředků zpracování

zpracovatel

je odpovědný za přesun, přenos a jiné obdobné nakládání s daty jménem vlastníka, ale neodpovídá za data samotná

uživatel

konzumenti dat, uživatelé služeb

subjekt

ten, o kom data vypovídají

Umístění dat

přibývá legislativních a jiných požadavků na geografické omezení zpracování a uložení dat, případně i jejich přenosy
definované typy dat nesmějí opustit jurisdikci původu
kompenzačním opatřením může být odpovídající šifrování

Údržba dat

zahrnuje zpracování, analyzování a sdílení dat
řízení přístupu
aplikaci odpovídajících bezpečnostních opatření
Princip minimálních oprávnění (least priviledge)
Princip ochrany do hloubky (defense in depth)

Uchovávání dat

je třeba pro každý typ dat stanovit dobu uchování:
na jedno stranu se snažíme / musíme se snažit minimalizovat dobu držení dat
na druhou stranu určité záznamy je nutno uchovávat kvůli legislativním a jiných požadavků – účetní záznamy, platová a personální data apod.

Likvidace dat

nutno posoudit, zda před likvidací dat není třeba je nabídnout příslušné autoritě (např. zákon o archivnictví)
zjistit potřebnou úroveň likvidace dat a případně rovněž jejich nosičů
kontrola reziduí
procesy pro likvidaci a dokumentaci likvidace dat

Remanence dat

technicky smazaná data mohou být stále zjistitelná analýzou nosiče
v zásadě dva přístupy

- vyčištění od dat – smazání, přepsání (i vícenásobné předepsaným způsobem), nulování, degaussing
- likvidace nosiče - drcením, tavením, mletím, …

odstranění označení znovupoužívaných nosičů
smluvní ošetření v případě cloudových služeb, nelze provádět mazání, nutno ukládat pouze šifrovaná data
kryptografické mazání dat – ponechám data, smažu klíče

Zajištění dostatečné retence aktiv

pro zajištění paměti organizace

z regulatorních důvodů (personální data, auditní stopa, důkazy, …)
stanovení pravidel (často vázáno na archivační a skartační znaky dat) a politiky odpovědnosti, aktualizace, kontroly
určení vhodné doby retence je obecně složitý problém
právo být zapomenut (GDPR)
minimalizace retence zmenšuje expozici

Opatření pro zajištění bezpečnosti dat

- technická – brání zneužití a neautorizovanému přístupu (řízení přístupu, firewally, filtry, šifrování, …)
- administrativní – politiky použití, standardy, postupy (clear desk, need to know, …)
- fyzické – kontrola fyzické přístupnosti (stráže, recepční, systémy kontroly vstupu/výstupu, kamery, prostorová ochrana , …)

Stavy dat

v klidu

uložená data, nejsou aktivně čtena, zapisována ani jinak zpracovávána
řízení přístupu – autorizační mechanismus a separace, hardwarové moduly TPM (trusted platform module)
šifrování – samošifrující zařízení (SED, FDE, …), kryptografické tokeny, šifrování při uložení dat

data při přenosu

přenášená prostřednictvím sítě včetně VPN
šifrování na úrovní sítě (link encryption)
end-to-end šifrování na úrovní aplikace
nejde jen o šifrování za účelem zajištění utajení, ale i autenticity a integrity

data při použití

aktivně zpracovávaná data v RAM, CPU keších a registrech
autentizace, autorizace, provozní a auditní záznamy, *fyzická ochrana*

Určení rozsahu ochrany a přizpůsobení

nutné pro nastavené odpovídající politiky a úrovně ochrany

- rozsah – jaká data, jaké prostředky
- přizpůsobení – parametrizace

Kompenzační opatření

ne vždy je možné aplikovat požadovaná opatření (náročnost nasazení, neúměrné snížení komfortu či použitelnosti systému, …)

požadované opatření nahradíme něčím, co směřuje k původnímu cíli (např. nejsme schopni zavést SOD – zvýšíme logování)