Hodnocení a testování bezpečnosti

hodnocením rozumíme vyhodnocování vlastnosti objektu (např. pravděpodobnost …, předpokládaná velikost …)
audit je pak formálně prováděným hodnocením
výstupem hodnocení bývá report detailně popisující provedená zkoumání a nálezy

Návrh a validace hodnocení, strategie testování a auditu

explicitní stanovení rozsahu a zamýšlených cílů (účelu) zkoumání
vhodné je postupovat podle určité metodologie – opakování auditu dle stejné metodologie umožňuje srovnávat a hodnotit efektivitu investic

Interní audit

rozhodně ho musí provádět někdo jiný, než autor politiky
nebezpečí konfliktu zájmů a sdílení stejného (špatného) názoru
výhodou znalost prostředí, kultury, systémů, lze provádět častěji
vhodné zejména pro

- hledání slabin, rutinní kontroly patchů
- kontroly procesů, např. řízení změn, školení, certifikace
- simulace útoků

Externí audit

absence střetu zájmů
svěží pohled „odjinud“
někdy se jedná o naplnění regulatorního požadavku
zpravidla větší zkušenosti, ale menší znalost objektu auditu

Audit třetí stranou

typicky v rámci kontroly dodavatelského řetězce
provozován pracovníky odběratele, nebo nezávislým auditorem
objektem bývají provozní postupy, procesy správy a zabezpečení dat apod.

Testování bezpečnostních opatření

ověřování funkčnosti bezpečnostních opatření je nezbytností

Hodnocení slabin

slabiny se objevují častěji, než lze provádět audit či hodnocení rizik
nutno rutinně hledat slabiny přinejmenším kritických komponent
po nalezení nové slabinu provést hodnocení dopadu, relevantnost a stanovit prioritu nápravy

aktualizovaný inventář aktiv zahrnující hodnocení dopadu na obchodní operace a klasifikaci aktiva je nezbytnou prerekvizitou
dostatečnou častost lze zajistit pouze automatizovaným hledáním (zpravidla dodávají dodavatelé řešení, případně open-source komunity)
založeno na sledování komunikace, případně specifickém testování aplikace / systému
hodnocení slabin je definováno

- povinností – daných regulatorně, smluvně, nebo legislativně
- hloubkou, rozsahem a pokrytím – včetně schopnosti scaneru se autentizovat a testovat jako oprávněný uživatel
- podporou používaných platforem
- kompatibilitou s cloudovým prostředím

scanování může být zdrojem problémů:

- zvýšení (komunikační) zátěže
- falešných incidentů
- porušení segmentace sítí
- zanesení integrity dat (zejména logů, statistik) rezidui testů
- těžkosti pří různém vlastnictví testovaných komponent či procesů

Penetrační testování

založeno na kodexu etického hackera
snaha najít zejména známé slabiny s zmapovat rozsah a dopad možného incidentu
výstupem vždy report
různé přístupy k plánování testů

- white box
- gray box
- black box

důležité je stanovit správně rozsah testů vzhledem k (omezenému) času a nákladům na provedení
pentest zpravidla probíhá ve standardních fázích

- průzkum prostředí – získání znalosti o cílovém objektu
- skenování a zkoušení – hledání slabit a metod útoku
- využití nabytých poznatků – v dohodnutém rozsahu test využitelnosti slabin a rozsah získané kontroly
- rozšíření průniku - tzn. co dále lze získat / docílit
- reporting – co přesně bylo provedeno, odhaleno, získáno, doporučení pro nápravu

je třeba zajistit, aby

- penetrační testování nespustilo reakci na incident nebo dokonce proces zotavení po katastrofě
- minimalizovala se pravděpodobnost způsobení opravdového incidentu
- tým testováním nemohl být činěn odpovědným za prováděné (dohodnuté) akce

Kontroly logů

ověření, že všechny potřebné logy se generují, zpracovávají a uchovávají
kontrola, že zpracování opravdu objeví nesrovnalosti
ověření, že všechny předepsané mechanismy fungují

Syntetické transakce

tedy simulované aplikační transakce, kterými se ověřuje funkčnost cílových systémů
kontroluje se, že systém odpoví očekávanou odezvou
používají se pro

- SLA monitoring
- monitoring integrity dat
- monitoring systémů a služeb

zhusta více vypovídající, než technický monitoring systému

Kontroly kódu a testů

tzn ověřování kvality testování (citlivost, pokrytí, opakovatelnost)
identifikace slabin procesu
statické i dynamické metody testování

Testování zneužití

jak se systém chová při nechtěném či záměrném zadání nesmyslných vstupů
co se stane při nesprávném zacházení se zařízením

Analýza pokrytí testů

stanovení, kolik procent funkcionality testování pokrývá
ověřování požadavků na testování a validace testovacích plánů

- pokrytí větví / variant
- pokrytí podmínek
- funkční pokrytí
- pokrytí příkazů
- pokrytí rozhodování pokrytí parametrů

je třeba zvážit senzitivitu na vstupní data, dopad na bezpečnost pracovníků a cíle organizace

Testování rozhraní

sleduje se přístupnost, nepopiratelnost, existence slabin, zabezpečení
ověřuje se shoda s dokumentací, vhodnost akceptačních testů, session management autentizace, …

Simulace narušení a útoku

pomocí automatických nástrojů se zkoumají dopady obvyklých metod útoku
kombinace hledání slabin, automatického penetračního testování s využitím databáze známých metod útoku (rootkit)
předmětem zkoumání je, zda zareaguje příslušný bezpečnostní mechanismus – správně, včas, v dostatečném rozsahu

Kontroly shody

… s příslušnými relevantními požadavky
obvykle formou auditu – bodové hodnocení
nebo formou hodnocení výkonu bezpečnostních mechanismů za stanovené období

Shromažďování dat o bezpečnostních procesech

cílem je hodnocení stavu a provozu bezpečnostních opatření
založeno na průběžném monitoringu:
vychází z hodnocení rizik a návrhu programu bezpečnosti
na jeho základě se stanoví strategie tvorby a zpracování logů
provede se povolení a nastavení logování na všech systémech
zavede se centralizace zpracování
automatizace monitoringu
nasazení pokročilých metod automatického vyhodnocování (trendy, clustery, prahové hodnoty, neobvyklosti, …) včetně strojového učení a umělé inteligence

Technická opatření a procesy

nebývá problém, zpravidla obsahují prostředky pro tvorbu logů

Administrativní opatření

bývají implementována ve formě politik, pravidel či procedur
je třeba se orientovat na shromažďování a vyhodnocování artefaktů:

- záznamy o obchůzkách
- protokoly o incidentech
- vydaná osvědčení o absolvování školení
- výsledky testování
- vydané certifikáty

hodnotí se
- dopad politiky
- efektivita vzdělávání
- technologická efektivita – kolik případů provedení nepovolené operace

Správa účtů

účtem rozumíme sadu kredenciálů používaných pro přístup k zdroji
správa bývá implementována mixem administrativních a různých technických opatření
administrativní – formální žádostí o přidělení přístupu, proces schvalování, přidělení a odejmutí
technické – technická podpora administrativního procesu, vlastní prostředky IAM, řízení přístupu na úrovni komunikace, klíče pro volání API apod.
fyzické – vstupní / výstupní zařízení, kontrolované zóny, stráže, prostředky kontroly vstupu / pohybu / výstupu (karty, visačky, …)
řeší se
- správná doba reakce na požadavek
- včasnost obdržení upozornění
- vhodnost prováděných kontrol
- správné provozování procesů

Kontrola a schválení managementem

management je odpovědný za všechny aspekty provozu organizace a správu dat
hodnocení, audity a kontinuální monitoring musí, mimo jiné, produkovat data pro podporu řízení organizace a rozhodování,
vstupy do procesu řízení rizik
rozhodování o správném způsobu jejich kontroly
schvalování procesů bezpečnosti a hodnocení jejich efektivity
tedy management musí schválit plánovaný monitoring a očekávané výstupy

Kontrola shody

celá řada předpisů definuje rozsah kontroly managementem
- ISO 27001
- RedRAMP od NIST
- různé systémy certifikace a akreditace – obecná úroveň SOC2 vyžaduje, aby management stanovil měřítka výkonu opatření
- COBIT

a toto je třeba naplnit

Klíčové indikátory výkonu a rizika

je nutné nejen sledovat výkon a efektivitu stávajících opatření, ale i zamýšlet se nad budoucím vývojem hrozeb a očekávanými změnami rizik
KPI- hodnocení stávajících opatření na základě vhodných metrik
KRI – povědomí o nadcházejících hrozbách a vývoji rizik
nutné rozhodnout, jaké indikátory využívat na základě jejich přesnosti a vypovídací hodnoty

Klíčové indikátory výkonu (KPI)

v návaznosti na vývoj KPI se rozhoduje o úpravě stávajících opatření, či jejich náhradě novými, proto musí být předem definovány výchozí hodnoty a stanoveny horní a dolní hranice akceptovatelného rozsahu
běžné metriky:
střední čas na detekci (MTTD)
střední čas na řešení (MTTR)
bezpečnostní skóre – mnoho dodavatelů poskytuje systém hodnocení správnosti nastavení produktu či jeho bezpečnostních mechanismů, nutno přizpůsobit aktuálním podmínkám
návratnost investic – tj. hodnoceni redukce rizika a indukovaných nákladů vs. TCO bezpečnostních opatření

Klíčové indikátory rizika

popisují, jaký dopad na organizaci má měnící se povaha hrozeb
na jejich základě se provádí proaktivní úprava opatření a dlouhodobá manažerská rozhodnutí
zdrojem hodnocení je provoz obvyklých bezpečnostních opatření, ale hodnotí se jiná kriteria:

- počet výskytu malware
- počty oprav po zavedení SW
- neuspěšná přihlášení
- portscany
- množství a druhy incidentů
- počty nálezů auditu
- výskyt phishingu,
- …

Kontrola záloh

hodnotí se integrita vlastních zálohovaných informací
funkčnost procesu obnovy

vhodnost strategie zálohování pro skutečné potřeby obnovy

Školení a povědomí

vyhodnocuje se úspěšnost školení a vytváření povědomí
obvyklé metriky:

- počty vyškolených pracovníků
- dlouhodobá znalost potřebných informací a budování návyků
- shoda s potřebami posluchačů
- pokrytí celé problematiky bezpečnosti

Obnova po katastrofě a plány kontinuity

je nutné dbát o to aby plány byly funkční, proveditelné, všem zainteresovaným známé a odpovídaly požadavkům
metriky:

- existence a aktuálnost plánů
- znalosti klíčových pracovníků
- systém výcviku nových pracovníků
- dostupnost aktuální verze plánů
- zachycení všech klíčových činností v plánech (kompletnost)
- existují změny, které dosud nejsou zohledněny v plánech (aktuálnost)

nálezy nutno shrnout do zprávy, doplnit o doporučení

Náprava

veškeré nálezy z kontrol musí být sepsány, prioritizovány, navrženo řešení a stanoven časový rámec pro jeho realizaci
plán musí zahrnovat:

- detail nálezu
- podmínky pro zmírnění dopadů
- priotritizace
- čas na vyřešení
- nutné zdroje
- milníky implementace

Správa výjimek

pokud nález nelze vyřešit (zmírnit jeho dopad na akceptovatelnou mez), je nutné pro provoz příslušného řešení stanovit výjimku
musí být

- popsaná (tj, zejména jaké je riziko)
- evidována
- popsán důvod, proč nelze řešit
- časově omezená
- schválená
- stanovena kompenzační opatření

Provozování auditu

audit – porovnání reálného stavu organizace s deklarovaným stavem (standard, smluvní závazky, stanovený cíl, …)
namísto jednorázové kontroly stavu v určitém čase se prosazuje myšlenka „kontinuálního“ auditu – na základě artefaktů se zkoumá provoz v určitém období

je doporučeno postupovat podle některého ze standardů:

- ISO/IEC 15408 - Information technology – Security techniques – Evaluation criteria for IT security (společně s ISO 18045 - …methodology of IT security Evaluation)
- ISO/IEC 27006 - Information technology – Security techniques – Requirements for bodies providing audit and certification of information security management systems
- NIST 800-53A – Assesing Security and Privacy Controls in Federal Informations Systems and Organizations
- …

pro redukci nákladů na audit je možné kompletní audit všech aktiv nahradit auditem pouze vybraného reprezentativního vzorku aktiv

vnitřní audit
výhodou znalost prostředí a kultury
nebezpečí plynoucí z nezávislosti auditora
vhodný jako příprava na externí audit (omezení rizika dopadu na obchodní aktivity pro případ neúspěšného auditu)
vnější audit
obvykle vyžadován regulátorem, může být využit ve vztahu k zákazníkům (v rámci jejich SCM kontrol)
často jediná možnost, jak angažovat dostatečně erudované praocovníky
nezávislost a nezaujatý svěží pohled „odjinud“
audit třetí stranou

provádí zpravidla zákazník, nebo jiný obchodní partner
vychází z faktu, že vlastník nebo kontrolér dat je za ně odpovědný i v případě pochybení zpracovatele
obvyklé oblasti zkoumání:

- jaké standardy používají pro volbu opatření a provoz
- rozsah sdílených informací
- reakce na riziko, evidence slabin a incidentů
- existence plánů pro zmírnění/kontrolu nálezů