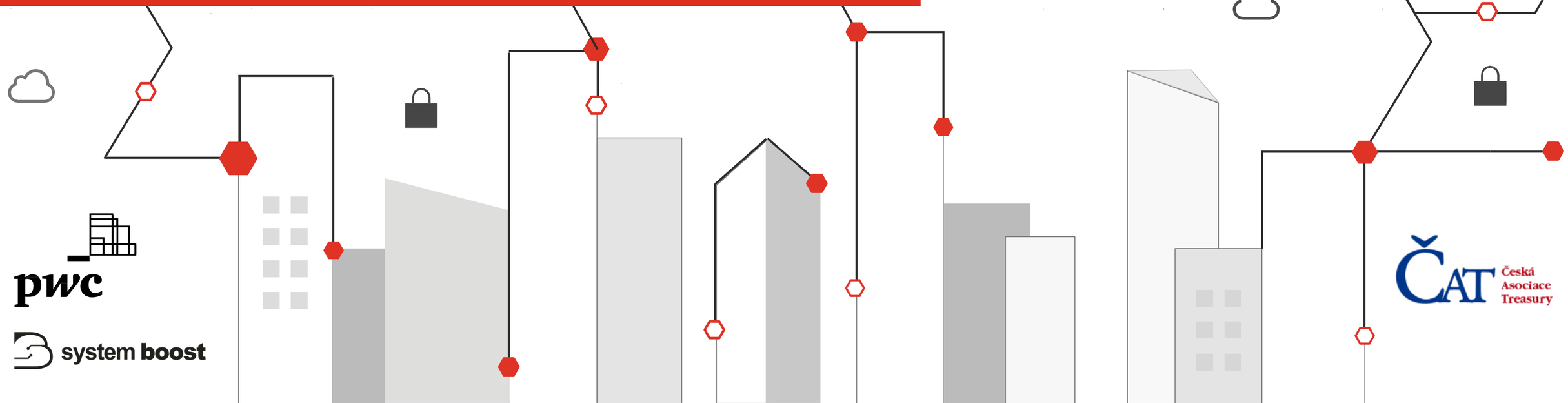
2021

Kyberbezpečnost

Kybernetické útoky – kontinuita podnikání a cyber security due diligence



pwc

system boost

ČAT Česká Asociace Treasury

O čem si dnes budeme povídat?

1. Zajištění kontinuity podnikání je úkol všech (manažerské desatero)
2. Cyber security due diligence

Kyberbezpečnost

1. Zajištění kontinuity podnikání je úkol všech (manažerské desatero)

Business Continuity Management

- Odolnost podniku je schopnost podniku zajistit kontinuitu podnikání i během mimořádných událostí.
- V dnešní významně konkurenční, a zároveň změnami ovlivněné, době je to jedna z nejdůležitějších schopností podniku vůbec.
- Z tohoto důvodu by měly podniky být schopny předvídat mimořádné události, a zároveň by měly mít připravené strategie, jakým způsobem se s mimořádnou událostí vyrovnat, v případě, že nastane.
- Měly by být schopny vyhodnotit minulé události a zároveň se z nich poučit, tak aby na ně byly v budoucnu připraveny.

Business Continuity Management

- BCM…
  - se zaměřuje na vytvoření pravidel a plánů, prevenci a snížení následků závažných incidentů nebo katastrof,
  - je součástí provozních procesů, které tato pravidla realizují.

- Cílem BCM je předejít negativním jevům, nebo alespoň zmírnit jejich následky, a co nejrychleji zajistit obnovu běžného provozu.

BCM – klíčové pojmy

01

Aktivum

Cokoliv, co má pro organizaci nějakou hodnotu, a je tedy potřeba chránit.

Aktivum může mít hmotnou i nehmotnou podobu a hodnotu.

02

Business Impact analýza (BIA)

Je základem celého procesu řízení kontinuity činností organizace.

Sestává z technik a metod, díky kterým může organizace účinně řídit rizika spojená s klíčovými aktivy podílejícími se na Core Bussinesu.

03

Disaster Recovery plán (DRP)

Shromažďuje postupy pro zajištění obnovy služeb po živelných pohromách a jiných zásadních událostech.

Je to v podstatě návod, jak v co nejkratším čase s minimem výdajů a rizik obnovit chod kritických aktiv.

Role DOPADu při řešení krizové situace

01 Přístup k rozhodování v rámci krizové situace lze popsat jako identifikaci možných maximálních dopadů na chod organizace.

02 Rozhodovací proces by měl generovat pokyny nebo opatření k ošetření těchto dopadů a přispět tak ke zvládnutí krizové situace v co nejkratším čase.

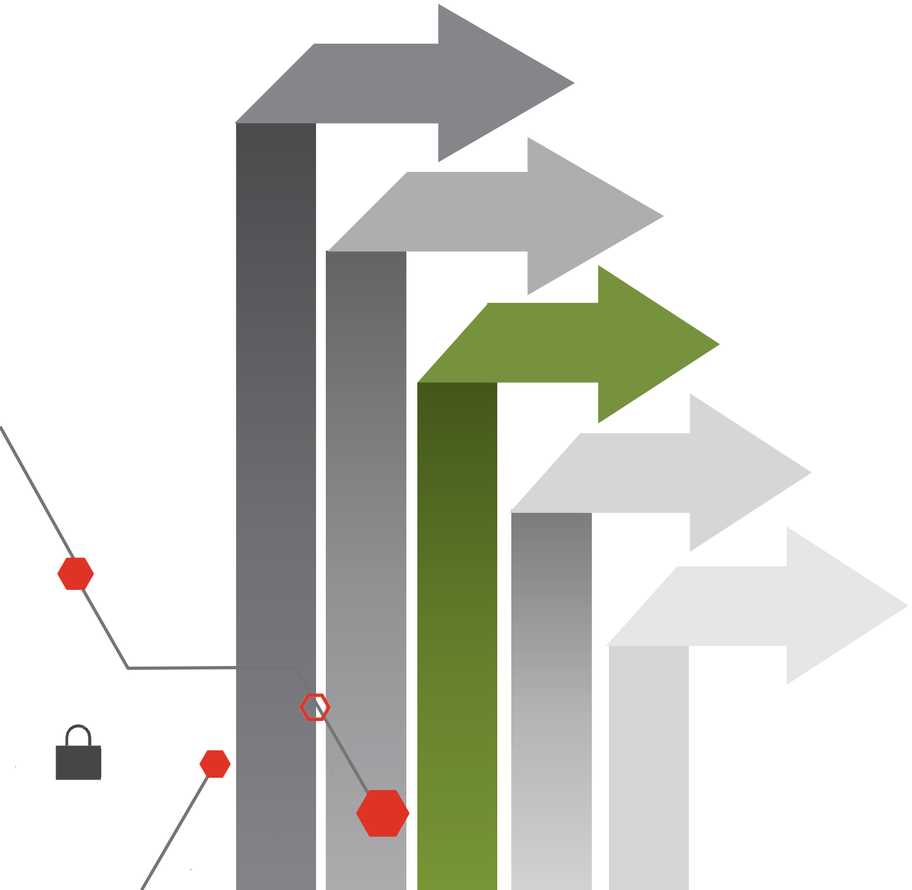
03 Při zvažování a odhadování maximálního možného dopadu je vždy nejdůležitější dopad na lidský život a zdraví.

04 Při určování dopadu jsou nápomocny výstupy z analýzy dopadů, která identifikuje klíčové procesy a aplikace z pohledu obchodních a strategických cílů organizace.

05 Klíčové mohu být také procesy a systémy, které nemají návaznost na obchodní cíle, ale jsou v oblasti, která je řízena externí legislativou.

Role ROZSAHu při řešení krizové situace

Rozsah odhadovaného dopadu má závislost na přístupu ke zdrojům, umožňujících návrat do normálního stavu před krizí:



- Data/informace, které aktivum procesuje.
- HW včetně požadované konfigurace umožňující očekávanou funkci.
- SW včetně požadované konfigurace a nastavení umožňující poskytovat očekávané procesy zpracování dat/informací.
- Lokalita, kde bude HW, SW a personál schopen zajistit obnovu funkce spravovaného aktiva.
- Personál s odpovídající znalostí, který je schopen spravované aktivum nejen obsluhovat, ale případně i nastavovat.

Zdroje při řešení krizové situace

- Zdroje a zejména jejich dostupnost jsou důležitým předpokladem pro úspěšné zvládnutí krizové situace.
- Je standardním procesem, že po vyhlášení krizové situace se zjednodušují interní procesy v oblasti zajišťování zdrojů.
- Jsou navyšovány limity pro nákupy, jsou zjednodušovány rozhodovací a schvalovací postupy, a to vše se snahou zajistit co nejrychlejší přístup ke zdrojům nezbytným pro zvládnutí krizové situace.

Personál

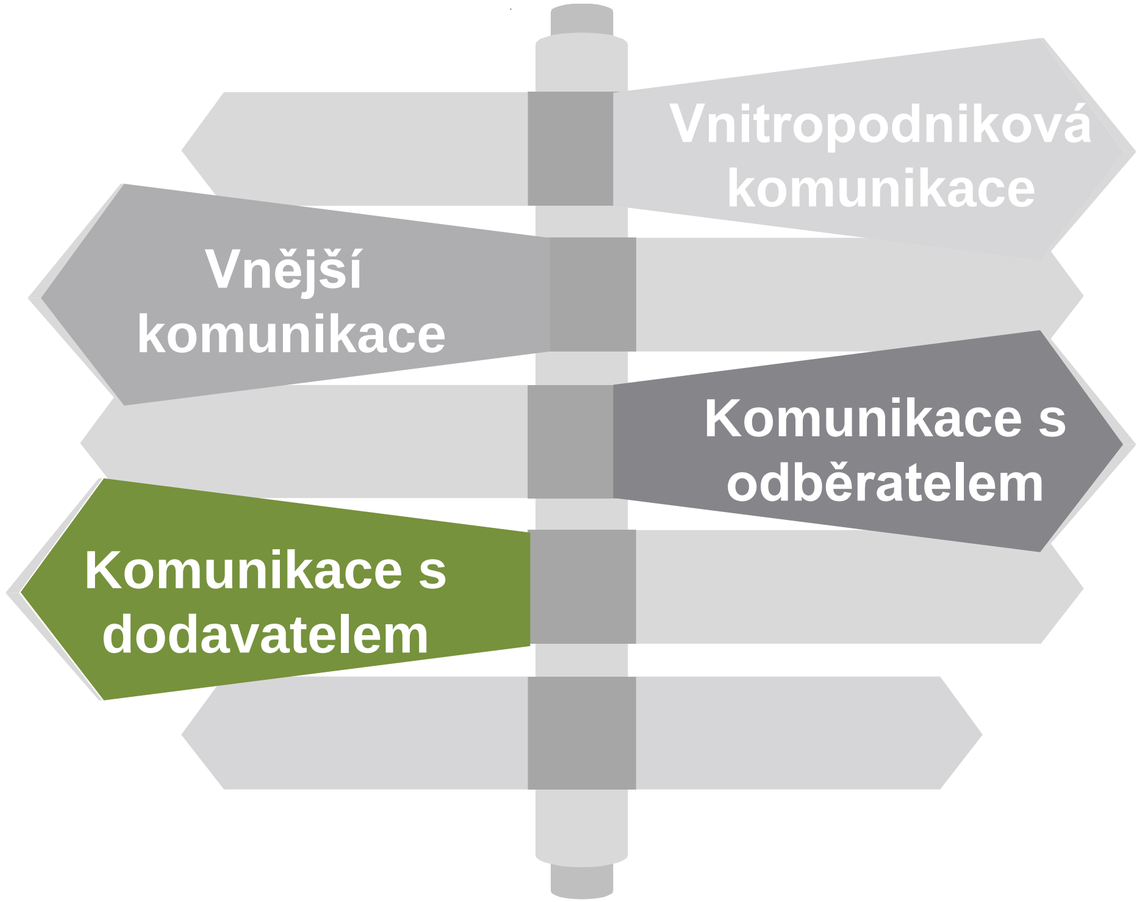
Náhradní lokalita

Náhradní SW a HW prostředí

Ostatní zdroje

Role KOMUNIKACE při řešení krizové situace

- Komunikace je klíčovým elementem pro úspěšné zvládnutí krizové.
- Jedná se o komunikaci jak dovnitř, tak vně organizace, a to nejen k odběratelům, ale zejména k významným dodavatelům, podílejícím se na provozu spravovaného aktiva.
- Důležitá je komunikační matice, která je vytvořena právě pro krizové situace a kde jsou zahrnuty všechny zainteresované osoby.
- Tuto komunikační matici je potřeba nejen udržovat aktuální a pravidelně ji kontrolovat, ale zejména pravidelně testovat, aby byl zajištěno a ověřeno, že všechny zapojené strany jsou seznámeny s jejich rolí v rámci komunikace.



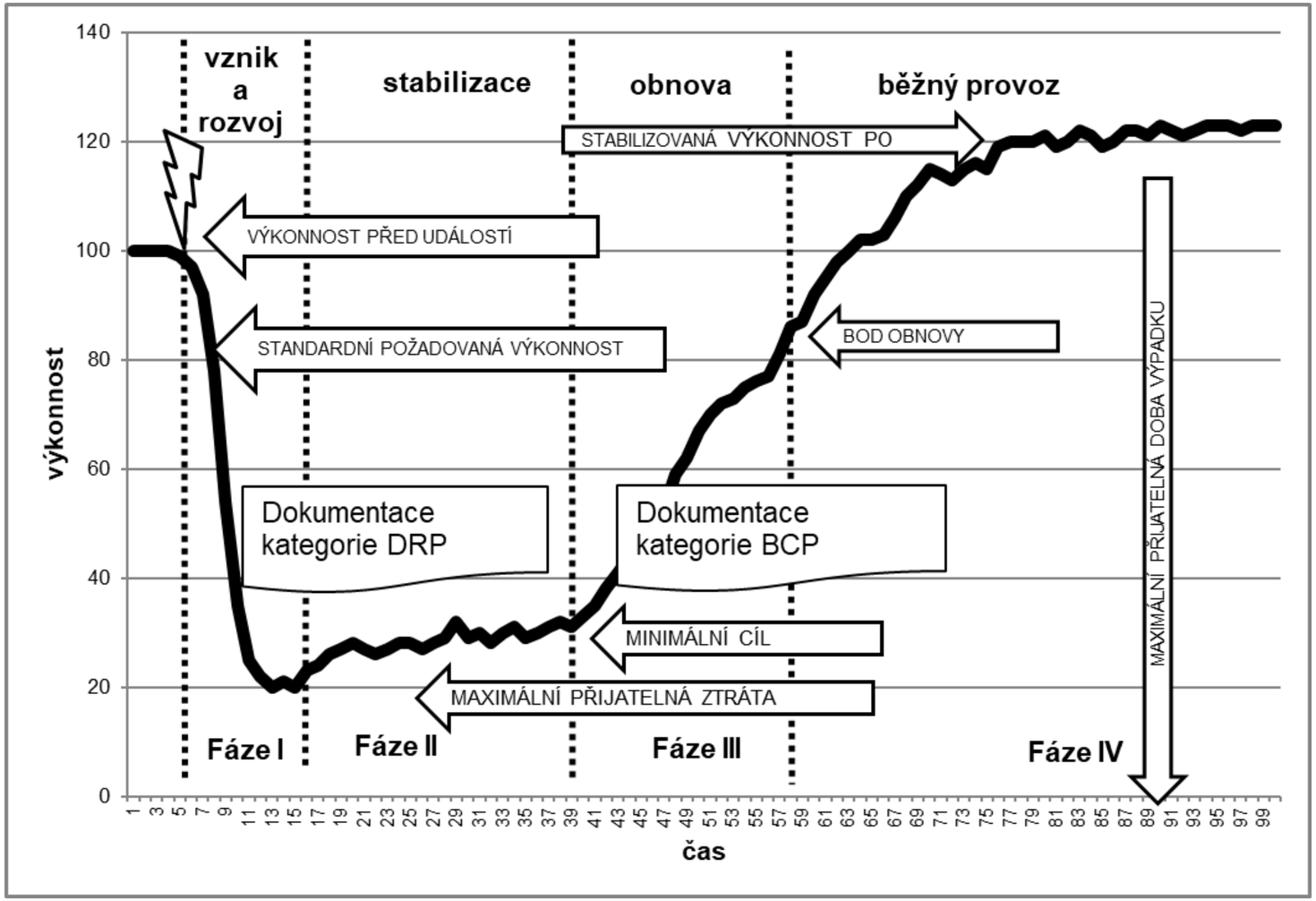
Cíl řešení krizové situace

- Mohlo by se zdát, že cíl tohoto kroku je jasný, zřejmý a pochopitelný – tedy vyřešení krizové situace, což je návrat do stavu před havárií.
- Prvním reálným krokem k vyřešení krize je dostat službu do bodu, definovaného jako minimální cíl kontinuity činností. Je to tedy chvíle, kdy služba generuje očekávané výstupy, nicméně v omezené míře.
- Tento minimální cíl se standardně stanovuje jako procento normálního provozu služby (např. 20 %).
- Minimální cíl je stanoven správcem služby v rámci zpracování Plánů kontinuity, či plánů obnovy (BCP, DRP).

Cíl řešení krizové situace

- Plán se připravuje v době, kdy není správce pod časovým tlakem a má dostatek času k promyšlení a zvážení jednotlivých kroků k řešení krize.
- Také v rámci pravidelného testování je často odhaleno nemálo informací a faktů, které nebylo možno v rámci přípravy identifikovat. Je tedy nutné po každém testování aktualizovat dokumentaci o nově získané informace z testování.
- Volba odpovídajících testovacích scénářů nejvíce přibližujících se reálným možnostem havárie výrazně napomáhá přípravě na neočekávané situace.

Obecný model zvládání mimořádné události



Manažerské desatero kybernetické bezpečnosti 1/3

1. Znám z paměti aktuálních 10 nejvýznamnějších rizik pro naši společnost a službu v mé správě.

2. Znám byznys procesy, na něž jsou navázány služby v mé správě.

3. Znám ukazatele standardní výkonnosti služby v mé odpovědnosti a ukazatele minimální úrovně služby (minimální cíl).

4. Mám aktuální zpracovaný DRP a BCP (havarijní plán a plán kontinuity), od posledního úspěšného testu neuběhl více než 1 rok.

5. Analýzu dopadu a rizik (resp. její aktualizaci) nemám starší než 1 rok.

Manažerské desatero kybernetické bezpečnosti 2/3

6. Od posledního školení v oblasti kybernetické bezpečnosti neuplynul více než 1 rok (školení pro mě i mé podřízené).

7. Ověřoval jsem si v posledním měsíci, že mám přístup a k dispozici provozní dokumentaci (k mnou spravované službě), která je aktuální a úplná, a není k dispozici žádná nová směrnice, se kterou jsem se řádně neseznámil.

8. Znám výsledky a doporučení posledního auditu zahrnující mou službu, na nepokrytých identifikovaných doporučeních v mé působnosti aktivně pracuji.

9. Znám složení Krizového štábu, mám k dispozici aktuální kontakty (telefonní číslo), vím, kde se nachází místnost pro krizové řízení (war room).

Manažerské desatero kybernetické bezpečnosti 3/3

10. Vím, kam a jak nahlásit havárii/incident, jaké informace a jak mám uchovat, abych umožnil jeho následné vyšetření.

11. Znám všechny své významné dodavatele služeb pro spravovanou službu a pravidelně prověřuji jejich schopnost řídit rizika s dopadem na mnou spravovanou službu.

12. U každého incidentu, který jsem u své služby řešil, jsem byl schopen identifikovat jeho příčiny a stanovit opatření k zamezení jeho opakování.

Kyberbezpečnost

2. Cyber security due diligence

Odhalení skrytých nákladů a dopadů do hodnoty společnosti při transakcích…

Přínosy Cyber Security Due Diligence

Potvrzení očekávání

Ověření si svých očekávání plynoucích z akvizice

Odhalení reputačních rizik

Finanční důvody

Snížení finančních dopadů a ztrát

Odhalení skrytých nákladů

Odhad nákladů za inovaci či restrukturalizaci

Bezpečnostní

Identifikace bezpečnostních hrozeb

Odhalení exitujících podvodných aktivit uživatelů

Personální

Identifikace dovedností uživatelů k předcházení bezpečnostních incidentů

Technické

Identifikace problémů s nekompatibilitou systémů

Zjištění při akvizicích a fúzích společností

- Nesoulad akvírované společnosti při akvizici či fúzi s regulatorními předpisy.
- Neočekávané vysoké investiční náklady na sjednocení (Security Maturity Level).
- Neověřené funkčnosti vnitřních Cyber Security procesů.
- Finanční či reputační dopady odcizených či zveřejněných dat, která byla odcizena před vlastní akvizicí.
- Finanční dopady při narušení bezpečnosti ze strany regulátorů z důvodu nefunkčních nebo nesprávně nastavených Cyber Security procesů.

Zjištění při akvizicích a fúzích společností

- Neočekávané „díry“ systémů, které mohou být díky zvýšení pozornosti v důsledku fúze zneužity (v důsledku publicity transakce).

- Neočekávané finanční dopady na opravu systémů a procesů, které byly předmětem akvizice akvírované společnosti.

Kritéria pro volbu Cyber Security Due Diligence

Kritérium	Cesta odhadu	Cesta posouzení
Cena	Nízká	Vysoká
Časová náročnost	Střední	Vysoká
Eliminace dopadů (finanční, reputační atd)	Nízká	Vysoká
Komplexita	Nízká	Vysoká
Míra součinnosti	Vysoká	Vysoká
Míra důvěry	Nízká	Vysoká

Cyber Security Due Diligence ve 4 krocích

Analýza

- Kontrola dokumentovaných informací
- Inicializační prověření společnosti (aktivní a pasivní ověření bezpečnosti a procesů)

Automatické ověření

- Automatický audit IT aktiv
- Automatické kontroly zranitelností
- Ověření bezpečnostního povědomí uživatelů

Manuální ověření

- Ověření souladu s regulatorními předpisy
- Ověření souladu s bezpečnostními normami
- Ověření identifikovaných zranitelností
- Kontrola procesů GDPR

Shrnutí výsledků

- Příprava výsledné zprávy
- Stanovení nákladů a opatření

Fáze analýzy

Průběh

- Sběr a kontrola informací o procesech a způsobech fungování kupujícího (vytvoření base line) a stanovení možných odchylek
- Sběr a kontrola informací o procesech a způsobech fungování akvírované společnosti
- Definování testovaných oblastí
- Stanovení regulatorních předpisů kladených na účastníky transakce
- Inicializační aktivní a pasivní skenování dle metodiky OSINT
- Stanovení a identifikace cenných aktiv akvírované společnosti (o co má primárně nakupující zájem) – Databáze zákazníků, informační systémy, procesy

Cíle

- Stanovení cenných aktiv a k nim definování kritických oblastí, které budou podrobeny testování
- Získání podkladů k rozhodnutí, zda pokračovat do další fáze

Výstupy

- Odhad časové a finanční náročnosti
- Definování přínosů a očekávání
- Dokumentované informace o fungování akvírované společnosti

Automatické ověření

Průběh

- Audit aktiv společnosti se zaměřením na nejcennější z nich
- Nasazení automatických skenovacích nástrojů do prostředí akvírované společnosti
- Konfigurace a sběr informací z vnitřní a vnější části společnosti (test systémů, procesů a lidí)
- Kontrola existence a funkčnosti procesů řízení bezpečnosti, včetně kontroly funkčnosti zvyšování povědomí o Cyber Security u zaměstnanců a partnerů
- Vyhodnocení nálezů a porovnání s informacemi z předchozí fáze, včetně definice míst k dalšímu šetření

Cíle

- Automatické ověření oblasti bezpečnosti s minimálně vynaloženým úsilím, včetně ověření funkčnosti zavedených opatření

Výstupy

- Sestavení mapy zranitelných míst organizace, jejich ohodnocení a projednání se zájemcem akvírované společnosti
- Orientační návrh ceny náprav či změn nutných k umožnění adopce společnosti

Manuální ověření

Průběh

- Manuální prověření nálezů a zjištění pro ujištění se o potencionálních dopadech
- Posouzení aktuálního stavu systémů, služeb, procesů, či smluvních závazků vůči nastavené baseline
- Kontrola vůči normám, zákonům a regulatorním předpisům
- Provedení kontrol vztažených k ochraně soukromí a ověření fungování požadovaných procesů
- Posouzení odhadu nákladů na změny a úpravy systémů, procesů a dalších kontrolovaných částí akvírované společnosti

Cíle

- Formou manuálního posouzení budou ověřeny výsledky automatizovaných testů a prošetřeny další oblasti, které mohou mít dopady do hodnoty společnosti, produktů, či služeb

Výstupy

- Soubor ověřených zjištění (zneužité zranitelnosti, chyby systému, atd…)
- Seznam identifikovaných chyb a nefunkčností v procesech
- Seznam identifikovaných nesrovnalostí v compliance

Shrnutí výsledků

Průběh

- Sestavení závěrečného reportu kontroly a souladu v průsečíku nákladů na sjednocení Security Maturity Levelu
- Kontrola výsledků se zástupcem kupujícího
- Stanovení dopadu do jednání o akvizici

Cíle

- Sestavení kompletního podkladu pro sjednocení Security Maturity Level v kontextu oblastí testování, včetně odhadu očekávaných nákladů, které jsou nutné pro sjednocení

Výstupy

- Finální závěrečný report stavu akvírované společnosti
- Stanovení dopadu do vyjednávání o ceně a pravidlech transakce

Výchozí rámec testování

- Základním standardem může být „Information System Security Assessment Framework“ (ISSAF)
- Komplexní rámec se zaměřením na management a procesy (jako jediný)
- Rámec poskytuje kontrolu oblastí:
  - Procesního charakteru
  - Technického zabezpečení
  - Projektového managementu
  - Strategie řízení kvality a bezpečnosti
  - Fyzického zabezpečení
  - Právního charakteru, zejména smluvního zajištění (úroveň NDA, možnosti kontrol, záruky a sankce…)

- Rámec testování není technologicky ani procesně omezen

Pokryté oblasti kontroly 1/2

- Project Management
- Guidelines And Best Practices
- Review Of Information Security Policy And Security Organization
- Evaluation Of Risk Assessment Methodology
- Technical Control Assessment
- Technical Control Assessment - Methodology
- Password Security
- Password Cracking Strategies
- Operating System Security Assessment
- Database Security Assessment
- Storage Area Network (San) Security
- Switch, Router Security Assessment
- Firewall Security Assessment
- Intrusion Detection System Security Assessment
- VPN Security Assessment
- Anti-Virus System Security Assessment And Management Strategy
- Web Application Security Assessment
- Internet User Security
- Source Code Auditing
- Binary Auditing (Reverse engineering)
- Social Engineering
- Physical Security Assessment

Pokryté oblasti kontroly 2/2

- Incident Analysis
- Review Of Logging / Monitoring & Auditing Processes
- Business Continuity Planning And Disaster Recovery
- Security Awareness And Training
- Outsourcing Security Concerns
- Knowledge Base

- Legal Aspects Of Security Assessment Projects
- Non-Disclosure Agreement (NDA)
- Security Assessment Contract
- Request For Proposal Template
- Desktop Security
- Penetration Testing Lab Design

Minimalistický rámec testování

- Active and Passive Device Discovery
- Remote Network Scans
- Automated Software Inventory
- Automated Account Inventory
- Automated Vulnerability Scan
- Privilege Review
- Domain Configuration Analysis
- Network Infrastructure Analysis
- Network Security Traffic Analysis
- Social Engineering

- Incident Response Plans
- Disaster Recovery Plans
- Business Continuity Plans
- Log Analysis
- OWASP Top 10*
- Training Records
- Study Previous Assessments
- Study Previous Audits
- Instructions & Procedures

Alternativní cesty a použitelné rámce testování

Lze zvolit alternativní cesty s ohledem na:

- Čas
- Finanční náročnost
- Komplexitu organizace

Je vhodné volit veřejně známé a uznávané testovací rámce:

- Opakovatelnost testování v čase a možnost eliminace neshod
- Lze volit i průsečíky mezi rámci (oblastmi kontroly)

	Focus			Tools	Easy to use	Integration to the context of IS/IT management
	Management	High level	Technical			
OSSTMM	No	Yes	No	No	No	No
ISSAF	Partially	Yes	Yes	Yes	No	Partially
PTES	No	Yes	Yes	Yes	Yes	No
OWASP	No	Yes	Yes	Yes	Yes	No
NIST SP 800-115	No	Yes	No	No	Yes	No

Případové situace

Případová situace 1

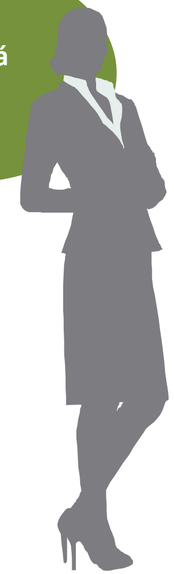
Příklad

Zájemce se rozhodoval o zakoupení společnosti, jejíž informační systém měl být v lepší technologické kondici, než-li informační systém zájemce. Společnost v průběhu testování zjistila, že systém je nemigrovatelný, obsahuje vendor lock-in a procesy společnosti zájemce nelze přizpůsobit, tak aby bylo možné využívat systém akvírované společnosti.

Důsledek

Pokles zájmu o danou společnost, snížení ceny společnosti a lepší vyjednávací pozice zájemce, jelikož došlo ke změně zájmových oblastí (zájemce změnil zájem z adopce informačního systému na zákazníky akvírované společnosti).

Případová situace 2



Příklad

Zájemce se rozhodl o koupení společnosti z důvodu rozšiřování svého portfolia o nový e-commerce produkt, jelikož chtěl kontinuálně přejít z retail businessu do e-commerce. Během provedeného testu se zjistilo, že systém byl vytvořen akvírovanou společností, existují zde závislosti na klíčových osobách společnosti a systém je postaven na starých a nemoderních konceptech. Tento systém by nebyl schopen v blízkém horizontu odbavit více než aktuální počet zákazníků a rozšíření by znamenalo nákup systému nového.

Důsledek

Zájemce odmítl nákup dané společnosti a rozhodl se pro investici do jiného řešení, jelikož hodnota akvírované společnosti klesla v důsledku e-commerce systému.

Děkujeme Vám za pozornost a prosíme Vaše otázky...