Bezpečnost při provozu

zahrnuje:

- fyzickou bezpečnost – dat i prostor
- reakci na incidenty
- podporu vyšetřování
- nakládání s důkazy
- digitální forenzní analýzu

provoz bezpečnosti by měl podporovat obchodní a vnitřní operace organizace s minimem dodatečných nákladů a komplikací

Podpora vyšetřování

shromažďování forenzních důkazů je vysoce specializovaná činnost prováděná odborníky – je však třeba být připraven spolupracovat
důkazem jakákoliv informace (shromážděná v průběhu vyšetřování incidentu) podporující dané tvrzení:

- logy
- záznamy (např. kamer, turniketů, …)
- počítačové soubory
- komponenty počítačů (disky, paměťová média)
- vytištěné materiály
- otisky prstů, vlasy, vzorky DNA, …

Shromažďování digitálních důkazů

… často velmi krátkodobé a volatilní záznamy (i prosté vypnutí zařízení je může zničit)
začíná v iniciálních fázích reakce na incident
nutno zajistit, aby se shromážděnými skutečnostmi bylo zacházeno tak, aby mohly sloužit jako důkazní materiál:

- zaznamenávat veškeré skutečnosti: data, časy, místa, veškeré provedené operace, kým
- vždy vytvořte kopie (ideálně binární celého zařízení)– a je-li to možné, analyzujte kopie
- zamezte nechtěným změnám – vylučte vypnutí, restart zařízení, provoz programů, zablokujte zápisy
- verifikujte integritu – např. spočítáním hashů všech dat / souborů

vyšetřování obvykle mívá vysokou prioritu a je nutno zajistit součinnost
nutno využívat izolovaných dedikovaných prostředků, aby se zabránilo kontaminaci zkoumaných (digitálních) důkazů
pro sběr důkazů

- nástroje pro zabránění zápisu (write blockers) a tvorbu obrazů (imagers)
- faradayovy kontejnery – zvláště při zajišťování mobilních zařízení)
- nástroje pro záznam audia a videa - pro dokumentaci vyšetřování

pro analýzu

- analyzátory komunikace
- nástroje SIEM a SOAR
- nástroje pro analýzu logů (BI)
- nástroje pro obnovu (smazaných) dat
- nástroje pro správu virtuálních strojů
- software pro reverzní inženýrink
- binární analyzátory a debugery
- hashovací nástroje (pro zajištění integrity dat)
- specifické toolkity pro daná prostředí

je třeba definovat **postupy pro případ incidentu**, které pamatují i na shromažďování budoucích důkazů (ISO27041 – 3, ISO27050) zahrnující:

- definici priorit (nemůžete mít vše najednou)
  - co nejrychlejší návrat k normálu
  - minimalizace škody
  - zaznamenání maxima detailů o incidentu
- identifikaci datových zdrojů (zejména těch volatilních a krátkodobých)
- plány, jak uchovat a zaznamenat potřebné informace – s prioritizací volatilních dat (logy, obsahy RAM) a využitím formálních vyšetřovacích postupů
- dokumentace a zachování integrity – záznam o provedených akcích, nakládání s daty, časová razítka apod.
- vyhledávání skrytých a smazaných dat
- provedení analýzy shromážděných informací – soudní ohledání

Artefakty

digitální stopy dokumentující interakci uživatele nebo programu s objektem
Locardův princip – pachatel zároveň vytváří stopy svého působení a maže jiné objekty

počítače – práce v prostředí zanechává specifické stopy (záznamy o instalaci / deinstalaci programů, provedení určitých příkazů, restarty, vypnutí / zapnutí ochran, změny konfigurací, změny nastavení ochrany, logy aplikací, IDS, firewallů, předchozí verze, recovery points, zálohy, indexy…
Windows: events (Event Log, včetně odpovídajících analyzátorů) smazané soubory ve filesystému, recycle bin, Windows registry, metadata, skryté a systémové oblasti, swap
macOs: Console, Trahs, Time Machine backup, Spotlight, vyhledávání, historie PLIST soubory, …
Linux: obecně obsah /tmp a /var, případně /opt či /usr,
Prohlížeče obecně: historie, cache, cookies, uložená hesla, …

sítě – celá řada aktivních prvků ukládá logy, často je možné zjistit důležité informace z dosud probíhající komunikace (NetFlow, WireShark, pcap)

mobilní zařízení – dnes často šifrování lokálního úložiště a vzdálené uložení dat, tedy nutno získat příslušné soudní příkazy, hledání odcizených zařízení pomocí příslušných lokalizačních služeb či ve spolupráci s operátory, možnost zařízení vzdáleně uzamknout či smazat (nebo alespoň wallet), nutno prověřit všechna připojení (3-5G, Wifi, bluetooth, NFC, …), zařízení nevypínat, ale zabránit mu v komunikaci (Faradayova klec).

Monitoring a logování

logování je proaktivní (definice strategie pro tvorbu logů) i reaktivní (záznamm činností spojených s incidentem) i následné (analýza) opatření
definice strategie monitoringu, výběr efektivních nástrojů a provádění monitoringu a kontrol je základním elementem řízení rizik

IDS a IPS

detekují a případně reagují (IPS) na „známky“ napadení – přesněji, na chování, které je neobvyklé, nebo odpovídající známým útokům
síťové IDS – zpravidla samostatné zařízení skenující veškerou komunikaci, integrováno s firewallem, proxy apod.
aplikační (host-based) IDS – reaguje na antimalware, případně udržuje hash povolených programů a aplikací
dnes nahrazováno šířeji pojatými EDR (endpoint detetection and response) řešeními zahrnujícími antimalware, řízení konfigurací, detekci napadení (HIDS)

potíž s IDS / IPS je v tom, že „neobvyklé“ ne vždy znamená útok

SIEM

správa bezpečnostních informací a událostí (security information and event management)
obecně jde o více či méně integrované mechanismy pro agregaci logů a jejich centrální vyhodnocování / vytěžování zahrnující tyto kroky:

- centralizace
- normalizace
- korelace a detekce – propojování akcí v různých systémech
- pokročilá detekce – např. korelace s HR systémem, evidencí pracovních cest apod.
- alerting

Kontinuální monitoring

vzhledem k rychle se vyvíjejícím hrozbám již nepostačují “bodové“ kontroly jako periodické výroční audity a akreditace
nutností jsou časté kontroly a ověření, že používaná opatření efektivně minimalizují riziko
základem podpora na úrovni politiky a managementu
hlavní aspekty strategie

- definice referenčních hodnot – doporučená (minimální) nastavení, použití obecných rámců (CIS benchmark, STIG,), prioritizace kontrol kritických služeb
- automatizace – nejen kontrol, ale i vyhodnocování logů, analýza událostí, chování uživatelů, apod.
- frekvence – rovnováha mezi včasností detekce a náklady na analýzu
- vhodnost metrik – je třeba se zamyslet, jaké ukazatele jsou relevantní pro rozhodování o nutnosti změny
- definice akčních plánů – za jakých okolností a jak je nutno reagovat na změnu metriky
- vyvážení nákladů a získané hodnoty

Monitoring výstupu

útočník se často snaží něco odcizit – informace, zařízení, materiál, klidně i odpad
nutno hlídat, jaká data a zařízení opouštějí bezpečný perimetr

DLP (data leakage prevention) – nástroj lze „naučit“ rozpoznávat chráněná data různých charakteristik, ten potom provádí screening komunikace, může upozornit administrátora nebo zabránit přenosu
… často bývá používáno i pro detekci nežádoucích vstupních dat
samozřejmě nutno na fyzické úrovni kontrolovat vstup a výstup zařízení

Správa logů

logy jsou nezbytnou prerekvizitou mnoha bezpečnostních aktivit, zejména monitoringu a řízení incidentů
hlavní oblasti činnosti:
Definice auditovatelných událostí a prahových hodnot – tedy co vše se bude logovat, odvíjí se od znalosti hrozeb:

- úspěšné a neúspěšné pokusy o přístup
- změny oprávnění
- změny nastavení bezpečnostních nástrojů
- manipulace se senzitivními daty
- transakce nad senzitivními daty

nutné informace pro rekonstrukci operace:

- ID subjektu
- časový záznam
- identifikátor zařízení
- cílové objekty
- identifikátor politiky dle které logováno

zajištění integrity, důvěryhodnosti a utajení logů
uložení v odděleném systému s rozdílným nastavením přístupů (tzn. jiný administrátorský tým)
na druhou stranu, je nutno zachovat dostupnost logů pro účely analýzy
problémem je doba retence a z toho pramenící objem
nutno respektovat různé požadavky na dobu retence (zákonné – personální a účetní požadavky, oborové, smluvní)

Zpravodajství o hrozbách

cílem je mít povědomí o aktuálních hrozbách a moci tak proaktivně reagovat na ohrožení
zdroje informací

- vlastní „threat hunting“

- veřejně dostupné kanály – např CZeRT, informační kanály dodavatelů systémů a aplikací, …
- často poskytováno jako služba dodavatele SOAR či SIEM řešení
- zájmová oborová sdružení často rovněž poskytují informace o relevantních hrozbách

hrozby nutno vyhledávan na různých úrovních:
strategické – nutnost změnit politiku, zavést nová opatření apod.
taktické – informace o novém útoku / nástroji poslouží k úpravě nastavení stávajících opatření umožňující detekci
operační – porozumění technice útočníka, nástrojům, postupům

Analýza chování uživatelů a entin

entitou zde rozumíme technický subjekt
definujeme normální očekávané chování – hledáme odchylky

Správa konfigurací

formální proces identifikace klíčových aktiv jejichž stav (konfigurace) musí být řízena

- položky konfigurace – celé systémy, jednotlivá rozhraní, zdrojový k=´d, …
- výchozí stav (baseline) – bezpečná konfigurace položky, jeho změna vyžaduje formální změnový požadavek a schválení (změnové řízení)

předpisy pro správu konfigurací zahrnují

- hardware
- software
- role pro řízení přístupu
- odpovědnosti, potřebné zdroje

Provisioning

instalace a nasazení zařízení, systému nebo aplikace – mělo by podléhat standardnímu procesu
pravidla pro pořizování pouze schválených zařízení / řešení
konfigurace v souladu s požadovaným výchozím stavem – obvykle zahrnuje hardening
v současné době příklon ke kontejnerizaci, použití VM, případně technologii IaC – infrastructure as code
postupy pro testování, akceptaci a přechod do produktivního používání

Inventář aktiv

vložení nového aktiva do inventáře je klíčovým elementem správy konfigurací – nelze udržovat věc, o které nevím
proaktivní správa inventáře zahrnuje integraci s nákupním systémem, systémy pro automatickou aplikaci patchů a řízení upgrade apod.
označení či vymazání vyřazovaných aktiv

Výchozí stav (baseline)

… souhrn odsouhlasených atributů systému / zařízení
slouží jako referenční bod pro určení míry rizika, je nutno jej udržovat v dobrém stavu vzhledem k známým hrozbám a doporučením
řízení změn potom chápeme jako přechod od jednoho výchozího stavu k dalšímu
pro většinu systémů jsou definovány doporučené konfigurace, které lze chápat jako základ pro definic výchozího stavu

Automatizace

chybná konfigurace je jednou z nejčastějších příčin bezpečnostního incidentu
audit nastavení je proto klíčovou aktivitou pro zajištění bezpečnosti
vhodné používat automatické nástroje pro kontrolu nastavení – skanery slabin, kontrolery shody, apod.
metoda neměnné infrastruktury – nastavení je statické, změny se neprovádějí za provozu, ale výhradně v průběhu odstávek, např. změnou definic IaC

Aplikace fundamentálních bezpečnostních konceptů

je třeba důsledně prosazovat základní koncepty:

- need-to-know
- separace odpovědností
- bezpečnost dvou osob (two person security)
- rotace pracovníků
- definice SLA
- minimální oprávnění

předpokladem aplikace těchto konceptů je odpovídající architektura systému, organizačních směrnic a celé atmosféry uvnitř organizace

Správa privilegovaných účtů

tzn. účtů s rozsáhlými pravomocemi
nutno definovat kritéria, pro identifikaci privilegovaných účtů

doplňující požadavky na správu – striktní uplatnění minimálních oprávnění, dodatečné prověření držitelů, vyšší nároky na monitoring
využití výhradně k účelům, pro které jsou rozšířená oprávnění nutná

- provisioning – dodatečné schvalovací kroky, podrobná dokumentace, sledování držitele, dodatečné prověření
- použití – časově omezené a automaticky ukončené, oddělené od rutinní práce uživatele (elevace, sudo, impersonace, …), „break the glass“, rozšířené logování, vyšší nároky na autentizaci
- kontrola – zvláštní pozornost operacím prováděným privilegovaným účtem, zvýšený monitoring a manuální kontrola logů
- odebrání – obvykle požadováno, aby záznamy spojené s použitím účty bylo zachovány déle

Ochrana datových zdrojů

aplikace postupů a prostředků pro ochranu aktiv organizace
médiem rozumíme cokoliv, co může nést data

Označování

indikace senzitivity uložených dat
samotná data mají v sobě obsahovat údaj o seznitivitě (watermark, standardní záhlaví nebo metadata, jmenná konvence pro název souboru, …)
nutno školit znalosti o systému znační a pravidlech pro nakládání s informačními aktivy

Ochrana médií

… aplikací bezpečnostních opatření dle senzitivity
základem fyzické zabezpečení – bezpečné uložení, přenos v uzamčených schránkách, bezpečnostní zámky, zajištění neustálého dohledu
šifrování obsahu
zajištění integrity – hashování, digitální podpisy a pečetě
striktní pravidla pro zacháznení s médii při transportu

Sanitizace a vyřazování

ne vždy možné – celá řada médií neumožňuje bezpečné smazání / přepsání dat
certifikované přepsání původních dat – pokud je postačující a médium umožňuje
cryptoshredding – pokud data ukládáme výhradně zašifrovaná, postačí smazání příslušného klíče
fyzická destrukce – ve všech ostatních případech

Řízení incidentů

událost – jsou pozorovatelné akce a operace (rutinní přihlášení, zápis do souboru, spuštění programu, …)
incident – neplánovaná událost s negativním dopadem; vyžaduje prošetření a nápravu

Plán řízení incidentů

dokumentuje nástroje, zdroje a procesy správy incidentů
obsahuje:

- definici typů incidentů
- seznam členů týmu pro reakci na incident
- role a odpovědnosti týmu
- potřebné zdroje a kontrolní seznamy
- postupy pro jednotlivé fáze zvládání incidentu

kategorizace incidentů:

- kritičnost – rozsah dopadu na provoz
- urgentnost – jak rychle nutno vyřešit, aby se předešlo neakceptovatelným důsledkům

plán musí být pravidelně testován za účelem identifikace nedostatků či chyb i kvůli trénování zainteresovaných pracovníků
může být nutné angažovat i dodavatele a další třetí strany

Detekce

aby organizace mohla reagovat, incident musí být rozpoznán

- automatickým nástrojem
- analýzou logů
- uživateli

nutno okamžitě zahájit dokumentaci všech činností
rozhodnout, zda opravdu jde o incident
spustit proces reakce na incident

Reakce

identifikace kritičnosti
kategorizace typu incidentu
zjištění dopadu
na základě zjištěných skutečností sestavení odpovídajícího týmu reakce
shromáždění informací i incidentu a stanovení postupu pro návrat k normálu

pro předpokládané incidenty by měly existovat předem dokumentované postupy založené na seznamech činností
jednou z prvních činností je shromažďování stop, včetně zajištění záznamu o nakládání s nimi
iniciální reporting o stavu
průběžné zpracovávání dokumentace zahrnující:

- shrnutí detekce
- provedené kroky prošetření a reakce na incident zahrnující čas, jméno pracovníka a účel aktivity
- shromážděné informace
- zdroj útoku
- seznam všech zdrojů relevantních informací

Zmírňování dopadů

probíhají operace pro vyřešení incidentu
zejména izolace, nebo uzavření (zdroje / dopadu) incidentu
následně příprava práce na obnově a návratu k normálu
vše je třeba dokumentovat
součástí reporting stavu a výhledu

Reporting

- je třeba zajistit včasné a průběžné informování všech zainteresovaných stran management,
- uživatelé,
- veřejnost,
- regulační orgány
- vládní organizace
- oborové organizace
- orgány činné v trestním řízení
- obchodní partneři
- zákazníci a dodavatelé

Pokud dojde ke kompromitaci či poškození osobních dat, bývá potřeba rpovést specifický reporting úřadům a subjektům dotčených dat.

Obnova

vlastní práce na návratu k normálnímu provozu
nemusí být součástí všech incidentů

Náprava

analýza příčin incidentu a návrh nápravných opatření
případná finanční vyrovnání a odškodnění

Poučení

dokumentace veškerých poznatků z průběhu a řešení incidentu
nutné změny pro zabránění opakování incidentu
co se osvědčilo, co moc nepomohlo

Provoz detektivních a preventivních opatření

opatření, která brání útoku, nebo alespoň snižují pravděpodobnost jeho provedení
mějte na mysli paradigma ochrany do hloubky
nejde jen o technologické prostředky, musí je spravovat a používat lidé, kteří vědí co a proč dělají
je třeba stále porovnávat stav a výběr opatření se stavem hrozeb a vlastního informačního systému
opatření zahrnují

- firewally
  - bezestavové
  - stavové
  - proxy brány (web app fw., api gw, …)
  - osobní fw
  - ngfw – kombinace fw se strojovým učením a umělou inteligencí
- IDS a IPS
- Whitelisting / blacklisting
- Bezpečnostní služby třetích stran
  - audit (SOC)
  - Digitální vyšetřování a reakce na incidenty
  - Zpravodajství o hrozbách
- Sandboxing a kontejnerizace
- Honeypots a honeynet
- Antimalware
- Nástroje strojového učení a umělé inteligence … pro IDS, SIEM, EDR, DLP a další automatické prostředky

Správa slabin a záplat

je nezbytné sledovat průběžně výskyt nových slabin
posuzovat jejich relevanci
aplikovat pathce, pokud nejsou, zavést odpovídající kompenzační opatření

Správa záplat

udržování přehledu o dostupných záplatách a aktualizacích
plánování jejich nasazení
zvážení automatické aplikace (FUJ)
obecný proces správy záplat zahrnuje:

- detekci slabin
- publikaci záplaty
- vyhodnocení vhodnosti záplaty
- testování
- aplikace / nasazení a sledování průběhu
- rollback
- dokumentaci

Správa slabin

je kriticky důležité včas objevit slabiny používaných prostředků a plánovat včas odpovídající kroky
zahrnuje celou řadu aktivit

- lov hrozeb (threat hunting) – vyhledávání zdrojů ohrožení s odhadem, jaké slabiny mohou využívat
- hledání slabin – zpravidla prostřednictvím automatických nástrojů, rychlé, leč pouze známé slabiny
- red teaming – zpravidla manuální posuzování zabezpečení daného aktiva, umožňuje objevit i neznámé slabiny
- penetrační testování a odměny za chyby

Participace na správě změn

veškeré plánované změny je třeba posuzovat z hlediska bezpečnosti
nutno zahrnout odpovídající testy
zdokumentovat veškeré změny (CMDB)
sledovat proces implementace změny

- standardní změny – nízké riziko, implicitně odsouhlaseny (standardní patche, rozšíření kapacity, instalace SW ze schváleného seznamu, …)
- normální změny – vyžadují úplné provedení změnového řízení, mívají vlastní projektový plát, testování, akceptaci, nasazení
- urgentní změny – v nestandardních situacích (např. incident), nezbytné pro zachování provozu, formální náležitosti a schválení jakož i posouzení z hlediska bezpečnosti může být provedeno zpětně

Implementace strategií obnovy

je třeba předem zajistit prostředky pro obnovu v případě incidentu
zahrnuje provádění dopadových analýz, enumeraci kritických aktiv, vyhodnocování potřeb organizace
RTO – recovery time objective
RPO – recovery point objective
MTD / MAD – maximum tolerable / alovable downtime

Strategie zálohování

- diferenční zálohy
- inkrementální zálohy

plánování záloh musí odrážet požadované parametry obnovy (ne vždy se obnovuje poslední stav)
údržba integrity a utajení záloh

- průběžné kontroly integrity záložních dat
- testovací obnova
- nutnost nakládat se zálohami jako s ostrými daty

redundantní úložiště

- RAID
- storage mirroring

Cloudová úložiště

- nutné specifické řešení utajení
- často samotné použití cloudu zahrnuje redundanci (součástí služby)

Strategie obnovy prostor

záložní prostory v geograficky oddělených lokalitách
rozdělení personálu, zdrojů, procesů
různé úrovně přípravy záložních kapacit

- hot site
- warm site
- cold site
- cloud bursting (dočasné využití cloudu), nebo navýšení kapacity

Distribuované zpracování

informační systém lze distribuovat mezi několik lokalit a zajistit datovou konzistenci
zpravidla vyšší provozní náklady i architektonická složitost

Odolnost systému a vysoká dostupnost

informační systém musí být již ve fázi návrhu architektury plánován s ohledem na požadavky dostupnosti, rozsahu výpadků, výkonu, odezvy, …
automatická detekce výpadků a restart chybějících služeb
prostředky jako

- load ballancery
- clustery
- redundance
- rerouting požadavků
- prioritizace
- QoS
- fault-tolerance

Implementace procesů obnovy po katastrofě

obnova zahrnuje veškeré činnosti návratu k normálnímu provozu po zvláště rozsáhlých incidentech
zotavení je užší soubor činností směřujících k zajištění provozu pouze klíčových služeb
katastrofa je formálně deklarována na základě oficiálního rozhodnutí
obnova je součástí rozsáhlejšího rámce plánování a zajištění kontinuity obchodních operací

Reakce

nejvyšší bezpečnostní manažer je zpravidla členem skupiny osob oprávěnných deklarovat stav katastrofy
prováděné činnosti záleží na charakteru katastrofy, měly by být prováděny dle předem navržených a odsouhlasených plánů

- zajištění záchrany životů, zdraví a bezpečnosti personálu
- koordinovaná reakce – řízené akce dozorované koordinátorem
- jasná a konzistentní komunikace
- dokumentace provedených prací

Personál

zajištění života, zdraví a bezpečnosti lidí je primární cíl
nutno definovat potřebné odbornosti, lidské pokrytí, role jednotlivých pracovníků a jejich odpovědnosti
zde pomůže prováděná rotace pracovníků a cross-training
zajištění pracovních podmínek (jídlo, pití, toaletní potřeby, odpočinek, odreagování, ale i péče o rodinné příslušníky)

Komunikace

informování všech zainteresovaných stran (stakeholders)
one-voice
vhodné roveň informovanosti pro vnitřní i vnější příjemce informací

Vyhodnocení

zjištění rozsahu a prioritizace akcí
identifikace zdroje a povahy incidentu
identifikace aktuálního a očekávaného dopadu
výsledky posouzení musí mít k dispozici vedení a příslušní výkonní pracovníci

Zotavení a Obnova

omezený provoz zpravidla soustředěn na zajištění klíčových funkcí a procesů
až po jejich zajištění se přejde k obnově původní lokality, nebo zahájení přesunu jinam
obnova již zpravidla probíhá za klidnějších podmínek mimo režim ohrožení

Výcvik a povědomí

plány zachování kontinuity a obnovy musí být dokumentovány
musí být prováděné školení personálu v oblasti bezpečnosti

- ochrana života a zdraví
- bezpečnostní plány
- rozpoznání nebezpečí a první reakce
- pokročilá školení pro personál mající odpovědnost v rámci procesů obnovy
- pravidelná cvičení
- rutinní testování

Poučení

co fungovalo, co nefungovalo
shrnutí a doporučení
analýza příčin

Testování plánů obnovy

je nutné pro zajištění jejich funkčnosti
umožní odhalit chyby, nelogičnosti, neopodstatněné předpoklady, neproveditelné kroky
přispívá ke zvyšování povědomí
na druhou stranu je nákladné, omezující a riskantní

Pročítání

úzká skupina manažerů a zástupců zájmových skupin na společném sezení prochází jednotlivé kroky plánu
verifikují se informace, sleduje se návaznost kroků, ověřuje se adekvátnost zdrojů
cílem je najít očividné chyby, chybějící informace apod.

Procházky

podobné jako pročítání, ale provádí se přímo na místě
ověřuje se dosažitelnost jednotlivých lokací, chybějící vybavení, personál se seznamuje s prostředím

Simulace

něco jako požární poplach
tým obnovy dostane za úkol provést obnovu konkrétní služby v alternativní lokalitě
kontrolují se všechny technické kroky, jejich návaznost, proveditelnost, časování, …

Paralelní test

paralelně s během primárního systému se provádí jeho obnova v záložní lokalitě
následně kontrola přesměrování komunikace a použití nového systému
významně náročné na zdroje
komplexní test všech aspektů plánu (tedy skoro všech)

Plné přerušení

toto je opravdové dráždění hada bosou nohou – vypne se živý fungující systém, předstírá se ztráta kapacit a provede se obnova příslušné části služeb a otestování jejich provozu
významně riskantní (uvažte, kam to asi tak obnovíte) a drahé (je vypnuto)
ani tohle neotestuje úplně všechno, ale je to nejblíže, kam se můžete dostat

Účast na plánování kontinuity operací

ač pracovníci odpovědní za bezpečnost nejsou vlastníky BC procesů, měli by vnášet vstupy týkající se postupů v případě omezení operací:
fyzické zabezpečení v době omezeného provozu
modifikace bezpečnostních funkcí
ověření plánů kontinuity z hlediska bezpečnosti
podpora při provádění testů

Implementace fyzické bezpečnosti

formulace požadavků na fyzické uspořádání prostředí – zahrnuje nejen samotné prostory kde probíhá zpracování informací, ale i jejich okolí
požadavky na přístupové metody a prostředky
vytyčení perimetrů
definice fyzických prostředků (bariéry, zóny) technických prostředků (čtečky, turnikety, osobní identifikátory) a administrativních kontrol
body vstupu a výstupu

- recepce nebo ostraha
- vstupní zařízení
- senzory
- kamery
- stráže

návrh okolí budov – terasy, vodní prvky, stromy … mohou sloužit jako bariéry
stavební provedení – pevnost konstrukcí, jejich nepřekonatelnost, osvětlení a další náležitosti umožňující používání

Bezpečnost personálu

cestování – mobilní pracovníci mohou potřebovat odpovídající pojištění, lékařské zajištění, obecné proškolení o bezpečnosti v cílové destinaci
musí být školeni jak na cestách chránit vybavení, bezpečně pracovat a nakládat s informacemi, pravidla pro sanitizaci zařízení po návratu z cesty, při podezření ze zneužití, ztrátě apod., použití sdílených prostředků
zajištění bezpečného vzdáleného přístupu, bezpečného používání sítí a jiných veřejných prostředků

koordinace s ostatními odvětvími bezpečnosti – zejména požární, zdravotní, případně silovými složkami

zahrnuje i alternativní postupy pro případ krizí a katastrof
krizová komunikace musí být založena na jednoduchých, snadno použitelných postupech

vydírání – pracovníci by měli mít k dispozici prostředky, jak signalizovat, že jsou nucení provést určitou akci aniž by se vystavovali nebezpečí (např. zadání specifického hesla, určitá věta pronesená při komunikaci) přičemž odezva musí vypadat „normálně“.