
AUDIT A KONTROLNÉ ČINNOSTI V KYBERNETICKEJ BEZPEČNOSTI ZÁKLADY



Financované
Európskou úniou
NextGenerationEU

PLÁN [OBNOVY]



KOMPETENČNÉ
CENTRUM
KYBERNETICKEJ
BEZPEČNOSTI

STU

SLOVENSKÁ TECHNICKÁ
UNIVERZITA V BRATISLAVE

OBSAH

1. **Úvod:** Prečo je táto téma dnes kritická?
2. **Prehľad auditov a kontrolných činností:** Základné definície a rozdiely.
3. **Nevyhnutnosť pre digitálnu bezpečnosť:** Strategické výhody auditov.
4. **Pohľad bežného používateľa:** Kybernetická hygiena ako osobná kontrola.
5. **Pohľad systémového administrátora:** Technická implementácia a typy auditov.
6. **Certifikovaný audit podľa legislatívy SR:** Povinnosti a procesy.
7. **Strategický dohľad a pokročilé metodiky:** Penetračné testovanie a riadenie rizík.
8. **Osvedčené postupy a bežné chyby:** Ako sa vyhnúť nástrahám.
9. **Kľúčové princípy a definície:** Základné pojmy.
10. **Záver:** Zhrnutie a strategické odporúčania.

ÚVOD: KONTEXT A DÔLEŽITOSŤ

- Digitálna transformácia priniesla obrovské príležitosti, ale zároveň aj zvýšené riziká v oblasti kybernetickej bezpečnosti.
- V tomto dynamickom prostredí sa kybernetické audity a kontrolné činnosti stali neoddeliteľnou súčasťou riadenia rizík a ochrany digitálnych aktív.
- Táto prezentácia poskytuje komplexný prehľad týchto kľúčových aspektov z pohľadu bežných používateľov, administrátorov aj bezpečnostných špecialistov.

ČO JE KYBERNETICKÝ AUDIT?

- **Definícia:** Audit je systematický, nezávislý a zdokumentovaný proces získavania objektívnych dôkazov a ich objektívne vyhodnotenie s cieľom určiť mieru plnenia stanovených kritérií.
- V kontexte kybernetickej bezpečnosti ide o nezávislé a dôkladné preskúmanie úrovne informačnej bezpečnosti v organizácii.
- Zahŕňa detailnú kontrolu systémových záznamov, aktivít a súvisiacej dokumentácie.
- Audity sú typicky vykonávané nezávislými tretími stranami, aby sa zabezpečila objektivita a eliminoval konflikt záujmov.

ČO SÚ KONTROLNÉ ČINNOSTI?

- **Definícia:** Kontrolné činnosti sú akcie, politiky a postupy zavedené s cieľom zabezpečiť, aby sa riadiace smernice na zmiernenie rizík vykonávali efektívne.
- Ide o zistenie stavu alebo overenie výsledku určitej činnosti.
- Vykonávajú sa na všetkých úrovniach organizácie a v celom technologickom prostredí.
- Príklady zahŕňajú autorizácie, schvaľovania, overovania, zosúlad'ovania a preskúmania výkonnosti.
- Kľúčovým cieľom je prevencia, detekcia alebo náprava nežiaducich udalostí.

KLÚČOVÝ ROZDIEL: AUDIT VS. HODNOTENIE

- Hoci sa často zamieňajú, ide o dva odlišné mechanizmy.
- **AUDIT:**
 - Je hodnotením v danom čase.
 - Overuje, či sú konkrétne bezpečnostné opatrenia **zavedené**.
 - Porovnáva stav s kontrolným zoznamom (napr. pre účely súladu).
- **HODNOTENIE (Assessment):**
 - Je analýza na vysokej úrovni.
 - Určuje **účinnosť** zavedených opatrení.
 - Poskytuje pohľad na celkovú kybernetickú zrelosť organizácie.
 - Ideálne by malo hodnotenie predchádzať auditu a slúžiť ako príprava.

NÁSTRAHY PRÍSTUPU ZAMERANÉHO LEN NA SÚLAD

- Organizácia môže technicky prejsť auditom (kontroly sú prítomné), no napriek tomu zostať zraniteľná, ak sú tieto kontroly neúčinné, zle nakonfigurované alebo zastarané.
- Čisto compliance-driven stratégia, charakterizovaná „mentálnym zaškrtávaním políčok“, je nedostatočná na dosiahnutie skutočnej bezpečnostnej odolnosti.
- Tento prístup môže vytvoriť falošný pocit bezpečia, zatiaľ čo v systémoch pretrvávajú významné zraniteľnosti.
- **Ciel'**: Integrovať overovanie súladu (audity) s hodnotením výkonnosti (hodnotenia) pre proaktívny prístup založený na rizikách.

NEVYHNUTNOSŤ AUDITOV (1/2)

- **Identifikácia zraniteľností a rizík:** Pomáhajú určiť aktíva, hrozby a zraniteľnosti, ktoré by útočníci mohli zneužiť.
- **Ochrana citlivých informácií:** Overujú, či sú dáta šifrované, prístup k nim je obmedzený a sú zavedené robustné ochranné postupy.
- **Zabezpečenie súladu s predpismi (Compliance):**
 - Sú nevyhnutné na preukázanie súladu s príslušnými reguláciami.
 - Na Slovensku je kľúčový Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti (ZoKB).
 - Pomáhajú predchádzať vysokým pokutám a poškodeniu reputácie.

NEVYHNUTNOSŤ AUDITOV (2/2)

- **Zabezpečenie kontinuity podnikania (Business Continuity):**
 - Znižujú riziko narušenia obchodných operácií v dôsledku kybernetických incidentov.
 - Minimalizujú prestoje a umožňujú rýchlu obnovu po incidente.
- **Získanie a udržanie dôvery zákazníkov:** Preukazujú proaktívny záväzok k ochrane údajov, čím vzbudzujú dôveru.
- **Podpora neustáleho zlepšovania:** Identifikujú medzery v bezpečnostných rámcoch a oblasti vyžadujúce zlepšenie, čím poskytujú plán pre zvyšovanie celkovej bezpečnosti.

STRATEGICKÝ POHĽAD: BEZPEČNOSŤ AKO FUNKCIA PODNIKANIA

- Kybernetické audity a kontroly nie sú len technické náklady, ale základné piliere celkovej obchodnej stratégie a riadenia.
- Priamo ovplyvňujú hospodársky výsledok tým, že:
 - Predchádzajú nákladným narušeniam.
 - Pomáhajú vyhnúť sa regulačným pokutám.
 - Udržiavajú reputáciu na trhu.
 - Zabezpečujú neprerušované operácie.
- Dochádza k posunu vnímania bezpečnosti z „nákladového centra“ na „strategickú funkciu“ nevyhnutnú pre dlhodobý úspech a odolnosť.

ČO JE TO AUDIT?

- Predstavte si kybernetický audit ako pravidelnú **digitálnu zdravotnú prehliadku**.
- Kontroluje váš počítač, telefón a online účty, aby potvrdil, že sú v bezpečí pred hrozbami ako vírusy alebo hackeri.
- Jeho hlavným cieľom je zaistiť, že vaše osobné informácie sú primerane chránené.
- Keď organizácie (napr. banka) prechádzajú auditom, znamená to uistenie, že služby, ktoré používate, sú pravidelne preverované na slabé miesta.

AUDIT – OSOBNÁ KYBERNETICKÁ HYGIENA

- Základné bezpečnostné kontroly sú pre používateľa "**dobré kybernetické návyky**".
- Tieto jednoduché, každodenné opatrenia sú v podstate **osobnými kontrolnými činnosťami**, ktoré znižujú vaše riziko.
- Príklady osobných kontrolných činností:
 - Používanie silných a jedinečných hesiel (ideálne cez správcu hesiel).
 - Inštalácia a pravidelná aktualizácia antivírusového softvéru.
 - Udržiavanie aktuálneho operačného systému a aplikácií.
 - Overovanie odkazov v e-mailoch pred kliknutím.
 - Používanie viacfaktorovej autentifikácie (MFA).
- Osobná kybernetická bezpečnosť je aktívny a nepretržitý proces.

DEFINÍCIE

- **Kybernetický audit:** Systematické a nezávislé hodnotenie stavu informačnej a kybernetickej bezpečnosti s cieľom identifikovať riziká, posúdiť zraniteľnosti a zabezpečiť súlad s rámcami ako NIST, ISO 27001 a COBIT.
- **Kontrolné činnosti:** Konkrétne politiky, postupy a mechanizmy implementované na presadzovanie riadiacich smerníc a riešenie rizík v IT prostredí.
 - Zahŕňajú autorizácie, overovania, fyzické kontroly, a ďalšie akcie navrhnuté na zabezpečenie kontrolovaného prostredia.

TYPY IT AUDITOV (1/2)

- Administrátori sú priamo ovplyvnení rôznymi typmi IT auditov:
 - **Hodnotenia kybernetickej bezpečnosti:** Posudzujú *účinnosť* kontrol ako sú správa záplat, kontroly prístupu, šifrovanie a plány reakcie na incidenty.
 - **Audity súladu s IT (Compliance):** Overujú, či organizácia spĺňa regulačné požiadavky (napr. GDPR). Administrátori sú zodpovední za technickú implementáciu týchto kontrol.
 - **Audity systémov a aplikácií:** Zameriavajú sa na výkon a bezpečnosť konkrétnych systémov (ERP, CRM). Zahŕňajú predimplementačné a postimplementačné preskúmania.

TYPY IT AUDITOV (2/2)

- **Audity infraštruktúry:** Hodnotia celé IT prostredie vrátane hardvéru, softvéru, sietí a dátových centier z hľadiska konfigurácie, výkonu a škálovateľnosti.
- **Audity obnovy po havárii a kontinuity podnikania (BCDR):** Posudzujú schopnosť organizácie udržať prevádzku počas neočakávaných udalostí a skúmajú postupy zálohovania a obnovy.
- **Prevádzkové audity:** Zameriavajú sa na prevádzkové politiky a postupy, testujú ich primeranosť a dodržiavanie zo strany personálu.

AUDIT A HOLISTICKÝ PRÍSTUP

- Široká škála typov auditov podčiarkuje prepojenú povahu zodpovedností systémového administrátora.
- Úloha administrátora sa neobmedzuje na jeden aspekt bezpečnosti; jeho práca ovplyvňuje viacero domén auditu.
- Je nevyhnutné mať **široké a integrované pochopenie**, ako rôzne IT komponenty prispievajú k celkovej bezpečnosti a súladu.
- To si vyžaduje proaktívne a komplexné bezpečnostné myslenie, kde každá zmena konfigurácie či nasadenie záplaty zohľadňuje potenciálny vplyv na výsledky auditu.

CERTIFIKOVANÝ AUDIT V SR – LEGISLATÍVNY RÁMEC

- Audit kybernetickej bezpečnosti sa na Slovensku riadi príslušnou legislatívou:
 - Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti (ZoKB)
 - Vyhláška č. 493/2022 Z. z. o audite kybernetickej bezpečnosti
 - Vyhláška č. 492/2022 Z. z., ktorou sa ustanovujú znalostné štandardy v oblasti kybernetickej bezpečnosti (definuje požiadavky na audítora)
- Audit u prevádzkovateľa základnej služby (PZS) môže vykonávať iba **certifikovaný audítor** kybernetickej bezpečnosti.

CIELE CERTIFIKOVANÉHO AUDITU V SR

- Hlavným cieľom auditu kybernetickej bezpečnosti je:
 - Overenie aktuálneho **stavu kybernetickej bezpečnosti** v organizácii.
 - Určenie **miery zhody** systémov s požiadavkami zákona a vyhlášok.
 - Monitorovanie **účinnosti prijatých bezpečnostných opatrení**.
 - Vyhodnotenie **aktuálnosti bezpečnostnej dokumentácie**.

POVINNOSTI PREVÁDZKOVATEĽA ZÁKLADNEJ SLUŽBY (PZS)

- PZS je povinný vykonať audit kybernetickej bezpečnosti v rozsahu stanovenom vyhláškou, v závislosti od klasifikácie informácií a kategorizácie systémov.
- **Frekvencia auditu:**
 - **Do 2 rokov** od zaradenia do registra PZS.
 - Následne pravidelne **každé 2 roky**.
 - Pri každej **zmene majúcej významný vplyv** na bezpečnostné opatrenia.

ZMENA S VÝZNAMNÝM VPLYVOM

- Zmenou s významným vplyvom, ktorá si vyžaduje vykonanie auditu, je najmä:
 - Zmena **kategórie sietí a informačných systémov** základnej služby.
 - Prekročenie **dopadových kritérií** základnej služby.
 - Zmena **parametrov** základnej služby.
 - **Nasadenie, zmena alebo vyradenie** kľúčového informačného systému alebo technológie, od ktorej závisí poskytovanie základnej služby.

PROCES PO AUDITE

- 1. Závěrečná správa:** Auditovaná organizácia je povinná do 30 dní od ukončenia auditu predložiť Národnému bezpečnostnému úradu (NBÚ) závěrečnú správu.
- 2. Opatrenia na nápravu:** Správa musí obsahovať aj navrhnuté opatrenia a lehoty na ich odstránenie.
- 3. Akčný plán:** Jednotlivé opatrenia sa musia premietnuť do **Akčného plánu kybernetickej bezpečnosti**.
- 4. Dohľad:** Plnenie akčného plánu sa pravidelne (najmenej polročne) predkladá **Bezpečnostnému výboru**.

STRATEGICKÝ DOHLAD A RIADENIE RIZÍK

- Audity sú kritickou súčasťou rámca kybernetického riadenia (Governance) a strategického riadenia rizík.
- **Hodnotenie rizík** je kľúčové pre presun kybernetickej bezpečnosti z technického sila do oblasti obchodného riadenia.
- Umožňuje vedeniu robiť informované rozhodnutia o kompromisoch medzi silou kontrol, agilitou a toleranciou rizika.
- Zrelý proces hodnotenia rizík identifikuje a prioritizuje riziká na základe ich pravdepodobnosti, potenciálneho dopadu a aktuálnych informácií o hrozbách.

POKROČILÉ METODIKY – PENETRAČNÉ TESTOVANIE

- Tieto metódy simulujú útoky v reálnom svete a poskytujú hlbší pohľad na skutočný bezpečnostný stav organizácie.
- **Penetračné testovanie (Pentesting):** Autorizovaný a kontrolovaný pokus o nájdenie a zneužitie zraniteľností v systémoch, sieťach a aplikáciách.
- **Typy podľa úrovne znalostí:**
 - **Black Box:** Bez predchádzajúcich znalostí (perspektíva externého útočníka).
 - **White Box:** S úplnými znalosťami (simulácia vnútornej hrozby).
 - **Grey Box:** S čiastočnými znalosťami (kombinácia oboch prístupov).

POKROČILÉ METODIKY – CIELE PENETRAČNÉHO TESTOVANIA

- **Testovanie siete:** Hodnotenie bezpečnosti firewallov, smerovačov, serverov a pracovných staníc.
- **Testovanie webových aplikácií:** Identifikácia zraniteľností špecifických pre webové technológie (napr. OWASP Top 10).
- **Testovanie API:** Zameranie na bezpečnostné zraniteľnosti v programovacích rozhraniach aplikácií.
- **Testovanie cloudu (IaaS, PaaS, SaaS):** Hodnotenie bezpečnosti cloudovej infraštruktúry a aplikácií.
- **Testovanie IoT:** Posúdenie bezpečnosti pripojených zariadení a ich interakcií.

POKROČILÉ METODIKY – SOCIÁLNE INŽINIERSTVO

- Testovanie sociálneho inžinierstva kontroluje **útočnú plochu založenú na ľudskom faktore**.
 - Zahŕňa simuláciu útokov ako **phishing** alebo **pretexting**.
 - **Cieľ**: Trénovať zamestnancov, aby rozpoznali a odolali pokusom o manipuláciu, ktorých cieľom je odhalenie citlivých informácií.
 - Tento prístup uznáva, že „**ľudský firewall**“ je rovnako **kritický** ako ten technický a že najslabším článkom často nie je technická chyba, ale **človek**.
-

OSVEDČENÉ POSTUPY – BEŽNÉ CHYBY A ÚSKALIA (1/2)

- **Podcenenie rozsahu a zdrojov:** Považovať audit za rýchle "zaškrtnutie políčok" vedie k neúplným informáciám a stresu.
- **Nedostatočná dokumentácia a dôkazy:** Chýbajúce, nejasné alebo neaktuálne politiky a záznamy sú istou cestou k zisteniam auditu.
- **Nedostatok komunikácie a spolupráce:** Zlá komunikácia medzi oddeleniami a audítormi vedie k nedorozumeniam a oneskoreniam.

OSVEDČENÉ POSTUPY – BEŽNÉ CHYBY A ÚSKALIA (2/2)

- **Zanedbávanie preauditových hodnotení:** Čakať na oficiálny audit, aby sa objavili slabé miesta, je recept na neúspech. Predauditové hodnotenia sú kľúčové.
- **Zameranie sa výlučne na súlad:** Prílišný dôraz na "zaškrtávanie políčok" bez skutočného zlepšenia bezpečnosti je nebezpečné.

Súlad sa nerovná bezpečnosť.

- **Nové výzvy:**
 - Zvýšená zložitosť (ransomvér, dodávateľský reťazec).
 - Obmedzené zdroje (finančné, ľudské).
 - Regulačný tlak.
-

KLÚČOVÉ PRINCÍPY BEZPEČNOSTI

- **Princíp najnižších oprávnení (PoLP):** Každý používateľ alebo systém má len také práva, ktoré sú nevyhnutne potrebné na výkon jeho úloh.
- **Princíp oddelenia právomocí (SoD):** Žiadna osoba nemá úplnú kontrolu nad všetkými fázami kritického procesu, čím sa minimalizuje riziko zneužitia a chýb.
- **Princíp vylúčenia konfliktu záujmov:** Osoba vykonávajúca audit alebo kontrolu nemôže kontrolovať samú seba alebo činnosti, ktoré sama vykonáva.

KLÚČOVÉ DEFINÍCIE (VÝBER)

- **Interný audit:** Vykonávaný samotnou organizáciou alebo v jej mene (audit prvou stranou).
- **Externý audit:** Vykonávaný stranami so záujmom v organizácii (zákazníci - audit druhou stranou) alebo nezávislými organizáciami (certifikácie - audit treťou stranou).
- **CIA triáda:** Základné piliere informačnej bezpečnosti – Dôvernosť, Integrita, Dostupnosť (Confidentiality, Integrity, Availability).
- **PZS (Prevádzkovateľ základnej služby):** Subjekt kľúčový pre fungovanie štátu, definovaný Zákonom o kybernetickej bezpečnosti.

ZHRNUTIE

- Vaše každodenné digitálne návyky sú v skutočnosti **osobnými kontrolnými činnosťami**.
- Aktívna účasť na dobrej kybernetickej hygiene je nevyhnutná pre vašu osobnú ochranu a prispieva k celkovej bezpečnosti organizácie.
- **Kľúčové akcie:** Silné heslá, viacfaktorová autentifikácia, opatrnosť pri e-mailoch a pravidelné aktualizácie.

ZHRNUTIE

- IT administrátor a MKB sú prvej línii implementácie a riadenia bezpečnostných kontrol.
- Úloha MKB presahuje technické úlohy a vyžaduje si strategické pochopenie rôznych typov auditov.
- **Kľúčové akcie:**
 - Dôsledné uplatňovanie princípu najmenších oprávnení (PoLP).
 - Komplexné posilnenie systémov (hardening).
 - Efektívna správa logov a riadenie zraniteľností.
 - Prechod k automatizovaným a nepretržitým bezpečnostným procesom.

ZHRNUTIE

- Audity a kontroly sú strategickým imperatívom zameraným na **obchodný dopad a riadenie rizík**.
- Je nevyhnutné využívať pokročilé metodiky na odhalenie sofistikovaných zraniteľností.
- **Kľúčové akcie:**
 - Rozsiahle penetračné testovanie a testovanie sociálneho inžinierstva.
 - Navrhovanie a hodnotenie robustných kontrolných rámcov (NIST CSF, ISO 27001).
 - Využívanie kvantitatívnych metodík riadenia rizík (napr. FAIR, OCTAVE).

ZÁVEREČNÉ MYŠLIENKY

- Úspešná implementácia auditov a kontrol si vyžaduje **holistický a nepretržitý prístup**.
- Organizácie musia prekonať mentalitu „zaškrtávaní políčok“ a prijať filozofiu **skutočného zlepšovania bezpečnosti**.
- To si vyžaduje proaktívne plánovanie, dostatočné zdroje, jasnú komunikáciu a nepretržité vzdelávanie.
- Integrácia kybernetickej bezpečnosti do základnej obchodnej stratégie je nevyhnutná pre budovanie odolného a dôveryhodného digitálneho prostredia.

STRATEGICKÁ INVESTÍCIA

Pravidelné audity a robustné kontrolné činnosti nie sú len nákladom, ale **strategickou investíciou**, ktorá:

- Chráni kritické aktíva.
- Zabezpečuje súlad s legislatívou.
- Udržiava dôveru zákazníkov.
- Zabezpečuje kontinuitu podnikania v neustále sa vyvíjajúcom prostredí kybernetických hrozieb.

ĎAKUJEM ZA POZORNOST

- Otázky a odpověde