



Kompetenčné
a certifikačné
centrum
kybernetickej
bezpečnosti

PRÁVNE POŽIADAVKY NA CLOUD, V KONTEXTE KYBERNETICKEJ BEZPEČNOSTI

Virtuálna konferencia Kybernetická bezpečnosť a cloudové služby

28. 5. 2021, Ivan Makatura



AGENDA

- Cloud computing z pohľadu bezpečnosti
- Požiadavky právnych predpisov na bezpečnostné opatrenia pre cloud
- Požiadavky technických noriem na bezpečnostné opatrenia pre cloud
- Certifikačná schéma na posudzovanie cloudových riešení



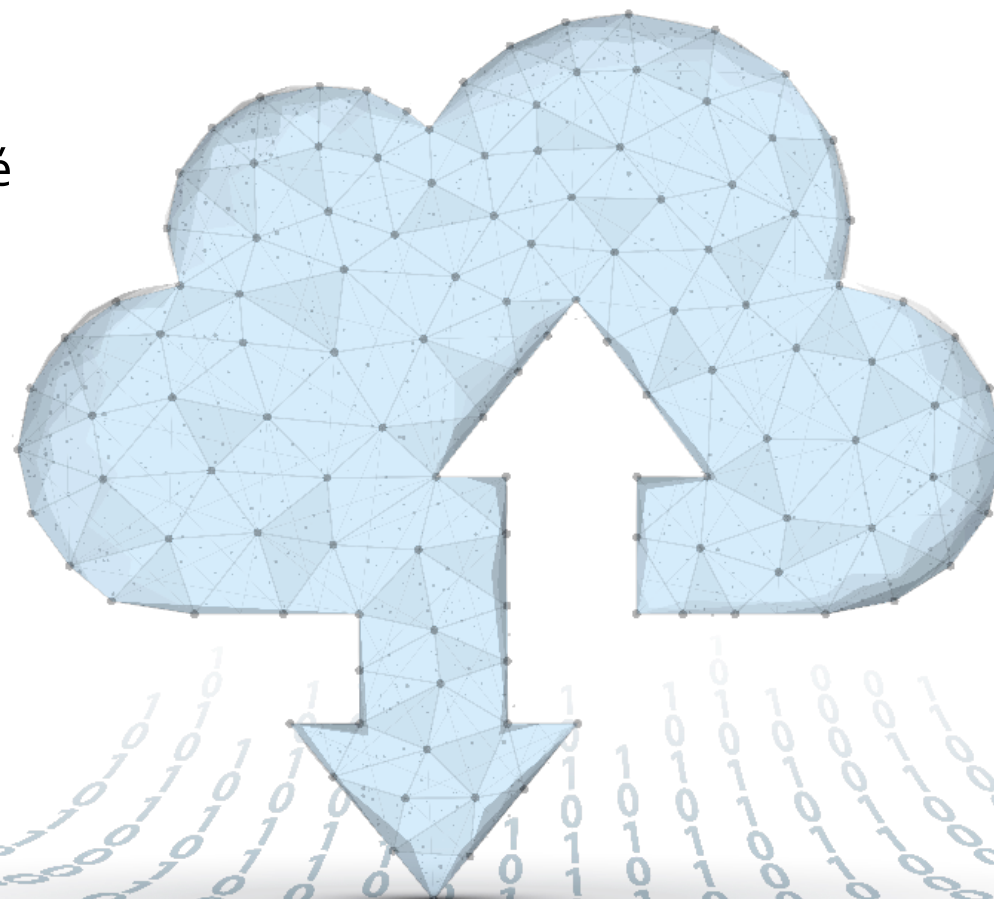
Cloud computing z pohľadu bezpečnosti

PRÁVNE POŽIADAVKY NA CLOUD, V KONTEXTE KYBERNETICKEJ BEZPEČNOSTI



CLOUD COMPUTING

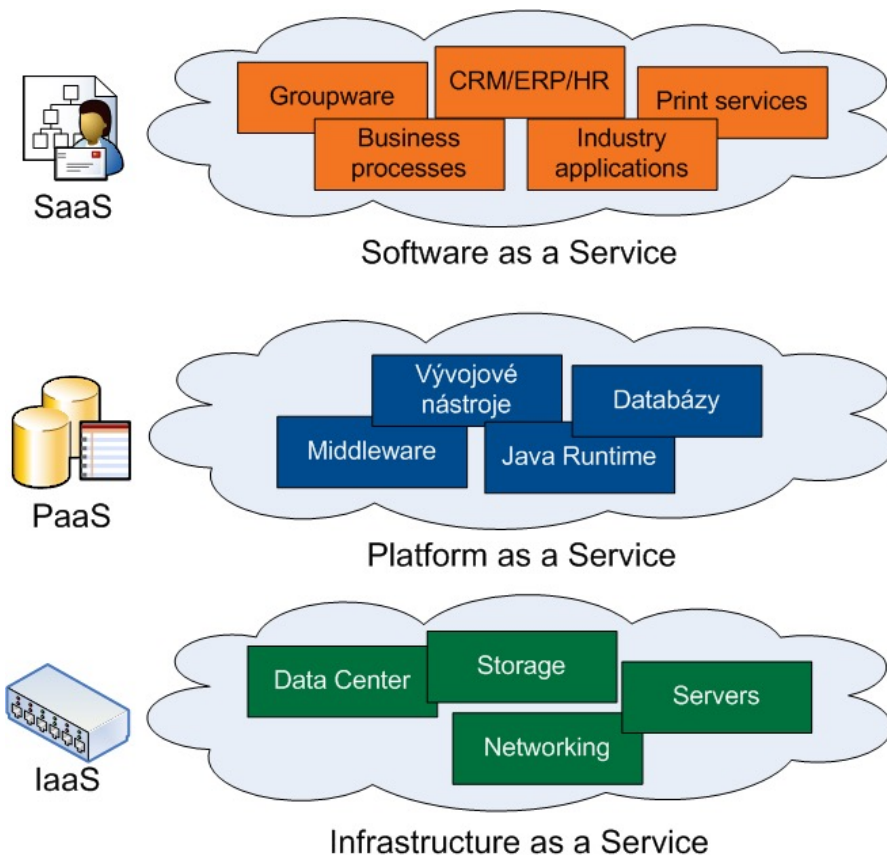
- Architektonický model, ktorý umožňuje prístup na požiadanie k zdieľanému fondu konfigurovateľných výpočtových zdrojov ktoré je možné efektívne poskytnúť s minimálnym úsilím na riadenie, alebo interakciu s poskytovateľom služieb (**Zdroj: NIST**)
- **Poskytovanie výpočtového výkonu prostredníctvom služieb tretej strany cez verejné počítačové siete**





CHARAKTERISTICKÉ ČRTY CC

- Virtualizácia infraštruktúry, geografická nezávislosť
- Zdieľanie technických prostriedkov viacerými „nájomníkmi“ (**multi tenancy** - poskytovateľ obsluhuje viacero klientov)
- Samoobslužnosť (**self service** - klient si objednáva služby cez samoobslužné rozhranie)
- Služby na požiadanie (**on demand** - klient sám iniciuje zapnutie/vypnutie služby; vyššia dynamika zmien infraštruktúry)
- Oddeľovanie údajov (**data segregation** - zabezpečenie, že dáta sú izolované od dát ostatných zákazníkov)
- Vzdialený prístup používateľov, vzdialená administrácia
- Zásobník zdrojov (**resource pooling** - dynamické pridelenie aktív)
- Prispôsobiteľnosť (**rapid elasticity** - možnosť rýchlo sa prispôbiť požiadavkám)
- Meranie spotreby (**metering** – účtovanie len skutočne využitých služieb)
- Vyššie požiadavky na robustnosť, stabilitu a redundanciu komunikačných kanálov





TOP 7 HROZIEB CC PODĽA CLOUD SECURITY ALLIANCE

#1: Zlomyseľné používanie Cloud Computingu

- Použitie CC ako botnetov; Použitie CC na šírenie exploitov a malware; CC ako spamové a phishingové domény; použitie CC pre DDoS; „CAPTCHA solving“ farmy; atď.

#2: Nezabezpečené rozhrania

- Nevhodne navrhnuté rozhrania pre interakciu s CC (napr. nedostatočná šifrová ochrana, nedostatočná autentizácia a anonymný prístup ku zdrojom, nedostatočné možnosti logovania a monitorovania, atď.)

#3: Zlomyseľní interní používatelia

- Nedostatočná ochrana pred zneužitím CC zo strany interných zamestnancov poskytovateľa CC; atraktívna príležitosť pre zneužitie CC (napr. zvedavosť, hobby hacking, priemyselná špionáž, sabotáž, získanie kontroly nad službami, atď.)

#4: Problémy zdieľanej technológie

- Možné obmedzenia súvisiace s nedostatočným odhadom zdrojov a zlým kapacitným plánovaním v infraštruktúrnom prostredí, ktoré je zdieľané viacerými zákazníkmi; neexistujúce SLA; nevhodný alebo neexistujúci change management, atď.



TOP 7 HROZIEB CC PODĽA CLOUD SECURITY ALLIANCE

#5: Strata alebo odcudzenie informácií

- Nedostatočná autentizácia alebo autorizácia; zlé použitie šifrovacích metód; strata šifrovacích kľúčov; strata informácií pri vymazávaní; chyby v referenčnej integrite; nedostatočné postupy pre havarijnú obnovu dát; neexistujúca retenčná stratégia, atď.

#6: Odcudzenie identít alebo kompromitácia služieb

- Zdieľanie identít; neexistujúca viacfaktorová autentizácia; nevhodné procesy vzdialeného prístupu; možné úmyselné presmerovanie zdrojov; sniffing dát; atď.

#7: Nejasný rizikový profil

- Neschválené alebo unáhlené zmeny infraštruktúry CC odôvodňované požiadavkami biznisu; nedostatočný verzioning; pozabudnutý, alebo potlačený patch management; postupné zníženie pozornosti a benevolencia v bezpečnostných procesoch; chýbajúci incident manažment, atď.



Požiadavky právnych predpisov na bezpečnostné opatrenia pre cloud

PRÁVNE POŽIADAVKY NA CLOUD, V KONTEXTE KYBERNETICKEJ BEZPEČNOSTI



EURÓPSKA PRÁVNÁ ÚPRAVA



- Smernica (EÚ) 2016/1148 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii (**NIS**)
 - ➡ Zákon č. 69/2018 Z.z. o kybernetickej bezpečnosti
- Nariadenie (EÚ) 2019/881 o agentúre ENISA (Agentúra Európskej únie pre kybernetickú bezpečnosť) a o certifikácii kybernetickej bezpečnosti informačných a komunikačných technológií (**CyberAct**)
- Nariadenie (EÚ) 2016/679 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov; všeobecné nariadenie o ochrane údajov (**GDPR**)
 - ➡ Zákon č. 18/2018 Z.z. o ochrane osobných údajov



NÁRODNÁ PRÁVNÁ ÚPRAVA



- Zákon č. **69/2018** Z.z. o kybernetickej bezpečnosti
 - Vyhláška NBÚ č. **164/2018** Z.z., ktorou sa určujú identifikačné kritériá prevádzkovanvej služby (kritériá základnej služby)
 - Vyhláška NBÚ č. **165/2018** Z.z., ktorou sa určujú identifikačné kritériá pre jednotlivé kategórie závažných kybernetických bezpečnostných incidentov a podrobnosti hlásenia kybernetických bezpečnostných incidentov
 - Vyhláška NBÚ č. **362/2018** Z.z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení
 - Vyhláška NBÚ č. **436/2019** Z.z. o audite kybernetickej bezpečnosti a znalostnom štandarde audítora
- Zákon č. **95/2019** Z.z. o informačných technológiách vo verejnej správe
 - Vyhláška ÚPVII č. **179/2020** Z.z., ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy



ROZSAH BEZPEČNOSTNÝCH OPATRENÍ PODĽA VYHLÁŠKY Č. 362/2018 Z.Z.

Bezpečnostné opatrenie podľa § 20 ods. 3 zákona	Kategória I	Kategória II	Kategória III
a) Organizácia informačnej bezpečnosti	Odporúčané	Odporúčané	Povinné
b) Riadenie aktív, hrozieb a rizík	Odporúčané	Povinné	Povinné
c) Personálna bezpečnosť	Odporúčané	Povinné	Povinné
d) Riadenie dodávateľských služieb, akvizície, vývoja, údržby IS	Odporúčané	Povinné	Povinné
e) Riadenie technických zraniteľností systémov a zariadení	Odporúčané	Povinné	Povinné
f) Riadenie bezpečnosti sietí a informačných systémov	Odporúčané	Povinné	Povinné
g) Riadenie prevádzky	Odporúčané	Povinné	Povinné
h) Riadenie prístupov	Odporúčané	Povinné	Povinné
i) Kryptografické opatrenia	Odporúčané	Odporúčané	Povinné
j) Riešenie kybernetických bezpečnostných incidentov	Povinné	Povinné	Povinné
k) Monitorovanie, testovanie bezpečnosti, bezpečnostné audity	Odporúčané	Povinné	Povinné
l) Fyzickej bezpečnosti a bezpečnosti prostredia	Odporúčané	Odporúčané	Povinné
m) Riadenia kontinuity procesov	Odporúčané	Povinné	Povinné

Príloha č. 3 k vyhláške č. 362/2018 Z. z. vo verzii predpisu účinná od 01.21.2019



KATEGORIZÁCIA BEZPEČNOSTNÝCH OPATRENÍ PRE ITVS

Vyhláška č. 179/2020 Z.z. ÚPVII ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy:

§ 2 Bezpečnostné opatrenia

- 1.** Bezpečnostné opatrenia informačných technológií verejnej správy tvoria **minimálne bezpečnostné opatrenia troch kategórií** pre jednotlivé oblasti podľa prílohy č. 2.
- 2.** Pri duplicite alebo nekompatibilite minimálnych bezpečnostných opatrení rôznych kategórií, ktoré môžu byť aplikované na konkrétne informačné technológie verejnej správy, majú prednosť ustanovenia upravujúce opatrenia vyššej kategórie.
- 3.** Ak sa aplikuje bezpečnostné opatrenie aj podľa osobitného predpisu, aplikuje sa bezpečnostné opatrenie podľa zákona, **ak jeho cieľom je dosiahnuť vyššiu úroveň bezpečnosti** sietí a informačných systémov ako podľa osobitného predpisu.





APLIKÁCIA POVINNOSTÍ NA SAMOSPRÁVU

Obec, ktorá
je aj krajským
mestom,

Samosprávny
kraj

- Vzťahujú sa na ňu minimálne bezpečnostné opatrenia Kategórie I a Kategórie II a a Kategórie III
- Ako PZS implementuje bezpečnostné opatrenia podľa zákona č. 69/2018 Z.z.

Obec nad
6000
obyvateľov,

- Vzťahujú sa na ňu minimálne bezpečnostné opatrenia Kategórie I a Kategórie II
- Ako PZS implementuje bezpečnostné opatrenia podľa zákona č. 69/2018 Z.z.

Obec so
štatútom
mesta nad
6000
obyvateľov
okrem
krajských
miest,

Mestská časť
s právnou
subjektivitou

Obec do
6000
obyvateľov,

- Vzťahujú sa na ňu minimálne bezpečnostné opatrenia Kategórie I
- Ako PZS implementuje bezpečnostné opatrenia podľa zákona č. 69/2018 Z.z.

Obec so
štatútom
mesta do
6000
obyvateľov

Obec
do 1000
obyvateľov

- Vzťahujú sa na ňu minimálne bezpečnostné opatrenia Kategórie I
- alebo implementuje bezpečnostné opatrenia podľa zákona č. 69/2018 Z.z. ak ich cieľom je dosiahnuť vyššiu úroveň bezpečnosti



Požiadavky technických noriem na bezpečnostné opatrenia pre cloud

PRÁVNE POŽIADAVKY NA CLOUD, V KONTEXTE KYBERNETICKEJ BEZPEČNOSTI



STN EN ISO/IEC 27002:2013

Informačné technológie - Bezpečnostné metódy - Pravidlá dobrej praxe riadenia informačnej bezpečnosti

A.05 Politiky informačnej bezpečnosti	A.06 Organizácia informačnej bezpečnosti	A.07 Personálna bezpečnosť
A.08 Riadenie aktív	A.09 Riadenie prístupov	A.10 Šifrovanie, kryptografia
A.11 Fyzická bezpečnosť a bezpečnosť prostredia	A.12 Prevádzková bezpečnosť	A.13 Komunikačná bezpečnosť
A.14 Akvizícia, vývoj a údržba informačných systémov	A.15 Riadenie vzťahov s dodávateľmi	A.16 Riešenie incidentov informačnej bezpečnosti
A.17 Riadenie kontinuity	A.18 Riadenie súladu	

- súbor pravidiel dobrej praxe informačnej bezpečnosti vrátane výberu, implementácie a riadenia, berúc do úvahy úroveň identifikovaného rizika v organizácii
- Norma obsahuje **113 bezpečnostných opatrení** rozdelených do **14 oblastí**
- Strategické výhody systému riadenia informačnej bezpečnosti podľa ISO 27x (ISMS):
 - ISO/IEC 27001 je celosvetovo uznávaný rámec pre najlepšie skúsenosti z praxe informačnej bezpečnosti
 - Holistický a previazaný prístup integrujúci „end to end“ služby informačnej bezpečnosti
 - Poskytuje jednotnú terminológiu
 - Dodáva procesný model pre zosúladenie a následné zlepšovanie služieb



ISO/IEC 27017:2015

Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services

- súbor pravidiel dobrej praxe, ktorý poskytuje **dodatočné odporúčania** na implementáciu bezpečnostných opatrení **nad rámec opatrení uvedených v ISO/IEC 27002**, v kontexte cloudových služieb
- Odporúča **zmenu pre 37 opatrení** uvedených v ISO/IEC 27002 a **7 nových špecifických opatrení**, ktoré nie sú uvedené v ISO/IEC 27002:
 1. Zdieľané roly a zodpovednosti v prostredí cloudového prostredia
 2. Odstránenie a vrátenie aktív zákazníka cloudovej služby po ukončení zmluvy
 3. Ochrana a oddelenie virtuálneho prostredia zákazníka od prostredia ostatných zákazníkov
 4. Požiadavky na hardening virtuálnych strojov
 5. Postupy pre správčovské činnosti v cloudovom prostredí
 6. Umožnenie zákazníkovi monitorovať príslušné aktivity v prostredí cloudového prostredia
 7. Zosúladenie riadenia bezpečnosti pre virtuálne a fyzické siete
- Norma nie je prevzatá do sústavy STN!



STN EN ISO/IEC 27018:2019

Informačné technológie - Bezpečnostné metódy - Súbor postupov na ochranu osobných údajov (OÚ) pre verejné cloudy v pozícii spracovateľov OÚ

- súbor pravidiel dobrej praxe, ktorý poskytuje dodatočné odporúčania na implementáciu bezpečnostných opatrení **na ochranu osobných údajov** v súlade s princípmi ochrany súkromia, **v kontexte verejných cloudových služieb**
- Kľúčové princípy v STN EN ISO/IEC 27018:2019:
 - „Informácie identifikovateľné ako osobné“ (Personally Identifiable Information) namiesto „osobné údaje“
 - Poskytovateľ cloudových služieb je chápaný ako sprostredkovateľ
- **36 špecifických opatrení**, ktoré nie sú uvedené v ISO/IEC 27002 je **odporúčaných v 12 oblastiach**:

1. Politiky informačnej bezpečnosti	8. Komunikačná bezpečnosť
2. Organizácia informačnej bezpečnosti	9. Akvizícia, vývoj a údržba informačných systémov
3. Personálna bezpečnosť	10. Riadenie vzťahov s dodávateľmi
4. Riadenie aktív	11. Riadenie kontinuity
5. Šifrovanie, kryptografia	12. Riadenie súladu
6. Fyzická bezpečnosť a bezpečnosť prostredia	
7. Prevádzková bezpečnosť	



CERTIFIKÁCIA NIE JE BEZPEČNOSTNÉ OPATRENIE

- Na základe zákona č. 264/1999 Z.z. o technických požiadavkách na výrobky a o posudzovaní zhody slovenské technické normy prestali byť od 1.1.2001 záväzné
- Všetky prezentované technické normy sú tzv. návodové normy (guidelines) týkajúce sa bezpečnostných opatrení:



- **STN EN ISO/IEC 27002:2013** Informačné technológie - Bezpečnostné metódy - Pravidlá dobrej praxe riadenia informačnej bezpečnosti



- **ISO/IEC 27017:2015** Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services



- **STN EN ISO/IEC 27018:2019** Informačné technológie - Bezpečnostné metódy - Súbor postupov na ochranu osobných údajov (OÚ) pre verejné cloudy v pozícii spracovateľov OÚ

**Ani jedna z vyššie uvedených technických noriem
nie je certifikačnou normou!**



Overovanie úrovne kybernetickej bezpečnosti

PRÁVNE POŽIADAVKY NA CLOUD, V KONTEXTE KYBERNETICKEJ BEZPEČNOSTI



VŠEOBECNÝ ÚČEL OVEROVANIA ÚROVNE BEZPEČNOSTI

Získať objektívnu informáciu o stave ochrany informácií, najmä:

- Zhodnotiť súlad aktuálneho stavu kybernetickej bezpečnosti so stanovenými bezpečnostnými cieľmi
- Posúdiť:
 - Zhodu prijatých opatrení so stanoveným rozsahom opatrení
 - Účinnosť implementovaných bezpečnostných opatrení
 - Bezpečnostnú architektúru (napr. tzv. „security by design“)
 - Bezpečnosť aplikácií (napr. tzv. „data protection by default“)
 - Vyspelosť procesu riadenia bezpečnosti
- Identifikovať zraniteľnosti a hrozby
- Stanoviť úrovne rizík
- Atestovať spôsobilosti organizácie v oblasti kybernetickej bezpečnosti



METÓDY OVEROVANIA ÚROVNE BEZPEČNOSTI

- Overované entity a prvky sú v procese overovania úrovne bezpečnosti všeobecne nazývané ako „**objekty posúdenia**“ (z angl. „assessment objects“)
- Štyri základné prístupy ako sa môže subjekt uistiť o požadovanej úrovni KB:

1. Posúdenie



2. Testovanie



3. Audit



4. Certifikácia (Posudzovanie zhody)



Pre ostatné tri prístupy je zásadné, aby existovala **formálna špecifikácia**

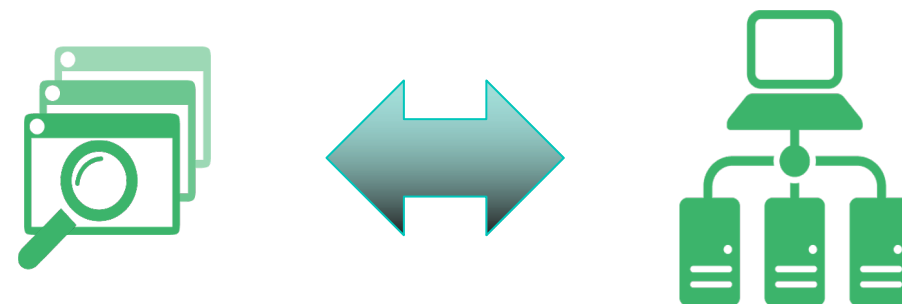


POSUDZOVANIE BEZPEČNOSTI

Dokazovanie, že sa splnili určené požiadavky týkajúce sa objektu posudzovania

Typické metódy:

- Analýza rizík
- Rozdielová analýza
- Analýza súladu
- Analýza funkčných dopadov (BIA)
- Porovnávanie v rámci odvetvia (benchmarking)
- Prieskum



Primárny účel:

- Poskytnúť ucelenú informáciu o stave KB a rizikách KB formou technickej správy
- Použiť konsolidované výstupy na sledovanie trendu (napr. KRI/KPI)

Pre posudzovanie je typické, že môže byť vykonané vlastným hodnotením



TESTOVANIE BEZPEČNOSTI

Proces, v ktorom je jeden alebo viac objektov posudzovania vystavených podľa opakovateľného postupu určitým podmienkam, s cieľom porovnať ich aktuálne a očakávané charakteristiky

Typické metódy:

- Detekcia zraniteľností, scannovanie zraniteľností
- Penetračné testovanie
- Revízia softvérového kódu (code review)
- Integračné testovanie
- Výkonnostné testovanie (performance test)

Primárny účel:

- Získanie informácií o charakteristikách objektov v kontexte KB



Pre testovanie je typická požiadavka na vysokú mieru zručnosti

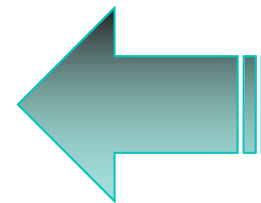


AUDIT BEZPEČNOSTI

Systematický, nezávislý a zdokumentovaný proces získavania záznamov, konštatovaní faktov alebo iných dôležitých informácií a ich objektívneho posudzovania s cieľom určiť rozsah, v akom sa splnili určené požiadavky

Typické metódy:

- Auditné rozhovory a dotazníky
- Porovnávanie deklarovaneho a skutkového stavu
- Preskúmanie zdokumentovaných informácií
- Vzorkovanie (vykonáva sa, ak nie je praktické alebo efektívne preverenie všetkých dostupných informácií v priebehu auditu)



Primárny účel:

- Získanie informácie o nezhodách a rizikách formou konsolidovanej správy
- Iniciácia návrhov na zmenu jestvujúcich resp. Implementáciu ďalších bezpečnostných opatrení

Pre audit je typická požiadavka na nestrannosť

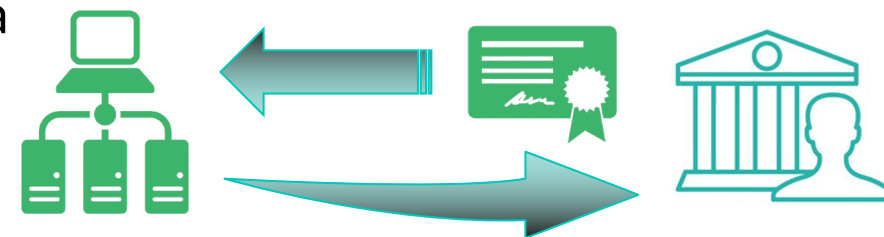


CERTIFIKÁCIA BEZPEČNOSTI

Atestácia nezávislým akreditovaným orgánom posudzovania zhody, týkajúca sa charakteristík objektu posudzovania

Typický proces:

1. **Žiadosť** o posúdenie zhody
2. **Vyhodnotenie** (overenie, že objekt spĺňa kvalifikačné kritériá)
3. **Atestácia** (rozhodnutie o splnení kvalifikačných kritérií)
4. **Dohľad** (priebežné posudzovanie, že objekt naďalej spĺňa kritériá)



Primárny účel:

- Deklarácia primeranej úrovne kybernetickej bezpečnosti výrobkov, služieb a procesov
- Posilnenie transparentnosti posudzovania a dôvery v bezpečnosť výrobkov, služieb a procesov

Pre certifikáciu je typická požiadavka na akreditáciu a dohľad



POROVNANIE METÓD OVEROVANIA ÚROVNE BEZPEČNOSTI

Metóda	Určený nástroj	Opakovateľný postup	Formálna špecifikácia	Nestrannosť	Dôkazy	Certifikovaná osoba	Akreditácia	Dohľad
Posudzovanie	✗	✗	✗	✗	✗	✗	✗	✗
Testovanie	✓	✓	✓	✗	✗	✗	✗	✗
Audit	✓	✓	✓	✓	✓	✓	✗	✗
Certifikácia	✓	✓	✓	✓	✓	✓	✓	✓



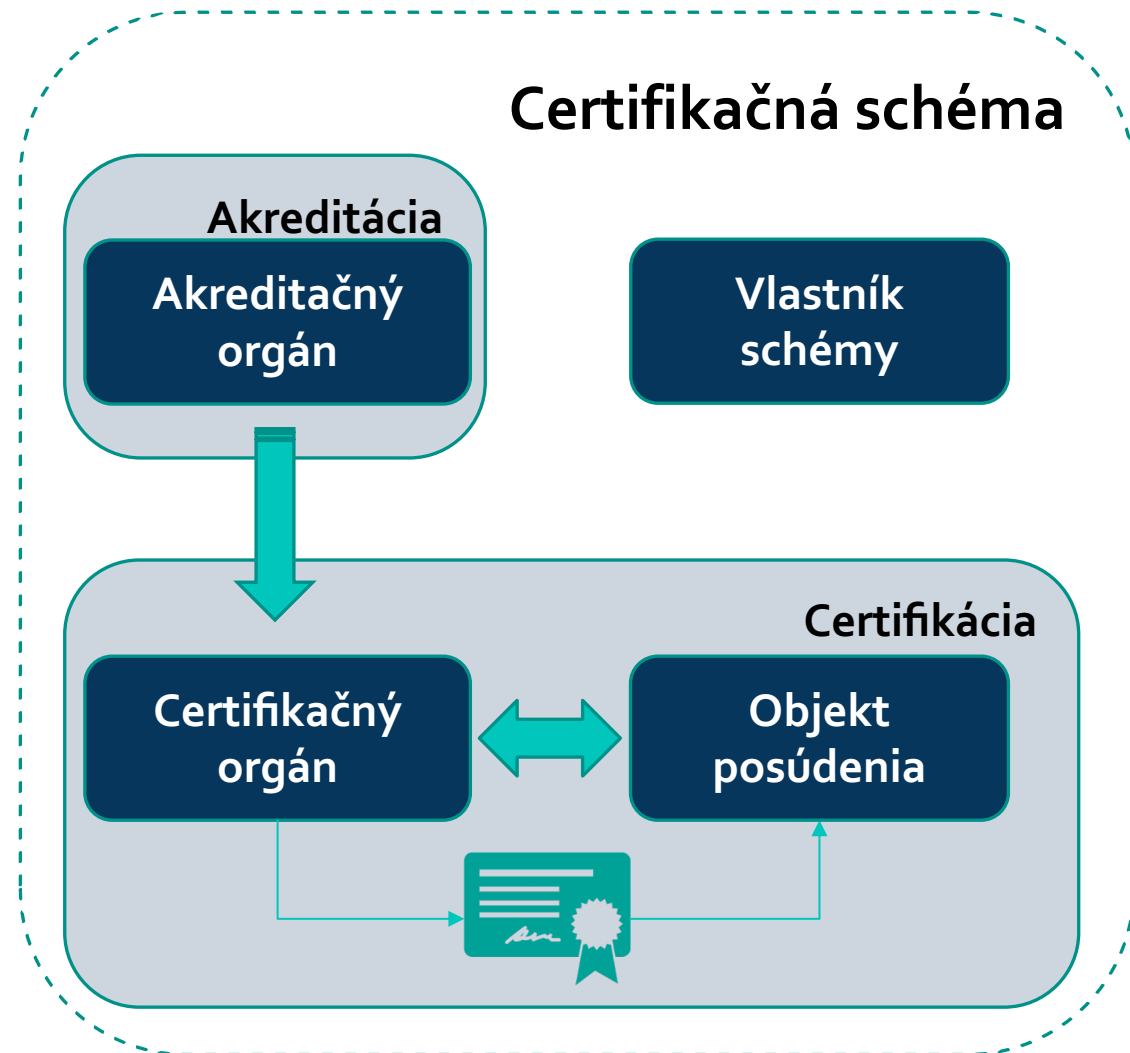
Certifikačná schéma na posudzovanie cloudových riešení

PRÁVNE POŽIADAVKY NA CLOUD, V KONTEXTE KYBERNETICKEJ BEZPEČNOSTI



PROCES AKREDITÁCIE PRE POSUDZOVANIE ZHODY

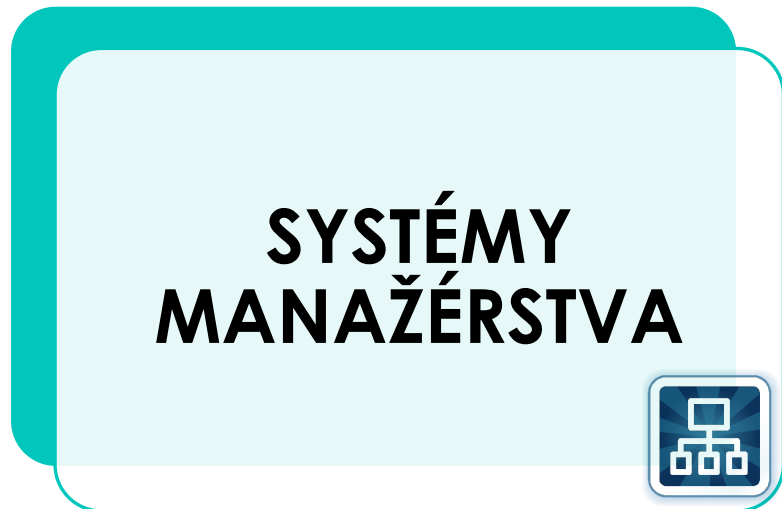
- **Certifikačná schéma:** systém certifikácie, ktorý sa vzťahuje na určené produkty, na ktoré sa aplikujú rovnaké určené požiadavky, osobitné pravidlá a postupy.
(ISO/IEC 17065: 2012, čl. 3.9)
- **Akreditačný orgán:** autoritatívny orgán, ktorý vykonáva akreditáciu. (V Slovenskej republike je vnútroštátnym akreditačným orgánom Slovenská národná akreditačná služba - SNAS. Postavenie SNAS a jej pôsobnosť určuje zákon č. 505/2009 Z. z. o akreditácii orgánov posudzovania zhody)
(STN EN ISO/IEC 17000: 2005, čl. 2.6)
- **Certifikačný orgán:** orgán vykonávajúci posudzovanie zhody treťou stranou podľa certifikačnej schémy
(ISO/IEC 17065: 2012, čl. 3.12)
- **Certifikácia:** atestácia treťou stranou týkajúca sa produktov, procesov, systémov alebo osôb.
(STN EN ISO/IEC 17000: 2005, čl. 5.5)



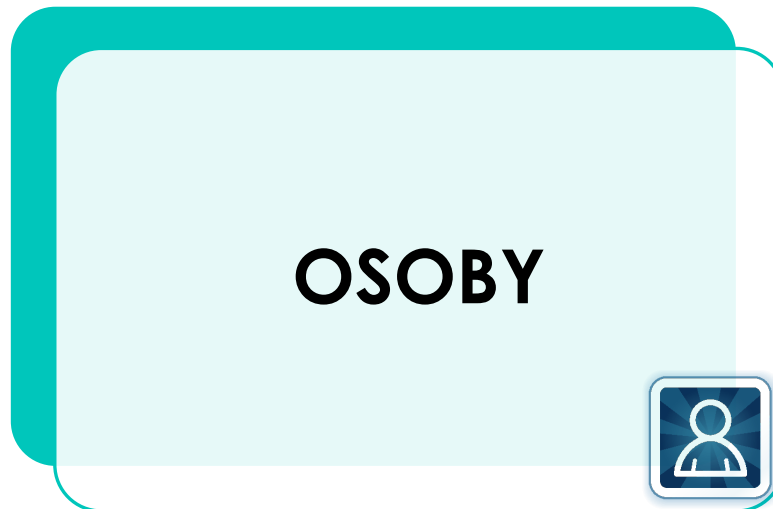


OBJEKTY POSUDZOVANIA ZHODY V OBLASTI BEZPEČNOSTI

(ISO/IEC 17021-1: 2015)



(ISO/IEC 17024: 2012)



(ISO/IEC 17065: 2012)

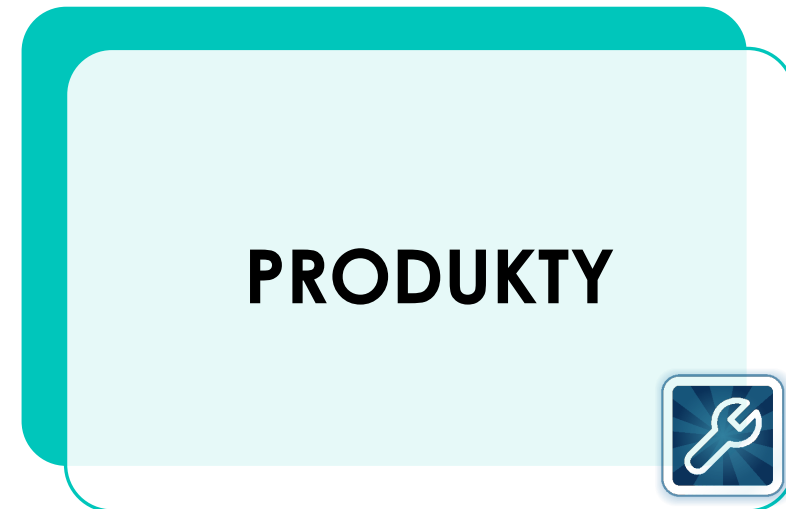


Schéma podľa Nariadenia 2008/765



POŽIADAVKY NA ORGÁNY POSUDZOVANIA ZHODY

STN EN ISO/IEC 17021-1

- Posudzovanie zhody - požiadavky na orgány
vykonávajúce audit a certifikáciu systémov manažérstva

STN EN ISO/IEC 17024

- Posudzovanie zhody - všeobecné požiadavky na orgány
vykonávajúce certifikáciu osôb

STN EN ISO/IEC 17065

- Posudzovanie zhody - požiadavky na orgány
vykonávajúce certifikáciu výrobkov, procesov a služieb



CERTIFIKAČNÉ SCHÉMY

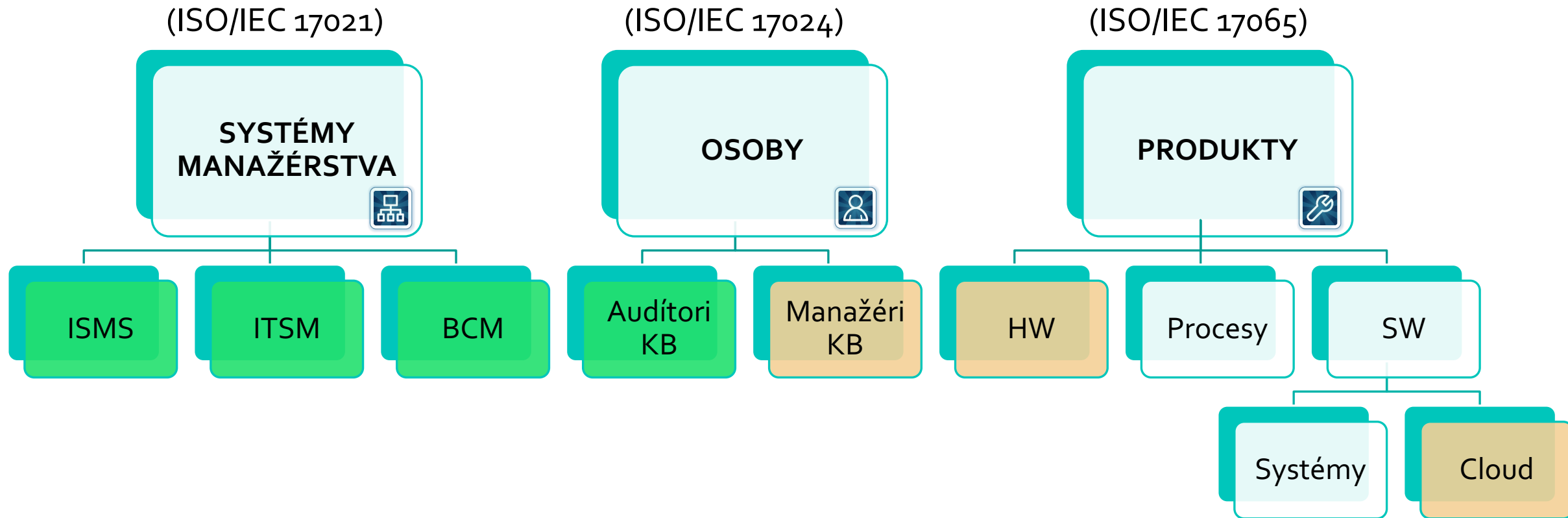


Schéma podľa Nariadenia 2008/765



CERTIFIKÁCIA VÝROBKU, PROCESU ALEBO SLUŽBY PODĽA NARIADENIA EÚ 881

Stupne dôveryhodnosti výrobku procesu alebo služby:

Základná

- Splňa stanovené bezpečnostné požiadavky
- Obsahuje požadované bezpečnostné funkcie
- Hodnotený na úrovni:
 - známych **základných rizík**
- Hodnotiace činnosti zahŕňajú aspoň:
 - Preskúmanie **technickej dokumentácie**
- Možné je **vlastné posúdenie** (self-assessment)

Pokročilá

- Hodnotený na úrovni:
 - Známych rizík,
 - Rizík incidentov, ktoré vykonávajú **subjekty s obmedzenými zručnosťami** a zdrojmi
- Hodnotiace činnosti zahŕňajú aspoň:
 - Preukázanie neexistencie **verejne známych zraniteľností**
 - **Test** ktorý preukazuje, že produkty IKT, procesy IKT alebo služby IKT správne plnia **potrebné bezpečnostné funkcie**

Vysoká

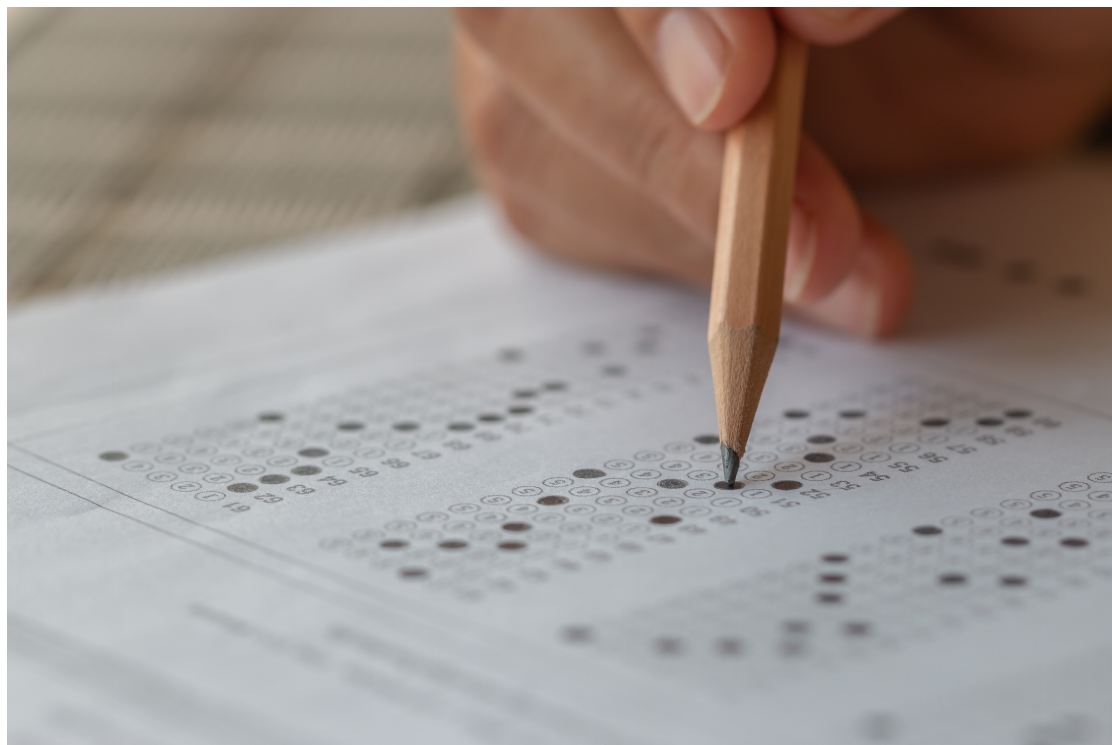
- Hodnotený na úrovni:
 - Rizika najpokročilejších kybernetických útokov, ktoré vykonávajú **subjekty so značnými zručnosťami** a zdrojmi
- Hodnotiace činnosti zahŕňajú:
 - Preukázanie neexistencie **verejne známych zraniteľností**
 - Preukázanie, že produkty, služby alebo procesy IKT správne plnia **najpokročilejšie potrebné bezpečnostné funkcie**
 - posúdenie ich odolnosti proti zručným útočníkom prostredníctvom **testovania prieniku**



ZÁVER

- Bezpečnostné opatrenia (aj pre cloud) sú uvedené vo Vyhláške NBÚ č. 362/2018 Z.z., a Vyhláške ÚPVII č. 179/2020 Z.z
- Cloud computing nie je systém manažérstva, ale produkt, resp. služba. Nemožno ho certifikovať podľa ISO/IEC 27001
- Certifikácia produktov v kybernetickej bezpečnosti je ošetrovaná nariadením (EÚ) 2019/881 o kybernetickej bezpečnosti
- Certifikácia nie je bezpečnostné opatrenie, ale spôsob preukázania zhody
- STN EN ISO/IEC 27002, ISO/IEC 27017, STN EN ISO/IEC 27018 nie sú certifikačné normy, ale súbor odporúčaní na bezpečnostné opatrenia podľa dobrej praxe
- Orgán posudzovania zhody, ktorý má ambíciu certifikovať cloudové služby musí byť akreditovaný podľa *STN EN ISO/IEC 17065 Posudzovanie zhody - požiadavky na orgány vykonávajúce certifikáciu výrobkov, procesov a služieb*
- Podmienkou žiadosti o akreditáciu je existencia certifikačnej schémy
- ENISA má pripravené dve certifikačné schémy relevantné pre cloud:
Certifikačná schéma pre posudzovanie výrobkov procesov a služieb v kybernetickej bezpečnosti a
Certifikačná schéma pre posudzovanie cloudových služieb
- Využívanie európskej certifikácie kybernetickej bezpečnosti a EÚ vyhlásenia o zhode by malo ostať dobrovoľné
- Členským štátom je umožnené prijať vnútroštátne predpisy, ktorými stanovia **povinnú certifikáciu podľa európskeho systému certifikácie** kybernetickej bezpečnosti v súlade so smernicou (EÚ) 2015/1535
- Členské štáty majú k dispozícii európsku certifikáciu kybernetickej bezpečnosti **aj v súvislosti s verejným obstarávaním** podľa smernice 2014/24





Ochrana vlastnických práv

Všetky autorské práva k tomuto dokumentu sú vyhradené pre Kompetenčné a certifikačné centrum kybernetickej bezpečnosti (ďalej len „KCCKB“). Autorské práva k tomuto dokumentu má a autorské práva k tomuto dokumentu vykonáva KCCKB.

Vlastnícke práva tretích strán

Všetky ochranné známky a iné obdobné právne chránené označenia spomenuté v tomto dokumente sú výhradným vlastníctvom ich vlastníkov, ktorí sú, pokiaľ sa nejedná o KCCKB, v dokumente označení vo forme príslušnej citácie.

Akékoľvek kopírovanie či iné neoprávnené použitie celého dokumentu alebo jeho časti, v elektronickej alebo listinnej podobe, bez predchádzajúceho písomného súhlasu jeho autorov, napr. KCCKB, je zakázané. Porušenie vlastnických a iných súvisiacich práv bude riešené v zmysle právnych predpisov Slovenskej republiky.

Limity informácií

Informácie obsiahnuté v tomto dokumente sú poskytované iba na informačné účely a bez akejkoľvek záruky, výslovnej či implicitnej. Názov KCCKB, logo KCCKB a ďalšie produkty a služby KCCKB sú ochrannými známkami KCCKB. Ostatné názvy spoločností, produktov alebo služieb môžu byť ochrannými známkami, alebo značkami služieb iných organizácií.



www.cybercompetence.sk



www.linkedin.com/company/cybercompetence



[@CybercenterSk](https://twitter.com/CybercenterSk)