Vytvárame dôveru už od roku 1866

Manažér kybernetickej bezpečnosti

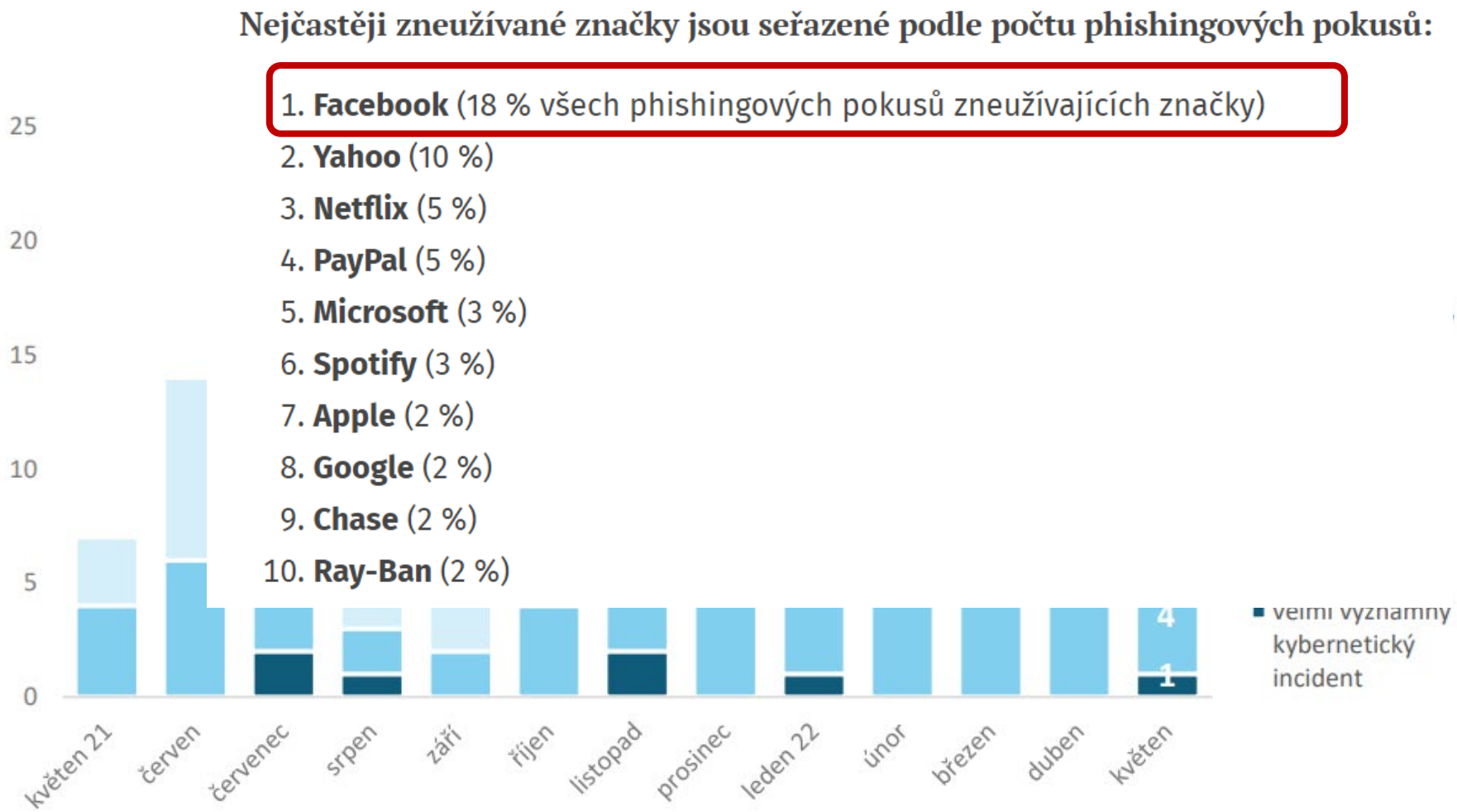
TÜV SÜD Slovakia

Viac istoty.
Viac hodnoty.

O mne

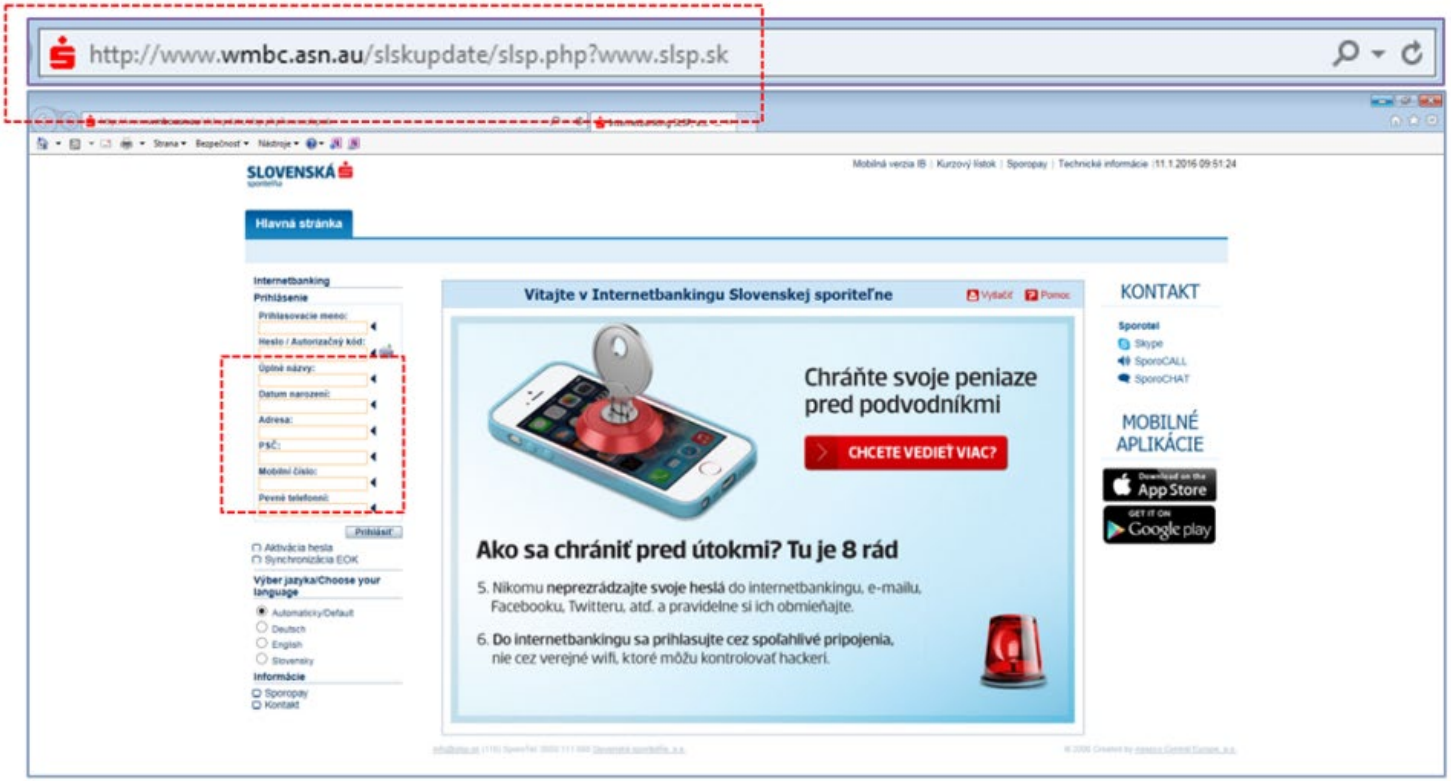
- Audítor kybernetickej bezpečnosti, Vedúci audítor pre systémy ISO/IEC 27001, ISO 22301, ISO 20000-1 a ďalšie.
- Od roku 2014 - spoločnosť **ZLIN Aircraft a.s**. – vedenie útvaru kvality a oddelenia IT
- Od roku 2017 – **Univerzita Tomáše Bati ve Zlíně – Fakulta aplikovanej informatiky** – odborný riešiteľ pre projekty Bezpečnostného výskumu Ministerstva vnitra ČR
- Od roku 2017 – **Univerzita Tomáše Bati ve Zlíně - Fakulta aplikovanej informatiky -** odborná lektorka predmetov: *Modelovanie krízových situácií* a *Manažment bezpečnostného inžinierstva*

Prečo zákonná povinnosť kybernetickej ochrany?



Prečo zákonná povinnosť kybernetickej ochrany?

Slovakia



Prečo zákonná povinnosť kybernetickej ochrany?

Slovakia

Zranitelnosti

Koncem května se objevila nová kritická zranitelnost CVE-2022-30190, také známá jako „Follina“, která se dotýká kancelářského balíku Microsoft Office. Útočníci skrze ni mohou spustit škodlivý kód i bez toho, aniž by oběť povolila makra. To činí phishingové útoky mnohem jednodušší. Zranitelnosti začaly ihned zneužívat hackerské skupiny, včetně APT skupin podporovanými vládami třetích zemí. NÚKIB proto na svých webových stránkách na zranitelnost upozornil a poskytl několik doporučení, jak zranitelnost mitigovat do doby, než bude dostupná opravná aktualizace.

Ransomware

Ransomwarové útoky od začátku roku stabilně tvoří přibližně pětinu incidentů, které NÚKIB eviduje, a stejně tomu bylo i v květnu. Dva z květnových incidentů byly způsobeny právě ransomwary, které jsou nabízeny jako služba a v kybernetickém prostoru je útočníci celosvětově nasazují od léta 2021.

Prečo zákonná povinnosť kybernetickej ochrany?

Slovakia

Zaměřeno na bezpečnostní opatření: Řízení dodavatelů

NÚKIB v květnu řešil několik závažných případů, které zdůrazňují potřebu procesu řízení dodavatelů. V jednom z kybernetických incidentů, který napadené organizaci způsobil značné škody, se útočník dostal do sítě své oběti skrze kompromitovaný VPN účet její servisní firmy. V tuto chvíli není jasné, jak servisní společnosti přihlašovací údaje k tomuto účtu unikly, ani jak se k nim útočník dostal. Útočník je použil jako vstupní bod do napadené organizace, odkud se pak laterálně rozšířil do dalších systémů.

Aktuálne

Varovanie pred zvýšeným rizikom kybernetických bezpečnostných útokov

21. júna 2022

Národné centrum kybernetickej bezpečnosti SK-CERT **varuje** pred zvýšeným rizikom kybernetických bezpečnostných útokov a to najmä na infraštruktúru **prevádzkovateľov základných služieb a prvkov kritickej infraštruktúry**.

Pokračujúca vojna na Ukrajine je príznačná nie len devastujúcimi fyzickými útokmi Ruska na infraštruktúru a obyvateľstvo Ukrajiny, ale aj **kontinuálnymi kybernetickými útokmi** ako na infraštruktúru Ukrajiny, tak aj na infraštruktúru členských štátov EÚ a NATO. Z dôvodu, že Slovenská republika je členským štátom EÚ a takisto aj NATO, **zvyšuje sa riziko**, že útočníci sa pri svojich aktivitách zamerajú aj na kybernetický priestor Slovenskej republiky. Národné centrum kybernetickej bezpečnosti preto vyhodnocuje **riziko kybernetických bezpečnostných útokov** na infraštruktúru prevádzkovateľov základných služieb a prvkov kritickej infraštruktúry ako **veľmi vysoké**.

Prečo Manažér kybernetickej bezpečnosti

- Požiadavka legislatívy Slovenskej republiky
- Zákon č. 69/2018 z.z. **Zákon o kybernetickej bezpečnosti**
- Zákon č. 95/2019 z.z. **Zákon o informačných technológiách vo verejnej správe**

Aký je rozdiel medzi MKB a AKB?

- **Audítor kybernetickej bezpečnosti** je osoba, ktorá posudzuje mieru plnenia požiadaviek zákona a mieru aplikácie bezpečnostných opatrení u prevádzkovateľa základnej služby.

- **Manažér kybernetickej bezpečnosti** je osoba, ktorá je zodpovedná za výkon role implementátora bezpečnostných opatrení do chodu organizácie.

- Pozor! Nie je to ITák!

Postavenie zákona 69 a role Manažéra KB

Slovakia

§ 20 Bezpečnostné opatrenia

(1) Bezpečnostnými opatreniami na účely tohto zákona sú úlohy, procesy, role a technológie v organizačnej, personálnej a technickej oblasti, ktorých cieľom je zabezpečenie kybernetickej bezpečnosti počas životného cyklu sietí a informačných systémov. Bezpečnostné opatrenia realizované v závislosti od klasifikácie informácií a kategorizácie sietí a informačných systémov a v súlade s bezpečnostnými štandardami v oblasti kybernetickej bezpečnosti sa prijímajú s cieľom predchádzať kybernetickým bezpečnostným incidentom a minimalizovať vplyv kybernetických bezpečnostných incidentov na bezpečnosť prevádzkovania služby. Bezpečnostné opatrenia sú všeobecné, realizované v závislosti od klasifikácie informácií a kategorizácie sietí a informačných systémov a v súlade s bezpečnostnými štandardami v oblasti kybernetickej bezpečnosti pre všetky siete a informačné systémy a sektorové, ktoré sa realizujú na základe špecifík kategorizácie sietí a informač
súlade s

(2) Klasifikác
základe v
integritu

(3) Bezpečnc
a) organ
b) riaden
c) perso
d) riaden
e) riaden
f) bezpe
g) hodnc
h) ochrany proti škodlivému kódu,
i) sieťovej a komunikačnej bezpečnosti,
j) akvizície, vývoja a údržby informačných sietí a informačných systémov,
k) zaznamenávania udalostí a monitorovania,
l) fyzickej bezpečnosti a bezpečnosti prostredia,
m) riešenia kybernetických bezpečnostných incidentov,
n) kryptografických opatrení,
o) kontinuity prevádzky,
p) auditu, riadenia súladu a kontrolných činností.

(4) Bezpečnostné opatrenia musia zahŕňať najmenej

a) určenie manažéra kybernetickej bezpečnosti, ktorý je pri návrhu, prijímaní a presadzovaní bezpečnostných opatrení nezávislý od štruktúry riadenia prevádzky a vývoja služieb informačných technológií a ktorý spĺňa znalostné štandardy pre výkon roly manažéra kybernetickej bezpečnosti,
b) detekciu kybernetických bezpečnostných incidentov,
c) evidenciu kybernetických bezpečnostných incidentov,
d) postupy riešenia a riešenie kybernetických bezpečnostných incidentov,
e) určenie kontaktnej osoby pre prijímanie a evidenciu hlásení,
f) pripojenie do komunikačného systému pre hlásenie a riešenie kybernetických bezpečnostných incidentov a centrálneho systému včasného varovania.

Samohodnotenie

- Samohodnotenie účinnosti prijatých bezpečnostných opatrení v zmysle zákona o kybernetickej bezpečnosti -NBU (gov.sk)

Samohodnotenie v zmysle zákona o kybernetickej bezpečnosti

Vážený prevádzkovateľ základnej služby (PZS),

tento formulár samohodnotenia je určený pre tých PZS, ktorí:

1. majú v období od 1. augusta 2021 do 31. decembra 2023 povinnosť auditu podľa zákona č. 69/2018 Z.z. vo kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „zákon č. 69/2018 Z. z."),
2. majú len informačné systémy kategórie I. a II. podľa vyhlášky Národného bezpečnostného úradu č. 362/2018 Z.z.z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení (ďalej len „vyhláška č. 362/2018 Z. z.") a
3. majú určeného manažéra kybernetickej bezpečnosti.

Certifikačná schéma Manažéra KB

- [NBU-Certifikacna_schema_20200319_v3.4.pdf (gov.sk)]

3.1.2 Minimálne požiadavky na vzdelanie a prax

Minimálne požiadavky na úroveň vzdelania a prax žiadateľa o overenie odbornej spôsobilosti:

Vzdelanie a požadovaný doklad	Prax a spôsob jej preukázania (alternatívy predložených dokumentov)
Úplné stredné všeobecné vzdelanie a úplné stredné odborné vzdelanie (doklad o získanom stupni vzdelania a o získanej kvalifikácii)	• skúsenosti v oblasti informačných technológií - najmenej **7 rokov praxe** (životopis s uvedením kontaktu na overiteľnú referenciu), • z toho skúsenosti v oblasti riadenia IT služieb, riadenia informačnej bezpečnosti, riadenia rizík, alebo architektúry IT - najmenej **5 rokov praxe** • medzinárodný certifikát z oblasti riadenia IT služieb, riadenia informačnej bezpečnosti, riadenia rizík, alebo architektúry IT sa považuje za započítateľnú odbornú prax (nepovinný, nahrádza 1 rok praxe)
Vysokoškolské vzdelanie prvého stupňa (doklady o absolvovaní štúdia)	• skúsenosti v oblasti informačných technológií - najmenej **5 rokov praxe** (životopis s uvedením kontaktu na overiteľnú referenciu), • z toho skúsenosti v oblasti riadenia IT služieb, riadenia informačnej bezpečnosti, riadenia rizík, alebo architektúry IT - najmenej **3 roky praxe** • medzinárodný certifikát z oblasti riadenia informačnej bezpečnosti sa považuje započítateľnú odbornú prax (nepovinný, nahrádza 1 rok praxe)
Vysokoškolské vzdelanie druhého stupňa (doklady o absolvovaní štúdia)	• skúsenosti v oblasti informačných technológií - najmenej **3 roky praxe** (životopis s uvedením kontaktu na overiteľnú referenciu), • z toho skúsenosti v oblasti riadenia IT služieb, riadenia informačnej bezpečnosti, riadenia rizík, alebo architektúry IT - najmenej **1 rok praxe** • medzinárodný certifikát z oblasti riadenia IT služieb, riadenia informačnej bezpečnosti, riadenia rizík, alebo architektúry IT sa považuje za odbornú prax (nepovinný, nahrádza 1 rok praxe)

Osobitné požiadavky na spôsobilosť – 21 bodov

Slovakia

1. Znalosť procesov a systému riadenia informačnej a kybernetickej bezpečnosti
2. Znalosť zásad organizácie informačnej a kybernetickej bezpečnosti
3. Znalosť zásad personálnej bezpečnosti
4. Znalosť zásad riadenia prístupov a identít
5. Znalosti o spôsobe používania kryptografických bezpečnostných mechanizmov
6. Znalosť princípov testovania kybernetickej bezpečnosti

Osobitné požiadavky na spôsobilosť – 21 bodov

7. Znalosť právnych predpisov, požiadaviek na súlad a noriem vzťahujúcich sa na kybernetickú bezpečnosť, najmä:
   - smernice Európskeho parlamentu a Rady (EÚ) 2016/1148 zo 6. júla 2016 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii,
   - nariadenia Európskeho parlamentu a Rady (EÚ) 2019/881 zo 17. apríla 2019 o agentúre ENISA (Agentúra Európskej únie pre kybernetickú bezpečnosť) a o certifikácii kybernetickej bezpečnosti informačných a komunikačných technológií a o zrušení nariadenia (EÚ) č. 526/2013 (akt o kybernetickej bezpečnosti)
   - nariadenia Európskeho parlamentu a Rady (EÚ) č. 910/2014 z 23. júla 2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu,
   - zákona č. 69/2018 Z.z.
   - vyhlášky č. 362/2018 Z.z.
   - vyhlášky Národného bezpečnostného úrade č. 164/2018 Z. z. ktorou sa určujú identifikačné kritériá prevádzkovanej služby (kritériá základnej služby),
   - vyhlášky Národného bezpečnostného úradu č. 165/2018 Z. z. ktorou sa určujú identifikačné kritériá pre jednotlivé kategórie závažných kybernetických bezpečnostných incidentov a podrobnosti hlásenia kybernetických bezpečnostných incidentov,
   - vyhlášky Národného bezpečnostného úradu č. 166/2018 Z. z. o podrobnostiach o technickom, technologickom a personálnom vybavení jednotky pre riešenie kybernetických bezpečnostných incidentov,
   - zákona č. 95/2019 Z. z.
   - vyhlášky č. 179/2020 Z. z.
   - zákona č. 45/2011 Z. z. o kritickej infraštruktúre v znení neskorších predpisov,
   - zákona č. 272/2016 Z. z. o dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (zákon o dôveryhodných službách),
   - medzinárodných noriem rady ISO/IEC 27000 „Informačné technológie - Bezpečnostné metódy - Systémy riadenia informačnej bezpečnosti“,
   - medzinárodných noriem rady ISA/IEC 62443 „Security for Industrial Automation and Control Systems“ ak sa takáto znalosť na dohodnutú prácu vyžaduje.

Osobitné požiadavky na spôsobilosť – 21 bodov – Ochrana osobných údajov

Slovakia

8. Znalosť právnych predpisov a požiadaviek na súlad vzťahujúcich sa na ochranu osobných údajov, najmä:
   - nariadenia Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov)
   - zákona č. 18/2018 Z. z. o ochrane osobných údajov a o doplnení niektorých zákonov v znení neskorších predpisov,
   - smernice Európskeho parlamentu a Rady2002/58/ES z 12. júla 2002, týkajúca sa spracovávania osobných údajov a ochrany súkromia v sektore elektronických komunikácií (smernica o súkromí a elektronických komunikáciách) a jej implementácie v zákone č. 351/2011 Z. z. o elektronických komunikáciách v znení neskorších predpisov
9. Znalosť štandardov a zásad ochrany osobných údajov, vrátane metodických usmernení Úradu na ochranu osobných údajov Slovenskej republiky a Výboru na ochranu údajov (EÚ)

Osobitné požiadavky na spôsobilosť

10. Schopnosť navrhovať a uplatniť bezpečnostné stratégie a politiky
11. Znalosť procesov a metodík riadenia rizík
12. Znalosť postupov analýzy rizík
13. Znalosť typických hrozieb a postupov pre identifikáciu hrozieb a zraniteľností
14. Znalosť bezpečnostných mechanizmov
15. Znalosť princípov podnikovej architektúry, orientácia v architektúrnych rámcoch
16. Znalosť procesov riešenia kybernetických bezpečnostných incidentov
17. Znalosť princípov plánovania havarijnej obnovy prevádzky
18. Znalosť procesov riadenia kontinuity činností
19. Znalosť metód posudzovania rizík a schopnosť ich aplikovať v rámci organizácie
20. Schopnosť analyzovať a kvantifikovať riziká
21. Schopnosť analyzovať a hodnotiť bezpečnostné mechanizmy a riešenia

Kde sa to naučím? Skrátený kurz

Slovakia

[Školenia a online kurzy v TÜV SÜD Akadémii | TÜV SÜD Slovakia (tuvsud.com)]

VYBERTE SI Z NAŠICH KURZOV A POVÝŠTE VAŠE VEDOMOSTI NA NOVÚ ÚROVEŇ:

VZDELÁVANIE E-LEARNINGOVOU FORMOU

ZAMERANÉ NA ROZVOJ KVALITY

INFORMAČNÁ BEZPEČNOSŤ

KYBERNETICKÁ BEZPEČNOSŤ

- **Kurz:** Manažér kybernetickej bezpečnosti (Cyber Security Manager)
- **Certifikačná skúška:** Manažér kybernetickej bezpečnosti - NOVÉ
- **Certifikačná skúška:** Audítor kybernetickej bezpečnosti

Kde sa to naučím? Vzdelávací program

Slovakia

Školenia a online kurzy v TÜV SÜD Akadémii | TÜV SÜD Slovakia (tuvsud.com)

INFORMAČNÁ BEZPEČNOSŤ

- Základy informačnej bezpečnosti **Nové školenie!**
- Interný audítor systémov manažérstva podľa ISO/IEC 27001
- Preškolenie interných audítorov podľa normy STN ISO/IEC 27001
- DPO - Data Protection Officer: GDPR a ochrana osobných údajov podľa 18/2018 Z.z.
- TISAX (Trusted Information Exchange Assessment Security)
- Manažér riadenie rizík v IT
- Manažér kontinuity v podnikaní (manažér BCMS) / interný audítor podľa ISO 22301
- Manažér kybernetickej bezpečnosti (Cyber Security Manager)
- Informačné technológie vo verejnej správe podľa zákona č. 95/2019 Z.z. **Nové školenie!**
- Audítor kybernetickej bezpečnosti
- Riadenie kvality softvéru podľa noriem radu ISO/IEC 25000

KYBERNETICKÁ BEZPEČNOSŤ

- **Kurz:** Manažér kybernetickej bezpečnosti (Cyber Security Manager)
- **Certifikačná skúška:** Manažér kybernetickej bezpečnosti - NOVÉ

Akreditovaná skúška Manažéra kybernetickej bezpečnosti

Slovakia

[Certifikačná skúška Manažér kybernetickej bezpečnosti | TÜV SÜD Slovakia (tuvsud.com)]

1. Nutné splniť požiadavky na PRAX a vzdelanie
2. Doložiť požadované dokumenty
3. Vykonať skúšku (150 minút a 100 otázok)

Opravná skúška zdarma.

CERTIFIKAČNÁ SKÚŠKA MANAŽÉR KYBERNETICKEJ BEZPEČNOSTI

Odborná skúška pre certifikáciu osôb v oblasti Manažér kybernetickej bezpečnosti podľa zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov vykonávaná v súlade s normou ISO/IEC 17024:2012 a certifikačnou schémou overovania odbornej spôsobilosti manažéra kybernetickej bezpečnosti, ktorú vydal Národný bezpečnostný úrad SR (ďalej len "NBÚ") ako orgán dohľadu v oblasti kybernetickej bezpečnosti.

Odborná skúška je vykonávaná formou písomného testu obsahujúceho 100 otázok (v časovom rozsahu 150 min) zo znalosti všeobecne záväzných právnych predpisov a príslušných technických noriem o podmienkach výkonu činnosti manažéra kybernetickej bezpečnosti (ďalej len "MKB") a o bezpečnostných opatreniach v kybernetickej bezpečnosti.

POŽIADAVKY NA ŽIADATEĽA O CERTIFIKÁCIU MKB

- splnenie **všeobecných** požiadaviek na spôsobilosť žiadateľa - požiadavky na vzdelanie a prax - v zmysle kap. 3.1 certifikačnej schémy NBÚ (ďalej len "CS NBÚ").
- splnenie **osobitných** požiadaviek na spôsobilosť žiadateľa - požadované znalosti - v zmysle kap. 3.2 CS NBÚ
- splnenie **predpokladov na výkon činnosti** MKB - v zmysle kap. 3.1.4, 3.1.5 a 3.1.6 CS NBÚ

REGISTRAČNÝ FORMULÁR NA CERTIFIKAČNÚ SKÚŠKU

Názov

Skúška Manažér kybernetickej bezpe

Titul

Meno*

Priezvisko*

E-mail*

Telefónne číslo*

Termín skúšky

- - Prosím, vyberte si termín skúšky -

FAKTURAČNÉ ÚDAJE

Názov spoločnosti*

Ale čo ak takého človeka nemám?

Slovakia

- Zabezpečíme Vám službu **Externe riadený Manažér kybernetickej bezpečnosti**, ktorý bude **nezávislý od riadenia prevádzky** a bude spĺňať **kvalifikačný štandard** definovaný zákonom.

Na čo si dať pozor?

- **<u>Nie všetko čo je lacné je i dobré</u>**. Pozor na necertifikovaných Manažérov kybernetickej bezpečnosti, ktorí neabsolvovali AKREDITOVANÚ skúšku Manažéra kybernetickej bezpečnosti.

Zoznam certifikačných orgánov:

- **Kompetenčné a certifikačné centrum kybernetickej bezpečnosti**
- **TÜV SÜD Slovakia s.r.o.**

- Zmluva! Pozor na to, čo v zmluve s manažérom kybernetickej bezpečnosti máte.

Ďakujem za pozornosť

Prípadné ďalšie otázky smerujte na:
lucia.mrazkova@partner.tuvsud.com
Akadémia:
gabriela.barzikova@tuvsud.com

Slovakia

Viac istoty.
Viac hodnoty.