Partner konferencie KYBERNETICKÁ BEZPEČNOSŤ 2023

ISIT SK SOFTWARE cybersecurity

KYBERNETICKÁ BEZPEČNOSŤ, OCHRANA OSOBNÝCH ÚDAJOV, WHISTLEBLOWING, eLEARNING, FYZICKÁ A OBJEKTOVÁ BEZPEČNOSŤ v rokoch 2023 - 2024

K riadeniu kybernetickej bezpečnosti v organizácii sa môže pristupovať formálnym spôsobom, ktorý predstavuje vytvorenie množstva rôznych dokumentov, tabuliek, podkladov, smerníc a statických analýz, alebo kontrahovať expertov pracujúcich prevažne s excelovskými tabuľkami vytvárajúcimi statické analýzy rizík, alebo – pracovať účelne, systémovo a efektívne prostredníctvom špeciálnych modulov softvérovej aplikácie a s pomocou nej riadiť on-line proces analýzy rizík v oblasti kybernetickej bezpečnosti v organizácii.

Automatizované riadenie | Dosiahnutie finančných úspor
Legislatívny súlad | Moderné riešenie | Optimalizácia

STRUČNÁ ANOTÁCIA MODULOV APLIKÁCIE ISIT SOFTWARE SK/CZ PRE SAMOSTATNÉ RIADENIE PROCESOV BEZPEČNOSTI V ORGANIZÁCII

Modul KBO

Komplexný nástroj pre riadenie kybernetickej bezpečnosti, ochrana kľúčových aktív definovanými opatreniami s riadením rizík, priama komunikácia NBU/NUKIB.

Modul GDPR s väzbami posúdenia DPIA

Komplexné detailné riadenie bezpečnosti osobných údajov súladné so zmenami v legislatíve, interným auditom, personálnou bezpečnosťou ai.

Modul Whistleblowing s riadením korupčných rizík

Bezpečnosť dát a garantovaná dôvernosť - ochrana identity Oznamovateľa s riadeným procesom vyšetrenia oznámenia.

Modul Fyzická a objektová bezpečnosť

Prierezové riadenie fyzickej a objektovej bezpečnosti naprieč procesmi v organizácii (personálna bezpečnosť, riadenie 3 strán, opatrenia FOB kamerové systémy, kľúčový poriadok, riadenie aktív FOB atď. – vhodné pre odbory bezpečnosti a kríz. riadenia, obecné polície, SBS ai.).

Modul E-learning

Vzdelávací nástroj na budovanie a udržiavanie bezpečnostného povedomia v organizácii vrátane testovania užívateľov a generovania osvedčenia o úspešnom absolvovaní.

BEZPEČNOSTNÝ PORTÁL ISIT

Web aplikačná časť pre nahlasovanie bezpečnostných udalostí s manažmentom bezpečnostných incidentov (GDPR, KBO) a ďalších informácií prístupná len pre oprávnené osoby a vlastníkov aktív organizácie. Umiestnenie na webovom sídle organizácie s riadeným prístupom.

ISIT SK
SOFTWARE cybersecurity

MODUL KYBERNETICKÁ BEZPEČNOSŤ - KBO

3 hlavné dôvody prečo riadiť kybernetickú bezpečnosť softvérom:

1. Softvér predstavuje výkonný nástroj pre riadenie kybernetickej a informačnej bezpečnosti informačných systémov prevádzkujúcich základnú službu v zmysle zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti, ako aj informačných systémov verejnej správy v zmysle zákona č.95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov.

2. Softvér zabezpečuje on-line riadenie procesu analýzy rizík, automaticky prispôsobuje analýzu rizík na realizáciu jednotlivých opatrení, ktoré sú zavádzané priebežne v zmysle plánu implementácie navrhovaných bezpečnostných opatrení.

3. Softvér pomáha v prípade budovania nových informačných systémov alebo ich častí analyzovať vo fáze návrhu jednotlivé prvky pripravovanej architektúry z hľadiska bežných kybernetických a informačných hrozieb a navrhovať potrebné eliminačné bezpečnostné opatrenia

FUNKCIONALITA MODULU KBO :

- Komplexné riadenie procesov, vedenie evidencií a generovanie tlačových výstupov
- Obsahuje Automatizovanú analýzu rizík s možnosťou výberu zo 4 bezpečnostných modelov s namapovanými kolekciami opatrení ku konkrétnym hrozbám pre jednotlivé aktíva/skupiny aktív (best practices, podľa zákona č. 69/2018 o kybernetickej bezpečnosti, podľa zákona č. 95/2019 o ITVS a vyhlášky č. 362/2018 Z. o obsahu bezpečnostných opatrení, obsahu a štruktúre bezpečnostnej dokumentácie, podľa ISO/IEC 27xxx)
- Kolekcie aktív, resp. skupiny aktív obsahujú nielen aktíva informačných technológií, ale aj aktíva tzv. OT systémov (operational technologies, v odbornej terminológii označované aj ako ICS – Industrial Control System alebo IACS – Industrial Automation and Control Systems).
- Komplexný incident manažment s generovaním hlásenia o bezp. incidente
- Samostatné riadenie personálnej bezpečnosti.
- Riadenie tretích strán pristupujúce k informačno-komunikačným technilógiam organizácie
- Aplikácia je škálovateľná ako konzola pre manažéra KB, ale zároveň je pripravená na komplexné riadenie KB so zapojením všetkých vlastníkov aktív, rizík až po riadiace zložky (admin/klient). Eliminuje potrebu trvalej prítomnosti externých poradcov na bezpečnosť, čím znižuje náklady a zároveň udržiava súlad riadenia KB s platnou legislatívou.
- Evidencia a riadenie aktív informačno-komunikačných technológií, resp. v rozsahu potrebnom pre ISMS (Systém riadenia bezpečnosti informácií - Information Security Management System - ISMS) v organizáci

ISIT SK SOFTWARE cybersecurity

VÝHODY MODULU KBO:

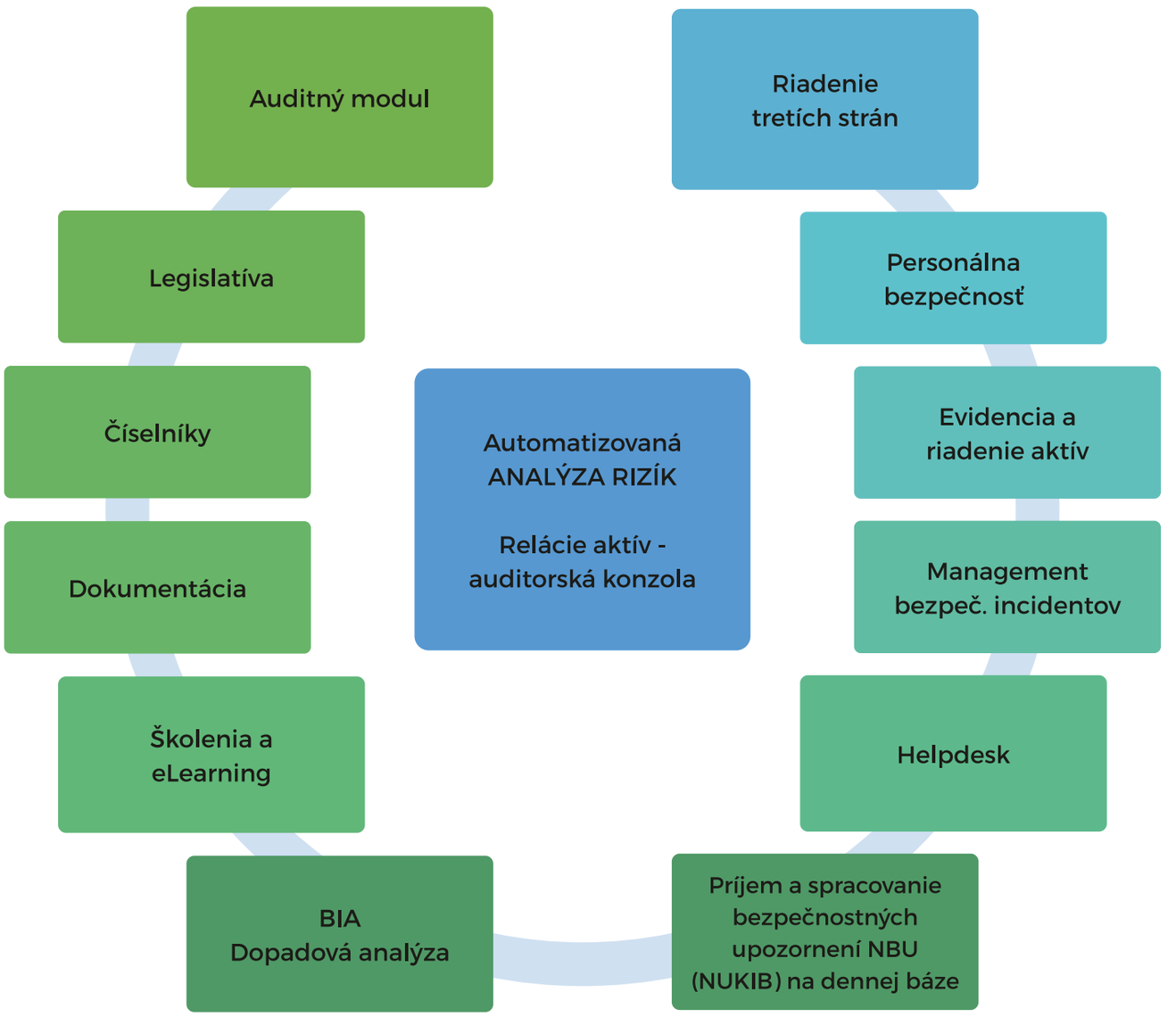
Softvér ako znalostné riešenie v module KBO :

- Je dôležitým nástrojom a pomôckou pre manažéra informačnej a kybernetickej bezpečnosti rovnakého funkčného významu, ako je napr. účtovný softvér pre účtovníka.
- Je poistený na 1 mil. eur (všeobecná zodpovednosť za škodu) pre územie EU
- Získal Osvedčenie o súlade s platnou legislatívou v oblasti kyberbezpečnosti
- Stal sa súčasťou odbornej literatúry Kybernetická (ne)bezpečnost – Problematika bezpečnosti v kyberprostoru, autor Petr Sedlák a kol. 10-2021 vydavatelství CERM ako implementačné riešenie KYBE pre KII a Z
- Môže slúžiť ako individuálne riešenie pre samotnú organizáciu, tak aj na riadenie sektorových procesov KB pre riadiace / ústredné orgány v rámci sektoru resp. na riadenie prístupu tretích strán a ich dodávateľov

Modul KBO disponuje:

- Intuitívnym ovládaním, ktoré zvládne nielen expert ale aj informovaný laik
- Predvyplnenými číselníkmi v moduloch, nepotrebujete dopĺňať množstvo dát a súvislostí
- Zrozumiteľnými a prehľadnými výstupmi v elektronickej alebo tlačenej forme vrátane Záverečnej správy
- Aktuálne naprogramovanými cca 50 tisíc väzbami medzi aktívami, hrozbami, zraniteľnosťami a ochr. opatreniami, čo výrazne zjednodušuje Vašu prácu v automatizovanej Analýze rizík
- Konzolou relácií aktív, kde Manažér IB/KB môže aktívne vykonávať zmeny v Analýze rizík
- Auditným modulom cieľov a opatrení podľa prílohy A a maticou RASCI
- Univerzálnosťou použitia, nie je potrebná customizácia softvéru pre zákazníka
- Príjemnou cenou pri širokom využití, s plnou podporou autorov softvéru

GRAFICKÉ ZNÁZORNENIE MODULARITY MODULU
KYBERNETICKÁ BEZPEČNOSŤ ORGANIZÁCIE



ISIT SK SOFTWARE cybersecurity

PERSONÁLNA BEZPEČNOSŤ
Vedie evidenciu prístupov k informačným a komunikačným systémom organizácie, prístupových rolí a prenos oprávnení, vedie evidenciu zverených aktív, kontroluje rozvoj bezpečnostného povedomia.

RIADENIE TRETÍCH STRÁN
Vedie evidenciu tretích strán, povolených prístupov k informačno-komunikačným technológiám organizácie, špecifikuje rozsah činností apod.

RIADENIE AKTÍV
Vedie evidenciu aktív, opis ich vlastností, vedie evidenciu ich vlastníkov a správcov, osôb.

IMPORT AKTÍV A VYBRANÝCH ČÍSELNÍKOV
Umožňuje načítanie zoznamu aktív a naplnenie vybraných číselníkov z externého súboru v podporovanom štandardnom formáte pre výmenu dát (xml, csv, xls).

ANALÝZA RIZÍK
Výnimočný nástroj na realizáciu Analýzy rizík, ako účinného prostriedku na objektívnu identifikáciu slabých miest organizácie.

GAP Analýza
Nástroj umožňuje v úvode procesu, resp. pred procesom analýzy rizík vykonať GAP analýzu.

Relácie aktív
Slúži ako špeciálna manažérska konzola zameraná na Analýzu rizík, umožňuje aktívny vstup do modifikačného režimu Analýzy rizík, modifikuje prednastavenú paletu atribútov.

MANAŽMENT BEZPEČNOSTNÝCH INCIDENTOV
Vedie súhrnnú evidenciu o životnom cykle incidentu, komplexne riadi bezpečnostné incidenty, generuje hlásenia o bezpečnostnom incidente SK-CERT-u ai.

MANAŽMENT AUDITOV, MATICA RASCI, CIELE RIADENIA A OPATRENIA
Obsahuje funkčný manažment auditov, kompetenčnú maticu RASCI ako auditný nástroj pre identifikáciu rolí a zodpovednosti v rámci procesu.

ŠKOLENIA
Systematicky riadi zvyšovanie povedomia používateľov v oblasti KB prostredníctvom interných školení alebo e-Learningových kurzov.

DOKUMENTÁCIA
Vedie evidenciu povinných dokumentov a informácií, politík a metodík.

PRÍJEM A SPRACOVANIE BEZPEČNOSTNÝCH VAROVANÍ NBÚ / MANAŽMENT BEZPEČNOSTNÝCH VAROVANÍ
Umožňuje príjem a následné spracovanie bezpečnostných varovaní zverejňovaných a poskytovaných SK-CERT s automatizovaným upozornením pre vlastníkov/správcov relevantných aktív, ktorých sa bezpečnostné varovanie týka.

ISIT SK SOFTWARE cybersecurity

ANALÝZA RIZÍK

Pred spustením Automatizovanej AR zadávate nasledovné informácie:

Základné informácie o IKS, primárne a podporné aktíva s vlastníkmi, voľbu bezpečnostného modelu, klasifikáciu a kategorizáciu informácií.

Vytvárate si Vstupnú AR, Priebežné AR a Testovacie AR.

SK
Bezpečnostné modely

- Bezpečnostný model pre IS podľa **Best practices**
- Bezpečnostný model pre IS prevádzkujúci ZS podľa zákona č. 69/2018 Z. z. o KB
- Bezpečnostný model pre IS VS podľa zákona č. 95/2019 Z. z. o ITVS
- Bezpečnostný model podľa ISO / IEC 27xxx
  - Základný (114 opatrení)
  - Rozšírený (850 opatrení)
  - Zdravotníctvo ISO IEC 27799

CZ
Bezpečnostní modely

- Bezpečnostní model pro IS podle zákl. pravidel IB a nejlepší praxe
- Bezpečnostní model pro IS podle Vyhlášky o KB č. 82/2018 Sb.
- Bezpečnostní model pro IS podle Vyhlášky a zákl. pravidel IB
- Bezpečnostní model podle ISO / IEC 27xxx
  - Základní (114 opatření)
  - Rozšířený (850 opatření)
  - Zdravotnictví ISO IEC 27799

ISIT SK SOFTWARE cybersecurity

ANALÝZA RIZÍK

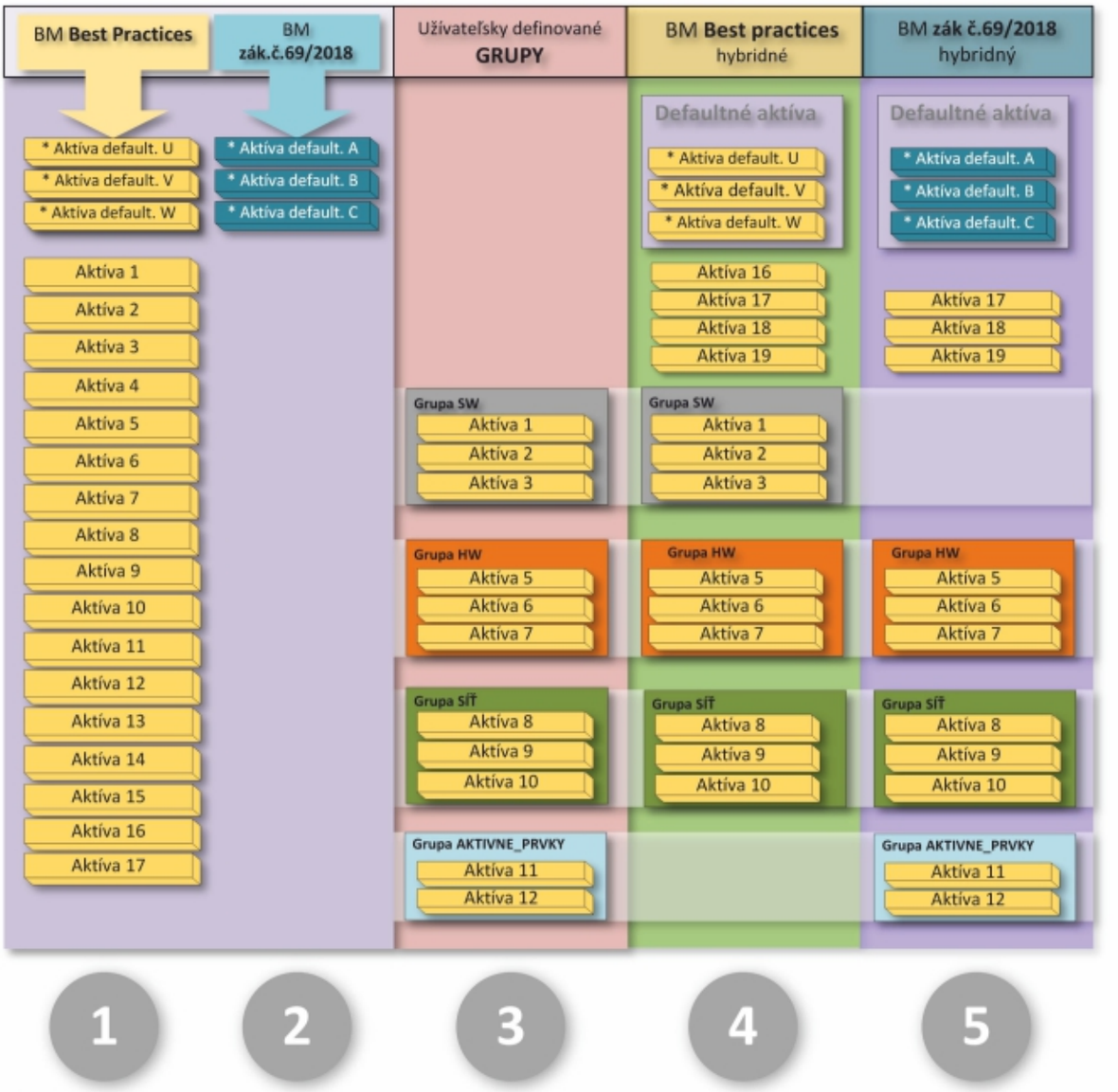
Práca s Automatizovanou analýzou rizík obsahuje:

- Voľba rozsahu identifikácie rizík
- Popisy aktív / skupín aktív
- Identifikácia hrozieb a zraniteľností
- Identifikácia ochranných opatrení
- Prehľady
- Katalóg rizík
- Identifikácia následkov (dopadov) s prehľadom hrozieb, zraniteľností a atribútov CIA
- Analýza rizík s kompletnými prehľadmi hrozieb, zraniteľností, dopadov CIA, hodnoty aktíva, pravdepodobnosti a miery rizika
- Riadenie rizík s vyhodnotením rizika
- Prijatie zostatkových rizík
- Viazanosti vlastníka s aktívami / skupinou aktív a ich opatreniami
- Monitorovanie rizík
- Exporty a generovanie Záverečnej správy

ISIT SK SOFTWARE cybersecurity

ANALÝZA RIZÍK - GRUPY AKTÍV

Novinkou od roku 2023 je jedinečná funkcia pre prácu s informačnými aktívami, ktorá umožňuje používateľmi zoskupovať a kombinovať informačné aktíva priradené k jednotlivým bezpečnostným modelom do používateľmi vytvorených a definovaných grúp a tieto následné využiť v procese analýzy rizík kybernetickej bezpečnosti.



1 - Bezpečnostný model Best Practices

2 - Bezpečnostný model podľa zákona č.69/2018 Z. z. alebo č.95/2019 Z. z.

3 - Priradenie aktív do používateľmi definovaných grúp

4 - Bezpečnostný model Best Practices s vybranými používateľkými grupami

5- Bezpečnostný model podľa zákona č.69/2018 Z. z. s vybranými používateľkými grupami

ISIT SK SOFTWARE cybersecurity

ZÁVEREČNÁ SPRÁVA

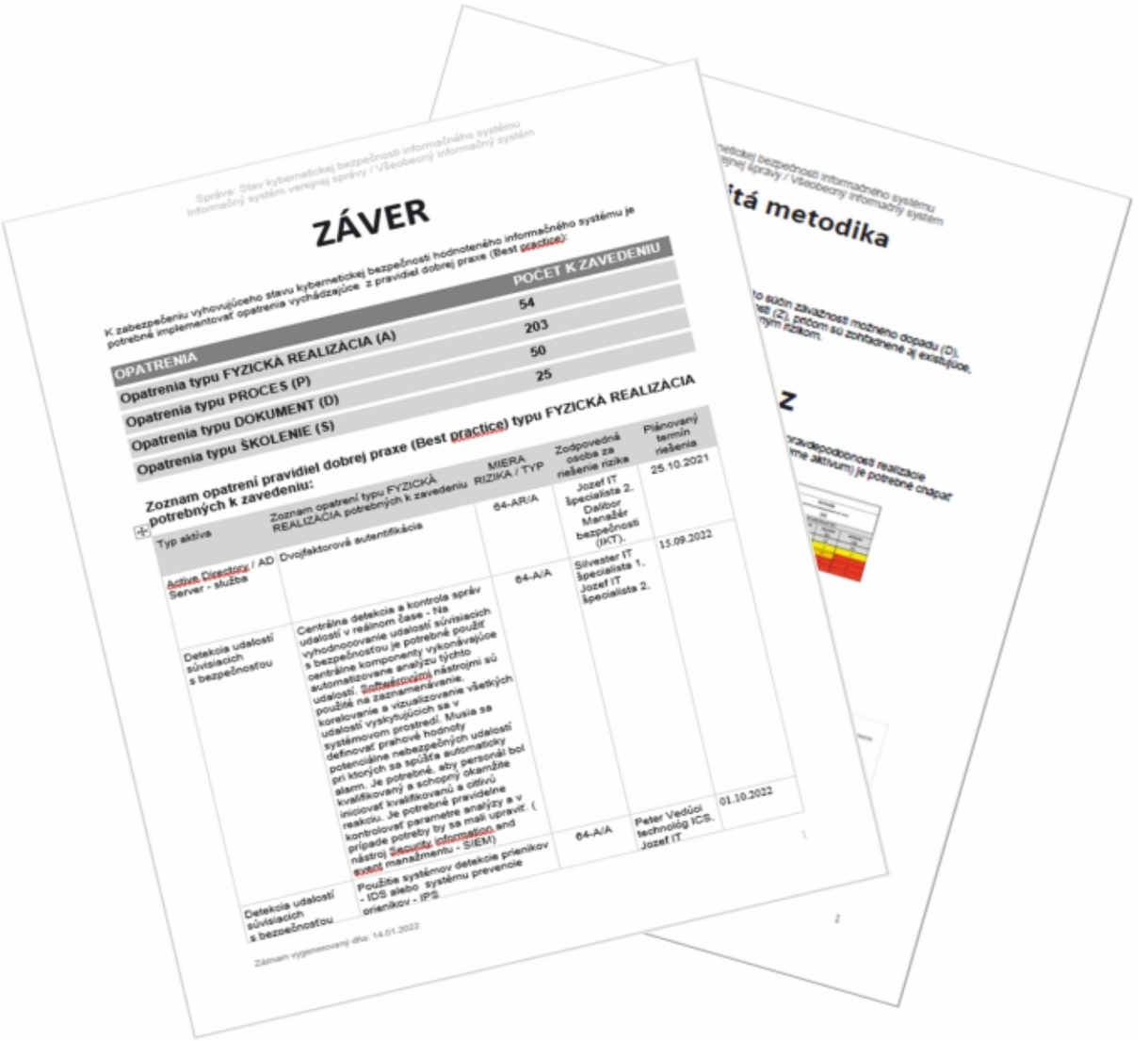
Záverečná správa obsahuje vygenerované informácie obsiahnuté v aplikácii, pričom užívateľ si volí z jednotlivých parciálnych častí záverečnej správy:

- Správa kybernetickej bezpečnosti IS
- Závery z analýzy rizík skúmaného IS
- Aktíva
- Analýza rizík - výstup
- Záver
- Vyhlásenie o aplikovateľnosti
- Legislatívne východiská Kb
- Použitá metodika
- Označenie používané na zabezpečenie zdieľania citlivých informácií
- Podporné služby

Záverečná správa obsahuje ako textovú časť, tak aj grafické a číselné znázornenie vybraných informačných blokov:

ISIT SK SOFTWARE cybersecurity

VÝŇATOK ZO ZÁVEREČNEJ SPRÁVY



Správa: Stav kybernetickej bezpečnosti informačného systému
Informačný systém verejnej správy / Všeobecný informačný systém

ZÁVER

K zabezpečeniu vyhovujúceho stavu kybernetickej bezpečnosti hodnoteného informačného systému je potrebné implementovať opatrenia vychádzajúce z pravidiel dobrej praxe (Best practice):

OPATRENIA	POČET K ZAVEDENIU
Opatrenia typu FYZICKÁ REALIZÁCIA (A)	54
Opatrenia typu PROCES (P)	203
Opatrenia typu DOKUMENT (D)	50
Opatrenia typu ŠKOLENIE (S)	25

Zoznam opatrení pravidiel dobrej praxe (Best practice) typu FYZICKÁ REALIZÁCIA potrebných k zavedeniu:

Typ aktíva	Zoznam opatrení typu FYZICKÁ REALIZÁCIA potrebných k zavedeniu	MIERA RIZIKA / TYP	Zodpovedná osoba za riešenie rizika	Plánovaný termín riešenia
Active Directory / AD Server - služba	Dvojfaktorová autentifikácia	64-AR/A	Jozef IT špecialista 2. Dalibor Manažér bezpečnosti (IKT).	25.10.2021
Detekcia udalostí súvisiacich s bezpečnosťou	Centrálna detekcia a kontrola správ udalostí v reálnom čase - Na vyhodnocovanie udalostí súvisiacich s bezpečnosťou je potrebné použiť centrálne komponenty vykonávajúce automatizované analýzu týchto udalostí. Softvérovými nástrojmi sú použité na zaznamenávanie, korelovanie a vizualizovanie všetkých udalostí vyskytujúcich sa v systémovom prostredí. Musia sa definovať prahové hodnoty potenciálne nebezpečných udalostí pri ktorých sa spúšťa automatický alarm. Je potrebné, aby personál bol kvalifikovaný a schopný okamžite iniciovať kvalifikovanú a citlivú reakciu. Je potrebné pravidelne kontrolovať parametre analýzy a v prípade potreby by sa mali upraviť. (nástroj Security information and event manažmentu - SIEM)	64-A/A	Silvester IT špecialista 1. Jozef IT špecialista 2.	15.09.2022
Detekcia udalostí súvisiacich s bezpečnosťou	Použitie systémov detekcie prienikov - IDS alebo systému prevencie prienikov - IPS	64-A/A	Peter Vedúci technológ ICS. Jozef IT	01.10.2022

Záznam vygenerovaný dňa: 14.01.2022

ISIT SK SOFTWARE cybersecurity

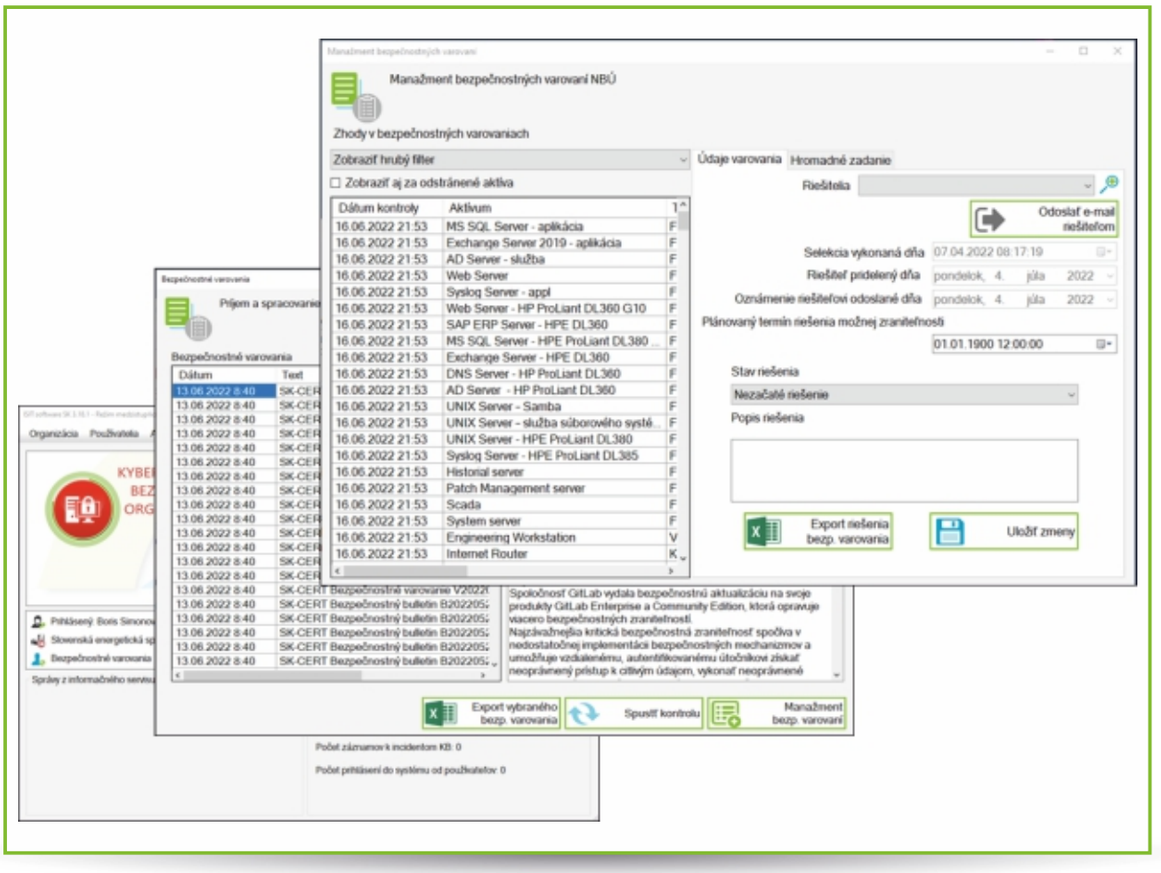
MANAŽMENT BEZPEČNOSTNÝCH VAROVANÍ z SK CERT NBÚ SR

V module KBO je integrovaná dôležitá funkcionalita vo forme nástroja umožňujúceho účinné predchádzanie negatívnym dopadom kybernetických hrozieb na informačné systémy, resp. informačno-komunikačné technológie, pomocou semi-automatického príjmu a spracovania bezpečnostných varovaní emitovaných SK-CERT NBÚ SR. Nástroj v polo-aktívnom režime vykoná vyhľadávanie v registri aktív prevádzkovateľa tie aktíva, ktoré majú vysokú relevanciu ku kritickým zraniteľnostiam uvedených v bezpečnostných varovaniach SK-CERT NBÚ SR. V prípade pozitívneho výsledku vyhľadávacieho procesu nástroj ponúka možnosť upovedomenia vlastníka/správcu aktíva na nutnosť kontroly a zavedenia nápravných opatrení na elimináciu kritickej zraniteľnosti spravidla informačného technického aktíva v jeho zodpovednosti.

S prihliadnutím na dôležitosť riadenia bezpečnostných varovaní ku konkrétnym aktívam organizácie, sme tento proces zvolili ako semi-automatický, teda s nevyhnutnosťou kontroly/zásahu manažéra KB.

Tri základné kroky:

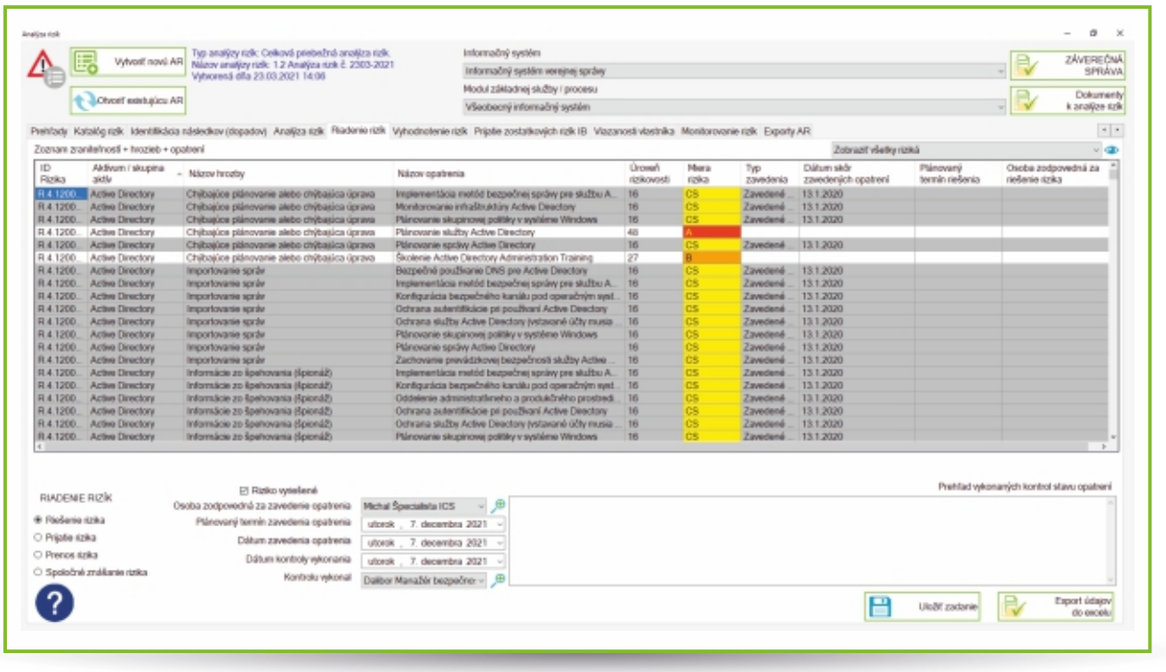
- **Príjem, publikácia a archivácia bezpečnostných varovaní;**
- **Kontrola potenciálne ohrozených informačných aktív kritickými zraniteľnosťami a emitovanie upozornení pre ich vlastníkov / správcov;**
- **Správa / manažment varovaní a nápravných opatrení.**



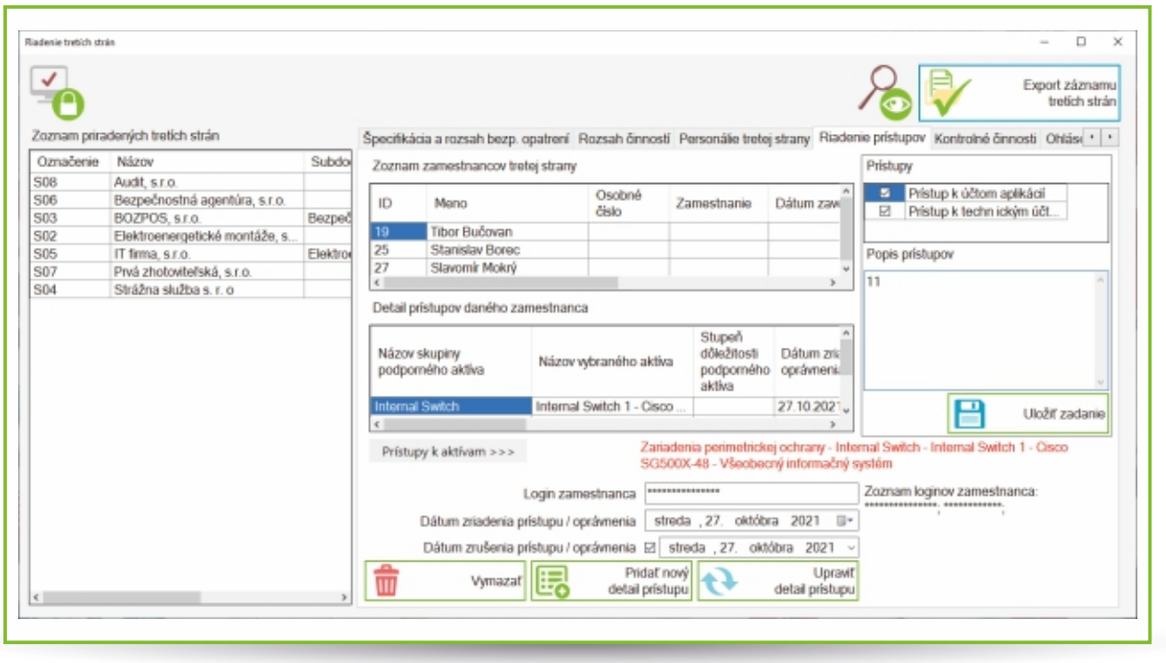
ISIT SK SOFTWARE cybersecurity

VYBRANÉ UKÁŽKY Z MODULU KBO

Riadenie rizík



Riadenie prístupov tretích strán



ISIT SK SOFTWARE cybersecurity

PRIPRAVENOSŤ MODULU KBO NA ROZŠÍRENIE REGULOVANÝCH ODVETVÍ O NOVÉ REGULOVANÉ SLUŽBY V ZMYSLE SMERNICE NIS2

Modul KBO aplikácie ISIT SOFTWARE SK/CZ obsahuje základné komponenty – aktíva OT/ICS systémov zraniteľné kybernetickými útokmi, tie to sú priebežne doplňované a rozširované o nové komponenty v zmysle odporúčaní medzinárodných profesne zameraných noriem.

Modul KBO spĺňa parametre riadenia procesov kybernetickej bezpečnosti ako podľa národnej tak aj európskej legislatívy a medzinárodných noriem, teda je pripravený na prácu pre každého manažéra KB resp. povinný subjekt v oblasti kybernetickej bezpečnosti.

Bližšie informácie: www.analyza-rizik.eu

ISIT SK SOFTWARE cybersecurity

Modul HELPDESK pre riadenie bezpečnosti

- Samostatný modul, ktorý slúži ako účinný nástroj k predchádzaniu vzniku bezpečnostných incidentov

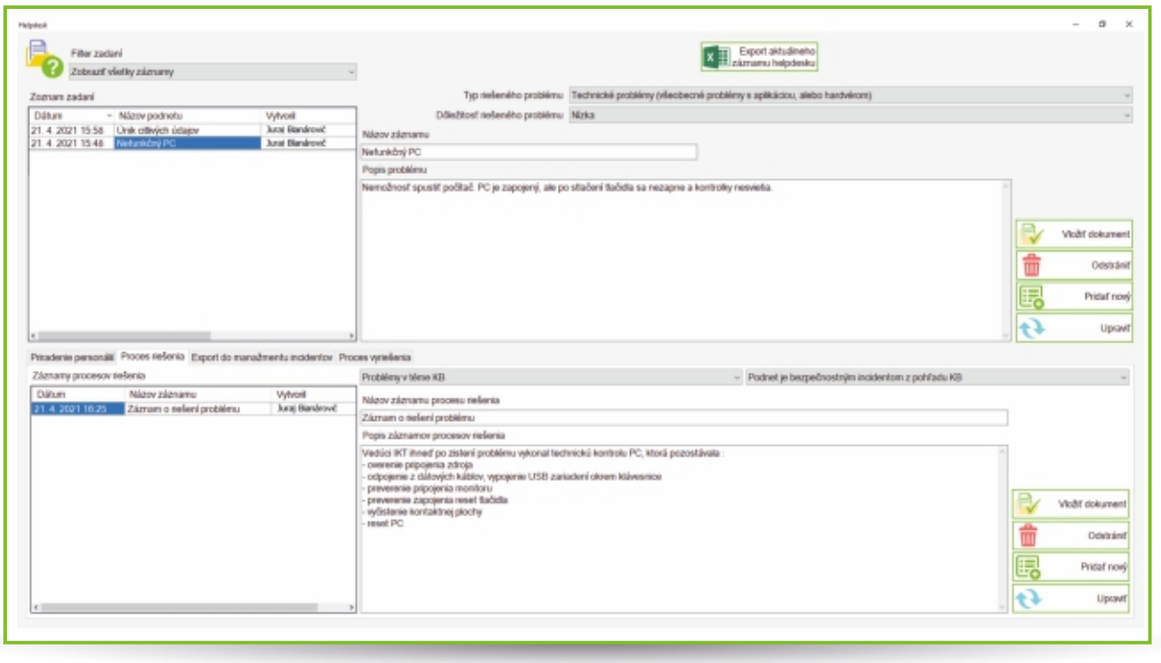
- Zaznamenáva životný cyklus udalosti od jeho vzniku, cez hlásenie, realizáciu až po vyriešenie vrátane personálneho obsadenia a kontroly

- Užívateľ vyberá z databázy o aký typ problému ide, upresní záznam k problému, aké dáta boli zasiahnuté, popis možnej škody, dopad a odhad závažnosti, zasiahnuté aktíva, riešenie problému a nápravné opatrenia

- Výstupom je súhrnná evidencia a prehľad riešenia udalosti / problému s postúpením správcovi systému a možností

- V prípade detekcie udalosti, ktorá je incidentom, prechádza kompletná informácia do manažmentu bezpečnostných incidentov

Ukážka z Helpdesku – Proces riešenia



ISIT SK SOFTWARE cybersecurity

Modul GDPR (eGDPR, GDPR s DPIA)

Samostatný modul na riadenie procesov ochrany osobných údajov vrátane väzieb posúdenia vplyvu (DPIA)

EVIDENCIE INFORMAČNÝCH SYSTÉMOV (AGEND, SPRACOVATEĽSKÝCH ČINNOSTÍ)

- Povinné info – názov, účel, právny základ, lehota spracúvania, rozsah OU, OD, spracovateľské operácie, príjemcovia, tretie strany, oprávnené osoby atď

ZOZNAMY A TLAČOVÉ ZOSTAVY

- Zamestnancov, oprávnených osôb, sprostredkovateľov, zodpovedných osôb, dotknutých osôb s archívom súhlasov, množstvo tlačových zostáv

MANAŽMENT BEZPEČNOSTNÝCH INCIDENTOV

- Komplexné riadenie incidentov s tlačovou zostavou ku každému incidentu a generovaním hlásenia pre dozorný orgán

BEZPEČNOSTNÁ DOKUMENTÁCIA

- Z údajov v softvéri sa generuje dokumentácia – záznam o spracovateľských činnostiach, smernice, kľúčový poriadok, poučenia oprávnených osôb ku konkrétnym účelom, odpovede dotknutých osobám, informácie o likvidácii, informačná povinnosť a i.

AUTOMATIZOVANÝ AUDITNÝ MODUL

- Kontrolný nástroj na zistenie nezhôd v riadení ochrany OÚ v organizácii s generovaním správy z interného auditu s grafickým percentuálnym znázornením aktuálneho stavu nastavenia ochrany OÚ v organizácii.

VÄZBY POSÚDENIA VPLYVU (DPIA)

- Obsahuje jednak evidenčnú časť aktív, cez hrozby, zraniteľnosti, hodnotu rizika až po ochranné opatrenia s generovaním výstupu

TEST PROPORCIONALITY

- Podrobne spracovaný test proporcionality pri oprávnenom záujme špeciálne pre kamerové monitorovacie systémy

KAMEROVÝ MONITOROVACÍ SYSTÉM

- Podľa nového usmernenia EDPB platného od 29.1.2020 s možnosťou generovania tabuľky označenia 1. vrstvy

eLearning

- Obsahuje prístup k okruhom školení so skúškou a osvedčením pre absolventa pre jednotlivé okruhy tém ochrany citlivých dát

ISIT SK SOFTWARE cybersecurity

KAMEROVÉ MONITOROVACIE SYSTÉMY

Samostatný podmodul v Module GDPR je v súlade s hlavným usmernením EDPB č. 3/2019 zo dňa 9.1.2020 ku kamerovým monitorovacím systémom.

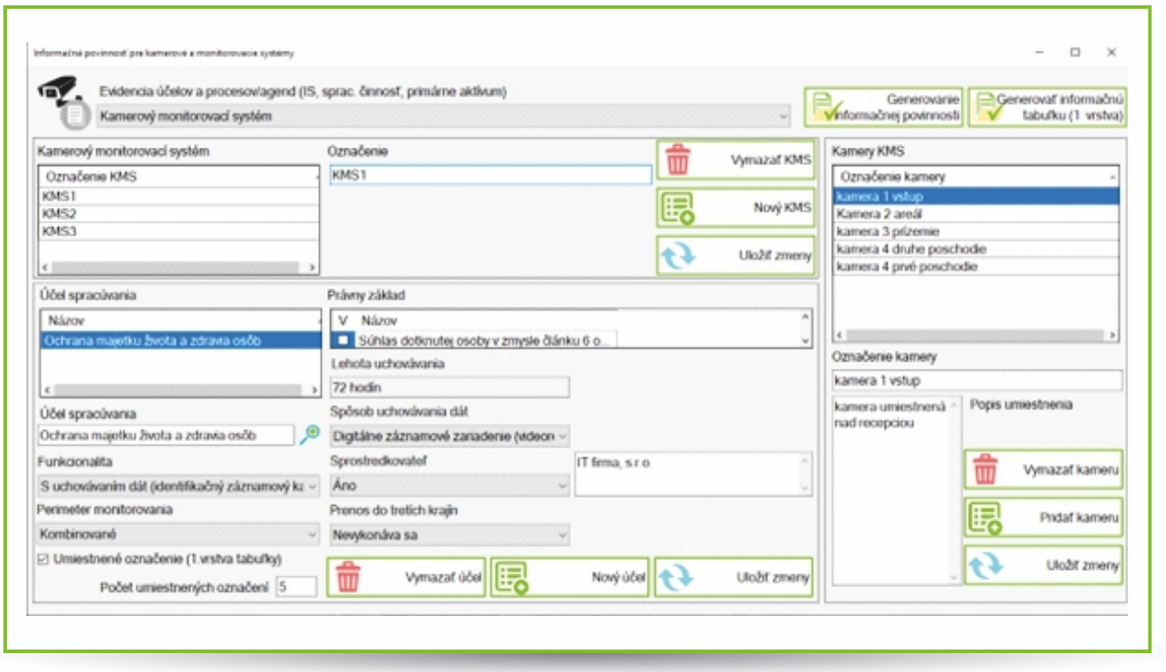
Obsahuje:

- Evidencie účelov, právnych základov spracúvania, spôsobu a perimetra monitorovania, evidencie jednotlivých kamier, umiestnenia a popis kamier, lehôt uchovávania, prístupov pre oprávnené osoby, sprostredkovateľov, práv dotknutých osôb
- Eviduje dokumentáciu pre KMS (napr. architektúra KMS, perimeter monitorovania – polohy kamier a iné)
- Obsahuje pripravené testy proporcionality s generovaním výsledku
- Automatické upozornenia na lehoty pri pravidelnom prehodnocovaní testov proporcionality
- Generovanie kompletnej informačnej povinnosti pre kamerové systémy (2. vrstva)
- Generovanie 1. vrstvy tabuľky s povinnými náležitosťami (viď obrázok)
- Výstupom môže byť samolepka alebo podklad pre inú formu grafického výstupu

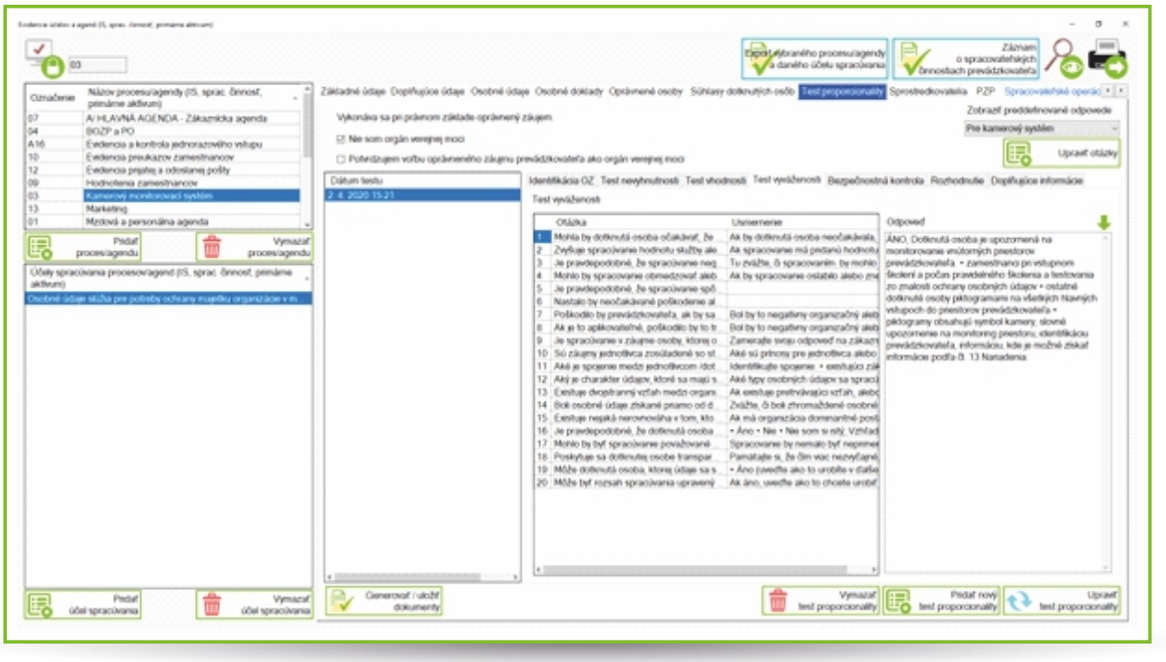
Označenie 1. vrstvy - Dôležité !! Kompletný popis prvej vrstvy - nestačí len piktogram kamery !

ISIT SK SOFTWARE cybersecurity

Evidencie KMS – Generovanie Informačnej povinnosti

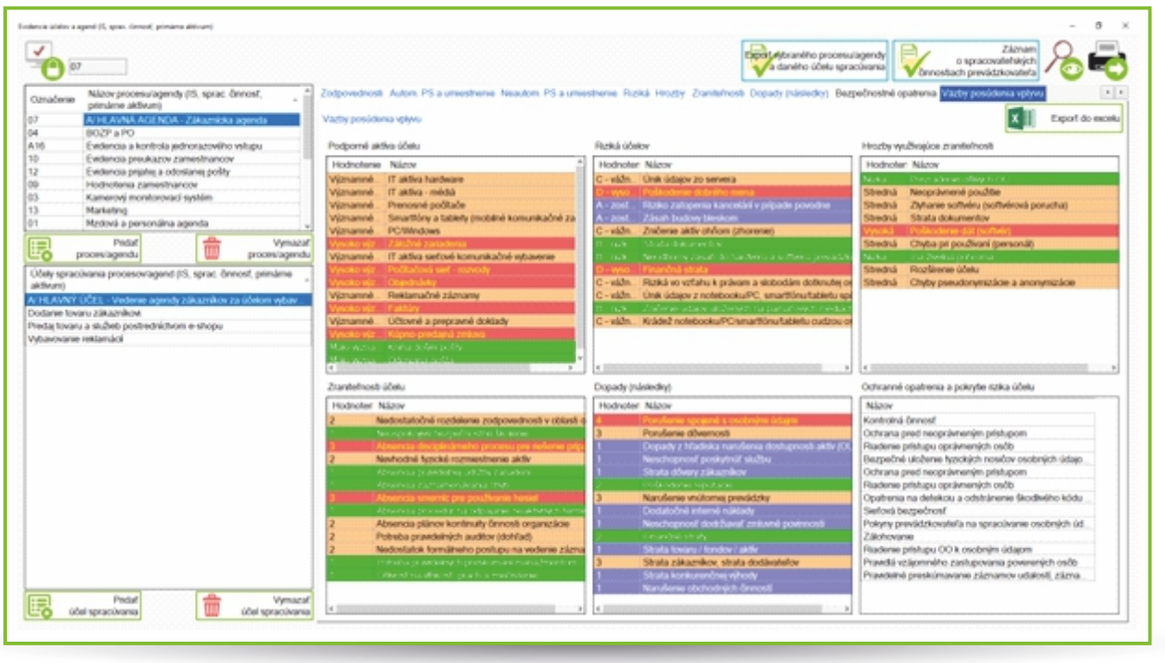


Test proporcionality - Dôležité !! Test je nevyhnutný pri každom Účele/agende, kde je určený právny základ Oprávnený záujem prevádzkovateľa



VYBRANÉ UKÁŽKY Z MODULU GDPR

Evidencie agend/procesov – Väzby posúdenia DPIA



Prínos používania softvérového modulu GDPR pre prevádzkovateľa:

- Absolútny prehľad o všetkých agendách, účeloch a procesoch s generovaním povinných výstupov – dokumentácia je aktuálna v danom čase , " nedegraduje v čase "
- Plný manažment poučení oprávnených osôb ku konkrétnym účelom podľa funkčných miest
- Súčasťou sú školenia pre oprávnené osoby a návštevy (tretie strany)
- Garancia legislatívneho súladu riadenia ochrany OU pre Zodpovednú osobu, štatutára a pri výkone kontroly dozorným orgánom, plná podpora autorov aplikácie
- Široká funkcionalita s prechodom do kybernetickej bezpečnosti
- Bohato naplnené číselníky so vzormi podľa zamerania prevádzkovateľov (verejná správa, školy, komerčné spoločnosti - obchod, výroba, eshop, ekonomika, služby a i)

Viac informácií získate na **www.isitslovakia.sk**

ISIT SK SOFTWARE cybersecurity

Modul WHISTLEBLOWING s riadením korupčných rizík

- **Kľúčové zmeny podľa Smernice EP a Rady EU č. 2019/1937 zo dňa 23. 10. 2019 o ochrane osôb, ktoré oznamujú porušenia práva Unie (smernica o whistleblowingu)**

- **Zmena z formálneho riadenia protikorupcie na funkčný systém whistleblowingu**

- **Dôraz na dôvernosť a bezpečnost podania oznamovateľa, ochrana jeho totožnosti, dôvernosť spracovania a vyhodnotenia oznámení spolu s požiadavkami na organizáciu a riešiteľa/auditora**

- **Účinná ochrana pred odvetnými opatreniami**

- **Elektronická časť oznamovacieho procesu musí byť riešená dôverným spôsobom, čo nedokáže garantovať emailové oznamovanie, ale výhradne softvérová aplikácia s web nahlasovacím formulárom a manažérskou konzolou pre riadený proces spracovania Oznámení.**

Riešenie VOS WB v module ISIT software SK/CZ:

Povinný subjekt má umiestnený odkaz na VOS WB na svojej web stránke, prostredníctvom ktorej ľubovoľný Oznamovateľ môže bezpečne s garanciou dôvernosti nahlásiť svoj Podnet s voľbou anonymného alebo chráneného oznámenia. Každé oznámenie má pridelený jedinečný ID, prostredníctvom ktorého sa môže dobrovoľne zidentifikovať aj anonymný oznamovateľ pre prechod do pozície chráneného oznamovateľa.

Aplikačnú časť softvérového modulu má inštalovanú Audítor / skupina Audítorov, ktorá prijíma, procesuje a vyhodnocuje všetky Oznámenia.

Dôvernosť pri spracúvaní je garantovaná administráciou portálu so zabezpečeným uchovávaním dát.

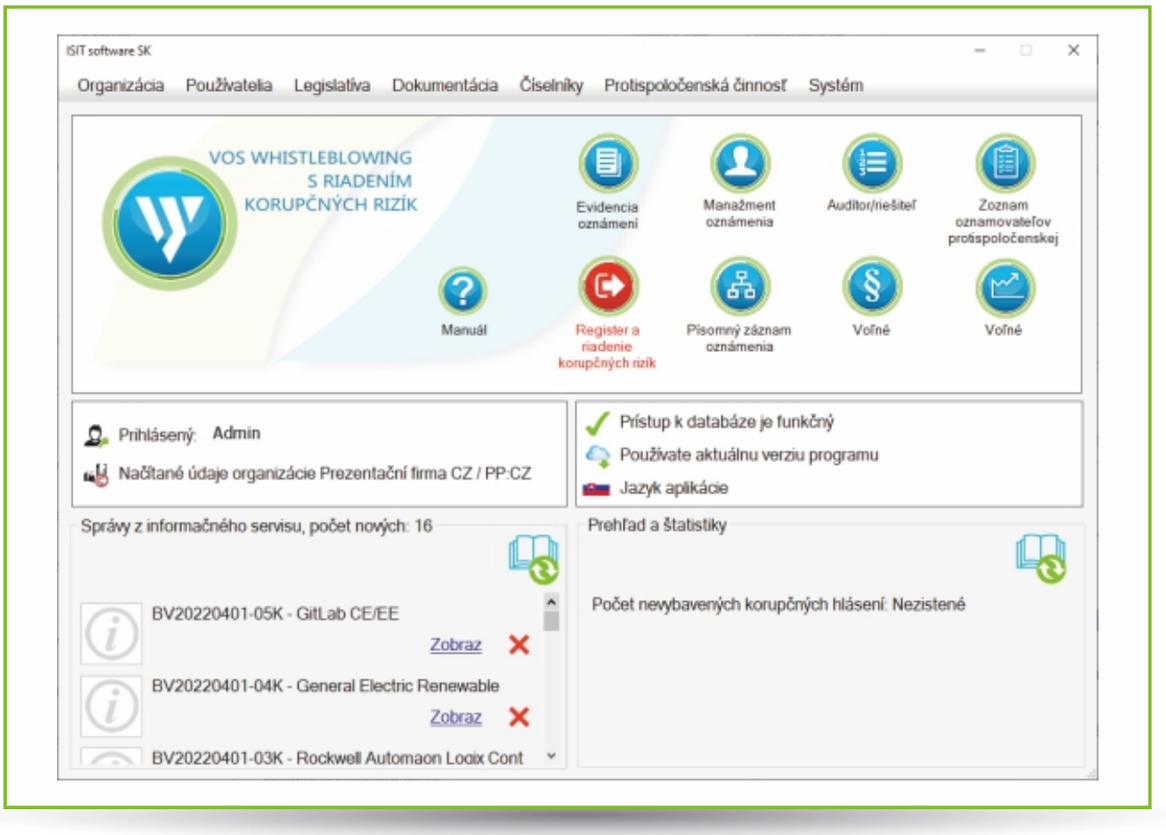
Riešenie je postavené ako na multiadmin platforme, kde jeden Audítor / právnická kancelária môže realizovať činnosť Whistleblowingu pre viacerých klientov pri dodržaní všetkých bezpečnostných parametrov tak aj na individuálnom riešení pre 1 konkrétnu organizáciu.

Viac informácií získate na **www.whistleblowing-software.eu**

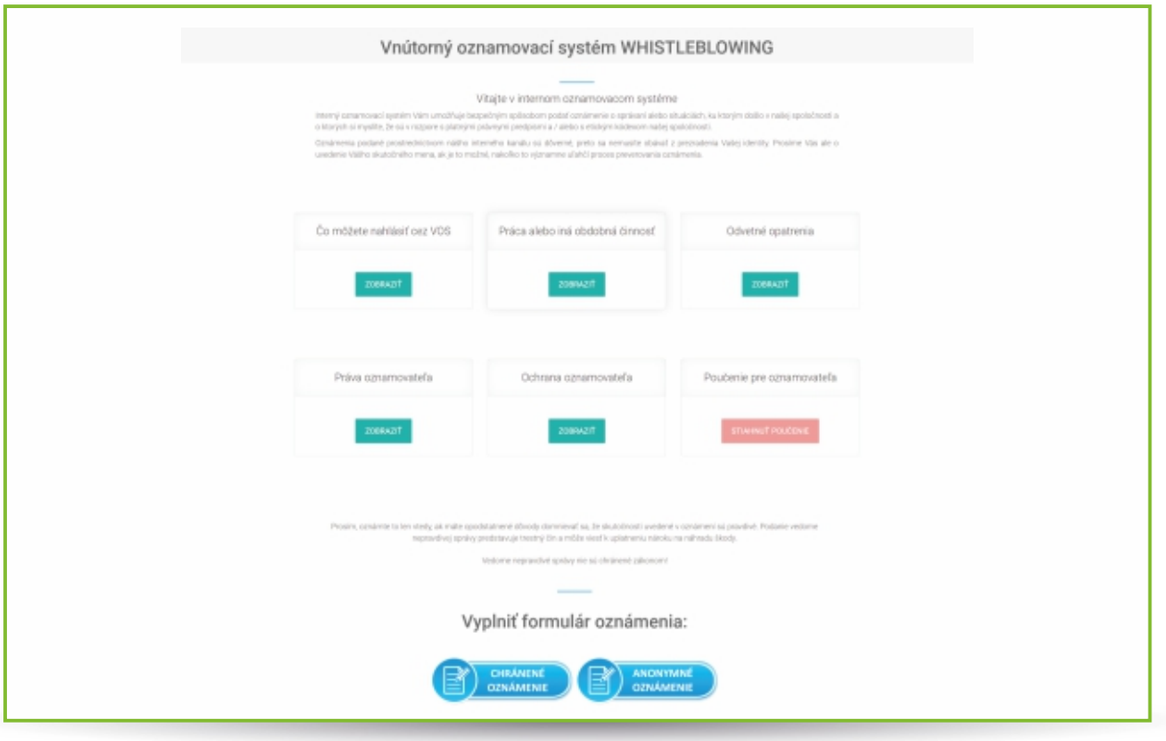
ISIT SK SOFTWARE cybersecurity

VYBRANÉ UKÁŽKY Z MODULU VOS WB

Úvodné okno modulu VOS WB (manažérska konzola)



Ukážka formuláru hlásenia (webklient)



E-LEARNING

E-learning ako webová služba v licencii ISIT software SK/CZ predstavuje moderný spôsob pre efektívne zdelávanie zamestnancov, konkrétne v oblasti ochrany osobných údajov/GDPR, Kyberbezpečnosti, riadení korupčných rizík a whistleblowingu. Prostredníctvom kurzov je možné jednoduchým spôsobom poskytnúť amestnancom všetky potrebné informácie a overiť ich znalosti skúškou. Tvorcovia kurzov sú držitelia certifikátov interný audítor, lead auditor v príslušnej oblasti s dlhoročnou praxou. Lekcie v kurzoch vieme doplniť podľa interných riadiacich aktov zákazníka

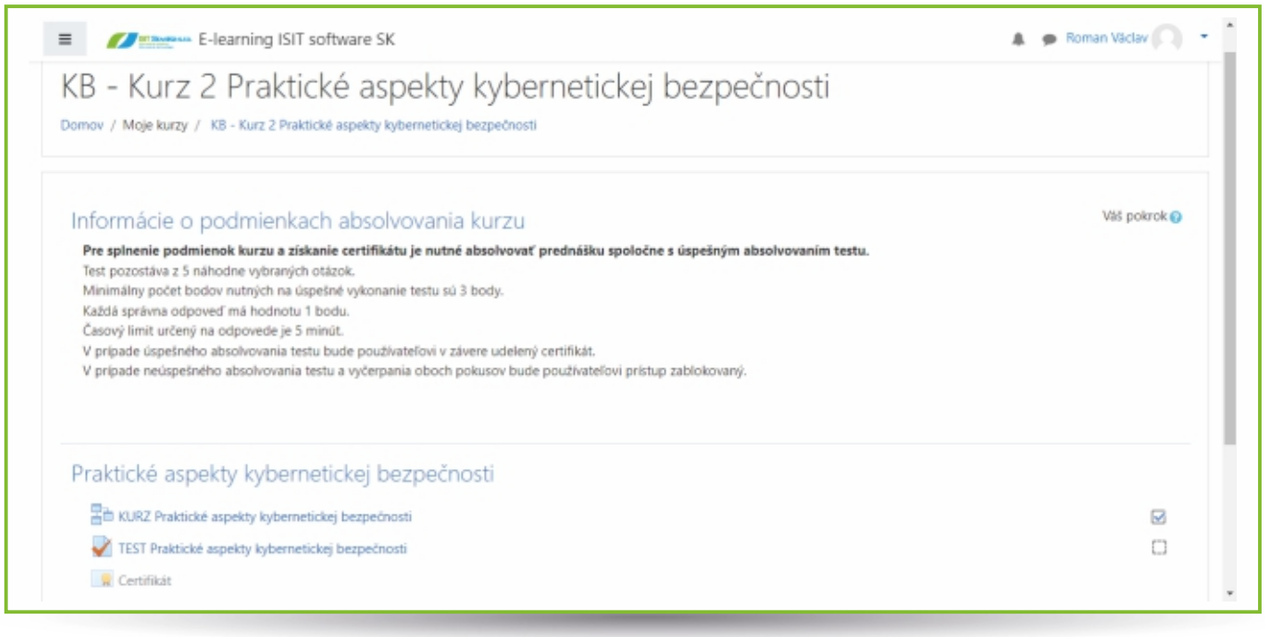
E-learningové kurzy poskytujú:

logickú postupnosť školenia po kapitolách
obsah podľa platnej legislatívy
priebežné overovanie vedomostí
záverečné overenie vedomostí testom (výber náhodných 5 otázok, 3 odpovede musia byť správne, ak sú nesprávne, ešte sú 2 opakovania testu)
generovanie osvedčenia o úspešnom absolvovaní školenia

E-learning ako služba v blokoch GDPR, KBO, Whistleblowing:

vzdelávanie administruje ISIT Slovakia s.r.o.
zákazník získava vygenerované klientske prístupy pre všetkých účastníkov na prístup do webslužby (email účastníka + vstupné heslo)
platená služba; doplnkovo možnosť naprogramovať lekcie podľa interných smerníc zákazníka
doplňujúci bonus – pri objednaní elearnigovej služby zákazník získava 10% zľavu na každé ďalšie služby a produkty našej spoločnosti (audit, školenia, ISIT software SK)

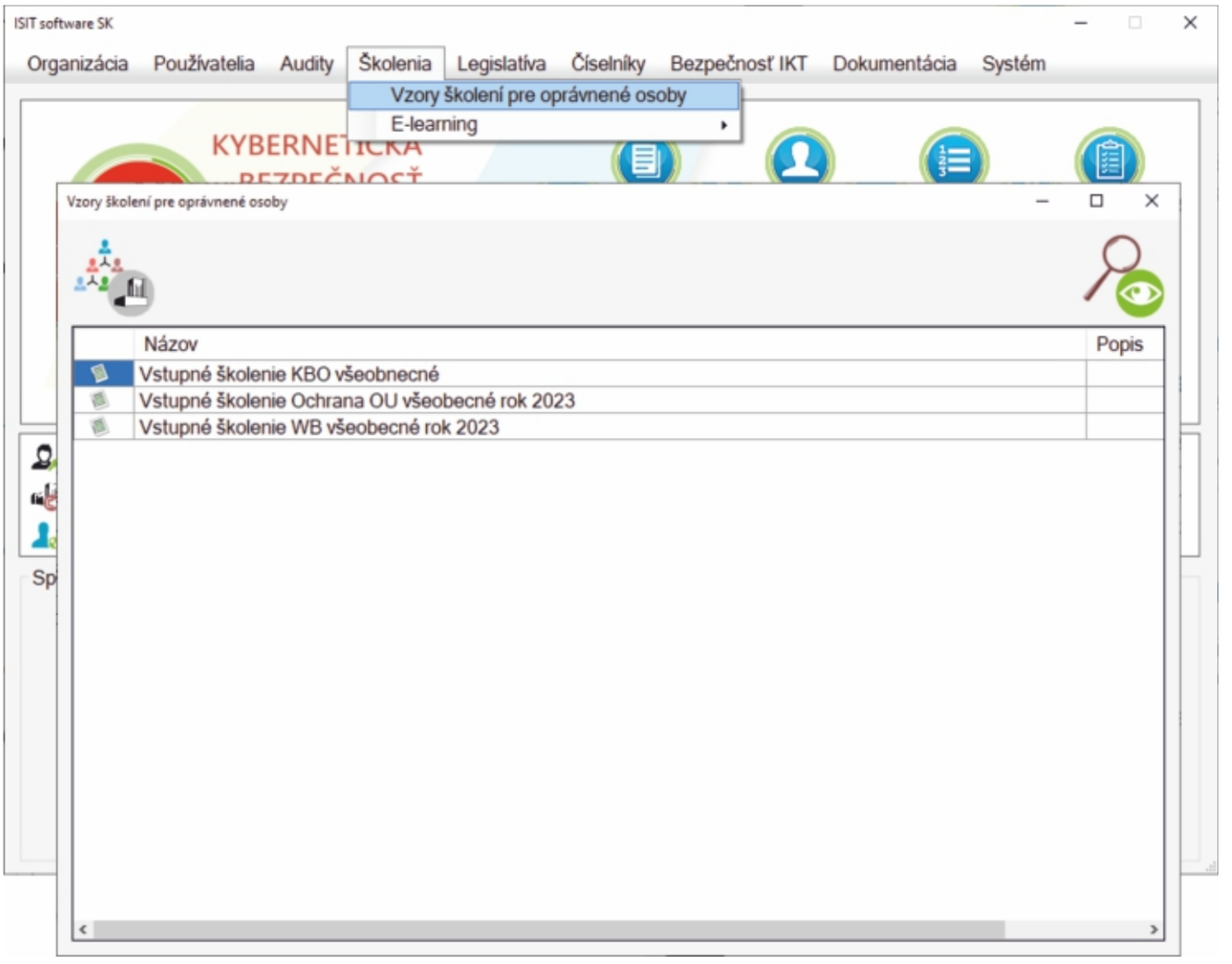
Ukážka z Elearningu – Kurz KB



BEZPEČNOSTNÝ PORTÁL ISIT

Bezpečnostný portál ISIT je samostatnou web aplikáciou, ktorá môže byť súčasťou web stránky povinného subjektu alebo jeho intranetu a je určená pre zamestnancov a zamestnancov dodávateľov povinného subjektu. Portál je prístupný aj na stránke **www.isitslovakia.sk** pre našich registrovaných zákazníkov, ktorým poskytujeme odborné služby (externá Zodpovedná osoba, externý manažér KB) . Slúži na okamžité a zároveň personalizované nahlasovanie udalostí súvisiacich s témou GDPR a KYBE pre internú alebo externú Zodpovednú osobu, manažéra KB , bezpečnostný výbor a iné určené osoby dôverným spôsobom. Z tohto portálu je možné špecialistom GDPR/KYBE buď spracovať parciálne všetky oznámené informácie, alebo využiť prepojenie na jednotlivé časti konkrétnych modulov aplikácie ISIT SOFTWARE SK/CZ na automatizáciu všetkých činností pri dodržaní termínov riešenia a zároveň o konkrétne naplnenie požiadaviek na personálne, technické a organizačné opatrenia pre zabezpečenie parametrov dôvernosti, dostupnosti a integrity .

ODBORNÉ ŠKOLENIA



Školenia pre zamestnancov organizácie:

- V každom module aplikácie ISIT SOFTWARE SK/CZ je preklik na vypracované školiace materiály GDPR, KYBE, WB
- Možnosť pripraviť video prezentácie ako vstupné školenia pre nových zamestnancov
- Elearningové vzdelávanie (popísané v samostatnej časti katalógu)
- školenia v moduloch GDPR, KYBE a WB sú pre držiteľov licencie bezplatne k dispozícii
- prezenčné školenia priamo pre zamestnancov (vedenie organizácie, stredný manažment) „na mieru“ procesov a riadiacich aktov organizácie. Ide o absolvovanie povinných preškolení v jedno alebo dvojročných intervaloch so zhrnutím noviniek v danej téme a zavedených pravidiel aj s vystavením osvedčení o absolvovaní školenia, pričom hlavným účelom je budovanie a udržiavanie bezpečnostného povedomia v organizácii. Cielené školenia akceptujú dozorné orgány ako účinné ochranné opatrenie.

Bližšie informácie: www.vaclav.sr

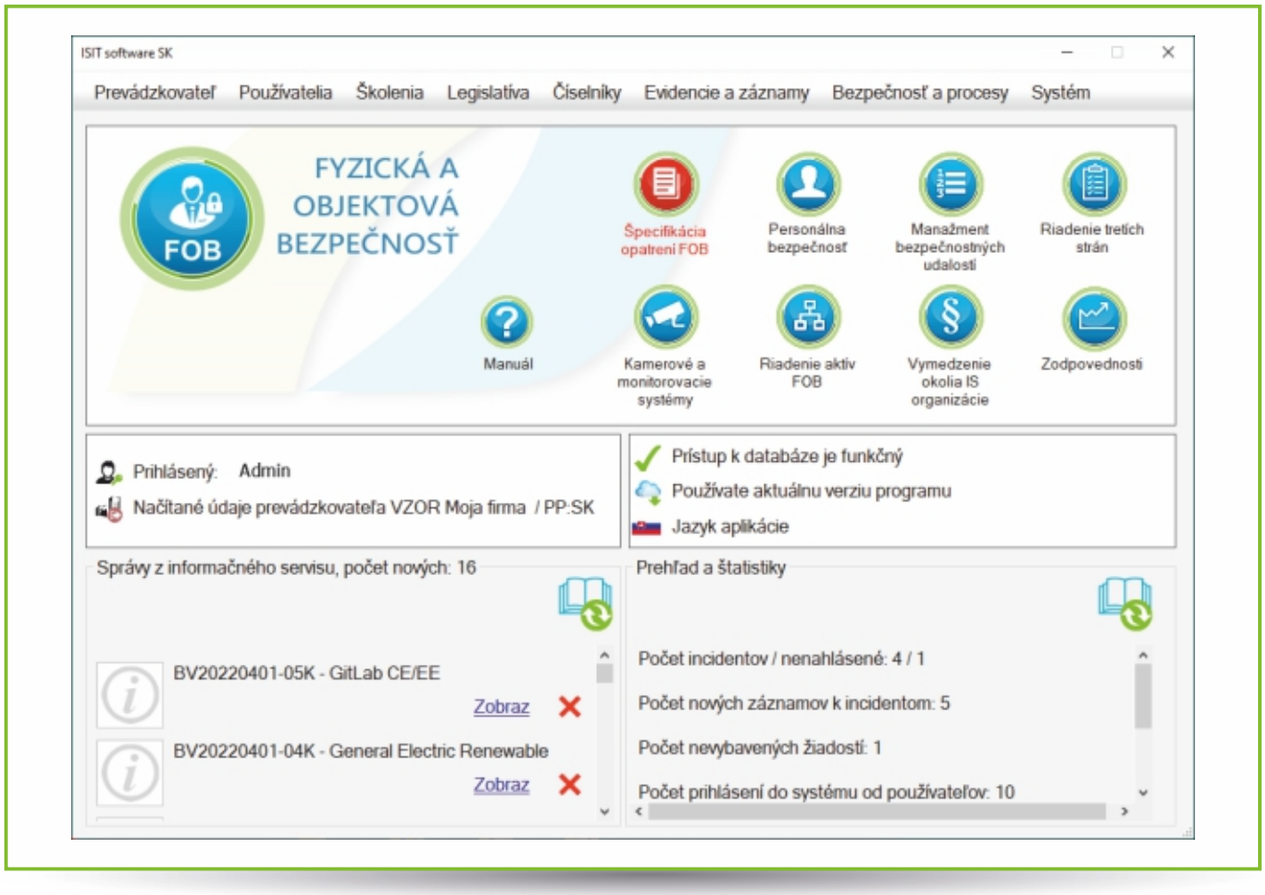
Modul FYZICKÁ A OBJEKTOVÁ BEZPEČNOSŤ

Pre rok 2022 pripravujeme nový modul procesnej aplikácie ISIT software SK/CZ zameraný na komplexné riadenie ochrany fyzickej a objektovej bezpečnosti (FOB). Používateľmi modulu sú najmä bezpečnostný riaditeľ s pracovníkmi vrátane štatutára organizácie, veliteľ a výkonná časť obecnej polície alebo SBS, odbory bezpečnosti a krízového riadenia a pod.

V jednotlivých segmentoch Personálna bezpečnosť, Riadenie tretích strán, Manažment bezpečnostných udalostí, Špecifikácia opatrení FOB, Vymedzenie okolia IS organizácie, Riadenie Aktív FOB poskytuje plnohodnotný support pre povinné osoby s podrobnými podkapitolami určenými pre kamerové a monitorovacie systémy s výstupmi pre kontrolné, dozorné orgány a súčinnosť s policajným zborom, riadením prístupov vrátane kľúčového poriadku, zabezpečením chránených priestorov (objektov a okolia), evidenčných častí aktív bezpečnosti atď.

Tento modul je prierezovým zjednocujúcim riešením pre každú organizáciu so zameraním na všeobecné riadenie FOB, teda bez legislatívnych vymedzení podľa GDPR alebo KBO.

Modul FOB možno považovať za procesný model riadenia obecnej FOB v organizácii ako predstupňa riadenia FOB podľa zákona o utajovaných skutočnostiach podľa príslušnej národnej legislatívy.



ISIT SK SOFTWARE cybersecurity

ISIT SK SOFTWARE cybersecurity					
RIEŠI TÉMU	**KYBERNETICKÁ BEZPEČNOSŤ**	**WHISTLEBLOWING** (Protispoločenská činnosť pri porušovaní práv Únie)	**GDPR – OCHRANA OSOBNÝCH ÚDAJOV**	**E-LEARNING**	**HELPDESK**
STRUČNÁ ANOTÁCIA MODULOV	Samostatný modul na riadenie procesov KB, generovanie výstupov, dokumentácie, smerníc – záverečnej správy s prehlásením o aplikovateľnosti (Statement of Applicability - SOA), vrátane evidencií Pracovný nástroj manažéra KB s presahom na vlastníkov aktív	Vnútorný oznamovací systém na bezpečné nahlasovanie porušení práv Únie a ochrane oznamovateľov a manažérska konzola na procesovanie udalostí Pracovný nástroj pre audítora / pověřenú osobu	Modul na riadenie procesov ochrany osobných údajov Elektronický záznam o sprac. činnostiach Generovanie povinnej dokumentácie Pracovný nástroj pre Zodpovednú osobu / DPO / Pověřenca	Vzdelávací nástroj na budovanie a udržiavanie bezpečnostného povedomia k jednotlivým modulom Testovanie užívateľov vrátane generovania osvedčenia o úspešnom absolvovaní	Modul na riadenie bezpečnostných udalostí v organizácii
VÝNIMOČNOSŤ	Komplexný proces riadenia kybernetických a informačných rizík, Automatizovaná Analýza rizík, Riadenie a prístup k aktívam, Systémové riadenie tretích strán, BIA – dopadová analýza	Bezpečné a dôverné nahlasovanie udalostí s ochranou oznamovateľov a systémovým bezpečným riadením procesu whistleblowingu	Procesné komplexné riadenie ochrany OÚ s množstvom výstupov do povinnej dokumentácie s udržiavaním v aktuálnom stave	Plná podpora e-vzdelávania v oblasti KB, GDPR, Whistleblowingu a ďalších oblastí	Samostatná platforma na riadenie akýchkoľvek bezp. udalostí s výstupmi na management BI
PRIDANÁ HODNOTA	Manažment bezpečnostných incidentov (MBI) Implementovaný Infoservis – príjem a spracovanie bezpečnostných varovaní poskytovaných Národným centrom	Podmodul riadenia korupčných rizík podľa ISO 37001	Interný auditný modul, Väzby posúdenia vplyvu (DPIA), Testy proporcionality, kamerové IS s generovaním I. vrstvy	Vypracované lekcie s kolekciami testových otázok kompetentnými autormi / audítormi z jednotlivých oblastí	Praktický manažment ľubovoľných bezpečnostných udalostí / udalostí v organizácii s členením na MBI GDPR a MBI KBO

LEGISLATÍVA EÚ, SK/CZ, Medzinárodné normy	**EÚ:** Smernica 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 **SR:** Zákon č. 69/2018 Z. z., Zákon č. 95/2019 Z. z., vrátane príslušných vyhlášok, **ČR:** Vyhláška č. 82/2018 Sb. **Medzinárodné normy:** ISO/IEC 27001:2013 ISO/IEC 27002:2013 ISO/IEC 27005:2013 ISO/IEC 27799:2013	**EÚ:** SMERNICA EURÓPSKEHO PARLAMENTU A RADY (EÚ) 2019/1937 z 23. októbra 2019 o ochrane osôb, ktoré nahlasujú porušenia práva Únie, **SR/ČR:** Metodika MSČR, počas r. 2022 bude vydaná národná legislatíva ČR/SR, **Medzinárodné normy:** Norma ISO 37001	**EÚ:** Nariadenie 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) **SR:** Zákon č. 18/2018 Z. z., Vyhláška 158/2018 Z. z. **ČR:** Zákon č. 110/2019 Sb.	▪ 18/2018 Z. z. zákon o ochrane osobných údajov ▪ 69/2018 Z. z. zákon o kybernetickej bezpečnosti ▪ 95/2019 Z. z. zákon o informačných technológiách vo verejnej správe	▪ Nariadenie 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) ▪ 69/2018 Z. z. zákon o kybernetickej bezpečnosti
ŠKÁLOVATEĽNOSŤ	Web klient MBI Manažérska konzola (hrubý klient), centrálna databáza pre n hrubých klientov	VOS Web klient Manažérska konzola (hrubý klient)	Web klient MBI Manažérska konzola (hrubý klient), centrálna databáza pre n hrubých klientov	Ľubovoľný počet užívateľov (študentov)	Web klient Manažérska konzola
IT RIEŠENIE (autonómne licencovanie pre každý modul samostatne)	▪ ADMIN – n KLIENT ▪ MULTIADMIN – 1 až 250 ADMIN – n KLIENT	▪ ADMIN – n KLIENT ▪ MULTIADMIN – 1 až 250 ADMIN – n KLIENT	▪ ADMIN – n WEB KLIENT ▪ MULTIADMIN – 1 až 250 ADMIN – n WEB KLIENT	▪ Webová služba	▪ ADMIN – n WEB KLIENT ▪ MULTIADMIN – 1 až 250 ADMIN – n WEB KLIENT
PODPORA, SLUŽBY	Komplexné externé služby, implementácia v prostredí zákazníka Maintenance do 15% z obstarávacej ceny	Komplexné externé služby, implementácia v prostredí zákazníka Maintenance do 15% z obstarávacej ceny	Komplexné externé služby, implementácia v prostredí zákazníka Maintenance do 15% z obstarávacej ceny	Administrácia portálu	Komplexné externé služby, implementácia v prostredí zákazníka Maintenance do 15% z obstarávacej ceny

Pomôcka pre zodpovedné osoby, štatutárov organizácií, personalistov, manažérov KYBE, pracovníkov IT.

Softvér vedie evidencie, zoznamy, generuje dokumenty, obsahuje vzory dokumentov, archivuje verzie, zaznamenáva logy.

Pravidelná aktualizácia a upgrade od autorov v súlade s platnou legislatívou. Dôležité upozornenia.

Poradenstvo a podpora špecialistov - audítorov IB. Individuálne riešenia. Služby na kľúč.

Technická a zákaznícka podpora. Zaškolenie k obslužnosti. Návody a používateľské príručky.

Nepretržitý vývoj aplikácie s dôrazom na bezpečnosť.

- V súčasnosti cca **2500 zákazníkov** pre oblasť GDPR vrátane základných a stredných škôl, miest a obcí v SR a desiatky zákazníkov pre oblasť KYBE a Whistleblowingu
- **Referenční zákazníci:** Finančná správa SR, Štatistický úrad SR, Úrad na ochranu os. údajov SR, Úrad pre reg. sieťových odvetví, Úrad komisára pre deti SR, Duslo Šaľa a.s., SEPS a.s., UP CZ a.s., Elektrárny Opatovice, a.s., Český hydrometeorologický ústav, a i. Na VUT Brno fakulta podnikatelská vo verzii Edukit slúži softvér ako výučbový nástroj pre študentov, manažérov kybernetickej bezpečnosti, ŠVPS SR + 40 RVPS, Min. dopravy SR, MPSVaR SR, Slovenská pošta a i.
- **Aktuálne ceny a možnosti prenájmu licencií** nájdete na **www.isitslovakia.sk**

QR kód k produktovému katalógu modulu KBO

Viac informácií o softvéri nájdete na našich web stránkach:

www.isitslovakia.sk
www.analyza-rizik.eu
www.whistleblowing-software.eu

Kontakt: info@isitslovakia.sk | 0910 905 154

Analýza Rizík ISIT Software Sk Cybersecurity