Modul Kybernetická bezpečnost organizace (KBO) jako součást znalostního softwaru ISIT software CZ určený pro komplexní řízení procesů bezpečnosti v organizaci

K hlavním tématům konference ISSS22, mezi které patří Řízení a rozhodování na základě dat, Rozvoj komunikační infrastruktury, Elektronizace zdravotnictví, Digitalizace specifických oblastí veřejné správy je zařazena také Kybernetická bezpečnost a krizové řízení.

ISIT SOFTWARE CZ s.r.o. s partnerem ATS-TELCOM PRAHA a.s. na konferenci ISSS2022 prezentuje moderní softwarové řešení **ISIT software CZ** a jeho procesně samostatný nástroj - **Modul Kybernetická bezpečnost organizace.** Pro úplnost je nutno poznamenat, že softwarové řešení **ISIT software CZ** kromě již zmíněného modulu Kybernetická bezpečnost organizace, se skládá také z dalších nástrojů, samostatných modulů zaměřených na řízení bezpečnosti dle legislativních okruhů – GDPR, Whistleblowing, Helpdesk, Elearning, Fyzická a objektová bezpečnost.

Kybernetická bezpečnost pomáhá identifikovat, hodnotit a řešit hrozby v kyberprostoru, snižovat kybernetická rizika a eliminovat dopady kybernetických útoků, které se realizují prostřednictvím informační kriminality, kyberterorismu a kybernetické špionáže ve smyslu posilování důvěrnosti, integrity a dostupnosti dat, systémů a dalších prvků informační a komunikační infrastruktury.

Nástrojů na podporu řízení kybernetické bezpečnosti v organizacích existuje celá řada. Orientace mezi nimi rozhodně není jednoduchá. Tak proč si vybrat **ISIT software CZ s jeho procesně samostatným nástrojem - modulem Kybernetická bezpečnost organizace?**

Hlavním cílem, osou při vývoji byla a je snaha prakticky pomoci uživateli tohoto nástroje při správě agendy kybernetické bezpečnosti v organizaci.
Program je navržen tak, aby dokázal uživatelům i s menšími zkušenostmi v oblasti kybernetické bezpečnosti, resp. v zajišťování bezpečnosti sítí informačních systémů reálně pomoci a dosáhnut požadovaného cíle – identifikaci konkrétních bezpečnostních opatření, které je nutno implementovat na prvcích informačně-komunikačních technologiích organizace za účelem dosažení požadované úrovně odolnosti primárních procesů organizace vůči kybernetickým bezpečnostním hrozbám.

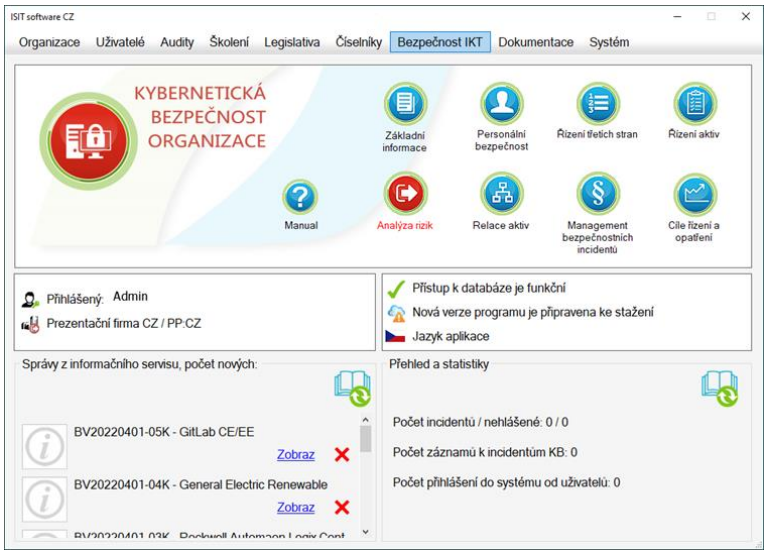
Hlavním cílem je tedy snaha o zabezpečení důvěrnosti, integrity a dostupnosti dat ve všech fázích jejich zpracovávaní tak, aby nedošlo k negativnímu ovlivnění primárních procesů organizace, jimiž se dosahuje samotný účel existence organizace.

Modul Kybernetická bezpečnost organizace programu ISIT software CZ pro uživatele poskytuje v reálném čase přehled o stavu kybernetické bezpečnosti. Pomáhá aktivně specifikovat zranitelná místa v zabezpečení informačně-komunikačních technologií, kybernetické hrozby, které mají potenciál tyto slabé místa využít, identifikuje a ohodnotí rizika kybernetické bezpečnosti informací.

Program umožňuje sledovat, jak se mění hodnota jednotlivých rizik kybernetické bezpečnosti informací v závislosti od implementace navržených opatření a tím i celkový obraz kybernetické bezpečnosti ve společnosti. Umožní provádět interní kontrolu plnění povinností uložených zákonem o kybernetické bezpečnosti zaměřených na bezpečnostní opatření blíže upravená vyhláškou č. 82/2018 Sb., o kybernetické bezpečnosti formou vycházející z ISMS auditů.

Modul Kybernetická bezpečnost organizace programu ISIT software CZ vychází jak z požadavků české legislativy pro oblast kybernetické bezpečnosti, aktuálního zákona i vyhlášky o kybernetické bezpečnosti, tak i z norem ISO 27001.

Stručný popis hlavní funkcionality modulu KBO aplikace ISIT software CZ



Nástroj ISIT Software CZ umožňuje:

Vedení evidence základních informací o správci nebo provozovateli základní služby, významného informačního systému, systému kritické informační infrastruktury;

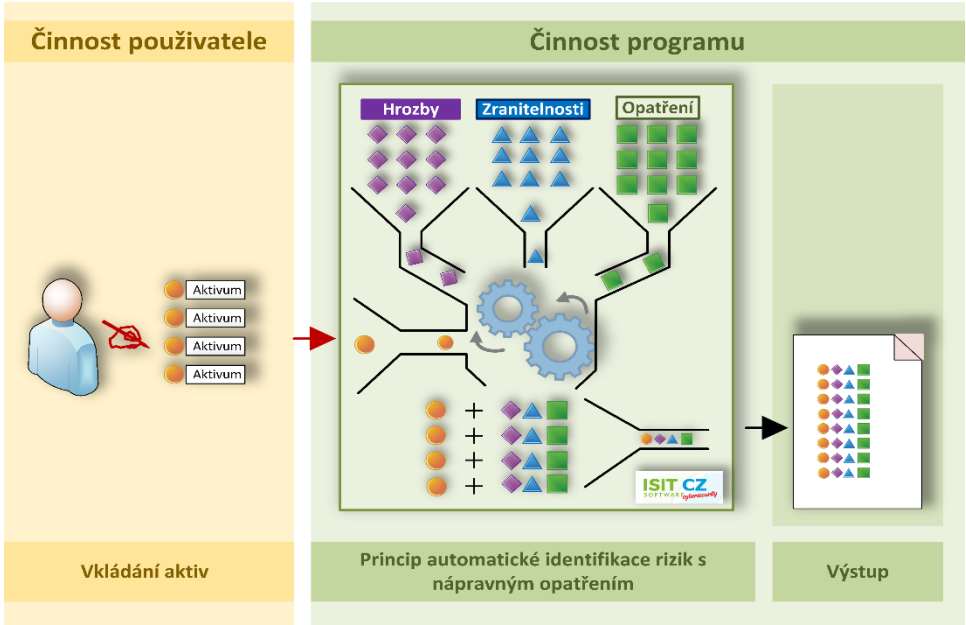
Řízení personální bezpečnosti v rozsahu vedení seznamů o vlastních zaměstnancích s uvedením kromě základních personálií, procesních rolí, funkčního zařazení i informace o přístupu a přístupových oprávněních k informačním systémům provozovaných organizací, absolvovaných školeních, odpovědnostech zaměstnance, svěřených aktivech, přesunech oprávnění atd.;

Řízení třetích stran v rozsahu vedení základních informací o třetích stranách, rozsahu povolených činností, povolených přístupech, evidence smluv, seznamu a popisu třetí stranou přijímaných bezpečnostních opatření, seznamu zaměstnanců třetí strany, řízení jejich přístupů k aktivům organizace, atd.;

Řízení aktiv v rozsahu evidence a popisu aktiv, evidence vlastníků aktiv, osob odpovědných za zavedení bezpečnostního opatření snižujících riziko, správce aktiv, hodnocení aktiv atd.;

Automatizovaná Analýza Rizik, Řízení rizik kybernetické bezpečnosti v rozsahu automatické identifikace rizik, tzn. přiřazení relevantních hrozeb, jejich zranitelností a nápravných opatření bezprostředně po vložení, resp. zapsání aktiv uživatelem do programu, automatizované analýzy rizik, uživatelem řízený proces řešení rizik a plánu zvládání rizik. Proces řízení rizik je přímo závislý na volbě souladu s požadavky na kybernetickou bezpečnost podle zvolených právních nebo obecně uznávaných norem.

Princip automatické identifikace rizik

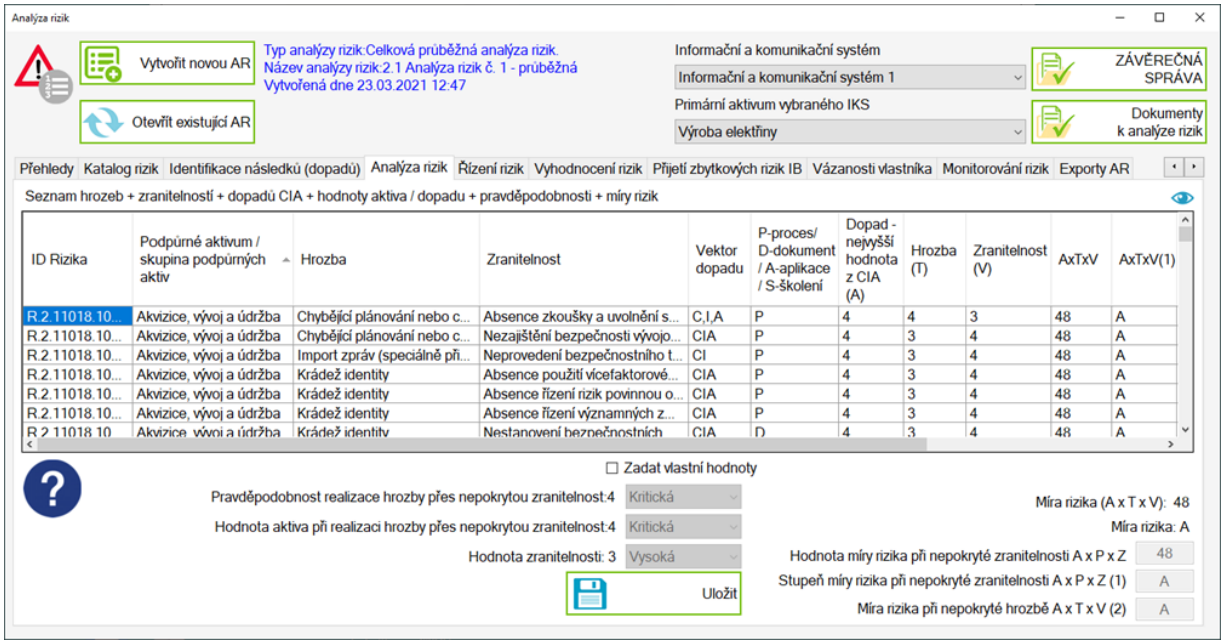


Uživatelský výběr z voleb :

- volba řízení rizik kybernetické bezpečnosti podle uceleného komplexu opatření ve smyslu doporučení mezinárodně akceptovaných standardů kybernetické bezpečnosti pravidel dobré praxe (Best practices),
- volba řízení rizik v souladu s požadavky na kybernetickou bezpečnost dle vyhlášky o kybernetické bezpečnosti č. 82/2018 Sb.
- volba řízení rizik v souladu s požadavky na kybernetickou bezpečnost kombinací požadavků vyhlášky o kybernetické bezpečnosti č. 82/2018 Sb. a požadavků na bezpečnost uživatelem vybraných podpůrných a technických aktiv z uceleného komplexu opatření ve smyslu doporučení mezinárodně akceptovaných standardů kybernetické bezpečnosti, pravidel dobré praxe (Best practices)
- volba řízení rizik v souladu s požadavky na kybernetickou bezpečnost podle požadavků ISO/IEC 27001: 2013/, ISO/IEC 27002: 2013 a požadavků na řízení informační bezpečnosti ve zdravotnictví ISO 27799: 2016;

Součástí Řízení rizik kybernetické bezpečnosti je vedení evidence osob odpovědných za zavedení nápravného opatření, za přijetí rizika, za přenos rizika a za společné snášení rizika;

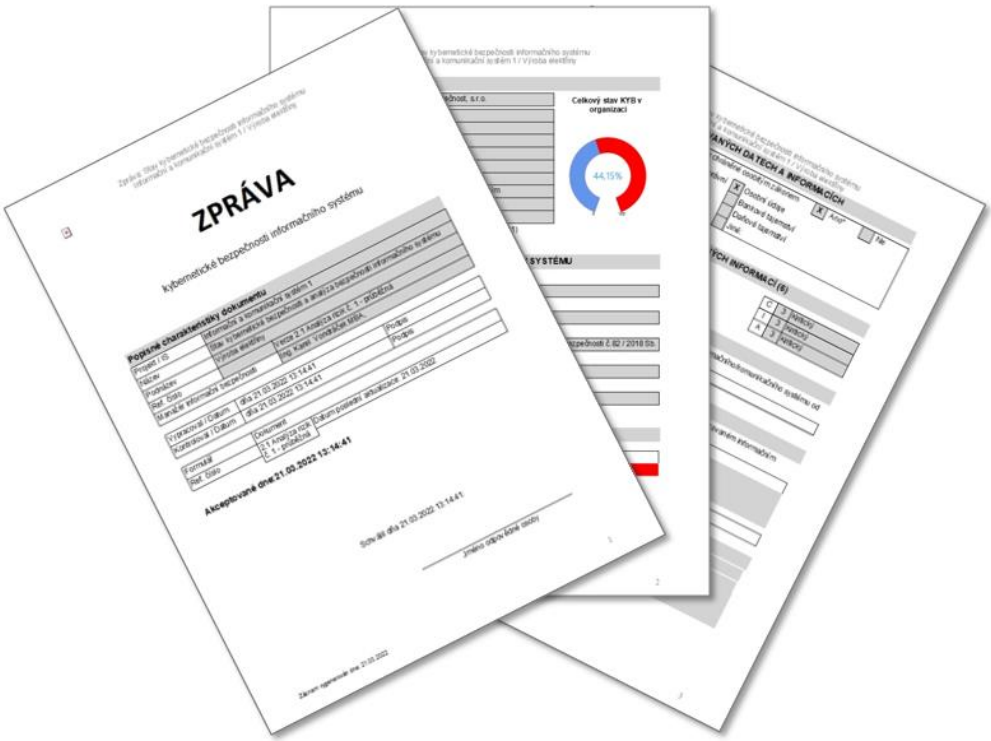
Ukázka – Analýza rizik



Řízení incidentů kybernetické bezpečnosti v rozsahu evidence záznamů o incidentu, kategorii, popisu a stavu závažného incidentu, druhu incidentem zasažených údajů, zasažené moduly základní služby nebo primárního procesu, evidence důkazů, informací o kritičnosti aktiv, řešení kybernetického incidentu, zamezujících a nápravných opatření, jakož i zaslání výstupu z nástroje v předepsané formě hlášení o kybernetickém bezpečnostním incidentu na dozorový orgán, případně na jiný definovaný e-mail.

Generování závěrečné zprávy ve formě jednotlivých kapitol, resp. volitelných částí:

- Správa kybernetické bezpečnosti informačního systému
- Závěry z analýzy rizik zkoumaného informačního systému
- Aktiva
- Analýzy rizik – výstup
- Závěr
- Prohlášení o aplikovatelnosti
- Příloha 1 - legislativní východiska
- Příloha 2 – Použitá metodika
- Příloha 3 – Označení používané k zajištění sdílení citlivých informací (TLP)
- Podpůrné služby



Management automatického příjmu a zpracování bezpečnostních varování NBÚ (NUKIB) na aktuální hrozby a zranitelnosti s detekcí aktiv v systému s určením ochranných opatření a upozorněním pro definované osoby v systému.

Speciální přidanou hodnotou pro zákazníky, kteří jsou řídícím orgánem pro jiné organizace v sektorové působnosti máme připravené **multilicenční řešení** na řízení KB v rámci resortu nebo na řízení jednotlivých organizačních jednotek v robustní organizaci. ISIT software CZ podporuje a napomáhá dlouhodobě udržovat systém řízení KB v organizaci a zároveň v multiverzi umožňuje plnohodnotně řídit KB v resortních organizacích, a to včetně změn a bezpečnostních incidentů. Průvodním profitem je možnost centrální správy nastavení, seznamů hrozeb, opatření a skóringu, ale zejména možnost centrálního systému upozorňování na HW a SW zranitelnosti, jakož i centrálního řízení zasílání hlášení o kybernetických incidentech, čímž víte jednak optimálnější analyzovat stav KB v resortu a zároveň minimalizovat možnosti vzniku bezpečnostních incidentů.

Licencování jednotlivých modulů aplikace je nezávislé, tzn. každý modul může využívat jiný počet uživatelů. Při zakoupení software v dohodnutém licencování za koncovou cenu je součástí této ceny **12 měsíců bezplatná podpora** - update. Po uplynutí 12 měsíců od instalace softwaru je možnost volitelného maintenance ve výši 15 % z pořizovací ceny na dalších 12 měsíců.

Podpůrné služby jsou Podpora při instalaci, zaškolení obsluhy pro admin a klient licence, metodická podpora při naplňování dat a realizaci tiskových výstupů, auditních činností, Analýzy rizik a Závěrečné zprávy, provedení rozdílového auditu, customizace dle požadavků zákazníka, identifikace aktiv a jiné služby v oblasti KB (samostatně placené služby).

Produkt je pojištěn na 1mil EUR - odpovědnost za způsobenou škodu pro území EU.

Modul KBO aplikace ISIT software CZ obdržel dne 12.10.2021 **Osvědčení o kompatibilitě** programového vybavení a shodě s požadavky Vyhlášky o kybernetické bezpečnosti č. 82/2018 Sb. od Fakulty podnikatelské VUT Brno.