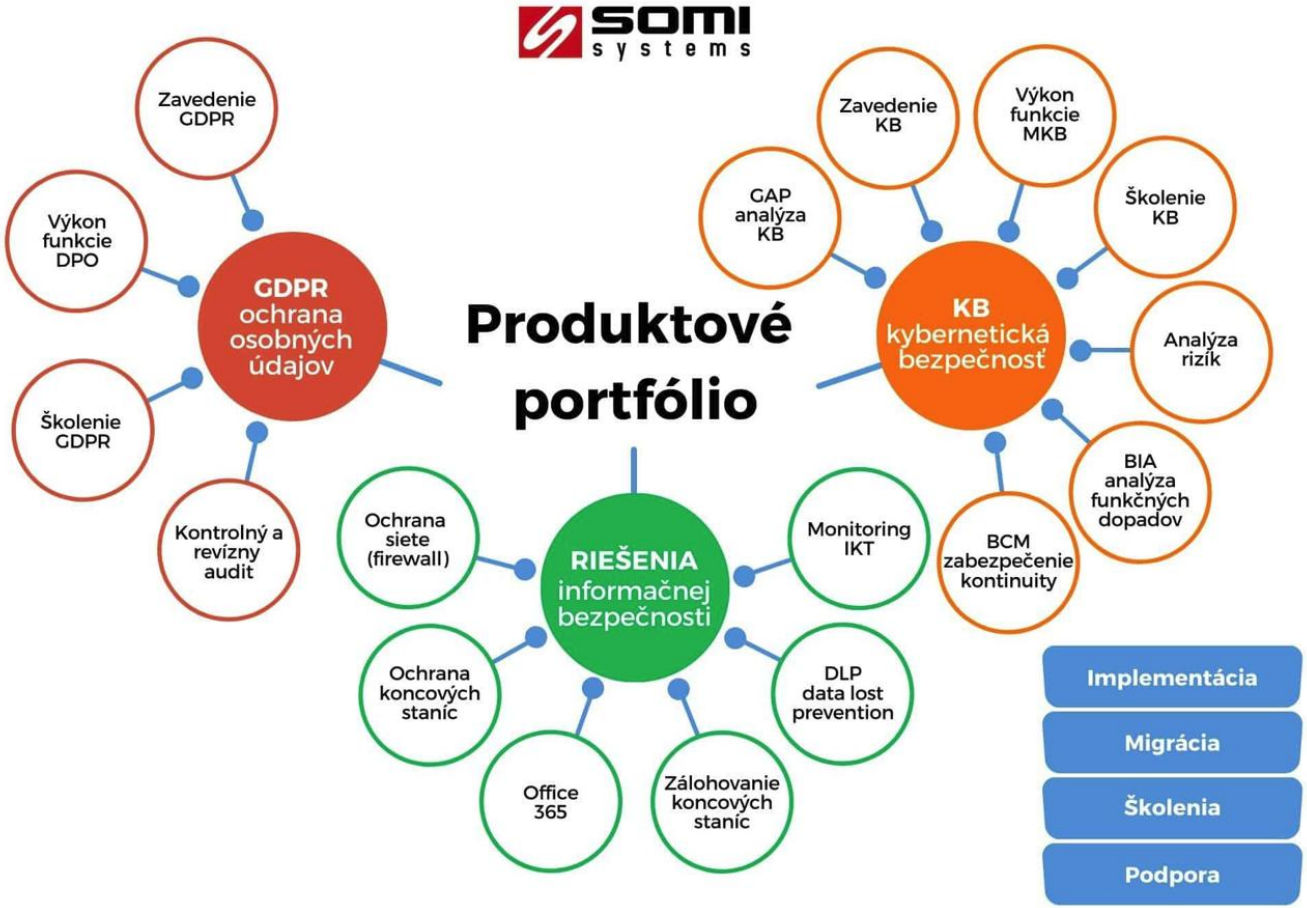
SOMI Systems a.s.

- úspešne zvládnutých 32 rokov na poli informačnej a kybernetickej bezpečnosti - spolu s viac ako 400 spokojnými zákazníkmi
- riešime všetky vaše otázky spojené s kybernetickou bezpečnosťou - vrátane technických riešení
- sme profesionáli v implementácii zákona o kybernetickej bezpečnosti a výkonu funkcie MKB
- sme profesionáli v implementácii nariadenia GDPR a výkonu funkcie Zodpovednej osoby
- garancia nadštandardnej podpory a supportu
- pravidelné školenia, E-learning a vzdelávania

Viac informácií na www.somi.sk

Produktové portfólio



SOMI systems

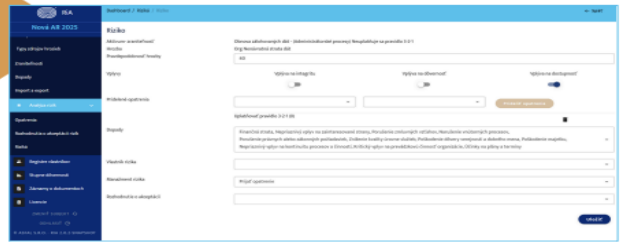
RIA – SW pre riadenie rizík

POSUDZOVANIE RIZIKA:

Softvér RiA je navrhnutý ako inovatívny systém pre implementáciu procesu riadenia rizík do prostredia organizácie. Tento proces zahŕňa určenie vonkajších a vnútorných súvislostí, posúdenie rizík a vypracovanie plánu ošetrenia rizík. Riziká sa posudzujú z hľadiska ich dôsledkov pre organizáciu a pravdepodobnosti ich výskytu.

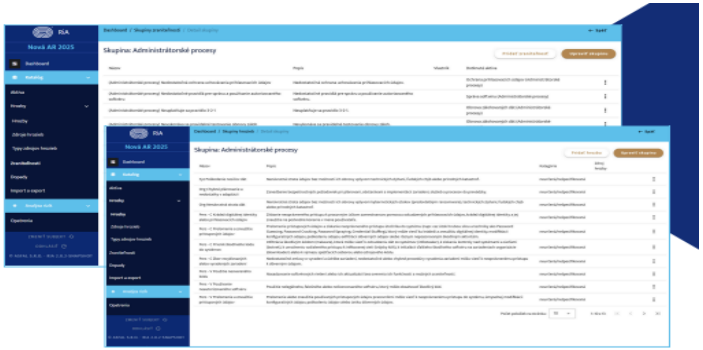
RiA je efektívnym nástrojom riadenia rizík pre manažérov kybernetickej bezpečnosti. Syntetizuje informácie o aktívach a rizikách pre vedúcich zamestnancov, vlastníkov aktív, vlastníkov rizík alebo iné súvisiace roly a uľahčuje spoluprácu s audítormi. Zabezpečuje sledovanie vývoja rizík a opatrení na ich elimináciu v reálnom čase, čím organizácii umožňuje systematicky reagovať na novo vznikajúce hrozby a zraniteľnosti.

RIA POSKYTUJE PREHĽADNÝ PRÍSTUP K IDENTIFIKÁCII, ANALÝZE A HODNOTENIU RIZÍK A ZJEDNODUŠUJE PROCES ROZHODOVANIA O POTREBE PRIJATIA OPATRENÍ NA ICH ELIMINÁCIU.



FUNKCIE SOFTVÉRU RIA:

- Dashboard subjektu – prehľad kľúčových informácií na jednom mieste.
- Správa aktív, zraniteľností, hrozieb a ich zdrojov, následkov a vzťahov medzi nimi.
- Registre vlastníkov a súvisiacej dokumentácie (rozhodnutia o akceptácii rizík a pod.).
- Tvorba komplexnej analýzy rizík a hodnotenie rizík pomocou rizikového indexu.
- Katalóg opatrení, plán ošetrenia rizík a prioritizácia ošetrenia rizík.
- Generovanie prehľadov vo formáte PDF - manažérsky report, výstupy z katalógov a analýzy rizík
- Správa identít – centralizovaná kontrola používateľských identít a oprávnení.



ARCHITEKTÚRA SOFTVÉRU:

Softvér RiA je navrhnutý podľa štandardnej trojvrstvovej architektúry, ktorá pozostáva z troch vrstiev:

- **Webová vrstva -** predstavuje používateľské rozhranie, zabezpečuje autentifikáciu a autorizáciu používateľov na základe pridelených rolí.
- **Servisná vrstva -** poskytuje služby prístupu k dashboardu subjektu, služby zostavovania katalógov aktív, hrozieb, zraniteľností a opatrení, služby vytvárania a hodnotenia rizikových scenárov, služby zostavovania registra vlastníkov alebo iných objektoch v súvislosti s riadením rizika, služby pre vytváranie formalizovaných výstupov vo forme reportov.
- **Dátová vrstva -** uchováva údaje o objektoch v riadení rizika.

SPÔSOB DODANIA:

- **Standalone delivery** – softvér sa dodáva ako obraz virtuálneho počítača s vopred nakonfigurovaným operačným systémom a potrebnými komponentmi.

RIA ZABEZPEČUJE SÚLAD S BEZPEČNOSTNÝMI ŠTANDARDMI A PODPORUJE ROZHODOVACIE PROCESY ZAINTERESOVANÝCH OSÔB.

somi systems

BCM – Business Continuity Management

BUSINESS CONTINUITY MANAGEMENT (BCM)

Neočakávané prerušenie prevádzky organizácie môže nastať z rôznych dôvodov – ako následok kybernetického bezpečnostného incidentu, poruchou technológie, chybou v procesoch alebo na základe prírodných udalostí.
Riedenie kontinuity činností (BCM) predstavuje súbor opatrení a procesov, ktoré vašej organizácii poskytnú efektívne havarijné plánovanie spolu s implementáciou technicko-systémových opatrení. Súčasťou sú plány kontinuity činností, ktoré umožňujú v prípade skutočného incidentu alebo zlyhania procesov, služieb či technológií vrátiť sa k produktívnej činnosti najrýchlejším a najefektívnejším možným spôsobom a tým minimalizovať možné negatívne dopady.

ZAISTITE NEPRETRŽITÚ ČINNOSŤ VAŠICH KĽÚČOVÝCH ČINNOSTÍ A PROCESOV, AJ V PRÍPADE NEOČAKÁVANÝCH UDALOSTÍ.

POŽIADAVKY:

- Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti.
- Vyhláška č. 362/2018 Z. z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie.
- Zákon č. 95/2019 Z. z. o informačných technológiách vo verejnej správe.

NAŠE RIEŠENIE:

- **Zadefinujeme scenáre rôznych udalostí,** ktoré môžu mať negatívny vplyv na bežné činnosti organizácie.
- **Stanovíme požiadavky na zdroje** (adekvátne finančné, materiálno-technické a personálne), ktoré budú potrebné na implementáciu vybraných stratégií kontinuity činností.
- **Vypracujeme analýzu funkčných dopadov** a kvalifikujeme potencionálne dopady a straty v prípade prerušenia alebo narušenia prevádzky pri všetkých procesoch vašej organizácie.
- **Vypracujeme plán kontinuity** na stanovenie požiadaviek a zdrojov, plán reakcie na incidenty, politiku a ciele kontinuity, evakuačné postupov, plány havarijnej obnovy prevádzky, plán údržby a kontroly BCM systému.

- **Vypracujeme stratégiu riadenia kontinuity,** ktorej súčasťou je aj schválenie časových rámcov na obnovu činností a hodnotenie spôsobilosti tretích strán zaručiť kontinuitu dodávateľských činností.
- **Zavedieme postupy zálohovania a obnovy siete** a informačných systémov po ich narušení alebo zlyhaní.
- **Vypracujeme plán pravidelného preverovania záloh** a testovania obnovy záloh.
- **Zabezpečíme vám výkon funkcie manažéra riadenia kontinuity** spolu s precvičovaním zavedených krízových plánov.
- **Budeme vykonávať pravidelné interné audity a kontroly BCM.**
- **Zabezpečíme pravidelné preškolovanie zamestnancov** a precvičovanie zavedených krízových plánov.

SÚLAD S MEDZINÁRODNE UZNÁVANÝM ŠTANDARDOM

"Sektor „Verejná správa", podsektor „Informačné systémy", ktorý je počtom Prevádzkovateľov základných služieb (PZS) najväčší, už dlhodobo vykazuje vysokú mieru zanedbávania témy kybernetickej bezpečnosti. Ak si uvedomíme vysokú atraktivitu tohto sektora pre útočníkov, zanedbávanie kybernetickej bezpečnosti a ignorovanie jej dôležitosti môže mať katastrofický dopad na poskytovanie základných služieb štátu, ochranu osobných údajov všetkých občanov a verejný poriadok." (zdroj: NBÚ)

So systematickým prístupom k plánovaniu kontinuity činností môžu organizácie výrazne urýchliť zotavenie po kritickej negatívnej udalosti.

BCM SPOČÍVA V ZABEZPEČENÍ NEPRETRŽITEJ PREVÁDZKY A RÝCHLEJ OBNOVY ČINNOSTÍ PO NARUŠENÍ, ČI UŽ V DÔSLEDKU KYBERNETICKÝCH ÚTOKOV, TECHNICKÝCH PORÚCH ALEBO INÝCH NEOČAKÁVANÝCH UDALOSTÍ.

somi systems

Certifikácia

Systém manažérstva kvality
EN ISO 9001:2015

Systém manažérstva realizácie služieb a školení
STN EN ISO 14001:2015

Systémy manažérstva informačnej bezpečnosti
ISO/IEC 27001:2022

Manažér kybernetickej bezpečnosti
MKB

Systém manažérstva realizácie služieb a školení
STN EN ISO 22301:2021

SOMI systems

V SOMI Systems a.s. sme presvedčení, že nevyhnutnou súčasťou dnešnej rýchlo meniacej sa doby v technologickom svete, je zdieľanie informácií.

Preto spolu s každou nami realizovanou službou, získavate aj prístup k plnohodnotným školeniam, pravidelnému vzdelávaniu, e-learningom, najnovším článkom na blogu a vzdelávacím infografikám.