SOMI Systems a.s.

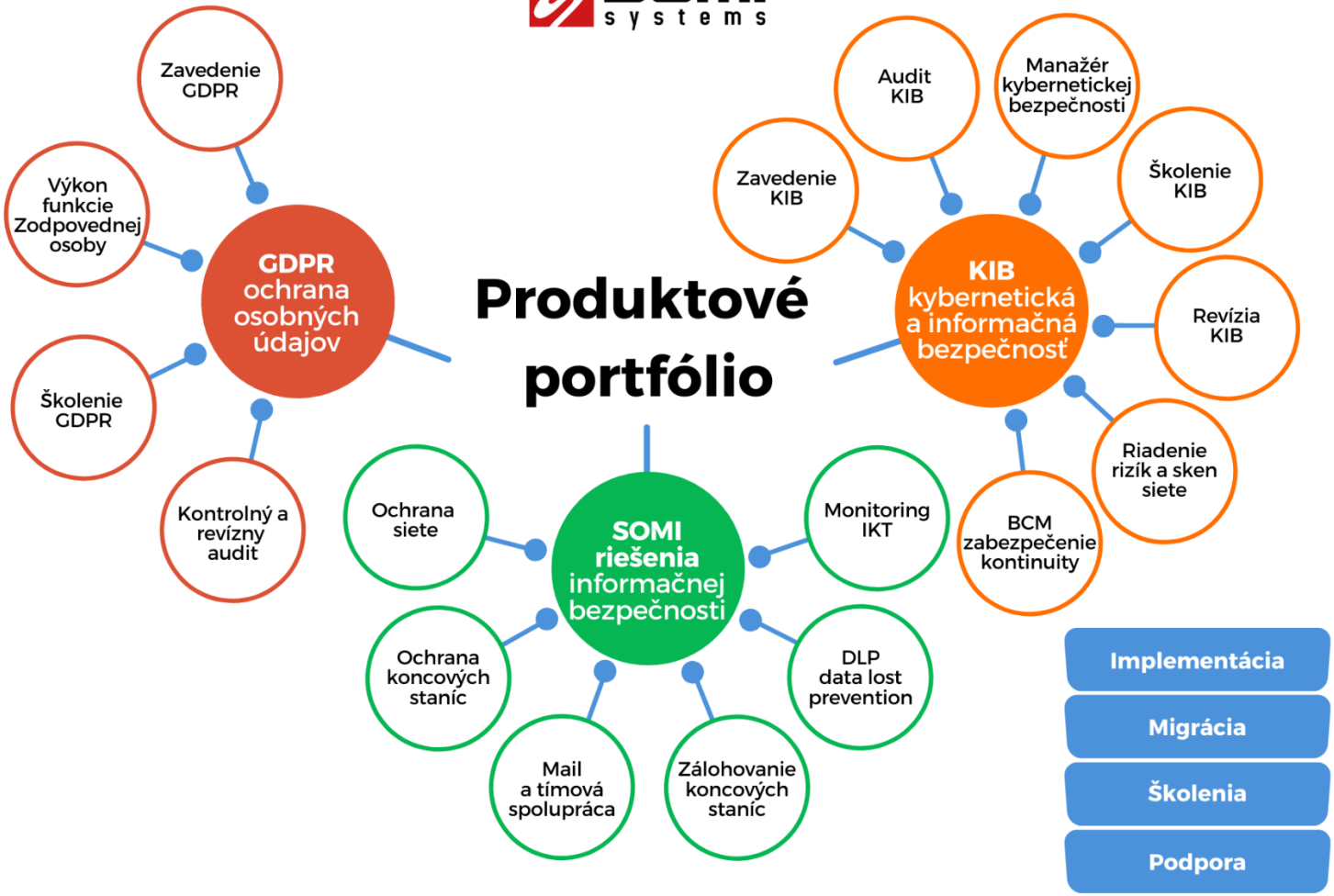
- úspešne zvládnutých 30 rokov na poli informačnej a kybernetickej bezpečnosti - spolu s viac ako 400 spokojnými zákazníkmi
- riešime všetky vaše otázky spojené s kybernetickou bezpečnosťou - vrátane technických riešení
- sme profesionáli v implementácii zákona o kybernetickej bezpečnosti a výkonu funkcie MKB
- sme profesionáli v implementácii nariadenia GDPR a výkonu funkcie Zodpovednej osoby
- garancia nadštandardnej podpory a supportu
- pravidelné školenia, E-learning a vzdelávania

30 ROKOV sme tu s vami

SOMI systems

Viac informácií na www.somi.sk

Produktové portfólio



KYBERNETICKÁ BEZPEČNOSŤ

Kybernetická bezpečnosť je súbor technológií, postupov a procesov, ktoré organizáciám pomáhajú chrániť svoje počítačové systémy, siete, dáta a iné aktíva pred kybernetickými hrozbami a útokmi.

V praxi to znamená vykonať analýzu, spracovanie a zavedenie bezpečnostnej politiky v rozsahu, ktorý korešponduje s požiadavkami bezpečnostných opatrení zákona č.: 69/2018 Z. z. o kybernetickej bezpečnosti. Naplnenie požiadaviek zákonov, ktoré definujú úroveň bezpečnostných opatrení v organizáciách je neľahká úloha, ktorá kladie vysoké nároky na personálne a materiálne zdroje. Kľúčovým faktorom pre úroveň kybernetickej bezpečnosti sú popri technickom zabezpečení hlavne znalosti a skúsenosti.

NEMUSÍTE SA TRÁPIŤ BEZPEČNOSTNÝMI POVINNOSŤAMI, KTORÉ VÁM ZO ZÁKONA VYPLÝVAJÚ. ZABEZPEČÍME ICH ZA VÁS.

Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti:

- Komplexne upravuje oblasť kybernetickej a informačnej bezpečnosti,
- zavádza základné bezpečnostné požiadavky a opatrenia dôležité pre koordinovanú ochranu informačných, komunikačných a riadiacich systémov,
- zároveň do slovenského právneho poriadku transponuje európsku Smernicu o sieťovej a informačnej bezpečnosti (NIS2).

KOMPLEXNÉ ZAVEDENIE KYBERNETICKEJ BEZPEČNOSTI A PRÍPRAVA NA AUDIT ZAHŔŇA:

- Kontrolu súladu s požiadavkami kybernetickej bezpečnosti (GAP analýza).
- Testy zraniteľností, monitoring lokálnej infraštruktúry.
- Vypracovanie dokumentácie.
- Návrh opatrení a procesov na dosiahnutie súladu,
- Poradenstvo pri zavádzaní opatrení a procesov eliminácie kybernetických útokov.
- Návrh nástrojov pre sledovanie a vyhodnocovanie kyber útokov.
- Školenia zamestnancov v problematike kybernetickej bezpečnosti.
- Asistencia pri audite podľa zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti.
- Výkon funkcie Manažéra kybernetickej bezpečnosti.

PREVÁDZKOVATEĽ ZÁKLADNEJ SLUŽBY

Prevádzkovateľ základnej služby je povinný do 12 mesiacov odo dňa oznámenia o zaradení do registra prevádzkovateľov základných služieb, **prijať a dodržiavať všeobecné bezpečnostné opatrenia najmenej v rozsahu:**

- organizácie kybernetickej a informačnej bezpečnosti,
- riadenia aktív, hrozieb a rizík,
- personálnej bezpečnosti,
- riadenia kybernetickej a informačnej bezpečnosti s tretími stranami,
- riadenia bezpečnosti informačných systémov a sietí,
- hodnotenia zraniteľností a bezpečnostných aktualizácií,
- ochrany proti škodlivému kódu, sieťovej a komunikačnej bezpečnosti,
- riadenia prevádzky a prístupov,
- kryptografických opatrení,
- riešenia kybernetických bezpečnostných incidentov,
- monitorovania, testovania bezpečnosti a bezpečnostných auditov,
- fyzickej bezpečnosti a bezpečnosti prostredia,
- kontinuity prevádzky, auditu, riadenia súladu a kontrolných činností.

VZDELÁVANIE ZAMESTNANCOV

Pravidelné vzdelávanie v problematike kybernetickej a informačnej bezpečnosti pomáha zamestnancom správne reagovať na neustále sa meniace hrozby, čo je základom ochrany pred kybernetickými útokmi. Znalosť a dodržiavanie bezpečnostných politík je základom pre zodpovedné správanie sa pri práci s firemnými a osobnými údajmi.

KYBERNETICKÁ BEZPEČNOSŤ NIE JE IBA NÁKLADNOU POVINNOSŤOU, ALE PREDSTAVUJE NEVYHNUTNÝ PRVOK PRE OCHRANU AKTÍV A UDRŽANIE SI KONKURENCIESCHOPNOSTI V DNEŠNOM DIGITÁLNOM SVETE.

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 postupy, 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 spôsobilostí 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.

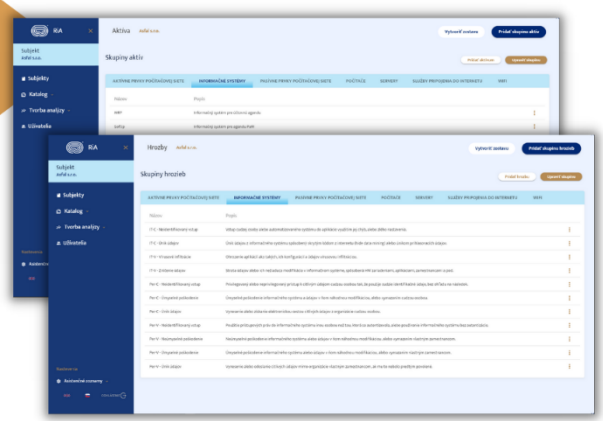
BCM SPOČÍVA V ZABEZPEČENÍ NEPRETRŽITEJ PREVÁDZKY A RÝCHLEJ OBNOVY ČINNOSTÍ PO NARUŠENÍ, ČI UŽ V DÔSLEDKU KYBERNETICKÝCH ÚTOKOV, TECHNICKÝCH PORÚCH ALEBO INÝCH NEOČAKÁVANÝCH UDALOSTÍ.

ANALÝZA A RIADENIE RIZÍK

Základom kybernetickej bezpečnosti je identifikácia, analýza a riadenie rizík postavená na veľmi dobrom poznaní organizácie. Riziká sú často tvorené veľkým počtom rozmanitých aktív, ktoré sú vystavené ešte väčšiemu počtu hrozieb.

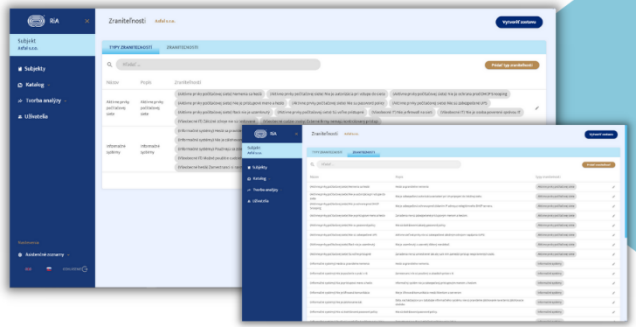
Systém RiA je navrhnutý tak, aby organizáciám poskytoval jednoduchý a prehľadný prístup k identifikácii, analýze a riadeniu rizík. Systém umožňuje umožňuje navrhnúť a prijať efektívne opatrenia na potlačenie a elimináciu rizík a kybernetických hrozieb. Zabezpečuje sledovanie vývoja rizík a opatrení na ich elimináciu v reálnom čase, čím organizáciám umožňuje rýchlo a efektívne reagovať na nové hrozby. Analýza rizík je vyhodnocovaná podľa najhoršieho scenára, ktorý môže nastať.

RIA PREDSTAVUJE JEDINEČNÝ NÁSTROJ PRE VEDÚCICH PRACOVNÍKOV, MANAŽÉROV KYBERNETICKEJ BEZPEČNOSTI, VLASTNÍKOV AKTÍV A MANAŽÉROV PRE RIADENIE RIZÍK.



FUNKCIE SYSTÉMU RIA:

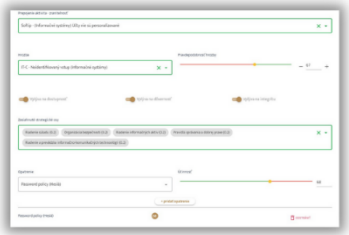
- Správa aktív, vlastníkov aktív, zraniteľností, vlastníkov zraniteľností, hrozieb, opatrení, vzťahov, rizík a vlastníkov rizík.
- Webové rozhranie, ktoré umožňuje jednoduchý a prehľadný prístup k všetkým službám systému s výstupmi vo forme PDF zostáv.
- Pokročilý manažment a evidencia používateľov, vrátane prideľovania rolí a oprávnení. Každý používateľ má prístup len k tým údajom a funkciám, ktoré mu boli pridelené, čo umožňuje efektívne zabezpečiť bezpečnosť a dôvernosť údajov.



ARCHITEKTÚRA SYSTÉMU:

Systém RiA je navrhnutý podľa štandardnej trojvrstvovej architektúry, ktorá pozostáva z webovej vrstvy, servisnej vrstvy a dátovej vrstvy:

- **Webová vrstva** poskytuje užívateľské rozhranie a zabezpečuje autentifikáciu a autorizáciu užívateľov.
- **Servisná vrstva** poskytuje služby prístupu k základným údajom o subjekte a jeho aktívach, služby zostavovania a editácie rizík, službu registra opatrení a službu pre poskytovanie formalizovaných výstupov.
- **Dátová vrstva** uchováva údaje o aktívach, rizikách a opatreniach.



SPÔSOB DODANIA:

- **Standalone delivery** – systém je dodaný ako obraz virtuálneho počítača s vopred nakonfigurovaným systémom a jeho súčasťami.
- **Software as Service** – funkcie systému sú sprístupňované ako služba poskytovaná autorom a správcom služieb systému RiA.

Systém umožňuje aj porovnávanie dát v rôznych časových obdobiach (analýza histórie). Je možné porovnať podobné časové obdobia, čo je veľmi užitočné, keď zaťaženie prostredia nie je rovnomerné Napr. porovnanie od pondelka rána do utorka popoludnia neprináša žiadne cenné informácie.

ÚLOHOU SYSTÉMU RIA JE NIELEN ZOSTAVIŤ ANALÝZU RIZÍK A PODPORIŤ TAK RIADENIE RIZÍK, ALE NAJMÄ UMOŽNIŤ SLEDOVANIE VÝVOJA RIZÍK A OPATRENÍ NA ICH ELIMINÁCIU V REÁLNOM ČASE.

MONITOROVANIE PREVÁDZKY IKT

Pre zabezpečenie kontinuity prevádzky informačných systémov je potrebné pravidelné monitorovanie IKT technológií. Monitorovanie slúži na identifikáciu kapacitných požiadaviek a trendov, tak aby nedošlo ku kritickému výpadku, spomaleniu alebo inej neočakávanej poruche funkčnosti. Monitorovanie IKT technológií sa uskutočňuje implementáciou nástroja na zaznamenávanie (logov) o ich činnosti a činností ich používateľov. Logy sú pravidelne vyhodnocované a v prípade neobvyklej alebo kritickej udalosti musí správca IKT aktívna vykonať potrebné opatrenia. Súčasťou riešenia sú aj systémy ochrany pred škodlivým kódom.

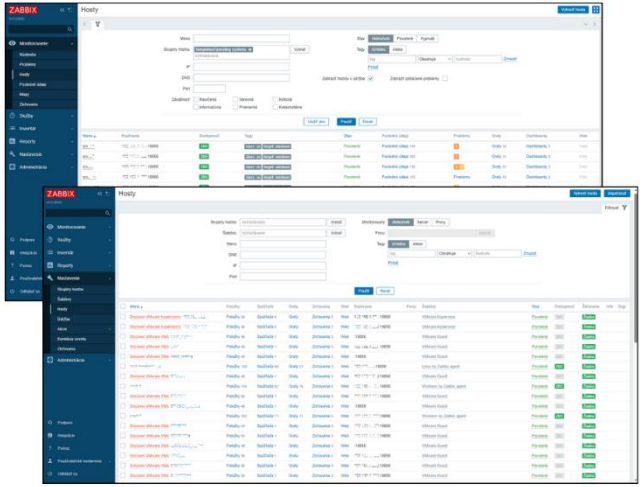
MONITOROVANIE PREVÁDZKY ZABEZPEČÍ AKTUÁLNY PREHĽAD O STAVE A TAK ISTO O PROBLÉMOCH MONITOROVANÝCH ZARIADENÍ.

ZABBIX SERVER

Zabbix Server 6.0 LTS je výkonný monitorovací nástroj, ktorý umožňuje sledovať výkon IT systémov, monitorovať zariadenia, aplikácie a služby, a zabezpečiť rýchlu reakciu na problémy.

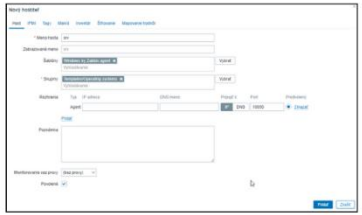
Tento pokročilý nástroj je rozdelený do šiestich kariet:

- **Monitorovanie**
- **Služby**
- **Inventár**
- **Reporty**
- **Nastavenia**
- **Administrácia**



VÝHODY KOMPLEXNÉHO MONITORINGU

- Škálovateľnosť a možnosť monitorovať rôzne druhy zariadení ako sú fyzické a virtuálne servery, sieťové prvky, dátové úložiská a iné zariadenia, ktoré dokážu poskytnúť údaje o svojej prevádzke.
- Prevádzka v reálnom čase s možnosťou vizualizácie prostredníctvom grafov, máp a rôznych náhľadov.
- Monitoring informuje o vzniknutých problémoch správcu príslušnej služby alebo servera, čo umožňuje hneď na počiatku vzniku problému prijať príslušné opatrenia a zabrániť tak vzniku negatívneho dopadu na prevádzku. Informácia o probléme sa posiela viacerými komunikačnými kanálmi ako je mail, SMS, Jabber alebo vlastný komunikačný kanál.



Systém umožňuje aj porovnávanie dát v rôznych časových obdobiach (analýza histórie). Je možné porovnať podobné časové obdobia, čo je veľmi užitočné, keď zaťaženie prostredia nie je rovnomerné Napr. porovnanie od pondelka rána do utorka popoludnia neprináša žiadne cenné informácie.

Prístup do systému je realizovaný prostredníctvom webového rozhrania s možnosťou personalizovať prístupové práva. Webové rozhranie je natívne a poskytuje množstvo spôsobov prezentácie vizuálneho prehľadu. Na jednej obrazovke je možné zobraziť toľko grafov, koľko je potrebné. Automatická obnova a zmena časovej periódy sú samozrejmosťou.

PREDNOSŤOU TOHOTO SYSTÉMU JE PODROBNÝ HISTORICKÝ PREHĽAD O PROBLÉMOCH, KTORÉ BOLI NA JEDNOTLIVÝCH ZARIADENIACH ZISTENÉ.

ZÁLOHOVANIE KONCOVÝCH STANÍC

Neustále narastajúce objemy dát a rastúce nároky na ich uchovávanie, riešia prakticky všetky organizácie. Nie nadarmo sa hovorí, že používatelia pracujúci na počítačoch sa delia len do dvoch skupín – na tých čo pravidelne zálohujú a na tých ktorí o svoje dáta ešte neprišli.

NEVYHNUTNOSŤ ALEBO TECHNOLOGICKÝ VÝSTRELOK?

Hrozieb, ktoré môžu zapríčiniť stratu dôležitých údajov je veľa – od živelných pohrôm, zlyhania hardvéru alebo softvéru, cez stratu alebo krádež počítaču, serveru, notebooku, telefónu až po sofistikované útoky napríklad prienikom pomocou sociálneho inžinierstva, phishingových útokov, trójskych koní, spywar-u alebo ransomvérových útokov.

Práve ransomvérové útoky sú fenoménom posledných rokov a z praxe vieme, že aj organizácie na Slovensku sú častým cieľom. Tento druh útoku sa rýchlo vyvíja a napreduje – nie len, že škodlivý kód dáta zašifruje a útočník žiada vysoké „výpalné“ za ich znovu sprístupnenie, ale po novom, útočníci už žiadajú výpalné aj za ich nezverejnenie.

NA TENTO PROBLÉM MÁME EFEKTÍVNE RIEŠENIE VYZNAČUJÚCE SA JEHO BEZPEČNOSŤOU, SKVELÝM MANAŽMENTOM A RÝCHLYM NASADENÍM.

VÝHODY:

- Centralizovaná ochrana dát s rýchlym nasadením.
- Komplexné multiplatformové riešenie.
- Jednoduché zálohovanie vďaka jednotnému riadiacemu panelu, vytváraniu zostáv a upozorneniam.
- Inteligentná správa šírky pásma.
- Maximalizácia dostupnosti úložiska.
- Maximálna bezpečnosť vďaka šifrovaniu, pokročilému riadeniu oprávnení a manažmentu správcov.

ČO BY SA MALO ZÁLOHOVAŤ?

Určite všetko, čoho strata by bola akýmkoľvek spôsobom citeľná – osobné údaje, personálna a mzdová agenda, právna agenda, zdravotné záznamy, zmluvy, know-how, pracovné dáta. Čiže pokiaľ ste organizácia závislá od vašich dát, zálohovať potrebujete a to tak, aby bolo možné v čo najkratšom čase obnovením zo záloh pokračovať v činnosti. Na prvý pohľad to vyzerá tak, že riešenie je finančne a časovo náročné, čo ale vôbec nemusí byť pravda. Základom je diverzifikácia rizika straty, správne nastavenie procesov a čo možno najrýchlejšia možnosť obnovy a návrat k normálnej činnosti.

KTO BY MAL URČITE ZÁLOHOVAŤ?

V skratke je to každý, ktorého činnosť, podnikanie a fungovanie je postavené na dátach a súboroch – štátna správa, verejná správa (mestá a obce), zdravotníctvo (nemocnice, ústavy, laboratória), školstvo a vzdelávanie (materské, základné, stredné a vysoké školy), súkromný sektor, energetika, finančný sektor, výrobné podniky, e-shopy, veľko a malo predajcovia atď.

SAMOZREJMOSŤOU JE ŠIFROVANÝ PRENOS VYUŽÍVAJÚCI NAJMODERNEJŠIE TECHNOLÓGIE, ČO ZABEZPEČÍ NAJVÄČŠÍ MOŽNÝ ŠTANDARD OCHRANY DÁT A KOMUNIKÁCIE.

TÜV SÜD Slovakia s.r.o.
Jašíkova 6, Bratislava, 821 03, www.tuvsud.com/sk-sk

Certifikačný orgán pre certifikáciu osôb s registračným číslom 153/O-012
akreditovaný Slovenskou národnou akreditačnou službou podľa normy ISO/IEC 17024:2012

na základe úspešne absolvovaného certifikačného procesu vydáva

Certifikát

Manažér kybernetickej bezpečnosti

pre držiteľa:

RNDr. Daniel Schikor
narodený [redacted]

Certifikačný orgán týmto potvrdzuje plnenie kvalifikačných požiadaviek v súlade s Certifikačnou schémou overovania odbornej spôsobilosti manažéra kybernetickej bezpečnosti, verzia 1.1 NBÚ

Evidenčné číslo certifikátu	Dátum vydania	Platnosť do
0545/20/22/MKB/153/O-012	07.12.2022	06.12.2025

Držiteľ certifikátu podlieha dohľadu certifikačného orgánu. V prípade porušenia zmluvných podmienok môže byť v súlade s postupmi certifikačného orgánu platnosť certifikátu pozastavená alebo ukončená.

NBÚ

Ing. Peter Šustek
vedúci Certifikačného orgánu osôb
TÜV SÜD Slovakia s.r.o.

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.

Viac informácií na www.somi.sk

SOMI systems