

RIADENIE KONTINUITY ČINNOSTÍ - BCM

v zmysle zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti

Business Continuity Management (BCM), predstavuje súbor opatrení a procesov zameraných na zníženie dopadov pri vzniku kybernetického bezpečnostného incidentu.

Riadenie kontinuity činností (BCM) je súbor dokumentov a opatrení, ktoré organizácii poskytnú efektívne havarijné plánovanie spoločne s implementáciou technicko-systémových opatrení. Súčasťou kontinuity je aj plán obnovy kľúčových procesov organizácie v prípade bezpečnostného incidentu.

Je dôležité vedieť ako správne reagovať na potencionálne hrozby a ako informačné systémy v prípade vzniku kybernetického incidentu čo najefektívnejšie a najrýchlejšie vrátiť do plnohodnotnej prevádzky.

www.somi.sk

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.

BCM RIEŠENIE:

- **Definícia scenárov rôznych udalostí**, ktoré môžu mať negatívny vplyv na bežné činnosti organizácie.
- **Stanovenie požiadaviek na zdroje** (adekvátne finančné, materiálno-technické a personálne), ktoré budú potrebné na implementáciu vybraných stratégií kontinuity činností.
- **Vypracovanie analýzy funkčných dopadov** a kvalifikovanie potencionálnych dopadov a strát v prípade prerušenia alebo narušenia prevádzky pri všetkých procesoch v organizácii.
- **Ďalej je potrebné vypracovať:** plán kontinuity na stanovenie požiadaviek a zdrojov, plán reakcie na incidenty, politiku a ciele kontinuity, analýzu funkčných dopadov, stratégiu riadenia kontinuity vrátane evakuačných postupov, plány havarijnej obnovy prevádzky, plán údržby a kontroly BCM systému.
- **Zaviesť postupy zálohovania** a obnovy siete a informačných systémov po ich narušení alebo zlyhaní.
- **Vypracovať plán pravidelného preverovania záloh** a testovania obnovy záloh.
- **Zabezpečiť výkon funkcie manažéra riadenia kontinuity spolu s precvičovaním zavedených krízových plánov** a zabezpečiť podporu pri audite z NBÚ.
- **Vykonávať pravidelné interné audity a kontroly BCM**.
- **Zabezpečiť pravidelné preškoľovanie zamestnancov** a precvičovanie zavedených krízových plánov.

VYPRACOVANÉ V SÚLADE 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."

Citát zo správy o kybernetickej bezpečnosti v SR (rok 2021) vypracovaný NBÚ



SOMI Systems a.s.
Lazovná 69, 97401
Banská Bystrica

www.somi.sk
048/41 46 759
info@somi.sk