sapie

SPRIEVODCA DIGITÁLNOU BEZPEČNOSŤOU

PRE MALÉ A STREDNÉ PODNIKY

VEDENIE A MANAŽMENT FIRMY

- ☑ Máme definované a zdokumentované pravidlá, postupy a opatrenia
- ☑ Vieme, kto je zodpovedný za jednotlivé oblasti, v rámci bezpečnosti
- ☑ Pravidelne testujeme odolnosť voči hrozbám, a vieme ju odmerať

DENNÁ PREVÁDZKA

Dokumentácia a informovanosť:

- ☑ Máme aktuálny a podrobný zoznam firemných IT zariadení a používaných aplikácií
- ☑ Máme identifikované dáta, s ktorými pracujeme, a ich dôležitosť; dáta majú životný cyklus
- ☑ Máme zoznam legitímnych užívateľov, každý má svoj účet

Správa identít:

- ☑ Používateľom prideľujeme a odoberáme prístupy a práva podľa nevyhnutnej potreby
- ☑ Kontrolujeme a odstraňujeme nepotrebné a nepoužívané prihlasovacie účty

Riadenie rizík:

- ☑ Monitorujeme činnosť IT zariadení, sledujeme dianie v systémoch, sieťach a aplikáciách, vďaka čomu vieme odhaliť neautorizované aktivity a odstraňujeme neautorizované zariadenia a aplikácie

Technické prostriedky:

- ☑ Dáta máme uložené iba šifrovane podľa klasifikačnej schémy (poznámka: dáta môžu byť uložené aj nešifrovane, ak to nevyžaduje buď klasifikačná schéma, alebo dáta nie sú senzitívnej povahy)
- ☑ Zariadenia majú bezpečné nastavenie (nie default nastavenie; zabezpečenie silným a jedinečným heslom; notifikácie sa nezobrazujú na zamknutej obrazovke;..)
- ☑ Vzdialený prístup do aplikácií či siete vyžaduje viacfaktorové overovanie
- ☑ Pravidelne aplikujeme bezpečnostné opravy a aktualizácie
- ☑ Máme ochranu pred škodlivým software na všetkých zariadeniach
- ☑ Máme implementovanú segmentáciu siete
- ☑ Filtrujeme prístup na internet voči škodlivému obsahu

sapie

HR A INTERNÉ VZDELÁVANIE

- ☑ Informujeme a vzdelávame zamestnancov o:
  - rizikách a hrozbách v digitálnom priestore
  - pravidlách bezpečného a želaného správania sa, používania firemných zariadení, aplikácií a dát, a práci s citlivými údajmi
  - tom, čo robiť a koho kontaktovať pri podozrení na bezpečnostný incident
- ☑ Máme vytvorené procesy pre odchod zamestnancov s nadštandardnými oprávneniami

KOMUNIKÁCIA SO ZÁKAZNÍKMI A DODÁVATEĽMI

- ☑ Máme aktuálny a podrobný zoznam dodávateľov služieb, a pravidelne vyhodnocujeme, od ktorých vyžadujeme dodržiavanie bezpečnostných pravidiel

PRÍPRAVA A REAKCIA NA NÚDZOVÉ SITUÁCIE

- ☑ Zálohované dáta, zálohy nastavení zariadení, hesiel, aplikácií máme uložené oddelene, a sú šifrované, a máme ich v prípade potreby kam obnoviť
- ☑ Vieme, čo je pre nás kybernetický incident, a čo robiť v prípade, že nastane (kto má čo na starosti; máme vopred pripravený plán; máme zoznam potrebných kontaktov)

Dokument je pripravený v spolupráci s nasledovnými firmami a ich odborníkmi na jednotlivé aspekty kybernetickej bezpečnosti. Dokument vychádza z odporúčaní CIS Controls, reflektuje na najzraniteľnejšie oblasti slovenských malých a stredných podnikov, a prináša základné odporúčania pre zvýšenie ich kybernetickej bezpečnosti. Dokument je pripravený aj vďaka grantovej podpore od Center for International Private Enterprise.

sapie · Liga za digitálny rast · CIPE · ANECT · bugino · CITADLO · Evolveum · Excalibur · itaps · IstroSec · KINIT · mastercard · piano · Qubit Conference · SYNAPSA · Void