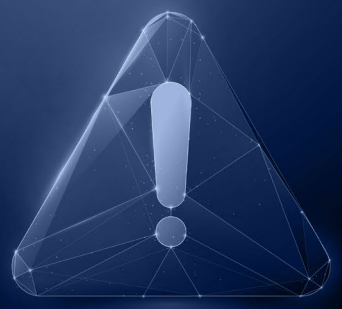
10 MANAŽÉRSKYCH CHÝB
KTORÉ VEDÚ K INCIDENTU



1 CHÝBAJÚCE, ALEBO FORMÁLNE RIADENIE RIZÍK

Neochota zaviesť štandardizované, konsolidované a udržateľné riadenie kybernetických rizík môže viesť k podceňovaniu reálnych hrozieb, čím sa organizácia stáva zraniteľnejšou voči kybernetickým incidentom.

Je potrebné implementovať a udržiavať riadenie rizík, ako bežnú súčasť všetkých procesov.

2 BEZPEČNOSŤ IZOLOVANÁ OD PREVÁDZKY

Organizačná štruktúra, v ktorej prevádzkové procesy a kybernetická bezpečnosť nie sú vzájomne prepojené, vedie k nesúladom a potenciálnym zlyhaniam v ochrane informačných aktív.

Spolupráca prevádzky a kyberbezpečnosti je nevyhnutná pre efektívnu ochranu organizácie.

3 PRESVEDČENIE, ŽE PENIAZE VYRIEŠIA VŠETKO

Prílišné spoliehanie sa na rozpočet, bez súčasného zlepšovania procesov a budovania silnej organizačnej kultúry, nevedie k reálnej odolnosti voči kybernetickým hrozbám.

Udržateľná kybernetická bezpečnosť si vyžaduje rovnováhu medzi finančnými prostriedkami a efektívnym riadením procesov.

4 VNÍMANIE KYBERNETICKEJ BEZPEČNOSTI AKO PREKÁŽKY

Kybernetická bezpečnosť by nemala byť považovaná za prekážku alebo zbytočný náklad.

Bezpečnosť musí byť neoddeliteľnou súčasťou podpory a ochrany základných činností organizácie, pričom prispieva k udržaniu a posilneniu jej dobrého mena.

5 KULTÚRA VINY

Podpora kultúry viny vytvára atmosféru strachu, kde zamestnanci vykonávajú len nevyhnutné minimum. Utajovanie alebo popieranie problémov a rizík však vedie ku skreslenému vnímaniu reality.

Kultúra zodpovednosti, otvorená, trasnsparentná komunikácia a efektívny kontrolný systém sú kľúčové pre udržateľnú úroveň odolnosti voči hrozbám.

6 PREHNANÁ TOLERANCIA RIZIKA

Prílišné riskovanie a vágne vyhlásenia o akceptácii rizika môžu viesť k vážnym dôsledkom, ktoré procesy riadenia kontinuity nemusia zvládnuť a poistenie nemusí pokryť.

Je nevyhnutné mať jasne definované a realistické rámce pre akceptáciu rizika, aby sa minimalizovali potenciálne škody.

7 NEREÁLNE OČAKÁVANIA

Nastavenie nereálnych očakávaní od bezpečnostných opatrení a procesov riadenia bezpečnosti môže viesť k zlyhaniam.

Je dôležité mať jasný, realistický plán, ktorý zohľadňuje aktuálne spôsobilosti a dostupné personálne, finančné a časové zdroje.

8 TECHNOKRATICKÁ BEZPEČNOSTNÁ STRATÉGIA

Zameranie sa na technológiu, bez dostatočného dôrazu na ľudí, ich vzdelávanie a angažovanosť, vedie k zraniteľnostiam, ktoré technológia sama o sebe nedokáže pokryť.

Ľudský prvok v stratégii kybernetickej bezpečnosti nesmie byť prehliadaný.

9 IGNOROVANIE VNÚTORNÝCH HROZIEB

Vnútorné hrozby predstavujú významné riziko, ktoré môže pochádzať od zamestnancov alebo dodávateľov organizácie. Tieto osoby môžu úmyselne, neúmyselne alebo z neznalosti spôsobiť incident, ako je únik citlivých informácií, zastavenie prevádzkových činností alebo nenávratnú stratu dát.

Včasná identifikácia a riadenie vnútorných hrozieb je nevyhnutné pre komplexnú ochranu organizácie.

10 CHÝBAJÚCE RIADENIE KONTINUITY

Prírodné katastrofy, kybernetické útoky, nedostupnosť zdrojov, alebo závažné poruchy technológie bez krízového plánu môže viesť k dlhodobým výpadkom produkcie, strate dôvery zákazníkov, reputačným škodám a v konečnom dôsledku aj k finančným stratám.

Prostredníctvom procesu riadenia kontinuity činností (Business Continuity Management - BCM) organizácia dokáže reagovať na nečakané udalosti a obnoviť svoje kľúčové aktivity v čo najkratšom čase.

Spolufinancovaný Európskou úniou

Financované Európskou úniou. Vyjadrené názory a postoje sú názormi a vyhláseniami autora(-ov) a nemusia nevyhnutne odrážať názory a stanoviská Európskej únie. Európska únia za ne nepreberajú žiadnu zodpovednosť.

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Kompetenčné a certifikačné centrum kybernetickej bezpečnosti

ISBN 978-80-69011-39-7
Verzia V.1

www.cybercompetence.sk