

10 KROKOV KU KYBERNETICKEJ BEZPEČNOSTI

1

Riadenie rizík

Na zabezpečenie vašich údajov a systémov si osvojte prístup založený na riziku

2

Trénujte a vzdelávajte

Spoločne budujte bezpečnosť uplatniteľnú pre všetkých zamestnancov vo vašej organizácii

3

Správa aktív

Identifikujte dáta a ostatné informačné aktíva a namapujte procesy, ktoré sú nimi podporované

4

Architektúra a konfigurácia

Navrhujte, implementujte, udržiavajte a spravujte systémy bezpečným spôsobom

5

Správa zraniteľnosti

Chráňte systémy počas celého ich životného cyklu

6

Správa identity a riadenie prístupu

Riadte kto a čo môže pristupovať k vašim dátam a informačným aktívam

7

Bezpečnosť dát

Kontrolujte funkčnosť zálohovacieho procesu a overujte proces obnovy

8

Logovanie a monitorovanie

Navrhňte svoje systémy tak, aby ste boli schopní detegovať a vyšetrovať incidenty

9

Riešenie incidentov

Vopred si naplánujte reakcie na kybernetické incidenty

10

Zabezpečenie dodávateľského reťazca

Spolupracujte so svojimi dodávateľmi a obchodnými partnermi



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 nepreberá žiadnu zodpovednosť.



NCC-SK
SLOVAKIA CYBERSECURITY
COORDINATION CENTRE



ECCC
EUROPEAN CYBERSECURITY
COMPETENCE CENTRE



Kompetenčné
a certifikačné
centrum
kybernetickej
bezpečnosti

www.cybercompetence.sk