

Komora manažérov kybernetickej bezpečnosti

Partnerstvo pri príprave budúcich odborníkov kybernetickej bezpečnosti



Ing. Rastislav Kopper

Kto sme – KMKB



Naša identita

Občianske združenie združujúce približne 300 manažérov kybernetickej bezpečnosti z praxe.

300+ odborníkov

Manažéri kybernetickej bezpečnosti z praxe

Komplexné služby

Metodiky, školenia, cvičenia, mentoring

Naša misia

Prepájame priemysel, školy a verejný sektor. Ponúkame metodiky, školenia, cvičenia a mentoring s cieľom posilniť pripravenosť absolventov podľa potrieb trhu a legislatívy.

Prepojenie sektorov

Priemysel, školy a verejný sektor

Prečo NIS2 a nový zákon o kybernetickej bezpečnosti

Legislatívny rámec zvyšuje nároky na prax a vyžaduje si kvalifikovaných odborníkov.

01

Riadenie rizík

NIS2 a národná implementácia NBÚ vyžadujú systematické riadenie kybernetických rizík

02

Zvládanie incidentov

Povinnosť efektívne reagovať na bezpečnostné incidenty a minimalizovať ich dopad

03

Kontinuita služieb

Zabezpečenie neprerušného fungovania kritických služieb a procesov

04

Preukázateľnosť

Dokumentácia a dôkazy o implementácii bezpečnostných opatrení

Talentová potrubná trasa = prepojená cesta od strednej školy cez terciárne vzdelávanie až po juniorské pracovné pozície v praxi. Školy formujú vstup do tejto trasy.

Dopyt po základne pripravených absolventoch rastie naprieč odvetvami vo verejnom aj súkromnom sektore.



Tri ilustračné incidenty z praxe

Reálne situácie, ktorým možno predchádzať správnou prípravou a povedomím.



1

Škodlivá príloha

Šifrovanie dát po otvorení infikovanej prílohy v e-maile. Následok: prerušenie výroby alebo výučby, vysoké náklady na obnovu systémov a dát.

2

Únik osobných údajov

Neúmyselný únik osobných údajov porušujúci GDPR cez nesprávne zdieľaný Excel súbor alebo cloudový priečinok s nevhodnými prístupovými právami.

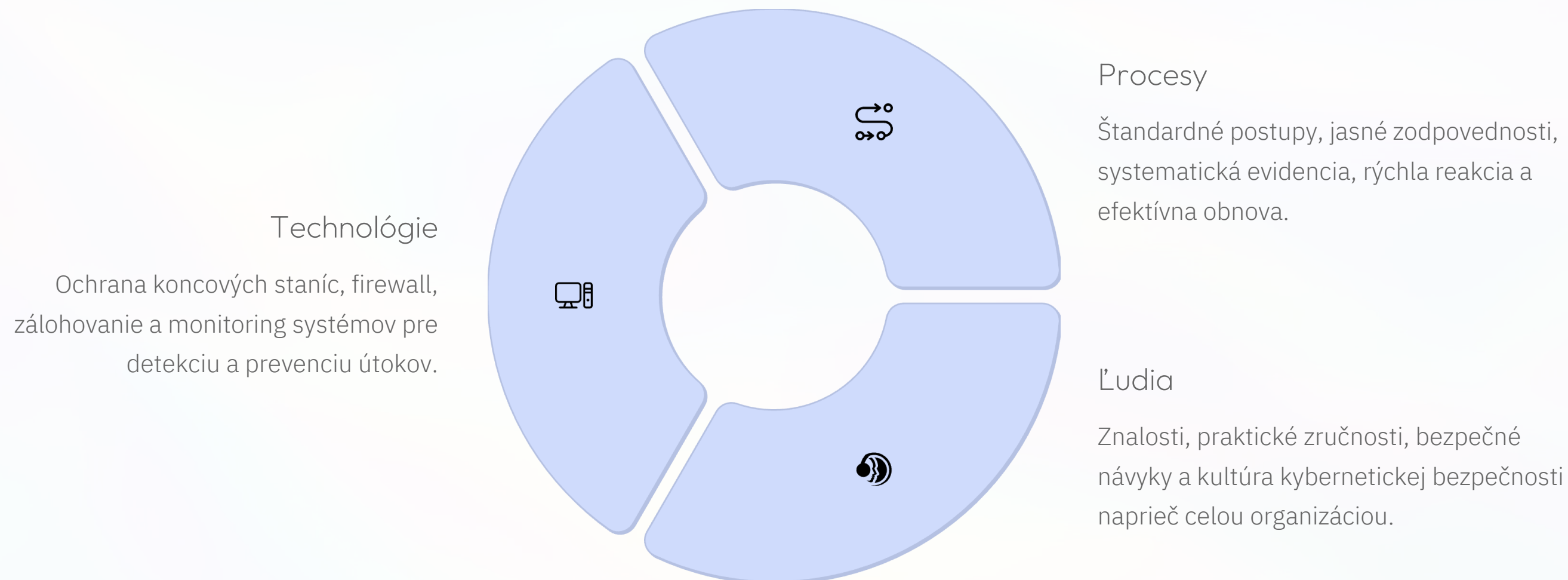
3

Chybná sieťová konfigurácia

Nesprávne nastavená sieťová infraštruktúra, najmä segmentácia a ACL (Access Control Lists), vedúca k výpadkom a vážnym bezpečnostným medzerám.

Prevenencia incidentov si vyžaduje zdroje

Technológie, procesy a ľudia – tri roviny pripravenosti na kybernetické hrozby.



Cybersecurity Awareness Training

Ľudia ako kľúčový zdroj

Povedomie, základné znalosti a správne hlásenie incidentov sú fundamentom bezpečnosti.

Základy bezpečného správania

- Silné heslá a viacfaktorová autentifikácia (MFA)
- Bezpečná práca s e-mailom a prílohami
- Opatrnosť pri používaní Wi-Fi a USB zariadení

Porozumenie infraštruktúre

Základné pochopenie prepojenia: PC → switch → firewall → server → databáza → cloud

Rozlišovanie incidentov

Nie každé hlásenie "nejde to" je bezpečnostný incident - napríklad prázdna tlačiareň, výpadok Wi-Fi alebo elektriny.





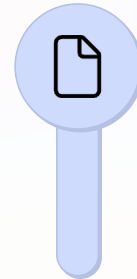
Prečo začínať už na stredných školách

Formovanie základov kybernetickej bezpečnosti pred vstupom do praxe je kľúčové.



Rozvoj kritického myslenia

Stredné školy dokážu rozvíjať kritické myslenie a základné infraštruktúrne a bezpečnostné kompetencie u študentov.



Praktické aktivity

Projekty a cvičenia prepájajú teoretické poznatky s reálnym kontextom a praktickými situáciami z praxe.



Ľahšie začlenenie

Absolvent so základnými znalosťami sa ľahšie a rýchlejšie začlení do firemného zaškoľovania a pracovných procesov.

Potrebné zručnosti absolventov

Job-ready minimum v kybernetickej bezpečnosti pre úspešný vstup do praxe.

Kritické myslenie a analytické uvažovanie
Schopnosť analyzovať situácie, identifikovať problémy a navrhovať riešenia

Sieťové pojmy
IP adresácia, DNS, DHCP, segmentácia siete a ich praktické využitie

Základy infraštruktúry
Pochopenie čo je server, switch, firewall, databáza a ako na seba nadväzujú

Bezpečnostné princípy
CIA triáda, princíp minimálnych oprávnení, zálohovanie a obnova dát

Práca s dátami

Pochopenie kde sú dáta uložené (PC, cloud, dátové centrum) a ako s nimi bezpečne narábať

GDPR základy

Osobné údaje, minimalizácia, bezpečné zdieľanie a anonymizácia informácií

Povedomie o incidentoch

Rozpoznať podozrivú situáciu, správne nahlásiť a nezasahovať neodborne



Riešenie: školenie pre učiteľov IT

Učiteľ ako multiplikátor bezpečnostných kompetencií v oblasti kybernetickej bezpečnosti.



Cielené školenia a metodiky

Metodické listy pre učiteľov IT vrátane ukážkových cvičení a praktických materiálov



Mikro-cvičenia

Praktické "mikro-cvičenia" realizovateľné v bežnej PC učebni bez špeciálneho vybavenia

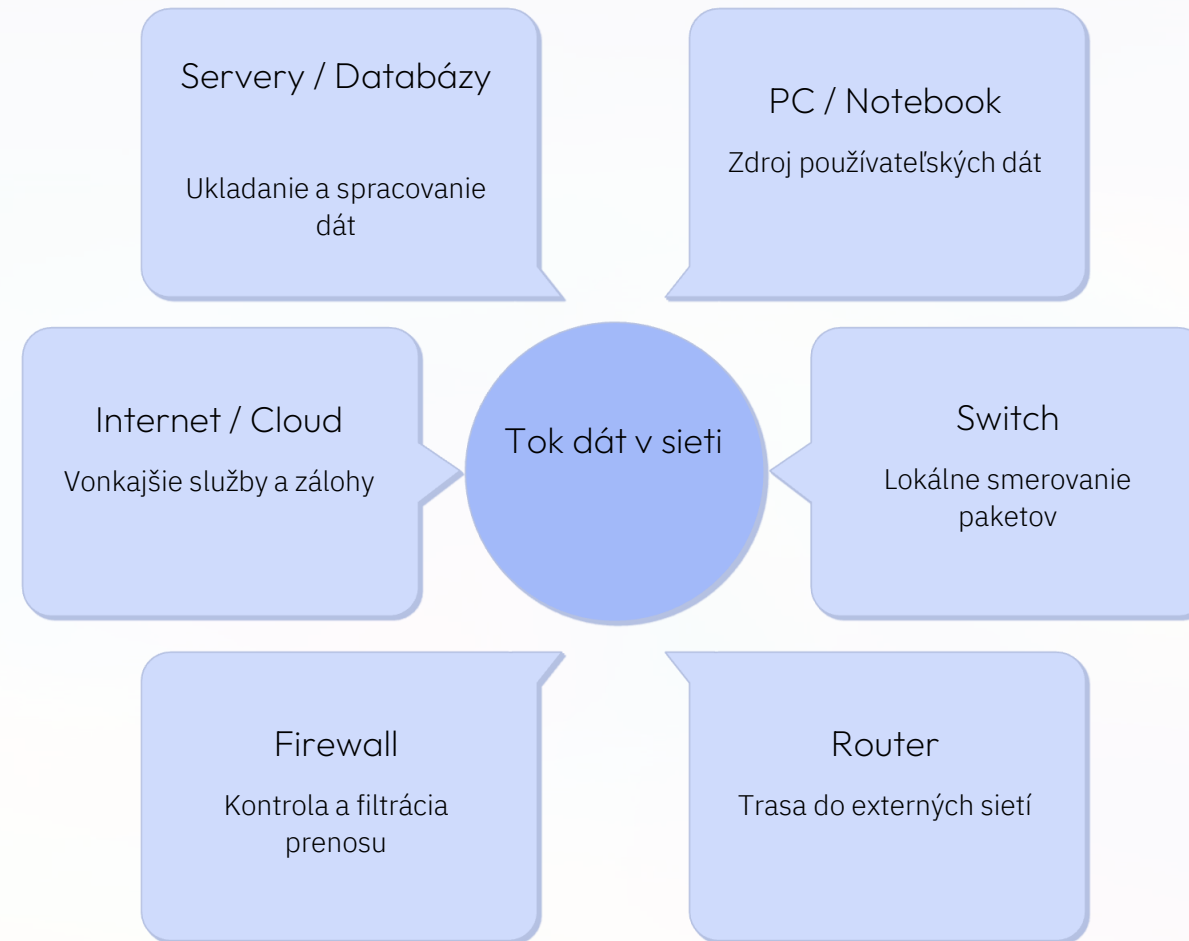


Hosťovské vstupy odborníkov

Spolupráca s odborníkmi z KMKB, spoločné vyhodnotenia a praktické odporúčania

Základné pochopenie fungovania siete

Sieť ako prepojený systém hmatateľných komponentov pre všetkých zamestnancov.



"Kde bývajú dáta"

Pochopenie ako pristupujeme k dátam - práva, logovanie, zálohy a ich umiestnenie v infraštruktúre.

Zodpovednosť za zariadenia

Každé pripojené zariadenie prináša zodpovednosť - aktualizácie, prístupové práva a bezpečnostné nastavenia.



Digitálna gramotnosť

Word, Excel, PowerPoint - kompetencie bez dodatočného zaškoľovania. Excel: filtre, kontingenčné tabuľky, XLOOKUP/VLOOKUP. Správne zdieľanie, kontrola prístupov, anonymizácia a bezpečné ukladanie.



edushield[®]
Protecting our future. one educator at a time



Spolupráca s KMKB

KMKB má odborníkov. Sme pripravení pomôcť. Hľadáme spoločne "ako na to".



Konzultácie a poradenstvo

Odborné konzultácie pre školy v oblasti kybernetickej bezpečnosti a prípravy študentov



Hosťovské prednášky

Praktické prednášky od odborníkov z praxe pre študentov a učiteľov



Metodiky a cvičenia

Pripravené metodické materiály, praktické cvičenia a mentoring programy



Spoločná príprava aktivít

Vyhodnotenie aktivít s ohľadom na požiadavky praxe a legislatívy

 **Kontakt:** rastislav.kopper@kmb.sk