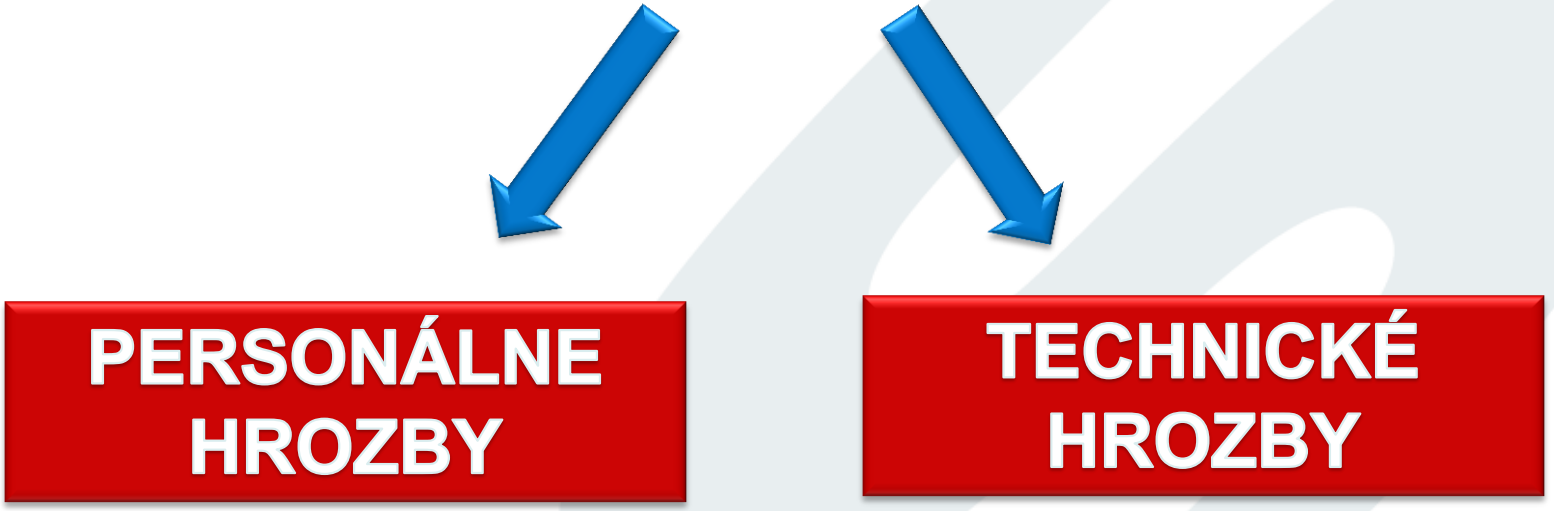
BEZPEČNÁ ŠKOLA

Daniel Schikor – schikor@somi.sk

Bezpečnostné projekty

Celkový počet projektov na školách	135
Základné školy	97
Stredné školy	33
Vysoké školy / univerzity	5
Celkovo vypracovaných projektov	575

ZISTENÉ NEDOSTATKY



Heslá sa pravidelne nemenia, nenastavená zložitosť hesla – 85%

- Jediná ochrana Vašich údajov v počítači a internetových službách (e-mail, internet banking, súkromné dáta)
- Sprístupnenie dát a obsahu cudzím osobám

Bezpečnostná smernica, autorizácia pri prihlásení do siete.

Nekontrolované používanie USB zariadení – 100%

- Strata dát
- Sprístupnenie neželaných údajov tretím stranám
- Zavírenie PC a serverov

Bezpečnostná smernica, kontrola používania USB zariadení (napr. NOD32).

Nezabezpečenie USB zariadení pri prenose citlivého obsahu – 100%

- Sprístupnenie citlivých údajov tretím stranám
- Negatívne meno, negatívna reklama

Bezpečnostná smernica, zabezpečenie obsahu heslom alebo šifrovaním.

Nedostatočné a nepravidelné zálohovanie – 70%

- Strata dôležitých dát
- Nikto sa nespýta, či to bolo úmyselne, alebo nie
- Zdĺhavé a prácne znovu obnovovanie stratených údajov (ak vôbec!!!)

Vybudovanie centrálneho zálohovacieho úložiska pre všetky počítače a aplikácie.

Žiadna kontrola mailovej komunikácie, používanie freemailových služieb – 75%

- Neželaný únik dát prostredníctvom e-mailu
- Súkromná pošta zmiešaná s pracovnou agendou
- Zvýšený počet neželaných e-mailov (spamov)
- Vysoké riziko zavírenia počítača mailovými vírusmi

Umiestnenie mailového servera vo vlastných priestoroch.

Dôležité IS sú uložené v počítači, v ktorom sa vykonávajú aj iné činnosti a iná agenda – 78%

- Neúmyselné zmazanie údajov v informačnom systéme
- Znefunkčnenie informačného systému pri inej činnosti
- Zlyhaním jedného počítača „padnú“ všetky IS a agendy
- Celá škola nemôže fungovať bežný spôsobom

Zriadenie samostatného servera pre informačné systémy.

Nekontrolovaný prístup k internetovému obsahu – 80%

- Voľný prístup žiakov a študentov k nevhodnému obsahu na internete (hry, facebook, erotické stránky, kyberšikana...)
- Nemožnosť kontroly sťahovaného obsahu z Internetu
- Zvýšené riziko zavírenia počítačov a školskej siete
- Zdĺhavé ručné nastavovanie blokovaných stránok
- Zlé meno školy, žaloby, udania, súd...

Vybudovanie internetového prístupového bodu.

Všetky počítače sú umiestnené na jednej sieti, vrátane Wi-Fi – 83%

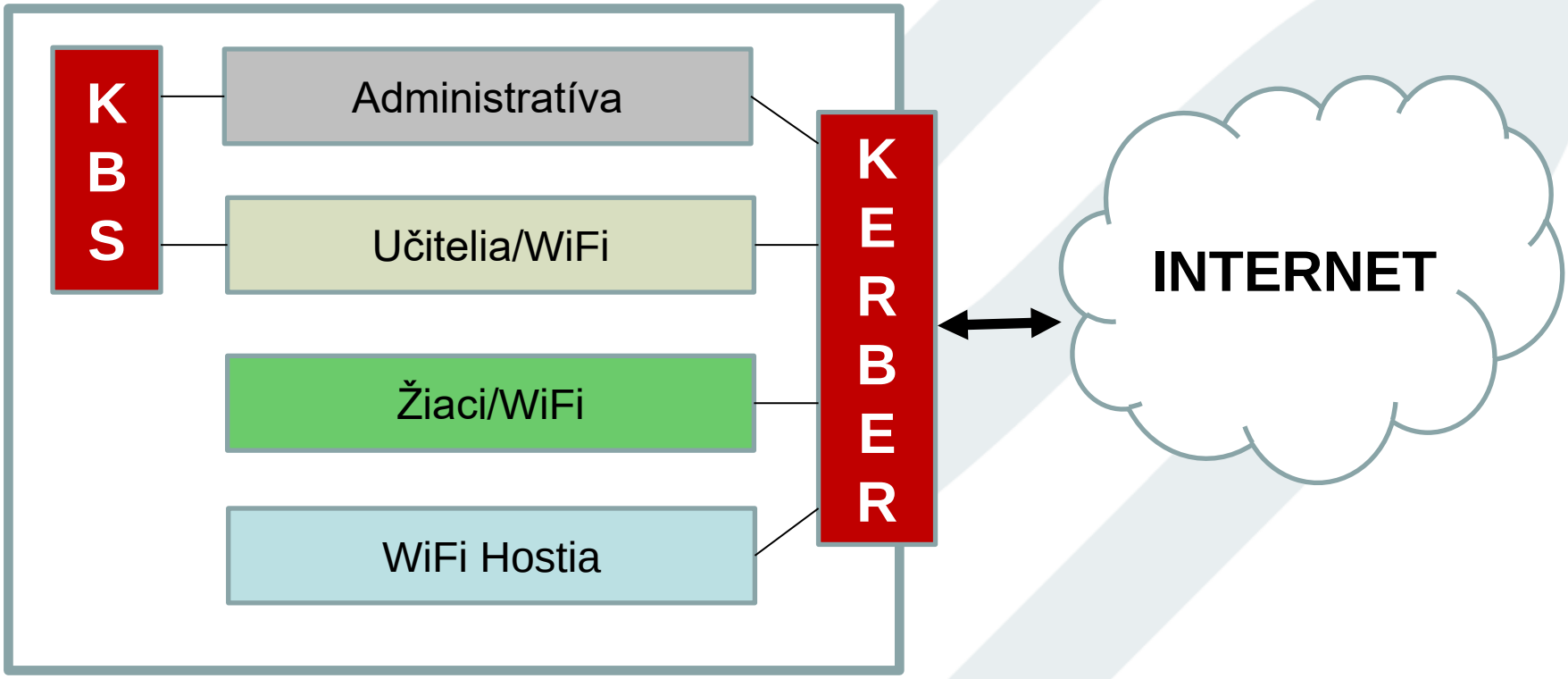
- Svojvoľný prístup kohokoľvek do akéhokoľvek počítača v lokálnej sieti
- Krádež dát - jednoduchý prístupu k údajom osobami, ktoré na to nemajú oprávnenie
- Zahltenie Wi-Fi siete, výpadky siete
- Nemožnosť nastavenia rôznych pravidiel pre jednotlivé siete (administratíva, učitelia, žiaci, návštevy...)

Oddeliť administratívnu časť od počítačov žiakov a Wi-Fi siete.

Čo odporúčame urobiť

- Vykonať kvalitnú rizikovú analýzu IT infraštruktúry a odhaliť možné hrozby.
- Vypracovať interné dokumenty pre informačnú bezpečnosť a oboznámiť s nimi zamestnancov.
- Bezprostredne vykonať opatrenia, ktoré eliminujú najväčšie riziká:
  - Oddeliť jednotlivé siete
  - Zabezpečiť kontrolu prístupových bodov do internetu
  - Zabezpečiť kontrolu internetového obsahu a mailovej komunikácie
  - Centralizovať IS a zabezpečiť ich pravidelné zálohovanie
- Kontrolovať dodržiavanie zavedených pravidiel, pravidelne oboznamovať zamestnancov s novinkami v informačnej bezpečnosti.

Ako na to


KBS
Administratíva
Učitelia/WiFi
Žiaci/WiFi
WiFi Hostia
KERBER
INTERNET

SOMI systems

Bezpečná škola