KYBERNETICKÁ BEZPEČNOSŤ

OD KOHO VLASTNE ZÁVISÍ?

Rastislav Janota

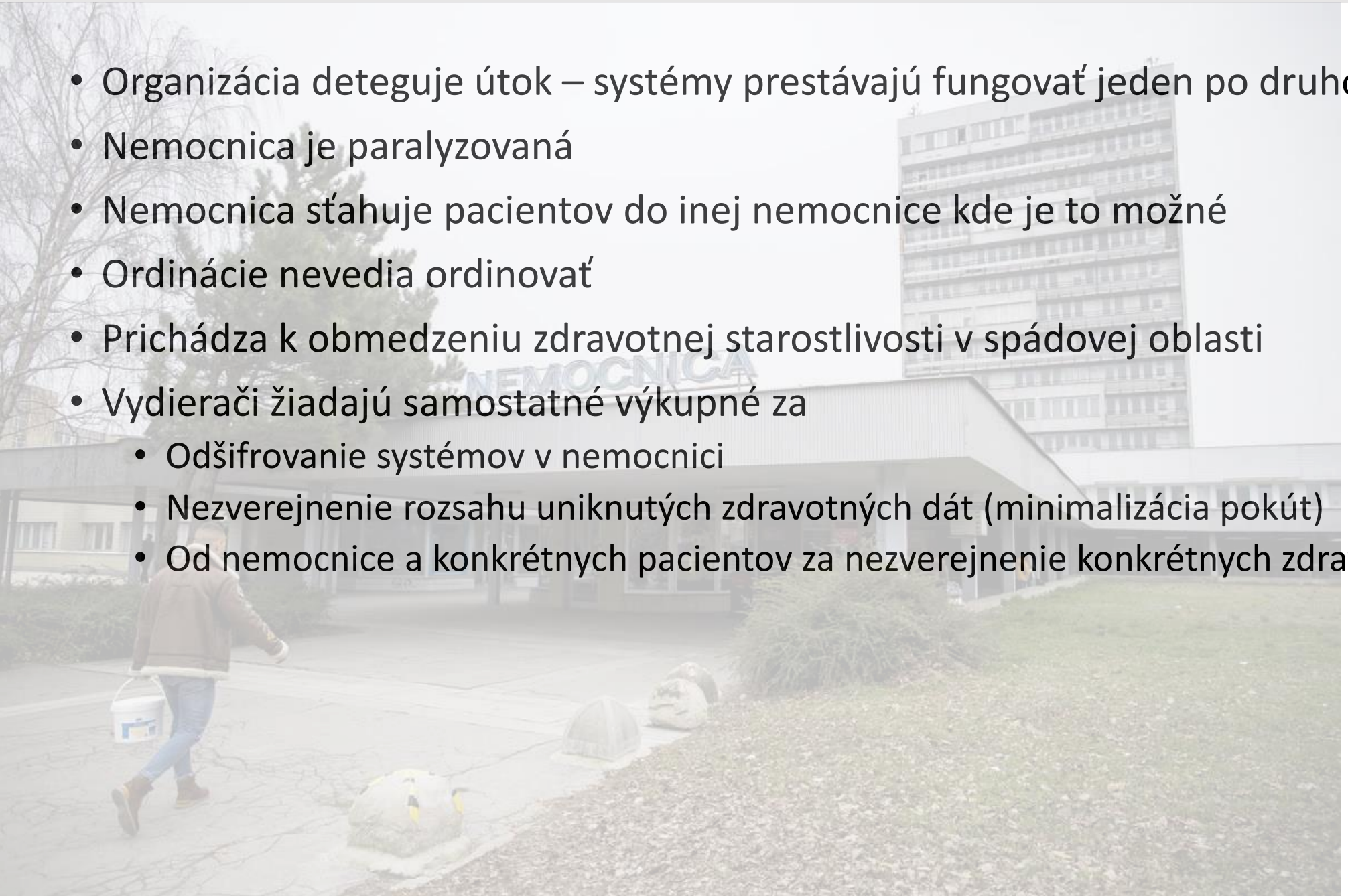
Riaditeľ

Národné centrum kybernetickej bezpečnosti SK-CERT

Príklad 1 / Ransomware útok na teplárenskú spoločnosť

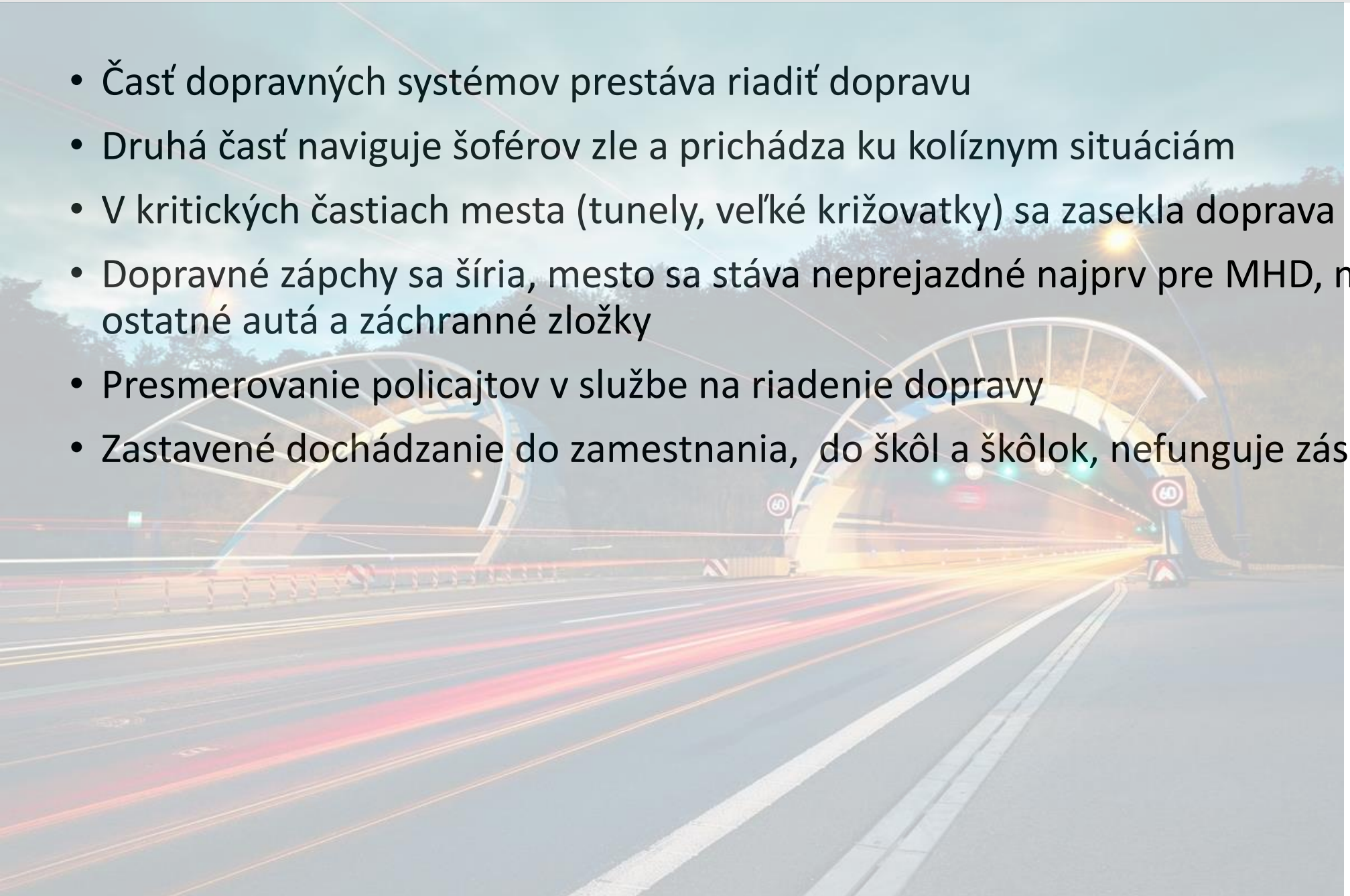
- Organizácia deteguje útok – systémy prestávajú fungovať jeden po druhom
- Riadiace stredisko stratilo možnosť riadiť výrobu
- Výroba tepla sa automaticky vypína
- Zákazníkom chýba teplá voda a majú studené radiátory
- Prvé reakcie sú od pripojených kritických organizácii – nemocnice, zdravotné strediská ale samozrejme organizácie, občania, firmy
- Nemocnica sťahuje pacientov do inej nemocnice
- Zdravotné strediská ordinujú len niektoré
- Ľudia sa snažia nakúpiť rýchlo elektrické ohrievače do bytov, tieto zapájajú
- Prichádza k preťaženiu distribučnej siete elektriny a selektívnemu vypínaniu

PRÍKLAD 2 / RANSOMWARE ÚTOK NA NEMOCNICU



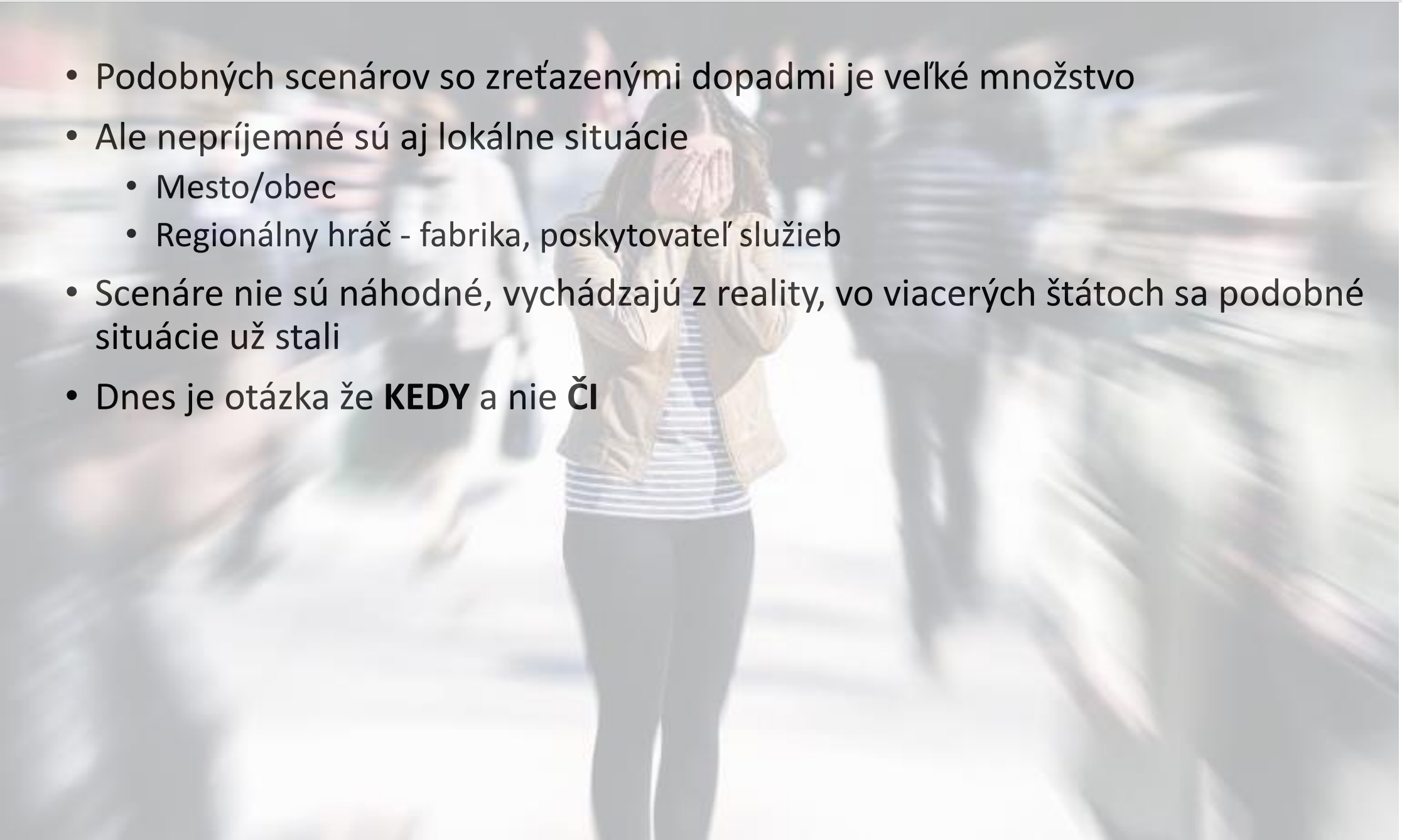
- Organizácia deteguje útok – systémy prestávajú fungovať jeden po druhom
- Nemocnica je paralyzovaná
- Nemocnica sťahuje pacientov do inej nemocnice kde je to možné
- Ordinácie nevedia ordinovať
- Prichádza k obmedzeniu zdravotnej starostlivosti v spádovej oblasti
- Vydierači žiadajú samostatné výkupné za
  - Odšifrovanie systémov v nemocnici
  - Nezverejnenie rozsahu uniknutých zdravotných dát (minimalizácia pokút)
  - Od nemocnice a konkrétnych pacientov za nezverejnenie konkrétnych zdravotných dát

PRÍKLAD 3 / ÚTOK NA RIADIACI SYSTÉM CESTNEJ DOPRAVY



- Časť dopravných systémov prestáva riadiť dopravu
- Druhá časť naviguje šoférov zle a prichádza ku kolíznym situáciám
- V kritických častiach mesta (tunely, veľké križovatky) sa zasekla doprava
- Dopravné zápchy sa šíria, mesto sa stáva neprejazdné najprv pre MHD, následne pre ostatné autá a záchranné zložky
- Presmerovanie policajtov v službe na riadenie dopravy
- Zastavené dochádzanie do zamestnania, do škôl a škôlok, nefunguje zásobovanie

REALITA



- Podobných scenárov so zreťazenými dopadmi je veľké množstvo
- Ale nepríjemné sú aj lokálne situácie
  - Mesto/obec
  - Regionálny hráč - fabrika, poskytovateľ služieb
- Scenáre nie sú náhodné, vychádzajú z reality, vo viacerých štátoch sa podobné situácie už stali
- Dnes je otázka že **KEDY** a nie **ČI**

KYBERNETICKÁ BEZPEČNOSŤ

- **Sa týka nás všetkých**
- Predstava, že *“ja nie som zaujímavý“* nefunguje
  - Každý je zaujímavý – každý má cenné údaje – najmenej tie svoje vlastné
  - Každý má nejaké zariadenia (telefón, počítač, rôzne IOT zariadenia a pod)
- Každý (z nás) je zraniteľný
  - Ako dlho vydržíme bez telefónu? Bez elektriny? Bez vody či tepla? Bez zubára?
  - Predstavme si nedostupné bankomaty, či nefungujúcu platbu kartou v obchodoch
  - Obmedzené služby, problém nakúpiť pohonné hmoty, nefungujúce semafory
- Aj firmy sú veľmi zraniteľné
  - Operatívne – zastavená výroba či nemožnosť poskytovať svoje služby
  - Dlhodobé problémy
    - Únik know-how, poškodenie dobrého mena, odliv zákazníkov ku konkurencii
  - V oboch prípadoch veľké finančné škody, možné prepúšťanie, či úplné zavretie firmy

- Sústredenie na VŠETKY tri atribúty bezpečnosti samostatne aj v súvislosti
  - Dôvernosť údajov (confidentiality) – k informácii, ktorú údaje obsahujú nemajú prístup nepovolané osoby
  - Integrita údajov (integrity) – údaje nemôžu byť modifikované bez toho, aby si to oprávnená osoba všimla
  - Dostupnosť údajov (availability) – oprávnená osoba má údaje (službu, produkt, proces) k dispozícii kedykoľvek, keď o to požiada

- Zodpovednosť je neprenosná
  - Business zodpovednosť majiteľa resp. vedenia/top managementu
  - Nemožnosť preniesť akúkoľvek zodpovednosť (ani business zodpovednosť ani zákonné zodpovednosti) na tretie strany
  - Outsourcing (aj cloud je len OBYČAJNÝ outsourcing) pomáha s výkonom vybraných činností ale NEPREBERÁ zodpovednosť

ĎAKUJEM

Rastislav Janota

rastislav.janota@nbu.gov.sk

NÁRODNÝ BEZPEČNOSTNÝ ÚRAD

SK CERT