

Lesk a bída krizových plánů



Monika Kudrlová
Jaroslav Pejčoch
T-SOFT a.s.





Jak jsme na tom?

Prověrka cvičením



Všetchno je o
lidech...



Záchranka

Pacient č.:	68	
Vůz č.:	725	
Pacient č.:	26	
Vůz č.:	519	
Pacient č.:	20	
Vůz č.:	128	
Pacient č.:	3	
Vůz č.:	516	
Pacient č.:	14	
Vůz č.:	620	
Pacient č.:	35	
Vůz č.:	620	

Cvičení záchranky (HZS, PČR, nemocnice)

- Profesionálové, kteří vše berou vážně
- Cvičí různé situace, používají figuranty
- Přesně dané a popsané postupy jednotlivých rolí
- Operativní cvičení zaměřené jednak na správnost postupu, ale i čas, jak dlouho činnost trvá
- Každá role má svého rozhodčího



Ústřední orgán



Požár na resortu A

- Zájem top managementu, dobrá příprava
- Během cvičení diskuse a hledání, jak problémy řešit
- Krizař
 - cvičení bojkotoval, nedodal podklady
 - cvičení se nezúčastnil, ve scénáři vynechán = byl na dovolené 😊
- V suterénu je dětská skupina, na kterou nikdo nepomyslel a děti by uhořely ☹️

1

Kybernetický útok na resortu B

- Slovíčkaření a formalismus (strach z namazaných schodů...)
- Texty a dokumenty, které by při skutečném útoku resort vydával, byly připraveny a dopilovány k naprosté dokonalosti
- Součástí cvičení byl i penetrační test, v noci a během cvičení probíhal utajený cvičný DDOS
- Informace o DDOS na cvičné zasedání krizového štábu nedoputovala (vše v pořádku, nic se neděje)

5

Blackout



Blackout v Praze



- Velké cvičení, dlouhá příprava
 - Problémy s vyhledáním důležitých dat
 - Rezervovanost ke spolupráci
 - Metro jako problém, posléze jako záchrana
 - Společný obraz situace
- Skutečný výpadek - celé cvičení proběhlo na diesel agregátech
- Otevřená a tvrdá diskuse (nemocnice, zásobování operátorů naftou, ...)
- Spolupráce s médii, veřejný portál

Blackout okresního města

- Skvělá spolupráce na přípravě scénáře
- Při vlastním cvičení řekl moderátor jenom jednu větu, zbytek už si účastníci vydiskutovali sami
- Když nebylo jasné, kdo by měl danou činnost řešit, sami se hlásili „To zajistíme my!“
- Nespolupracujícího účastníka-rolí (správa majetku) sami zaúkolovali, že danou problematiku musí vyřešit



Blackout ve státním podniku

- Nezájem při přípravě
- Zlehčování a výsměch od pracovníků ICT
- Vlastní cvičení zcela formální, otrávení účastníci
- ICT by nemělo problém blackout přestát a všechna oddělení by bez problémů bez ICT mohla pracovat (šli by domů, celá agenda by počkala, až elektrická energie zase naběhne)
- ... k čemu je tedy to ICT?

5



Požár v celostátní organizaci

3

- Dvě hodnocení, jedno pouze pro přísně úzký okruh lidí
- Několik hodně závažných nedostatků v tichosti odstraněno
- Nefunkční EPS, obsluha vrátnice vůbec neví, co má dělat, není schopna volat HZS, otevřít turnikety
- Požární hlídka nervózní a neumí velet (při evakuaci)
- Neexistence operativní karty (dokumentace pro HZS)
- Budova včetně datového centra za miliardu by lehla popelem, ale management by neměl problém zajistit finance na výstavbu nové
- Dobrá spolupráce při přípravě scénáře a snaha zadavatele o nápravu, ale po 5 letech je vše téměř stejné



Kybernetický útok na výzkumnou organizaci

- Zodpovědný a aktivní ředitel
- Příprava scénáře posloužila jako jistý druh analýzy (existující stav ICT, největší hrozby, způsob monitoringu a detekce, dopady do fungování organizace) se závěry, co a jak udělat lépe
- Největší problém by byla ztráta dat (3 petaB historických dat = obtížnost offline záloh), bez nich nedostanou nový výzkumný projekt
- Vstřícnost a zájem ICT
- Vlastní cvičení ani neproběhlo, není potřeba
- Nejasný postup jak případně zaplatit výkupné (v Bitcoinech)

1



Závěr

Krizové plány nestačí – je potřeba krizová připravenost.