

Notifikácie bezpečnostných incidentov



Zuzana Hečko

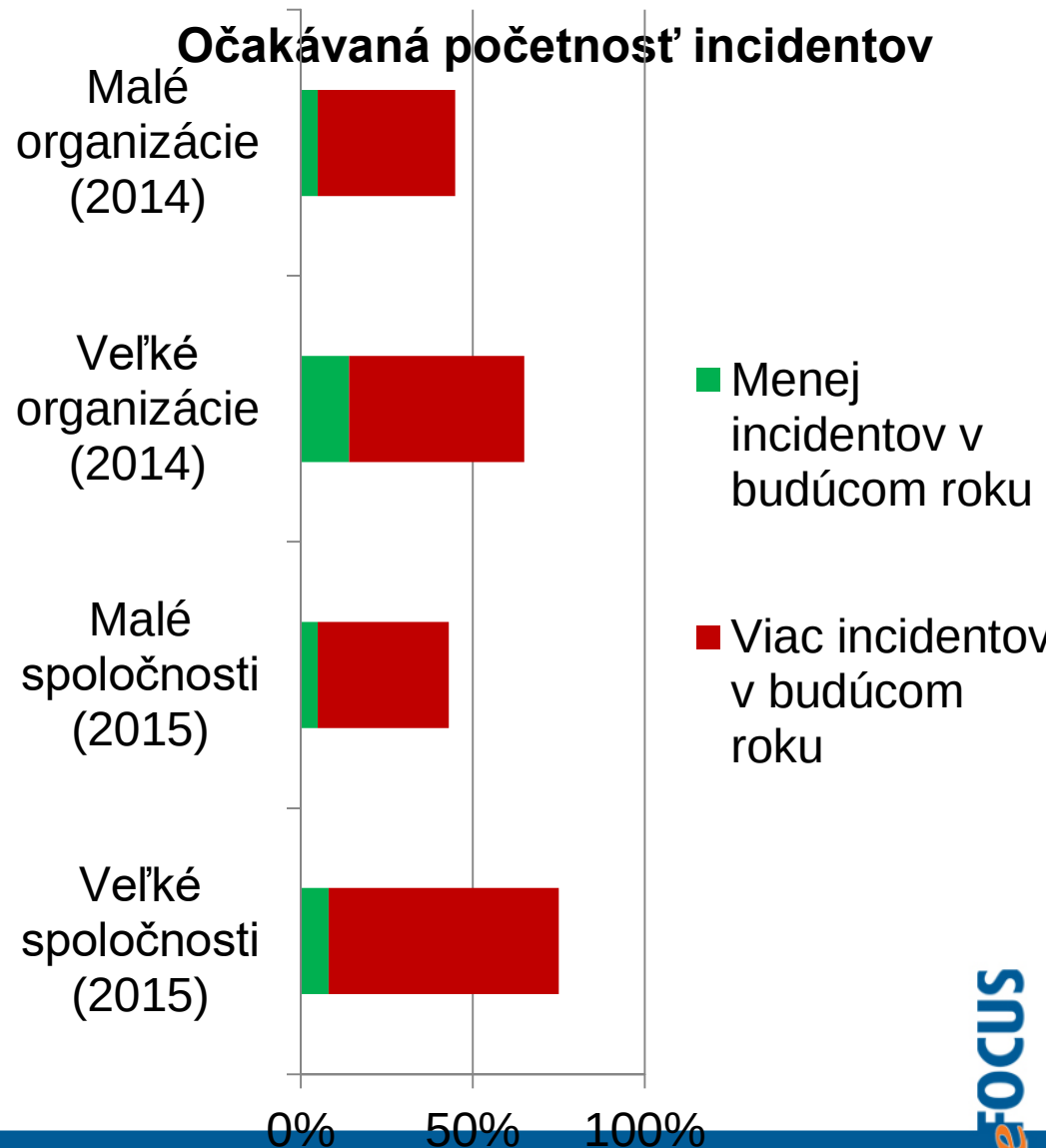
Allen & Overy Bratislava, s.r.o.

eFOCUS

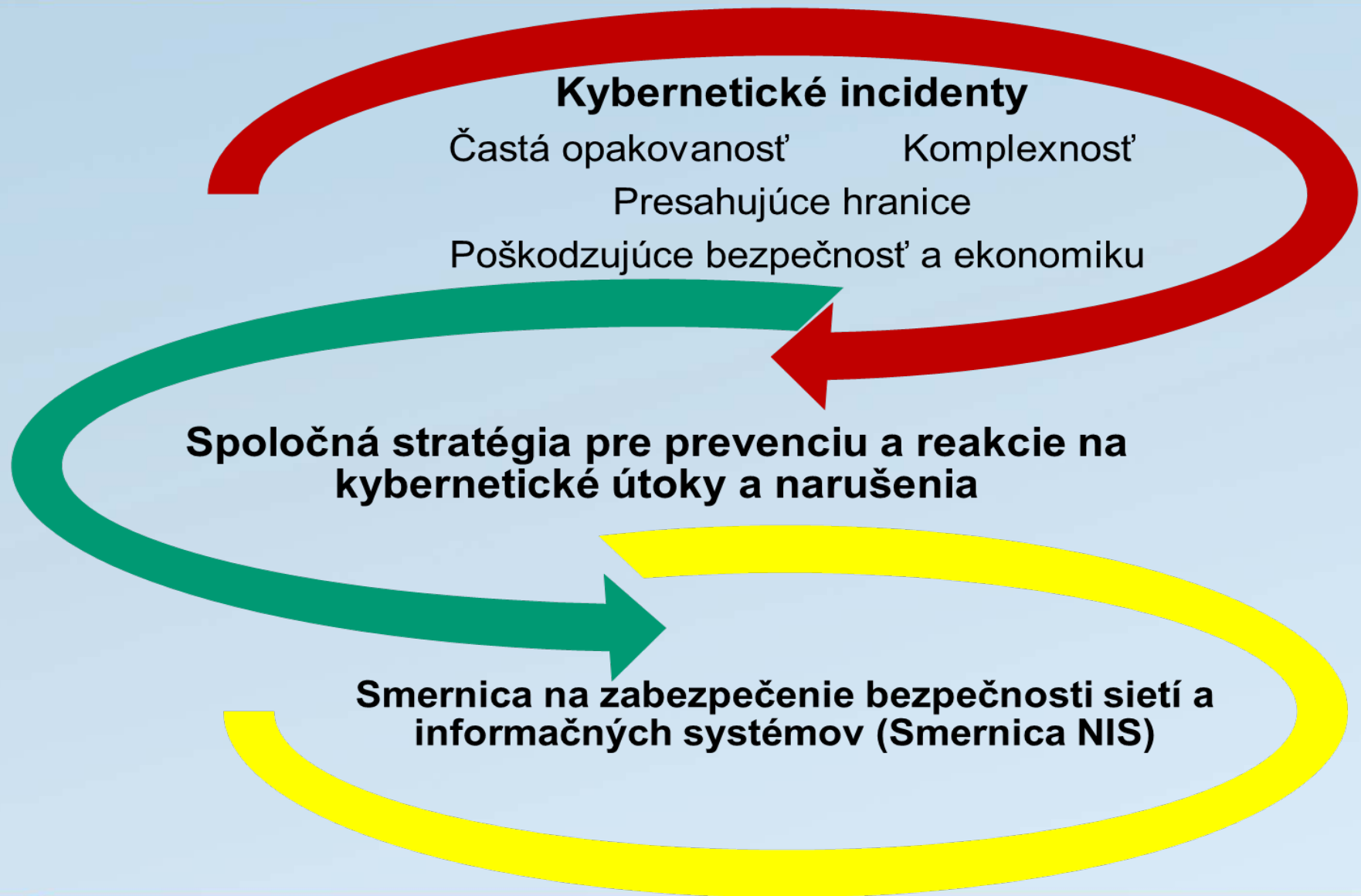
Logo partnera

Bezpečnostné incidenty

- U 9 z 10 veľkých spoločností došlo k narušeniu bezpečnosti
- 71% veľkých spoločností bolo postihnutých bezpečnostnými incidentmi a 66% z nich vážnymi incidentmi
- 77% malých spoločností bolo postihnutých bezpečnostnými incidentmi a 25% z nich vážnymi



Prečo je (údajne) potrebné notifikovať incidenty?



Oznamovacia povinnosť

Legislatívne snahy však vyústili do situácie, kde jeden (a ten istý) incident bude potrebné (súčasne) oznámiť viacerým regulátorom

Oznamovacia povinnosť podľa Smernice NIS

Oznamovacia povinnosť podľa
všeobecného nariadenia o ochrane údajov

Oznamovacia povinnosť podľa Smernice o
platobných službách



Koľko času zostáva?

- **Smernica NIS-** prijatá Európskym parlamentom **6. júla 2016**, publikovaná **19. júla 2016**, v účinnosti od **1. augusta 2016**, implementácia jednotlivými členskými štátmi do **9. mája 2018**, implementácia v kompetencii NBÚ
- **Všeobecné nariadenie o ochrane osobných údajov (GDPR):** **máj 2018**
- **Smernica o platobných službách 2015/2366 (PDS2)-** implementácia do **januára 2018**, v kompetencii MF SR



Oznamovacia povinnosť podľa GDPR

- **Kto musí oznamovať?**
 - Každý prevádzkovateľ a sprostredkovateľ
- **Ktoré incidenty je potrebné oznámiť?**
 - Personal Data breach „Porušenie ochrany osobných údajov“
 - Porušenie bezpečnosti, ktoré vedie k náhodnému alebo nezákonnému zničeniu, strate, zmene, neoprávnenému poskytnutiu osobných údajov, ktoré sa prenášajú, uchovávajú alebo inak spracúvajú, alebo neoprávnený prístup k nim
- **Komu je potrebné incident oznámiť?**
 - Úradu na ochranu osobných údajov
 - Taktiež dotknutým osobám (vo vybraných prípadoch)
- **Do kedy je potrebné incident oznámiť?**
 - Bez zbytočného odkladu resp. najneskôr do 72 hodín od okamihu, ako sa prevádzkovateľ dozvedel, že došlo k porušeniu ochrany osobných údajov.
 - Ak nie je možné oznámenie podať do 72 hodín, malo by sa k oznámeniu pripojiť odôvodnenie omeškania
- **Sankcie**
 - Až do výšky EUR 10 000 000 resp. 2% z globálneho ročného obratu spoločnosti podľa toho, ktorá suma je vyššia



Oznamovacia povinnosť podľa smernice NIS

- **Kto musí oznamovať?**
 - **Operators of essential services** (prevádzkovatelia základných služieb): energetika, transport, bankovníctvo, zdravotníctvo a pod. Nie telekom.
 - **Digital Service providers** (poskytovatelia digitálnych služieb): internetové obchody (s výnimkou poskytovania služieb porovnávania cien), internetové vyhľadávače, služby cloud computingu
- **Ktoré incidenty je potrebné oznámiť?**
 - „**Incident**“ je každá udalosť, ktorá má skutočne nepriaznivý vplyv na bezpečnosť sietí a informačných systémov
 - **Prevádzkovatelia základných služieb** bez zbytočného odkladu oznamujú incidenty, ktoré majú závažný vplyv (*significant impact*) na kontinuitu základných služieb, ktoré poskytujú.
 - **Poskytovatelia digitálnych služieb** musia oznámiť každý incident, ktorý má závažný vplyv (*substantial impact*) na poskytovanie služby, ktorú poskytujú.
- **Komu je potrebné incident oznámiť?**
 - CSIRT (Computer Security Incident Response Teams)
 - CSIRT môže rozhodnúť o zverejnení incidentu
- **Do kedy je potrebné incident oznámiť?**
 - Bez zbytočného odkladu



Oznamovacia povinnosť podľa PDS2

- **Kto musí oznamovať?**
 - **PSP:** Poskytovatelia platobných služieb
 - Úverové inštitúcie, inštitúcie elektronických peňazí (E-money), poštové podniky, platobné podniky)
- **Ktoré incidenty je potrebné oznámiť?**
 - Závažné prevádzkové alebo bezpečnostné incidenty (major operational and security incidents)
- **Komu je potrebné incident oznámiť?**
 - TBD (kompetentný orgán)
 - Ak má incident finančný dopad na užívateľov, tak aj užívateľom
 - Príslušný orgán domovského členského štátu po prijatí oznámenia bez zbytočného odkladu informuje EBA a ECB
 - EBA a ECB posúdia relevantnosť incidentu pre iné relevantné orgány EÚ a zodpovedajúcim spôsobom ich informujú. ECB informuje členov Európskeho systému centrálnych bánk o otázkach relevantných pre platobné systémy.
 - PSP musia aspoň raz ročne poskytnúť štatistické údaje o podvodoch súvisiacich s rôznymi platobnými prostriedkami
- **Do kedy je potrebné incident oznámiť?**
 - Bez zbytočného odkladu



Malé rady na záver

- Pravidelné vykonávanie interného auditu ohľadne bezpečnostných incidentov naprieč spoločnosťou
- Proaktívna identifikácia zraniteľných oblastí
- Príprava reakcie na incidenty a plánov na obnovu („incident response“ and „recovery plans“)
- Zriadenie nezávislého tímu reakcie (incident response team), ktorý zahŕňa právny team
- Spolupráca s dodávateľmi a ich subdodávateľmi na pravidelnej báze
- Implementácia školení a programov na zvyšovanie informovanosti

Ďakujem za pozornosť



Zuzana HEČKO

Senior Associate

Allen & Overy, Bratislava, s.r.o.

Tel.: +421(2) 5920 2438

Zuzana.Hecko@allenovery.com



eFOCUS

Informácie obsiahnuté v tejto prezentácii nepredstavujú konkrétne právne poradenstvo a nemali by byť použité ako základ právneho poradenstva bez overenia.

Allen & Overy znamená Allen & Overy LLP a/alebo jej spriaznené osoby. Pojem partner sa používa na označenie člena Allen & Overy LLP, zamestnanca alebo konzultanta s obdobným postavením a kvalifikáciou, prípadne osoby s obdobným štatútom v jednej zo spriaznených osôb.