

## Synergie všeho (skoro)

**ISSS 2017**

**Ing. Aleš Špidla**

**Prezident Českého institutu manažerů informační bezpečnosti**

**[ales.spidla@cimib.cz](mailto:ales.spidla@cimib.cz)**

**Specialista pro kybernetickou bezpečnost CENDIS, s.p.**

**[ales.spidla@cendis.cz](mailto:ales.spidla@cendis.cz)**



## Základní motta

- Kybernetická bezpečnost není primárně otázkou zákonů, je hlavně otázkou pudu sebezáchovy instituce, firmy i jednotlivce (Špidla)



## Základní motta

- Kybernetická bezpečnost není primárně otázkou zákonů, je hlavně otázkou pudu sebezáchovy instituce, firmy i jednotlivce (Špidla)
- V Alláha věř, ale velblouda přivaž (Arabské přísloví)



## Základní motta

- Kybernetická bezpečnost není primárně otázkou zákonů, je hlavně otázkou pudu sebezáchovy instituce, firmy i jednotlivce (Špidla)
- V Alláha věř, ale velblouda přivaž (Arabské přísloví)
- Chtěj nemožné, abys dosáhl možného (Židovské přísloví)



## Základní motta

- Kybernetická bezpečnost není primárně otázkou zákonů, je hlavně otázkou pudu sebezáchovy instituce, firmy i jednotlivce (Špidla)
- V Alláha věř, ale velblouda přivaž (Arabské přísloví)
- Chtěj nemožné, abys dosáhl možného (Židovské přísloví)
- Máte-li pocit, že je všechno v naprostém pořádku, potom jste zcela určitě něco přehlédli (Murphy)



## **GDPR - General data protection regulation - Obecné nařízení o ochraně osobních údajů**

### **Co to je**

#### **Nařízení !!!**

- Platí od 14.4.2016 s účinností od 25.5.2018
- Nahrazuje předchozí směrnici 95/46 a zákon 101/200 Sb.
- Sjednocuje přístup k OÚ v zemích EU plus Norsko, Island a Lichtenštejnsko
- Ostatní země, které působí na evropském trhu
- Revoluce v ochraně osobních údajů
- Posílení práv subjektů osobních údajů
- Všude stejně, včetně sankcí – nemalých
- Regulátorem v ČR ÚOOÚ
- Částečně podřízen Evropskému sboru pro ochranu osobních údajů (EDPB) – WP29

#### **Proč?**

- Nejednotná legislativa na společném trhu
- Problémy při přeshraničním předávání osobních údajů mezi různými jurisdikcemi
- Snowden



## eIDAS

**Nařízení Evropského parlamentu o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním (evropském) trhu**

**- Účinnost od 1.7.2016 – přechodné období pro ČR 2 roky**

- Uznávání prostředků pro elektronickou identifikaci fyzických (el.podpis) a právnických (el.pečeť) osob
  - Vytvoření Národní identitní autority - stát garantuje vaši identitu v kyberprostoru – je to něco nového?
- Pravidla pro služby vytvářející důvěru,
- Úplné elektronické podání

Jen tak na okraj – 74% útoků jde přes zneužitou (špatně zabezpečenou) identitu  
... a zase ty pokuty - až 2 mil. Kč



## Zákon o kybernetické bezpečnosti v novelizované podobě (NIS)

### Rozšíření záběru

- Poskytovatelé základních služeb (určí NBÚ)

ZKB - základní službou je služba, jejíž poskytování je závislé na sítích elektronických komunikací nebo informačních systémech a jejíž narušení by mohlo mít významný dopad na zabezpečení společenských nebo ekonomických činností v některém z těchto odvětví

- energetika,
- doprava,
- bankovníctví,
- infrastruktura finančních trhů,
- zdravotnictví,
- dodávky a rozvody pitné vody,
- digitální infrastruktura
- chemický průmysl
- veřejná správa,

ZKB - informačním systémem základní služby je informační systém, na jehož fungování je závislé poskytování základní služby,





## Zákon o kybernetické bezpečnosti v novelizované podobě (NIS)

### Dopadová určující kritéria

Dopadové určující kritérium je naplněno v okamžiku, kdy narušení bezpečnosti informací v informačním systému a síti základní služby může způsobit některý z následujících dopadů:

- a) omezení základní služby postihující více než 50 000 – 100 0001 osob,
- b) závažné omezení či narušení jiné základní služby, nebo omezení či narušení provozu prvku kritické infrastruktury,
- c) hospodářskou ztrátu vyšší než 250 – 500 milionů Kč1,
- d) nedostupnost služby poskytované alespoň 50 000 – 100 0001 osobám, která není nahraditelná jinou službou,
- e) oběti na životech s mezní hodnotou více než 100 mrtvých nebo 10001 zraněných osob vyžadujících lékařské ošetření,
- f) ohrožení veřejné bezpečnosti v minimálním rozsahu správního území obce s rozšířenou působností,
- g) kompromitaci citlivých údajů o nejméně 200 000 osobách.

### Odvětová určující kritéria

Speciální průřezová kritéria a jejich prahové hodnoty budou nastaveny tam, kde je to relevantní, na základě výsledků jednání pracovní skupiny

Např. ve zdravotnictví jedno z kritérií - Specializované zdravotnické zařízení, které má v České republice méně než x alternativních zařízení se stejným zaměřením



## Zákon o kybernetické bezpečnosti v novelizované podobě (NIS)

### Poskytovatelé digitální služby

- on-line tržiště, které spotřebiteli nebo prodávajícím umožňuje on-line uzavírat s prodávajícím podnikatelem kupní smlouvu nebo smlouvu o poskytnutí služeb, a to prostřednictvím internetové stránky on-line tržiště nebo prostřednictvím internetové stránky prodávajícího, který využívá službu poskytovanou on-line tržištěm,
- internetový vyhledávač, který umožňuje provádět vyhledávání v zásadě na všech internetových stránkách, a to na základě dotazu uživatele na jakékoliv téma v podobě klíčového slova, sousloví nebo jiného zadání, přičemž služba poskytuje odkazy, na nichž lze nalézt informace související s požadovaným obsahem, nebo
- Služba cloud computingu, který umožňuje přístup k rozšířitelnému a přizpůsobitelnému úložišti nebo výpočetním zdrojům, které je možné sdílet



## Zákon o kybernetické bezpečnosti v novelizované podobě (NIS)

### Některé zajímavé povinnosti poskytovatelů digitální služby

Orgány veřejné moci, jsou povinny si ve smlouvě, kterou uzavírají s poskytovatelem služeb cloud computingu, zajistit alespoň, že jim budou na základě jejich žádosti bez zbytečného odkladu poskytnuty informace a data, která pro ně poskytovatel služeb cloud computingu uchovává, a bez zbytečného odkladu umožněna jejich kontrola.

Nezbytnými náležitostmi smlouvy jsou

- zakotvení povinnosti poskytovatele služeb zohlednit bezpečnostní politiky odběratele služeb,
- stanovení úrovně poskytovaných služeb,
- systém schvalování subdodavatelů služby cloud computingu,
- podmínky ukončení smluvního vztahu z pohledu bezpečnosti,
- řízení kontinuity činností v souvislosti s poskytovanou službou cloud computingu,
- určení vlastníka uchovávaných dat,
- dohoda o důvěrnosti smluvního vztahu“.,
- stanovení úrovně ochrany dat z pohledu důvěrnosti, dostupnosti a integrity,
- pravidla zákaznického auditu a
- stanovení povinnosti poskytovatele služeb informovat odběratele o kybernetických bezpečnostních incidentech souvisejících s plněním smlouvy.

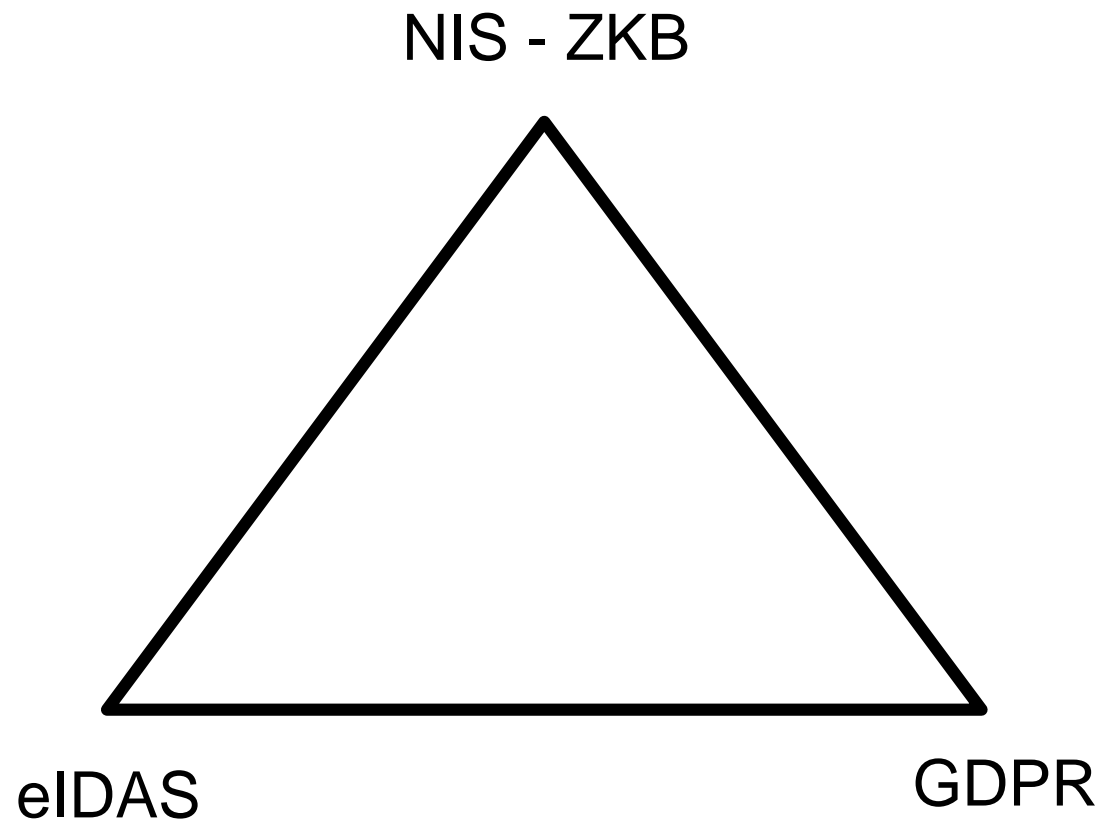
...a pokuty – až 5 mil. Kč



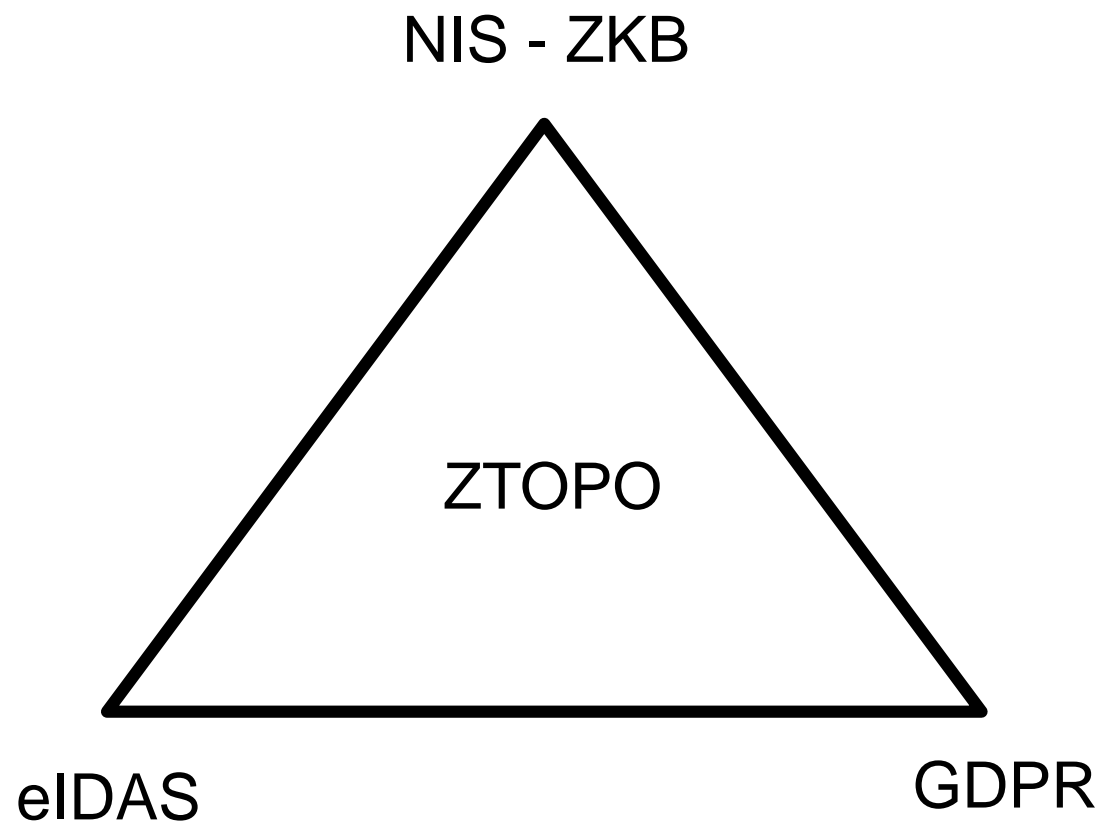
**Není to jednoduché, je to trojité**



Není to jednoduché, je to trojité - minimálně



Není to jednoduché, je to trojité - minimálně



Proč teda ten trojúhelník - Aby se nezměnil v Bermudský



## Jak se neutopit?

### Přesvědčit sebe a vedení že je nutno:

- Přestat si lhát
- Nepodceňovat reputační riziko
- Zahodit zodpovědnostní ping-pongový míček
- Nevnímat jednotlivé vrcholy izolovaně (ušetří to čas, peníze i nervy)
- Nebát se pořádku
- Zpracovat GAP analýzy
- Navrhnout opatření
- Implementovat opatření
- Nevymlouvat se na blížící se volby
- Se nikdy nezastavit (nekonečno v PDCA cyklu)





DĚKUJI ZA POZORNOST

[Ales.spidla@cimib.cz](mailto:Ales.spidla@cimib.cz)  
[Ales.spidla@cendis.cz](mailto:Ales.spidla@cendis.cz)

