# ÚVOD DO PROBLEMATIKY GDPR, EIDAS, NIS

**SECURITY IT**

**Ing. Aleš Špidla**

**Prezident Českého institutu manažerů informační bezpečnosti**

ales.spidla@cimib.cz

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

ales.spidla@cendis.cz

## Základní motta

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

# Základní motta

- Kybernetická (informační) 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 (informační) 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 (informační) 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

GDPR je další nástroj pro uplatnění a vymáhání kybernetické bezpečnosti v oblasti osobních údajů

….. Více až paní Eva Škorničková

## eIDAS

**Nařizeni Evropského parlamentu o elektronické identifikaci a službach vytvářejících důvěru pro elektronické transakce na vnitřním (evropském) trhu - - Účinnost od 1.7.2016 – přechodné období pro ČR 2 roky – předepisuje zajistit:**

- Schopnost identifikovat a autentizovat osoby nebo organizace v rámci elektronických on-line služeb v rámci států EU.
- Schopnost ověřovat platnost zaručených elektronických podpisů a zaručených elektronických pečetí založených na kvalifikovaných certifikátech, které byly vydány v jiných státech EU.
- Schopnost ověřit formáty zaručených elektronických podpisů a zaručených elektronických pečetí stanovené v prováděcím rozhodnutí Komise č. 2015/1506/EU.
- Schopnost podepisovat a pečetit dokumenty tak, aby byly ověřitelné i v jiných státech EU.
- Zajistit prostředky pro používání kvalifikovaného elektronického podpisu a používání kvalifikovaných elektronických pečetí. (do 3Q 2018)
- Schopnost opatřovat podepsané, případně zapečetěné elektronické dokumenty, kterými právně jedná, kvalifikovaným elektronickým časovým razítkem. (do 3Q 2018)
- Schopnost validovat a autentizovat web
- Schopnost elektronického doporučeného doručování
- Schopnost zajištění právní prokazatelnosti a dlouhodobé čitelnosti uloženého elektronického dokumentu.

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,
- bankovnictví,
- 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 relevatní, na základě výsledků jednání pracovní skupiny

Např. ve zdravotnictví jedno z kriterií - 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,
- internetový vyhledávač,
- Služba cloud computingu

# 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.

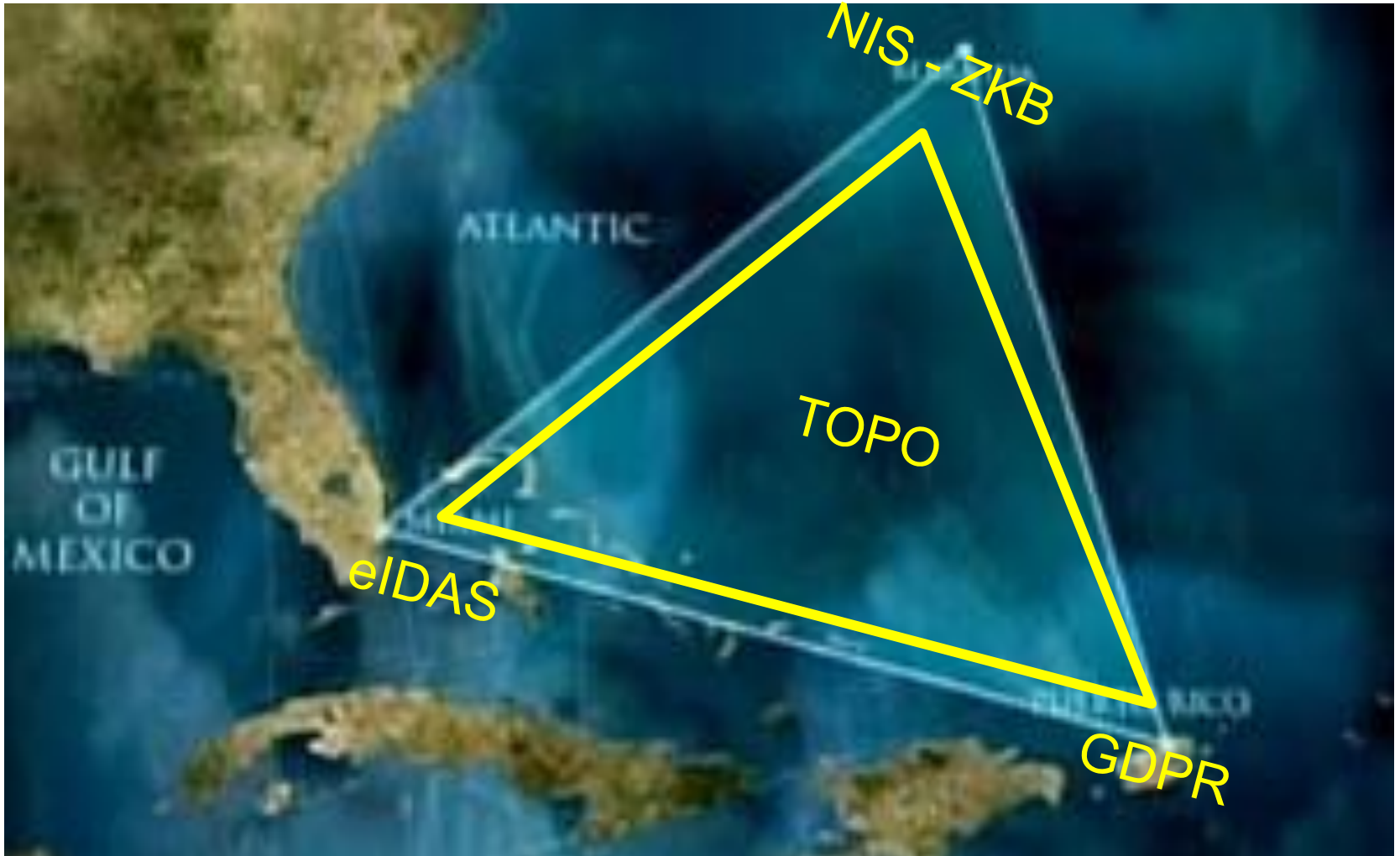
Nezbytnými náležitostmi smlouvy jsou

- 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

## …… řešte to komplexně

## … a proč - proto



## Jak se neutopit?

## Důležité:

- Strategické rozhodnutí vrcholového managementu o cílovém stavu
  - reálné povýšení úrovně ochrany informací
  - formální naplnění požadavků všech nařízení
- Implementace
  - projekt napříč organizací
  - liniová aktivita
  - průřezový tým složený z kompetentních zaměstnanců  doplněný externími experty
- Vstupy pro analýzy a schopnost navrhovat alternativní řešení a opatření
- Schopnost integrovat dílčí řešení do komplexního řešení
- Odpovídající úroveň zapojení interního týmu při implementaci
- Uvědomovat si, že jde o zásadní změnu bezpečnostní kultury instituce

## Jak se neutopit?

**Přesvědčit sebe a vedení že je nutno:**

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

ČIMIB

# DĚKUJI ZA POZORNOST

Ales.spidla@cimib.cz
Ales.spidla@cendis.cz