GDPR a kybernetická bezpečnost (ale kdyby jenom to)

Seminář OnSECURE GDPR

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 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)

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, 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

eIDAS

Nařizeni Evropského parlamentu o elektronicke identifikaci a službach 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
  - překážky charakteru legislativního, technického i organizačního
  - nepřipravenost řady právních předpisů jak na požadavky vyplývající z nařízení eIDAS, tak i na deklarované cíle ve vládních materiálech a dlouhodobých strategiích
  - rozvoj e-Governmentu je často podceňován, žádné kroky ke změně právních předpisů, žádné kroky k obstarání alespoň dílčích nástrojů pro budoucí konstrukci ÚEP
- … a také nejasnost v kompetencích uvnitř institucí – zodpovědnostní ping-pong

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

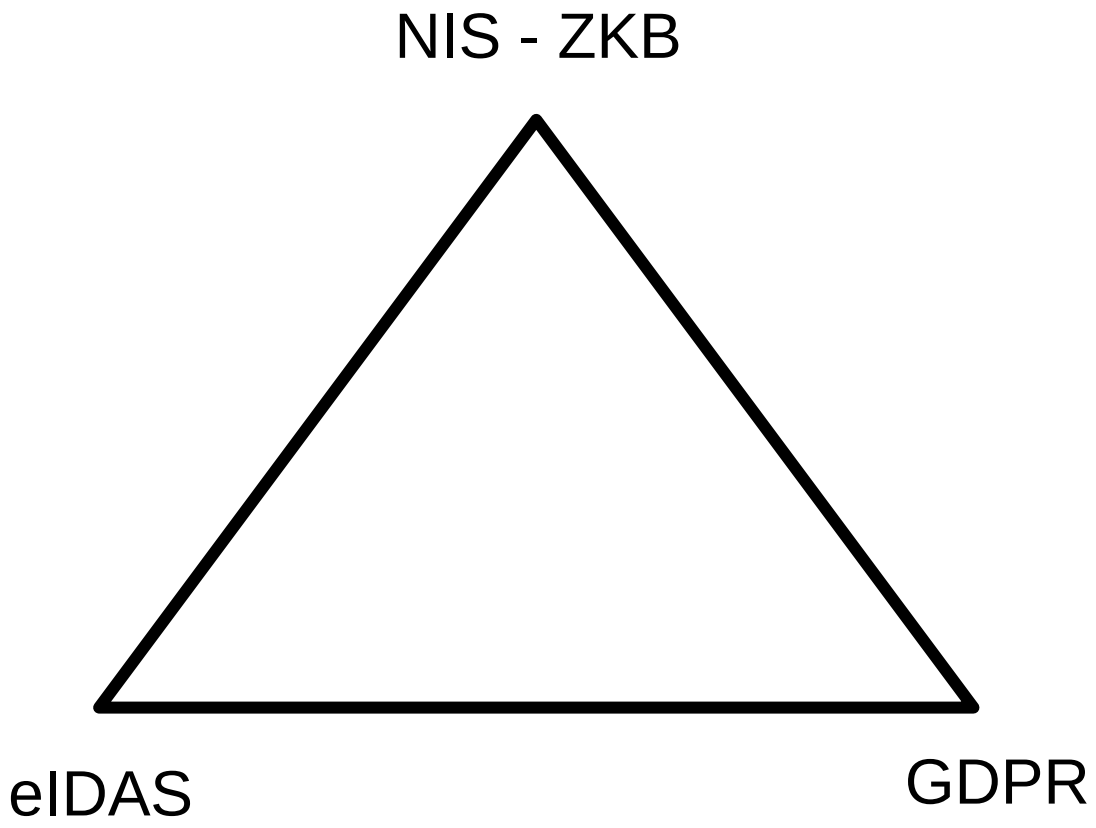
GDPR

O tom lépe hovořila paní Eva Škorničková

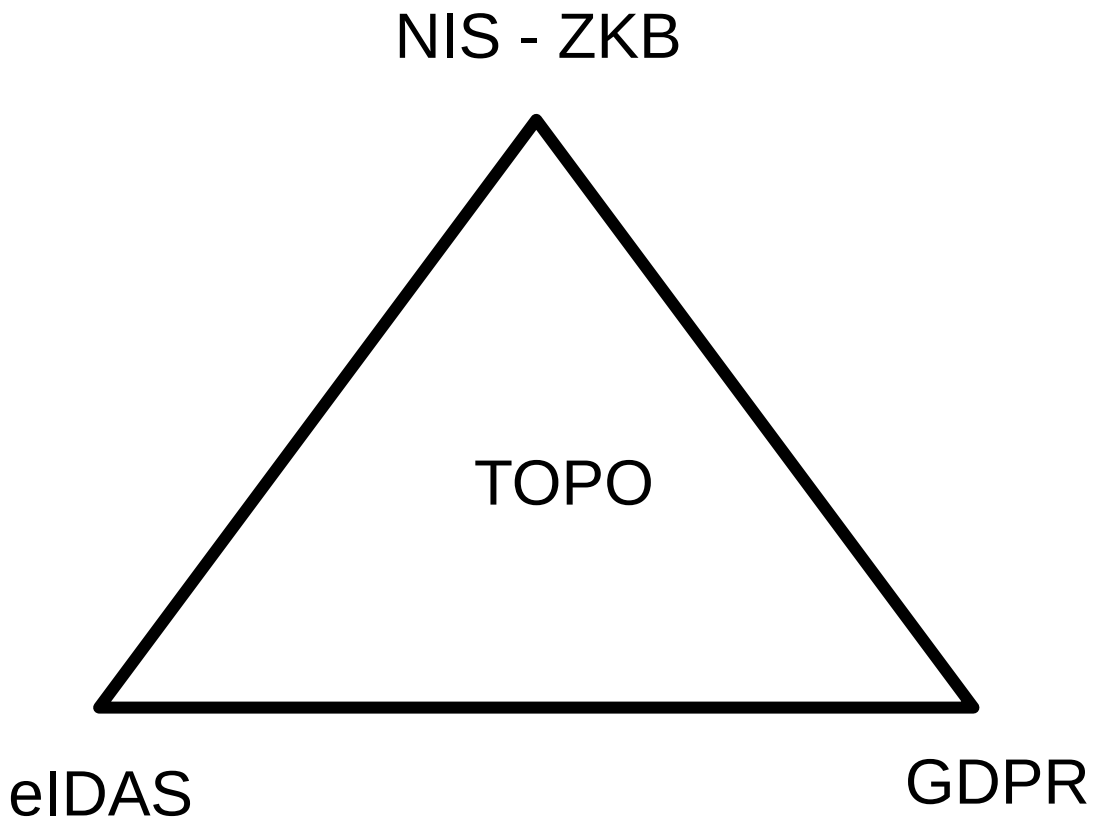
….. a zase ty pokuty – opravdu vysoké

Není to jednoduché, je to trojité - minimálně

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, že se nás to netýká
- Nepodceňovat reputační riziko
- Zahodit zodpovědnostní ping-pongový míček
- Nevnímat jednotlivé vrcholy izolovaně (ušetří to čas, peníze i nervy)
- (nechat si) Zpracovat GAP analýzy
- (nechat si) Navrhnout opatření
- (nechat si) 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