Porušení zabezpečení osobních údajů a kybernetický bezpečnostní incident v kontextu internetu věcí

František Kasl

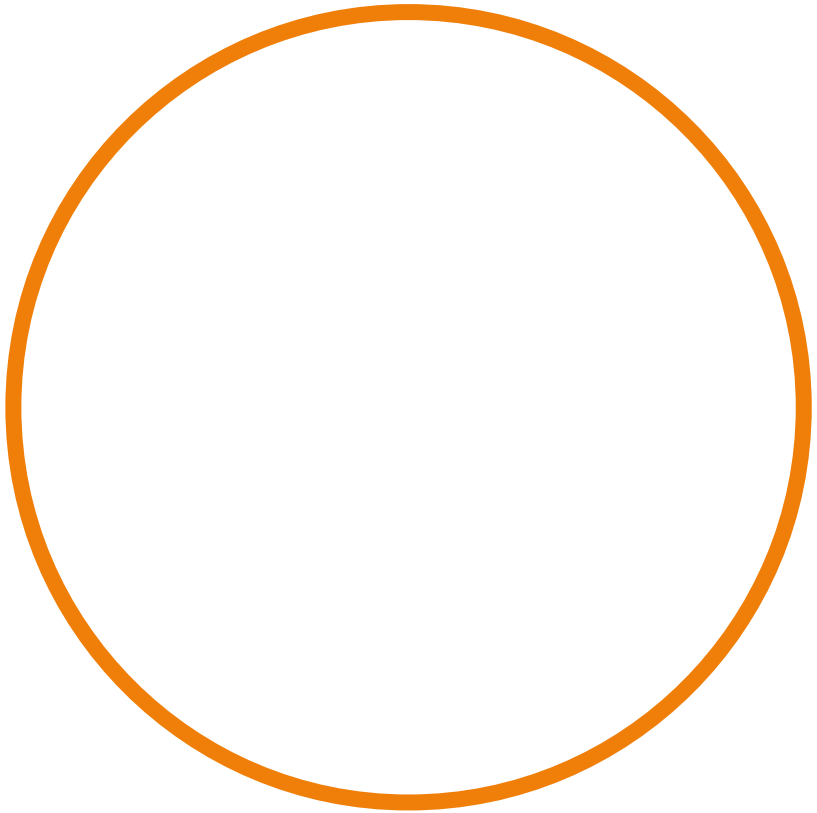
ÚPT PrF MU

Porušení zabezpečení osobních údajů

- *„porušení zabezpečení, které vede k náhodnému nebo protiprávnímu zničení, ztrátě, změně nebo neoprávněnému poskytnutí nebo zpřístupnění přenášených, uložených nebo jinak zpracovávaných osobních údajů.“*
  - článek 4 bod 12 Obecného nařízení
- Obecně jde při zajišťování bezpečnosti informačních a komunikačních systémů o úsilí, které vyžaduje **neustálé přizpůsobování se dynamickému vývoji existujících a nově vznikajících hrozeb**
- **Porušení nemůže být zcela vyloučeno, ale pouze omezeno**
  - reflektováno performativním pravidlem v článku 32 Obecného nařízení

Ohlašování porušení zabezpečení osobních údajů

- Sekundární povinnost
  - **Cíl = zvýšení transparentnosti vůči dozorovým úřadům a subjektům údajů, aby bylo dosaženo snížení dopadů a vzniklé škody v důsledku porušení**
- Původ instrumentu
  - California Security Breach Information Act, Senate Bill No. 1386 ze dne 25. září 2002
- Před Obecným nařízením
  - pouze úzká sektorová úprava pro poskytovatele veřejně dostupných služeb elektronických komunikací na základě směrnice 2009/136/ES, kterou se měnila směrnice o soukromí a elektronických komunikacích
- **Články 33 (vůči ÚOOÚ) a 34 (vůči subjektu údajů) Obecného nařízení zavedena plošně pro všechny správce**
  - **Trigger = jakkékoliv porušení, ledaže je nepravděpodobné, že by toto porušení mělo za následek riziko pro práva a svobody fyzických osob**
  - **Ohlašování vůči dozorovému úřadu** = určitý mezistupeň, který má sloužit ke zpřehlednění situace a posouzení, zda jsou zapotřebí následná opatření ze strany dozorového úřadu vůči danému správci, či zda je na místě přímo oznámit daný incident dotčeným fyzickým osobám



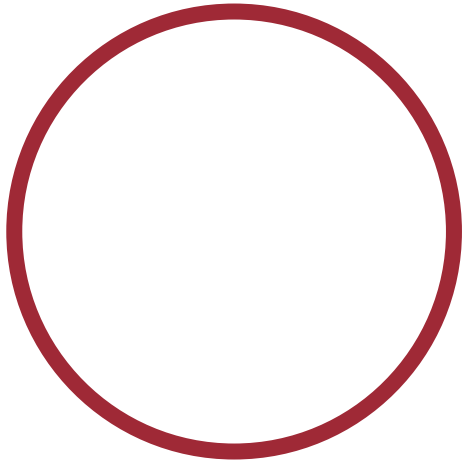
Kybernetický bezpečnostní incident

- *„**narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací** v důsledku kybernetické bezpečnostní události“*, tedy události, *„která může způsobit narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací*
  - Srov. § 7 zákona č. 181/2014 Sb. o kybernetické bezpečnosti.

- **Úzký okruh povinných subjektů**
  - Správce/provozovatel IS a KS kritické informační infrastruktury
  - Správce/provozovatle významného informačního systému
  - Správce/provozovatel IS základní služby
  - Zajišťovatel významné sítě
  - Poskytovatel digitální služby (online tržiště/internetový vyhledávač/cloud computing)

Hlášení kybernetického bezp. incidentu

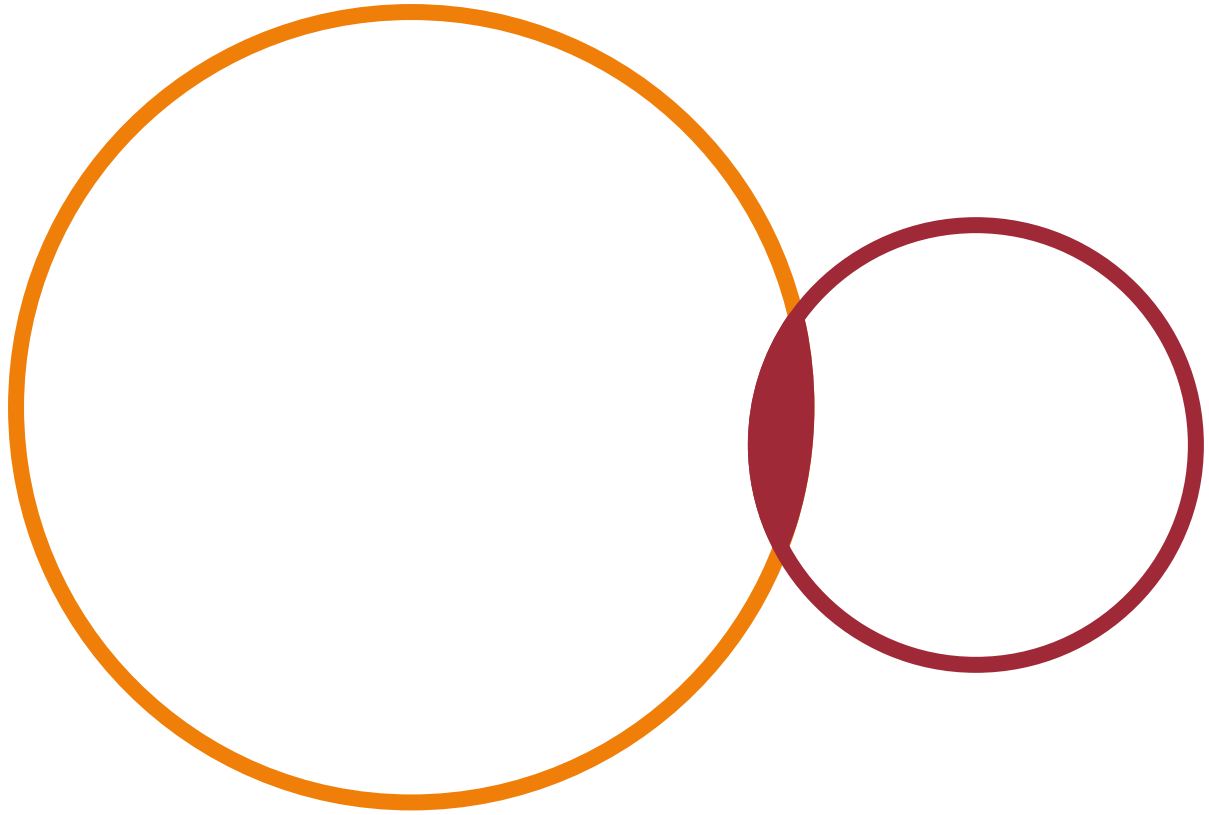
- **vůči příslušnému CERTu** (NÚKIB x CZ.NIC)
- pouze omezený okruh povinných subjektů (§8) + u některých pouze incident s významným dopadem
  - **+ dobrovolná hlášení - §8(6) ZoKB**
- součást preventivních a reaktivních funkcí systému kybernetické bezpečnosti
- **Cíl = zajištění adekvátní informovanosti dozorových autorit pro případné včasné vydání reaktivního či ochranného opatření pro zajištění funkcionalit daných stěžejních informačních systémů, sítí a informací v nich**



Situační překryv a odlišující znaky

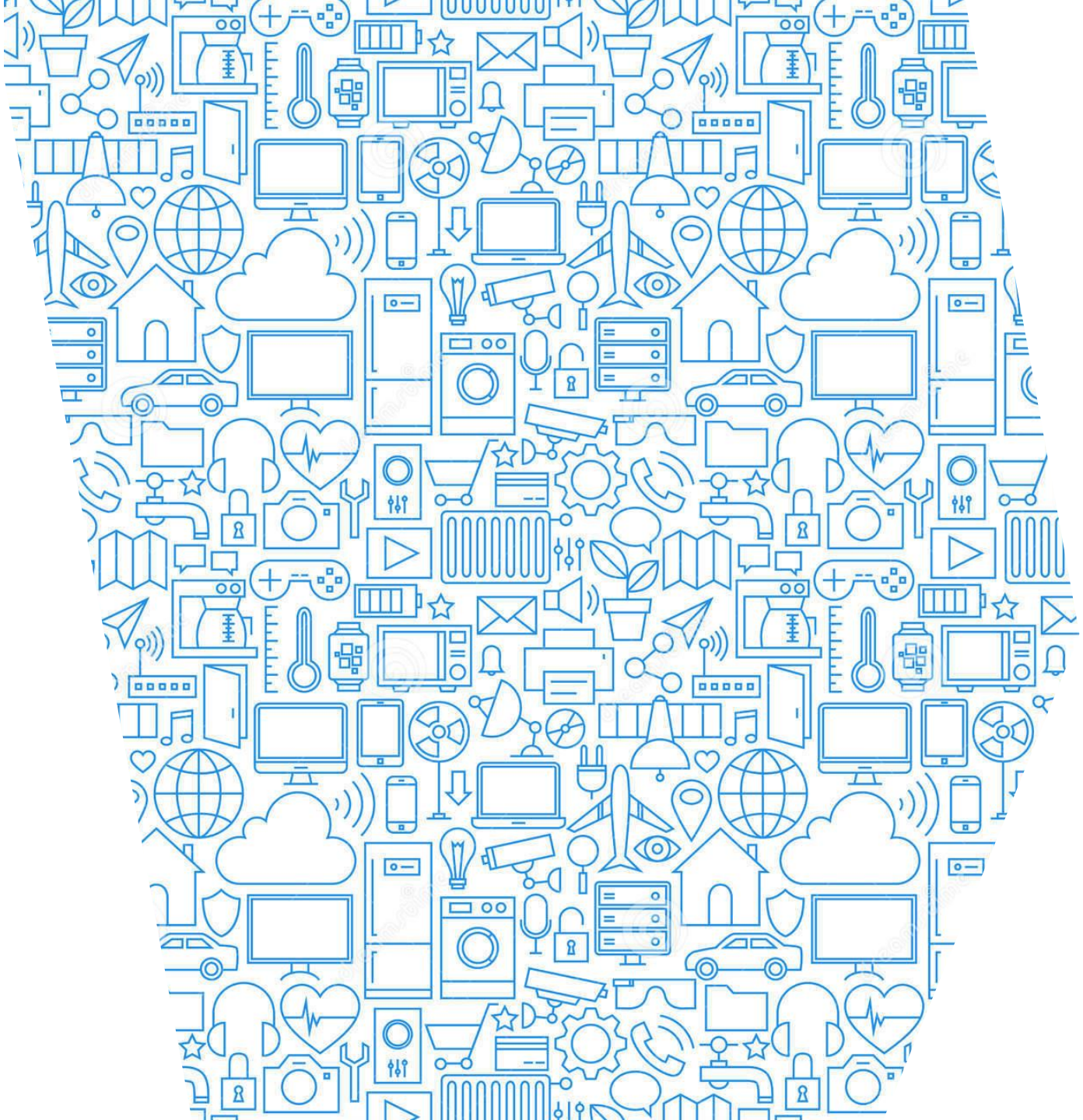
- **Informace v IS v řadě případů představují osobní údaje**
  - překryv situací notifikace dle obou právních režimů

- **Odlišující znaky**
- 1) **Účel**
  - Obecné nařízení = ochrana subjektů údajů, tedy minimalizace výsledné újmy na jejich zájmech a právech
  - ZoKB = zajištění funkcionality a provozu přenosových sítí, IS a minimalizace dopadů daného incidentu
- 2) **Institucionální recipient**
  - Obecné nařízení = ÚOOÚ = instituce specializovaná na dozor nad řádným zpracováváním OÚ
  - ZoKB = v/n CERT = instituce specializovaná na hodnocení kyberbezp. rizik a adekvátní reakci skrze opatření



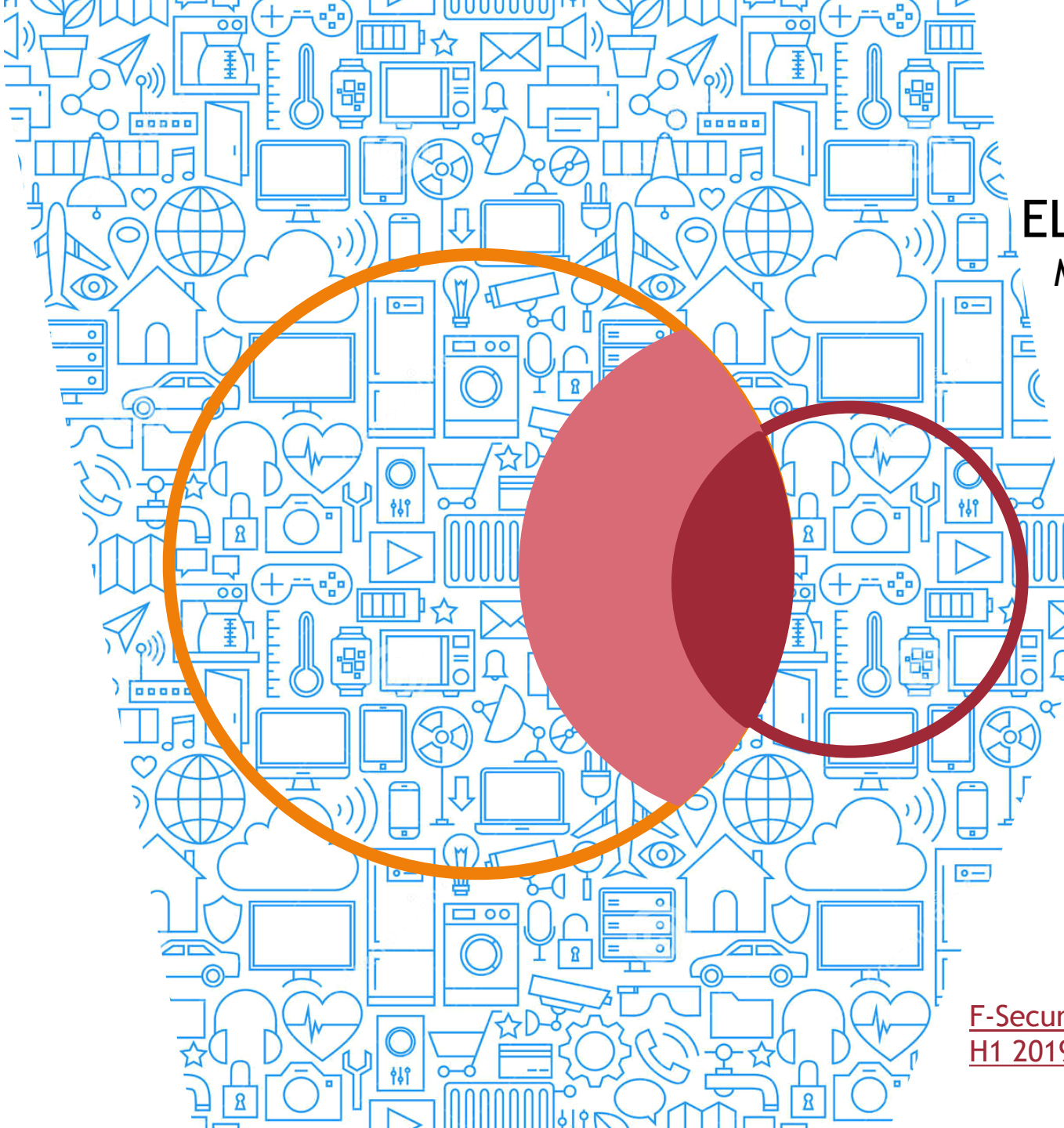
Internet věcí

- Nové technologické prostředí propojenosti a digitalizace služeb a činností
- **Trend přibývající penetrace trhu i výbavy běžného uživatele v prostředí kanceláří, domovů i na veřejných prostor novými zařízení s prvky ICT**
- Rostoucí komplexita shromažďování OÚ za pomoci senzorů / zpracovávání vedoucí k profilování / responzivita a adaptabilita zařízení
  - **Rostoucí závislost činností FO i PO na řádném fungování a spolehlivosti ICT prvků a jejich propojenosti za pomoci sítí**
    - **Rostoucí riziko újmy v důsledku incidentů/porušení zabezpečení**
- Mnohovrstvý jev, který přesahuje pouhou technologickou evoluci a vytváří nové výzvy a možnosti v celém spektru oborů a činností
- **Zde: Klíčová není konkrétní technologická forma, ale širší důsledek = penetrace společnosti ICT technologiemi a závislost činností na zpracování OÚ**
  - Vyšší prolínání problematiky zabezpečení zpracování OÚ a kybernetické bezpečnosti



Moderní hrozby a regulatorní rigidita

- Prostředí internetu věcí přináší **nové formy hrozeb a novou úroveň rizika a intenzity spojenou s existujícími formami hrozeb**
- **Plošné incidenty zasahující IoT zařízení** u velkého množství uživatelů má **potenciál hrozby srovnatelný s významnými kybernetickými incidenty**
- Existující regulatorní rámec na tyto incidenty neaplikuje povinnosti a dozor instituce specializované v oblasti kybernetické bezpečnosti, ale pouze ÚOOÚ, tedy rámce zpracování OÚ
- **Nástroj ohlašování porušení zabezpečení osobních údajů se tak stává quasinástrojem pro shromažďování aktuálních informací o plošné situaci z hlediska kybernetické bezpečnosti X bez vhodného využití**
- Responsivita a časové hledisko jsou klíčové při snaze o minimalizaci dopadů a omezení šíření těchto hrozeb X současný rámec na to není adaptován
- Vznikající reálný problém, který vede k neadekvátní reakci a nevhodným tokům informací
- **Dobrovolná hlášení incidentů (§8(6) ZoKB) umožňují určitou flexibilitu**
  - X většina relevantních subjektů má omezené povědomí o této právní úpravě, pokud na ně přímo nedopadá
  - bude zapotřebí plošnější a responsivnější regulatorní řešení, pokud se tyto hrozby stanou častějšími, což je zřejmý trend



ELF/Mirai.AT!tr

Mal/Generic-S

Trojan.Linux.Mirai.4!C

WannaCry

Brickerbot

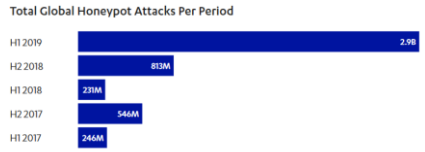
Linux/GenericAA-GR

ELF/Trojan.GDNL-5

TROJ_GEN.F04JC00CC19

Win32/Backdoor.805

...



F-Secure
H1 2019 Security Report

Možné východisko

- Do budoucna je zřejmě nevyhnutelné, aby se **okruh povinných subjektů dle ZoKB dále rozšiřoval**
- Současně bude mít **větší význam dobrovolná spolupráce a podporu subjektů**, které nemají zákonem kladené přímé povinnosti
- V řadě případů je však otázkou smysluplnost ohlašovací povinnosti vůči ÚOOÚ
  - **priorita v případě plošného incidentu je řešení kyberbezpečnostních otázek**
  - ÚOOÚ není personálně ani odborně vybaven na adekvátní podporu a reakci
  - **subjektem pro podporu a řešení těchto situací bude v konečném důsledku CERT**
- **Lze si tedy představit výjimku z ohlašovací povinnosti vůči ÚOOÚ v podobě povinnosti hlášení incidentu CERTu**
  - + následnou spolupráci mezi CERTem a ÚOOÚ ve směru účelného řešení ochrany dotčených osobních údajů = ex post analýza jednání subjektů a případné oznamování subjektům údajů
  - bez odborné podpory CERTu není ohlašování těchto incidentů ÚOOÚ příliš účelné
  - výsledná újma způsobená incidentem je silně závislá na rychlosti adekvátní reakce / reaktivních a ochranných opatřeních vůči ostatním subjektům užívajícím stejné technologie/zařízení
  - **notifikační povinnost má směřovat k maximálně efektivnímu řešení dané situace, což se pro předmětné případy přes ÚOOÚ nezdá být reálné**

Děkuji za pozornost!