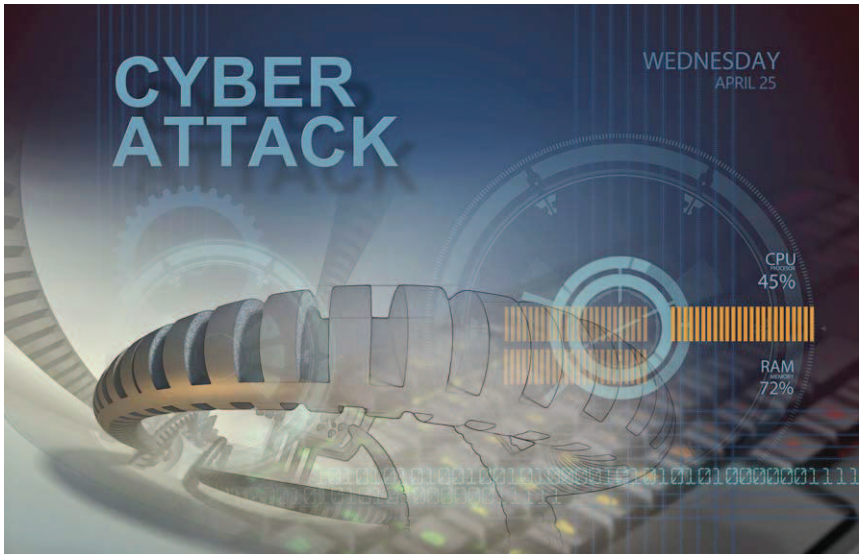
Vliv současné legislativy na **Incident management**

Jaromír Veber



V posledních letech začalo platit několik předpisů, které mohou mít v organizacích vliv na proces incident managementu. Tyto předpisy se vztahují, jak na státní, tak i soukromé organizace a přímo ovlivňují podobu tohoto procesu. V minulosti legislativa do této oblasti prakticky nezasahovala, a pokud ano, tak pouze ve velmi omezené míře. V poslední době však přibývá legislativy, která do této oblasti více či méně zasahuje. Na základě této přibývající legislativy je možné shledat nově vzniklý požadavek na proces incident managementu a jeho zavedení a dodržování.

O jakou legislativu se tedy jedná?

Jedná se především o novelizovaný **zákon o kybernetické bezpečnosti** [2] (s ohledem na směrnici NIS [1]), a to zejména prostřednictvím vyhlášky o kybernetické bezpečnosti [3]. Dále se jedná o nařízení **GDPR** [4], které bude do národní legislativy rozvíjet nový zákon o zpracování osobních údajů. A dále zákon **o platebním styku** [5] (implementující směrnici PSD2 [6]) a s ním související předpisy evropského orgánu pro bankovnictví [7, 8].

Zákon o kybernetické bezpečnosti

Zákon se vztahuje pouze na omezený počet právních subjektů v České republice (dále jen ČR), nicméně se jedná často o významné organizace. Zákon zajišťuje koordinaci reakce na bezpečnostní incidenty v prostředí významné infrastruktury (Kritická informační infrastruktura a Významné informační systémy), a za tímto účelem je nutné mít k dispozici informace o incidentech. Zákonem jsou tedy kladeny požadavky na: **zavedení incident managementu** dle §4 odst. 3) zákona. Konkrétnější informace jsou specifikovány v §14 vyhlášky o kybernetické bezpečnosti. Tyto specifikace mají následující podobu; **dodavatelé** služeb cloud computingu jsou povinni **hlásit bezpečnostní incidenty** svým zákazníkům dle §4 odst. 5) zákona a ti hlásí incidenty úřadům (Národní úřad pro kybernetickou a informační bezpečnost a národní CERT) dle §8 zákona a §14 a §32 vyhlášky. Zákon také s ohledem na řešení incidentů stanovuje povinnost zavádět **reaktivní opatření** dle pokynů úřadů, při bezpečnostních incidentech dle §13 zákona a §33 vyhlášky. Tento koncept samozřejmě znamená pro subjekty, na které se vztahuje (zákon zavádí více kategorií, které mají různé povinnosti), potřebu mít funkční incident management procesy, a mimo to také doplnit proces o činnost hlášení incidentů.

GDPR

Nařízení se vztahuje na velké množství právních subjektů v ČR, protože téměř každá organizace zpracovává osobní údaje. Účelem nařízení je zajistit bezpečnost osobních údajů, a v případě, že dojde k incidentu v této oblasti, minimalizovat dopady, které z těchto incidentů plynou. Dohled nad dodržováním nařízení zajišťuje dozorový úřad v případě ČR se jedná o Úřad pro ochranu osobních údajů (dále jen ÚOOÚ). Nařízení přímo nedefinuje, jaké by měl incident management mít náležitosti, avšak stanovuje určité povinnosti, které není možné bez **zavedení incident managementu** dodržet. Jedná se konkrétně o povinnosti: v článku 33 odst. 1 **hlásit incidenty úřadu** (za určitých okolností), v odst. 2 **hlásit incidenty zákazníkům** (za určitých okolností) a v odst. 5 **incidenty dokumentovat**. Dále lze z obsahu článku 28 vyplývá pro dodavatele, kteří se účastní zpracování osobních údajů, povinnost **hlásit bezpečnostní incidenty** správcům.

Zákon o platebním styku

Zákon se vztahuje na omezené množství právních subjektů v ČR, které jsou zapojeny do procesu poskytování platebních služeb. Účelem zákona je mimo jiné zajistit bezpečnost platebního styku, a v případě, že dojde k incidentu v této oblasti, minimalizovat jeho dopady. Dohled nad dodržováním tohoto zákona v ČR zajišťuje Česká národní banka. Zákon nedefinuje, jaké by měl incident management mít náležitosti. V tomto ohledu pravděpodobně zákonodárci předpokládali, že platební instituce budou mít již zaveden nějaký druh incident managementu. Zákon však definuje určité povinnosti, ze kterých však vyplývá, nutnost **zavedení incident managementu** v určité formě. V §221 je stanovena povinnost **hlásit incidenty** (za určitých okolností) a to jak dohledovému orgánu, tak uživatelům. Předpis EBA/GL/2017/17 [8] v bodě 5.5 definuje povinnost **zavést incident management**. A dokonce zahrnuje i proces ponaučení se z incidentů dle 8.2. Materiál

Obr 1 : Schéma procesu incident managementu

EBA/GL/2017/10 [7] dále rozvíjí pravidla pro hlášení incidentů včetně klasifikace a postupu oznámení. Výslovně není v zákoně definováno, že by měla instituce bezpečnostní události a incidenty dokumentovat, avšak její obecnou povinností dle §31 zákona o platebním styku je uchovávat dokumenty a záznamy o plnění povinností dle tohoto zákona, a to samozřejmě zahrnuje i tuto dokumentaci.

Co asi vedlo legislativce k zásahu v této oblasti?

Zákon o kybernetické bezpečnosti svým obsahem tak trochu předběhl dobu a požadavky směrnice NIS [1] v oblasti incident managementu a zavedl povinnost tohoto procesu s předstihem. Pokud bychom však toto opominuli a zvažovali pouze směrnici NIS [1], která vedla k novele zákona, tak všechna tato legislativa vešla v platnost v průběhu minulého roku. Důvodem těchto změn je podle všeho snaha o sjednocování legislativy na celoevropskou úroveň tak, aby incidenty bylo možné sledovat a řešit jednotně na celoevropské úrovni.

Jak legislativa proces ovlivní?

Podstatné je, jak se výše zmíněné zákonné požadavky promítají do konkrétních kroků procesu incident managementu. Připomeňme si základní schéma incident managementu tak, jak jej zmiňuje ISO/IEC 27035-1:2016 [9].

Schéma (viz Obr 1) představuje obecný postup procesu bez většího detailu. Pro účely tohoto článku je však tento detail dostačující. Pravidla představená zmíněnou legislativou vedou k tomu, že organizace, na kterou se popsaná pravidla vztahují, by měla mít připravený proces pro management incidentů, jehož průběh a základní kroky popisuje zmíněné schéma.

V každém případě je důležité do průběhu incident managementu zahrnout také činnost hlášení incidentu třetím stranám. K doplňujícím hlášením může docházet v průběhu 2. a 3. kroku.

K hlášení nedochází v 1. kroku procesu, ačkoliv se to z jeho názvu přímo nabízí, protože v případě tohoto kroku dochází pouze k „podání zpráv“ (hlášení), že došlo k události, jinému zpravidla bezpečnostnímu týmu, který má za úkol provést vyšetřování bezpečnostní události a sběr dostupných informací, které se k události váží. Bezpečnostní incident může být dále hlášen třetím stranám až v době, kdy je o něm získáno **dostatečné množství informací**, aby bylo možné posoudit, zda se jedná o incident či nikoliv. Navíc je důležité mít k dispozici tyto informace pro pověřenou osobu, která rozhodne, zda má dojít k hlášení, a které třetí strany mají být o incidentu informovány. Konkrétní informace, které mají být součástí hlášení, jsou již definovány jednotlivými zákony a doprovodnými předpisy.

Kromě hlášení incidentů je třeba vést dokumentaci k bezpečnostním incidentům, které byly prověřovány. Dokumentace událostí a incidentů v ideálním případě prostupuje celým procesem incident managementu. Součástí těchto záznamů s ohledem na výše uvedenou legislativu by mělo být i posouzení, zda incidenty hlásit, např. jaké důvody vedly k tomu, že k hlášení nedošlo. Taková dokumentace je podstatnou součástí auditní stopy, díky které je možné následně prokazovat soulad s uvedenými zákony. Předpisy také požadují, aby součástí záznamů byla i navrhovaná a zavedená opatření v reakci na daný incident.

Legislativa přímo nezasahuje do přípravné fáze procesu, který je s ohledem na incident management také důležitý, protože preventivně působí na snížení množství incidentů, lepší detekci incidentů, nebo zvýšení množství informací, které budou o incidentu dostupné. Uvedené předpisy nechávají dotčeným subjektům v přípravě tohoto procesu relativní volnost, ale některá opatření mohou do tohoto kroku zasáhnout, např. zákon o kybernetické bezpečnosti prostřednictvím reaktivních opatření.

Nejde jen o proces incident managementu

Jak bylo zmíněno výše, legislativa nezasahuje pouze do oblasti incident managementu, ale také do řízení dodavatelů. S těmi je třeba v každém případě uzavřít takové smlouvy, aby události, které mohou znamenat incident bezpečnosti informací, byly těmito dodavateli co nejdříve hlášeny organizaci a dále postoupeny incident managementu.

Závěrem

Současná legislativa, které podléhá nemalé množství organizací v ČR i EU, již nyní definuje pravidla pro incident management, kterých se musí tyto organizace držet. To pro ně znamená nejen potřebu incidenty řešit ad-hoc, ale mít připraven fungující proces, který zajistí realizaci všech legislativních požadavků, které se na ně uplatní. ■

Literatura

[1] Směrnice (EU) 2016/1148, o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii (NIS), Evropský parlament a Rada EU, 2016.
[2] Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů.
[3] Vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat.
[4] Nařízení (EU) 2016/679, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (GDPR), Evropský parlament a Rada EU, 2016.
[5] Zákon č. 370/2017 Sb., o platebním styku.
[6] Směrnice (EU) 2015/2366, o platebních službách na vnitřním trhu, kterou se mění směrnice 2002/65/ES, 2009/110/ES a 2013/36/EU a nařízení (EU) č. 1093/2010 a zrušuje směrnice 2007/64/ES, Evropský parlament a Rada EU, 2015.
[7] Obecné pokyny EBA/GL/2017/10, k oznamování významných incidentů podle směrnice (EU) 2015/2366 o platebních službách na vnitřním trhu (PSD2), EBA, 2017.
[8] Obecné pokyny EBA/GL/2017/17, k bezpečnostním opatřením v souvislosti s operačními a bezpečnostními riziky platebních služeb podle směrnice (EU) 2015/2366 (PSD2), EBA, 2017.
[9] ISO/IEC 27035-1:2016. Information technology – Security techniques – Information security incident management – Part 1: Principles of incident management. 1. ISO, 2016.

Jaromír Veber

Autor článku působí jako Security Specialist ve společnosti AEC (Risk & Compliance Division).