MEZINÁRODNÍ BEZPEČNOSTNÍ INSTITUT

Mezinárodní bezpečnostní instut, z.ú.,
Na Ořechovce 580/4, Praha 6, PSČ 162 00
IČO: 07313209

Kdy a jak hlásit bezpečnostní kybernetické incidenty.

Zdroj:
https://www.enisa.europa.eu/news/enisa-news/when-how-to-report-security-incidents

V prosinci 2018 byla zveřejněna a vstoupila v platnost sada telekomunikačních pravidel s názvem European Electronic Communication Code (dále jen „EECC“). EECC aktualizuje telekomunikační balíček EU z roku 2009 a připravuje půdu pro zavádění optických vláken, vysokokapacitní sítě a mobilní sítě nové generace (5G). Země Evropské Unie (dále jen „EU“) musí transponovat tuto směrnici EU do vnitrostátního práva do konce roku 2020. Důležitou součástí EHSC je ochrana spotřebitele a bezpečnost elektronických zařízení komunikace. Rozsah služeb zahrnuje více služeb a definuje pojmy „zabezpečení“ a „bezpečnostní incidenty“. Článek 40 EECC obsahuje podrobné bezpečnostní požadavky na elektroniku poskytovatelů komunikace a článek 41 zmocňuje příslušný orgán, pokud jde o provádění a prosazování těchto požadavků. Článek 40 konkrétněji požaduje, aby poskytovatelé veřejných elektronických komunikací - sítě nebo služby řídí bezpečnostní rizika spojená s bezpečností sítí a služeb - přijali bezpečnostní opatření včetně případného šifrování. Vyžaduje také od poskytovatelů hlásit významné události příslušným vnitrostátním orgánům, které by měly hlásit tyto bezpečnostní incidenty agentuře ENISA a Evropské Komisi (dále jen „EK!) ročně. Tento dokument popisuje formáty a postupy pro přeshraniční podávání zpráv a výroční zprávy souhrnné zprávy podle článku 40 EHSC.

Odstavec 2 článku 40 popisuje tři typy hlášení incidentů:

1) Hlášení národních incidentů od poskytovatelů CA,
2) ad-hoc hlášení incidentů mezi příslušnými orgány a agenturou ENISA,
3) roční souhrnné hlášení od příslušných orgánů do úřadu EC a ENISA.

Tento pokyn se zaměřuje na ad-hoc podávání zpráv a roční souhrnné zprávy. Články 40 a 41 EHSC nahrazují články 13a a b rámcové směrnice o telekomunikacích. Tento dokument nahrazuje pokyn k hlášení incidentů podle článku 13a, který vypracovala Skupina ECASEC (dříve skupina odborníků podle článku 13a) podle starého právního rámce. (Expertní skupina

MBI MEZINÁRODNÍ BEZPEČNOSTNÍ INSTITUT

Mezinárodní bezpečnostní instut, z.ú.,
Na Ořechovce 580/4, Praha 6, PSČ 162 00
IČO: 07313209

ECASEC je skupina příslušných orgánů v oblasti telekomunikační bezpečnosti, zřízená v roce 2010 vyvinout společný celoevropský přístup k provádění článku 13a.)

Dokument poskytuje pokyny vnitrostátním orgánům, které dohlížejí na bezpečnost v EU v oblasti elektronických komunikací a dalších příslušných orgánů o provádění odstavce 2 článku 40 EECC. Tento dokument se zaměřuje nato, kdy a jak hlásit bezpečnostní incidenty agentuře ENISA, EK a mezi příslušnými orgány. Tento dokument je navržen a publikován agenturou ENISA a potvrzen a přijat ECASEC skupina.

CÍLOVÉ PUBLIKUM: Tento dokument je určen vnitrostátním ministerstvům, vnitrostátním regulačním orgánům a příslušným orgánům v roce 2006 členské státy EU, orgánům pověřeným prováděním článku 40. Tento dokument může být užitečný také pro odborníky pracující v oblasti elektronických komunikací v EU sektoru a pro odborníky pracující v oblasti informační bezpečnosti.
CÍL: Tento dokument zveřejňuje agentura ENISA, aby poskytl certifikačním úřadům pokyny ohledně technické dokumentace provádění hlášení událostí popsaných v čl. 40 odst. 2 EHSC.
AKTUALIZACE: Agentura ENISA tyto pokyny pravidelně aktualizuje, je-li to nutné a po dohodě s příslušnými orgány. Tato verze (V. 2.2) je aktualizací verze 2.1 Pokynů k hlášení incidentů. Celková struktura zůstala do značné míry nezměněna.

Hlavní změny jsou:

- Aktualizované definice zabezpečení a bezpečnostních incidentů a sladění textu a terminologie použitá s ustanoveními EHSC.
- Širší rozsah služeb a incidentů.
- Nové prahové hodnoty pro každoroční hlášení událostí.
- Aktualizovaná šablona hlášení incidentů.
- Příklady narušení bezpečnosti, které spadají do oblasti působnosti EECC.

Citace definice pojmů „bezpečnost“ a „bezpečnostní incident“ v EECC. Článek 2 …. 21) **„bezpečnost sítí a služeb“** schopnost sítí elektronických komunikací a služby, které na dané úrovni důvěry odolávají všem činům, které ohrožují dostupnost, autenticitu, integritu nebo důvěrnost těchto sítí a služeb, uložených nebo přenášené nebo zpracovávané údaje nebo související služby nabízené těmito osobami nebo k nim přístupné sítě nebo služby

elektronických komunikací …. 42) **„bezpečnostním incidentem“** událost, která má skutečný nepříznivý dopad na bezpečnost sítě nebo služby elektronických komunikací.

EECC definuje tři kategorie služeb elektronických komunikací:

- služba přístupu na internet,
- mezilidská komunikační služba,
- služby spočívající zcela nebo převážně v přenosu signálů,
- služby používané k poskytování služeb mezi stroji a k vysílání.

Relevantní parametry dopadu bezpečnostního incidentu:

a) počet uživatelů ovlivněných bezpečnostním incidentem;

b) doba trvání bezpečnostního incidentu;

c) zeměpisné rozšíření oblasti zasažené bezpečnostním incidentem;

d) rozsah, v jakém je ovlivněno fungování sítě nebo služby;

e) rozsah dopadu na hospodářské a společenské činnosti.

Struktura dokumentu:

Mezinárodní bezpečnostní instut, z.ú.,
Na Ořechovce 580/4, Praha 6, PSČ 162 00
IČO: 07313209

PŘÍLOHA A: ŠABLONA ZPRÁVY O INCIDENTECH
PŘÍLOHA B: PŘÍKLADY INCIDENTÚ