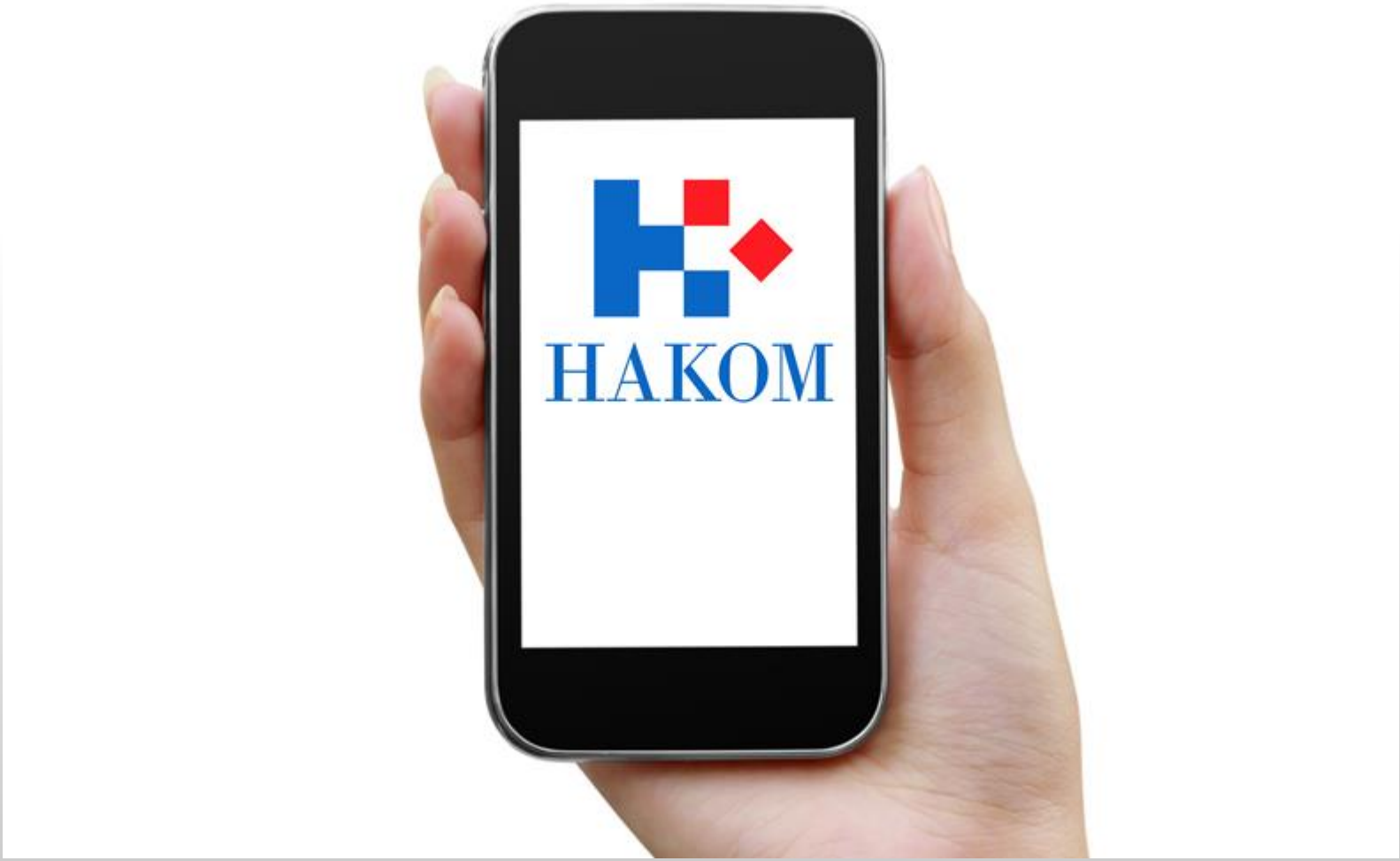
Uloga regulatora vezano za sigurnost mreža i usluga u elektroničkom komunikacijskom sektoru



Izvor :http://terraconbusinessnews.com/hakom-priopcenje-za-medije-od-4-srpnja-vrijede-nova-korisnicka-prava-a-hakom-ce-pojacati-nadzor-nad-operatorima/

Pravni izvor

- Zakon o elektroničkim komunikacijama
  - Pravilnik o načinu i rokovima provedbe mjera zaštite sigurnosti i cjelovitosti mreža i usluga
- Nacionalna strategija kibernetičke sigurnosti i Akcijski plan za njenu provedbu
  - G. Tehnička koordinacija u obradi računalnih sigurnosnih incidenata
    - Cilj G.1 Kontinuirano unaprjeđivati postojeće sustave za prikupljanje, analizu i pohranu podataka o računalnim sigurnosnim incidentima te voditi brigu o ažurnosti drugih podataka bitnih za brzu i efikasnu obradu takvih incidenata.

Nacionalna strategija kibernetičke sigurnosti i Akcijski plan za njenu provedbu

- Mjera G.1.1 Definirati taksonomije, uključujući pojam značajnog incidenta, definirati protokole za razmjenu anonimiziranih podataka o značajnim sigurnosnim incidentima, te uspostaviti platformu ili tehnologiju za razmjenu podataka. Nositelj Nacionalni CERT, ZSIS, HAKOM, HNB ;(12mj)
  - Taksonomija je rezultat suradnje ZSIS i Nacionalnog CERT-a, a pri realizaciji podršku je pružila radna skupina sastavljena od predstavnika tijela različitih sektora, HAKOM-a, HNB-a, MORH-a, MUP-a, HANFA-e te stručnjaka s FER-a i FOI-a.

- Mjera G.1.2 Sektorski nadležna tijela prikupljaju podatke o incidentima od dionika, poput regulatora i drugih CERT-ova iz njihove sektorske nadležnosti te objedinjavaju na sektorskoj razini. (kontinuirano)

- Mjera G.1.3 Izvješćivati dionike unutar sektora o računalnim sigurnosnim incidentima. Periodično izvješćivati Nacionalno vijeće za kibernetičku sigurnost o trendovima, stanju i značajnijim incidentima iz prethodnog razdoblja. (kontinuirano)

Suradnja CERT-a i HAKOM-a

Računalno-sigurnosni incident		Uvjeti prijave računalno-sigurnosnog incidenta
Kategorija	Potkategorija	
Uspješno ostvarena kompromitacija	Malware URL	Zlonamjerna funkcionalnost aktivna je duže od 12 sati.
	Phishing URL	
	Spam URL	
	Web Defacement	
	Sustav zaražen zlonamjernim kodom	
	C&C	
	Korisnički račun	
Pokušaj neovlaštenog pristupa	Pogađanje zaporki	Potrebno je prijaviti svaki slučaj detektiranog pokušaja neovlaštenog pristupa.
	Pokušaj iskorištavanja ranjivosti	
Dostupnost	DoS -Volumetrički napad	Potrebno je prijaviti napade na infrastrukturu operatora koji pruža uslugu pristupa internetu.
	DoS - Napad na aplikacijskom sloju	
Prijevare	Phishing	Potrebno je prijaviti svaki detektirani slučaj ciljanog phishing napada (kampanje) prema davatelju usluge pristupa internetu koji za cilj ima stjecanje financijske koristi, krađu osjetljivih podataka ili pokretanje zlonamjernog programa.
Ciljani napad – APT (eng. Advanced persistent threat)		Potrebno je prijaviti svaki slučaj ovakvog oblika napada.
Ostalo		Prijava po procjeni operatora davatelja usluga

Pravilnik o načinu i rokovima provedbe mjera zaštite sigurnosti i cjelovitosti mreža i usluga

- Operatori su obvezni provesti odgovarajuće tehničke i ustrojstvene mjere za osiguranje sigurnosti i integriteta svojih javnih komunikacijskih mreža i/ili usluga.

- Operatori su obvezni obavijestiti Agenciju u slučaju kršenja sigurnosti ili integriteta javnih komunikacijskih usluga.

- Izvješćivanje o sigurnosnim incidentima:
  - U roku najviše 1 sat nakon ispunjavanja kriterija za izvješćivanje
  - U roku od najviše 1 sat nakon otklanjanja incidenta
  - U roku od najviše 20 dana od dana otklanjanja incidenta.

- Izvješćivanje o računalno - sigurnosnim incidentima:
  - U roku najviše 24 sata nakon otkrivanja incidenta
  - U roku od najviše 20 dana od dana otklanjanja incidenta.

Dodatne obveze operatora

- Operatori su obvezni elektroničkim putem jednom godišnje, najkasnije do kraja mjeseca siječnja dostaviti Agenciji dokumentiranu sigurnosnu politiku za prethodnu godinu koja obuhvaća poduzete mjere sigurnosti i pripadajuće norme.

- Operator mora najmanje jednom godišnje provesti reviziju informacijskog sustava kako bi se utvrdilo jesu li ispunjene minimalne mjere sigurnosti .

- Nalaz revizije, zajedno s planom uklanjanja uočenih nedostataka, potrebno je dostaviti Agenciji do 30. svibnja tekuće godine za prethodnu godinu.

Izvor: https://www.digitaltveurope.com/comment/will-5g-survive-its-expectations-or-buckle-under-its-own-weight/

Procjena rizika infrastrukture 5G mreža- Preporuka Komisije (EU) 2019/534

- Države članice trebale bi do **30. lipnja 2019.** provesti procjenu rizika infrastrukture 5G mreža.
- Države članice trebale bi Komisiji i ENISA-i dobaviti nacionalne procjene rizika do **15. srpnja 2019.**
- Države članice trebale bi u suradnji s ENISA-om te uz potporu Komisije do **1. listopada 2019.** zajednički preispitati izloženost Unije rizicima koji se odnose na infrastrukturu na kojoj se temelji digitalni ekosustav, posebno n5G mreže.
- Skupina za suradnju trebala bi utvrditi mjere najbolje prakse na nacionalnoj razini te do **31. prosinca 2019.** dogovoriti skup mogućih odgovarajućih, učinkovitih i razmjernih mjera za smanjenje rizika kibersigurnosti utvrđenih na nacionalnoj razini i razini Unije, s pomoću kojeg će komisija izraditi minimalne zajedničke zahtjeve za daljnje osiguravanje visoke razine kibersigurnosti 5G mreža u cijeloj Uniji.
- Države članice trebale bi do **1. listopada 2020.** u suradnji s Komisijom procijeniti učinke preporuke kako bi se utvrdili odgovarajući daljnji koraci.

HVALA NA POZORNOSTI !