

VLADA REPUBLIKE HRVATSKE

Zagreb, 1. travnja 2021.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |  |
| --- | --- |
| **Predlagatelj:** | Sigurnosno-obavještajna agencija |

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |  |
| --- | --- |
| **Predmet:** | Prijedlog odluke o mjerama i aktivnostima za podizanje nacionalnih sposobnosti pravovremenog otkrivanja i zaštite od državno sponzoriranih kibernetičkih napada, Advanced Persistent Threat (APT) kampanja te drugih kibernetičkih ugroza |

Banski dvori | Trg Sv. Marka 2 | 10000 Zagreb | tel. 01 4569 222 | vlada.gov.hr

***Prijedlog***

Na temelju članka 31. stavka 2. Zakona o Vladi Republike Hrvatske („Narodne novine“, br. 150/11., 119/14., 93/16. i 116/18.), Vlada Republike Hrvatske je na sjednici održanoj \_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2021. donijela

**ODLUKA**

**o mjerama i aktivnostima za podizanje nacionalnih sposobnosti pravovremenog otkrivanja i zaštite od državno sponzoriranih kibernetičkih napada, Advanced Persistent Threat (APT) kampanja te drugih kibernetičkih ugroza**

**I.**

Ovom se Odlukom određuju mjere i aktivnosti za podizanje nacionalnih sposobnosti za pravovremeno otkrivanje i zaštitu od državno sponzoriranih kibernetičkih napada, Advanced Persistent Threat (APT) kampanja te drugih kibernetičkih ugroza.

Mjere i aktivnosti iz stavka 1. ove točke temelje se na sustavu SK@UT, kao sustavu za otkrivanje, rano upozorenje i zaštitu od državno sponzoriranih kibernetičkih napada, APT kampanja te drugih kibernetičkih ugroza.

**II.**

Mjere iz točke I. ove Odluke su pristupanje različitih skupina tijela i pravnih osoba definiranih u točkama III., IV., V. i VI. ove Odluke, a aktivnosti iz točke I. ove Odluke sastoje se od provedbe odgovarajućih procjena potreba i sigurnosnih procjena u svrhu pristupanja sustavu SK@UT, sklapanja sporazuma o pristupanju te kontinuiranog praćenja stanja kibernetičke sigurnosti u tijelima i pravnim osobama koje su pristupile u sustav SK@UT.

Za provedbu mjera i aktivnosti iz stavka 1. ove točke nadležna je Sigurnosno-obavještajna agencija (u daljnjem tekstu: SOA), koja to provodi u suradnji sa Zavodom za sigurnost informacijskih sustava (u daljnjem tekstu: ZSIS).

**III.**

Zadužuju se ministarstva da pristupe sustavu SK@UT u najkraćem mogućem roku.

**IV.**

Zadužuju se i druga tijela državne uprave, državna tijela nadležna za državne informacijske infrastrukture te druga državna tijela da, na temelju sigurnosne procjene SOA-e, pristupe sustavu SK@UT.

**V.**

Zadužuje se SOA da, u suradnji s nadležnim sektorskim tijelima određenim Zakonom o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga („Narodne novine“, broj 64/18.) i Zakonom o kritičnim infrastrukturama („Narodne novine“, broj 56/13.), u najkraćem mogućem roku, provede procjenu i operatorima ključnih usluga, davateljima digitalnih usluga te operatorima kritične nacionalne infrastrukture, za koje se utvrdi potreba, predloži pristupanje sustavu SK@UT.

**VI.**

S ciljem dodatne zaštite nacionalnog kibernetičkog prostora, sustavu SK@UT mogu pristupiti i druge pravne osobe registrirane u Republici Hrvatskoj, koje podnesu zahtjev SOA-i, pod uvjetom da SOA temeljem sigurnosne procjene takvom zahtjevu udovolji.

**VII.**

Zadužuju se SOA i ZSIS da sa svakim pravnim subjektom koji pristupa sustavu SK@UT sklope sporazum klasificiran odgovarajućim stupnjem tajnosti, kojim se utvrđuju međusobna prava i obveze, odnosno tehnički i drugi uvjeti za pristupanje i korištenje sustava SK@UT.

**VIII.**

Ova Odluka stupa na snagu danom donošenja.

KLASA: \_\_\_\_\_\_\_\_\_\_\_

URBROJ:\_\_\_\_\_\_\_\_\_\_

Zagreb, \_\_\_\_\_\_\_\_\_\_\_\_

PREDSJEDNIK

mr. sc. Andrej Plenković

**OBRAZLOŽENJE**

SK@UT je sustav za otkrivanje, rano upozorenje i zaštitu od državno sponzoriranih kibernetičkih napada, APT[[1]](#footnote-1) kampanja te drugih kibernetičkih ugroza, koji su razvili Sigurnosno-obavještajna agencija (SOA) i Zavod za sigurnost informacijskih sustava (ZSIS). SK@UT se sastoji od distribuirane mreže senzora, smještenih u informacijskim sustavima ključnih državnih tijela i pravnih osoba, centralne platforme u SOA-i, glavnih nadzornih centara u SOA-i i ZSIS-u te lokalnih nadzornih centara u tijelima i pravnim osobama koje su pristupile u sustav.

Ova Odluka donosi se na temelju uspješno provedenog testiranja učinkovitosti sustava SK@UT na užem skupu ključnih tijela državne uprave. Time je ostvaren početni cilj podizanja nacionalnih sposobnosti za pravovremeno otkrivanje i zaštitu od državno sponzoriranih kibernetičkih napada i APT kampanja, u okviru kojeg su sustavu SK@UT pristupila sva ministarstva i većina ključnih tijela državne uprave te je uključeno više osjetljivih segmenata državne informacijske infrastrukture (npr. hrvatska zdravstvena informacijska infrastruktura).

Točkom II. ove Odluke definiraju se mjere pristupanja različitih skupina tijela i pravnih osoba sustavu SK@UT, kao i aktivnosti provedbe odgovarajućih procjena potreba i sigurnosnih procjena u svrhu pristupanja sustavu SK@UT, sklapanja sporazuma o pristupanju te kontinuiranog praćenja stanja kibernetičke sigurnosti u tijelima i pravnim osobama koje su pristupile u sustav SK@UT. Točkom II. se utvrđuje Sigurnosno-obavještajna agencija (SOA) kao nadležno tijelo za provedbu ovih mjera i aktivnosti, koja to provodi u suradnji sa Zavodom za sigurnost informacijskih sustava (ZSIS).

Mjerama iz točaka III. i IV. ove Odluke utvrđuje se način pristupanja sustavu SK@UT za državni sektor u užem smislu.

U cilju daljnjeg podizanja nacionalnih sposobnosti za pravovremeno otkrivanje i zaštitu od državno sponzoriranih kibernetičkih napada i APT kampanja, kao i drugih kibernetičkih napada, te s ciljem dodatne zaštite kritične informacijske infrastrukture, mjerom iz točke V. ove Odluke, zadužuje se Sigurnosno-obavještajna agencija (SOA), da u suradnji s nadležnim sektorskim tijelima[[2]](#footnote-2) i u najkraćem mogućem roku, provede aktivnost procjene potrebe i operatorima ključnih usluga, davateljima digitalnih usluga te operatorima kritične nacionalne infrastrukture, za koje se utvrdi potreba, predloži pristupanje sustavu SK@UT.

U cilju dodatne zaštite nacionalnog kibernetičkog prostora, definira se mjera iz točke VI. ove Odluke, kojom se omogućava uključenje u sustav SK@UT i za druge pravne osobe registrirane u Republici Hrvatskoj, ako podnesu zahtjev SOA-i i ako SOA provedbom aktivnosti sigurnosne procjene[[3]](#footnote-3) utvrdi opravdanost tog zahtjeva.

Točkom VII. ove Odluke utvrđuje se aktivnost obaveze sklapanja sporazuma o pristupanju Sustavu SK@UT, za svako pojedino tijelo ili pravnu osobu iz točaka III., IV., V., i VI. ove Odluke. Sporazum se sklapa između nositelja sustava SK@UT, SOA-e i ZSIS-a, te svakog pojedinog tijela ili pravne osobe koja pristupa sustavu. Sporazumom se utvrđuju međusobna prava i obaveze, odnosno tehnički i drugi uvjeti za pristupanje i korištenje sustava SK@UT, a svaki pojedini sporazum označava se odgovarajućim stupnjem tajnosti.

U cilju podizanja svijesti najšire javnosti u Republici Hrvatskoj o kibernetičkim ugrozama i o važnosti zaštite nacionalnog kibernetičkog prostora, ova Odluka donosi se bez određivanja stupnja tajnosti. Proširenim opsegom tijela i pravnih osoba koje uvodi ova Odluka, nadležnim tijelima se osigurava povećana vidljivost hrvatskog kibernetičkog prostora i podiže se ukupna sposobnost i otpornost Republike Hrvatske za rješavanje kibernetičkih napada velikih razmjera i kibernetičkih kriza[[4]](#footnote-4), te se stvaraju bolji uvjeti za proces atribucije[[5]](#footnote-5) kibernetičkih napada na Republiku Hrvatsku.

Sredstva za provedbu mjera i aktivnosti u cilju daljnjeg podizanja nacionalnih sposobnosti za pravovremeno otkrivanje i zaštitu od državno sponzoriranih kibernetičkih napada i APT  kampanja te drugih kibernetičkih ugroza, osigurana su u financijskom planu SOA-e.

1. APT kampanja (Advanced Persistent Threat – napredna ustrajna prijetnja) je vrsta kibernetičkog napada koju obilježava visoka razina stručnosti i prikrivenosti počinitelja kibernetičkog napada u dužem razdoblju, s konačnim ciljem krađe povjerljivih informacija, ucjene ili stvaranja štete. [↑](#footnote-ref-1)
2. Nadležna sektorska tijela u okviru Zakona o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga („Narodne novine“ broj 64/18) obuhvaćaju tijela nadležna za sektore energetike, prijevoza, bankarstva, infrastruktura financijskog tržišta, zdravstva, opskrbe vodom za piće i njezine distribucije, digitalne infrastrukture, poslovnih usluga za državna tijela, kao i davatelje digitalnih usluga (internetsko tržište, internetske tražilice i usluge računalstva u oblaku). Dodatna nadležna sektorska tijela vezana su uz Zakon o kritičnim infrastrukturama („Narodne novine“ broj 56/13). [↑](#footnote-ref-2)
3. *Sigurnosna procjena SOA-e* obuhvaća procjenu važnosti poslovnih usluga državnog tijela ili pravne osobe za gospodarstvo ili društvo u cjelini, procjenu globalnog, nacionalnog i sektorskog stanja kibernetičke sigurnosti te njihovog mogućeg utjecaja na razinu rizika kibernetičke sigurnosti pojedine pravne osobe, kao i procjenu arhitekture poslovnog i operativnog mrežnog i informacijskog sustava koji pojedina pravna osoba koristi. [↑](#footnote-ref-3)
4. *Kibernetička kriza* je stanje koje može nastati u suvremenom društvu zbog visokog stupnja ovisnosti o mrežnim i informacijskim sustavima i kibernetičkom prostoru, a uslijed čega sve veći broj incidenata i napada u kibernetičkom prostoru može uzrokovati poremećaje u društvenom, političkom i ekonomskom smislu i time utjecati na sigurnost ljudi, demokratski sustav, političku stabilnost, gospodarstvo, okoliš i druge nacionalne vrijednosti, odnosno općenito na nacionalnu sigurnost Republike Hrvatske. [↑](#footnote-ref-4)
5. *Atribucija kibernetičkog napada* označava proces pridjeljivanja odgovornosti za izvršenje kibernetičkog napada koji je uzrokovao štetu ili kibernetičku krizu, koji je rezultat niza analitičkih aktivnosti koje nadležna tijela provode na tehničkoj i sigurnosno-obavještajnoj razini, a s krajnjim ciljem otkrivanja i utvrđivanja činjenica, njihovog povezivanja i procjene njihove vjerojatnosti, kako bi se omogućilo razmatranje i donošenje političke odluke o atribuciji, zajedno s odabirom odgovarajućih diplomatskih instrumenata koji će se primijeniti u svakom pojedinom slučaju atribucije, pri čemu kontekst atribucije može biti nacionalni, EU ili NATO. Primjer procesa atribucije predstavlja *prva atribucija kibernetičkih napada na EU razini* za niz kibernetičkih napada atribuiranih akterima iz Ruske Federacije, NR Kine i Sjeverne Koreje, što je uključilo i rusku vojnu obavještajnu službu GRU te niz povezanih pojedinaca i kibernetičkih APT grupa iz Rusije, Kine i Sjeverne Koreje (*Council Decision (CFSP) 2020/1127 of 30 July 2020 and (CFSP) 2020/1537 of 22 October 2020 amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States*). [↑](#footnote-ref-5)