РЕПУБЛИКА СРБИЈА
РАТЕЛ
РЕГУЛАТОРНА АГЕНЦИЈА ЗА ЕЛЕКТРОНСКЕ КОМУНИКАЦИЈЕ И ПОШТАНСКЕ УСЛУГЕ

СРБ-ЦЕРТ

Иако је концепт рада од куће и раније постојао у култури појединих професија и организација, тренутна ситуација у вези са COVID-19 проузроковала је његову масовну примену. С једне стране, рад од куће је омогућио даље функционисање организација што може ублажити предстојећу економску кризу, док је с друге стране поставио нове изазове пред сајбер безбедност како појединаца тако и организација.

Компромитовање уређаја појединаца у тренутној ситуацији може угрозити, не само њихове податке, већ и системе и податке организација, посебно државних институција или малих и средњих предузећа где рад од куће није био уобичајена пракса.

Како би се избегле овакве ситуације, неопходно је користити препоручена техничка решења за рад на даљину, као и радити на константном унапређењу личне сајбер културе.

У складу са наведеним, Национални ЦЕРТ препоручује корисницима:

Уколико сте у могућности, користите **службени рачунар са уредно ажурираним оперативним системом и антивирусним програмом**. Коришћење приватних рачунара или мобилних уређаја уноси додатне ризике због могуће неажурности оперативног система и апликација, непостојања антивирусне заштите и врсте садржаја којима се приступа, те би организација у овом случају требало да уведе одговарајуће мере заштите. Коришћењем Network Access Control (NAC) система може се проверити тренутно стање уређаја и блокирати приступ ресурсима организације уколико нису задовољени унапред дефинисани услови. С друге стране, помоћу Mobile Device Management (MDM) система може се управљати великим бројем мобилних уређаја, обављати редовно ажурирање софтвера које користе, и раздвојити лични и пословни подаци.

1) Израда **процедура за безбедан рад од куће** за запослене и радно ангажоване.

2) **Неопходна је провера линкова на које се у мејлу захтева клик од стране корисника и потребно је бити опрезан приликом дељења информација** било путем мејла или телефона обзиром да је актуелан је велики број Phishing и Social Engineering напада који као тему користе COVID-19 вирус и покушавају да искористе стање општег страха и потребу за хитном реакцијом код људи.

3) **Не треба делити уређај који се користи за потребе посла** са децом или осталим члановима домаћинства. У супротном може доћи до ненамерног брисања података који припадају организацији и/или инфекције уређаја малициозним софтвером.

4) **Редовно ажурирати оперативне системе и софтвере** који су на приватним уређајима, а који се користе за приступ ресурсима организације.

5) Када се приступа интернет апликацијама или сајтовима који траже **логовање**, пожељно је **користити двофакторску аутентификацију** (уколико је подржана) **или посебну лозику за сваки од налога.** Двофакторска аутентификација у општем случају подразумева да је за успешно логовање, поред корисничког имена и лозинке, неопходно унети и привремени код који корисник прими на мобилни уређај. За потребе чувања лозинки корисницима се препоручује употреба апликација за управљање лозинкама (Password Manager).

6) **Потребно је пажљиво одабрати комуникациону платформу за одржавање састанака** са запосленима пратећи препоруке своје организације и поузданих јавних извора.

7) Приоритет свих корисника треба да буде **безбедност локалне мреже.** За разлику од ситуације када се рад обавља у просторијама организације, у кућним условима најчешће се користи **бежична WiFi мрежа**. Како би обезбедили заштићен приступ WiFi мрежи, препорука је да се промене подразумеване поставке (име и лозинка налога за подешавање WiFi Access Point-a, Service Set Identifier (SSID) име бежичне мреже), подеси јака лозинка за приступ мрежи, као и најјача доступна енкрипција. Старији, слабији облици шифрирања, као што је Wired Equivalent Privacy (WEP), нису сигурни и не треба их користити.

8) **Потребно је редовно правити резервну копију свих важних фајлова и датотека (бекап). Бекап** је препоручен као обавезна мера превенције јер пружа могућност да се подаци поврате у случају закључавања или брисања, што укључује могућност људске грешке, физичко оштећење хардвера или сајбер напад. Креирање резервне копије треба да буде организовано тако да оригинални подаци постоје на две локације које нису на истом уређају, тј. да је друга (резервна) локација изолована. Примери за безбедно чување резервних копија у изолованом окружењу су: клауд бекап (Cloud backup) или физичко чување резервних копија ван мреже (offline) нпр. на екстерном хард диску.

9) Приликом обављања службених дужности, потребно је да запослени **има приступ мрежи организације помоћу Virtual Private Network (VPN) мреже.** VPN технологија омогућава организацијама бољу заштиту од губитка и/или компромитације података, тако што се између локалне мреже прави безбедан и шифрован тунел, преко јавног интернета до мреже организације. Као додатни вид мере заштите препоручује се коришћење двофакторске аутентификације за VPN приступ. Организације треба да омогуће **централизовано логовање активности** корисника који се повезују путем VPN мреже како би се на време детектовало неуобичајено понашање и спречило да компромитовани уређај запослених угрози ресурсе организације.

10) Свака организација која је препозната Законом о информационој безбедности дужна је да **пријави значајна нарушавања безбедности својих система надлежном ЦЕРТ-у.**

Препоруке релевантних међународних организација о безбедносним аспектима рада од куће можете пронаћи на следећим линковима:

- https://www.enisa.europa.eu/tips-for-cybersecurity-when-working-from-home
- https://www.sans.org/security-awareness-training/sans-security-awareness-work-home-deployment-kit

СРБ-ЦЕРТ

#odbraniseznanjem