Iako je koncept rada od kuće i ranije postojao u kulturi pojedinih profesija i organizacija, trenutna situacija u vezi sa COVID-19 prouzrokovala je njegovu masovnu primenu. S jedne strane, rad od kuće je omogućio dalje funkcionisanje organizacija što može ublažiti predstojeću ekonomsku krizu, dok je s druge strane postavio nove izazove pred sajber bezbednost kako pojedinaca tako i organizacija.

Kompromitovanje uređaja pojedinaca u trenutnoj situaciji može ugroziti, ne samo njihove podatke, već i sisteme i podatke organizacija, posebno državnih institucija ili malih i srednjih preduzeća gde rad od kuće nije bio uobičajena praksa.

Kako bi se izbegle ovakve situacije, neophodno je koristiti preporučena tehnička rešenja za rad na daljinu, kao i raditi na konstantnom unapređenju lične sajber kulture.

U skladu sa navedenim, Nacionalni CERT preporučuje korisnicima:

1) Ukoliko ste u mogućnosti, koristite službeni računar sa uredno ažuriranim operativnim sistemom i antivirusnim programom. Korišćenje privatnih računara ili mobilnih uređaja unosi dodatne rizike zbog moguće neažurnosti operativnog sistema i aplikacija, nepostojanja antivirusne zaštite i vrste sadržaja kojima se pristupa, te bi organizacija u ovom slučaju trebalo da uvede odgovarajuće mere zaštite. Korišćenjem Network Access Control (NAC) sistema može se proveriti trenutno stanje uređaja i blokirati pristup resursima organizacije ukoliko nisu zadovoljeni unapred definisani uslovi. S druge strane, pomoću Mobile Device Management (MDM) sistema može se upravljati velikim brojem mobilnih uređaja, obavljati redovno ažuriranje softvera koje koriste, i razdvojiti lični i poslovni podaci.

2) Izrada procedura za bezbedan rad od kuće za zaposlene i radno angažovane.

3) **Neophodna je provera linkova na koje se u mejlu zahteva klik od strane korisnika i potrebno je biti oprezan prilikom deljenja informacija** bilo putem mejla ili telefona obzirom da je aktuelan je veliki broj Phishing i Social Engineering napada koji kao temu koriste COVID-19 virus i pokušavaju da iskoriste stanje opšteg straha i potrebu za hitnom reakcijom kod ljudi.

4) **Ne treba deliti uređaj koji se koristi za potrebe posla** sa decom ili ostalim članovima domaćinstva. U suprotnom može doći do nenamernog brisanja podataka koji pripadaju organizaciji i/ili infekcije uređaja malicioznim softverom.

5) **Redovno ažurirati operativne sisteme i softvere** koji su na privatnim uređajima, a koji se koriste za pristup resursima organizacije.

6) Kada se pristupa internet aplikacijama ili sajtovima koji traže **logovanje**, poželjno je **koristiti dvofaktorsku autentifikaciju** (ukoliko je podržana) **ili posebnu lozinku za svaki od naloga**. Dvofaktorska autentifikacija u opštem slučaju podrazumeva da je za uspešno logovanje, pored korisničkog imena i lozinke, neophodno uneti i privremeni kod koji korisnik primi na mobilni uređaj. Za potrebe čuvanja lozinki korisnicima se preporučuje upotreba aplikacija za upravljanje lozinkama (Password Manager).

7) **Potrebno je pažljivo odabrati komunikacionu platformu za održavanje sastanaka** sa zaposlenima prateći preporuke svoje organizacije i pouzdanih javnih izvora.

8) Prioritet svih korisnika treba da bude **bezbednost lokalne mreže**. Za razliku od situacije kada se rad obavlja u prostorijama organizacije, u kućnim uslovima najčešće se koristi **bežična WiFi mreža**. Kako bi obezbedili zaštićen pristup WiFi mreži, preporuka je da se promene podrazumevane postavke (ime i lozinka naloga za podešavanje WiFi Access Point-a, Service Set Identifier (SSID) ime bežične mreže), podesi jaka lozinka za pristup mreži, kao i najjača dostupna enkripcija. Stariji, slabiji oblici šifriranja, kao što je Wired Equivalent Privacy (WEP), nisu sigurni i ne treba ih koristiti.

9) **Potrebno je redovno praviti rezervnu kopiju svih važnih fajlova i datoteka (bekap). Bekap** je preporučen kao obavezna mera prevencije jer pruža mogućnost da se podaci povrate u slučaju zaključavanja ili brisanja, što uključuje mogućnost ljudske greške, fizičko oštećenje hardvera ili sajber napad. Kreiranje rezervne kopije treba da bude organizovano tako da originalni podaci postoje na dve lokacije koje nisu na istom uređaju, tj. da je druga (rezervna) lokacija izolovana. Primeri za bezbedno čuvanje rezervnih kopija u izolovanom okruženju su: klaud bekap (Cloud backup) ili fizičko čuvanje rezervnih kopija van mreže (offline) npr. na eksternom hard disku.

10) Prilikom obavljanja službenih dužnosti, potrebno je da zaposleni **ima pristup mreži organizacije pomoću Virtual Private Network (VPN) mreže**. VPN tehnologija omogućava organizacijama bolju zaštitu od gubitka i/ili kompromitacije podataka, tako što se između lokalne mreže pravi bezbedan i šifrovan tunel, preko javnog interneta do mreže organizacije. Kao dodatni vid mere zaštite preporučuje se korišćenje dvofaktorske autentifikacije za VPN pristup. Organizacije treba da omoguće **centralizovano logovanje aktivnosti** korisnika koji se povezuju putem VPN mreže kako bi se na vreme detektovalo neuobičajeno ponašanje i sprečilo da kompromitovani uređaj zaposlenih ugrozi resurse organizacije.

11) Svaka organizacija koja je prepoznata Zakonom o informacionoj bezbednosti dužna je da **prijavi značajna narušavanja bezbednosti svojih sistema nadležnom CERT-u**.

Preporuke relevantnih međunarodnih organizacija o bezbednosnim aspektima rada od kuće možete pronaći na sledećim linkovima:

- 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

SRB-CERT

#odbraniseznanjem