

Kibernetska varnost (ni) na dopustu

Kibernitje:
www.kibernitje.si



10 varnostnih ukrepov za službeni prenosnik

- vnos gesla ob zagonu računalnika
- vnos močnega gesla ali prstnega odtisa za dostop do operacijskega sistema*
- zaklenjen zaslon z močnim geslom ali prstnim odtisom*
- šifriranje diska oziroma podatkov*
- zaklenjene nastavitve varnostnega programa z geslom
- zaklenjen zagon iz USB-ključka
- zaklenjen dostop do BIOS-a
- posodobljen operacijski sistem in vsi programi*
- omejitev internetnega dostopa na VPN z večfaktorsko avtentikacijo*
- večfaktorska avtentikacija za vse storitve*

**velja tudi za pametne telefone in tablice*

Napotki za IT-ekipe

- Omejite zunanji dostop do internih storitev zgolj na povezave VPN.
- Seznanite zaposlene z nevarnostmi uporabe tujih omrežij Wi-Fi in javnih računalnikov.
- Določite standardne postopke za primere izgube oziroma kraje službenih naprav.
- Poskrbite za varnostne kopije pred odhodom na dopust.
- Prilagodite načrt za odzivanje na varnostne incidente v primerih odsotnosti.
- Namestite in preizkusite javno dostopne storitve za skupinsko delo v primeru izpada internih storitev.

Izogibajte se tveganeu vedenju



Če le morete, pustite službene naprave med dopustom - v službi.

Pri pripravi nasvetov o uporabi službenih naprav med dopustom so sodelovali:

Adrien Žitko, SIQ
Boštjan Špehonja, Go-Lix
Matjaž Kolnik, NIL
Miha Lavrič, CREAPLUS
Tadej Hren, SI-CERT

Projekt so podprli:



Pazite na svoje naprave

Ne puščajte nezavarovanih prenosnikov v avtomobilu, hotelski sobi, šotoru, na jedilni mizi, stolu ali na drugih vidnih lokacijah.

Zaklepajte zaslon naprave, ko je ne uporabljate – tudi če prekinete uporabo samo za minuto – in še posebej, če ste na javnem mestu.

Izogibajte se polnjenju mobilnih naprav v javnih USB-polnilnicah.

Pri letalskih prevozih ne dajte naprav v oddano prtljago.

Pazljivo pri dostopanju do interneta

Ne priklaplajte se na odprta omrežja Wi-Fi, še posebej ne na letališčih, v trgovskih središčih in gostinskih lokalih.

Priklaplajte se samo na zaščitena omrežja Wi-Fi in še to le ob uporabi zaščite, kot so požarni zid, VPN, protivirusni program in šifriranje podatkov.

Prenašajte vsebine samo iz zaupanja vrednih virov

Ne prepuščajte službenih računalnikov otrokom za igranje igrice, uporabo družbenih omrežij in gledanje pretočnih vsebin.

Ne prenašajte nelegalnih, piratskih vsebin, na primer filmov preko torrentov.

Prenašajte le preverjene aplikacije iz uradnih virov (Google Play, App Store ...).

Ne razkrivajte občutljivih podatkov

V družbenih omrežjih ne objavljajte slik, iz katerih se lahko razbere občutljive podatke (naslov vaše lokacije, letalske karte, potni listi, bančne kartice).

Z objavami v družbenih omrežjih kriminalce obveščate, kdaj vas ni doma ali v hotelski sobi – omejite objave in preprečite oškodovanje vaše lastnine, vključno s službenimi napravami.

Umaknite vse listke z občutljivimi podatki, ki ste jih nalepili doma ali v službi.

