MINUTKA

ZA VARNOST IN ZASEBNOST

10.11.2022 3/2022

Zlata pravila:

1.

Uporabljajte močna gesla in jih redno spreminjajte.

2.

Ne klikajte na nenavadne povezave ali pojavna okna.

3.

Bodite previdni pri odpiranju e-pošte, če ne poznate pošiljatelja.

4.

Bodite pozorni na svoje objave na družbenih omrežjih.

5.

Če je mogoče službenih naprav ne uporabljajte za osebne namene.

Top 3 grožnje

oktober 2022

1. Zloraba osebnih podatkov

2. Phishing

3. Zastarela programska oprema

Kaj je novega?

Pozor, ponoven porast direktorskih prevar! Spletni napadalci tokrat prevare širijo prek SMS, WhatsApp in ostalih popularnih aplikacij. Prevare prepoznate po tem, da vas »direktor« nujno prosi za posredovanje občutljivih podatkov, bančno nakazilo na točno določen naslov, ali nakup darilnih kartic.

Nasvet: *Bodite pozorni na nenavadne prošnje, pomanjkljivo vsebino in vse zahteve, ki od vas zahtevajo hitro reakcijo. Če niste prepričani ali je zahteva legitimna, vedno preverite pri direktorju. Pozorni bodite predvsem na prošnje po večjih denarnih zneskih in po posredovanju občutljivih podatkov.*

Brskalnik Brave je že dolgo poznan kot brskalnik, ki se trudi svojim uporabnikom dati kar največ zasebnosti, pri čemer pa se trudi kar najmanj motiti delovanje spletnih strani. Tokrat je v nabor funkcionalnosti dodal še možnost, da ob obisku spletnih strani uporabniku ne prikaže pasice o piškotkih, ki je za večino uporabnikov moteča in nepotrebna.

Nasvet: *Če je le mogoče, namesto brskalnikov, ki jim je manj za vašo zasebnost, uporabite brskalnik Brave. Če to ni mogoče na delovnem mestu, pa vsaj doma.*

Skupina kiber-kriminalcev *Crimson Kingsnake* trenutno izvaja phishing napad, v katerem se prek e-pošte predstavljajo za predstavnike velikih svetovnih odvetniških in revizijskih hiš, ter tarče opozarjajo na lažna zapadla plačila.

Nasvet: *Vedno dvakrat preverite resničnost poslanega e-poštnega sporočila, ki od vas zahteva kakršnokoli aktivnost. Če niste prepričani ali gre za legitimno zahtevo ali ne, vedno preverite pri sodelavcu na relevantnem področju.*

Tema tedna: Kako izbrati primerno geslo?

Izbira primernega gesla je ena najpogostejših tem na informacijsko varnostnih izobraževanjih, hkrati pa še vedno eno najpogostejših vprašanj, takoj ko omenimo informacijsko varnost. Ker pa gre za izjemno pomembno temo, je prav, da vse dileme rešimo enkrat za vselej.

Da bi razumeli zakaj je močno geslo tako pomembno, moramo najprej razumeti kako pride do zlorabe gesel. Če želijo spletni kriminalci priti do vašega gesla, lahko to storijo na dva načina. Prvi način vključuje uporabo programa, ki proti vašemu geslu preizkusi seznam besed ali besednih zvez, ki se pogosto uporabljajo kot gesla. Drugi način pa vključuje sistematično ugibanje gesla, kjer program preizkusi vse možne kombinacije znakov – od 0000000 do žžžžžžž.

Iz obeh načinov lahko takoj ugotovimo katera gesla so najranljivejša: kratka gesla, ki vsebujejo zgolj eno običajno besedo, ime ali številko. Zato lahko sklepamo, da mora biti dobro geslo dovolj dolgo in vsebovati več različnih in naključnih znakov. Toda kako dolgo in kako si tako geslo zapomniti?

Trenutno (november 2022) velja, da mora varno geslo vsebovati najmanj 16 znakov, z vsaj enim posebnim znakom – to pravilo seveda velja, če gre za 16 naključnih znakov. Vendar pa si je 16 naključnih znakov težko zapolniti. Zato velja upoštevajte naslednje nasvete:

- Se vam že dlje časa poje neka pesem? Verz pesmi je lahko odlično geslo, saj brez težav doseže več kot 30 znakov. Če zamenjate še kakšen *s* za *$*, ali *e* za *€*, pa ste zmagovalci. Verzov pesmi (sploh v slovenščini) ni na seznamu pogostih gesel, hkrati pa jih lahko redno in brez težav zamenjate.
- Tako kot verz pesmi lahko uporabite tudi stavek iz knjige ali vam ljubo misel.

Če gre za daljši verz ali stavek, lahko geslo sestavite z združitvijo prvih črk vsake besede v stavku.

Ne pozabite:

1. najmanj 16 znakov z najmanj enim posebnim znakom

2. uporaba besednih zvez s posebnim pomenom

3. katero izmed črk zamenjajte s posebnim znakom

SGB varnostno svetovanje

InfoHiša