Newsletter Nacionalnog CERT-a – CERT info

Sadržaj

Tema mjeseca: Zaštita korisničkog računa

U današnjem digitalnom dobu, zaštita korisničkog računa nije samo preporuka - ona je nužnost. Kako se tehnologija razvija, tako napreduju i metode kibernetičkih kriminalaca. Od krađe identiteta do ransomware napada, prijetnje su raznolike i često usmjerene na najslabiju kariku: korisnika. Zaštita računa znači zaštitu osobnog i profesionalnog identiteta, a sve počinje pametnim i dosljednim praksama kibernetičke sigurnosti.

Autentifikacija

Autentifikacija je prva linija obrane. Tradicionalne lozinke više nisu dovoljne. Korisnicima se preporučuje korištenje višestruke autentifikacije (MFA), što znači da je za pristup korisničkom računu potrebno koristiti dva ili više različitih oblika autentifikacije. Autentifikacija se može vršiti s pomoću nečega što znamo, nečega što imamo ili nečega što jesmo.

Ono što znamo može biti korisničko ime i lozinka, ali korištenje dvije različite lozinke za jedan korisnički račun, ne zadovoljava uvjet višestruke autentifikacije, jer obje lozinke spadaju u skupinu autentifikacije s pomoću onoga što znamo.

Nešto što imamo može se odnositi na token ili fizički ključ/karticu bez kojih nije moguće pristupiti računu. Broj tokena nije poznat prije nego se generira, a on može biti dostavljen putem poruke, poziva, maila ili generiran na fizičkom tokenu ili aplikaciji na našem uređaju.

Nešto što jesmo, odnosi se na naše biometrijske podatke, tj. za autentifikaciju se mogu koristiti naše fizičke osobine kao što su otisak prsta, sken šarenice oka, boja glasa i sl. Kako bi autentifikacija bila višestruka, potrebno je koristiti barem dva različita oblika autentifikacije.

Lozinka

Iako ne postoji savršena lozinka koja štiti 100%, kao ni jednoglasni konsenzus stručnjaka oko pravila dobre lozinke, postoje određene smjernice koje trebamo pratiti kako bi ona bila što sigurnije.

Nacionalni CERT savjetuje da:

- Stavite prioritet na duljinu lozinke (barem 16 znakova)
- Kombinirajte slova (velika i mala), brojeve i znakove
- Ne koristite iste lozinke za različite sustave, pogotovo ne za privatne i poslovne račune
- Ne koristite česte fraze ili sljedove znakova (123456789, qwertz, asdfgh i sl.)
- Ne dijelite lozinke s drugima
- Ne šaljite lozinke mailom, porukama i drugim nesigurnim kanalima komunikacije
- Ako već zapisujete lozinke na papir, ne ostavljajte takve zapise na vidljivim mjestima
- Ako možete, ne koristite prave riječi (lozinke nasumičnih znakova su ipak malo sigurnije)
- Izbjegavajte spremanje lozinki u internetske preglednike
- Koristite password manager/upravitelj lozinki
- Ako imate mogućnost, uključite višestruku autentifikaciju!

Preuzmite infografiku i postavite je na vidljivo mjesto na poslu ili u domu

Upravitelj lozinki

Kako ne bi morali pamtiti brojne lozinke, korisnici često koriste istu lozinku za sve servise. Nažalost, to predstavlja ozbiljan sigurnosni rizik. U tom slučaju, ako napadač ukrade lozinku korisnika na jednom servisu, može ju iskoristiti i za pristup drugim servisima. Nažalost, ni korištenje različitih lozinki za svaki servis nije samo po sebi dovoljno. Ako korištene lozinke nisu dovoljno složene, napadač može dobiti pristup korisnikovom računu napadom uzastopnim pogađanjem (eng. brute-force attack). Kako bi se doskočilo problemu pamćenja većeg broja složenih lozinki, koriste se tzv. upravitelji lozinkama (engl. password managers) koji omogućavaju generiranje i pohranu većeg broja složenih lozinki u šifriranom obliku. Do lozinki u izvornom obliku se dolazi poznavanjem samo jedne, glavne lozinke (engl. master password) koja omogućava dešifriranje ostalih lozinki. Zahvaljujući ovakvom pristupu, krajnji korisnik mora zapamtiti samo jednu, glavnu lozinku, ali može koristiti različite, složene lozinke za različite servise. Jedan od takvih alata je i KeePass o kojem više možete pročitati ovdje.

Biometrija

Biometrija (eng. biometrics) se odnosi na metode raspoznavanja ljudi na temelju jedne ili više svojstvenih osobina i značajki. Biometriju je moguće podijeliti na fizička svojstva i svojstva u ponašanju. Fizička svojstva se svakako odnose na oblik tijela ili dijelove tijela pojedinca. Neki od primjera su: otisci prstiju, tehnike prepoznavanja lica, DNK, geometrija ruku i dlanova, itd. Svojstva u ponašanju se odnose na npr. ritam tipkanja na računalu, glasovno prepoznavanje,

držanje osobe, itd. Ljudske osobine ili svojstva koja zadovoljavaju sljedeće kriterije mogu se koristiti kao sredstvo za identifikaciju:

- **univerzalnost** - svaka osoba bi trebala imati karakterističnо svojstvo/osobinu
- **jedinstvenost** - govori koliko su biometrijska svojstva/osobine pojedinaca različite
- **trajnost** - govori koliko je biometrijsko svojstvo/osobina otporna na starenje
- **mogućnost prikupljanja** - govori koliko je jednostavno prikupiti uzorke za potrebna mjerenja

Kibernetička higijena u radu kod kuće

Razvoj tehnologije značajno je promijenio radne navike i prakse poslovanja. Mnogi poslovi više ne zahtijevaju odlazak u ured i mogu se obavljati iz bilo kojeg prostora, ako su zaposleniku dostupni internet i signal. Prilikom rada od kuće potrebno je pridržavati se nekih pravila ponašanja kao i prilikom rada u uredu. Standardna pravila kibernetičke higijene i dalje vrijede, a uključuju korištenje snažnih lozinki, redovito ažuriranje sustava, stvaranje sigurnosnih kopija podataka, korištenje sigurne mreže te korištenje snažnih lozinki.

Za siguran rad od kuće nužno je napraviti nekoliko dodatnih koraka. Potrebno je promijeniti lozinku kućnog WiFi-a, kako se neželjene osobe ne bi mogle spojiti na mrežu i pregledavati promet koji njome prolazi. Ne zaboravite kako se poslovni uređaji, kao i poslovni računi ne bi trebali koristiti za privatne stvari. Djeca ne bi trebala koristiti poslovna računala za svoje potrebe, kao što ni zaposlenici ne bi trebali koristiti poslovne račune za servise koji nisu vezani uz rad. Uređaj uvijek zaključajte kada ga ne koristite, a i kod kuće budite oprezni – izbjegavajte nesigurne internetske stranice i ne preuzimajte datoteke iz nepoznatih izvora. Više o savjetima za rad od kuće možete pročitati na infografici koja se nalazi ovdje.

Statistika obrađenih incidenata – travanj 2025.

Prema dostupnim statistikama Nacionalnog CERT-a za travanj 2025. godine vidljivo je kako je najveći broj prijavljenih i obrađenih incidenata u kategoriji „phishing napad“.

Phishing napad	**40**	**28%**
Neželjene poruke	36	26%
Ostale vrste financijski motivirani prijevara	21	15%
Napadačka infrastruktura	14	10%
Pogađanje pristupnih podataka	13	9%
Kompromitiran uređaj	3	2%
Ispad usluge	2	1%
Kompromitiran informacijski sustav	2	1%
Krađa podataka	2	1%
Pokušaj iskorištavanja ranjivosti	2	1%
Poslovne prijevare	**2**	1%
Krađa pristupnih podataka	**1**	1%
Neovlaštena izmjena sadržaja	**1**	1%
Ucjenjivački napadi	**1**	1%
Uskraćivanje usluge	**1**	1%
Ukupno	**141**	

Najava događanja

23.6. 2025. - Dan žena u inženjerstvu

30.6.2025. - Dan društvenih mreža

Prethodni brojevi

Newsletter Nacionalnog CERT-a – CERT info – siječanj 2025.

Newsletter Nacionalnog CERT-a – CERT info – veljača 2025.

Newsletter Nacionalnog CERT-a – CERT info – ožujak 2025.

Newsletter Nacionalnog CERT-a – CERT info – travanj 2025.