

Kibernetska varnost

Varnost v oblaku

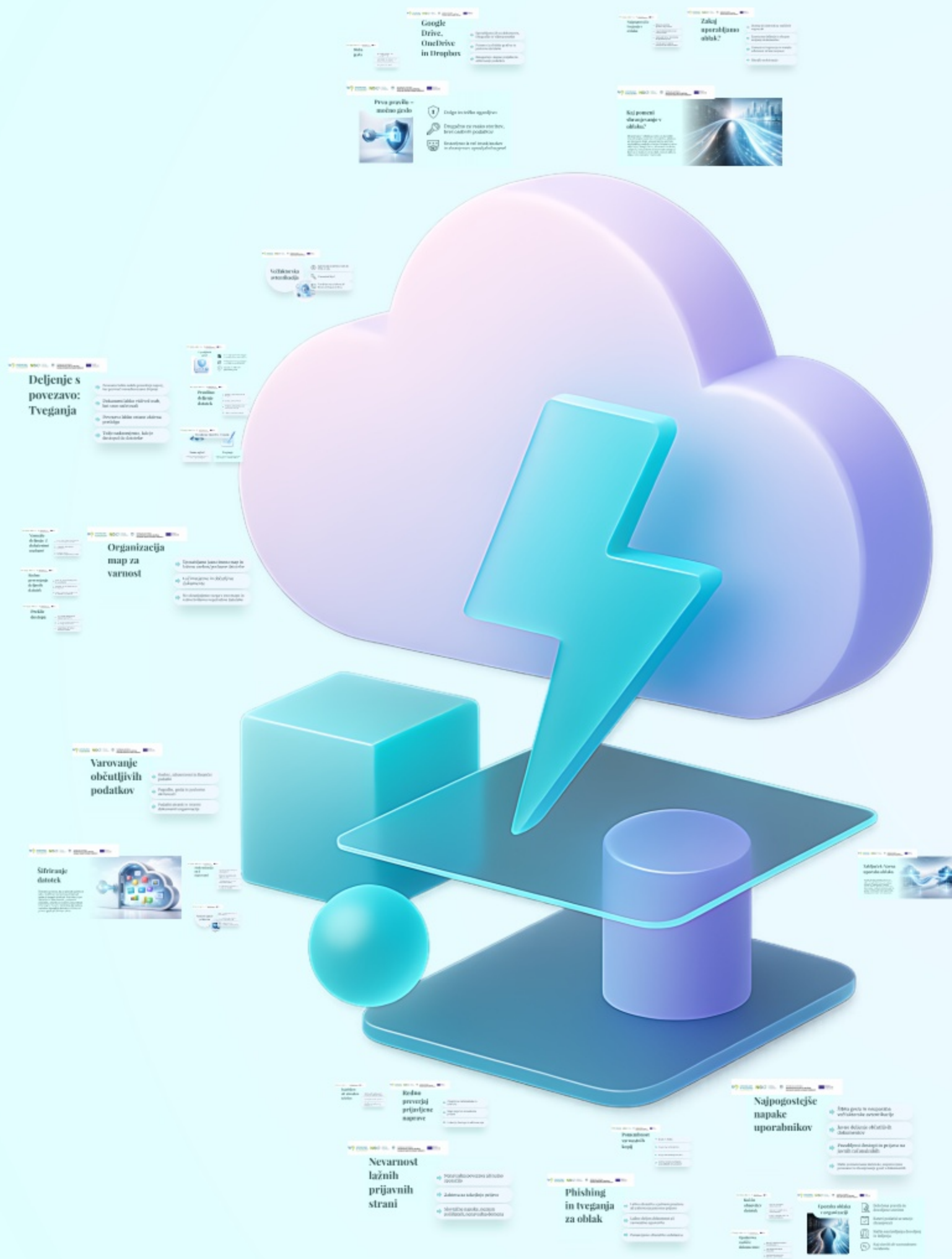
Kako zaščitimo datoteke v Google Drive, OneDrive ali Dropboxu

Predavatelj: dr. Miha Dvojmoč

Naročnik: SSA d.o.o.

Izvajalec: MD svetovanje d.o.o.

Datum: 5. 12. 2024



Kaj pomeni shranjevanje v oblaku?

Shranjevanje v oblaku pomeni, da datoteke niso shranjene samo na računalniku, telefonu ali zunanjem disku, ampak tudi na spletnih strežnikih ponudnika storitve. Primeri storitev vključujejo Google Drive, Microsoft OneDrive, Dropbox, iCloud Drive in Box. Oblak omogoča dostop do datotek od kjer koli, vendar zahteva odgovorno ravnanje z varnostjo.



Zakaj uporabljamo oblak?

- ➔ Dostop do datotek na različnih napravah
- ➔ Enostavno deljenje in skupno urejanje dokumentov
- ➔ Varnostno kopiranje in manjša odvisnost od ene naprave
- ➔ Hitrejšše sodelovanje

Najpogostejša tveganja v oblaku

- ➔ Šibka gesla in kraja uporabniškega računa
- ➔ Napačno deljenje datotek ali javne povezave
- ➔ Izguba naprave ali zlonamerna programska oprema
- ➔ Nepooblaščen dostop in pomotoma izbrisane datoteke

Google Drive, OneDrive in Dropbox

- Uporabljamo jih za dokumente, fotografije in videoposnetke
- Primerni za šolska gradiva in poslovne datoteke
- Omogočajo skupne projekte in arhiviranje podatkov



Prvo pravilo – močno geslo



Dolgo in težko uganljivo



Drugačno za vsako storitev,
brez osebnih podatkov



Sestavljeno iz več besed/znakov
in shranjeno v upravljalniku gesel

Slaba gesla

- ➔ Preprosta zaporedja (npr. 123456, geslo123)
- ➔ Osebni podatki (npr. ime otroka, datum rojstva, ime hišnega ljubljénčka)
- ➔ Isto geslo za vse račune



USPOSABLJAMO
IN PRILAGAJAMO
TRAINING AND ADJUSTMENT



NAČRT ZA
OKREVANJE
IN ODPORNOST



REPUBLIKA SLOVENIJA
MINISTRSTVO ZA DELO, DRUŽINO,
SOCIALNE ZADEVE IN ENAKE MOŽNOSTI



Financira
Evropska unija
NextGenerationEU

Večfaktorska avtentikacija



Aplikacija za potrjevanje ali
SMS-koda



Varnostni ključ



Potrditev na telefonu ali
biometrična potrditev



Upravljalnik gesel



Ni si treba zapomniti vseh gesel
in omogoča ustvarjanje močnih



Zmanjša ponovno uporabo gesel
in pomaga pri varnejši prijavi



Opozarja na šibka ali
ponovljena gesla

Pravilno deljenje datotek

- ➔ Deljenje z določeno osebo ali skupino
- ➔ Deljenje prek povezave
- ➔ Možnost samo za ogled ali z možnostjo urejanja
- ➔ Začasno ali trajno deljenje

Dovoljenja: Ogled vs. Urejanje



Samo ogled

Prejemnik lahko dokument vidi, ne more pa ga spreminjati.

Urejanje

Prejemnik lahko dokument spreminja, dopolnjuje ali celo izbriše vsebino.

Deljenje s povezavo: Tveganja

- ➔ Povezavo lahko nekdo posreduje naprej, kar povzroči nenadzorovano širjenje
- ➔ Dokument lahko vidi več oseb, kot smo načrtovali
- ➔ Povezava lahko ostane aktivna predolgo
- ➔ Težje nadzorujemo, kdo je dostopal do datoteke

Varnejše deljenje: Z določenimi osebami

- ➔ Dostop imajo samo izbrani uporabniki in lažje nadzorujemo dovoljenja
- ➔ Po potrebi lahko dostop prekličemo
- ➔ Manjša je možnost nenadzorovanega širjenja povezave

Redno preverjanje deljenih datotek

- ➔ Preverite, kdo ima dostop in ali je ta še potreben
- ➔ Preglejte, ali ima oseba pravico do urejanja
- ➔ Preverite, ali so aktivne javne povezave in ali je treba dostop preklicati

Preklic dostopa

- ➔ Ko je projekt zaključen ali oseba ne sodeluje več
- ➔ Če smo datoteko delili pomotoma ali obstaja varnostni sum
- ➔ Kadar dokument vsebuje občutljive podatke



Organizacija map za varnost



Uporabljamo jasna imena map in ločimo osebne/poslovne datoteke



Ločimo javne in občutljive dokumente



Ne shranjujemo vsega v eno mapo in redno brišemo nepotrebne datoteke

Varovanje občutljivih podatkov

- Osebni, zdravstveni in finančni podatki
- Pogodbe, gesla in poslovne skrivnosti
- Podatki strank in interni dokumenti organizacije

Šifriranje datotek

Šifriranje pomeni, da so podatki zaščiteni tako, da jih brez ustreznega ključa ali gesla ni mogoče prebrati. Koristno je pri občutljivih dokumentih, poslovnih podatkih, arhivih in hrambi pomembnih informacij. Za zelo občutljive datoteke je smiselno uporabiti dodatno zaščito, na primer geslo ali šifriran arhiv.





Sinhronizacija med napravami

- ➔ Spremembe se prenesejo na druge naprave
- ➔ Izbris na eni napravi lahko vpliva na oblak
- ➔ Okužena datoteka se lahko sinhronizira naprej
- ➔ Uporabnik mora paziti, katere naprave so povezane

Varnost naprav je ključna



Zaklepanje računalnika in telefona



Posodabljanje sistema in protivirusna zaščita



Previdnost pri javnih računalnikih in odjava po uporabi



Izgubljen ali ukraden telefon

- ➔ Naprava naj bo zaklenjena in omogočeno oddaljeno brisanje
- ➔ Uporabljajte biometrijo ali PIN
- ➔ Ob izgubi spremenite geslo, preverite prijavljene naprave in odstranite dostop izgubljeni napravi

Redno preverjaj prijavljene naprave

- ➡ Prijavljene računalnike in telefone
- ➡ Stare naprave in neznane prijave
- ➡ Lokacije dostopa in aktivne seje

Nevarnost lažnih prijavnih strani

- ➡ Nenavadna povezava ali nujno sporočilo
- ➡ Zahteva za takojšnjo prijavo
- ➡ Slovnične napake, neznan pošiljatelj, nenavadna domena

Phishing in tveganja za oblak

- ➔ Lažno obvestilo o polnem prostoru ali zahteva za ponovno prijavo
- ➔ Lažno deljen dokument ali varnostno opozorilo
- ➔ Ponarejeno obvestilo sodelavca

Pomembnost varnostnih kopij

- ➔ Kopija v oblaku
- ➔ Kopija na računalniku
- ➔ Kopija na zunanjem disku
- ➔ Ločena varnostna kopija pomembnih dokumentov

Koš in obnovitev datotek

- ➔ Obnovitev pomotoma izbranih datotek
- ➔ Obnovitev, če nekdo izbriše skupni dokument
- ➔ Dostop do starejših različic ali obnova celotne mape

Zgodovina različic dokumentov

- Omogoča ogled in obnovitev prejšnjih različic
- Popravljanje napačnih sprememb
- Ugotavljanje, kdaj je bila datoteka spremenjena

Uporaba oblaka v organizaciji



Določena pravila in
dovoljene storitve



Kateri podatki se smejo
shranjevati



Način nastavljanja dovoljenj
in deljenja



Kaj storiti ob varnostnem
incidentu



Najpogostejše napake uporabnikov



Šibka gesla in neuporaba
večfaktorske avtentikacije



Javno deljenje občutljivih
dokumentov



Pozabljeni dostopi in prijava na
javnih računalnikih



Slabo poimenovane datoteke, nepreverjene
povezave in shranjevanje gesel v dokumentih



USPOSABLJAMO
IN PRILAGAJAMO
TRAINING AND ADJUSTMENT



NAČRT ZA
OKREVANJE
IN ODPORNOST



REPUBLIKA SLOVENIJA
MINISTRSTVO ZA DELO, DRUŽINO,
SOCIALNE ZADEVE IN ENAKE MOŽNOSTI



Financira
Evropska unija
NextGenerationEU

Zaključek: Varna uporaba oblaka

Varnost v oblaku je pomembna, ker so naše datoteke dostopne prek interneta in pogosto deljene z drugimi. Ključni ukrepi vključujejo močna gesla, večfaktorsko avtentikacijo, previdno deljenje, redno preverjanje dostopov, varne naprave, previdnost pri lažnih povezavah, varnostne kopije in urejeno strukturo datotek. Oblak je zelo uporabno orodje, vendar je varen le toliko, kolikor odgovorno ga uporabljamo.



Kibernetska varnost

Varnost v oblaku

Kako zaščitimo datoteke v Google Drive, OneDrive ali Dropboxu

Predavatelj: dr. Miha Dvojmoč

Naročnik: SSA d.o.o.

Izvajalec: MD svetovanje d.o.o.

Datum: 5. 12. 2024

