

Kibernetska varnost

Povzetek za udeležence izobraževanja • Oktober 2026

Kibernetska varnost varuje naše naprave, račune ter osebne in poslovne podatke pred zlorabo. Tehnična zaščita je pomembna, veliko pa lahko naredimo tudi sami: preverimo nenavadne zahteve, zaščitimo svoje račune in ob sumu prevare hitro obvestimo pristojno osebo.

Kaj varujemo in zakaj

Informacijska varnost temelji na treh načelih: zaupnosti, da podatke vidijo le pooblaščen osebe; celovitosti, da podatki ostanejo pravilni in brez nepooblaščenih sprememb; ter razpoložljivosti, da so podatki in storitve dostopni, ko jih potrebujemo.

Varnostni incident lahko podjetju povzroči prekinitev dela, izgubo podatkov in zaupanja ter finančno škodo. Posameznik se lahko sooči s krajo identitete, izgubo denarja, izsiljevanjem in stresom.

Najpogostejše grožnje

- Socialni inženiring in phishing: napadalec z lažno identiteto ali prepričljivo zgodbo poskuša doseči, da razkrijemo podatke, odpremo priponko ali izvedemo plačilo.
- Zlonamerna programska oprema: omogoča krajo podatkov ali dostop do naprave. Izsiljevalska programska oprema oziroma ransomware lahko podatke zašifrira, napadalci pa lahko grozijo tudi z objavo ukradenih podatkov.
- Zloraba računov: napadalec pridobi geslo ali ga ugane ter račun uporabi za krajo informacij in nadaljnje prevare.
- Tehnični napadi: izkoriščanje ranljivosti sistemov in aplikacij, prestrezanje komunikacij ter napadi DoS oziroma DDoS, ki onemogočijo dostop do storitev.

Gesla in večfaktorsko preverjanje

Za vsak račun uporabljajte dolgo in edinstveno geslo. Osebnih in službenih gesel ne uporabljajte izmenično. Pri ustvarjanju in varnem shranjevanju gesel vam lahko pomaga upravljalnik gesel, ki ga odobri organizacija.

Vključite večfaktorsko preverjanje pristnosti (MFA). Poleg gesla zahteva še dodaten dokaz, na primer potrditev v aplikaciji ali varnostni ključ. MFA zmanjša možnost zlorabe računa, vendar ne odpravi vseh tveganj. Potrdite le prijavo, ki ste jo sami sprožili, in nikomur ne posredujte potrditvenih kod.

Kako prepoznamo spletno prevaro

Phishing je lažno predstavljanje z namenom kraje podatkov ali druge zlorabe. Sporočilo lahko posnema banko, dostavno službo, sodelavca ali vodstvo podjetja. Prepričljiv videz, znan logotip in pravilna slovenščina še ne dokazujejo pristnosti.

Preverjanje sporočila pred ukrepanjem

1. **Pošiljatelj.** Preverite celoten e-poštni naslov in domeno, ne le prikazanega imena. Podobne črke ali dodan znak lahko prikrijejo prevaro.
2. **Povezava.** Pred klikom preverite dejanski cilj povezave. Če ste v dvomu, odprite storitev prek znanega zaznamka ali sami vpišite njen uradni naslov.
3. **Zahtevani podatki.** Bodite posebej previdni ob zahtevah za gesla, potrditvene kode, podatke kartice ali druge zaupne informacije.
4. **Priponke.** Ne odpirajte nepričakovanih priponk. Zaradi navodil v sporočilu ne omogočajte makrov ali druge aktivne vsebine.
5. **Nujnost in pritisk.** Opozorila o takojšnji blokadi računa, grožnje ali zahteve za nujno nakazilo so razlog za dodatno preverjanje.
6. **Vsebina in podpis.** Preverite, ali zahteva ustreza običajnemu sodelovanju in ali se podpis ujema s pošiljateljem. Slovnične napake so lahko znak prevare, njihova odsotnost pa ni dokaz varnosti.
7. **Neodvisna potrditev.** Nenavadno zahtevo preverite po že znani telefonski številki ali prek drugega zaupanja vrednega kanala. Ne uporabite kontaktnih podatkov iz sumljivega sporočila.

Prevara se lahko pojavi po različnih kanalih

Poleg e-pošte napadalci uporabljajo sporočila SMS (smishing), telefonske klice (vishing) in kode QR (quishing). Ciljani napadi na določeno osebo ali organizacijo se imenujejo spear phishing, napadi na vodilne pa whaling. Nekatera sporočila so namenjena predvsem namestitvi zlonamerne programske opreme.

Umetna inteligenca pomaga ustvarjati prepričljiva besedila in posnemati glasove. Tudi znan glas ali osebno nagovarjanje zato nista zadostna potrditev identitete.

Primer iz predstavitve: lažna prijavna stran je lahko videti povsem enako kot prava. Odločilna razlika je lahko v spletnem naslovu, na primer v dodatni črki ali zamenjavi črke »m« z znakoma »rn«. Pred vnosom podatkov vedno preverite domeno.

Varno ravnanje pri vsakdanjem delu

Kontrolni seznam za uporabnika

- Uporabljam različna gesla za različne račune in imam vključeno MFA.
- Ob odhodu od naprave zaklenem računalnik in telefon.
- Redno nameščam odobrene posodobitve in upoštevam navodila IT.
- Ne priklopljam neznanih ključkov USB in ne nameščam nepreverjenih programov.
- Uporabljam zaupanja vredna omrežja ter upoštevam pravila za delo na daljavo.
- Na družbenih omrežjih premišljeno objavljam osebne in službene podatke.
- Podatke shranjujem na odobrenih mestih, arhiviram in brišem pa jih skladno s pravili organizacije.
- Pred nakazilom ali spremembo podatkov prejemnika nenavadno zahtevo dodatno preverim.

Kaj zagotavlja organizacija

Podjetje potrebuje jasna varnostna pravila, redno usposabljanje zaposlenih, posodobljene sisteme in ustrezne varnostne rešitve. Dostopi naj bodo omejeni na podatke in opravila, ki jih zaposleni potrebuje za delo. Pomembni so tudi šifriranje občutljivih podatkov, varnostne kopije s preverjanjem obnovitve, spremljanje dogodkov in vnaprej določen postopek ob incidentu.

Kako ravnati ob sumu incidenta

Praktični opomnik za uporabo ob izobraževanju

1. Ustavite se. Ne klikajte nadaljnjih povezav, ne odpirajte priponk in ne potrjujte nepričakovanih zahtev za prijavo.
2. Čim prej obvestite službo IT oziroma osebo, ki je v organizaciji zadolžena za varnost. Uporabite dogovorjeni kanal za prijavo.
3. Povejte, kaj se je zgodilo: katero sporočilo ste prejeli, kaj ste odprli in ali ste vnesli podatke ali potrdili prijavo. Prijavite tudi napako, ki ste jo že storili.
4. Shranite sporočilo in podatke o dogodku za obravnavo ter sledite navodilom pristojne ekipe. Hitro obvestilo lahko omeji škodo.

Dodatno gradivo iz predstavitve

SI-CERT: <https://www.cert.si/>

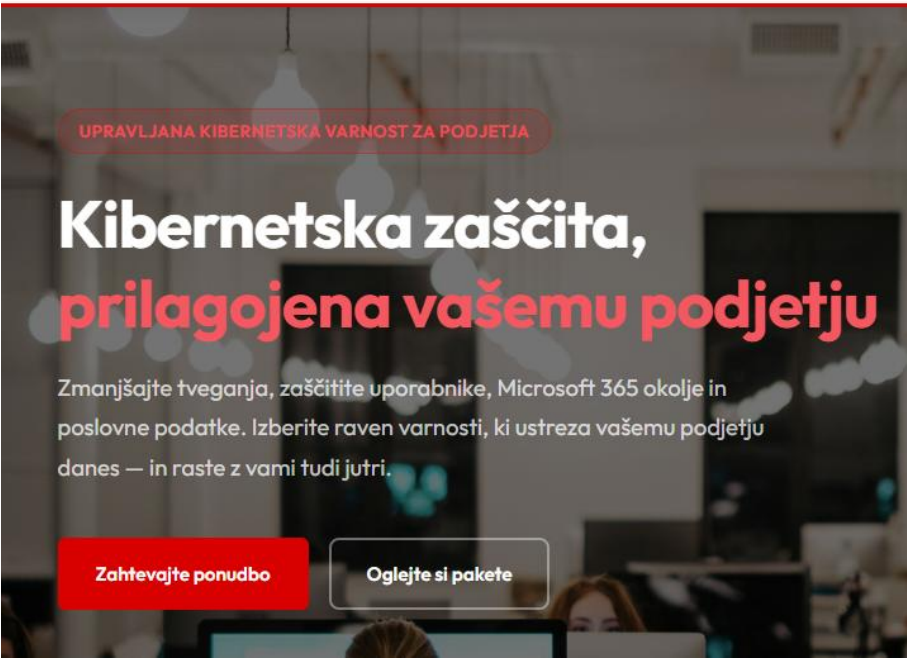
Varni na internetu: <https://www.varninainternetu.si/>

Varni v pisarni: <https://www.varnivpisarni.si/>

Pazi.se: <https://pazi.se/>

Vir: predstavitev Kibernetaska varnost, oktober 2026, vključno z opombami predavatelja. Vsebina je strnjena in jezikovno urejena za udeležence; statistike in posamezne zgodbe o incidentih so izpuščene. Postopek ob sumu incidenta je dodan kot praktični opomnik.

UShield360

The banner features a blurred background of an office interior with people working at computers. At the top, a red pill-shaped button contains the text 'UPRAVLJANA KIBERNETSKA VARNOST ZA PODJETJA'. Below this, the main headline reads 'Kibernetaska zaščita, prilagojena vašemu podjetju', with 'Kibernetaska zaščita,' in white and 'prilagojena vašemu podjetju' in red. A paragraph of text follows: 'Zmanjšajte tveganja, zaščitite uporabnike, Microsoft 365 okolje in poslovne podatke. Izberite raven varnosti, ki ustreza vašemu podjetju danes — in raste z vami tudi jutri.' At the bottom, there are two buttons: a red one labeled 'Zahtevajte ponudbo' and a white one with a red border labeled 'Oglejte si pakete'.

<https://ushield360.com>