VODIČ ZA SIGURNO KORIŠTENJE REGISTRA UNIJE

1. Uvod

Ovaj vodič je namijenjen svim korisnicima hrvatskog dijela Registra Unije i objašnjava sigurnosne mjere sustava. Nacionalni administrator hrvatskog dijela Registra Unije ulaže maksimalne napore kako bi se Registar Unije zaštitio od neovlaštenog pristupa. Korisnici također imaju ulogu u tom kontinuiranom procesu a ovaj vodič objašnjava kako koristiti Registar Unije na siguran način.

Proteklih godina zabilježene su krađe i pokušaji krađe emisijskih jedinica i njihovog korištenja u svrhu prijevare. Nacionalni administrator zajedno sa Europskom Komisijom čini sve kako bi spriječio kriminalne radnje. Ovaj vodič opisuje kako spriječiti zlonamjerno korištenje Vašeg računala i dobivanje neovlaštenog pristupa računima u Registru unije.

2. Minimalni sigurnosni zahtjevi

Preduvjet za korištenje Registra Unije je da korisnici ispunjavaju slijedeće minimalne sigurnosne zahtjeve:

2.1. Računala

Da bi se prijavili u Registar Unije, korisnici moraju koristiti računalo koje pruža njihova tvrtka ili vlastito računalo ako je to u skladu sa sigurnosnom politikom njihove tvrtke.

2.2. Ažuriranja softvera

Operativni sustav i drugi softver instaliran na računalu treba biti ažuriran s najnovijim sigurnosnim nadogradnjama.

2.3. Ograničenja administratorskih ovlasti

Administratorske račune na računalu trebaju koristiti pouzdane osobe i instalirati samo ovlaštene i pouzdane programe. Općenito, računalo treba biti zaštićeno koliko je to moguće.

Za spajanje na Registar Unije i Internet, korisnici moraju koristiti računalo na kojem se prijavljuju kao "Korisnik", a nikada kao "Administrator" računala.

Radnička cesta 80, 10000 Zagreb; Tel.: +385 1 4886 840, 5502 900; Fax: +385 1 4886 850; ghgregistry.admin@mingor.hr; https://mzoe.gov.hr i www.haop.hr

2.4. Antivirusni softver

Obveza je korisnika da redovito ažurira antivirusni softver i softver za vatrozid (eng. *firewall*), najmanje jednom tjedno.

Potpuno i dubinsko skeniranje za provjeru protiv virusa i zlonamjernih programa (*malware*) mora biti konfigurirano tako da se automatski izvodi najmanje svaka dva tjedna koristeći suvremeni antivirusni i anti-zlonamjerni softver.

2.5. Zaključavanje računala

Računala moraju imati konfiguriran čuvar zaslona (eng. *screensaver*) tako da se nakon više od 15 minuta neaktivnosti računalo zaključa. Mora se primjenjivati pravilo da se računalo ne ostavlja bez nadzora osiguravajući da se čuvar zaslona uvijek pokreće kada korisnik nije za svojim računalom.

Prije nego napustite računalo, uvijek se prvo odjavite ili zaključajte svoj profil kako mu nitko drugi ne bi mogao pristupiti dok ste odsutni.

2.6. Upravljanje prijenosnim medijima

Korisnici ne smiju priključivati nepoznate USB uređaje na svoje računalo.

Preporuča se konfiguriranje računala za deaktiviranje uporabe USB uređaja te da sustav zapisuje događaje povezivanja USB uređaja (eng. *event log*).

2.7. Popis pouzdanog softvera

Preporučljivo je definirati popis ovlaštenog softvera instaliranog na korisničkim računalima.

Preporučuje se da IT administratori osiguraju da nijedan drugi softver nije instaliran na korisničkom računalu.

Preporučuje se uklanjanje neovlaštenog softvera.

2.8. Pregledi i zapisi događaja

Vanjski pristup, događaji pristupa računalu moraju biti prijavljeni i analizirani od strane administratora. Za svaku anomaliju treba provesti temeljiti pregled.

Radnička cesta 80, 10000 Zagreb; Tel.: +385 1 4886 840, 5502 900; Fax: +385 1 4886 850; ghgregistry.admin@mingor.hr; https://mzoe.gov.hr i www.haop.hr

2.9. Sigurna internetska veza

Svaka upotreba Registra mora biti učinjena putem sigurne internetske veze.

Sigurna veza mora sadržavati zaštitu između interne mreže na kojem se nalazi korisničko računalo i Interneta, uključujući sustav za otkrivanje upada na razini mreže i računala i antivirusnu zaštitu.

Sigurna veza mora ograničiti pristup Internetu koristeći funkcije crnog popisa (eng. *blacklist*).

2.10. Obrazovanje korisnika

Korisnici moraju biti osposobljeni za korištenje Registra Unije i obrazovani u pitanjima informacijske sigurnosti.

Korisnici moraju izbjegavati dijeljenje računala kojima se prijavljuju u Registar Unije s drugim osobama.

Poveznice za pristup Registru Unije u e-mail porukama se ne smiju nikada otvarati.

Europska Komisija, Središnji administrator, Nacionalni administrator ili korisnička podrška nikad neće tražiti korisnike njihovu lozinku ili bilo kakav softver.

Nacionalni administrator šalje svu elektroničku poštu s adrese ghgregistry.admin@mingor.hr.

Korisnici ne smiju otvarati privitke e-mailova koji ne potječu od Nacionalnog administratora.

Ako korisnici imaju bilo kakav razlog za sumnju u porijeklo primljenih e-mail poruka, moraju odmah kontaktirati Nacionalnog administratora.

2.11. Konfiguracija računala

Računalo mora biti konfigurirano tako da se ne koristi funkcija "automatsko prijavljivanje". Nakon pokretanja operativnog sustava ili pokretanja softvera, uvijek se mora tražiti lozinka za prijavu.

Internet preglednik mora biti konfiguriran tako da ne pohranjuje korisničko ime i lozinku te da se svi privremeno pohranjeni podaci (kao što su povijest, lozinke, kolačići) automatski brišu prilikom zatvaranja preglednika.

Podizanje sustava sa CD/DVD ili USB uređaja treba biti onemogućeno (konfiguracijom BIOS-a). Korisnici ne smiju biti u mogućnosti pristupiti postavkama BIOS-a (zaključanog snažnom lozinkom i drugačijom od lozinke za prijavu).

Računala moraju biti konfigurirana tako da se na računalu koje se koristi za prijavu u Registar Unije ne mogu dijeliti datoteke s vanjskim korisnicima izvan organizacije korisnika (npr. pomoću softvera za dijeljenje datoteka kao što je BitTorrent).

Radnička cesta 80, 10000 Zagreb; Tel.: +385 1 4886 840, 5502 900; Fax: +385 1 4886 850; ghgregistry.admin@mingor.hr; https://mzoe.gov.hr i www.haop.hr

Računalo mora biti konfigurirano tako da se korisnik ne spaja na Internet s korisničkim računom administratora računala već sa korisničkim računom ograničenog (standardnog) korisnika.

Korisnici ne smiju imati mogućnost instaliranja softvera pomoću korisničkog računa s kojim se povezuju s Internetom i prijavljuju u Registar Unije.

2.12. Upotreba registra Unije

Lozinka za prijavu u Registar Unije je strogo osobna. Svaka radnja u Registru Unije izvedena s određenim korisničkim imenom i lozinkom smatra se izvedenom pod odgovornošću korisnika.

Svi ovlašteni korisnici Registra Unije moraju osigurati da korisnička imena, lozinke i SMS jednokratni kôdovi ne postanu poznati drugim osobama, uključujući ostale vlasnike računa u Registru Unije.

Nacionalni administratori ili Europska Komisija mogu tražiti od korisnika da komunicira svoje korisničko ime telefonom, ali niti Europska Komisija niti Nacionalni administratori nikada neće tražiti lozinku od krajnjih korisnika.

Da biste pristupili Internet stranici Registra, preporučuje se uvijek upisivanje adrese web stranice izravno u adresnu liniju preglednika. Za Registar Unije to je https://unionregistry.ec.europa.eu/euregistry/HR/index.xhtml. Ako korisnici ne upisuju adresu, svaki put kada se povežu, moraju provjeriti da je uspostavljena SSL veza (URL u adresnoj traci preglednika počinje sa "https" a ne "http") i da je SSL certifikat koji se pojavljuje kada kliknete na zaključavanje ikone preglednika izdan od strane "GlobalSign RSA OV SSL CA 2018" za URL "*.unionregistry.ec.europa.eu" (vidjeti poglavlje Sigurnost Internet stranica).

Kada napuštaju svoje računalo korisnici se moraju odjaviti iz Registra Unije kako neovlaštene osobe ne bi mogle pristupiti računu u Registru Unije.

Korisnici moraju poduzeti razumne mjere predostrožnosti kako bi spriječili neovlašteno korištenje mobilnih uređaja čiji brojevi se koriste za prijavu u Registar Unije.

Mobilni uređaj koji prima jednokratne SMS kôdove za prijavu u Registar Unije ne smije se istodobno upotrebljavati za transakcije na Internetu.

Radnička cesta 80, 10000 Zagreb; Tel.: +385 1 4886 840, 5502 900; Fax: +385 1 4886 850; ghgregistry.admin@mingor.hr; https://mzoe.gov.hr i www.haop.hr

3. Mjere sigurnosti za korištenje mobilnog telefona

Koristite samo broj Vašeg osobnog mobilnog telefona za prijavu u Registar. Dijeljenje broja mobilnog telefona s drugim osobama oslabljuje sigurnost Registra.

Postavite lozinku ili PIN kako biste osigurali svoj mobilni uređaj od neovlaštenog korištenja.

Ako se prijavljujte u Registar preko istog uređaja na koji primate SMS kôd postoji mogućnost otkrivanja korisničkog imena, lozinke, SMS kôda i kôda koji generira EU Login mobilna aplikacija drugim aplikacijama koje bi to mogle zloupotrijebiti.

Nikada nemojte dijeliti korisničko ime, lozinke, SMS kôdove i kôdove koje generira EU Login mobilna aplikacija s drugim osobama. Nacionalni administrator Vas nikada neće tražiti te podatke.

4. Sigurnost Internet stranica

Uvijek se prijavljujte u Registar putem Internet stranice Ministarstva gospodarstva i održivog razvoja.

Nikada nemojte otvarati poveznice sa drugih Internet stranica da biste se prijavili u Registar jer na taj način riskirate da otvorite lažnu stranicu te da svoje osobne podatke otkrijete trećim osobama.

Kako biste bili sigurni da radite u Registru na siguran način savjetujemo da uvijek poduzmete sljedeća dva koraka:

1. Provjerite URL Internet stranice. Adrese su:
    a) https://webgate.ec.europa.eu/cas/eim/external/register.cgi (EU Login)
    b) https://unionregistry.ec.europa.eu/euregistry/HR/index.xhtml (Registar Unije).
2. Provjerite SSL certifikat Internet stranice. Uputu kako to učiniti možete pronaći na sljedećoj stranici: https://www.globalsign.com/en/blog/how-to-view-ssl-certificate-details

U tablici ispod naći ćete podatke o SSL certifikatima korištenima za navedene Internet stranice. Ako podaci certifikata ne odgovaraju podacima u tablici, nipošto ne upisujte svoje korisničke podatke na toj stranici te hitno prijavite uočene nepravilnosti Nacionalnom administratoru.

Radnička cesta 80, 10000 Zagreb; Tel.: +385 1 4886 840, 5502 900; Fax: +385 1 4886 850; ghgregistry.admin@mingor.hr; https://mzoe.gov.hr i www.haop.hr

Internet stranica EU Login	Internet stranica Registra Unije
Izdavač certifikata: CN = GlobalSign Organization Validation CA - SHA256 - G2 O = GlobalSign nv-sa C = BE	Izdavač certifikata: CN = GlobalSign RSA OV SSL CA 2018 O = GlobalSign nv-sa C = BE
Subjekt certifikata: CN = *.ec.europa.eu O = European Commission L = Brussels S = Brussels-Capital Region C = BE	Subjekt certifikata: CN = *.unionregistry.ec.europa.eu O = European Commission L = Brussels S = Brussels-Capital Region C = BE

5. E-mail komunikacija

Sve e-mail poruke koje šalje Nacionalni administrator su digitalno potpisane S/MIME certifikatom.

Ako primite e-mail poslan od Nacionalnog administratora obavezno provjerite da li je to stvarni pošiljatelj e-maila na slijedeći način:

Kliknite na znak potpisa u e-mail poruci i zatim

1. kliknite na "Details",
2. kliknite na "View information",
3. kliknite na "Certification Path" i provjerite da li je subjekt certifikata isti kao e-mail adresa Nacionalnog administratora (E = ghgregistry.admin@mingor.hr)

Kako bi ste neometano primali e-mail poruke od Nacionalnog administratora, Registra Unije i EU Login-a, dodajte ih u svom e-mail programu na popis sigurnih pošiljatelja (*safe senders*).

Radnička cesta 80, 10000 Zagreb; Tel.: +385 1 4886 840, 5502 900; Fax: +385 1 4886 850; ghgregistry.admin@mingor.hr; https://mzoe.gov.hr i www.haop.hr

6. Lozinka

Za pristup računalu i Registru Unije uvijek koristite jaku lozinku.
Jaka lozinka mora zadovoljiti slijedeće uvjete:

- mora biti duga najmanje deset znakova,
- mora sadržavati:
  - barem jedno veliko slovo
  - barem jedno malo slovo
  - barem jednu brojku
  - barem jedan specijalni znak

Ne koristite lozinke koje netko drugi može lako otkriti ili pogoditi (kao što je npr. ime kućnog ljubimca ili datumi rođendana) te ne koristite istu lozinku za različite aplikacije. Nikad nemojte spremati lozinke na isto mjesto gdje i korisnička imena. Također nikad ih nemojte spremati u nezaštićene datoteke na računalu. Ne dozvolite da druge osobe gledaju u Vaš ekran dok upisujete svoje korisničko ime i lozinku.

Preporuke za odabir lozinke možete pronaći na poveznici:
https://www.microsoft.com/en-us/research/publication/password-guidance/

7. Dodatne mjere

Ako je računalo koje koristite dio tvrtkine mreže njegova sigurnost spada u nadležnost IT administratora. Osim prethodno navedenih mjera ne preostaje još puno što možete učiniti kako biste bolje zaštitili svoje računalo. Ipak, možete proslijediti ovaj vodič svojim IT administratorima da ju pročitaju (naročito poglavlje 2. Minimalni sigurnosni zahtjevi) i osiguraju da Vaša računalna mreža bude odgovarajuće zaštićena.

8. Služba za podršku korisnicima Registra Unije

Adresa:

Ministarstvo gospodarstva i održivog razvoja
Radnička cesta 80
10 000 Zagreb
Hrvatska

E-mail: ghgregistry.admin@mingor.hr

Telefon: +385 1 5581 660

Radno vrijeme: radnim danom od 09:00 do 15:00h po srednjeeuropskom vremenu

9. Ograničenje odgovornosti

Sadržaj ovog vodiča ne podliježe nikakvim pravima i Ministarstvo gospodarstva i održivog razvoja nije odgovorno za bilo koje aktivnosti na Vašem računalu.

Radnička cesta 80, 10000 Zagreb; Tel.: +385 1 4886 840, 5502 900; Fax: +385 1 4886 850; ghgregistry.admin@mingor.hr; https://mzoe.gov.hr i www.haop.hr