Informacijska varnost in delo od doma

Matej Kovačič
https://telefoncek.si

Delo od doma

Prednosti:

- fleksibilnejše,
- omogoča večjo samoorganizacijo in večjo samostojnost zaposlenih,
- stroškovno učinkoviteje,
- ima lahko višjo produktivnost.

Slabosti:

- pomisleki glede nadzora nad opravljenim delom,
- strah, da bo kakovost opravljenega dela slabša,
- vprašanje pripadnosti zaposlenih, občutek povezanosti,
- usklajevanje dela in zasebnega življenja pri zaposlenih.

Smiselnost uvedbe odvisna od tipa organizacije.

Tehnološki izzivi

Tehnološki izzivi dela od doma/na daljavo:

- infrastruktura v organizaciji (oddaljeni dostopi, videokonferenčni sistemi,...),
- infrastruktura pri zaposlenih (strojna in programska oprema),
- oddaljeno vzdrževanje,
- varnost terminalne opreme.

Uporaba oblačnih storitev ali lastne infrastrukture?

Pri delu od doma morajo zaposleni imeti ustrezen nabor veščin, ne smemo pa pozabiti na trening.

Razpoložljivost

Razpoložljivost zagotavlja zanesljiv in pravočasen dostop do informacijskega sistema, ko ga uporabniki potrebujejo.

Zanesljiv in razpoložljiv informacijski sistem v organizaciji predstavlja temelj za nemoteno izvajanje delovnih in poslovnih procesov in ima zato ključno vlogo pri učinkovitosti poslovanja.

V primeru izrednih razmer mora biti informacijski sistem zasnovan tako, da bo razpoložljiv ne samo znotraj organizacije, pač pa tudi oddaljeno.

Delo na daljavo

Digitalizacija poslovanja in delo na daljavo niso možni v vseh gospodarskih panogah v enaki meri.

Kjer pa je to mogoče, pa je priprava na to smiselna.

Spremembe je treba uvajati premišljeno in sistematično.

1. Priprava ustrezne infrastrukture na strani organizacije.
2. Zagotovitev podpore delu na daljavo pri zaposlenih.
3. Izobraževanje zaposlenih.
4. Občasno izvajanje dela na domu/na daljavo (trening).

Poseben poudarek na zagotavljanju varnosti.

S tem bo organizacija bolje pripravljena na potencialno krizo, kar pa je bistvenega pomena za preživetje v primeru izrednih dogodkov.

Infrastruktura v podjetju

Oddaljeni dostop:

- VPN

Orodja za oddaljeno sodelovanje.

- koledarji in dodeljevanje nalog,
- deljenje datotek,
- upravljanje dokumentov.

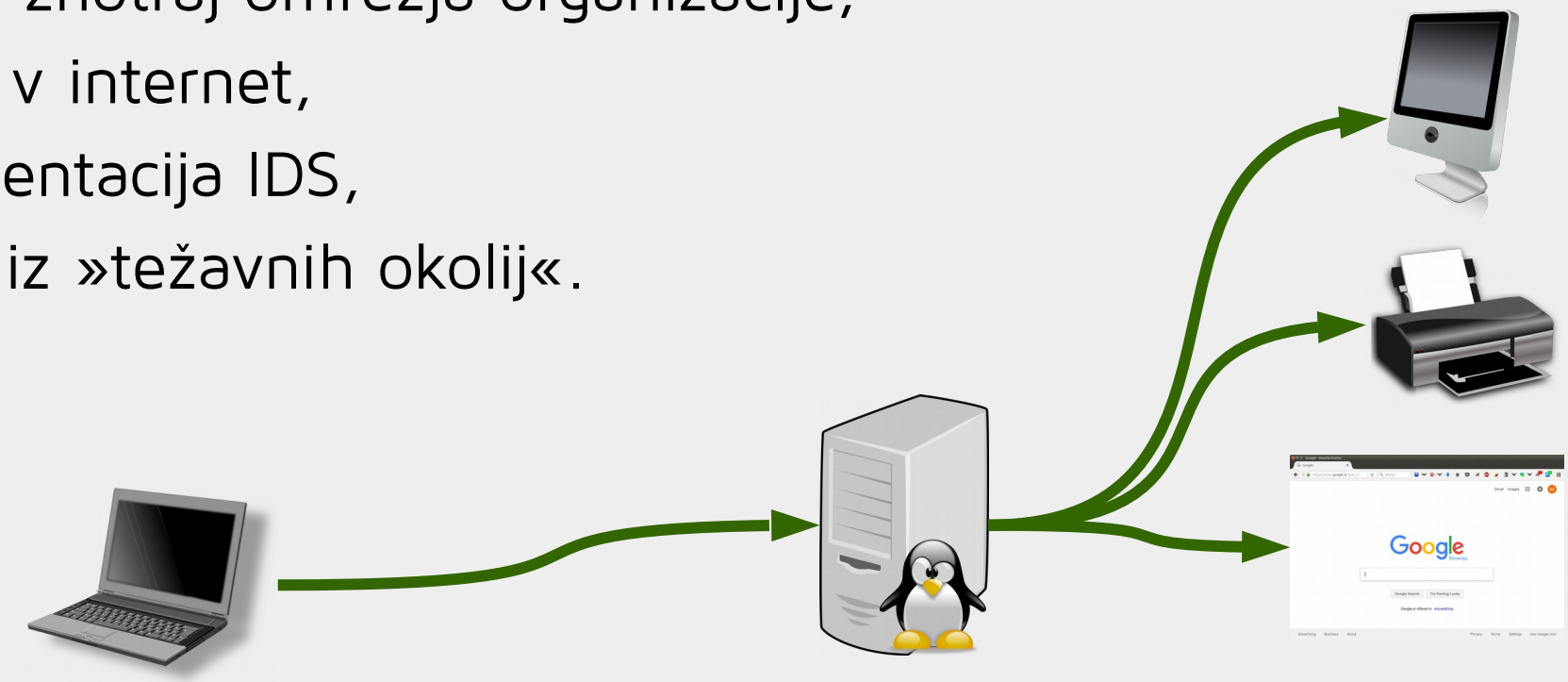
Orodja za oddaljeno komunikacijo:

- e-pošta,
- hipno sporočanje,
- videokonferenčni sistemi.

VPN

VPN omogoča povezavo računalnika ali omrežja z oddaljenim omrežjem, običajno preko šifriranega tunela.

- storitve znotraj omrežja organizacije,
- prehod v internet,
- implementacija IDS,
- dostop iz »težavnih okolij«.



Varnost e-pošte

Poštni strežnik:

- varnostni protokoli za preverjanje pristnosti e-pošte (SPF - Sender Policy Framework, DKIM - DomainKeys Identified Mail in DMARC - Domain-based Message Authentication, Reporting & Conformance),
- strežniški diski so šifrirani,
- protivirusni in protismetni filtri,
- podpora šifriranim protokolom (POP3s/IMAPs/SMTPs).

Poštni odjemalci:

- šifriranje e-pošte (GPG),
- dvofaktorska avtentikacija (Yubikey,...).

Videokonferenčni sistemi

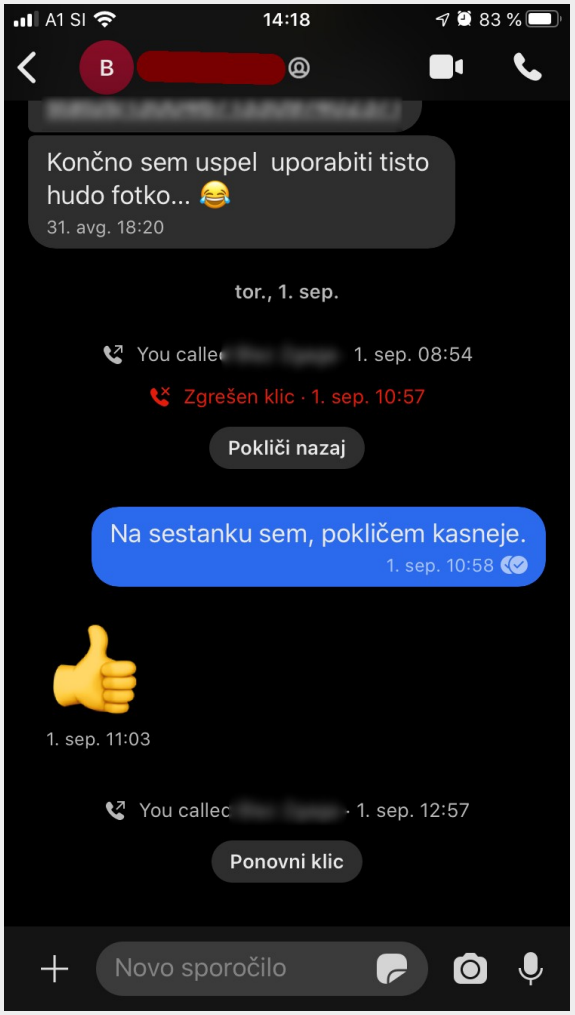
Strojna in programska oprema, pasovna širina.

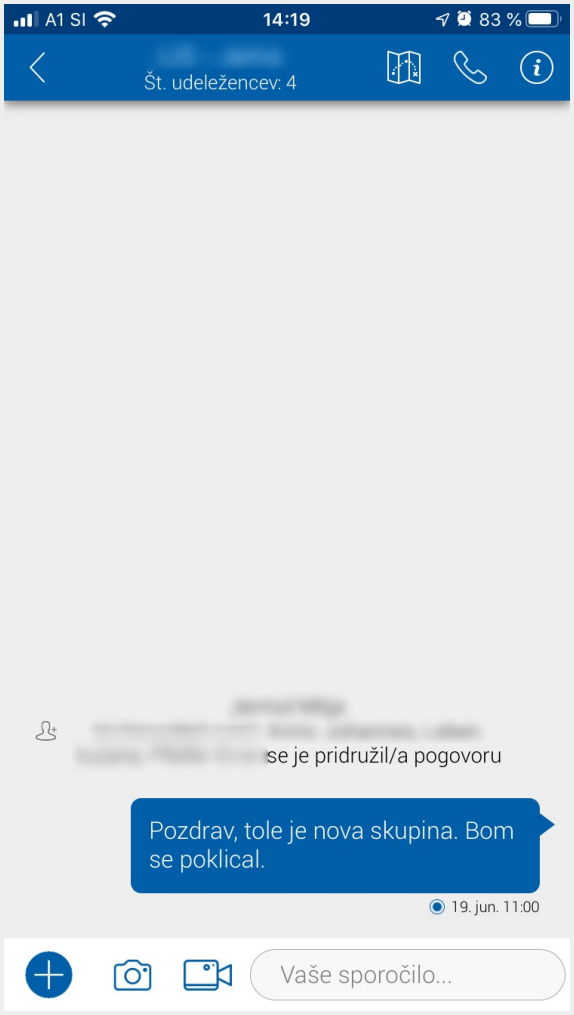
Videokonferenčni sistemi vs. webinarji.

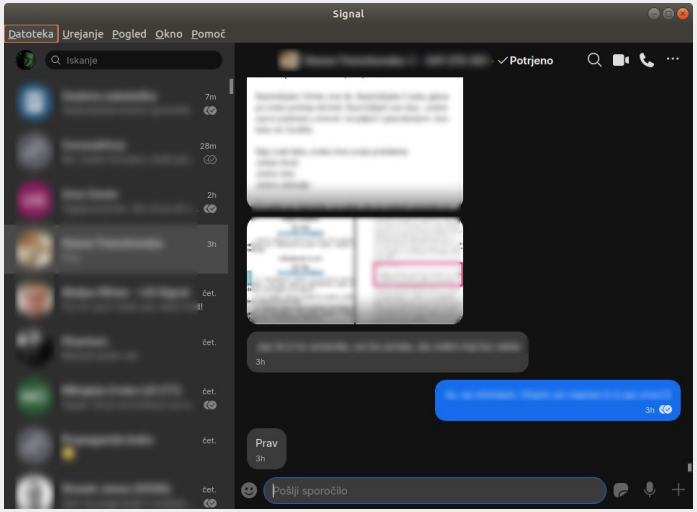
Nekatere rešitve omogočajo šifriranje od začetne do končne točke (t. i. E2E – end-to-end šifriranje).

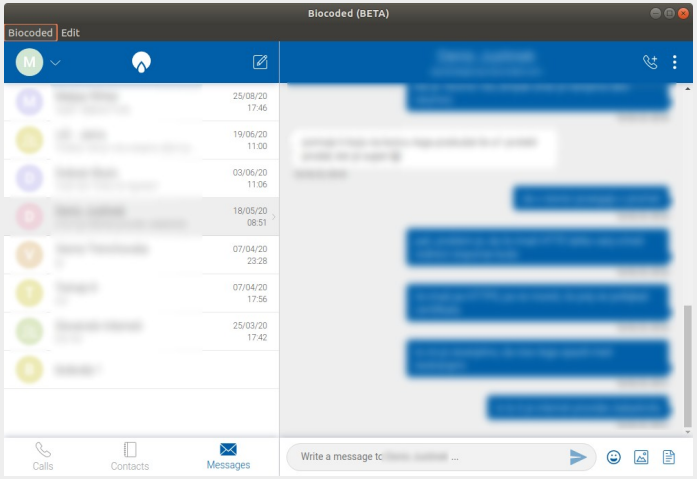
Nekatere rešitve tečejo v spletnem brskalniku (ne zahtevajo nameščanja posebne programske opreme).

Varno hipno sporočanje









E2E: Signal in Biocoded.

Infrastruktura pri zaposlenih

Ustrezna strojna in programska oprema.

Bo v primeru krize mogoče kupiti potrebno strojno opremo?

- električni razdelilci,
- omrežni in drugi kabli, razni pretvorniki,
- slušalke z mikrofonom, spletna kamera,
- WiFi, BT, ethernet vmesniki,
- rezervna miška, tipkovnica,...

Zmogljivost internetne povezave?

Infrastruktura pri zaposlenih

Zagotavljanje varnosti in zagotavljanje vzdrževanja.

BYOD: da ali ne?

Organizacija naj opravi ustrezno presojo varnosti: opredeliti in analizirati tveganja, zagotoviti postopke in ukrepe za zagotavljanje varnosti.

Na napravah v lasti zaposlenih organizacija ne more vsiljevati preveč strogih varnostnih politik, saj bi to lahko pomenilo prevelik poseg v zasebnost uporabnikov oziroma zaposlene celo motiviralo k iskanju bližnjic.

Zato je pomembno izobraževanje uporabnikov.

Informacijska pismenost.

Varnost ni izdelek

Varnost ni izdelek oziroma nekaj, kar lahko kupimo, namestimo in pozabimo, pač pa gre za proces.

Varnostno kulturo je treba razvijati in gojiti neprestano.

Informacijska varnost in varnost v prometu: ni dovolj samo dober avto in opravljen izpit, znanje o varnosti je potrebno obnavljati in uporabljati neprestano.

Izobraževanje zaposlenih!

Fizični dostop do sistema

Nepooblaščeni dostop do podatkov.

Podtikanje prikritih mehanizmov za oddaljeni dostop ali krajo šifriranih podatkov (npr. programske aplikacije ali strojni dodatki).

Zavržene/**izgubljene** računalniške komponente, ki vsebujejo nosilce podatkov (trdi diski, tiskalniki, mobilni telefoni,...).

Nameščanje aplikacij z »dvojno funkcijo« (igre...).

Priklapljanje neznanih naprav na sistem (najdeni USB ključki, »polnjenje« mobilnih telefonov,...)

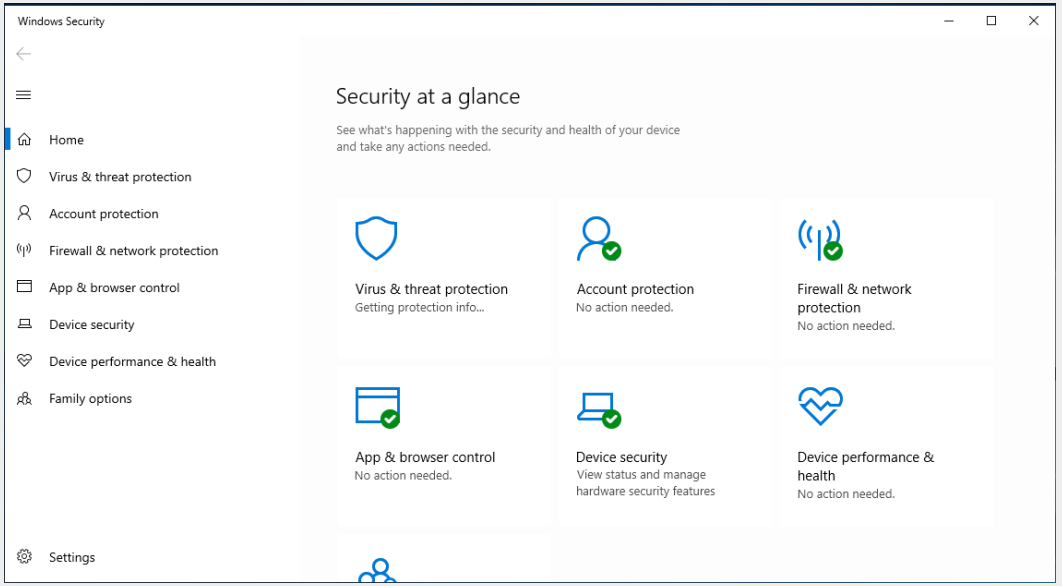
Večuporabniška okolja (eskalacija privilegijev).

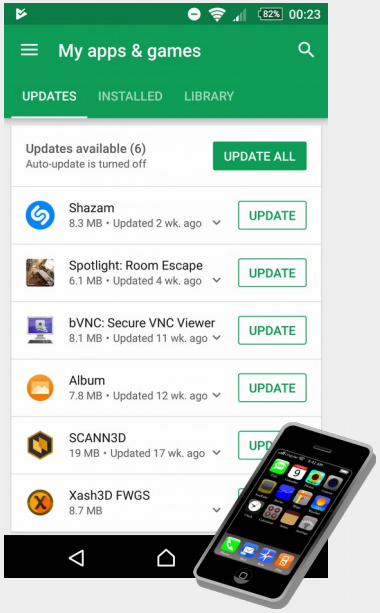
Osnovna zaščita

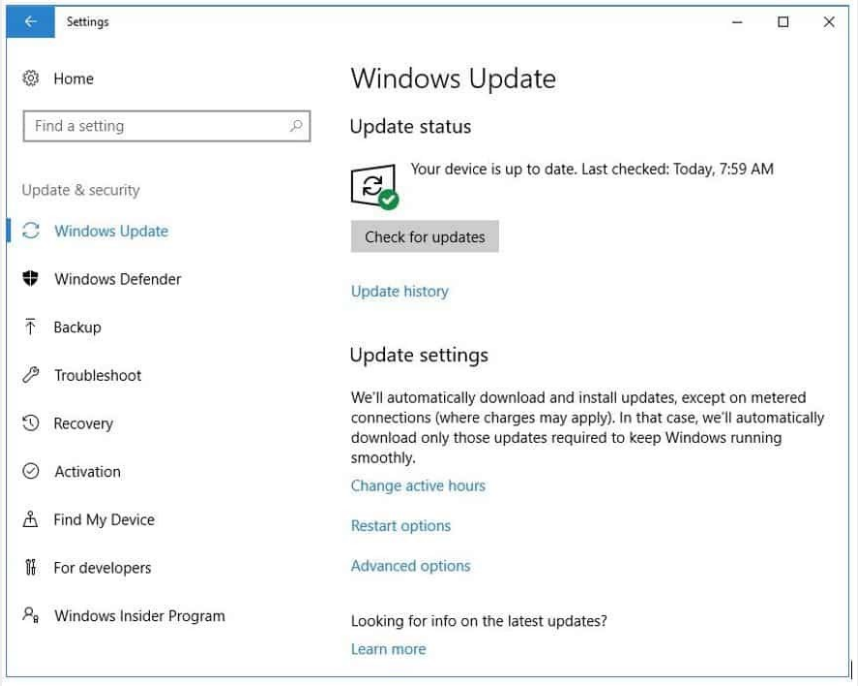
Nekatere tehnike osnovne zaščite računalniških sistemov:

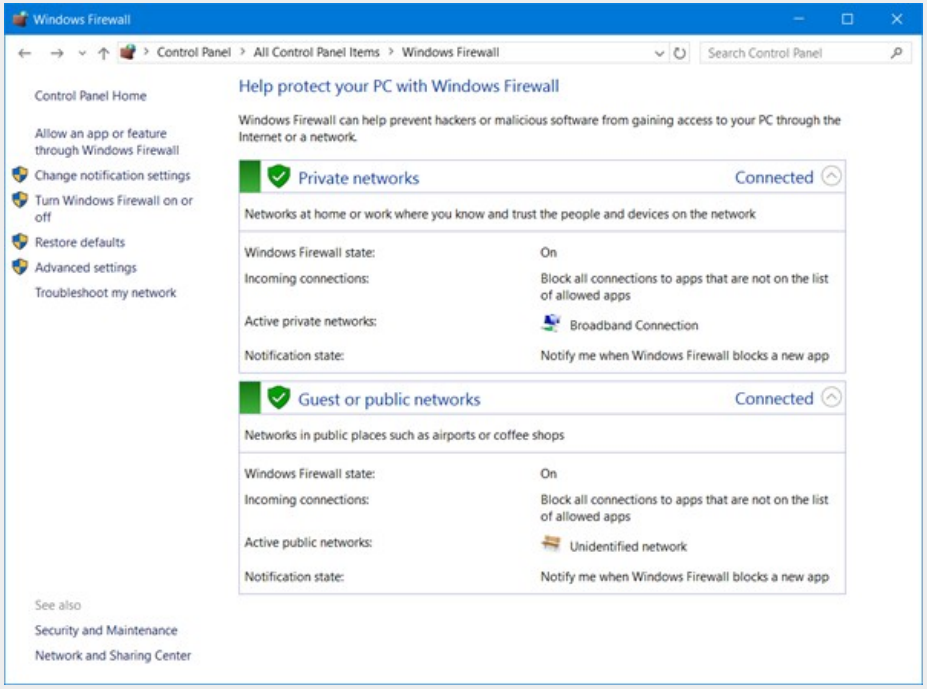
- uporaba ustreznih gesel;
- pazljivost pri večuporabniških sistemih;
- redno posodobljen sistem;
- požarni zid;
- uporaba protivirusnih in protismetnih programov;
- varnostno arhiviranje;
- ustrezna varnostna kultura;
- nameščanje samo tistih aplikacij, ki jih res potrebujemo;
- fizična varnost.

Osnovna zaščita









Gesla

Pravilo:

- čim daljše
- čim bolj kompleksno (mešanica črk in številk, po možnosti tudi mešanica velikih in malih črk ter številk)

Kako pomembno je posamezno geslo (za kaj ga uporabljamo)?

Gesla morajo biti med seboj (dovolj) različna.

Gesel ne »reciklirajmo«.

Geslo, za katerega sumimo, da je bilo zlorabljeno je potrebno **takoj spremeniti**.

Gesla...

Vir: Schneier.com, <http://www.schneier.com/blog/archives/2009/07/information_lea_1.html>.

Pri 4-mestnem geslu je vseh možnih kombinacij 10.000. V zgornjem primeru je možnih kombinacij samo še 24. Levo geslo je najbolj verjetno 1986 ali 1968, desno pa 1234.

Gesla

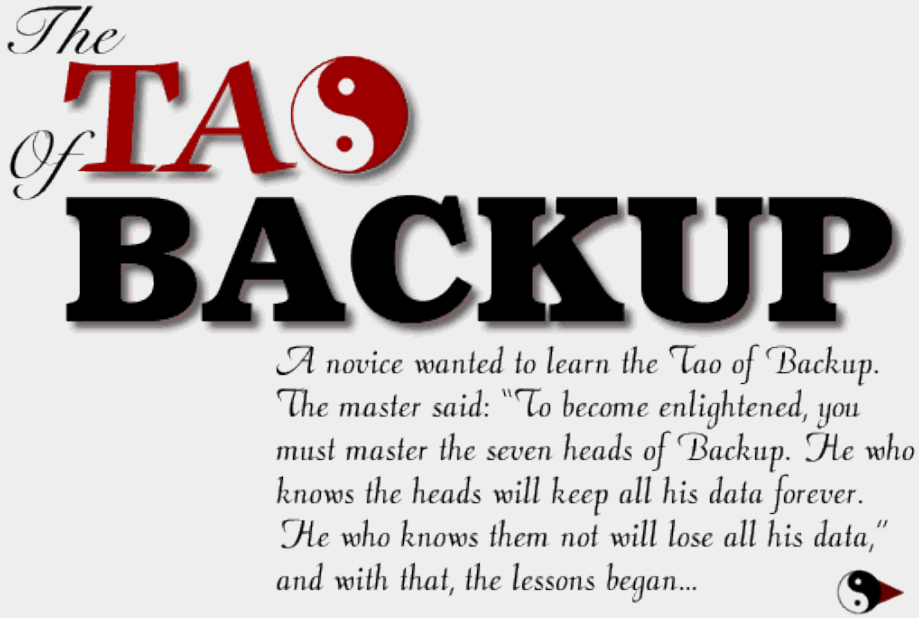
Enkratna gesla (OTP).

“Biometrična gesla”: biometričnih parametrov ni mogoče zamenjati oziroma preklicati, ponarejanje prstnih odtisov,...

Identiteta (“Kdo si?”) in avtentikacija (“Kako lahko to dokažeš?”) uporabnika morata ostaneta ločeni, kar pa pri uporabi biometričnih gesel ne velja.

Uporaba 2FA in MFA.

Varnostne kopije



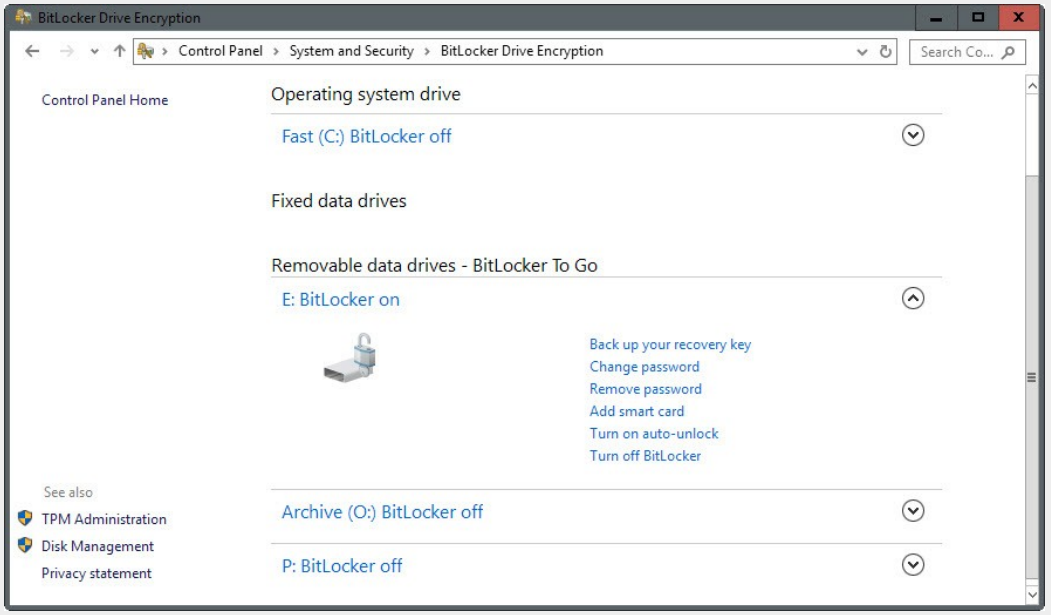
- uporaba (šifriranih?) oblačnih storitev (+/- dosegljivost,...);
- uporaba lokalnega NAS strežnika;
- arhiviranje samo pomembnih datotek;
- arhiviranje celotnega sistema (+ načrt okrevanja po katastrofi?);
- inkrementalne varnostne kopije.

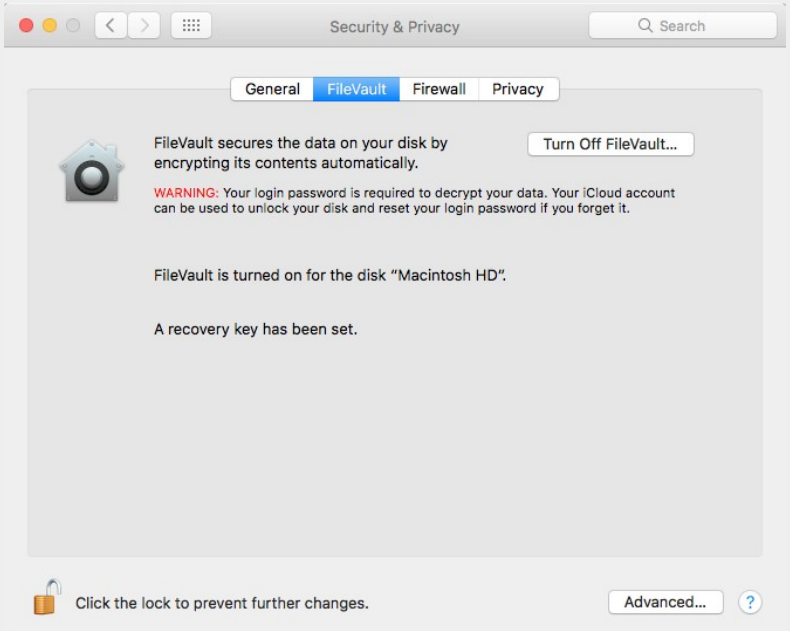
Naprednejša zaščita

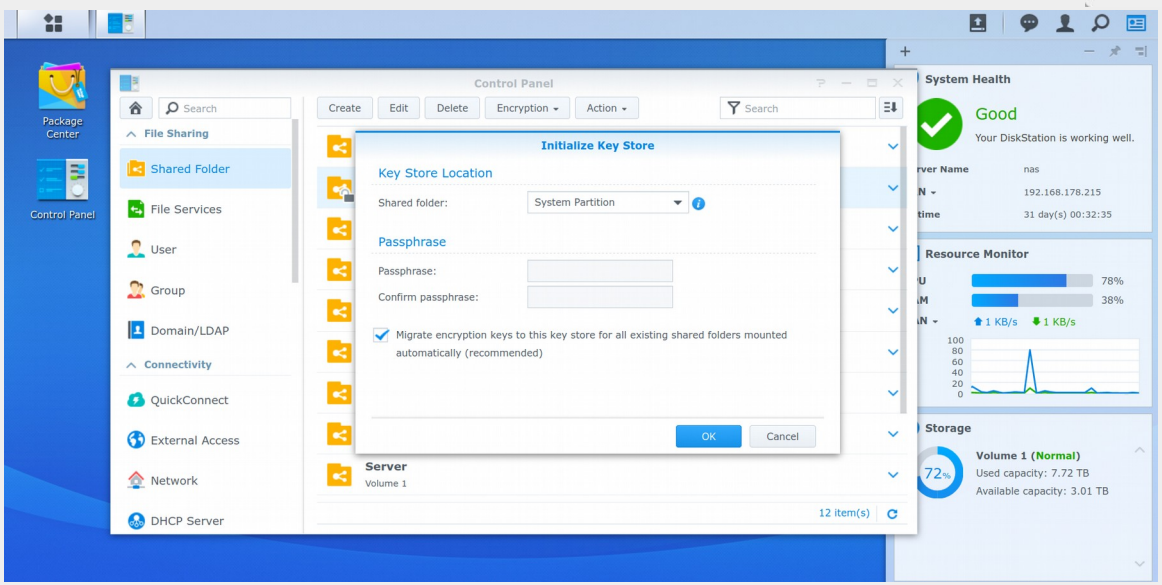
Nekatere tehnike naprednejše zaščite:

- **šifriranje** (*preprečimo dostop do vsebine*):
  - šifriranje nosilcev podatkov,
  - šifriranje elektronske pošte, neposrednih/hipnih sporočil, govorne in video komunikacije,
  - uporaba šifriranih povezav in protokolov (HTTPS,...),
- **trajno brisanje podatkov**,
- **anonimizacija** uporabe interneta (*preprečimo analizo prometnih podatkov*):
  - anonimizacijska omrežja,
  - "remailerji",
- **VPN**

Šifriranje nosilcev podatkov







Dodatne aplikacije

Dodatki za brskalnik:

- HTTPS Everywhere,
- odstranjevalci spletnih tehnologij za sledenje (angl. *online trackers*): Ghostery, Privacy Badger, Adblock Plus, uBlock Origin,...),
- NoScript.

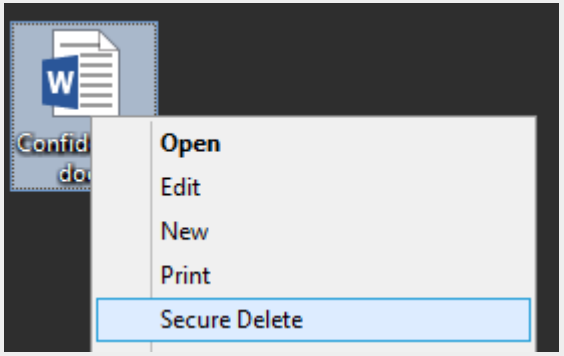
Odstranjevalci »nesnage« (BleachBit, CCleaner,...).

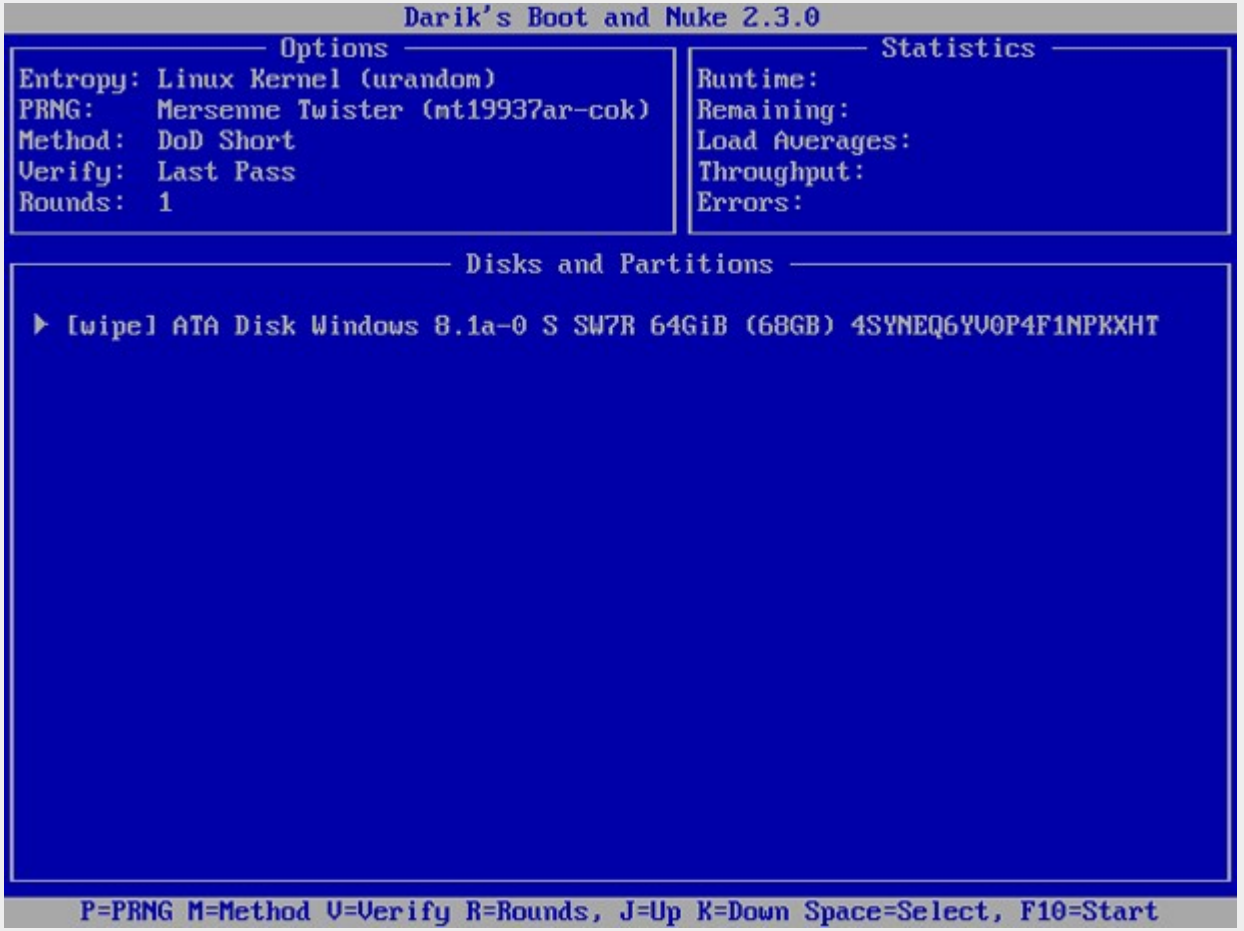
Blokada Windows telemetrije (Blackbird, WPD,... PiHole?).

Upravljavci gesel ((angl. *password manager*): Keepass, Lastpass, Bitwarden, Lesspass...).

Priporočljivo je, da so varnostni dodatki odprtokodni.

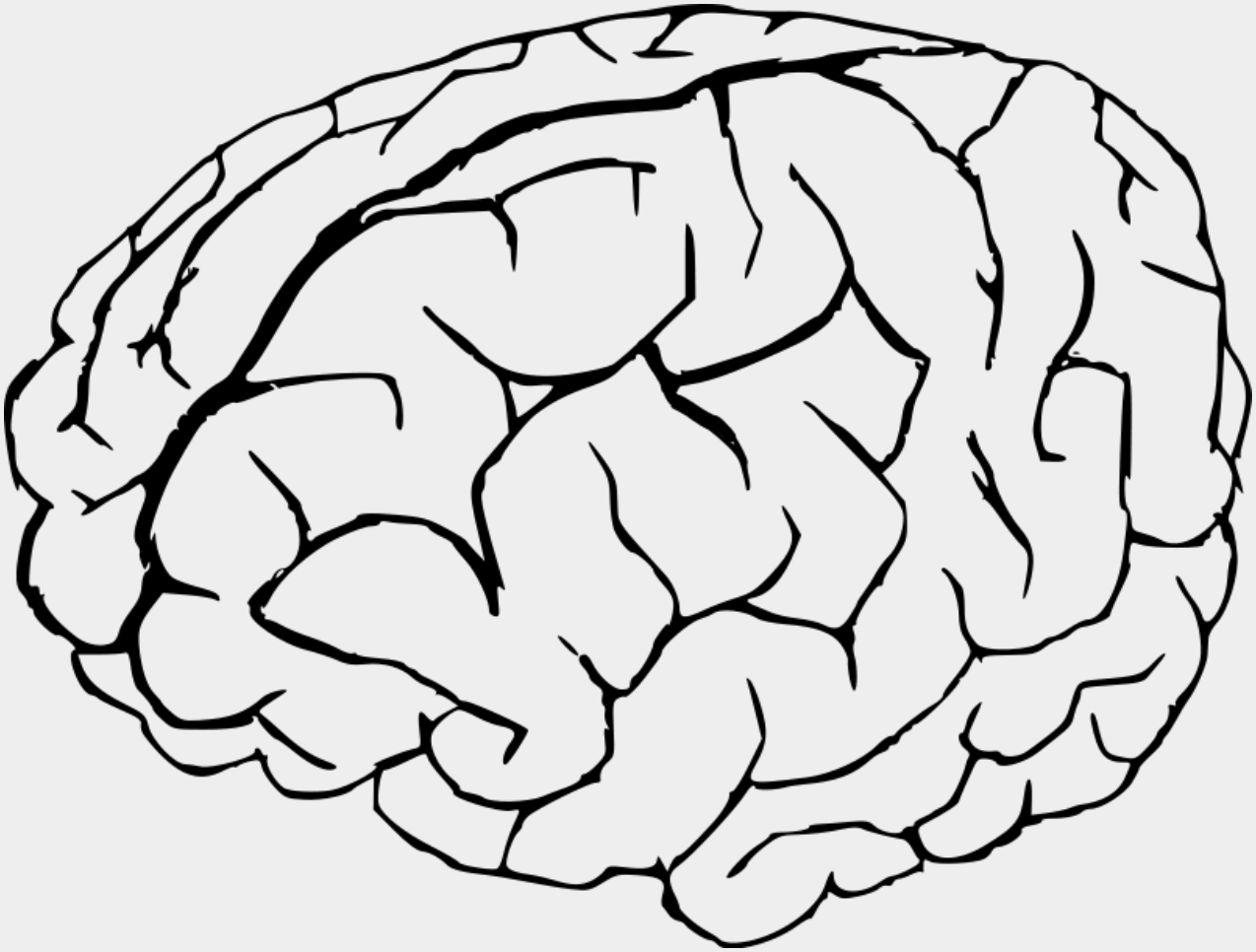
Trajno brisanje podatktov





Še bolj napredna zaščita

Nekaj znanja, doslednosti in zdrava pamet. ;-)



Primer phishing napada

```
From: Greg Hoglund <greg@hbgary.com> ISun, Feb 6, 2011 at
1:59 PM
To: jussi <jussij@gmail.com>

im in europe and need to ssh into the server. can you drop
open up firewall and allow ssh through port 59022 or
something vague?
and is our root password still 88j4bb3rw0cky88 or did we
change to 88Scr3am3r88 ?
thanks
```

```
From: jussi jaakonaho <jussij@gmail.com> ISun, Feb 6, 2011
at 2:06 PM
To: Greg Hoglund <greg@hbgary.com>

hi, do you have public ip? or should i just drop fw?
and it is w0cky - tho no remote root access allowed
```

```
From: Greg Hoglund <greg@hbgary.com> ISun, Feb 6, 2011 at
2:08 PM
To: jussi jaakonaho <jussij@gmail.com>

no i dont have the public ip with me at the moment because
im ready for a small meeting and im in a rush.
if anything just reset my password to changeme123 and give
me public ip and ill ssh in and reset my pw.
```

```
From: jussi jaakonaho <jussij@gmail.com> ISun, Feb 6, 2011
at 2:10 PM
To: Greg Hoglund <greg@hbgary.com>

ok,
takes couple mins, i will mail you when ready. ssh runs on
47152
```

Napad na informacijsko-varnostno podjetje HBGary (podjetje je za ameriško vlado izvajalo "napade" proti skupini Anonymous).

```
...a little later:

bash-3.2# ssh hoglund@65.74.181.141 -p 47152
[unauthorized access prohibited]
hoglund@65.74.181.141's password:
[hoglund@www hoglund]$ unset
[hoglund@www hoglund]$ unset HIST
[hoglund@www hoglund]$ unset HISTFLE
[hoglund@www hoglund]$ unset HISTFILE
[hoglund@www hoglund]$ uname -a;hostname
Linux www.rootkit.com 2.4.21-40.ELsmp #1 SMP
Wed Mar 15 14:21:45 EST 2006 i686 i686 i386
GNU/Linux
www.rootkit.com
[hoglund@www hoglund]$ su -
Password:
[root@www root]# unset HIST
[root@www root]# unset HISTFILE
[root@www root]# uname -a;hostname;id
Linux www.rootkit.com 2.4.21-40.ELsmp #1 SMP
Wed Mar 15 14:21:45 EST 2006 i686 i686 i386
GNU/Linux
www.rootkit.com
uid=0(root) gid=0(root)
groups=0(root),1200(varmistus
```

Varnost mobilnih komunikacij

Zaključek

Digitalizacija poslovanja in delo na daljavo niso možni v vseh gospodarskih panogah v enaki meri.

Kjer pa je to mogoče, pa je priprava na to smiselna.

Spremembe je treba uvajati premišljeno in sistematično.

1. Priprava ustrezne infrastrukture na strani organizacije.
2. Zagotovitev podpore delu na daljavo pri zaposlenih.
3. Izobraževanje zaposlenih.
4. Občasno izvajanje dela na domu/na daljavo (trening).

S tem bo organizacija bolje pripravljena na potencialno krizo, kar pa je bistvenega pomena za preživetje v primeru izrednih dogodkov.


Vprašanja?
https://telefoncek.si