UNIVERZA NA PRIMORSKEM
FAKULTETA ZA MATEMATIKO, NARAVOSLOVJE IN
INFORMACIJSKE TEHNOLOGIJE

Zaključna naloga

Zaščita podatkov pred krajo z uporabo enkripcije

(Data theft protection with the use of encryption)

Ime in priimek: Marko Poljanšek
Študijski program: Računalništvo in informatika
Mentor: doc. dr. Jernej Vičič
Somentor: doc. dr. Matjaž Kljun

Koper, julij 2016

Ključna dokumentacijska informacija

Ime in PRIIMEK: Marko POLJANŠEK

Naslov zaključne naloge: Zaščita podatkov pred krajo z uporabo enkripcije

Kraj: Koper

Leto: 2016

Število listov: 38 Število slik: 8 Število tabel: 6

Število referenc: 15

Mentor: doc. dr. Jernej Vičič

Somentor: doc. dr. Matjaž Kljun

Ključne besede: Enkripcija, BitLocker, Enkripcija celotnega diska, Prenosni računalnik, Prenosna naprava

Izvleček: Zaključna naloga opisuje problem varovanja podatkov pred krajo naprav. Naloga se osredotoči na varovanje teh podatkov s pomočjo enkripcije, zato je večji del naloge namenjen opisu različnih vrst ter tehnologij enkripcij podatkov. Naloga se osredotoča na varovanje shranjenih podatkov. V nalogi je tudi opisan postopek postavitve enkripcije BitLocker v podjetju, opisano je izbiranje sistema, testiranje in ugotovitve, prednosti ter slabosti končne postavitve.

Key words documentation

Name and SURNAME: Marko POLJANŠEK

Title of the final project paper: Data theft protection with the use of encryption

Place: Koper

Year: 2016

Number of pages: 38 Number of figures: 8 Number of tables: 6

Number of references: 15

Mentor: Assist. Prof. Jernej Vičič, PhD

Comentor: Assist. Prof. Matjaž Kljun, PhD

Keywords: Encryption, BitLocker, Full Disk Encryption, Laptop, Portable device

Abstract: The thesis describes the problem of protecting data from theft when device is stolen or lost. Focus is on the protection of such data by using encryption so the greater part of the thesis describes the different types of technologies of data encryption. Thesis focuses on the protection of stored data. The thesis also describes the process of installing the BitLocker encryption in the company, described is the selection of FDE product, testing and installation.

Zahvala

Zahvaljujem se mentorju, doc. dr. Jerneju Vičiču, za strokovno pomoč in sodelovanje pri izdelavi zaključne naloge. Zahvala gre tudi podjetju, Intesa SanPaolo Card d.o.o. za pomoč pri postavitvi enkripcije BitLocker ter dokumentacijo.

Kazalo vsebine

Kazalo tabel

Kazalo slik

Kazalo prilog

Seznam kratic

USB	Universal Serial Bus
BYOD	Bring Your Own Device
FDE	Full Disk Encryption
MBR	Master Boot Record
OS	Operating System
PBE	Pre-Boot Environment
PKI	Public Key Infrastructure
AD	Active Directory
LAN	Local Area Network
CD	Compact Disk
DVD	Digital Versatile Disc
SSO	Single Sign On
BSD	Berkeley Software Distribution
PGP	Pretty Good Privacy
AES	Advanced Encryption Standard
CLI	Command-Line Interface
GUI	Graphical User Interface
IT	Information Technology
MDM	Mobile Device Management
GPO	Group Policy Object
TPM	Trusted Platform Module
HDD	Hard Disc Drive
SSD	Solid-State Drive
OU	Organization Unit
SO	Security Office

1 Uvod

V današnji informacijski dobi se vsak dan srečujemo z različnimi vrstami hranjenja ter pošiljanja podatkov, ki se vedno manj hranijo v fizični (papirnati) obliki. Zaradi lažjega prenašanja, pošiljanja ter hranjenja, se jih shranjuje na različne digitalne medije, kateri so: ključki USB, trdi diski, mobilni telefoni, stacionarni in prenosni računalniki ter druge podobne naprave. Ker na te naprave lahko shranjujemo ogromno količino podatkov, to lahko posledično privede do rizičnih situacij, da ti podatki zaidejo v napačne roke, v primeru izgube ali kraje naprave. Da se zavarujemo pred tem, lahko uporabimo različne vrste enkripcije.

Enkripcija ali šifriranje podatkov je postopek pretvorbe podatkov s pomočjo kriptografskega algoritma ter ključa v tako obliko, da ga praviloma nepooblaščene osebe ne morejo razumeti [9].

Danes se uporabljajo simetrični in asimetrični enkripcijski algoritmi. Pri simetričnih algoritmih imata pošiljetelj in prejemnik skupen ključ, ki je poznan samo njima. Pri asimetričnih algoritmih pa obstajata javni ter zasebni ključ. Z javnim ključem lahko vsakdo zakriptira sporočilo ter ga pošlje prejemniku, ki ima zasebni ključ, s katerim je možno sporočilo dekriptirati. Tako ima možnost prebrati sporočilo le tista oseba, ki je lastnik zasebnega ključa. Na takšen način deluje enkripcija s certifikati.

Enkripcijo v večini primerov uporabljamo za namen komunikacije, da v primeru, če nekdo prisluškuje liniji, ne more razbrati sporočila, ki se trenutno pošilja. Za podatke, ki se shranjujejo na diskih ter prenosnih napravah, uporabljamo enkripcijske metode, namenjene za varno hranjenje podatkov.

Poleg vseh teh rizikov izgube podatkov, se zadnja leta pojavlja še tako imenovan fenomen BYOD (ang. Bring Your Own Device), kar pomeni, da delavci v podjetjih, za delo ter prenašanje podatkov, uporabljajo svoje osebne naprave. Kot vse novosti, ima tudi ta veliko prednosti ter slabosti, zato morajo podjetja dobro preštudirati ali prednosti pretehtajo ali ne.

Prednosti BYOD:

- Znižuje stroške podjetja pri nakupu naprav [2];
- Zvišuje produktivnost, saj delavci uporabljajo naprave, ki so jih vajeni [11];
- Višje zadovoljstvo delavcev, ker si lahko napravo izberejo sami [11].

Slabosti BYOD:

- Večja verjetnost, da informacije zaidejo v napačne roke [11];
- Težji nadzor nad napravami, kjer se hranijo podatki podjetja;
- Potrebno investirati v dodatno zaščito podatkov, s pomočjo ločenega okolja na napravah.

Medtem, ko BYOD pristop zveni privlačno, morajo podjetja dodatno upoštevati vse posledice, ki jih prinese omogočanje dostopa do poslovnih podatkov na osebnih napravah, nad katere nimajo, oziroma imajo zelo majhen nadzor. Čeprav se veliko delavcev počuti boljše, če lahko za delo uporabljajo svoje naprave, na katere so navajeni, večina ni naklonjenih k temu, da podjetje te naprave nadzira ter posledično dostopa do njihovih osebnih podatkov.

Za reševanje teh problemov imajo podjetja na voljo več rešitev:

- Postavljeno varno okolje, do katerega delavci dostopajo z dodatno avtentikacijo;
- Podatke varovati na kriptiranem virtualnem disk-u, za katerega potrebujemo dodatno avtentikacije, če želimo dostopati do podatkov.

2 Motivacija

2.1 Kensingtonova Študija

Kensigtonova študija prikazuje stroške, ki so nastali zaradi izgube ali kraje prenosnih naprav. V študijo so bile vključene naslednje naprave: prenosni računalniki, tablice ter mobilni telefoni. Ugotovljeno je bilo, da so stroški, zaradi izgube podatkov, večji od cene naprav. V večini primerov so nastali zaradi: zlorabe podatkov, ki so jih uporabili za pridobitev dostopov do sistemov podjetij, izsiljevanja ter sodb. Z izgubo ali krajo enega prenosnega računalnika povprečni strošek znaša več, kot $49.000, kar je za nekatere pogubno [4].

Statistični podatki kažejo, da se/je:

- vsakih 53 sekund izgubi 1 prenosni računalnik [4];
- vsako leto izgubi, v poprečju 70 milijonov mobilnih telefonov, s tem, da jih je le 7% najdenih [4];
- na leto izgubi 4,3% mobilnih telefonov, ki so v lasti podjetij [4];
- 80% stroškov izgubljenega prenosnega računalnika izvira iz izgubljenih podatkov [4];
- 52% prenosnih naprav ukradenih iz pisarn ali drugih delovnih mest ter 24% iz konferenc [4].

Pri majhnih ter srednje velikih podjetjih ugotovitve kažejo, da v večini ta nimajo nastavljene pravilne varnostne politike ali pa je ne uveljavljajo po pravilnem postopku. Podjetjem, ki so okrevala po vdorih, je l. 2010, njihov strošek, v povprečju, znašal $7.2 milijona, kar je posledično privedlo do propada nekaterih podjetij. Podjetja se morajo pred tem obvarovati, izučiti svoje delavce ter postaviti močno varnostno politiko in en del izmed navedenega, predstavlja enkripcija vseh podatkov v prenosnih napravah [4].

2.2 Študija Inštituta Ponemon

Poleg Kensingtonove študije, so leta 2010 podobno študijo izvedli tudi na inštitutu Ponemon, v povezavi s podjetjem Intel. V študijo so všteli podatke 329 podjetij iz privatnega ter državnega sektorja. Podatki iz podjetij so se zbirali v obdobju enega leta. V tem času so podjetja poročala število ukradenih ter izgubljenih prenosnih računalnikov. Skupno število je na koncu znašalo 86.455, kar znaša v povprečju 263 na podjetje. Skupno škodo so dobili tako, da so to število pomnožili s povprečnim stroškom enega izgubljenega ali ukradenega prenosnega računalnika. Izračun skupnih stroškov je tako znašal 2.1 biliona dolarjev, kar v povprečju znaša 6.4 milijona dolarjev na podjetje [5].

Študija se je osredotočala na velika podjetja, z veliko zaupnimi informacijami. Skupno število vseh prenosnih računalnikov, dodeljenih delavcem iz podjetij, je v vzorcu znašalo približno 3.7 milijona. Povprečno to znaša 11.174 prenosnih računalnikov na podjetje.

Tabela 1: Ključni statistični podatki študije Inštituta Ponemon [5]

Ključni statistični podatki iz vzorca	**Povprečje vzorca**	**Skupno**
Vzorec podjetij v študiji		329
Število dodeljenih prenosnih računalnikov	11 174	3 676 195
Število izgubljenih prenosnih računalnikov v enem letu	263	86 455
Od tega ukradenih	66	21 812
Od tega verjetno ukradenih	38	12 474
Od tega izgubljenih	159	52 169
Ponovno najdenih	12	3 936
Povprečna doba uporabe prenosnega računalnika	3.1 leta	
Razmerje letne izgube	2.32%	
Razmerje izgube v celotni dobi uporabe	7,12%	

Pie Chart 1: Distribution of participating companies by global headcount

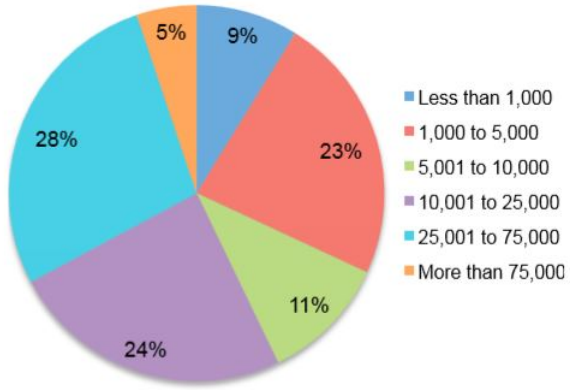
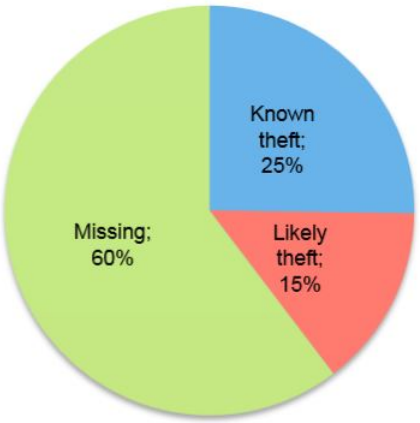


Table 2: Distribution of participating companies by industry classification

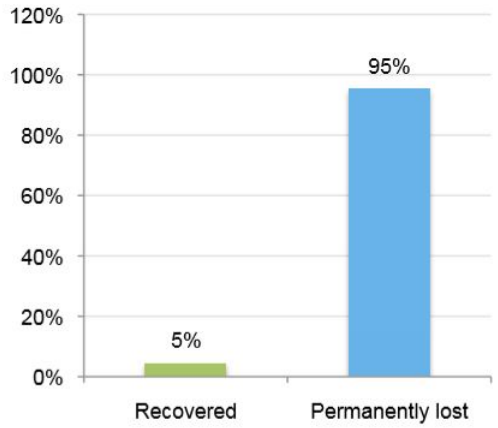
Industry	Pct%
Financial services	15%
Public sector	14%
Health & pharmaceutical	10%
Industrial	10%
Consumer	9%
Education & research	8%
Technology & software	8%
Retail	8%
Communications	7%
Services	7%
Transportation	3%
Other	1%
Total	100%

Slika 1: Procentualno število zaposlenih po določenih sektorjih v vzorcu. vir: [5]

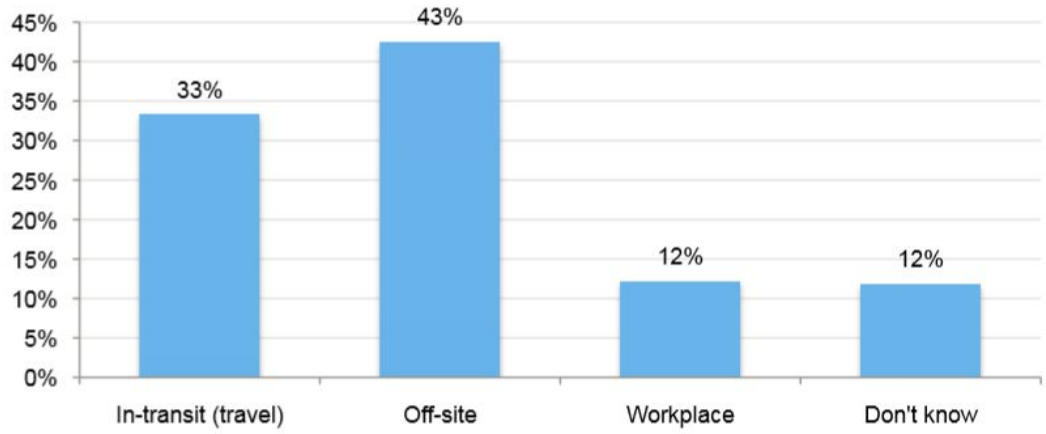
Pie Chart 2: Classification of lost or stolen laptops for the benchmark sample



Bar Chart 3: Percentage recovery rate among lost or stolen laptops for the benchmark sample

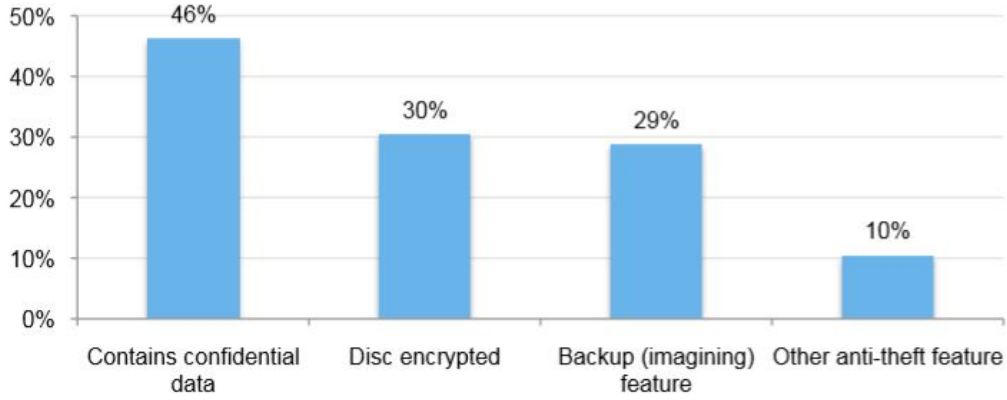


Slika 2: Procentualni prikaz ukradenih, izgubljenih in najdenih prenosnih računalnikov v vzorcu. vir: [5]



Slika 3: Lokacije izgubljenih prenosnih računalnikov. vir: [5]

Slika 3 prikazuje, da je: največ (43%) izgubljenih prenosnih računalnikov izven podjetja (domača pisarna, hotelske sobe, ...); na drugem mestu to med tranzitom (33%); na delovnem mestu znaša 12%; za 12% ni bilo možno izvedeti lokacije.



Slika 4: Zaščitenost podatkov. vir: [5]

Slika 4 prikazuje, da je: 46% vseh izgubljenih prenosnih računalnikov vsebovalo občutljive podatke; 30% uporabljalo enkripcijo diska; 10% uporabljalo neko drugo vrsto zaščite proti kraji; 29% bilo varnostno kopiranih.

Tabela 2: Podatki pridobljeni na vzorcu iz študije Inštituta Ponemon. [5]

Ekonomska računica	**Število**
Število vseh ukradenih prenosnih računalinkov	86 445
Število nekriptiranih prenosnih računalnikov	60 518
Število nekriptiranih prenosnih računalnikov z občutljivimi podatki	27 838
Povprečna škoda nekriptiranega izgubljenega prenosnega računalnika	$ 56 165
Skupni znesek	$ 1 563 521 270
Število kriptiranih prenosnih računalnikov	25 937
Število kriptiranih prenosnih računalnikov z občutljivimi podatki	11 931
Povprečna škoda kriptiranega izgubljenega prenosnega računalnika	$ 37 443
Skupni znesek	$ 446 732 433
Število prenosnih računalnikov brez občutljivih podatkov	46 686
Povprečna škoda ukradenega prenosnega računanika brez občutljivih podatkov	$ 4 078
Skupni znesek	$ 190 385 508
Skupna ekonomska računica vzorca	$ 2 200 639 211
Povprečna škoda na izgubljen prenosni računalnik	$ 25 454,16
Znesek ponovno najdenih prenosnih računalnikov	$ 100 187 565
Ekonomska računica po odštetju najdenih prenosnih računalnikov	$ 2 100 451 646
Povprečna škoda na podjetje	$ 6 384 352

V študiji je bilo tako prikazano, da je zelo pomembno pravilno izobraziti delavce. Poleg tega je prikazano tudi, da se z enkripcijo škoda, nastala pri izgubljenem oziroma ukradenem prenosnem računalniku zmanjša, za približno $ 20 000.

3 Enkripcija Podatkov

Rizičnost zlorabe podatkov, zaradi izgube ali kraje prenosnih naprav, je iz leta v leto višja, saj ima skoraj vsak posameznik v uporabi več naprav (prenosni računalnik, mobilni telefon, tablica, ...), na katere shranjuje svoje osebne podatke, kot tudi podatke podjetja, v katerem je zaposlen. Zato je potrebno zagotoviti najboljšo možno zaščito teh podatkov.

3.1 Začetki enkripcije

Starodavna oblika enkripcije izhaja iz časa starih Rimljanov, saj so jo uporabljali pri prenašanju sporočil z vojaško vsebino. Rimljani so šifrirali sporočila s tako imenovano Cezarjevo šifro, ki je vsako črko sporočila zamenjala s črko, ki je premaknjena z določeno fiksno številko, vzdolž po abecedi. Kot primer, lahko vzamemo naslov diplomske naloge in ga kriptiramo s Cesarjevo šifro, premaknjeno s fiksno številko, dve v desno:

Originalno sporočilo:
ZAŠČITA PODATKOV PRED KRAJO Z UPORABO ENKRIPCIJE

Kriptirano sporočilo:
ACUEKVC SRFCVMRŽ SŠGF MŠCLR A ZSRŠCČR GPMŠKSDKLG

Ker je Cezarjevo šifro preprosto razvozlati, so se pojavili novi enkripcijski algoritmi, ki jih je težje razbiti, oziroma dekriptirati, brez pravega ključa oziroma algoritma [9].

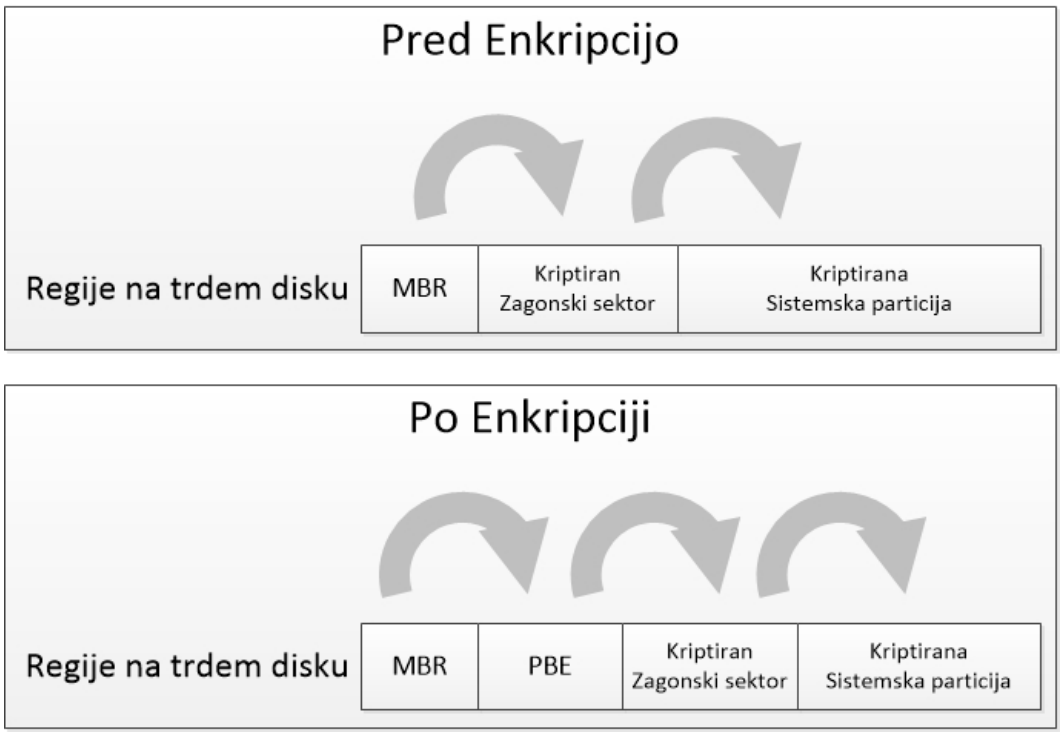
3.2 Tehnologije enkripcije

V ta namen uporabljamo različne tehnologije enkripcije podatkov na napravah. Najbolj pogosto uporabljene metode so: enkripcija celotnega diska - FDE (ang. Full Disk Encryption), enkripcija particije in virtualnih diskov ter enkripcija mape/datoteke (ang. File/folder encryption).

3.2.1 Enkripcija celotnega diska

Enkripcija celotnega diska (v nadaljevanju FDE) je proces enkripcije vseh podatkov na disku, ki se ga uporablja za zagon računalnika, vključno z operacijskim sistemom naprave, kar dovoljuje dostop do podatkov, šele po uspešni avtentikaciji s produktom FDE, ki se bazira na programski ali strojni osnovi [8].

Programska oprema FDE deluje tako, da preusmeri glavni zagonski zapis (ang. master boot record MBR). MBR je sektor na disku, ki vsebuje zapis lokacije programa ali operacijskega sistema, ki skrbi za zagon računalnika. Če računalnik ne uporablja nobene programske opreme FDE, MBR vsebuje zapis lokacije primarnega operacijskega sistema (v nadaljevanju OS). Programska oprema FDE ob namestitvi ustvari majhno particijo, ki vsebuje pred-zagonsko okolje (ang. pre-boot environment PBE), ki kontrolira dostop do računalnika. Poleg tega spremeni tudi MBR zapis tako, da ta kaže na okolje PBE. To okolje od uporabnika zahteva, da se avtenticira. Če je avtentikacija uspešna, FDE dekriptira disk ter zažene OS. Večina produktov FDE podpira uporabo mrežne avtentikacije (npr. AD avtentikacija, PKI) ter lokalne avtentikacije (npr. lokalna shramba ključa na ključku USB).



Slika 5: Sekvenca zagona računalnika s programskim produktom FDE.

Po uspešni avtentikaciji, produkt FDE dekriptira zagonske datoteke, ki so potrebne za zagon OS-a. Pri zagonu produkt FDE dekriptira datoteke, ko jih OS potrebuje za

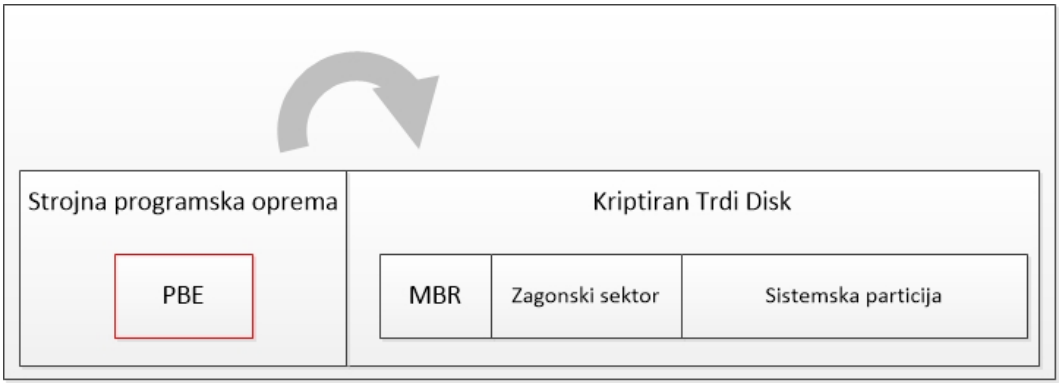
delovanje. Pri zagonu OS-a se uporabnik prijavi v sistem ter lahko normalno uporablja računalnik. Ko uporabnik odpira in shranjuje datoteke, produkt FDE transparentno dekriptira in kriptira sektorje na disku, kjer se nahajajo te datoteke. Ta proces nekoliko upočasni delovanje računalnika. Večja kot je datoteka, ki jo uporabnik odpira, bolj je to opazno. Uporabnik, ki uporablja računalnik, zaščiten s produktom FDE, lahko po navadi opazi počasnejše delovanje, le ob zagonu ter ugašanju OS-a. Upočasnitev je odvisna tudi od velikosti datotek na disku in velikosti ter hitrosti diska [8].

Ker uporaba produktov FDE spreminja način zagona računalnika, lahko povzroči tudi probleme pri delovanju. Npr. spreminjanje MBR zapisa lahko prepreči zagon računalnika, kjer se uporablja več OS-ov za zagon računalnika v primeru, da okolje PBE, ki ga produkt FDE ustvari ne zna zagnati upravitelja zagona, ampak direktno zažene enega od OS-ov, naloženih na disk-u. Povzroči lahko tudi probleme pri administraciji računalnikov ter pri uporabi bujenja preko mreže (ang. wake-on-LAN).

Produkti FDE se v večini uporabljajo za zaščito prenosnih računalnikov. Ker za avtentikacijo okolja PBE v večini zahtevajo osnovne računalniške komponente, kot je to npr. fizična tipkovnica, ker se OS še ni naložil [8].

FDE na strojni osnovi pomeni, da je produkt FDE tovarniško nameščen v strojno programsko opremo, do katere OS ter aplikacije nameščene na disku nimajo dostopa. Tako programski kot tudi strojni produkt FDE ponujata podobne zmožnosti preko drugačnega mehanizma. Ko uporabnik zažene napravo, ki je zaščitena s strojnim produktom FDE, disk zahteva, da se uporabnik avtenticira, preden dovoli zagon OS-a. Strojni produkt FDE je vgrajen v disk na tak način, da ga ni mogoče odstraniti ali izklopiti. Enkripcijska koda ter avtentikatorji, kot so to gesla in kriptografski ključi, so varno shranjeni na disku. Ker se enkripcija in dekripcija izvajata na strojnem nivoju, je upočasnitev delovanja naprave veliko manjša [8].

Največja razlika med programskimi in strojnimi produkti FDE je v tem, da je pri programski rešitvi možna centralizirana administracija, pri strojni pa se v večini primerov administrira lokalno. Strojna rešitev zahteva večji strošek administracije, kot programska rešitev. Strojna rešitev je varnejša ker: se vsa enkripcija zgodi znotraj diska; ne potrebuje kopije ključa v začasnem pomnilniku in je tako težje dostopna virusom, različnim škodljivim programom ter drugim nevarnostim; ne povzroča problemov pri delovanju, ker ne spreminja MBR zapisa [8].



Slika 6: Sekvenca zagona računalnika s strojnim produktom FDE.

Slika 6 prikazuje zagonsko sekvenco računalnika pri uporabi strojnega produkta FDE. V tem primeru vidimo, da se okolje PBE nahaja v strojni programski opremi, ne pa na trdem disku.

3.2.2 Enkripcija logičnih nosilcev (particij) ter enkripcija virtualnih diskov

Proces enkripcije virtualnih diskov (kontejnerjev, ki vsebujejo več datotek ter map) dopušča dostop do teh, le po pravilni avtentikaciji. Po avtentikaciji se virtualni disk mapira. Enkripcijo virtualnih diskov uporabljamo na vseh vrstah uporabniških naprav, kjer lahko hranimo podatke. Virtualni disk je datoteka, ki se nahaja na logičnem nosilcu.

Poznamo zagonske, sistemske ter podatkovne logične nosilce (particije), ki se nahajajo na računalniku. Proces enkripcije logičnega nosilca dopušča dostop do podatkov na njem, le po uspešni aventikaciji. Enkripcija logičnih nosilcev je večinoma uporabljena na podatkovnih logičnih nosilcih ter na izmenljivih disk-ih (ključkih USB, zunanjih trdih diskih, ...). Enkripcija zagonskih ter sistemskih nosilcev je posebna vrsta enkripcije FDE [8].

Enkripcija logičnih nosilcev ter enkripcija virtualnih diskov delujeta podobno. Za dostop se uporablja program, ki teče na OS-u. Ta nadzira branje ter pisanje podatkov na kriptiranem logičnem nosilcu ali virtualnem disku. Po zagonu OS-a, se kriptirani logični nosilec ali virtualni disk mapira po uspešni avtentikaciji, ko ga uporabnik potrebuje. Program nato avtomatsko po potrebi dekriptira ter kriptira sektorje. Tak način poveča čas branja ter shranjevanja podatkov, toda ta upočasnitev je vidna šele pri branju ter zapisovanju velikih datotek [8]. Upočasnjeno je lahko tudi mapiranje.

Ključna razlika med enkripcijo logičnih nosilcev ter enkripcijo virtualnih diskov je, da

so virtualni diski prenosljivi, logični nosilci pa niso. Virtualni disk je možno kopirati na drugi medij brez tikanja enkripcije, tako ga lahko zapečemo na CD ali DVD ali ga uporabljamo na medijih, ki niso bazirani na logičnih nosilcih. Enkripcija virtualnega diska omogoča enostavno varnostno kopiranje podatkov, saj ga lahko kopiramo na server ali prenosni medij. Prednost enkripcije virtualnih diskov je, da jih lahko hranimo na medijih, kjer potrebujemo tako zaščiteno kot tudi nezaščiteno hrambo podatkov (logični nosilec je lahko nezaščiten, na njega pa kopiramo kriptirani virtualni disk, v katerem so shranjene senzitivne informacije).

Nekateri produkti enkripcije virtualnih diskov omogočajo lažjo mobilnost tako, da na prenosni medij, poleg kriptiranega virtualnega diska, dodajo zagonske datoteke, s katerimi lahko na drugem računalniku namestimo gonilnike ali program, kar omogoči dekripcijo virtualnega diska, po uspešni avtentikaciji.

3.2.3 Enkripcija map in datotek

Enkripcija datotek je proces enkripcije individualnih datotek na shranjevalnem mediju ter zagotavlja dostop do kriptiranih datotek, le po pravilni avtentikaciji. Enkripcija map je zelo podobna enkripciji datotek, le da se v tem primeru izvaja enkripcija individualnih map. Nekateri OS-i nudijo že vgrajen način enkripcije datotek ter map, poleg tega pa obstaja tudi veliko programov, ki nam to omogočajo. Čeprav se slišita enkripcija map ter enkripcija virtualnih diskov zelo podobni, saj oboji vsebujejo več datotek, obstaja razlika. Virtualni disk je ena sama datoteka, kjer ni možen vpogled v vsebovane datoteke ter mape, dokler ta ni dekriptiran. Pri enkripciji map ali datotek je več transparentnosti, saj lahko vsak, ki ima dostop do datotečnega sistema, vidi imena ter meta podatke o datoteki ali mapi. Poleg tega lahko uporabnik dostopa tudi do imen datotek ter map in nekaterih meta podatkov, ki so vsebovane v kriptirani mapi, če le-te niso zaščitene preko kontrole dostopa, ki nam jo nudi OS.

Enkripcijo map ali datotek lahko implementiramo na veliko načinov, preko gonilnikov, servisov ter programov. Ko uporabnik poskuša odpreti kriptirano mapo ali datoteko, programska oprema najprej zahteva avtentikacijo uporabnika, nato pa avtomatsko dekriptira izbrano mapo ali datoteko. Vpliv na performance v delovanju je majhen [8]. Enkripcija map ali datotek se najpogosteje uporablja za uporabniške datoteke.

Večina produktov, za enkripcijo map ali datotek, ponuja več uporabniških načinov selekcije. Uporabnik lahko izbira:

- ročno, katero datoteko ali mapo bo kriptiral;

- lokacijo mape, kjer se vsebovane mape ali datoteke avtomatsko kriptirajo;
- tip datotek, ki se avtomatsko kriptirajo (npr. datoteke z določeno končnico);
- avtomatsko enkripcijo map ali datotek, ustvarjenih z določeno aplikacijo;
- avtomatsko enkripcijo vseh datotek določenega uporabnika.

3.3 Primerjava tehnologij enkripcije podatkov

Vsaka od opisanih tehnologij ima tako prednosti kot slabosti. Nekatere tehnologije so si med sabo zelo podobne in hkrati različne. Vse se uporablja v namene zaščite različnih občutljivih podatkov. Izbira tehnologije je tako pogojena z našimi zahtevami. Če na primer potrebujemo zaščito vseh podatkov na računalniku, je najboljša izbira enkripcija celotnega disk-a. V primeru, da si želimo kriptirati le podatke, na podatkovni particiji na disku, prenosnih trdih diskih ali ključkih USB, nam pride bolj prav enkripcija logičnih nosilcev. Če si želimo prenosljivost kriptiranih podatkov, brez potrebe dekripcije le teh pred kopiranjem, nam je na voljo enkripcija virtualnih diskov ali enkripcija map ter datotek. Vse tehnologije enkripcije podatkov zmanjšajo grožnjo zlorabe podatkov, v primeru izgube ali kraje naprave, poleg tega, tudi predstavljajo različne grožnje, v primeru okvare tehnologije. V nekaterih primerih lahko izgubimo tudi funkcionalnost naprave, v drugih pa samo izgubo podatkov (zato je vedno priporočeno, da imamo nekje shranjeno varnostno kopijo vseh podatkov). Nekatere tehnologije nas, v neki meri, varujejo tudi proti zlonamernim programom. Za lažjo odločitev, pri izbiri tehnologije, imamo spodaj tabelo, s primerjavo tehnologij med seboj.

Tabela 3: Primerjava tehnologij enkripcije podatkov [8]

Karakteristike	**Enkripcija celotnega diska**	**Enkripcija logičnih nosilcev**	**Enkripcija virtualnih diskov**	**Enkripcija map in datotek**
Tipično podprte platforme	Prenosni ter stacionarni računalniki.	Prenosni, stacionarni računalniki, izmenljivi mediji osnovani na logičnih nosilcih (npr. ključek USB).	Vsi tipi naprav, ki lahko shranjujejo podatke.	Vsi tipi naprav, ki lahko shranjujejo podatke.
Podatki, varovani s pomočjo enkripcije.	Vsi podatki na mediju (podatkovne datoteke, sistemske datoteke ter meta-podatki)	Vsi podatki na logičnem nosilcu (podatkovne datoteke, sistemske datoteke ter meta-podatki)	Vsi podatki v virtualnem disk-u (podatkovne datoteke, meta-podatki, vendar ne tudi sistemske datoteke)	Individualne mape ter datoteke (samo podatkovne datoteke)
Zamnjša grožnje v primeru izgube ali kraje naprave?	Da	Da	Da	Da
Zmanjša grožnje na aplikacijskem nivoju (zlonamerna programska oprema)	Ne	Kriptiran podatkovni logični nosilec v nekaterih primerih.*	V nekaterih primerih.*	V nekaterih primerih.*
Potencialne škode naprave v primeru okvare tehnologije	Izguba vseh podatkov ter funkcionalnost naprave.	Izguba podatkov na logičnem nosilcu; izguba funkcionalnosti naprave, vezane na zaščiteni, logični nosilec (podatkovni ali sistemski).	Izguba vseh podatkov, znotraj virtualnega diska.	Izguba vseh zaščitenih map ter datotek.
Prenosljivost kriptiranih podatkov	Ni prenosljivo.	Ni prenosljivo.	Prenosljivo.	Večinoma prenosljivo.

* Te enkripcijske tehnologije lahko varujejo podatke, samo proti nekaterim grožnjam na aplikacijskem nivoju, če se uporabnik ni avtenticiral za dostop podatkov v tej seji. V primeru SSO (single sign on) je uporabnik avtenticiran za dostop do teh podatkov pri OS avtentikaciji, torej podatki niso več varovani pred temi grožnjami takoj, ko se uporabnik avtenticira na OS.

3.4 Obstoječe rešitve na trgu

Za enkripcijo podatkov obstaja več različnih rešitev. Nekatere so že vključene v OS, druge pa se namesti kot aplikacijo na napravo.

- **BitLocker**

  Bitlocker spada v produkte, ki so že vključeni v OS: Windows OS (Windows Vista; Windows 7: Enterprise ter Ultimate; Windows 8, 8.1, 10: Proffesional ter Enterprise edicije; Windows Server: 2008, 2008R2, 2012, 2012R2).
  BitLocker prepreči osebam, ki poskušajo zagnati drugi OS, uporabiti program za razbijanje zaščite Windows datotečnega sistema ali izvajanje pregledovanja podatkov, shranjenih na zaščitenem disku. Ta zaščita se doseže s šifriranjem celotnega Windows nosilca. Z zaščito Bitlocker so šifrirane vse datoteke: uporabniške, sistemske, hibernacijske [10].

- **FileVault**

  FileVault tako kot BitLocker spada med produkte, ki so že vključene v OS, vendar za razliko, je ta vključen v OS: Apple Mac OS X, in sicer od verzije 10.3 dalje in ne v Windows OS.
  S primarno verzijo enkripcije FileVault, dodano v Mac OS X 10.3 (Panther), je lahko uporabnik kriptiral le domačo uporabniško mapo. Z verzijo 2 FileVault, vključeno v verzijo 10.7 (Lion) dalje, uporablja uporabniško geslo za enkripcijki ključ. Za enkripcijo celotnega diska uporablja AES-XTS medoto, z 256 bitnim ključem. Le nekateri uporabniki lahko odklenejo zaščiteni disk. Pri odklenjenemu zaščitenemu disku, lahko tudi drugi uporabniki uporabljajo računalnik, dokler ga ne ugasnemo [12].

- **TrueCrypt**

  Ta produkt ni več v razvoju, vendar je eden prvih odprtokodnih rešitev, iz katerega so kasneje nastali nekateri novi produkti. Podpira enkripcijo virtualnih diskov, logičnih nosilcev, celotnega diska, s pomočjo pred zagonske avtentikacije, če le ta uporablja particijski zapis MBR. Možno ga je uporabljati na več različnih OS - jih (Microsoft Windows, Mac OS X, Linux, Dragonfly BSD, Android) [14].

- **VeraCrypt**

  Izhaja iz TrueCrypt–a in je brezplačen odprtokodni produkt. Ponuja zelo podobne možnosti kot TrueCrypt, le da se še vedno razvija ter podpira manj OS-jev (Microsoft Windows, Mac OS X, Linux) [15].

- **AxCrypt**

  Odprtokodni produkt, ki je namenjen enkripciji individualnih datotek na Microsoft Windows OS-u. Datoteke, kriptirane s tem produktom, so enostavno prenosljive ter jih je možno pošiljati tudi preko elektronske pošte. Podpira tudi kreacijo samo-dekriptivnih datotek, kar pomeni, da ne potrebujemo instalacije AxCrypt produkta za dekripcijo takih datotek [1].

- **GNU Privacy Guard (GnuPG)**

  Je odprtokodna implementacija Preaty Good Privacy (PGP). Možna uporaba tako CLI kot GUI verzij produkta. GnuPG je poseben, saj je v večini namenjen kriptiranju datotek, namenjenih izmenjavi med več uporabniki. Uporablja hibridno enkripcijo, ker uporablja kombinacijo običajne simetrične kriptografije, za hitrejše delovanje ter kombinacijo javnega ključa, za lažjo ter varno izmenjavo ključa. Datoteke se tako kriptira z javnim ključem prejemnika [13].

- **7-Zip**

  7-zip je v osnovi namenjen za arhiviranje datotek, omogoča pa nam tudi enkripcijo le-teh z geslom, da ga lahko uporabimo kot produkt za enkripcijo virtualnih diskov. Podpira kreacijo samo-dekriptivnih arhivov, ki se dekriptirajo, ko uporabnik vpiše geslo, s katerim je bilo kriptirano [3].

3.4.1 Primerjava rešitev

Tako kot tehnologije enkripcije imajo tudi produkti, ki nam omogočajo uporabo teh tehnologij, prednosti ter slabosti. Nekateri produkti delujejo le na določenih OS-jih, drugi nam omogočajo uporabo na različnih OS-jih. Poleg tega se nekateri produkti osredotočajo le na eno tehnologijo, drugi pa nam ponujajo izbiro med večimi ali celo kombinacijo. Spodnja tabela nam tako prikazuje prednosti in slabosti vsakega opisanega produkta, za lažjo odločitev pri uporabi le-tega v našem okolju.

Tabela 4: Prednosti ter slabosti posameznih rešitev

	Prednosti	**Slabosti**
Bitlocker	- vključen v OS - enostavna uporaba - veliko načinov hranjenja ključa za obnovitev - več načinov avtentikacije	- vključen le v nekatere edicije Windows OS - na voljo le na Windows OS
FileVault	- vključen v OS - enostavna uporaba - AES 256bit enkripcija	- vključen le v Apple Mac OS X
TrueCrypt	- odprtokodni - brezplačen - podpora več OS - več načinov enkripcije	- ustavljen razvoj - odprtokodnost lahko predstavlja tudi nevarnost
VeraCrypt	- odprtokodni - brezplačen - podpora več OS - več načinov enkripcije.	- odprtokodnost lahko predstavlja tudi nevarnost
AxCrypt	- odprtokodnost - brezplačno - prenosljivost zaščitenih datotek	- podpira samo Microsoft Windows - odprtokodnost lahko predstavlja tudi nevarnost
GnuPG	- odprtokodnost - podprtost na več OS - enostavna izmenjava kriptiranih datotek	- potrebno varovanje privatnih ključev - potrebna izmenjava javnih ključev - odprtokodnost lahko predstavljatudi nevarnost
7-Zip	- enostavna uporaba - možna uporaba na več OS - ih	- podpira le enkripcijo z geslom

4 Metodologija

V podjetju, ki se ukvarja s kartičnim poslovanjem, kjer sem zaposlen, veliko zaposlenih uporablja prenosne računalnike, zato se daje poudarek na varnosti podatkov. V podjetju je bil že rešen problem z izgubo podatkov zaradi okvare ali izbrisa podatkov iz računalnikov, s pomočjo programa za varnostno kopiranje določenih tipov datotek na arhivski server, ko se ti računalniki nahajajo v notranji mreži. Ker pa ta program ne varuje pred nepooblaščenimi dostopi do teh podatkov v primeru izgube ali kraje naprave, je bilo potrebno postaviti še dodatno zaščito. Zato je bilo odločeno, da se vse podatke na prenosnih računalnikih zakriptira z enim od produktov FDE.

Po daljši raziskavi ter primerjavi produktov FDE je bilo odločeno, da se uporabi Microsoft-ovo rešitev - BitLocker, saj je podjetje že imelo vso infrastrukturo za postavitev. Rezultati raziskave so obširneje predstavljeni v nadaljevanju.

Za aktivacijo enkripcije BitLocker potrebujemo računalnik, naložen z enim od OS-ov: Windows 7 (Enterprise ali Ultimate verzijo), Windows 8, 8.1, ali 10 (Professional ali Enterprise verzijo) [6].

4.1 Izbira Rešitve

Preden je bila lahko izbrana rešitev, je bilo potrebno zbrati vse naše zahteve. Zahteve so bile zbrane na podlagi trenutnih potreb ter tudi z mislijo za prihodnost. Zahteve so bile zbrane v sodelovanju z SO (Security Office) oddelkom, saj je njihova glavna naloga skrb za ščitenje sistema ter podatkov, poleg tega pa so najbolj na tekočem z zadnjimi varnostnimi luknjami v sistemih.

Zahteve v našem primeru:

- Enkripcijo FDE vseh prenosnih računalnikov;
- Enkripcija vseh fiksnih diskov, v primeru večih particij ali večih diskov v računalniku;
- Centralna hramba obnovitvenih ključev;
- Enostavna aktivacija enkripcije FDE;

- Skalabilnost, v primeru povečanja števila kriptiranih računalnikov;
- Transparentno delovanje za uporabnika;
- Navodilo za uporabo (aktivacija ter administracija);
- V prihodnosti možna enkripcija vseh računalnikov;
- V prihodnosti možnost enkripcije prenosnih diskov ter ključkov USB.

Ko so bile zahteve zbrane, je nastopila izbira rešitve. Pričeli smo z raziskavo, ki se je najprej pričela pri iskanju različnih rešitev preko internet-a (mnenj drugih ljudi na forumih, prebiranje člankov, s primerjavami med različnimi produkti). Poleg tega smo za mnenja povprašali tudi podjetja (partnerje), ki nam nudijo IT podporo, kaj uporabljajo oni oziroma, kaj nam priporočajo. Tako smo imeli, s strani podjetij Microsoft ter IBM predstavitev, njihove rešitve. Na podlagi predstavitev je bilo ugotovljeno, da ima podjetje, za Microsoft-ovo rešitev BitLocker, že celotno infrastrukturo ter, če bi se odločili za njo, ne bi bilo potrebno investirati dodatno za infrastrukturo. IBM pa nam je v bistvu bolj prikazoval njihov MDM (Mobile Device Management) produkt, ki omogoča administracijo prenosnih naprav (prenosnih računalnikov, tablic, mobilnih telefonov). Produkt sicer omogoča tudi zagon enkripcije ter hranjenje ključev na prenosnih napravah, ampak je v osnovi namenjen kontroliranju prenosnih naprav (sledenje preko GPS-a, izbris vseh podatkov na daljavo), oziroma nam omogoča tudi varno okolje, pri uporabi BYOD. Poleg tega bi bilo za IBM-ov produkt potrebno še dodatno investirati v licence, postavitev dodatnih serverjev, za njihovo aplikacijo ter bazo podatkov, ki jo aplikacija potrebuje.

Rešitev je bila izbrana na podlagi mnenj drugih podjetij ter infrastrukture, ki jo že uporabljamo. Zato je bila izbrana rešitev Microsoft BitLocker, saj:

- je že integriran v OS, ki se ga uporablja na prenosnih računalnikih zaposlenih;
- je možno hraniti ključe na domenski kontroler, ki se ga je že uporabljalo za avtentikacijo uporabnikov ter računalnikov;
- je možna aktivacija preko grupne politike (ang. Group Policy GPO);
- je ta produkt transparenten za uporabnika, ker se ključ lokalno hrani v platformi TPM;
- je možno ta produkt uporabiti v prihodnosti za vse računalnike ter prenosne diske in ključke USB;

- ni bilo potrebno dodatno investirati v produkt.

Ko je bila rešitev izbrana, je bilo potrebno izdelati še načrt, postaviti testno okolje ter po uspešnem testiranju produkt postaviti v produkcijsko okolje. Postavitev, testiranje ter rezultati so obširneje opisani v naslednjih poglavjih.

5 Pilotna Postavitev

Najprej je bilo potrebno izbrati testno skupino prenosnih računalnikov, na kateri je bilo možno testirati brez povzročanja težav uporabnikom. Testno okolje je tako znašalo 5 različnih modelov, tako starejših kot tudi novejših. Nekateri so bili vgrajeni z navadnim trdim diskom HDD, drugi pa z diski SSD tako, da je bilo možno testirati tudi vpliv na različne tehnologije diskov. Specifikacije testnih prenosnih računalnikov predstavljene v tabeli spodaj:

Tabela 5: Specifikacije testnih prenosnih računalnikov

Model	**Lenovo T500**	**Lenovo Carbon X1**	**Lenovo T530**	**Acer P645-S**	**HP ProBook 650 G1**
OS	Win 7	Win 10	Win 7 ter Win 10	Win 7	Win 7
Starost	Več kot 5 let	Pol leta	3 leta	1 leto	2 leti
Processor	Core 2 Duo P8600	Intel Core i5-5200U	Intel Core i5-3320M	Intel Core i5-5300U	Intel Core i5-4600M
Disk	HDD ter SSD	SSD	HDD ter SSD	SSD	HDD
RAM	4 GB	8 GB	6 GB	4 GB	4 GB

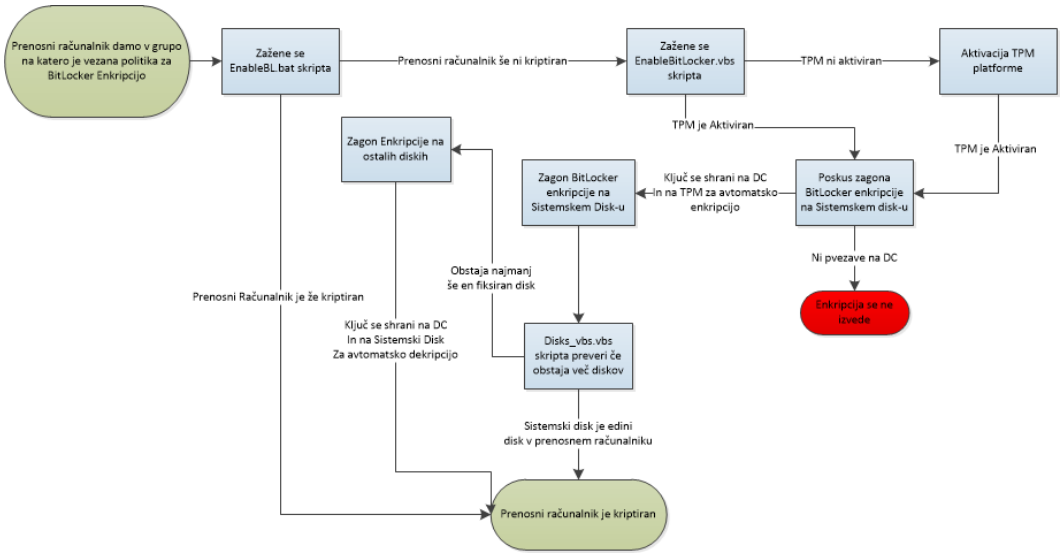
V tabeli 5 so predstavljeni modeli testnih prenosnih računalnikov ter njihove specifikacije. Na nekaterih modelih sta bili testirani obe tehnologiji diskov: HDD in SSD. Poleg tega sta bili na nekaterih modelih testirani dve verziji Windows OS: Windows 7 in Windows 10.

Za izvedbo je bilo potrebno najprej nastaviti pravilno GPO politiko tako, da je možno hranjenje obnovitvenih ključev na domenskem kontrolerju. V politiki je poleg tega tudi nastavljena moč enkripcije (256 bit) ter načina hranjenja ključev za avtomatsko dekripcijo sistemskega diska, ob pravilnem zagonu prenosnega računalnika (ključ se hrani v platformi TPM). Prav tako pa politika skrbi tudi, da se enkripcija ne izvede, dokler ključ ni zapisan v domenski kontroler.

Za vklop, aktivacijo platforme TPM in vklop enkripcije BitLocker, je bila uporabljena Microsoft-ova vbs skripta. Ker skripta v osnovi kriptira samo sistemsko particijo, smo naredili še eno skripto za vklop enkripcije ostalih fiksnih diskov, če so nameščeni v računalnik. Skripte so bile nastavljene tako, da se na prenosnemu računalniku zaženejo ob njegovem zagonu. Te skripte so vezane na GPO politiko, za lažje kontroliran vklop na prenosnih računalnikih. Spisali smo navodila za aktivacijo ter administracijo enkripcije. Navodila so spisana v angleškem jeziku (glej prilogo).

Delovanje skript:
V uporabi imamo kombinacijo Batch ter Visual basic skript:

- EnableBl.bat skripta (glej prilogo):
  - je glavna, saj skrbi za pravilno izvedbo;
  - se zažene, kot zagonska skripta ob vsakem zagonu računalnika;
  - nastavi, variable za logiranje postopka ter logira cel postopek izvedbe skripte;
  - preveri, če je TPM vklopljen in aktiviran:
    * Če ni aktiviran, sproži vklop in aktivacijo TPM-ja s pomočjo EnableBitLocker.vbs skripte, kar zahteva ponovni zagon računalnika.
    * Če je aktiviran, sproži BitLocker enkripcijo sistemskega diska s pomočjo EnableBitLocker.vbs skripte ter pošlje obnovitveni ključ na domenski kontroler.
  - S pomočjo disks_vbs.vbs skripte preveri, če je v računalniku v uporabi še kakšen fiksni disk:
    * Če obstaja še kakšen fiksni disk, zažene enkripcijo BitLocker tudi na teh diskih, pošlje obnovitvene ključe na domenski kontroler ter nastavi na avtomatski odklep ob zagonu računalnika.
    * Če ne obstaja, se tu izvedba skripte zaključi.
  - Ko se enkripcija disk-a zaključi, imamo vse podatke zaščitene z enkripcijo BitLocker.
- EnableBitLocker.vbs (pridobljeno iz Microsoft Script Center [7]):
  - je Microsoft-ova Visual Basic skripta, ki se jo uporablja za vklop in aktivacijo platforme TPM ter vklop enkripcije BitLocker.
- Disks_vbs.vbs (glej prilogo):
  - je Visual Basic skripta, ki izpiše vse fiksne diske, prisotne v računalniku, nam pomaga pri enkripciji vseh diskov v računalniku.



Slika 7: Diagram poteka enkripcije

Slika 7 nam prikazuje diagram poteka enkripcije prenosnega računalnika, z uporabljeno GPO politiko ter skriptami.

6 Rezultati

Testni prenosniki so bili na domeni premaknjeni v poseben OU (organization unit – organizacijska skupina). Testirano je bilo:

- Avtomatska enkripcija: se je začela izvajati takoj po ponovnem zagonu, ko je bil določen prenosnik prestavljen v testni OU.
- Enkripcija brez povezave z domenskim kontrolerjem: se ni začela izvajati, ker ni bilo možno narediti varnostne kopije ključa na domenski kontroler.
- Prenosni računalnik z ločenim podatkovnim diskom: uporabljene skripte nam omogočajo avtomatsko enkripcijo vseh fiksnih diskov ter avtomatsko dekripcijo le-teh ob pravilnem zagonu prenosnega računalnika. Ključi za avtomatsko dekripcijo nesistemskih diskov se hranijo na varni, uporabniku skriti lokaciji, na sistemskem disku.

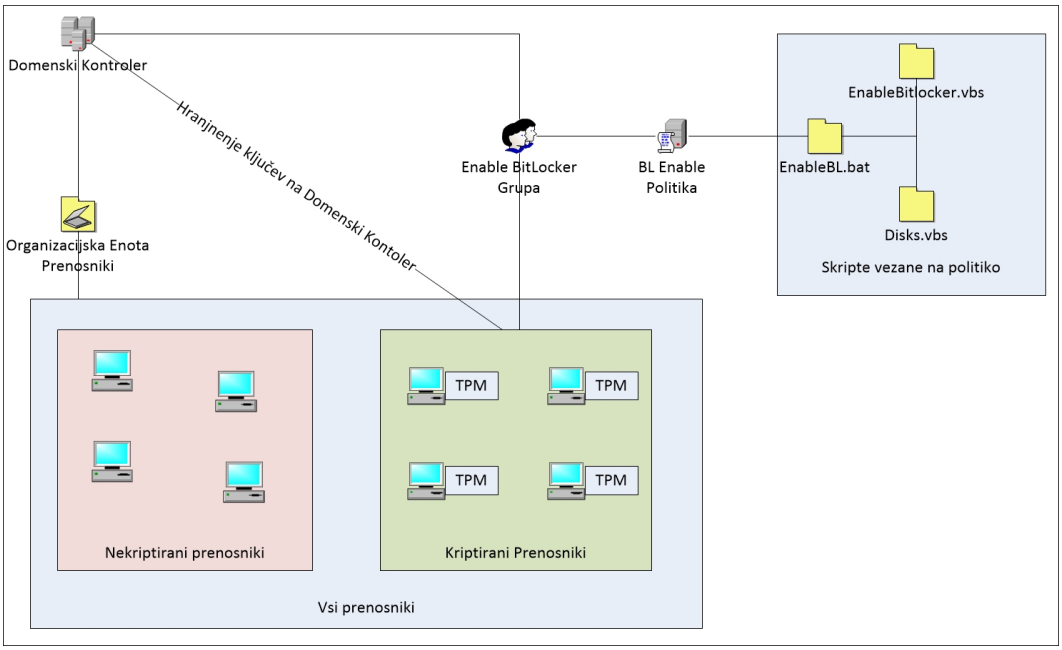
Po uspešni enkripciji je bilo testirano še:

- Enostavnost uporabe: avtomatska dekripticija preko platforme TPM nam omogoča, da kot uporabnik ne opazimo, da je prenosnik kriptiran.
- Zagon prenosnega računalnika iz prenosnega medija in dostop do podatkov na kriptiranem disku: dostop ni dovoljen; po ponovnem zagonu prenosnega računalnika sistem zahteva od uporabnika 48 mestni ključ, ki ga je možno pridobiti iz domenskega kontrolerja.
- Vdor v sistem z orodji, ki nam omogočajo pridobitev uporabniškega gesla: dostop ni dovoljen; po ponovnem zagonu prenosnega računalnika sistem zahteva od uporabnika 48 mestni ključ, ki ga je možno pridobiti iz domenskega kontrolerja.
- Vpliv na hitrost prenosnega računalnika: v tem primeru je velika razlika med prenosnimi računalniki. Pri starejših, s starejšimi procesorji, je upočasnitev večja, kot pri novejših, z novejšimi procesorji, saj ti procesorji podpirajo strojno AES dekripcijo. Velika razlika je tudi pri izbiri tehnologije diskovja, saj se pri novejših prenosnih računalnikih diski SSD veliko bolje izkažejo. Kar je povzeto tudi v naslednji tabeli:

Tabela 6: Problemi na testnih prenosnih računalnikih

Model	**Lenovo T500**	**Lenovo Carbon X1**	**Lenovo T530**	**Acer P645-S**	**HP ProBook 650 G1**
OS	Win 7	Win 10	Win 7 ter Win 10	Win 7	Win 7
Starost	Več kot 5 let	Pol leta	3 leta	1 leto	2 leti
Processor	Core 2 Duo P8600	Intel Core i5-5200U	Intel Core i5-3320M	Intel Core i5-5300U	Intel Core i5-4600M
Disk	HDD ter SSD	SSD	HDD ter SSD	SSD	HDD
RAM	4 GB	8 GB	6 GB	4 GB	4 GB
Problem	Počasno delovanje	Ni vidnih problemov	Počasno delovanje z diskom HDD	Ni vidnih problemov	Počasno delovanje zaradi diska HDD

Tabela 6 nam prikazuje probleme, ki so nastali v času testiranja. Najslabše se je, tekom testiranja, izkazal model Lenovo T500 prenosnih računalnikov, zaradi zastarele tehnologije procesorja, ki ne vsebuje strojne AES dekripcije. Pri teh prenosnih računalnikih tudi disk SSD ni veliko pripomogel k hitrosti. Pri modelu Lenovo T530 se je izkazalo, če menjamo disk HDD z SSD, se hitrost delovanja veliko izboljša. Pri modelu HP ni bilo testirano z diskom SSD, ker jih je v podjetju le 5 in bodo menjani z drugim modelom. Pri modelih Lenovo Carbon X1 in Acer P645-S ni bilo vidnih problemov, saj imata oba modela procesor, ki zmore strojno AES dekripcijo ter sta bila oba modela kupljena z že vgrajenim diskom SSD. Pri različnih verzijah Windows OS-a, ni bilo velikih razlik in tudi ni vplivalo na nastale probleme.



Slika 8: Postavitev sistema

Diagram na sliki 8 nam pokaže, kako so prenosni računalniki v OU-ju vseh prenosnih računalnikov vezani na domeno. Znotraj te enote so nekateri prenosni računalniki vezani na "Enable BitLocker"grupo, ki je vezana na "BL Enable"politiko. Ta politika zažene skripte na teh prenosnih računalnikih, ki poskrbijo za zagon enkripcije BitLocker. Vsak kriptirani prenosni računalnik pošlje svoj ključ na domenski kontroler, poleg tega pa ima ključ shranjen še lokalno na platformi TPM.

7 Zaključek in nadaljnje delo

Po uspešno zaključenem testiranju na testnih prenosnih računalnikih, se je začelo kriptirati tudi ostale prenosne računalnike po navodilih, napisanih v času testiranja. Zaradi potrebe po menjavi večjega števila starih prenosnih računalnikov, se je najprej začelo z enkripcijo novo izdanih prenosnih računalnikov. Tekom testiranja je bil nekaterim uporabnikom, poleg enkripcije, zamenjan disk HDD, s hitrejšim diskom SSD.

V podjetju se, zaradi uporabe ključkov USB, razmišlja o enkripciji le-teh. Ker smo uporabili za enkripcijo prenosnih računalnikov produkt BitLocker, je možna rešitev za ključke USB, tudi podprodukt BitLocker TO-GO. Zaradi dodatne varnosti bi bilo potrebno, v podjetju, kriptirati stacionarne računalnike, in sicer z enkripcijo BitLocker, ki je že na voljo Za enkripcijo službenih mobilnih telefonov, z Android OS-jem, pa je možno uporabiti enkripcijo, preko sistema MDM.

8 Literatura in viri

[1] Axcrypt. http://www.axantum.com/axcrypt/. *(Citirano na strani 16.)*

[2] D. Evans. What is byod and why is it important?, oct 2015. *(Citirano na strani 2.)*

[3] A. Henry. Five best file encryption tools, aug 2015. *(Citirano na strani 16.)*

[4] E. J. Hom. Mobile device security: Startling statistics on data loss and data breaches, 2010. *(Citirano na strani 3.)*

[5] P. I. LLC. The billion dollar lost laptop problem. Technical report, Ponemon Institute LLC, Traverse City, Michigan 49629 USA, sep 2010. *(Citirano na straneh 4, 5, 6 in 7.)*

[6] Microsoft. Windows 7 bitlocker^{TM} drive encryption security policy, aug 2011. *(Citirano na strani 18.)*

[7] Microsoft Corporation. Bitlocker deployment script - updated, dec 2014. *(Citirano na strani 22.)*

[8] K. Scarfone, M. Souppaya, and M. Sexton. Guide to storage encryption technologies for end user devices. *NIST Special Publication 800-111*, nov 2007. *(Citirano na straneh 9, 10, 11, 12 in 14.)*

[9] T. Vidmar. *Informacijsko Komunikacijski Sistemi*. Založba Pasadena, Ljubljana, 2002. *(Citirano na straneh 1 in 8.)*

[10] Wikipedia. Bitlocker. https://en.wikipedia.org/wiki/BitLocker. *(Citirano na strani 15.)*

[11] Wikipedia. Bring your own device. *(Citirano na strani 2.)*

[12] Wikipedia. Filevault. https://en.wikipedia.org/wiki/FileVault. *(Citirano na strani 15.)*

[13] Wikipedia. Gnu privacy guard. https://en.wikipedia.org/wiki/GNU_Privacy_Guard. *(Citirano na strani 16.)*

[14] Wikipedia. Truecrypt. https://en.wikipedia.org/wiki/TrueCrypt. *(Citirano na strani 15.)*

[15] Wikipedia. Veracrypt. https://en.wikipedia.org/wiki/VeraCrypt. *(Citirano na strani 16.)*

Priloge

A EnableBL.bat

```
:: EnableBL.bat
::
::*********************************************************************************
:: Checks TPM status, enables and activates TPM
:: Activates BitLocker Encryption on all system and fixed drives.
:: Sends recovery password to AD, sets all fixed drives to autounlock upon
   OS boot
:: Works with Windows 7, 8, 8.1, 10
:: Script must be run with admin privileges
:: Can be used as a logon script
:: Dependency:
:: - EnableBitLocker.vbs
:: - disks_vbs.vbs
::*********************************************************************************
::
:: Author: Marko Poljansek
::

@echo off
REM set the log files variables
set loglocation=%ProgramFiles%\_logs
set logfile="%loglocation%\ActivateTMP.log"
set logfile1="%loglocation%\EnableBL.log"
set logfile2="%loglocation%\EnableBLVBS.log"
set logfile3="%loglocation%\EnableBL1.log"
set logfile4="%loglocation%\EnableBLFixDrives.log"

REM If PC is already BitLocker protected go to end
if exist %logfile3% goto end

REM If PC was rebooted to activate TPM enable BitLocker Encryption
if exist %logfile1% goto enable
```

```
REM Check if TPM is Enabled and Activated
wmic /namespace:\\root\cimv2\security\microsofttpm path win32_tpm get
    IsEnabled_InitialValue | find /i "TRUE" > null
if %errorlevel% EQU 0 echo %date% %time% TPM is Enabled >> %logfile1%

wmic /namespace:\\root\cimv2\security\microsofttpm path win32_tpm get
    IsActivated_InitialValue | find /i "TRUE" > null
if %errorlevel% EQU 1 goto enable REM if everything is OK start BitLocker
    Encryption

REM If TPM is not enabled or activated, enable and/or acticate it first
echo aktivacija TPM-ja >> %logfile%
cscript "C:\Program Files\_Logs\EnableBitLocker.vbs" /on:TPM /l:%logfile%

:enable
REM Enable BitLocker on System drive
echo %date% %time% TPM is Activated. >> %logfile1%
echo %date% %time% - BitLocker vklop - zacetek. >> %logfile3%
cscript "C:\Program Files\_Logs\EnableBitLocker.vbs" /on:TPM /l:%logfile2%
echo %date% %time% - BitLocker vklop - konec. >> %logfile3%

REM Enable BitLocker on other fixed drives if they exist
cd "C:\Program Files\_logs\"
cscript disks_vbs.vbs >> disks.txt

FOR /F "eol=; skip=3 tokens=1* delims=, " %%i in (disks.txt) do (
   echo %date% %time% Disk %%i: Bitlocker started >> %logfile4%
   manage-bde -on %%i: -rp
   manage-bde -autounlock -enable %%i:
   echo %date% %time% Disk %%i: Bitlocker ended >> %logfile4%y
)

:end
REM Exit
```

B disks_vbs.vbs

```
'*********************************************************************************
' disks_vbs.vbs
'
' This script finds all fixed drives connected to the computer on computer
'
'*********************************************************************************

Dim goFS     : Set goFS     = CreateObject( "Scripting.FileSystemObject" )
   Dim dicDTypes : Set dicDTypes = buildDicMKV( _
      vbTextCompare, Split( "0 1 2 3 4 5" ), Split( "Unknown Removable Fixed
          Network CD-ROM RAM-Disk" ) _
   )
   Dim dicDrives : Set dicDrives = CreateObject( "Scripting.Dictionary" )
   Dim oWSH     : Set oWSH     = CreateObject( "WScript.Shell" )
   Dim sSysDir  : sSysDir      = oWSH.Environment( "PROCESS" )( "SYSTEMROOT" )
   Dim sSysDrive : sSysDrive   = goFS.GetDriveName( sSysDir )
   Dim sSDLetter : sSDLetter   = Left( sSysDrive, 1 )
   Dim oDrive
   For Each oDrive In goFS.Drives
      If     "Fixed" = dicDTypes( CStr( oDrive.DriveType ) ) _
         And sSDLetter <> oDrive.DriveLetter Then
         Set dicDrives( oDrive.DriveLetter ) = oDrive
      End If
   Next
   Dim sDrive
   For Each sDrive In dicDrives.Keys
      Set oDrive = dicDrives( sDrive )
      WScript.Echo oDrive.DriveLetter, oDrive.DriveType, dicDTypes( CStr(
          oDrive.DriveType ) )
   Next

Function buildDicMKV( vbCompMode, aKeys, aValues )
   Set buildDicMKV = CreateObject( "Scripting.Dictionary" )
```

```
   buildDicMKV.CompareMode = vbCompMode
   Dim nIdx
   For nIdx = 0 To UBound( aKeys )
      buildDicMKV.Add aKeys( nIdx ), aValues( nIdx )
   Next
End Function
```

C ISPC Bitlocker Documentation

ISPC Bitlocker Documentation

,

Date: 25.2.2016	Version 01
Author: Marko Poljanšek	

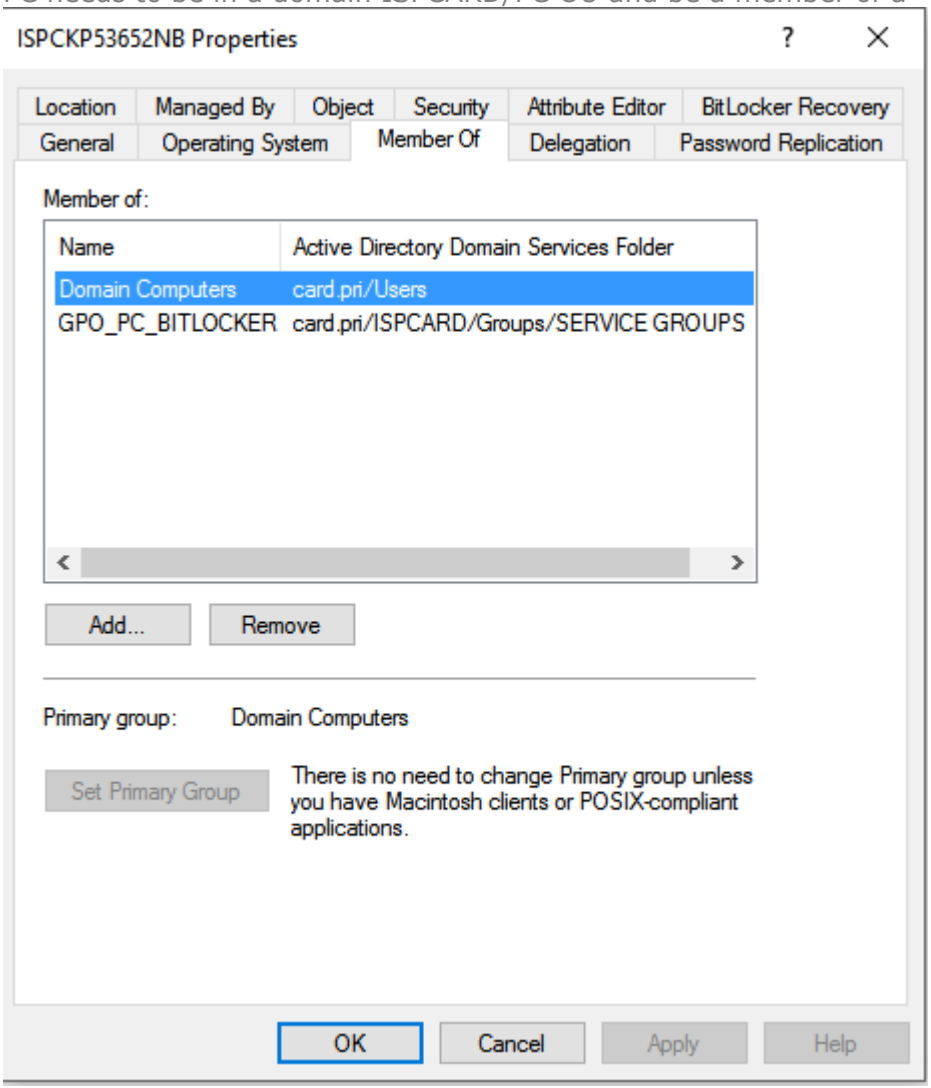
Requirements for BitLocker Drive encryption

- PC or Laptop with at least TPM (thrusted platform module) version 1.2 or newer.
- Microsoft Windows 7 or newer Microsoft OS installed.

Recommended:
- Before BitLocker is enabled BIOS upgrade to the latest version is recommended.
- All BIOS settings

Installing BitLocker encryption on ISPC PC

It is recommended that PC is as clean as it can be (fresh installation).
PC needs to be in a domain ISPCARD/PC OU and be a member of a »GPO_PC_BITLOCKER« group.



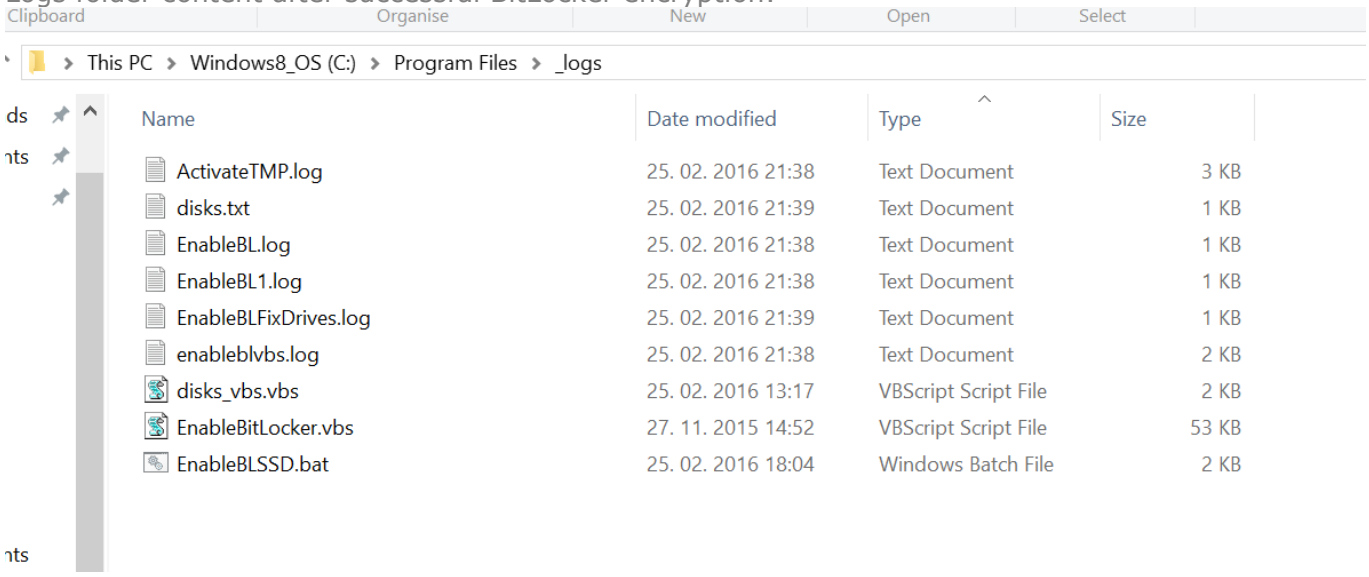
After that PC reboot is needed, it is recommended to run »`gpupdate /force`« before reboot.

TPM Activation: Some PCs already have TPM enabled and Activated in this case PC will automatically start BitLocker encryption upon boot. If TPM is not Activated PC will reboot and upon boot BIOS will ask you if you want to activate TPM and after reboot BitLocker encryption will start.

If Bitlocker Encryption does not start make sure that PC is in the right group in domain and GPO on PC is updated, you can run »gpupdate /force« in cmd to force GPO update.

Alternatively, you can check logs for errors. Logs are located in: »C:\Program Files_logs«

Logs folder content after successful BitLocker encryption:



If »_logs« folder does not exist GPO was not updated or PC is not a member of the right group or is not in right OU.

BitLocker Encryption can take from 30 minutes to couple of hours (depends on disk size and disk usage)

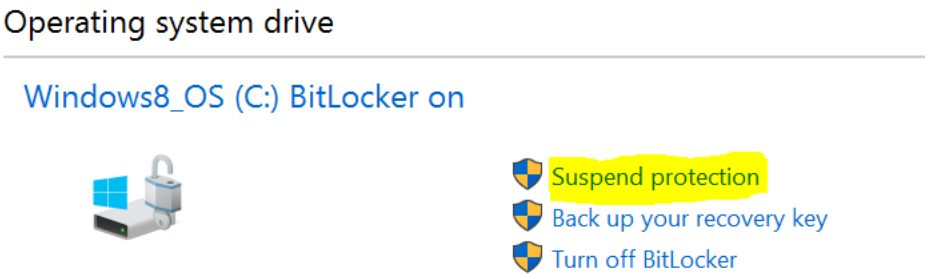
While BitLocker encryption is in progress PC is usable (can be slow) and can be even rebooted (after reboot Encryption proceeds automatically).

Non system drives are Read-only until encryption is complete.

Managing BitLocker Encrypted Computers for administrators

Changing or reconfiguring hardware or firmware (BIOS settings or update)

- Suspend BitLocker (only system drive)



- BIOS configuration
- Re-enable BitLocker (if needed, in most cases BitLocker after reboot re-enables automatically)

If TPM is not Suspended before BIOS changes PC will be marked as compromised and it will ask for BitLocker key. If this happens:

- Insert BitLocker Recovery key
- Suspend BitLocker
- Reboot PC
- Re-enable BitLocker

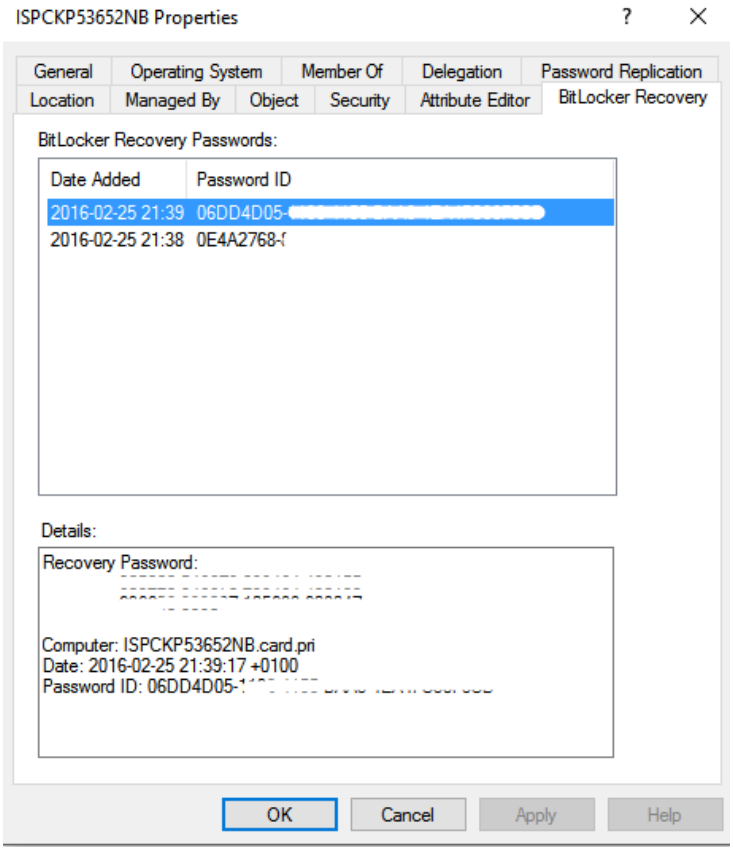
Updating Windows

- Windows can be updated without problems.

Location of BitLocker Recovery key.

When we enable BitLocker disk encryption, recovery key will automatically upload on domain and we can find it there:

- Find PC in domain
- Right click on it and open properties
- Recovery key is located under BitLocker Recovery tab



Checking Locally if PC have Disk Drives Encrypted

Status can be checked with CMD:

manage-bde –status

```
C:\WINDOWS\system32>manage-bde -status
BitLocker Drive Encryption: Configuration Tool version 10.0.10011
Copyright (C) 2013 Microsoft Corporation. All rights reserved.

Disk volumes that can be protected with
BitLocker Drive Encryption:
Volume C: [Windows8_OS]
[OS Volume]

    Size:                 234,19 GB
    BitLocker Version:    2.0
    Conversion Status:    Encryption in Progress
    Percentage Encrypted: 61,5%
    Encryption Method:    AES 128
    Protection Status:    Protection Off
    Lock Status:          Unlocked
    Identification Field: card.pri
    Key Protectors:
        TPM
        Numerical Password

Volume D: [DATA]
[Data Volume]

    Size:                 221,89 GB
    BitLocker Version:    2.0
    Conversion Status:    Encryption in Progress
    Percentage Encrypted: 72,7%
    Encryption Method:    AES 128
    Protection Status:    Protection Off
    Lock Status:          Unlocked
    Identification Field: card.pri
    Automatic Unlock:     Enabled
    Key Protectors:
        Numerical Password
        External Key (Required for automatic unlock)
```

or in Control panel under BitLocker Drive Encryption settings.

In case if secondary disk do not start Bitlocker Encryption it must be encrypted manualy:

Change "D:" with the letter of DATA disk.

```
manage-bde -on D: -rp
```

To enable autounlock of Data disk drive when system boots:

```
manage-bde -autounlock -enable D:
```

It is recommended to check if recovery key is succesfuly backed up on AD.

Add PIN to Startup for BitLocker protected System Drive

Additional option is enabled for adding PIN at startup if some users want to have it.

To enable PIN at startup GPO was changed a bit:

Require additional authentication at startup was changed so it allows startup PIN with TPM. Lenght of PIN is set to minimum of 5 and maximum of 20 numbers.

Only Administrators can enable BitLocker startup PIN.

Windows 7

To enable PIN at startup this command needs to be inserted in elevated command prompt:

```
manage-bde –protectors –add c: -TPMAndPIN
```

Windows 10

On Windows 10 PIN can be enabled the same way as on Windows 7 or via GUI:

Control Panel > System and Security > Bitlocker Drive Encryption

Chose how BitLocker is unlocked at startup and configure your PIN.