## Szyfrowanie danych na laptopach

Proces szyfrowania danych jest środkiem ostrożności, który ma na celu zminimalizowanie niebezpieczeństwa, że nieupoważnione podmioty wejdą w posiadanie danych zapisanych na urządzeniu. Spośród wielu dostępnych na rynku programów służących do szyfrowania danych, proponujemy wykorzystanie jednego z nich, o nazwie DiskCryptor, który jest udostępniany bezpłatnie na stronie <u>https://diskcryptor.net/wiki/Downloads</u>. Poniżej przedstawiamy informacje pomocne w procesie instalacji oprogramowania na urządzeniu wyposażonym w system Microsoft Windows 7.

## ETAP 1: Wykonanie kopii bezpieczeństwa, sprawdzenie systemu i przygotowanie do instalacji programu DiskCryptor

W pierwszej kolejności zaleca się wykonanie kopii bezpieczeństwa, tj. skopiowanie swoich plików na inny nośnik.

W kolejnym kroku należy sprawdzić, czy dysk w laptopie jest podzielony na partycje, bowiem szyfrowaniu będzie podlegać tylko jedna z nich. W tym celu należy z menu START wybrać pozycję Komputer, kliknąć prawy klawisz myszy i wybrać pozycję Zarządzaj.



Na ekranie pojawi się okno dialogowe:

🚁 Zarządzanie komputerem	and the state				ange man hann						x
<u>Plik Akja Widok Pomoc</u>											
(n 🔿 🖄 📰 🖉 🐨	X 🖆 🖻 🔍 😼										
🛃 Zarządzanie komputerem (loka	Wolumin	Układ	Тур	System plików	Stan	Pojemność	Wolne miejsce	% wolnego	Odpornoś	Akcje	
A 👔 Narzędzia systemowe	DATA (D:)	Prosty	Podstawowy	NTES	Zdrowy (Partycja podstawowa)	167,67 GB	147,45 GB	88 %	Nie	Zarządzanie dyskami	
Harmonogram zadań	Tastrzetone nrzez syst	Prosty Prosty	Podstawowy	NTES	Zdrowy (Kozruch, Plik stronicowania, Zrzut awaryjny, Partycja podstawowa Zdrowy (System, Aktowna, Partycja podstawowa)	<ol> <li>297,99 GB 100 MR</li> </ol>	222,62 GB 70 MB	75 % 70 %	Nie	Więcej akcji	•
Foldery udostępnione			· · · · · · · · · · · · · · · · · · · ·		Laterty (ayster), rangina, rangiga pousanonaj	200 100					
b 💩 Użytkownicy i grupy loł											
Wydajność											
Menedžer urządzeń	•										
Zarządzanie dyskami											
Usługi i aplikacje	Podstawowy Zast	zeżone pr.	zez syste 05	(C:)	DATA (D:)						
	Online Zdro	wy (System	, Aktywn: Zd	rowy (Rozruch, P	lik stronicowania, Zrzut awaryjny, Partycja podstawowa Zdrowy (Partycja p	odstawowa)					
	CD-ROM 0										
	DVD (E:)										
									-		
* m +	Nieprzydzielone P	rtycja pods	tawowa							l	

Rysunek nr 2.

W kolejnym kroku w lewej części okna dialogowego wybieramy pozycję Magazyn, a dalej Zarządzanie dyskami. Powyżej przedstawiono przykładowe okno dialogowe, w którym widoczne są 3 partycje (obszary danych) o nazwach: *OS (C:), DATA (D:)* i *Zastrzeżone przez system*. W zależności od konfiguracji Państwa komputerów partycje mogą się różnić.

Dane wrażliwe, które będą szyfrowane powinny znajdować się na partycji innej niż systemowa (zwykle oznaczonej literą C:). Jeżeli w Państwa komputerach jest tylko jedna partycja należy dokonać jej podziału. Zaleca się, aby podziału dysku na partycję dokonała osoba legitymująca się wiedzą i doświadczeniem informatycznym.

W przedstawionym przykładzie dane do szyfrowania znajdują się na partycji D:

## ETAP 2: DiskCryptor – instalacja i szyfrowanie danych

Proszę pobrać aplikację ze strony https://diskcryptor.net/wiki/Downloads i następnie uruchomić ją (plik o nazwie dcrypt setup.exe). Instalacja polega na zatwierdzaniu kolejnych komunikatów wyświetlanych na ekranie monitora. Zaleca się pozostawienie bez zmian ustawień domyślnych.

Po instalacji należy dokonać restartu systemu. Po restarcie, proszę uruchomić program o nazwie DiskCryptor z menu START/PROGRAMY. Możemy zostać poproszeni o zatwierdzenie otwarcia aplikacji. Klikamy kolejno przyciski "Uruchom" a następnie "Tak", aby kontynuować (rysunki nr 6 i 7).

Cay choesa unuchomić ten plik?	Cry choraz zezwolić następującemu programowi na wprowadzenie zmian na tym komputerze?
Typ: Aplikacja Od: DritteMPdorypt_setup.exe Usodnom Andaj	Matters programme Secretariany reprint & Basic Cyptor Lange Part Institutions pilots Profession 2 Statements
Zgwrze pyłaj przed otwarciem lego piłku Piki pochodzące z internetu mogą być użyteczme, ale ten typ piłku może tyć sakodowy da konzuczen. Unuchamaj wylącznie	100 Point monophy
Piki pochodzece z i terenetu moga być uzyteczne, ele ten typ piku moze być skotklavi da konzyman. Uuchanaji wykaznić oprogramowane pochodzące od zaufanych wydawców, <u>lakon iost</u> zastozenie?	Linus a trade a monomine a proved
unek nr 6	Rysunek nr 7

Na ekranie monitora pojawi się następujące okno dialogowe:

DiskCryptor 1.1.846.118					×
File Volumes Tools Help					Homepage
Disk Drives					Mount
Size	Label	Type	Status		
Hitachi HTS543280L9A300					Encrypt
	Zastrzeżone pr VeraCrypt	NTFS NTFS		boot	
🚍 E: 5.43 GB	DiskCreator	NTES			Married M.
C: 41.6 GB	OS	NTFS		sys	Mount All
all D: 0 bytes					Unmount All
Symbolic Link 11/1/Volume(33460)	id4-a25e-11e5-a5ba		3}		
Device (Device (Harddisk))	olume4				
Cipher					
Encryption mode Pkcs5.2 prf					
Info					

Rysunek nr 8.

Aby rozpocząć szyfrowanie danych za pomocą DiskCryptor wybieramy (zaznaczamy) wskaźnikiem myszy partycję, na której zapisane są dane do szyfrowania (w tym przykładzie jest to partycja D:) Proszę następnie kliknąć na przycisk "Encrypt". Powyższa akcja otworzy okno "ustawienia szyfrowania" (rysunek nr 9). W oknie tym można zmienić opcje: "Algorythm" i "Wipe Mode" lub pozostawić domyślne. Proszę wybrać przycisk "Next".

	ettings	
Algorithm:	AES	-
Nipe Mode:	None	•

Rysunek nr.9

DiskCryptor poprosi o hasło (rysunek nr 10). Wskazane jest, aby nadane hasło składało się z minimum 12 znaków, zawierało wielkie i małe litery oraz cyfry lub znaki specjalne. Po zakończeniu wprowadzania hasła dwukrotnie, klikamy na przycisk "OK", aby uruchomić szyfrowanie.

Volume Pa	ssword			
Password:	********			Show Password
Confirm:	*******			Use Keyfiles
Status:	Correct			Keyfiles
Layout:	QWERTY		Ŧ	
Password	Rating			
Unbrea			Digits	
		Caps Latin	Space	
		Small Latin		
Trivial	Breakable			
	01			

Rysunek nr 10.

Po zakończeniu procesu szyfrowania należy ponownie uruchomić komputer.

Po ponownym uruchomieniu sytemu zaszyfrowana partycja będzie widoczna, jednakże próba jej użycia zakończy się komunikatem:

Microsoft Windows	×
Przed użyciem dysku znajdującego się w dysków G: musisz go sformatować. Czy chcesz wykonać formatowanie?	stacji
Formatuj dysk A	nuluj

Rysunek nr 11.

Aby nie utracić danych zawartych na tej partycji należy wybrać opcję "Anuluj" i potwierdzić kolejny komunikat. W kolejnym kroku proszę wykonać czynności:

- uruchomić program DiskCryptor
- wskazać zaszyfrowaną partycję
- wybrać opcje "Mount" i potwierdzić wybranym wcześniej hasłem.

Więcej na temat szyfrowania można znaleźć pod adresami:

http://www.yac.mx/pl/pc-tech-tips/hardware/How to Use DiskCryptor to Encrypt Your Hard Drive.html http://www.yac.mx/pl/pc-tech-tips/windows/How\_to\_Use\_DiskCryptor\_to\_Encrypt\_Partitions\_in\_Windows.html https://diskcryptor.net/wiki/Main\_Page/pl

## UWAGA ważne!

Przy tego typu operacjach istnieje niewielkie ryzyko uszkodzenia lub utraty danych na nośniku, dlatego osoby nie mające doświadczenia powinny podchodzić bardzo ostrożnie do szyfrowania lub skorzystać z pomocy osób trzecich mających doświadczenie m.in. w zabezpieczeniu danych. Sąd Okręgowy w Warszawie nie ponosi odpowiedzialności za skutki uboczne i źle wykonane procedury związane z szyfrowaniem danych.