CRIPTAREA HARDDISK-ULUI CU UTILITARUL WINDOWS BITLOCKER

- parte a masurilor de securitate in vederea GDPR -

Una dintre masurile care trebuie luate in vederea alinierii la GDPR este securizarea datelor care se afla pe statiile de lucru, laptopurile, tabletele sau serverele din firma.

De la bun inceput, mentionez ca acest tutorial se refera numai la device-urile pe care ruleaza sistemul de operare Microsoft Windows. Utilitare asemanatoare pentru criptare sunt disponibile si pentru MacOS, iOS, UNIX sau Android.

Eu am optat pentru folosirea utilitarului care se regaseste deja integrat in sistemul de operare, si anume *BitLocker*. Acest utilitar este disponibil pentru Windows Professional, Windows Enterprise, Windows Server. Nu este disponibil pentru Windows Home Edition. Varianta de Windows pe care eu am lucrat este Windows 10 Professional, dar utilitarul este disponibil incepand cu Windows Vista. De asemenea, pentru toate operatiunile descrise mai jos sunt necesare drepturi de Administrator.

BitLocker este gratuit (dupa cum am mentionat vine preinstalat in Windows), algoritmul de criptare folosit este pe 128 sau 256 biti, iar criptarea se face hardware (daca device-ul este echipat cu *Trusted Platform Module* 1.2 minim – fig.1) sau software.

Acest tip de criptare face extrem de grea accesarea datelor de catre persoanele neautorizate, in caz de furt sau pierdere a device-ului, chiar si in eventualitatea conectarii hard-disk-ului la alt PC.

Device Manager		×
File Action View Help		
> 💻 Computer		^
> Disk drives		
> La Display adapters		
> WDV/CD-ROM drives		
> M Human Interface Devices		- 1
> The ATA/ATAPI controllers		
> 👘 Imaging devices		
> Explored s		
> Winde and other pointing devices		
> 💼 Modems		
> Monitors		
> P Network adapters		
Detable Daviers		
Portable Devices		
Print queuer		
Security devicer		
Trusted Distform Module 1 2		
Software devices		
Sound video and game controllers		
Se Storage controllers		
Sustem devices		
Universal Serial Bus controllers		
T superside and the controllers		V

Inainte de inceperea criptarii, va trebui sa activati doua optiuni in *Local Group Policy Editor*. Pentru aceasta apasati tastele Win + R, si scrieti *gpedit.msc* (fig.2).



Figure 2

In Local Group Policy Editor, navigati la Computer Configuration – Administrative Templates – Windows Components – BitLocker Drive Encryption – Operating System Drive.

Aici trebuie sa setati *Enable* doua optiuni (fig.3):

- 1. Require additional authentification at startup
- 2. Enable use of BitLocker authentification requiring preboot keyboard input on slates (fig.5)

Action View Help					- w.
Windows Components					
 Windows Components A ActiveX Installer Service Add features to Windows App Privacy App Privacy App Intime Application Compatibility AutoPlay Policies BitLocker Drive Encryption Field Data Drives Operating System Dri Removable Data Drive Connect Credential User Interface Delivey Optimization Delivey Gsdgets Destrop Gadgets Destrop Window Manage 	Operating System Drives Select an item to view its description.	Setting Allow network unlock at startup Allow Secure Boot for intentity validation Beguine additional authentication at startup Carling and authentication at startup Allow devices compliant with InstantGo or HSTI to opt out o Allow devices compliant with InstantGo or HSTI to opt out o Allow devices compliant with InstantGo or HSTI to opt out o Allow devices compliant with InstantGo or HSTI to opt out o Configure use of BitLocker authentication requiring preboot ke Configure use of passwords for operating system drives Configure TPM platform validation profile (Vindows State, Configure TPM platform validation profile for native UEEI fri Configure TPM platform validation profile for native UEEI fri Configure TPM platform validation profile for native UEEI fri Configure TPM platform validation profile for native UEEI fri Configure TPM platform validation profile for native UEEI fri Configure TPM platform validation profile for native UEEI fri Configure TPM platform validation profile for native UEEI fri Configure TPM platform validation profile for native UEEI fri Configure TPM platform validation profile for native UEEI fri Configure TPM platform validation profile for native UEEI fri Configure TPM platform validation profile for native UEEI fri Configure TPM platform validation profile for native UEEI fri	State Not configured Not configured	Comment No No No No No No No No No No No No No	
Device and Driver Compri Device Registration Digital Locker Edge UI Event Forwarding Event Log Service Event Log Service Event Logging Event Viewer File History Find My Device Gome Explorer Handwriting		E Reset platform validation data after BitLocker recovery E Use enhanced Boot Configuration Data validation profile	Not configured	No No	
>	Extended Standard				
3(5)					

La optiunea nr.1, trebuie sa avem grija ca, odata bifat *Enable*, sa fie bifat si *Allow BitLocker without a compatible TPM* (aceasta bifa este necesara in cazul in care sistemul nu este prevazut cu un modul de criptare hardware) (fig.4)



Figure 4

d Group Policy Edito						- 0
💭 Enable use of Bitl	ocker authenticat	ion requiring preboot keyboard input on slates 🛛 🚽 🗙				
Enable use of Bit	.ocker authentica	tion requiring preboot keyboard input on slates				
Previous Setting	Next Setting			State	Comment	
) Not Configured	Comment	· · · · · · · · · · · · · · · · · · ·	7	Not configured	No	
Enabled				Not configured	No	
) Disabled	a este a como co	2	Windows Serve PIN or password	Not configured Not configured	No	
	Supported on:	At least Windows Server 2012 or Windows 8	HSTI to opt out o	Not configured	No	
ptions:		Help:		Not configured Not configured	No	
		This policy setting allows users to turn on authentication options that require user input from the pre-boot environment, even if the platform lacks pre-boot input capability.	n for operating s system drives stem drives	Not configured Not configured Not configured	No No No	
		The Windows touch keyboard (such as that used by tablets) ion't available in the pre-boot environment where BitLocker requires additional information such as a PIN or Password.	system drives ca or BIOS based fi Windows Vista, or pative UFEI fir	Not configured Not configured Not configured	No No No	
		If you enable this policy setting, devices must have an alternative means of pre-boot input (such as an attached USB keyboard).	JRL er recovery	Not configured Not configured	No No	
		If this policy is not enabled, the Windows Recovery Environment must be enabled on tablets to support the entry of the Bitacker recovery password. When the Windows Recovery Environment is not enabled and this policy is not enabled, you cannot turn on BitLacker on a device that uses the Windows touch keyboard.	dation profile	Not configured	No	
		Note that if you do not enable this policy setting, options in the "Require additional authentication at startup" policy might not				
		OK Cancel Apply]			
Handwriti	ng v	enabled, you cannot tum on BitLocker on a device that uses the				
- "	>	Extended Standard				
g(s)						

Figure 5

Odata facute aceste setari, se poate incepe criptarea hard-disk-ului.

Pentru aceasta, vom deschide *This PC*, click dreapta pe drive-ul C, iar din meniul derulant vom selecta *Turn On BitLocker* (fig.6).



Figure 6

In continuare, se vor urma instructiunile pentru introducerea unei parole sau a unui PIN (fig. 7 si 8) si modalitatea de stocare a backup-ului parolei. Aici, eu am ales varianta printarii, dar puteti alege oricare dintre optiuni, in functie de preferinte (fig.9)



	Drive Tools	This PC	12	- 🗆 🗙
File Computer V	/iew Manage		-	~ 📀
Properties Open Rename	Access Map n media - driv	- StatLocker Drive Encryption (C:)		
Location $\leftarrow \rightarrow \sim \uparrow \blacksquare \rightarrow Th$	his PC >	Create a password to unlock this drive	ູ ບັ Search This PC	٩
A Quick access	✓ Folders (You should create a strong password that uses uppercase and lowercase letters, numbers, symbols, and spaces.		
Desktop 🖈		Enter your password		
👆 Downloads 🖈		•••••		
🔮 Documents 🖈		Reenter your password		
Pictures 🖈	-	•••••••		
J Music				
Videos				
Desktop	E.			
Chebrive	✓ Devices a			
This PC				
3D Objects	-	Tips for creating a strong password.		
Desktop				
🔮 Documents		Next Cancel		
🕹 Downloads	-			
10 items 1 item selected	1			8:3

Figure 8



Figure 9

In ferestrele urmatoare se vor selecta optiunile *New encryption mode* si *Run BitLocker System Check*, apoi *Restart now* (fig.10, 11 si 12).



Figure 10



Figure 11



Figure 12

Dupa restart, va aparea, inainte de incarcarea sistemului de operare, o fereastra prin care se solicita parola sau PIN-ul setate mai devreme (fig.13)

BitLocker
Enter the password to unlock this drive
Press the Insert key to see the password as you type.
Press Enter to continue Press Esc for BitLocker recovery



Dupa incarcarea sistemului de operare, criptarea hard-disk-ului va continua in background.

Daca hard-disk-ul este partitionat, va trebui sa reluati procedura pentru fiecare partitie.