Czy dysk komputera, na którym pracuję, jest zaszyfrowany bez mojej wiedzy i świadomego działania?.

Tak postawione pytanie może wprawić w zdumienie użytkownika.

Oznaczałoby to, że ktoś (pirat) zaszyfrował mój dysk w celu uzyskania korzyści (zapłać – albo pożegnaj się z danymi na dysku), a przecież po włączeniu komputera system podnosi się normalnie – nic mnie nie pyta o podanie klucza. Dane na swoim miejscu, czytelne. Jakie więc szyfrowanie ?.

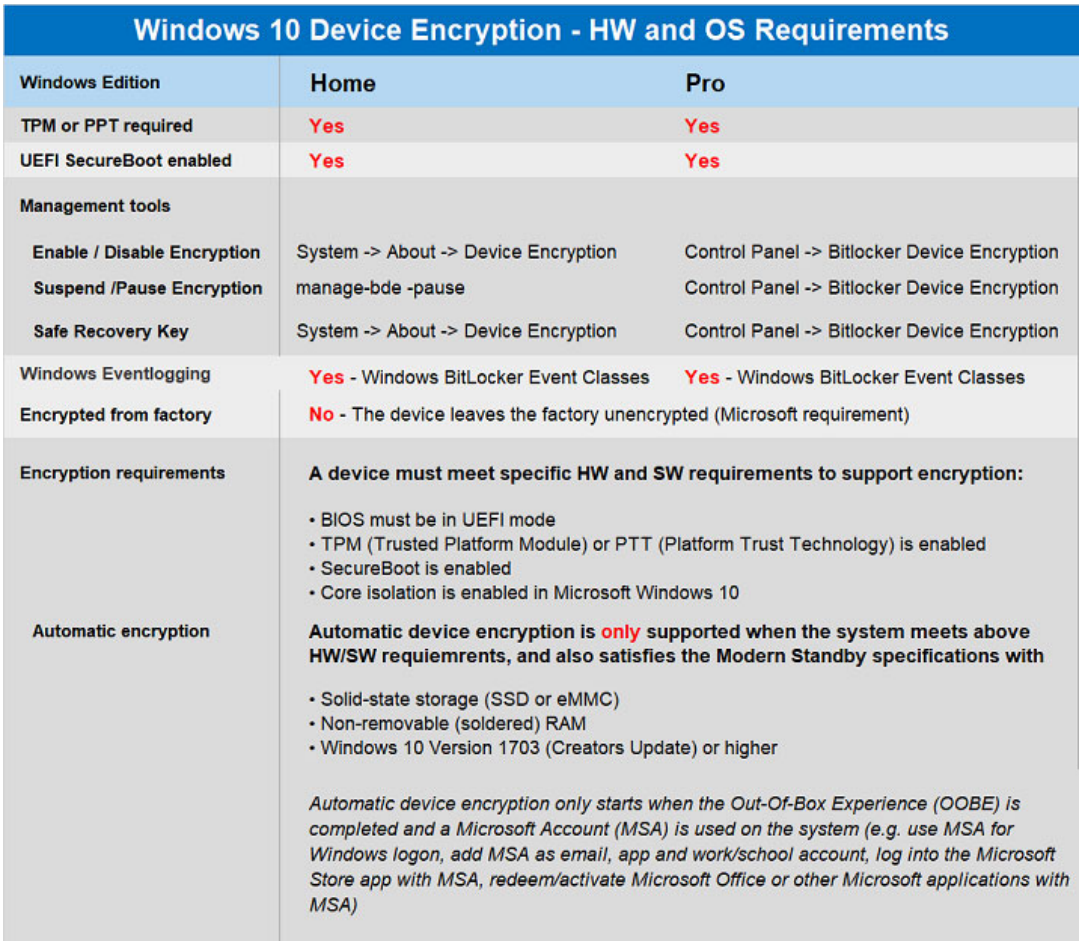
Z podobnym scenariuszem można się spotkać, kiedy staliśmy się ofiarą ataku typu Ransomware. Jest jednak zasadnicza różnica – wirus szyfruje tylko użyteczne dane (dokumenty, zdjęcia, itp.), podczas gdy Bitlocker (mechanizm wdrożony i rozwijany przez Microsoft, nawiasem mówiąc, bardzo dobry) – cały dysk. Tak zaszyfrowany dysk, wyjęty z komputera i włożony do innego, bez hasła, jest niedostępny.

Niestety tym „kimś" może być firma Microsoft – z tym, że nie chodzi tu o korzyść materialną. Raczej o daleko posuniętą „troskę" o bezpieczeństwo danych użytkownika. Wielki Brat wie lepiej i pragnie Cię uszczęśliwić nawet wbrew Twojej wiedzy. Czy Państwu to czegoś nie przypomina?.

Scenariusz implementacji.

1. Komputer musi być stosunkowo „nowy", np. ostatnio zakupione w przetargu AGH niektóre notebooki HP i komputery typu „All in One" firmy Dell.
2. W Biosie komputera muszą być włączone pewne ustawienia (UEFI, SecureBoot, TPM, itd.). Niestety, najczęściej domyślnie, są.
3. W systemie Windows 10, musi być włączona izolacja rdzenia. W maszynach, które na to pozwalają - najczęściej jest. Np.,: automatyczne włączanie na Dell OEM Windows 10 Factory Image.

4. W systemie używane jest konto Microsoft (MSA).



Windows 10 Device Encryption - HW and OS Requirements		
Windows Edition	**Home**	**Pro**
TPM or PPT required	Yes	Yes
UEFI SecureBoot enabled	Yes	Yes
Management tools		
Enable / Disable Encryption	System -> About -> Device Encryption	Control Panel -> Bitlocker Device Encryption
Suspend /Pause Encryption	manage-bde -pause	Control Panel -> Bitlocker Device Encryption
Safe Recovery Key	System -> About -> Device Encryption	Control Panel -> Bitlocker Device Encryption
Windows Eventlogging	Yes - Windows BitLocker Event Classes	Yes - Windows BitLocker Event Classes
Encrypted from factory	No - The device leaves the factory unencrypted (Microsoft requirement)	
Encryption requirements	**A device must meet specific HW and SW requirements to support encryption:** • BIOS must be in UEFI mode • TPM (Trusted Platform Module) or PTT (Platform Trust Technology) is enabled • SecureBoot is enabled • Core isolation is enabled in Microsoft Windows 10	
Automatic encryption	**Automatic device encryption is only supported when the system meets above HW/SW requiemrents, and also satisfies the Modern Standby specifications with** • Solid-state storage (SSD or eMMC) • Non-removable (soldered) RAM • Windows 10 Version 1703 (Creators Update) or higher *Automatic device encryption only starts when the Out-Of-Box Experience (OOBE) is completed and a Microsoft Account (MSA) is used on the system (e.g. use MSA for Windows logon, add MSA as email, app and work/school account, log into the Microsoft Store app with MSA, redeem/activate Microsoft Office or other Microsoft applications with MSA)*	

Rys. 1

Nie wgłębiając się w dalsze szczegóły- jeśli zaistnieją właściwe warunki, dysk po krótkim czasie użytkowania jest zaszyfrowany, a klucz szyfrowania POWINIEN się znaleźć na koncie Microsoft.

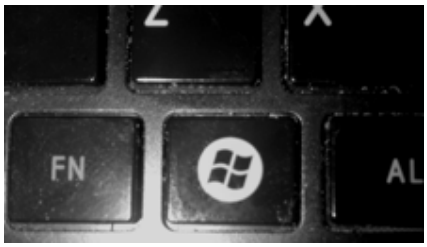
Proszę zwrócić uwagę na ostatni akapit Rys. 1. „Automatyczne szyfrowanie urządzeń uruchamia się tylko po zakończeniu pracy po włączeniu systemu (OOBE), a w systemie jest używane konto Microsoft (MSA) (np. Użyj konta MSA do Windows logowania, Dodaj element MSA jako wiadomość e-mail, aplikację i konto służbowe, zaloguj się do aplikacji Microsoft Store z użyciem konta MSA, Zrealizuj lub Aktywuj Microsoft Office lub inne aplikacje Microsoft z kontem MSA)”.

Wszystko co napisałem powyżej może wydawać się nieco skomplikowane. Dla przeciętnego użytkownika istotne jest:

CZY MÓJ DYSK JEST ZASZYFROWANY ?.

Sprawadzamy:

1. Klawisz Windows (logo systemy Windows) + R



2. Wpisujemy: diskmgmt.msc + Enter
3. Na dysku C patrzymy na opis. Normalnie powinniśmy zobaczyć: „zdrowy, rozruch, partycja podstawowa”. Dodatkowo, jeśli zobaczymy „zaszyfrowano Funkcją BitLocker” – nasz dysk jest zaszyfrowany.I co teraz?. Jak najszybciej powinniśmy ten klucz znaleźć.

Zaloguj się do konta Microsoft innego urządzenia, aby znaleźć klucz odzyskiwania:

- ***Jeśli posiadasz nowoczesne urządzenie, które obsługuje automatyczne szyfrowanie urządzeń, klucz odzyskiwania powinien znajdować się na koncie Microsoft.dows 10.***
- ***Jeśli urządzenie zostało skonfigurowane lub ochrona funkcją BitLocker została aktywowana przez innego użytkownika, klucz odzyskiwania może znajdować się w tym Microsoft koncie.***

Jeśli uda się klucz znaleźć, należy go bezzwłocznie zapisać.

Jeśli nie (a często to się zdarza) – mamy problem.

Klucz nie jest potrzebny dla normalnej pracy. Ale prędzej czy później pojawi się sytuacja awaryjna, a tu bez klucza nie naprawimy systemu, ani nie odzyskamy danych. Dodatkowo, podczas aktualizacji Biosu, albo przywracania systemu z kopii zapasowej, może dojść do utraty danych.

WNIOSKI.

1. Nowo zakupiony komputer z preinstalowanym systemem należy bezzwłocznie przekazać do serwisu. Raz, że preinstalowany system jest zawsze przestarzały (aktualizacje zwiększą bałagan). Dwa, na takim komputerze zainstalowano wiele niepotrzebnych programów producenta (CrapWare), obciążających system i rejestrujących nasze działania. Nie będzie również takich niespodzianek jak szyfrowanie.
2. W sytuacji zaszyfrowanego dysku, najlepiej zwrócić się o pomoc do specjalistów i indywidualnie ustalić tok dalszego postępowania - dopóki nie jest za późno.