V SOULADU S GDPR? JSTE

VAŠE SOUKROMÍ JE DŮLEŽITÉ

Uchovávání dat v bezpečí na cestách je velmi důležité – nejen pro podniky, ale také s osobní perspektivy.

Co když si zaměstnanec vezme data zákazníka domů na pevném disku a cestou ho ztratí nebo mu ho někdo ukradne? Co když někam založíte flashdisk USB s bankovními záznamy?

Celosvětově se každý rok poztrácí více než dva miliony těchto malých úložných zařízení a studie ukazují, že více než polovinu ztracených flashdisků USB někdo opět připojí.

Tomuto riziku lze čelit jednoduše pomocí šifrovaných zařízení, která zakódují data tak, že je dokáže přečíst jen někdo se správným kódem nebo klíčem.

Můžete si dovolit svá data **nešifrovat**?

Verbatim™

Technology you can trust

VĚDĚLI JSTE...?

14,717,618,286

ZTRACENÉ ČI ODCIZENÉ DATOVÉ ZÁZNAMY OD ROKU 2013

Pouze ve **4 %** případů byla tato data **šifrována**, a zlodějům tak nebyla k ničemu.

Z celkového počtu odcizených záznamů došlo k nejvyššímu nárůstu bezpečnostních incidentů v sektoru **sociálních médií**, a to z 1,51 % v roce 2017 na **56,18 %** v roce 2018. V tomto časovém období zaznamenaly významný pokles incidenty v sektoru zdravotnictví. Za první polovinu roku 2018 zaznamenaly sektory veřejné správy, vzdělávání, zábavy, finančních služeb a neziskových aktivit **o 50–100 % méně narušení bezpečnosti** než za předchozí rok.

Zdroj: Breach level index 17/04/19

FREKVENCE ZTRÁTY ČI ODCIZENÍ DAT

Každý den	Každou hodinu	Každou minutu	Každou sekundu
6 404 534	266 856	4 448	74

CO JE GDPR?

GDPR – OBECNÉ NAŘÍZENÍ O OCHRANĚ OSOBNÍCH ÚDAJŮ

Zavedením GDPR došlo ke sjednocení legislativy na ochranu osobních údajů na jednotném evropském trhu.

Díky tomu mají podniky jednodušší a jasnější právní prostředí, ve kterém se mohou pohybovat, a lidé větší slovo v tom, co společnosti smějí s jejich údaji dělat.

Zavádí se také přísnější pokuty pro společnosti, které nařízení nedodržují. Organizace mohou dostat pokutu až 4 % ročního obratu nebo 20 milionů €.

Kvůli tomu všemu je potřeba zajistit, aby byly vaše kritické a citlivé údaje vhodně chráněny, důležitější než kdy předtím.

MALWARE V KOSTCE

Viry: Připojením k souborům nebo infikováním dalších souborů se mohou nekontrolovatelně šířit, a poškodit tak základní funkce systému a smazat nebo zničit soubory.

Rootkity: Software, který umožňuje útočníkovi získat administrátorský přístup k počítačovému systému. Často bývá skrytý a nemusí si ho všimnout ani antivirus.

Spyware: Program, který se skrývá na pozadí, sleduje uživatele a zaznamenává si jejich činnost online, včetně hesel, čísel kreditních karet, chování při procházení webu a dalších věcí.

Trojské koně: Vydávají se za legitimní software a uživatel si je stáhne, protože si myslí, že je to něco užitečného. Místo toho však dojde k infikování počítače.

Červi: Jedná se o automaticky se kopírující programy, které mají za úkol šířit škodlivý kód. Pomocí síťových rozhraní mohou infikovat celé sítě, jak místní, tak po celém internetu.

Ransomware je typ malwaru se schopností nepozorovaně šifrovat vaše soubory a znemožnit vám práci se systémem, aby po vás mohl požadovat výkupné výměnou za klíč pro dešifrování.

256BITOVÉ ŠIFROVÁNÍ AES

CO JE 256BITOVÉ ŠIFROVÁNÍ AES?

AES je zkratka z anglického Advanced Encryption Standard, tedy pokročilý standard šifrování. Jedná se o symetrickou blokovou šifru, která se používá po celém světě k šifrování citlivých dat.

256bitové označuje délku klíče pro šifrování datového toku nebo souboru. K prolomení zprávy s 256bitovým šifrováním musí hacker nebo cracker vyzkoušet 2^{256}* různých kombinací.

Šifrování AES nikdy nebylo prolomeno a je bezpečné před útoky hrubou silou.

*2^{256} = 115 792 089 237 316 195 423 570 985 008 687 907 853 269 984 665 640 564 039 457 584 007 913 129 639 936

ÚLOŽNÁ ZAŘÍZENÍ S ODEMYKÁNÍM OTISKEM PRSTU

Využívají vaše jedinečné biometrické údaje ke kompletnímu zabezpečení dat

EXTERNÍ DISK
FINGERPRINT SECURE

- Přenosný pevný disk USB-C™ s integrovanou čtečkou otisků prstů
- Přístup pomocí otisku prstu oprávněného uživatele
- 256bitové hardwarové šifrování AES
- Až osm oprávněných uživatelů se zadaným otiskem prstu plus jeden správce (pomocí hesla)
- Ukládání a přenášení důvěrných údajů s ochranou před ztrátou a hackováním
- Kabel USB-C™ na USB-A a adaptér USB-C™
- Součástí je zálohovací software Nero

53650 1 TB | 53651 2 TB

USB DISK
FINGERPRINT SECURE

- Elegantní hliníkový disk USB 3.0 s integrovanou čtečkou otisků prstů
- Přístup pomocí otisku prstu oprávněného uživatele
- 256bitové hardwarové šifrování AES
- Až pět autorizovaných uživatelů a jeden správce
- Ukládání a přenášení důvěrných dat s ochranou před ztrátou a hackováním

49337 32 GB | 49338 64 GB | 49339 128 GB

USB DISK SECURE PRO

ŠIFROVANÝ DISK USB

- Povinné 100% šifrování disku
- Až 12místné heslo
- 256bitové hardwarové šifrování
- Předem nahraná intuitivní aplikace zabezpečení s automatickým spouštěním
- Algoritmus hashování hesla
- Zadávání hesla odolné vůči narušení – po 10 neúspěšných pokusech se disk vymaže
- Na hostitelském počítači nejsou vyžadována práva správce
- Kompatibilní s PC i Mac

98664 16 GB | 98665 32 GB | 98666 64 GB

ÚLOŽNÁ ZAŘÍZENÍ S PŘÍSTUPEM POMOCÍ KÓDU PIN

Pro přístup k datům vyžaduje zadání osobního kódu

SECURE PORTABLE HDD S NUMERICKOU KLÁVESNICÍ

- Povinné 100% 256bitové hardwarové šifrování AES
- 5- až 12místné heslo
- Zálohovací software NERO
- Kompatibilní s počítačem MAC i PC
- Type-C, USB 3.1 Gen 1
- Zadávání hesla odolné vůči narušení – po 20 neúspěšných pokusech vymaže data

53401 1 TB | 53403 2 TB

SECURE PORTABLE SSD S NUMERICKOU KLÁVESNICÍ

- Disky SSD využívají úložiště flash paměti pro vyšší rychlosti, výkon a spolehlivost
- Povinné 100% 256bitové hardwarové šifrování AES
- 5- až 12místné heslo
- Zálohovací software NERO
- Kompatibilní s počítačem MAC i PC
- Type-C, USB 3.1 Gen 1
- Zadávání hesla odolné vůči narušení – po 20 neúspěšných pokusech vymaže data

53402 256 GB

SECURE PORTABLE DISK USB S NUMERICKOU KLÁVESNICÍ

- 256bitové hardwarové šifrování AES bezproblémově šifruje všechna dat na disku v reálném čase
- Integrovaná numerická klávesnice pro zadávání kódu (až 12 číslic)
- Lze používat s televizí (funkce, která není k dispozici u běžných šifrovaných zařízení)
- LED indikátory napájení / stavu šifrování
- Kompatibilní s PC i Mac
- K dispozici ve verzi USB 3.0 nebo USB 3.1 GEN 1 s připojením USB-C™

USB 3.0: 49427 32 GB | 49428 64 GB | 49429 128 GB **USB-C™:** 49430 32 GB | 49431 64 GB | 49432 128 GB

SECURE Desktop HDD
Sada s pouzdrem S NUMERICKOU KLÁVESNICÍ

- Integrovaná numerická klávesnice pro zadávání kódu
- 256bitové hardwarové šifrování AES
- Pouzdro na pevný disk 3,5”
- Vhodné pro všechny standardní 3,5” interní pevné disky SATA
- Snadná instalace. Nejsou nutné podrobné technické znalosti
- Připojení USB-C™ na USB-A

53405

ZÁLOHOVÁNÍ A ARCHIVACE

Pravidelné zálohy chrání před náhodnou nebo záměrnou ztrátou dat, od hardwarových chyb a virů po lidskou chybu a krádež, protože je lze použít k obnovení původních datových souborů.

Volba správného média a procedury zálohování závisí na mnoha prvcích:

- Množství uložených dat
- Vnímaná hodnota dat
- Úroveň přijatelného rizika
- Doba, po kterou je třeba data uchovávat

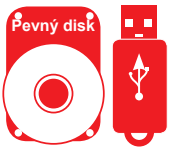
DOPORUČENÝ POSTUP – DODRŽUJTE PRAVIDLO ZÁLOHOVÁNÍ 3-2-1

3
MĚJTE NEJMÉNĚ TŘI KOPIE DAT

Kromě primárních dat byste také měli mít alespoň dvě další zálohy, což vám pomůže významně snížit riziko ztráty dat. Může jít o fyzická nebo cloudová řešení.

2
UKLÁDEJTE KOPIE NEJMÉNĚ NA DVOU TYPECH MÉDIÍ

Mezi osvědčené postupy patří uchovávání kopií dat alespoň na dvou typech úložišť, jako jsou interní jednotky pevného disku A vyměnitelná paměťová média (pásky, externí pevné disky, USB disky, SD karty, CD, DVD).



1
UCHOVÁVEJTE ALESPOŇ JEDNU KOPII MIMO PRACOVIŠTĚ

Je to vlastně zřejmé, ale není dobrý nápad uchovávat zařízení externího úložiště ve stejné místnosti jako produkční úložiště. Pokud dojde k požáru, zatopení nebo vloupání, přijdete o všechna svá data.

NEJLEPŠÍ OCHRANA PŘED ÚTOKEM ARCHIVUJTE SVÁ DATA

K úplné ochraně musí mít uživatel nebo organizace data zálohovaná a archivovaná offline.

Každé zařízení připojené k napadenému systému nebo síti je zranitelné.

Pokud je váš záložní pevný disk připojen k notebooku, když je nainstalován software ransomwaru, bude také zašifrován. Toto riziko může vyloučit archivace nejdůležitějších dat na optická média.

OPTICKÁ MÉDIA A MECHANIKY K ARCHIVACI

- Média Blu-ray, DVD, CD – nejlepší řešení pro dlouhodobé uchovávání (25–100 let)
- Používejte s externími vypalovačkami disků Blu-ray a DVD Verbatim
- Software Nero Burn&Archive je s vypalovačkami disků DVD a Blu-ray Verbatim zdarma

43888 | 43889 | 43890 | 98938 | 43894

TAŠKY SE ZABEZPEČENÍM RFID

ZABEZPEČENÉ TAŠKY S KAPSOU CHRÁNĚNOU POMOCÍ RFID

- Součástí řady jsou tašky na kolečkách, batohy, tašky na fotoaparáty, pouzdra na notebooky, brašny na zásilky
- Součástí je speciální kapsa zabezpečená čipy RFID na ochranu před naskenováním kreditních karet

Paris 49852 | London 49855

V SOULADU S GDPR? JSTE

Centrála Verbatim

Verbatim GmbH
Düsseldorfer Str. 13,
D - 65760 Eschborn,
Německo
T: +49 (0) 6196 900 10
E: info.germany@verbatim-europe.com

Verbatim™
Technology you can trust

www.verbatim-europe.cz/security