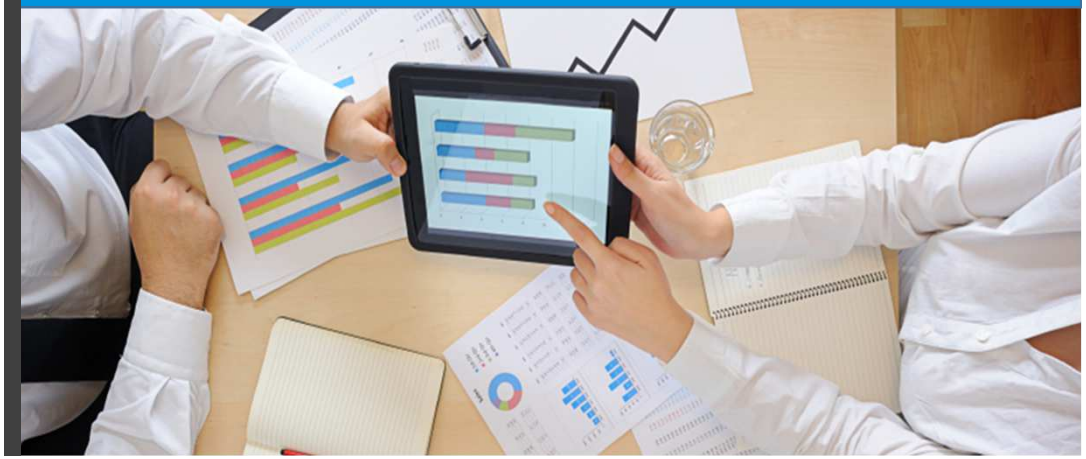
www.asociacebezpecnaskola.cz

ASOCIACE BEZPEČNÁ ŠKOLA

Fyzická ochrana datových úložišť



ASOCIACE BEZPEČNÁ ŠKOLA

Bezpečnost dat lze rozdělit celkem do čtyř bezpečnostních skupin:

- Fyzická
- Provozní
- Síťová
- Ochrana dat (ve smyslu replikace, zálohování, šifrování, archivace atd.)

Fyzickým zabezpečením dat se rozumí zabezpečení datových úložišť před neoprávněnou manipulací a krádeží.

Krádež dat ze serveru či jiného úložiště – byť uzavřeného v samostatné místnosti – je poměrně vysokým rizikem.

- náhodný zloděj, který se vloupá do objektu
- zaměstnanci, kteří fyzicky „navštíví“ nezabezpečené prostory a vyjmou HDD s daty, anebo si ho alespoň zkopírují.

Řada škol má navíc servery umístěny v běžných kancelářích, což tato rizika ještě zvyšuje.

ASOCIACE BEZPEČNÁ ŠKOLA

Odpovědnost správce dle GDPR - článek 24

1. S přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob zavede správce vhodná technická a organizační opatření, aby zajistil a byl schopen doložit, že zpracování je prováděno v souladu s tímto nařízením. Tato opatření musí být podle potřeby revidována a aktualizována.

2. Pokud je to s ohledem na činnosti zpracování přiměřené, zahrnují opatření uvedená v odstavci 1 uplatňování vhodných koncepcí v oblasti ochrany údajů správcem.

Příklad kamerový systém: Za provoz kamerového systému je vždy primárně odpovědný správce, který rozhodl o provozování kamerového systému. Podle výše uváděného článku musí správce s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob zavést vhodná technická a organizační opatření, aby zajistil a byl schopen doložit, že zpracování je prováděno v souladu s tímto nařízením.

ASOCIACE BEZPEČNÁ ŠKOLA

Odpovědnost správce dle GDPR - článek 24

Již dnes by mělo být běžné, že **provoz kamerového systému a jeho datové úložiště je zabezpečen proti neoprávněnému přístupu.**

Vhodným technickým opatřeními rozhodně není umístění těchto zařízení volně na recepci, vrátnici, pod stolem sekretářky a další často viděná řešení.

Provozovatel bude muset tato zařízení umístit nejlépe do místností typu „serverovna“, datové centrum nebo (alespoň) do samostatného rozvaděče typu rackové skříně, která bude uzamykatelná.

ASOCIACE BEZPEČNÁ ŠKOLA

Bezpečnostní technika pro fyzickou bezpečnost dat

Bezpečnostní technologie, vyžadují na provozovateli určitou míru znalosti na úrovni uživatele a správce. Předpokládá se údržba dle pokynů výrobce a v neposlední řadě znalost legislativy, která užívání a implementaci určitých systémů koriguje.

Základní pravidla:

- Slaboproudé systémy by měl navrhovat specialista v oboru s patřičnými oprávněními dovozců a výrobců.
- Systém by měl mít – minimálně při předání – projekt skutečného provedení.
- Systémy z oblasti požárně bezpečnostních řešení lze zadat pouze firmám s platným oprávněním k projektu, montáži a údržbě těchto systémů.
- Pravidelný servis a periodické prohlídky výrazně zvyšují bezpečnost, prodlužují životnost systémů a eliminují jejich selhání.
- Většina popsaných slaboproudých systémů je v základu bezobslužná, nikoliv bezúdržbová!

Ukázka chybně instalované techniky ve škole:

ASOCIACE BEZPEČNÁ ŠKOLA

Ukázka chybně instalované techniky ve škole:

ASOCIACE BEZPEČNÁ ŠKOLA

Ukázka chybně instalované techniky ve škole:

ASOCIACE BEZPEČNÁ ŠKOLA

ASOCIACE BEZPEČNÁ ŠKOLA

PZTS:
- ČSN CLC/TS 50131-7
- ČSN EN 50131-1 ed. 2

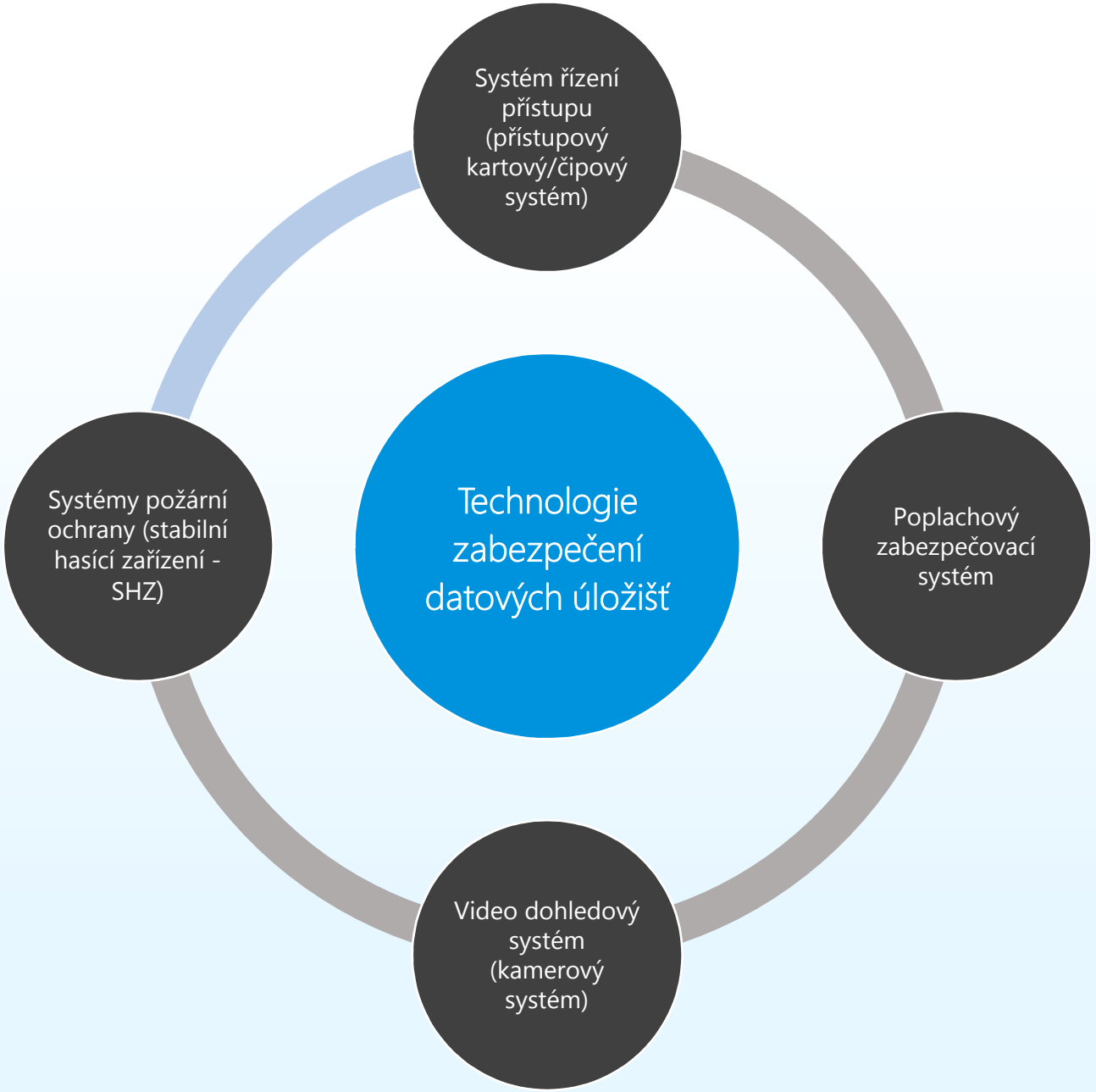
VSS (CCTV):
- ČSN EN 62676-1-1
- ČSN EN 62676-1-2
- ČSN EN 62676-4

Přístupové systémy (ACS):
- ČSN EN 60839-11-1 Požadavky na systém a komponenty
- ČSN EN 60839-11-2 Pokyny pro aplikace

Požární systémy:
- Vyhláška 246/2001 Sb.
- Vyhláška 23/2008 (ve znění pozdějších předpisů)
- Normy řady ČSN 73 08xx

Systémy zabezpečení místností s datovými úložišti:

ASOCIACE BEZPEČNÁ ŠKOLA



ASOCIACE BEZPEČNÁ ŠKOLA

Vstup(y) do místnosti s datovým úložištěm:

- všechny dveře zavřené, dveře odpovídající požadované bezpečnostní třídě dle například ČSN 73 4400 tabulka č.1
- vybaveny bezpečnostním zámkovým systémem ideálně elektromotorické zámky
- čtečka přístupového systému (ACS) na vstupu s jasnou identifikací vstupující osoby a centrálním nastavením oprávnění pro vstup
- klávesnice PZS pro vypnutí (vyjmutí) prostor úložiště ze stavu střežení
- kontakt neoprávněného otevření dveří zapojený do PZS
- kamerový systém snímající vstupní dveře

Uvnitř místnosti:

- pohybové detektory zapojené do PZS
- pokud jsou okna – detekce pomocí audio detektorů (rozbití skla) a detekce pomocí magnetických kontaktů (otevření oken)
- jednotlivé „rackové skříně“ osazeny magnetickým kontaktem pro snímání stavu jejich neoprávněného otevření
- monitorováno kamerou v dostatečném pokrytí
- monitoring teploty v rackových skříní

ASOCIACE BEZPEČNÁ ŠKOLA

Požární bezpečnost:

- detektory EPS (pokud je systém EPS instalován)
- Stabilní hasící zařízení (plynové) - SHZ

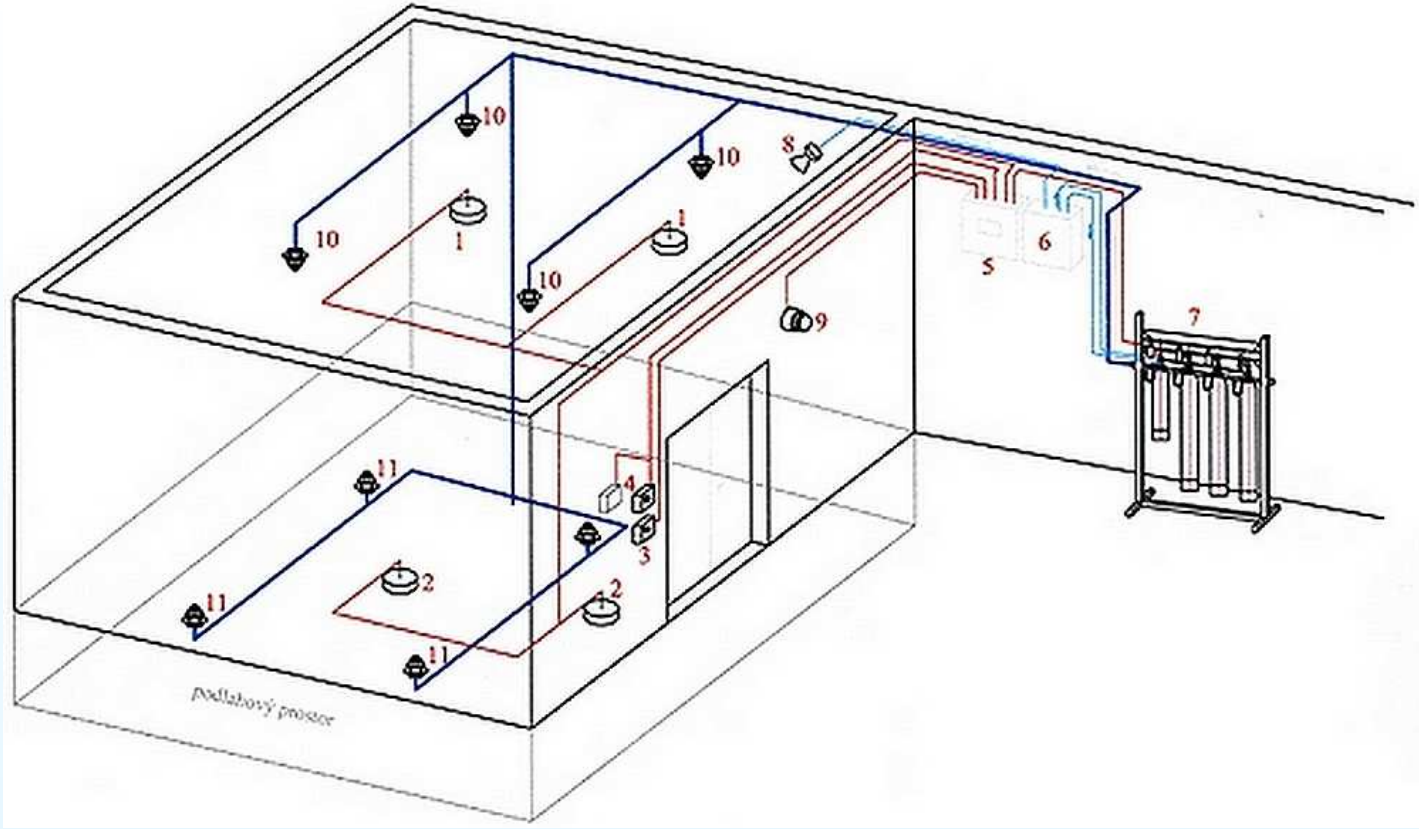
Výstupy bezpečnostních systémů:

- trvalá přítomnost obsluhy pro okamžitou detekci poplachu
- Napojení na DPPC (dříve Pult centrální ochrany)

Co to je Stabilní hasící zařízení

- Plynové stabilní hasicí zařízení se používají na hašení požárů v prostorech, kde by se aplikováním běžných hasicích prostředků jako je voda nebo pěna, mohla vzniknout větší škoda na majetku než by způsobil samotný požár.
- Princip hašení u chemických plynů spočívá v absorbování tepla, v důsledku čeho se oheň oslabí a udusí. Inertní plyny snižují koncentraci kyslíku v prostorech, v důsledku čeho se požár uhasí. Systém se uvádí do činnosti automaticky elektrickou požární signalizací prostřednictvím hlásičů, nebo se systém může spustit ručně.

Stabilní hasící zařízení – příklad:



PŘÍKLAD ZABEZPEČENÍ

ASOCIACE BEZPEČNÁ ŠKOLA

Proč řešit fyzická bezpečnostní opatření

ASOCIACE BEZPEČNÁ ŠKOLA

Provozovatel (správce) má novou povinnost. Jakékoli porušení zabezpečení osobních údajů správce bez zbytečného odkladu a pokud možno do 72 hodin od okamžiku, kdy se o něm dozvěděl, ohlásí dozorovému úřadu příslušnému podle článku 55, ledaže je nepravděpodobné, že by toto porušení mělo za následek riziko pro práva a svobody fyzických osob.

Pokud není ohlášení dozorovému úřadu učiněno do 72 hodin, musí být současně s ním uvedeny důvody tohoto zpoždění.

Z tohoto nařízení ještě více vyplývá důležitost chránit nahraná data.

Pokud k takovému úniku dojde, musí odpovědný subjekt situaci vyhodnotit a učinit všechny kroky, aby se důsledky bezpečnostního incidentu minimalizovaly. Tato zásada neznamená, že vše se musí okamžitě hlásit dozorovému úřadu, ale znamená, že správce dokumentuje veškeré případy porušení zabezpečení osobních údajů, přičemž uvede skutečnosti, které se týkají daného porušení, jeho účinky a přijatá nápravná opatření.

www.asociacebezpecnaskola.cz