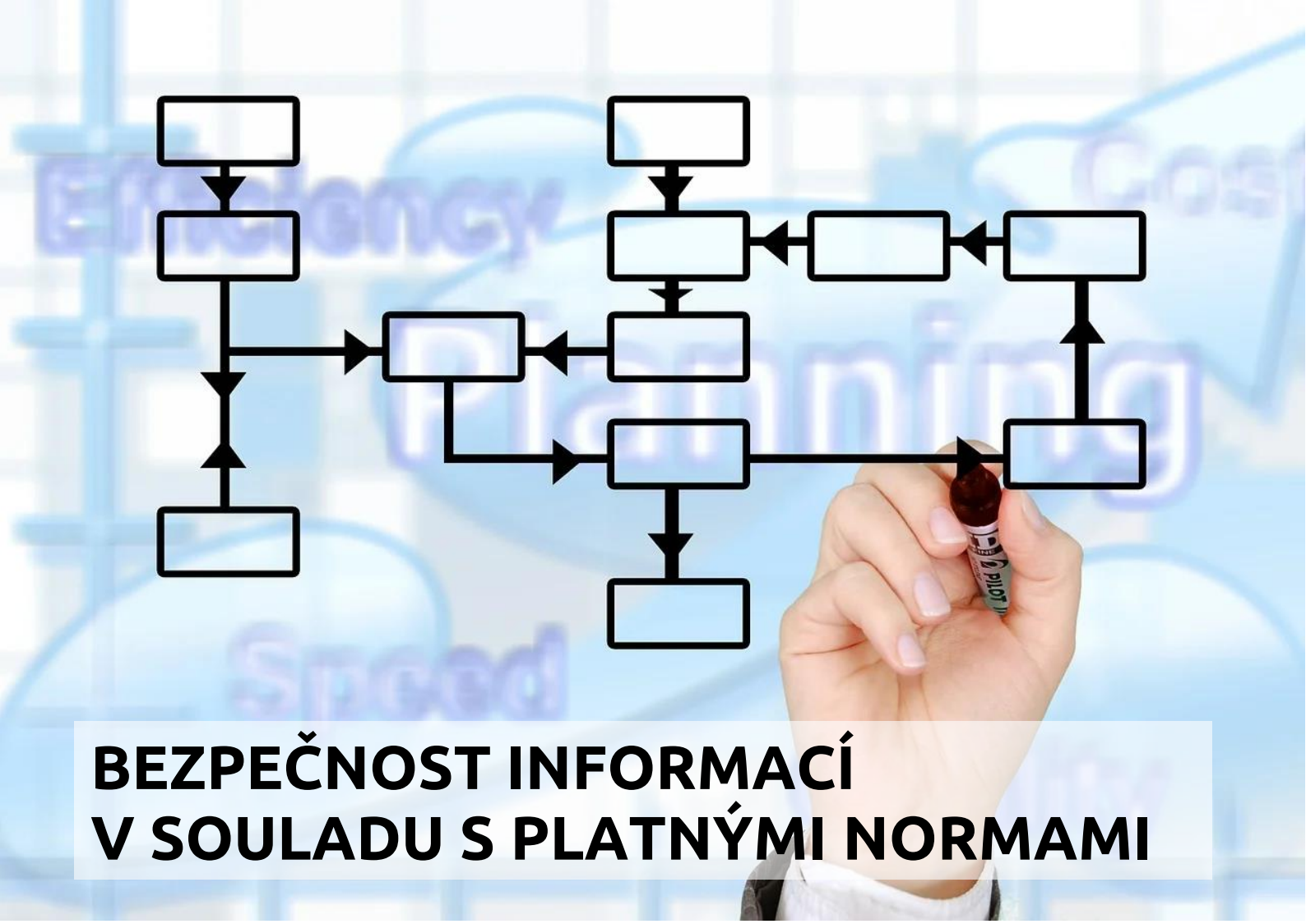

BEZPEČNOST INFORMACÍ V SOULADU S PLATNÝMI NORMAMI

INFORMACE JSOU CENNÉ AKTIVUM

Potřeba chránit informace jako cenné aktivum je dnes již nedílnou součástí strategie téměř každé obchodní společnosti a zákonem danou povinností pro instituce státní kritické infrastruktury. Nedostupnost provozních dat nebo únik citlivých informací může mít za následek výrazné ztráty.

SPOČÍTALI JSTE SI?

jakou hodnotu má pro Vaši společnost reputační riziko a ztráta dobrého jména? Víte kolik vás bude stát ztráta provozních dat nebo nedostupnost informačních sytémů?

MÁTE POVINNOST?

zavést sytém řízení informační bezpečnosti, kterou vám ukládá zákon? Odpovídáte za dodržování podmínek a soulad s nařízením GDPR?

DĚLÁTE DOST A VŠE POTŘEBNÉ?

pro ochranu informačních sytémů všude, kde jsou informační technologie využívány pro komunikaci, podporu procesů nebo správu dat?

89% SPOLEČNOSTI, KTERÉ IMPLEMENTOVALY STANDARD ISO27001, POVAŽUJE ZA NEJVĚTŠÍ PŘÍNOS VYLEPŠENÍ VLASTNÍHO ZABEZPEČENÍ INFORMACÍ.

Zdroj: IT Governance ISO27001 Global Report 2018

BEZPEČNOSTNÍ AUDIT

je prvním krokem k zavedení konzistentního systému řízení informační bezpečnosti. Umožní odhalit slabá místa a dá podněty k zavedení nápravných opatření pro dosažení shody s platnými normami. Pro systém řízení informační bezpečnosti existuje rámec daný skupinou norem ISO/EIC 27000. Z těchto norem pak vychází i české zákony a vyhlášky.

BEZPEČNOSTNÍ PORADENSTVÍ | AUDIT
INFORMAČNÍ BEZPEČNOSTI A SYSTÉM ŘÍZENÍ (ISMS)

thein.security

CO JE MOŽNÉ OČEKÁVAT:

Zaměřujeme se na posouzení stavu řízení informační bezpečnosti ve společnosti a na nastavení a průběžný monitoring bezpečnostní politiky pro ochranu citlivých dat a informačních aktiv před kybernetickými hrozbami.

Postupujeme v souladu s platnou legislativou (požadavky ČSN ISO/IEC 27001, zákon č. 181/2014 Sb., o kybernetické bezpečnosti, vyhláška č. 82/2018 Sb., o kybernetické bezpečnosti, GDPR).

IMPLEMENTACE systému řízení informační bezpečnosti zahrnuje několik kroků, které mohou být prováděny jednotlivě nebo jako součást komplexního projektu. Dají se také aplikovat na celou společnost nebo jen pro dílčí organizační složku či informačí systém:

- **STANOVENÍ ROZSAHU A CÍLŮ ZAVEDENÍ ISMS**
  S přihlédnutím k povaze informačních aktiv společnosti.
- **IDENTIFIKACE INFORMAČNÍCH AKTIV**
  Zmapování a ohodnocení informačních, podpůrných a technických aktiv společnosti.
- **ANALÝZA RIZIK A JEJICH OHODNOCENÍ**
  Identifikace a ohodnocení hrozeb, zranitelností a z nich vyplývajících rizik.
- **PROVEDENÍ SROVNÁVACÍ (GAP) ANALÝZY**
  Porovnání současného stavu se stavem definovaným normami a určení rozdílových parametrů.
- **NÁVRH OPATŘENÍ**
  Tvorba bezpečnostních standardů vymezených především stanovením celkové bezpečnostní politiky společnosti a následnou definicí řádů, směrnic, postupů, instrukcí a metodik.
- **IMPLEMENTACE NAVRŽENÝCH OPATŘENÍ**
  Změna či potvrzení nastavení stávajících systémů a na ně navazujících procesů.
- **MONITOROVÁNÍ A ZLEPŠOVÁNÍ SYSTÉMU**
  Návrhem to nekončí. ISMS je kontinuální proces jehož součástí jsou i pravidelné revize jeho fungování a průběžné korekce jeho nastavení.

VE VÝSLEDKU ZÍSKÁTE:

- znalost, která informační aktiva jsou nutná pro plynulý chod firmy a která data jsou klíčová
- ohodnocení finančních dopadů bezpečnostních rizik
- zjištění, co jsou největší rizika ve vašem IT prostředí a na jaké oblasti se máte přednostně zaměřit
- odůvodnění pro potřebné investice do bezpečnostních sytémů a argumenty pro komunikaci s vedením
- podklady pro rozhodování, do kterých opatření investovat a do kterých nikoliv

PROČ ZVOLIT NAŠE ŘEŠENÍ:

Pomůžeme vám udělat první krok k zavedení konzistentního systému řízení informační bezpečnosti, který je jedním z přepokladů k nastavení účinné ochrany proti dnešním kybernetickým nebezpečím.

STANEME SE VAŠÍM PARTNEREM
PRO OBLAST KYBERNETICKÉ BEZPEČNOSTI.

Od roku **2010** patříme k průkopníkům kybernetické bezpečnosti se zaměřením na **prevenci úniku citlivých dat**, obrany proti **sofistikovaným útokům**, detekce neznámého **malwaru** a aktivní ochrany proti **útokům DDoS**. Dodáváme služby a technologie do **hybridních prostředí** (on prem / cloud) a specializujeme se na **Zero Trust přístup.**

MŮŽEME STAVĚT NA POZITIVNÍ ZKUŠENOSTI
NAŠICH ZÁKAZNÍKŮ.

Spolupracují s námi velké korporace, mobilní operátoři, poskytovatelé internetu, finanční instituce a státní správa, včetně silových bezpečnostních složek.

PRO NAŠE ZÁKAZNÍKY
GARANTUJEME KVALITU.

Sami jsme držitelem certifikátu pro systém managementu informací dle ISO/EIC 27001 : 2013 a certifikátu pro systém managementu kvality dle EN ISO 9001 : 2015.

Pro více informací o Auditu informační bezpečnosti a možnostech implementace ISMS ve vaší společnosti kontaktujte naše obchodní zástupce na obchod.security@thein.eu nebo navštivte naše webové stránky.

Thein Security s.r.o., Pikrtova 1737/1a, 140 00 Praha 4 – Nusle,. e-mail: info.security@thein.eu
Společnost vedená u Městského soudu v Praze oddíl C, značka 109813, IČO: 27415546, DIČ: CZ27415546