Bezpečnost IT
(Security Risk Management)

Vývoji a provozu informačních systémů se věnujeme již více než 20 let. Nedílnou součástí této oblasti je **bezpečnost dat - primárních aktiv.** Jedná se o klíčovou problematiku ve všech IT produktech. Zaměřujeme se zejména na oblasti bezpečnosti definované normami ISO 27k, ISO 22301, ISO 31000, zákonem č. 181/2014 Sb. o kybernetické bezpečnosti a zákonem č. 253/2008 Sb. o legalizaci výnosů z trestné činnosti (AML), v rámci kterých působí i naši certifikovaní specialisté. Používáme SW nástroj pro řízení bezpečnosti - RAM, který umožňuje dynamickou správu a řízení aktiv, rizik, zranitelností, hrozeb a související bezpečnostní dokumentace.

Zaměřujeme se zejména na oblasti:

- **Řízení rizik informací - IRM - Information Risk Management**
  Pro bezpečnost informací je řízení rizik výchozí základnou. Pomůžeme Vám zavést procesy řízení rizik do Vaší organizace tak, aby nevytvářely negativní dopady, jako jsou složitá administrativa nebo vysoká cena bezpečnostních opatření a aby Vám pomáhaly identifikovat existující zranitelnosti a efektivně na ně reagovat vhodnými a účinnými opatřeními. Poskytneme Vám nástroje pro řízení rizik ověřené reálným provozem.

- **Řízení bezpečnosti informací - ISM - Information Security Management**
  Řízení bezpečnosti informací je oblastí zejména procesní a managerskou. Pomůžeme Vám s vytvořením systému bezpečnosti informací ve Vaší organizaci, a to jak v oblasti řízení bezpečnosti informačních systémů a implementaci technologií, tak i při tvorbě bezpečnostní dokumentace a přípravě havarijních plánů. Poskytneme Vám nástroje pro správu dokumentace, řízení aktiv a zavádění bezpečnostních opatření.

- **Řízení kontinuity činností - BCM - Business Continuity Management**
  Řízení kontinuity činností se zaměřuje na kritické podnikové procesy, definuje aktivity pro snížení rizika vzniku rušivé události. Cílem BCM je zabezpečit kritické procesy v organizaci při vzniku rušivé události. Pomůžeme Vám vytvořit strategii kontinuity činností a plány na zachování kontinuity činností Vašich klíčových procesů. Poskytneme Vám nástroje pro zvládání rušivých událostí a sdílení krizových postupů.

- **Řízení kybernetické bezpečnosti - CSM - Cyber Security Management**
  Řízení kybernetické bezpečnosti nabývá v současném světě na důležitosti. V České republice je kybernetická bezpečnost upravena zákonem č. 181/2014 Sb. Pomůžeme Vám s vytvořením systému řízení kybernetické bezpečnosti ve Vaší organizaci dle platného právního rámce, a to jak při tvorbě bezpečnostní dokumentace a přípravě havarijních plánů, tak i při provozu a rozvoji Vašeho IT. Poskytneme Vám nástroje pro správu bezpečnostní dokumentace, řízení aktiv a zavádění bezpečnostních opatření.

Naše služby

- SW nástroj pro řízení bezpečnosti
- bezpečnostní audit IT, ověření souladu, audity dle ISO 27001 (ISMS), zákona č. 181/2014 Sb. (ZoKB) a Nařízení 2016/679 (GDPR)
- implementace a nastavení systémů ISMS, ZoKB a GDPR, podpora interních procesů
- příprava na certifikaci / audit, bezpečnostní dokumentace, ad - hoc support
- externí a interní penetrační testy
- školící a vzdělávací služby

Naši klienti

- Ministerstvo školství, mládeže a tělovýchovy
- Ministerstvo pro místní rozvoj
- Centrum pro zjišťování výsledků vzdělávání
- Lesy České republiky
- Rehabilitační ústav Kladruby
- Arvato - Bertelsmann
- Pražská vodohospodářská společnost
- Podpůrný a garanční rolnický a lesnický fond
- Severočeské vodovody a kanalizace
- Český metrologický institut

PragoData a.s.
www.pragodata.com
Opletalova 1418/23, 110 00 Praha 1
info@pragodata.com