IB-CONSULTING
INFORMATION & BUSSINESS

Ing. Ivan Bělohlávek & IB-Consulting
Sedlákova 965/1, 674 01 Třebíč
IČO:14678870, DIČ: CZ5805131640
Telefon: 602758113
http://www.ib-consulting.cz, E-mail: ib@ib-consulting.cz

Plánování kontinuity IT činností (systém řízení bezpečnosti informací)

Plánování kontinuity IT činností lze definovat jako souhrn aktivit zaměřených na snížení rizika vzniku havárie a omezení dopadu havárie, tj. incidentu na kritické podnikové informační procesy.

Plánování kontinuity není jen plánem reakce na krizovou událost, ale obsahuje také důležitý preventivní aspekt. Jedním z hlavních výstupu tohoto procesu je plán zachování kontinuity IT činností (Business Continuity Plan). Kvalitní plány kontinuity činností jsou schopny minimalizovat následky mimořádných událostí a zároveň umožňují a urychlují uvedení provozu do normálního stavu.

Pokud si nejste jisti, zda chápete význam principu plánování kontinuity IT činností pro Vaši společnost, zamyslete se nad těmito otázkami:

- Víte dobře, co je třeba podniknout, aby Vaše společnost dokázala krizovým situacím předcházet?
- Víte jak efektivně a úsporně řešit informační katastrofy, a jak navrátit rychle společnost do normálního chodu?
- Znáte veškerá možná rizika, která mohou narušit činnost Vaší společnosti?
- Víte jaké dopady mohou mít rizika na klíčové informační procesy společnosti?
- Víte jak postupovat v krizových situacích?
- Jsou Vaše plány obnovy aktuální a použitelné?
- Zvládáte dobře i obtížnou část implementace systému bezpečnosti informací v prostředí Vaší organizace – testování navržených bezpečnostních plánů?
- Provádíte kontrolu úplnosti vytvořených bezpečnostních plánů?

Pokud jste při zodpovězení části uvedených otázek na rozpacích, je nutné doplnit své znalosti, které v současné době zahrnují velkou řádku odborných témat. Poznat systém bezpečnosti informací a umět ho úspěšně implementovat je složitá a odborná činnost, v této oblasti je Vám naše společnost plně k dispozici.

Systém řízení bezpečnosti informací pro ochranu osob a majetku

Důležitým základem pro stanovení odpovídajících bezpečnostních opatření je provedení bezpečnostní analýzy a vyhodnocení předpokládaných vnitřních a vnějších informačních rizik, základem pro provedení kvalitní analýzy je správné definování informačních aktiv společnosti, jejich monitoring včetně řešení incidentů.

Zpracování analýzy rizik obsahuje:

- Zpracování vnitřních norem pro zavedení systému řízení bezpečnosti informací dle standardu ISO/IEC 27001:2005.
- Poradenství v oblasti působnosti zákona č.101/2000 Sb., o ochraně osobních údajů.

Cílem je dosažení stavu, kdy jsou na efektivní míru omezeny hrozby na informační objekt a jeho zájmy a tento objekt je k omezení stávajících i potencionálních hrozeb efektivně a preventivně chráněn. Proto také nabízíme účinné řešení prostřednictvím produktů jako jsou technologie ochrany podnikových sítí - **Sophos Complete Security** a **Smart Security / Endpoint Security / Rychlý audit ISMS** od **ESETU** nebo nejmodernější produkty pro zálohování dat - **Acronis Backup** & **Recovery** a **CA ARCserve**.

Podrobné informace získáte na adrese naší společnosti:

Ing. Ivan Bělohlávek
Třebíč, Sedlákova 965/1
***GSM:** +420 602 758 113*
***E-mail:** ib@ib-consulting.cz*
www.ib-consulting.cz