PORADENSTVÍ V OBLASTI INFORMAČNÍCH TECHNOLOGIÍ

Globalizace a digitalizace procesů nabízejí společnostem skvělé příležitosti pro zvýšení efektivity a snížení nákladů. Pokročilá technologická řešení a automatizace jsou bezpochyby přidanou hodnotou Vašeho podnikání. Správné řízení technologií a zavedení bezpečnostních procesů je ale nutné, abyste udrželi krok s konkurencí. V oblasti IT Vám pomůžeme využít příležitosti digitální doby ve Váš prospěch a poradíme Vám, jak nastavit ochranné mechanismy zajištění bezpečnosti dat. Náš odborný tým má rozsáhlé zkušenosti a znalosti v oboru a služby, které poskytujeme, přinášejí klientům skutečnou hodnotu.

IT AUDIT

Pro správné posouzení IT je nutné posoudit organizaci ve všech rovinách, od technické přes organizační až po procesní. Širokému spektru oblastí, které je potřebné při IT auditu posoudit, odpovídá i široké spektrum legislativy, normativů a dalších standardů vůči kterým je možné nebo potřebné IT audit provádět. Na jedné straně analyzujeme IT prostředí našich klientů v rámci auditů ročních účetních závěrek, a to z hlediska pravidelnosti, ziskovosti a rostoucích požadavků úřadů. Zároveň také posuzujeme podnikové procesy v IT a kontrolujeme zranitelnost systémů. Součástí našich služeb je také kontrola fyzické a organizační bezpečnosti a poradenství týkající se bezpečnostních zásad. Naše služby představují:

- Audit systému řízení bezpečnosti informací (ISMS)
- Audit systému řízení IT služeb (ITSM)
- Audit ochrany osobních údajů (GDPR)
- Audity regulatorních požadavků v bankovním prostředí
- Technické audity posuzující stav v oblasti IT
- Ověření služeb třetích stran (SOC 1, SOC 2 a SOC 3, ISAE)
- Audit ekonomiky IT
- Ověření regulace platebních služeb (PSD2)
- Audity podle specifické regulace jednotlivých oborů

KYBERBEZPEČNOST

Kybernetická bezpečnost se v současné situaci stává jednou z nejdůležitějších témat fungování společností. Nové technologie a digitalizace procesů společnosti si vyžadují vyšší bezpečnostní standardy. Stále nové nároky klade také legislativa a požadavky regulátorů.

SOCIÁLNÍ INŽENÝRSTVÍ

Sociální inženýrství je nebezpečné kvůli elementu lidského pochybení uživatelů. Nemusí nutně znamenat chybu v softwaru nebo operačních systémů, a proto je důležité vědět, jak a jakým způsobem jsou lidé manipulováni sociálními inženýry, a tak se před těmito útoky bránit. Máme vlastní řešení pro phishingové kampaně zaměřené na prostředí Microsoft a Google. V této oblasti Vám nabídneme komplexní služby sociálního inženýrství a simulaci Vašeho prostředí přesně tak, jak to vyžadují úspěšné kampaně pomocí těchto nástrojů:

- Simulované podvržené e-maily
- Simulované falešné telefonní hovory
- Doporučení pro mitigaci rizik
- Průběžné testování formou aktuálních kampaní a následné zvyšování bezpečnostního povědomí

PENETRAČNÍ TESTOVÁNÍ

Penetrační testy umožňují zjistit, zda je prostředí Vaší sítě skutečně odolné. Hlavním důvodem, proč jsou penetrační testy zásadní pro zabezpečení organizace, je to, že pomáhají zaměstnancům naučit se, jak zvládnout jakýkoli typ útoku hackerů. Testováním vyhledáváme slabiny v systému a potenciální cíle hackerského útoku. Pomáháme tak našim

klientům chránit jejich sítě před vnějšími hrozbami a navrhneme Vám vhodná doporučení ke zmírnění dopadů.

TESTOVÁNÍ ZRANITELNOSTI

Řízení zranitelností (vulnerability management) je proces identifikace, hodnocení, nápravy a hlášení zranitelností zabezpečení v systémech a softwaru. Spolu s dalšími bezpečnostními taktikami se jedná o zásadní postup, který napomáhá společnostem rozpoznat rizika a minimalizovat rozsah rizik. Není zcela možné vždy pokrýt vše, ale příprava plánu správy zranitelnosti Vám může pomoci předejít těm nejrizikovějším zranitelnostem. Správa zranitelnosti vás vybaví procesem a nástroji pro pravidelnou identifikaci a nápravu Vašich nejkritičtějších a vysoce rizikových bodů zranitelnosti. Naše služby zahrnují zejména:

- Řízení zranitelností
- Posouzení rizik
- Pravidelné testování zranitelnosti a sledování nových hrozeb

ŠKOLENÍ KYBERBEZPEČNOSTI

Koncoví uživatelé jsou obvykle tím nejslabším místem Vaší sítě, a proto je znalost rizik, prevence a ochrany zásadní pro bezpečnost celé společnosti.Vaši zaměstnanci potřebují online školení v oblasti kybernetické bezpečnosti, aby chránili sebe a Vaši společnost před kybernetickými útoky, aby se naučili všechna důležitá pravidla a zásady bezpečnosti práce online. Tím, že zaměstnance informujete o bezpečnostních hrozbách, o tom, jak by na ně mohli reagovat, a o tom, jaké postupy mají následovat při identifikaci hrozby, posilujete nejzranitelnější články v řetězci.

ROBOTIZACE, AUTOMATIZACE A DIGITALIZACE FIREMNÍCH PROCESŮ

Naše řešení zahrnují automatizaci rutinních procesů, digitalizaci procesů a narovnání pracovních postupů. Tyto projekty jsou díky agilnímu přístupu schopny přinášet měřitelné výsledky během jednotek týdnů s minimálním vytížením Vašich zaměstnanců. Od počátku spolupráce se zamýšlíme především nad celkovou strategií firmy a očekávánými přínosy. Jedině tak každému klientovi umožníme využít přesně tu oblast, která je pro danou situaci nejvhodnější a zároveň minimálně naruší chod stávajících systémů, a to s návratností vložených investic v řádu měsíců. Naše služby zahrnují:

- Pokročilá digitalizace a vytěžování papírových dokumentů
- Softwarová robotizace firemních procesů (RPA)
- Automatizace firemních procesů (digitalizace formulářů, procesní workflow)
- Mobilní aplikace a webové stránky
- Softwarová řešení

IT PORADENSTVÍ A OUTSOURCING

Našim klientům napříč průmyslovými odvětvími pomáháme identifikovat, stanovit priority, vyvíjet a provádět technologické inovace podporující jejich obchodní cíle. Naše poradenství a řešení kombinují pohled na Vaše lidi, procesy a technologie a pomohou Vám vytvořit skutečnou hodnotu měřitelnou v čase.

- Řízení IT
- Řízení IT služeb
- Řízení IT projektů
- Výběr IT řešení

Martin Hořický, partner
e martin.horicky@bdo.cz
m +420 608 937 408

Tomáš Kubíček, Partner
e tomas.kubicek@bdo.cz
m +420 737 210 682