Případová studie

Řízení bezpečnosti jako klíč ke konjuktuře

AutoCont

Profil zákazníka

Společnost BOOM TISK, spol. s r.o. patří již několik let mezi nejvýznamnější polygrafické podniky v ČR.

Jako jedna z mála firem se soustředí na dodání komplexního řešení v oblasti ofsetového a digitálního tisku. Nevyrábí pouze jednotlivé produkty širokého rozsahu (letáky, katalogy, brožury, výroční zprávy, direct mail), ale svým klientům poskytuje servis v oblasti přípravy projektů, dokončujícího zpracování a řešení distribuce.

Firma byla založena v únoru 1995 a v následujících letech zaznamenala raketový růst. Dnes je BOOM TISK, spol. s. r.o. jedním z nejmoderněji vybavených a největších producentů hybridních tiskovin ve střední Evropě s kapacitou 1 mil. plnobarevných digitálních stran a 4,8 mil. ofsetových stran denně.

www.boomtisk.cz

Období realizace

Zahájení realizace projektu v roce 2011, zavedení systému řízení v průběhu roku 2012.

Výchozí situace a cíle projektu

V době před zahájením projektu na zavádění systému řízení bezpečnosti informací stála společnost BOOM TISK před významným rozhodnutím, které ovlivnilo prakticky veškeré další aktivity. Důležitým impulsem pro zahájení projektu - zavedení ISMS - byla příležitost uzavřít kontrakt se strategicky významným zákazníkem. Jedním z aspektů, které bylo nutno před završením obchodních jednání podpisem smlouvy zvážit, byla skutečnost, zda je společnost ochotná a schopná dodržet a naplnit nadstandardní požadavky potenciálního zákazníka. Mezi podmínky, jejichž splnění kontrakt vyžadoval, patřilo mimo jiné vypořádat se s vysokými bezpečnostními nároky zákazníka. Náročné požadavky na řešení bezpečnosti bylo nezbytné promítnout do oblasti ochrany samotných dat zákazníka i do celé infrastruktury informačních a komunikačních technologií potřebných pro jejich zpracování.

Společnost BOOM TISK není nováčkem na poli certifikace podle ISO norem, důsledně dbá na dodržování systému řízení kvality a je certifikována dle normy ISO 9001:2009 a ISO 12647-2:2004 pro kalibraci tiskového procesu. Tyto skutečnosti výraznou měrou ovlivnily pozdější úspěšné zahájení a také bezproblémový průběh společného projektu zavádění systému řízení bezpečnosti informací do života firmy.

Popis řešení

Díky dřívějším zkušenostem se zaváděním certifikovaného systému řízení kvality (ISO 9001) měli již představitelé společnosti dostatečně jasnou představu o tom, co je čeká v oblasti zavádění systému řízení bezpečnosti informací (= ISMS) založeného také na procesním přístupu. Bylo tedy možno přistoupit rovnou k identifikaci specifických bezpečnostních požadavků definovaných zákazníkem společnosti. Vzhledem ke skutečnosti, že doporučovaným a velmi často používaným etalonem pro řízení informační bezpečnosti, jak jej ostatně v rámci auditu uplatňoval i potenciální zákazník společnosti, je mezinárodní standard ISO 27001, bylo zavádění ISMS pouze rozšířeno o specifické požadavky tohoto zákazníka.

Na počátku došlo k ustavení projektového týmu, před kterým stál úkol definovat konkrétní kroky harmonogramu k naplnění všech požadovaných bezpečnostních opatření. Byla zpracována úvodní bezpečnostní analýza, která měla za cíl odhalit neshody stávajícího stavu zabezpečení informačního systému společnosti oproti normě, a dále navrhnout vhodné způsoby řešení. Plnění jednotlivých konkrétních úkolů, které z této analýzy vyplynuly, bylo již otázkou realizace podrobného harmonogramu činností. Ten vznikl průnikem požadavků analýzy a výsledků zákaznického auditu. Zde se opět projevila výhoda zkušeností s certifikací systému kvality, protože některé procesy byly již dokumentovány a stačilo rozšířit dokumentaci o příslušné kapitoly pokrývající oblast bezpečnosti. Poté byly doplněny požadované bezpečnostní směrnice a postupy, a zavedeny potřebné záznamy dokládající funkčnost zavedeného systému v požadovaném rozsahu.

Klíčovou snahou v průběhu celého projektu bylo na obou stranách využít stávající zavedené procesy a postupy, a efektivně přistupovat k implementaci jak organizačních, tak technických opatření. V rámci organizačních opatření se společnost rozhodla pro ekonomicky výhodnější outsourcing - tedy využívání služeb externího manažera bezpečnosti informací (Information Security Officer). Tím vyřešila otázku případného střetu zájmů, pokud by tuto kumulovanou funkci zastával některý ze stávajících zaměstnanců společnosti. V oblasti technických opatření bylo možné do jisté míry využít možností stávajících systémů ve smyslu využití dosud neaplikovaných bezpečnostních funkcí či upgrade případně přechod na novější verze. Náročné požadavky ze strany zákazníka si však také vyžádaly zavedení nových technologií, jako např. zvýšená ochrana na vnějším perimetru, filtrování komunikace či softwarový audit.

Případová studie

Akcelerace vývoje v rámci zkvalitnění bezpečnostních procesů

Jak je všeobecně známo, ne všechna opatření je nezbytně nutné zavést ihned, neboť celý proces řízení bezpečnosti má své časové nároky a systém je závislý především na lidském faktoru, takže si musí takzvaně “sednout”. Personál musí být připraven na změny a také patřičně proškolen v nových postupech a povinném používání bezpečnostních funkcí, na které dříve nebyl zvyklý. Stejně tak některé aktivity (např. změny v informačním systému či ve zpracování dat, analýzy rizik, interní audity, penetrační testy apod.) teprve s postupem času odhalí nové zranitelnosti, na které je nutné reagovat. Jde o standardní příklad životního cyklu PDCA (Plan-Do-Check-Act) v rámci neustálého zlepšování.

Důležité je, že se společnost dokázala vypořádat se všemi problémy a náročné období bylo korunováno úspěchem.

V tuto chvíli je možné konstatovat, že systém řízení bezpečnosti informací byl úspěšně nastartován, v průběhu jednoho roku také prakticky zaveden a nyní již lze ověřovat jeho fungování prostřednictvím opakovaných auditů. Dále existuje předpoklad, že v dohledné době bude celý projekt završen formální certifikací ISMS ze strany akreditovaného certifikačního orgánu.

Přínosy

Vždy je možné zlepšovat - to je účelem každého systému řízení. Nicméně co jiného by mohlo lépe potvrdit, že společnost je důvěryhodná, že dokáže splnit náročné bezpečnostní požadavky svých zákazníků a je schopná dostát svým závazkům, než získaný kontrakt.

Realizace projektu zavedení ISMS do praxe přinesla společnosti BOOM TISK kromě spokojeného zákazníka také další výhody:

- jednotný přístup k ochraně dat a ICT
- konkurenční výhodu
- finanční úspory (snížení nákladů na řešení bezpečnostních incidentů)
- bezpečné ICT a chráněná citlivá data
- důvěryhodnost a dobré jméno společnosti

AutoCont CZ a.s.
tel.: +420 910 971 971
e-mail: obchod@autocont.cz

IT profesionál 1. volby