Obecné zásady informační bezpečnosti

Vedení společnosti tímto stanoví jako součást své strategie následující obecné zásady informační bezpečnosti:

Důležitost zpracování informací

Zpracování informací hraje v naší činnosti klíčovou roli. Všechny podstatné strategické a operativní funkce a úkoly se neobejdou bez významné podpory informačních a komunikačních technologií (Information and Communication Technology, ICT). Jakýkoli výpadek ICT systémů se musí v co nejkratší době kompenzovat. Ani v dílčích úsecích našeho podnikání nesmí dojít k závažnému narušení. Protože jádrem naší činnosti je partnerský vývoj inovativních produktů v součinnosti s klienty a dodavateli, má pro nás ochrana těchto informací před neoprávněným přístupem a nepovolenými změnami existenční význam.

Nadřazené cíle

Disponibilita našich dat a ICT systémů je ve všech technických a ekonomických úsecích zajištěna tak, aby předpokládané nutné doby nečinnosti těchto systémů byly únosné. Funkční poruchy a narušení dat a ICT systémů jsou přípustné pouze v nepatrném rozsahu a ve výjimečných případech (*integrita*). Požadavky na *důvěrnost* mají standardní úroveň, zajišťující soulad s právními předpisy. Ve vztahu ke konstrukčním datům našich klientů a oddělení vývoje platí maximálně přísné požadavky na důvěrnost.

Standardní bezpečnostní opatření musí být v ekonomicky únosném vztahu k hodnotě chráněných informací a ICT systémů. Je nezbytné zamezit incidentům s velkými finančními dopady.

Všichni zaměstnanci podniku dodržují platné právní předpisy (například zákony a nařízení v oblasti ochrany osobních údajů), interní technologické a pracovní pokyny a uzavřené smlouvy. Je nutné zabránit porušování právních předpisů a smluv spojeného s negativními finančními a morálními dopady na podnik a zaměstnance.

Všichni zaměstnanci a vedení podniku si jsou vědomi své odpovědnosti za zacházení s ICT systémy a v maximální míře podporují realizaci bezpečnostní strategie.

Konkrétní cíle

Opožděná nebo nesprávná rozhodnutí managementu mohou vést k dalekosáhlým následkům. U zásadních rozhodnutí je proto důležité, aby měl management přístup

k aktuálním údajům. U těchto informací je třeba zajistit vysokou úroveň bezpečnosti z hlediska jejich disponibility a integrity.

Zákony na ochranu osobních údajů a zájmy našich zaměstnanců vyžadují, aby byla zajištěna důvěrnost osobních údajů zaměstnanců. Ochrana důvěrnosti dat a ICT aplikací, s nimiž pracuje personální oddělení, je proto zvlášť přísná. Totéž se týká také dat našich obchodních partnerů.

Ve vztahu k údajům o poptávkách a nabídkách, které dostáváme nebo předkládáme ve styku se zákazníky, a také ke konstrukčním datům našich zákazníků a našeho oddělení vývoje musíme zajistit vysokou úroveň důvěrnosti. Ztráta nebo odcizení těchto dat pro nás může znamenat konkurenční nevýhodu nebo vést k uplatnění nároků na náhradu škody proti naší firmě. Při ochraně důvěrnosti a předcházení manipulacím s daty zde uplatňujeme technická opatření a odpovědný přístup zaměstnanců.

Pro pracoviště logistiky a výrobní provozy je zajištěna disponibilita a funkční spolehlivost systémů. Tyto systémy mohou být mimo provoz jen po velmi krátkou dobu, protože takové prostoje mohou vést k přímému, ale i nepřímému snížení výnosů a mít nepříznivý dopad na spokojenost zákazníků.

Využívání internetu a portálových aplikací k získávání informací a ke komunikaci je pro nás samozřejmostí. Elektronická pošta nahrazuje tradiční způsoby komunikace v administrativě nebo je doplňuje. Uplatňováním vhodných opatření zajišťujeme, aby rizika spojená s jejím užíváním byla co nejmenší.

Management informační bezpečnosti

K dosažení cílů informační bezpečnosti byla vybudována vlastní organizační struktura. Byl jmenován pověřenec pro informační bezpečnost. Pověřenec pro informační bezpečnost podléhá ve své funkci přímo vedení firmy.

Vrcholové vedení poskytuje pověřenci pro informační bezpečnost dostatečné finanční a časové zdroje k tomu, aby se soustavně dále vzdělával, získával potřebné informace a plnil cíle informační bezpečnosti stanovené managementem podniku.

Administrátory bezpečnosti ICT a pověřence pro informační bezpečnost podporují v jejich činnosti uživatelé ICT.

Pověřenec pro informační bezpečnost musí být co nejdříve zapojen do všech projektů, aby tak už ve fázi přípravy projektu bylo zajištěno respektování bezpečnostních aspektů. Pokud jsou projektem dotčeny i osobní údaje, platí totéž i pro pověřence pro ochranu osobních údajů.

Uživatelé ICT se musí v záležitostech informační bezpečnosti řídit pokyny pověřence pro informační bezpečnost.

Bezpečnostní opatření

Pro všechny postupy, informace, aplikace a systémy ICT je určena odpovědná osoba, která zjišťuje potřebu ochrany a přiděluje přístupová oprávnění.

U všech odpovědných funkcí musí být stanoveno zastupování. Prostřednictvím instruktáží a vybavení potřebnou dokumentací je nutno zajistit, aby zástupci byli schopni řádně plnit své úkoly.

Budovy a vnitřní prostory jsou chráněny dostatečnou kontrolou přístupu. Na ochranu přístupu k ICT systémům jsou zřízeny přiměřené kontroly a pro přístup ke všem datům je vypracována restriktivní koncepce oprávnění.

Ve všech systémech se používají programy na ochranu proti počítačovým virům. Všechny přístupy k internetu jsou zabezpečeny vhodnými firewallovými systémy. Všechny programy zajišťující ochranu jsou nakonfigurovány a administrovány tak, aby poskytovaly účinnou ochranu a znemožňovaly manipulaci. Uživatelé prostředků ICT kromě toho přispívají svým odpovědným přístupem k účinné aplikaci těchto bezpečnostních opatření a v případě zjištění nestandardních situací informují odpovědné pracovníky.

Ztrátu dat nelze nikdy naprosto vyloučit. Důsledné uplatňování zálohování dat proto zaručuje, že provoz systémů ICT bude velmi brzy obnoven v případě, že dojde ke ztrátě nebo zjevnému porušení některých operativních dat. Informace jsou označeny jednotně a ukládají se tak, aby je bylo možné rychle najít.

Pohotová a důsledná reakce na bezpečnostní incidenty umožňuje omezit rozsáhlejší škody v důsledku havárií nebo jim popř. úplně předejít. Opatření pro případ havárie jsou sloučena do jednotné koncepce řešení havarijních situací. Naším cílem je dosáhnout toho, aby při výpadku systému nedošlo k přerušení chodu firmy a aby se v co nejkratší době podařilo obnovit disponibilitu postižených systémů.

Pokud zajišťujeme poskytování ICT služeb prostřednictvím externích subjektů, stanovíme jim ve smlouvách o poskytování služeb konkrétní bezpečnostní požadavky. Jestliže je v rámci plnění smlouvy nezbytné zpřístupnit dodavatelům údaje, pro něž je předepsán vysoký stupeň ochrany, pak od dodavatelů zvlášť a výslovně vyžadujeme dodržení zásady utajení. Zároveň se stanoví právo na kontrolu.

Uživatelé prostředků ICT se účastní školení o konkrétním využívání služeb ICT a o souvisejících bezpečnostních opatřeních. Vrcholové vedení přitom podporuje účelné další vzdělávání a zvyšování kvalifikace pracovníků.

Zlepšování bezpečnosti

Firma provádí pravidelné kontroly aktuálnosti a efektivity systému řízení informační bezpečnosti. Vedle toho se také pravidelně ověřuje, jestli dotčení pracovníci znají tato opatření, jestli lze opatření realizovat a integrovat do provozu společnosti.

Vedení podniku podporuje neustálé zlepšování úrovně bezpečnosti. Od zaměstnanců požadujeme, aby příslušným pracovištím předávali podněty k možným zlepšením nebo k odstranění nedostatků.

Průběžná revize předpisů a jejich dodržování zajišťuje dosahování žádoucí úrovně bezpečnosti a ochrany osobních údajů. Cílem analýzy nedostatků je dosáhnout zlepšení bezpečnostní situace a udržovat bezpečnost systémů ICT na úrovni odpovídající současnému stavu techniky.

Bamberg, 02.05.2018

vedení podniku

Thomas Mai

Stefan Frey - pověřenec pro informační bezpečnost -

Ralf Ruf