shaping concepts. forming ideas.

IDEAL AUTOMOTIVE



# Všeobecné zásady informačnej bezpečnosti

Vedenie spoločnosti týmto stanovuje ako súčasť svojej stratégie nasledujúce všeobecné zásady informačnej bezpečnosti:

## Dôležitosť spracovania informácií

Spracovanie informácií hrá v našej činnosti kľúčovú rolu. Všetky podstatné strategické a operatívne funkcie a úlohy sa nezaobídu bez významnej podpory informačných a komunikačných technológií (Information and Communication technology. ICT). Akýkoľvek výpadok ICT systémov sa musí v čo najkratšom čase kompenzovať. Ani v čiastkových úsekoch nášho podnikania nesmie dôjsť k závažnému narušeniu. Pretože jadrom našej činnosti je partnerský vývoj inovatívnych produktov v súčinnosti s klientmi a dodávateľmi, má pre nás ochrana týchto informácií pred neoprávneným prístupom a nepovolenými zmenami existenčný význam.

## Nadradené ciele

*Disponibilita* našich dát a ICT systémov je vo všetkých technických a ekonomických úsekoch zabezpečená tak, aby predpokladané nutné doby nečinnosti týchto systémov boli únosné. Funkčné poruchy a narušenia dát a ICT systémov sú prípustné iba v nepatrnom rozsahu a vo výnimočných prípadoch *(integrita)*. Požiadavky na *dôvernosť* majú štandardnú úroveň, zaisťujúcu súlad s právnymi predpismi. Vo vzťahu ku konštrukčným dátam našich klientov a oddelenia vývoja platia maximálne prísne požiadavky na dôvernosť.

Štandardné bezpečnostné opatrenia musia byť v ekonomicky únosnom vzťahu k hodnote chránených informácií a ICT systémov. Je nevyhnutné zamedziť incidentom s veľkými finančnými dôsledkami.

Všetci zamestnanci podniku dodržiavajú platné právne predpisy (napríklad zákony a nariadenia v oblasti ochrany osobných údajov), interné technologické a pracovné pokyny a uzavreté zmluvy. Je nutné zabrániť porušovaniu právnych predpisov a zmlúv spojeného s negatívnymi finančnými a morálnymi dopadmi na podnik a zamestnancov.

Všetci zamestnanci a vedenie podniku sú si vedomí svojej zodpovednosti za zaobchádzanie s ICT systémami a v maximálnej miere podporujú realizáciu bezpečnostnej stratégie.

## Konkrétne ciele

Oneskorené alebo nesprávne rozhodnutia manažmentu môžu viesť k ďalekosiahlym následkom.
Pri zásadných rozhodnutiach je preto dôležité, aby mal manažment prístup k aktuálnym údajom. Pri týchto informáciách je treba zabezpečiť vysokú úroveň bezpečnosti z hľadiska ich dostupnosti a integrity.

Zákony na ochranu osobných údajov a záujmy našich pracovníkov vyžadujú, aby bola zabezpečená dôvernosť osobných údajov zamestnancov. Ochrana dôvernosti dát a ICT aplikácií, s ktorými pracuje personálne oddelenie, je preto zvlášť prísna. To isté sa týka aj dát našich obchodných partnerov.

Vo vzťahu k údajom o dopytoch a ponukách, ktoré dostávame alebo predkladáme v styku so zákazníkmi, a tiež ku konštrukčným dátam našich zákazníkov a nášho oddelenia vývoja musíme zabezpečiť vysokú úroveň dôvernosti. Strata alebo odcudzenie týchto dát pre nás môže znamenať konkurenčnú nevýhodu alebo viesť k uplatneniu nárokov na náhradu škody proti našej firme. Pri ochrane dôvernosti a predchádzaniu manipuláciám s dátami tu uplatňujeme technické opatrenia a zodpovedný prístup zamestnancov.

Pre pracoviská logistiky a výrobné prevádzky je zaistená disponibilita a funkčná spoľahlivosť systémov. Tieto systémy môžu byť mimo prevádzky len po veľmi krátku dobu, pretože takéto prestoje môžu viesť k priamemu, ale aj nepriamemu zníženiu výnosov a mať nepriaznivý vplyv na spokojnosť zákazníkov.

Využívanie internetu a portálových aplikácií na získavanie informácií a na komunikáciu je pre nás samozrejmosťou. Elektronická pošta nahrádza tradičné spôsoby komunikácie v administratíve alebo ich doplňuje. Uplatňovaním vhodných opatrení zaisťujeme, aby riziká spojené s jej užívaním boli čo najmenšie.

## Management informačnej bezpečnosti

Na dosiahnutie cieľov informačnej bezpečnosti bola vybudovaná vlastná organizačná štruktúra. Bol vymenovaný poverenec pre informačnú bezpečnosť. Poverenec pre informačnú bezpečnosť podlieha vo

svojej funkcii priamo vedeniu firmy.

Vrcholové vedenie poskytuje poverencovi pre informačnú bezpečnosť dostatočné finančné a časové zdroje na to, aby sa sústavne ďalej vzdelával, získaval potrebné informácie a plnil ciele informačnej bezpečnosti stanovenej manažmentom podniku.

Administrátorov bezpečnosti ICT a poverencov pre informačnú bezpečnosť podporujú v ich činnosti užívatelia ICT.

Poverenec pre informačnú bezpečnosť musí byť čo najskôr zapojený do všetkých projektov, aby tak už vo fáze prípravy projektu bolo zaistené rešpektovanie bezpečnostných aspektov. Ak sú projektom dotknuté aj osobné údaje, platí to isté aj pre poverenca pre ochranu osobných údajov.

Používatelia ICT sa musia v záležitostiach informačnej bezpečnosti riadiť pokynmi poverenca pre informačnú bezpečnosť.

**Bezpečnostné opatrenia**

Pre všetky postupy, informácie, aplikácie a systémy ICT je určená zodpov
ochrany a prideľuje prístupové oprávnenia.

Pri všetkých zodpovedných funkciách musí byť stanovené zastupovan
vybavením potrebnou dokumentáciou je potrebné zabezpečiť, aby zástupcovia boli schopní riadne plniť svoje úlohy.

Budovy a vnútorné priestory sú chránené dostatočnou kontrolou prístupu. Na ochranu prístupu k ICT systémom sú zriadené primerané kontroly a pre prístup ku všetkým dátam je vypracovaná reštriktívna koncepcia oprávnenia.

Vo všetkých systémoch sa používajú programy na ochranu proti počítačovým vírusom. Všetky prístupy k internetu sú zabezpečené vhodnými firewallovými systémami. Všetky programy zaisťujúce ochranu sú konfigurované a administrované tak, aby poskytovali účinnú ochranu a znemožňovali manipuláciu. Používatelia prostriedkov ICT okrem toho prispievajú svojím zodpovedným prístupom k účinnej aplikácii týchto bezpečnostných opatrení a v prípade zistenia neštandardných situácií informujú zodpovedných pracovníkov.

Stratu dát nie je možné nikdy úplne vylúčiť. Dôsledné uplatňovanie zálohovania dát preto zaručuje, že prevádzka systémov ICT bude veľmi skoro obnovená v prípade, že dôjde k strate alebo zjavnému porušeniu niektorých operatívnych dát. Informácie sú označené jednotne a ukladajú sa tak, aby ich bolo možné rýchlo nájsť.

Pohotová a dôsledná reakcia na bezpečnostné incidenty umožňuje obmedziť rozsiahlejšie škody v dôsledku havárií alebo im poprípade úplne predísť. Opatrenia pre prípad havárie sú zlúčené do jednotnej koncepcie riešenia havarijných situácií. Naším cieľom je dosiahnuť to, aby pri výpadku systému nedošlo k prerušeniu chodu firmy a aby sa v čo najkratšom čase podarilo obnoviť disponibilitu postihnutých systémov.

Ak zabezpečujeme poskytovanie ICT služieb prostredníctvom externých subjektov, stanovíme im v zmluvách o poskytovaní služieb konkrétne bezpečnostné požiadavky. Ak je v rámci plnenia zmluvy potrebné sprístupniť dodávateľom údaje, pre ktoré je predpísaný vysoký stupeň ochrany potom od dodávateľov zvlášť a výslovne vyžadujeme dodržiavanie zásady utajenia. Zároveň sa stanovuje právo na kontrolu.

Používatelia prostriedkov ICT sa zúčastňujú školení o konkrétnom využívaní služieb ICT a súvisiacich bezpečnostných opatreniach. Vrcholové vedenie pritom podporuje účelné ďalšie vzdelávanie a zvyšovanie kvalifikácie pracovníkov.

**Zlepšovanie bezpečnosti**

Firma vykonáva pravidelné kontroly aktuálnosti a efektivity systému riadenia informačnej bezpečnosti. Vedľa toho sa tiež pravidelne overuje, či dotknutí pracovníci poznajú tieto opatrenia, či je možné opatrenia realizovať a integrovať do prevádzky spoločnosti.

Vedenie podniku podporuje neustále zlepšovanie úrovne bezpečnosti. Od zamestnancov požadujeme, aby príslušným pracoviskám odovzdávali podnety k možným zlepšeniam alebo na odstránenie nedostatkov.

Priebežná revízia predpisov a ich dodržiavanie zabezpečuje dosahovanie žiadúcej úrovne bezpečnosti a ochrany osobných údajov. Cieľom analýzy nedostatkov je dosiahnuť zlepšenie bezpečnostnej situácie a udržiavať bezpečnosť systémov ICT na úrovni zodpovedajúcej súčasnému stavu techniky.

Bamberg, 02.05.2018

| - vedenie spoločnosti - | | splnomocnenec za informačnú bezpečnosť |
|---|---|---|
| Thomas Mai | Stefan Frey | Ralf Ruf |