Wytyczne dotyczące bezpieczeństwa informacji

Zarząd uchwala niniejszym następujące wytyczne dotyczące bezpieczeństwa informacji jako element składowy swojej strategii:

Znaczenie przetwarzania informacji

Przetwarzanie informacji odgrywa kluczową rolę dla działalności naszego przedsiębiorstwa. Wszystkie istotne strategiczne i operacyjne funkcje i zadania są w znacznym stopniu wspomagane przez technologię informacyjną i komunikacyjną (information and communication technology – ICT). Konieczna jest możliwość przywrócenia sprawności systemów ICT po awarii w krótkim czasie. Nasza działalność nie może zostać przerwana nawet w obszarach częściowych. Ponieważ nasza kluczowa kompetencja polega na partnerskim rozwoju innowacyjnych produktów we współpracy z klientami i dostawcami, ochrona tych informacji przed nieupoważnionym dostępem oraz niedozwolonymi zmianami ma fundamentalne znaczenie.

Cele ogólne

Nasze dane oraz systemy ICT we wszystkich obszarach uzależnionych od technologii oraz działach handlowych są zabezpieczone pod względem *dostępności* w taki sposób, że spodziewane okresy przestoju mogą być tolerowane. Przypadki nieprawidłowego działania oraz odstępstwa w zakresie danych i system ICT są akceptowalne tylko w niewielkim zakresie i jedynie w wyjątkowych przypadkach (*integralność*). Wymogi w zakresie *poufności* znajdują się na normalnym poziomie, zorientowanym na zgodność z przepisami prawnymi. W przypadku danych konstrukcyjnych naszych klientów oraz działu rozwoju obowiązują maksymalne wymogi pod względem poufności.

Standardowe środki bezpieczeństwa muszą znajdować się w ekonomicznie uzasadnionym stosunku do wartości podlegających ochronie informacji oraz systemów ICT. Konieczne jest zapobieganie przypadkom szkód o wysokich skutkach finansowych.

Wszyscy pracownicy przedsiębiorstwa przestrzegają odnośnych przepisów (np. ustawy i regulacje dotyczące ochrony danych) wewnętrznych procedur i instrukcji roboczych oraz zawartych regulacji umownych. Należy unikać negatywnych skutków finansowych i niematerialnych dla przedsiębiorstwa oraz dla pracowników w wyniku naruszenia prawa oraz warunków umowy.

Wszyscy pracownicy oraz kierownictwo przedsiębiorstwa są świadomi swojej odpowiedzialności w zakresie obchodzenia się z systemami ICT i dokładając wszelkich starań wspierają strategię bezpieczeństwa.

Cele szczegółowe

Wydane z opóźnieniem lub błędne decyzje w zakresie zarządzania mogą pociągać za sobą daleko idące skutki. Dlatego dostęp do aktualnych danych podczas podejmowania ważnych decyzji ma dla

kadry kierowniczej szczególne znaczenie. Dla tych informacji należy zagwarantować wysoki stopień bezpieczeństwa w odniesieniu do dostępności i integralności.

Przepisy dotyczące ochrony danych osobowych oraz interesy naszych pracowników wymagają zapewnienia poufności danych pracowników. Dlatego też dane oraz aplikacje ICT w dziale kadr podlegają wysokiej ochronie poufności. To samo dotyczy danych naszych partnerów biznesowych.

Dane dotyczące zapytań i ofert od i dla naszych klientów oraz dane konstrukcyjne naszych klientów i naszego działu rozwoju podlegają bardzo wysokim wymogom w zakresie poufności. Ich utrata lub kradzież mogą powodować niekorzystną sytuację pod względem konkurencyjności lub skierowane przeciwko nam roszczenia odszkodowawcze. Zastosowane środki techniczne oraz duża staranność pracowników zapewniają ochronę poufności oraz zapobiegają manipulacjom.

Dla działów logistyki i zakładów produkcyjnych zapewniona jest dostępność oraz bezbłędne działanie systemów. Czasy przestoju są akceptowalne jedynie w bardzo niewielkim zakresie, ponieważ mogą one zarówno bezpośrednio jak i pośrednio prowadzić do zmniejszenia zysków oraz negatywnie wpływać na zadowolenie klientów.

Korzystanie z Internetu oraz aplikacji portalowych w celu uzyskiwania informacji oraz do komunikacji jest dla nas oczywiste. E-mail służy jako zamiennik lub jako uzupełnienie innych dróg komunikacji biurowej. Zastosowanie odpowiednich środków pozwala zagwarantować, że ryzyko korzystania jest tak niewielkie, jak to możliwe.

Zarządzanie bezpieczeństwem informacji

W celu osiągnięcia celów związanych z bezpieczeństwem informacji utworzona została organizacja bezpieczeństwa. Wyznaczony został pełnomocnik ds. bezpieczeństwa informacji. Pełnomocnik ds. bezpieczeństwa informacji odpowiada bezpośrednio przed zarządem.

Zarząd przekazuje do dyspozycji pełnomocnika ds. bezpieczeństwa informacji wystarczające zasoby finansowe i czasowe, by mógł on regularnie się dokształcać i informować, a także realizować cele związane z bezpieczeństwem informacji, wyznaczone przez kadrę kierowniczą.

Administratorzy bezpieczeństwa ICT oraz pełnomocnik ds. bezpieczeństwa informacji są wspierani w swej pracy przez użytkowników ICT.

Pełnomocnik ds. bezpieczeństwa informacji musi być włączany we wszystkie projekty we właściwym czasie, aby aspekty istotne dla bezpieczeństwa zostały uwzględnione już w fazie planowania. Jeśli w

danym przypadku wykorzystywane są dane osobowe, to samo dotyczy pełnomocnika ds. ochrony danych.

W kwestiach istotnych z punktu widzenia bezpieczeństwa użytkownicy ICT muszą przestrzegać instrukcji pełnomocnika ds. bezpieczeństwa informacji.

Środki bezpieczeństwa

Dla wszystkich procedur, informacji, aplikacji ICT oraz systemów ICT wyznaczana jest osoba odpowiedzialna, która określa potrzeby w zakresie ochrony i przyznaje uprawnienia dostępu.

Dla wszystkich odpowiedzialnych stanowisk należy wyznaczyć zastępstwa. Poprzez instrukcje i odpowiednią dokumentację należy zapewnić, że zastępcy są w stanie wypełniać swoje zadania.

Budynki i pomieszczenia są chronione przez wystarczającą kontrolę dostępu. Dostęp do systemów ICT jest chroniony przez odpowiednie kontrole dostępu, a dostęp do danych – przez restrykcyjną koncepcję uprawnień.

We wszystkich systemach ICT stosowane są programy antywirusowe. Dostęp do Internetu jest zabezpieczony odpowiednimi systemami firewall. Wszystkie programy antywirusowe są skonfigurowane i administrowane w taki sposób, że stanowią skuteczną ochronę i zapobiegają manipulacjom. Ponadto użytkownicy ICT wspierają stosowane środki bezpieczeństwa wykonując swoją pracę ze świadomością zasad bezpieczeństwa, a w przypadku wykrycia nieprawidłowości informują wyznaczone do tego organy.

Nigdy nie można całkowicie wykluczyć przypadków utraty danych. Kompleksowe zabezpieczenie danych pozwala więc zagwarantować, że praca systemów ICT może zostać ponownie podjęta po krótkim czasie, kiedy części operacyjnego zbioru danych zostaną utracone lub są niewątpliwie błędne. Informacje są oznaczone w sposób jednoznaczny i przechowywane w taki sposób, że możliwe jest ich szybkie odnalezienie.

W celu ograniczenia większych szkód na skutek nagłych przypadków lub też zapobiegania im, konieczne jest szybkie i konsekwentne reagowanie na zdarzenia związane z bezpieczeństwem. Środki podejmowane w nagłych przypadkach zostały przedstawione w oddzielnej koncepcji gotowości na wypadek sytuacji wyjątkowej. Naszym celem jest podtrzymanie krytycznych procesów biznesowych nawet podczas awarii systemu i przywrócenie dostępności systemów w dopuszczalnym okresie czasu.

Jeśli usługi ICT zlecane są instytucjom zewnętrznym, konkretne wymogi w zakresie bezpieczeństwa są przez nas określane w umowach o gwarantowanym poziomie świadczenia usług. W przypadku, gdy w celu realizacji umowy konieczne jest udostępnienie dostawcom danych o wysokim stopniu ochrony, są oni wówczas odrębnie i wyraźnie zobowiązani do zachowania poufności. Ustalane jest również prawo do kontroli.

Użytkownicy ICT biorą udział w szkoleniach w zakresie prawidłowego korzystania z usług ICT oraz związanych z nimi środków bezpieczeństwa. Kierownictwo przedsiębiorstwo wspiera przy tym odpowiednie do zapotrzebowania dokształcanie i doskonalenie zawodowe.

Poprawa bezpieczeństwa

System zarządzania bezpieczeństwem informacji jest regularnie kontrolowany pod kątem aktualności i skuteczności. Ponadto również podejmowane środki będą regularnie kontrolowane pod kątem tego, czy są znane pracownikom, których to dotyczy, a także czy są możliwe do zrealizowania oraz do zintegrowania z działalnością operacyjną zakładu.

Kierownictwo przedsiębiorstwa wspiera ciągłe zwiększanie poziomu bezpieczeństwa. Pracownicy są zachęcani do zgłaszania odpowiednim organom propozycji ulepszeń lub potencjalnych słabych punktów.

Dzięki ciągłej rewizji regulacji oraz ich przestrzeganiu zapewniony jest poziom bezpieczeństwa i ochrony danych, do którego dążymy. Analiza odstępstw na celu poprawę sytuacji w zakresie bezpieczeństwa oraz ciągłe utrzymywanie poziomu bezpieczeństwa ICT w aktualnym stanie.

Bamberg, 02.05.2018

- Zarząd -

Thomas Mai

Stefan Frey

- Pełnomocnik
ds. bezpieczeństwa informacji –

Ralf Ruf