Slajd 1

Firma TechMach jest firmą zajmującą się produkcją precyzyjnych części mechanicznych dla różnych branż w tym motoryzacyjnej i lotniczej.

jest tu około 50 pracowników i 60 urządzeń zaczynając od komputerów stacjonarnych po maszyny CNC do fizycznych serwerów.

Slajd 2

Aktywa naszej firmy to przedewszystkim

- Strona internetowa
- Wszelkiego rodzaju sprzęty fizyczne
- Organizacja bazy danych
- Organizacja pracowników

Slajd 3

Jeśli chodzi o potencjalne zagrożenia to jest ich całkiem sporo, na slajdzie wylistowaliśmy kilka z najważniejszych z nich, wśród nich możemy znaleźć takie rzeczy jak

- Wszelkiego rodzaju zagrożenia wewnętrzne takie jak
    - Wycieki informacji
    - Hasła na kartkach
    - Brak odpowiednich uprawnień
- Oraz zagrożenia zewnętrzne
    - Phising
    - ataki DDOS
    - Wirusy komputerowe

Slajd 4

Potencjalnych źródeł ryzyka może być całkiem sporo jednak z tych istotniejszych mamy na przykład

- Niedoedukowanych pracowników
- Wszelkiego rodzaju awarie
- Błędna konfiguracja sieci

Slajd 5

Ocene ryzyka obliczyliśmy na podstawie przedstawionej tabeli

Slajd 6

Tak się prezentuje ryzyko obliczone dla naszej firmy

Slajd 7

Nasza polityka bezpieczeństwa jest dość długa i wszystko zawiera się w dokumentacji dołączonej w osobnym pliku i porusza z najważniejszych rzeczy o:

- Poufności informacji
- Integralność informacji
- Dostępność informacji
- Rozliczalność operacji wykonywanych na informacjach

Slajd 8

Techniczne środki bezpieczeństwa, podzieliliśmy na Fizyczne oraz programowe

Slajd 9

Do zarządzania naszymi dostępami przygotowaliśmy tabelę z podziałem na rolę i uprawnieniami przypisanymi do każdej roli.

Slajd 10

Nasze szkolenie pracowników będzie składało się z kilku istotnych kroków takich jak:

1. Podstawy Bezpieczeństwa Informacji
2. Zagrożenia dla Bezpieczeństwa Informacji w Kontekście CNC
3. Zasady Bezpieczeństwa Przy Korzystaniu z Narzędzi i Systemów
4. Bezpieczeństwo Informacji w Pracy Biurowej
5. Zapobieganie Incydentom Bezpieczeństwa
6. Testy i Egzaminy Końcowe

Slajd 11

Cała nasza procedura monitorowania i reagowania na incydenty składa się z kilku kroków, takich jak:

1. Ocena Potrzeb i Wymagań
2. Wybór Systemu Monitorowania
3. Wdrożenie Systemu Monitoringu
4. Szkolenia Pracowników
5. Opracowanie Procedur Reagowania na Incydenty
6. Testy Systemu i Procedur

Slajd 12

Następna jest procedura reagowania na same już w sobie incydenty:

1. Wykrycie incydentu
2. Ocena Wpływu i Ustalenie Poziomu Ważności
3. Komunikacja z Klientami
4. Eskalacja do Właściwych Osób Reagujących
5. Delegowanie Ról związanych z Reagowaniem na Incydenty
6. Rozwiązanie Incydentu

Slajd 13

Procedure zarządzania łatkami i aktualizacjami możemy podsumować jako:

1. Utworzenie harmonogramu regularnych aktualizacji oprogramowania.
2. Wdrożenie procedur testowania łatek przed pełnym wdrożeniem.
3. Monitorowanie bieżących aktualizacji bezpieczeństwa dostarczanych przez dostawców.
4. Zapewnienie redundancji systemów w przypadku niepowodzeń podczas procesu aktualizacji.
5. Szkolenie personelu w zakresie procedur aktualizacyjnych i wdrażania łatek.
6. Przeprowadzanie regularnych audytów, aby ocenić skuteczność procesu aktualizacji.

Slajd 14

Nasz audyt bezpieczeństwa składa się z kilku kroków takich jak:

1. Opracowanie planu audytów wewnętrznych i zewnętrznych.
2. Określenie kluczowych obszarów do przeglądu, obejmujących zarządzanie dostępem, zabezpieczenia fizyczne i logikę systemów.
3. Przeprowadzanie audytów zgodnie z harmonogramem, identyfikując i dokumentując potencjalne zagrożenia.
4. Analiza wyników audytów w celu wprowadzenia niezbędnych poprawek i ulepszeń.
5. Utrzymywanie spójności z regulacjami i normami branżowymi w dziedzinie bezpieczeństwa informacji.
6. Edukacja pracowników w zakresie praktyk bezpieczeństwa informacji i ich roli w procesie audytu.

Slajd 15

Wybór dostawców także jest dość złożonym procesem wymagającym kilku etapów weryfikacji:

- Ustalenie standardów bezpieczeństwa dla dostawców i kontrahentów
- Opracowanie procedur oceny i monitorowania dostawców
- Zasady wyboru dostawców

Slajd 16

Ważnym aspektem naszego zespołu będzie specjalista od spraw bezpieczeństwa który musi być na bierząco z najnowszymi nowinkami dlatego przygotowaliśmy poniższy plan:

- Szkolenie dla specjalisty odpowiedzialnego za utrzymanie i monitorowanie systemu bezpieczeństwa
    - Identyfikacja kluczowych obszarów wiedzy
    - Szkolenia dotyczące najnowszych zagrożeń cybernetycznych
- Przygotowanie zespołu do skutecznego reagowania na incydenty
    - Plan reagowania na incydenty
    - Symulacje incydentów