LABORATORIUM BEZPIECZEŃSTWO TECHNOLOGII INFORMATYCZNYCH

Data wykonania ćwiczenia:	21.11.2023
Rok studiów:	3
Semestr:	5
Grupa studencka:	2
Grupa laboratoryjna:	2B

Ćwiczenie nr.	7

Temat: Projekt

Osoby wykonujące ćwiczenia:

1. Igor Gawłowicz
2. Mieszko Niezgoda
3. Dawid Machaj

Katedra Informatyki i Automatyki

Identyfikacja aktywów

Lista aktywów informacyjnych firmy

- Strona internetowa
- Oprogramowanie kontrolujące działanie maszyn
- Sprzęt fizyczny
    - Maszyneria
    - Komputery
        - PCs
        - Server
- Pracownicy
    - Kierownik
    - Pracownicy odpowiedzialni za maszyny
    - Pracownicy odpowiedzialni za komputery
        - Progamistów CNC
        - Operator bazy danych
    - Osoba odpowiedzialna za PR
    - Sprzątaczka
- Baza danych
    - Informacje klientów
        - Dane personalne
        - Informacje o zamówieniach
    - Informacje pracowników
        - Dane personalne
        - Informacje dotyczące warunków zatrudnienia
    - Dane technologiczne
        - Schematy
        - Patenty

Analiza zagrożeń

Potencjalne zagrożenia

- Zagrożenie wewnętrzne
    - Hasła na karteczkach przyczepionych do monitorów
    - Wyciek informacji przez sprzątaczkę
    - Wyciek informacji przez pracownika
    - Brak odpowiednich kwalifikacji pracowników przedzielonych do zadań
    - Brak odpowiednich autoryzacji w dostępie do zasobów
    - Poziom świadomości pracowników odnośnie bezpieczeństwa
- Zagrożenia zewnętrzne
    - Phishing
    - DDOS
    - Wirusy komputerowe
    - Ransomware

Potencjalne źródła ryzyka

- Niedoedukowani pracownicy
- Awaria sprzętu
- Cyberprzestępcy
- Błędna konfiguracja sieci
- Przestrzałe oprogramowanie
- Fizyczne uszkodzenie sprzętu
- Dostęp nieautoryzowanego użytkownika

Ocena ryzyka

Sposób wyznaczania ryzyka wg. Courtney'a

Koncepcja ryzyka wg. Courtney'a

R = P×C

- P – prawdopodobieństwo wystąpienia określoną ilość razy z ciągu roku, zdarzenia powodującego stratę dla organizacji
- C – strata dla danej organizacji będąca wynikiem pojedynczego wystąpienia zdarzenia powodującego stratę

Prawdopodobieństwo wystąpienia zdarzenia	**Wartość parametru f**	**Rząd wielkości szacowanej straty**	**Wartość parametru i**
raz na 300 lat	1	10 PLN	1
raz na 30 lat	2	100 PLN	2
raz na 3 lata	3	1 000 PLN	3
raz na 100 dni	4	10 000 PLN	4
raz na 10 dni	5	100 000 PLN	5
raz na dzień	6	1 000 000 PLN	6
10 razy dziennie	7	10 000 000 PLN	7
100 razy dziennie	8	100 000 000 PLN	8
1000 razy dziennie	9	1 000 000 000 PLN	9

Rozpocznijmy analizę ryzyka dla podanych zagrożeń w kontekście przedstawionej firmy oraz jej aktywów informacyjnych, wykorzystując metodologię wyznaczania ryzyka wg. Courtney'a, gdzie ryzyko (R) jest iloczynem prawdopodobieństwa (P) wystąpienia zdarzenia i straty dla danej organizacji (C).

Tabela ryzyka dla potencjalnych zagrożeń:

Oczywiście, uwzględnięc dane z poprzedniego zestawienia dla wypełnienia tabeli:

Zagrożenie	**Prawdopodobieństwo wystąpienia zdarzenia**	**Wartość parametru f**	**Rząd wielkości szacowanej straty**	**Wartość parametru i**	**Ryzyko (R = P × C)**
Hasła na karteczkach	raz na dzień	6	10 PLN	1	6
Wyciek informacji przez sprzątaczkę	raz na 10 dni	5	100 000 PLN	5	25
Wyciek informacji przez pracownika	raz na 100 dni	4	10 000 PLN	4	16
Brak odpowiednich kwalifikacji pracowników	raz na 30 lat	2	100 PLN	2	4
Brak odpowiednich autoryzacji w dostępie	raz na 3 lata	3	1 000 PLN	3	9
Phishing	raz na 10 dni	5	100 000 PLN	5	25
DDOS	raz na 100 dni	4	10 000 PLN	4	16
Wirusy komputerowe	raz na 30 lat	2	100 PLN	2	4
Ransomware	raz na 100 dni	4	10 000 PLN	4	16
Niedoedukowani pracownicy	raz na dzień	6	1 000 000 PLN	6	36
Awaria sprzętu	raz na 3 lata	3	1 000 PLN	3	9
Cyberprzestępcy	raz na 100 dni	4	10 000 PLN	4	16
Błędna konfiguracja sieci	raz na 10 dni	5	100 000 PLN	5	25
Przestarzałe oprogramowanie	raz na 30 lat	2	100 PLN	2	4
Fizyczne uszkodzenie sprzętu	raz na 100 dni	4	10 000 PLN	4	16
Dostęp nieautoryzowanego użytkownika	raz na dzień	6	1 000 000 PLN	6	36

Polityka bezpieczeństwa

1. Definicja bezpieczeństwa. Przez bezpieczeństwo informacji w systemach IT rozumie się zapewnienie:

- Poufności informacji (uniemożliwienie dostępu do danych osobom trzecim).
- Integralności informacji (uniknięcie nieautoryzowanych zmian w danych).
- Dostępności informacji (zapewnienie dostępu do danych, w każdym momencie żądanym przez użytkownika)
- Rozliczalności operacji wykonywanych na informacjach (zapewnie przechowywania pełnej historii dostępu do danych, wraz z informacją kto taki dostęp uzyskał).

Zarząd Firmy stosuje adekwatne do sytuacji środki aby zapewnić bezpieczeństwo informacji w Firmie.

- Oznaczanie danych

Jako dane podlegające szczególnej ochronie (informacje poufne) rozumie się:

- informacje o realizowanych kontraktach (zarówno planowane, bieżące jak i historyczne),
- informacje finansowe Firmy,
- informacje organizacyjne,
- dane dostępowe do systemów IT,
- dane osobowe,
- informacje stanowiące o przewadze konkurencyjnej Firmy,
- inne informacje oznaczone jako „informacji poufne" lub „dane poufne".

Zasada minimalnych uprawnień

```
W ramach nadawania uprawnień do danych przetwarzanych w systemach IT Firmy należy stosować zasadę „minimalnych uprawnień", to znaczy przydzielać minimalne uprawnienia, które są konieczne do wykonywania pracy na danym stanowisku.

Przykładowo:  pracując na komputerze PC każdy pracownik powinien posiadać tylko takie uprawnienia jakie są wymagane do realizacji swoich obowiązków (a nie na przykład uprawnienia administracyjne).
```

Zasada wielowarstwowych zabezpieczeń

```
System IT Firmy powinien być chroniony równolegle na wielu poziomach.  Zapewnia to pełniejszą oraz skuteczniejszą ochronę danych.

Przykładowo: w celu ochrony przed wirusami stosuje się równolegle wiele technik: oprogramowanie antywirusowe, systemy typu firewall, odpowiednią konfigurację systemu aktualizacji Windows.
```

2. Zasada ograniczania dostępu

Domyślnymi uprawnieniami w systemach IT powinno być zabronienie dostępu. Dopiero w przypadku zaistnienia odpowiedniej potrzeby, administrator IT przyznaje stosowne uprawnienia.

Przykładowo: domyślnie dostęp do bazy przechowującej dane klientów jest zabroniony. Stosowny dostęp zostaje przyznany osobie, której zajmowane stanowisko wiąże się z koniecznością pracy w tego typu systemie.

- Dostęp do danych poufnych na stacjach PC.
- Dostęp do danych poufnych w LAN realizowany jest na przeznaczonych do tego serwerach.
- Dostęp do danych poufnych (udany lub nieudany) na serwerach jest odnotowywany. Lista systemów objętych tego typu działaniami dostępna jest w osobnym dokumencie.
- Jeśli stacja PC jest komputerem przenośnym (laptopem) to musi ona być dodatkowo zabezpieczona (np. z wykorzystaniem szyfrowania dysku twardego – FDE).

- Dostęp do danych poufnych z zewnątrz firmy powinien odbywać się z wykorzystaniem kanału szyfrowanego (np. VPN, dostęp do e-mail poprzez protokół szyfrowany).
- Dostęp do danych poufnych poprzez firmową sieć WiFi powinien odbywać się z wykorzystaniem kanału szyfrowanego (np. VPN).

3. Zabezpieczenie stacji roboczych

- Stacje robocze powinny być zabezpieczone przed nieautoryzowanych dostępem osób trzecich.
- Minimalne środki ochrony to:
    - zainstalowane na stacjach systemy typu: firewall oraz antywirus,
    - wdrożony system aktualizacji systemu operacyjnego oraz jego składników,
    - wymaganie podania hasła przed uzyskaniem dostępu do stacji,
    - niepozostawianie niezablokowanych stacji PC bez nadzoru,
    - bieżąca praca z wykorzystaniem konta nieposiadającego uprawnień administracyjnych.
- Szczegółowe informacje dotyczące korzystania ze stacji roboczych można znaleźć w stosownym dokumencie.

4. Wykorzystanie haseł

- Hasła powinny być okresowo zmieniane.
- Hasła nie mogą być przechowywane w formie otwartej (nie zaszyfrowanej).
- Hasła nie powinny być łatwe do odgadnięcia, to znaczy:
    - powinny składać się z minimum 9 znaków, w tym jeden znak specjalny
    - nie mogą przybierać prostych form, np. 123456789, stanislaw, dom99, haslo, Magda8, itp.
- Hasła mogą być tworzone według łączenia „losowych" (tj nie istniejących w popularnych słownikach) sylab/słów, np,: mal-tra-laza-#topa. W ten sposób można uzyskać długie hasło stosunkowo proste do zapamiętania.

5. Odpowiedzialność pracowników za dane poufne

Każdy pracownik odpowiada za utrzymanie w tajemnicy danych poufnych, do których dostęp został mu powierzony.

1. Monitoring bezpieczeństwa

W celu zapewnienia ochrony informacji Zarząd może stosować monitoring wykorzystania firmowej infrastruktury informatycznej, w szczególności obejmujący następujące elementy:

- analiza oprogramowania wykorzystanego na stacjach roboczych,
- analiza stacji roboczych pod względem wykorzystania nielegalnego oprogramowania / plików multimedialnych oraz innych elementów naruszających Prawo Autorskie,
- analiza odwiedzanych stron WWW,
- analiza godzin pracy na stanowiskach komputerowych,
- analiza wszelakich dostępów (autoryzowanych oraz nieautoryzowanych) do systemów IT będących w posiadaniu Firmy,
- Analiza ruchu sieciowego pod względem komunikacji, szkodliwej dla bezpieczeństwa danych Firmy.

Monitoring bezpieczeństwa musi odbywać się z zachowaniem obowiązującego prawa.

2. Edukacja pracowników w zakresie bezpieczeństwa

Firma dba o cykliczną edukację pracowników w zakresie bezpieczeństwa informacji. Pracownicy w zależności od zajmowanego stanowiska mogą uczestniczyć w szkoleniach z zakresu:

- ochrony Danych Osobowych,
- świadomości istnienia problemów bezpieczeństwa,
- szczegółowych aspektów bezpieczeństwa.

3. Odpowiedzialność pracowników za dane dostępowe do systemów

Każdy pracownik zobowiązany jest do ochrony swoich danych dostępowych do systemów informatycznych. Dane dostępowe obejmują między innymi takie elementy jak:

- hasła dostępowe,
- klucze softwareowe (pliki umożliwiające dostęp – np. certyfikaty do VPN) oraz sprzętowe,
- inne mechanizmy umożliwiające dostęp do systemów IT.

  Przykłady ochrony danych dostępowych:

- nieprzekazywanie dostępów do systemów IT innym osobom (np. przekazywanie swojego hasła dostępowego osobom trzecim),
- nieprzechowywanie danych w miejscach publicznych (np. zapisywanie haseł dostępowych w łatwo dostępnych miejscach),
- Ochrona danych dostępowych przed kradzieżą przez osoby trzecie.

6. Transport danych poufnych przez pracowników

Zabrania się przenoszenia niezabezpieczonych danych poufnych poza teren Firmy. W szczególności zabrania się przenoszenia danych poufnych na nośnikach elektronicznych (np.: pendrive, nośniki CD) poza teren Firmy.

7. Korzystanie z firmowej infrastruktury IT w celach prywatnych

Zabrania się korzystania firmowej infrastruktury IT w celach prywatnych.

8. Sieć lokalna (LAN).

Sieć lokalna musi być odpowiednio chroniona przed nieuprawnionym dostępem, przykładowo:

- istotne serwery muszą być odseparowowane od sieci klienckich,
- gniazdka sieciowe dostępne publiczne muszą być nieaktywne,
- goście nie mogą uzyskiwać dostępu do sieci LAN.

Szczegółowe informacje dotyczące przyjętych metod ochrony zostały zawarte w osobnej procedurze.

9. Systemy IT / serwery

- Systemy IT przechowujące dane poufne (np. dane osobowe) muszą być odpowiednio zabezpieczone.
- W szczególności należy dbać o poufność, integralność i rozliczalność danych przetwarzanych w systemach.
- Szczegółowe informacje dotyczące przyjętych metod ochrony zostały zawarte w osobnej procedurze.

10. Dokumentowanie bezpieczeństwa

Firma prowadzi dokumentacje w zakresie:

- obecnie wykorzystywanych metod zabezpieczeń systemów IT,
- budowy sieci IT,
- ewentualnych naruszeń bezpieczeństwa systemów IT,
- dostępów do zbiorów danych / systemów udzielonych pracownikom.

Wszelkie zmiany w obszarach objętych dokumentacją, uwzględniane są w tejże dokumentacji.

11. Dane osobowe

Szczegółowe wytyczne dotyczące przetwarzania danych osobowych zawarte są w osobnym dokumencie.

12. Publiczne udostępnianie infrastruktury IT

Infrastruktura udostępniona publicznie musi być szczególnie zabezpieczona. Przykładowe środki bezpieczeństwa:

- Separacja od sieci LAN (np. z wykorzystaniem strefy DMZ)
- Wykonanie hardeningu systemu (zwiększenia bezpieczeństwa oferowanego domyślne przez system)
- Wewnętrzna lub zewnętrzna weryfikacja bezpieczeństwa systemu (np. poprzez realizację testów penetracyjnych)

13. Kopie zapasowe.

- Każde istotne dane (w tym dane poufne) powinny być archiwizowane na wypadek awarii w firmowej infrastrukturze IT.
- Nośniki z kopiami zapasowymi powinny być przechowywane w miejscu uniemożliwiającym dostęp osobom nieupoważnionym.
- Okresowo kopie zapasowe muszą być testowane pod względem rzeczywistej możliwości odtworzenia danych.

14. Dostęp do systemów IT po rozwiązaniu umowy o pracę

W przypadku rozwiązania umowy o pracę z pracownikiem, dezaktywowane są wszelakie jego dostępy w systemach IT.

1. Naruszenie bezpieczeństwa

   Wszelakie podejrzenia naruszenia bezpieczeństwa danych w Firmie należy zgłaszać w formie ustnej lub za pośrednictwem poczty elektronicznej do Zarządu Spółki.

   Każdy incydent jest odnotowywany w stosownej bazie danych, a Zarząd Firmy podejmuje stosowne kroki zaradcze.

2. Weryfikacja przestrzegania polityki bezpieczeństwa.

   Zarząd okresowo wykonuje wewnętrzny lub zewnętrzny audyt bezpieczeństwa mający na celu wykrycie ewentualnych uchybień w realizacji założeń polityki bezpieczeństwa.

Techniczne środki bezpieczeństwa

Fizyczne	**Programowe**
Firewall	Antywirus
Fizyczne kopie zapasowe	Szyfrowanie danych
Monitoring	Narzędzia kontrolujące ruch sieciowy
Identyfikatory/karty dostępu	VPN
Kontrola dostępu	Aktualizacje systemu
Zabezpieczenia antywłamaniowe	Zarządzanie podatnościami
	Audyt bezpieczeństwa
	Szkolenia pracowników
	Identyfikacja pracowników

Wdrożone technologie

- **RSA 512**
  - Bezpieczeństwo szyfru polega na trudności faktoryzacji dużych liczb złożonych, a jego działanie oparto o zastosowanie klucza publicznego i prywatnego.
- **TLS 1.3**
  - Transport Layer Security (TLS) to protokół kryptograficzny zapewniający bezpieczne połączenie i przesyłanie danych między serwerem a klientem w sieciach komputerowych. TLS stosuje szyfrowanie, uwierzytelnianie oraz integralność danych w celu ochrony informacji przesyłanych przez Internet.
- **VPN**
  - *ExpressVPN*
    - Usługa VPN oferowana przez firmę Express VPN International Ltd., zarejestrowaną na Brytyjskich Wyspach Dziewiczych. Oprogramowanie jest promowane jako narzędzie zapewniające bezpieczeństwo i poufność danych poprzez szyfrowanie ruchu internetowego użytkowników i maskowanie adresów IP.
- **NetFlow Analyzer**
  - Internetowe narzędzie do monitorowania ruchu sieciowego, analizujące dane eksportowe NetFlow z routerów Cisco monitorując ruch, w tym rozmiar ruchu, prędkość ruchu, pakiety, głównych mówców, wykorzystanie przepustowości i

czas największego wykorzystania.

- **Monitoring CCTV**
    - Monitoring wizyjny, wideonadzór, telewizyjny system dozorowy – system pozwalający na śledzenie z odległości zdarzeń rejestrowanych przez jedną do nawet kilkuset kamer przemysłowych.

Dodatkowe technologie:

- **Systemy detekcji ataków (IDS) i prewencji (IPS)**
    - Wprowadzenie systemów monitorujących ruch sieciowy w czasie rzeczywistym w celu wykrywania i reagowania na potencjalne ataki.
- **Oprogramowanie do zarządzania incydentami**
    - Wdrożenie systemu do skutecznego zarządzania incydentami bezpieczeństwa, w tym śledzenia, reagowania i raportowania.
- **Zabezpieczenia przed ransomware**
    - Wprowadzenie technologii skanowania zachowań plików i zaawansowanego oprogramowania anty-ransomware.

Zarządzanie dostepem

Autentykacja użytkownika będzie się odbywała za pomocą loginu i hasła.

Role w Firmie	Technik Serwisu CNC	Operator Maszyny CNC	Kierownik Produkcji	Specjalista ds. Bezpieczeństwa IT	Asystent Biurowy	Administrator Sieci	Administrator Bazy Danych
Dostęp do danych	Brak	Brak	Pełen	Ograniczony	Ograniczony	Ograniczony	Pełen
Zarządzanie finansami	Brak	Brak	Ograniczony	Brak	Ograniczony	Ograniczony	Ograniczony
Uprawnienia do zmian w systemie	Ograniczony	Brak	Ograniczony	Pełen	Ograniczony	Pełen	Ograniczony
Prawo do zatwierdzania transakcji	Brak	Brak	Ograniczony	Ograniczony	Ograniczony	Ograniczony	Ograniczony
Tworzenie nowych kont	Brak	Brak	Ograniczony	Ograniczony	Ograniczony	Ograniczony	Ograniczony
Dostęp do konfiguracji maszyn CNC	Pełen	Ograniczony	Brak	Ograniczony	Ograniczony	Ograniczony	Ograniczony
Dostęp do bazy danych	Ograniczony	Brak	Ograniczony	Ograniczony	Ograniczony	Ograniczony	Pełen

Audyt dostępów do systemu zawierający dane:

- Logowania
- Podjętych operacji
- Działań użytkownika

Szkolenie dla Pracowników

Oczywiście, uwzględnienie pracowników biurowych niezwiązanych bezpośrednio z obsługą maszyn CNC jest istotne ze względu na ogólne zasady bezpieczeństwa informacji w firmie. Poniżej przedstawiam zaktualizowany program szkoleń obejmujący zarówno pracowników biurowych, jak i tych zajmujących się obsługą maszyn CNC:s

Cele Szkolenia:

1. Zrozumienie podstawowych zasad bezpieczeństwa informacji.
2. Rozpoznawanie potencjalnych zagrożeń dla bezpieczeństwa informacji w środowisku pracy.
3. Zapoznanie się z narzędziami i technikami zapewniającymi ochronę informacji.

Moduły Szkoleniowe:

1. Podstawy Bezpieczeństwa Informacji

- Definicja bezpieczeństwa informacji.
- Wpływ niewłaściwego bezpieczeństwa informacji na firmę i klientów.
- Znaczenie świadomości bezpieczeństwa informacji dla pracowników.

2. Zagrożenia dla Bezpieczeństwa Informacji w Kontekście CNC

- Rozpoznawanie potencjalnych zagrożeń związanych z obsługą maszyn CNC.

- Przykładowe przypadki naruszeń bezpieczeństwa informacji w kontekście maszyn CNC.
- Szkodliwe skutki braku bezpieczeństwa informacji w tej branży.

3. Zasady Bezpieczeństwa Przy Korzystaniu z Narzędzi i Systemów

- Wprowadzenie do zasad bezpiecznego korzystania z narzędzi, oprogramowania i systemów w kontekście maszyn CNC.
- Omówienie procedur zabezpieczania danych i wrażliwych informacji w procesie obsługi maszyn.

4. Bezpieczeństwo Informacji w Pracy Biurowej

- Zasady bezpiecznego przechowywania i udostępniania danych w biurze.
- Ochrona informacji poufnych, danych klientów i wrażliwych dokumentów biurowych.
- Znaczenie świadomości zagrożeń cybernetycznych dla pracowników biurowych.

5. Zapobieganie Incydentom Bezpieczeństwa

- Techniki zapobiegania incydentom związanym z bezpieczeństwem informacji.
- Praktyki ochrony przed atakami z zewnątrz i wewnątrz firmy.
- Działania w sytuacji incydentu bezpieczeństwa - plan reagowania.

6. Testy i Egzaminy Końcowe

- Sprawdzenie zrozumienia zasad bezpieczeństwa informacji przez pracowników poprzez testy zakończeniowe.
- Egzamin końcowy oceniający zdobytą wiedzę i świadomość w zakresie bezpieczeństwa informacji.

Metody Szkoleniowe:

- Prezentacje multimedialne prezentujące zagadnienia bezpieczeństwa informacji w kontekście pracy na maszynach CNC oraz w biurze.
- Studia przypadków dotyczących incydentów związanych z bezpieczeństwem informacji w firmach zajmujących się maszynami CNC i biurowych.
- Warsztaty praktyczne z zastosowaniem narzędzi i procedur zapewniających bezpieczeństwo informacji w środowisku pracy.

Monitorowanie i Reagowanie na Incydenty:

Etapy Wdrożenia:

1. Ocena Potrzeb i Wymagań

- Przeprowadzenie analizy potrzeb firmy pod kątem monitorowania i reagowania na incydenty bezpieczeństwa.
- Identyfikacja obszarów wymagających szczególnej uwagi, w tym miejsc, w których konieczne jest wdrożenie systemów monitoringu.

2. Wybór Systemu Monitorowania

- Ocena dostępnych narzędzi i systemów monitoringu bezpieczeństwa informacji.
- Wybór odpowiedniego systemu uwzględniającego specyfikę branży CNC oraz potrzeby firmowe.

3. Wdrożenie Systemu Monitoringu

- Instalacja i konfiguracja systemu monitorowania bezpieczeństwa informacji.
- Testowanie funkcjonalności systemu w środowisku produkcyjnym i biurowym.

4. Szkolenia Pracowników

- Szkolenie personelu z zakresu korzystania z nowego systemu monitorowania.
- Edukacja zasad reagowania na incydenty bezpieczeństwa oraz korzystania z planu kontynuacji działania.

5. Opracowanie Procedur Reagowania na Incydenty

- Tworzenie procedur reagowania na różnego rodzaju incydenty bezpieczeństwa.
- Wypracowanie planu kontynuacji działania, uwzględniającego zabezpieczenie danych i ciągłość operacyjną w przypadku wystąpienia incydentu.

6. Testy Systemu i Procedur

- Przeprowadzenie testów systemu monitorowania oraz procedur reagowania na incydenty w warunkach symulacyjnych.
- Korekta i ulepszanie procedur na podstawie wyników testów.

Procedury reagowania na incydenty

1. Wykrycie incydentu

- **Monitorowanie i Alerty:** Używanie systemów monitoringu bezpieczeństwa informacji do ciągłego śledzenia i analizowania aktywności sieciowej oraz systemów w celu wykrycia nieprawidłowości, nieautoryzowanych dostępów lub anomalii.
- **Zgłaszanie i Identyfikacja:** Natychmiastowe zgłaszanie wszelkich podejrzanych aktywności do zespołu ds. bezpieczeństwa informacji w celu dokładnej identyfikacji incydentu.

2. Ocena Wpływu i Ustalenie Poziomu Ważności

- **Analiza Skutków:** Ocena skali incydentu, jego potencjalnych skutków i wpływu na operacje firmy.
- **Priorytetyzacja:** Ustalanie poziomu ważności incydentu w celu odpowiedniego zareagowania - od małych incydentów o niewielkim wpływie po poważne, krytyczne incydenty.

3. Komunikacja z Klientami

- **Komunikacja Wewnętrzna:** Informowanie wewnętrznych interesariuszy, włączając personel zarządzający, zespół IT oraz zainteresowane strony w firmie.
- **Komunikacja Zewnętrzna:** Jeśli incydent ma wpływ na klientów lub zewnętrzne interesariusze, należy dostarczyć im odpowiednich informacji, zgodnie z polityką i wymogami ochrony danych.

4. Eskalacja do Właściwych Osób Reagujących

- **Hierarchia Eskalacji:** Określenie łańcucha dowodzenia i procedur eskalacji incydentu do właściwych osób decyzyjnych i specjalistów.
- **Szybka Reakcja:** Ustalenie limitów czasowych dla eskalacji incydentu w zależności od jego poziomu ważności.

5. Delegowanie Ról związanych z Reagowaniem na Incydenty

- **Definicja Ról:** Przydzielenie konkretnych ról i odpowiedzialności w zespole ds. reagowania na incydenty, w tym lidera zespołu, analityków, specjalistów ds. komunikacji itp.
- **Szkolenie i Przygotowanie:** Zapewnienie odpowiedniego przeszkolenia i przygotowania członków zespołu do wykonywania swoich zadań w przypadku incydentu.

6. Rozwiązanie Incydentu

- **Isolacja i Minimalizacja Szkód:** Natychmiastowe działania w celu izolacji incydentu i ograniczenia jego wpływu na infrastrukturę i dane firmy.
- **Przywracanie Systemów:** Wykonanie procedur naprawczych i przywracanie usług, włączając odbudowę danych, zmiany haseł itp.
- **Analiza Incydentu:** Po zakończeniu incydentu przeprowadzenie szczegółowej analizy celem zrozumienia jego przyczyn, sposobów działania oraz wyciągnięcia wniosków mających na celu doskonalenie procedur reagowania na przyszłość.

Zarządzanie Łatkami i Aktualizacje:

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.

Audyt Bezpieczeństwa:

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.

Kontrola Dostawców:

1. **Ustalenie standardów bezpieczeństwa dla dostawców i kontrahentów:**
    - **Zasady dostępu do informacji:**
        - Określenie, kto w dostawcy ma dostęp do kluczowych informacji firmy.
        - Wymaganie korzystania z bezpiecznych metod uwierzytelniania.
    - **Ochrona danych osobowych:**
        - Zapewnienie zgodności z przepisami dotyczącymi prywatności, takimi jak RODO.
        - Określenie, jakie dane są traktowane jako poufne i wymagają szczególnej ochrony.
    - **Zasady przechowywania poufnych danych:**
        - Określenie okresów przechowywania danych w zależności od ich charakteru.
        - Wprowadzenie polityki niszczenia danych w sposób bezpieczny po zakończeniu okresu przechowywania.
2. **Opracowanie procedur oceny i monitorowania dostawców:**
    - **Proces oceny dostawców:**
        - Określenie, jakie dokumenty i informacje są wymagane od dostawcy w celu oceny zgodności z polityką bezpieczeństwa.
        - Ustalenie częstotliwości ocen, szczególnie w kontekście zmieniających się warunków rynkowych. s
    - **Audyty bezpieczeństwa:**
        - Określenie kryteriów audytu, takich jak obecność odpowiednich zabezpieczeń, polityk bezpieczeństwa, i monitoringu dostępu.
        - Przygotowanie procesu monitorowania ciągłego, aby upewnić się, że dostawcy utrzymują ustalone standardy.
3. **Zasady wyboru dostawców**
    - Reputacja w branży
    - Zaufanie
    - Jakość produktów
    - Wydajność

12. Szkolenie Zespołu Bezpieczeństwa:

1. **Szkolenie dla specjalisty odpowiedzialnego za utrzymanie i monitorowanie systemu bezpieczeństwa:**
    - **Identyfikacja kluczowych obszarów wiedzy:**
        - Cyberzagrożenia: Szkolenie z rozpoznawania różnych rodzajów cyberzagrożeń.
        - Bezpieczne praktyki: Zapoznanie z najlepszymi praktykami w zakresie bezpieczeństwa informacji.
        - Nowoczesne narzędzia: Szkolenie z korzystania z najnowszych narzędzi zabezpieczających.
    - **Szkolenia dotyczące najnowszych zagrożeń cybernetycznych:**
        - Kursy omawiające aktualne zagrożenia i metody ich przeciwdziałania.
        - Analiza konkretnych przypadków ataków, aby zrozumieć mechanizmy działania cyberprzestępców.

2. **Przygotowanie zespołu do skutecznego reagowania na incydenty:**
    - **Plan reagowania na incydenty:**
        - Szczegółowe określenie roli każdego członka zespołu w przypadku incydentu.
        - Przeprowadzenie symulacji incydentów w celu sprawdzenia gotowości zespołu.
    - **Symulacje incydentów:**
        - Organizacja symulacji różnych scenariuszy ataków.
        - Analiza reakcji zespołu i identyfikacja obszarów do doskonalenia.