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

$R = P \times C$

- 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

https://securitum.pl/baza-wiedzy/przykladowa-polityka-bezpieczenstwa/

Technizne środki bezpieczeństwa

Fizyczne	Programowe
Firewall	Antywirus
Fizyczne kopie zapasowe	Szyfrowanie danych
Monitoring	Narzędzia kontrolujące ruch sieciowy
Identyfikatory/karty dostępu	VPN

Wdrożone technologie

- RSA 512 Bezpieczeństwo szyfru polega na trudności faktoryzacji dużych liczb złożonych, a jego działanie oparto o zastosowanie klucza publicznego i prywatnego.
- VPN Chroni Twoje połączenie internetowe i prywatność online. VPN tworzy zaszyfrowany tunel dla Twoich danych, chroni Twoją tożsamość w sieci poprzez ukrycie adresu IP i pozwala Ci bezpiecznie korzystać z publicznych hotspotów Wi-Fi
- NetFlow Analyzer Jest internetowym narzędziem do monitorowania ruchu sieciowego, które analizuje dane eksportowe NetFlow z routerów Cisco monitorując ruch, w tym rozmiar ruchu, prędkość ruchu, pakiety, głównych mówców, wykorzystanie przepustowości i czas największego wykorzystania.

Zarządzanie dostepem

Autentykacja użytkownika będzie się odbywała za pomocą loginu i hasła.

Rola	Administrator systemu	Dostęp do komputerów biurowych	Odczyt bazy danych	Modyfikacja bazy danych	Dostęp do urządzeń sieciowych	Konfiguracja maszyn
Pracownik biurowy		X	X			
Pracownik lini produkcyjnej						
Prezes		X	X			
Kierownik działu		X	X			
Administrator sieci		X				X
Administrator bazy danych		X	X	X		
Specjalista od maszyn CNC		X				X

Audyt dostępów do systemu zawierający dane:

- Logowania
- Podjętych operacji

- Działań użytkownika