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

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.

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**	**Modifykacja bazy danych**	**Dostęp do urządzeń sieciowych**	**Konfiguracja maszyn**
Pracownik biurowy		X	X			

Rola	Administrator systemu	Dostęp do komputerów biurowych	Odczyt bazy danych	Modyfikacja bazy danych	Dostęp do urządzeń sieciowych	Konfiguracja maszyn
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