ZARZĄDZANIE BEZPIECZEŃSTWEM INFORMACJI Lab 5 - Przykładowa realizacja zadania na podstawie kancelarii prawnej

SPIS TREŚCI

ZADANIE 1 - AKTYWA

Krok 1: Proszę określić misję funkcjonowania podmiotu (po co podmiot działa) – misja może być wyrażona przez cele, które poprzez swoje funkcjonowanie chce osiągać podmiot. (*Np. Misją funkcjonowania placówki zdrowia jest leczenie pacjentów, dbanie o ich komfort przy dochodzeniu do zdrowia. Powiązanymi z tymi celami będą np. skuteczne leczenie, opieka itd.*).

Celem funkcjonowania kancelarii prawnej jest szeroko rozumiana pomoc prawna. Związane jest z tym przede wszystkim reprezentowanie klientów w sądzie i przed innymi urzędami.

Krok 2: Proszę zidentyfikować 10 procesów realizowanych w analizowanym podmiocie i wpisać je do poniższej tabelki. (*w czytanym przez Państwa tekście M. Ossowskiego wskazano podział na procesy „podstawowe i pomocnicze", „procesy operacyjne i procesy wspomagające" – wychodząc z tego podejścia proszę szeroko myśleć o identyfikacji procesów).

Następnie proszę zaproponować właściciela procesu – czyli podmiot, osobę, która będzie w firmie odpowiedzialna za dany proces.

Lp.	PROCES (NAZWA & KRÓTKI OPIS)	WŁAŚCICIEL
1	Obsługa klienta - podstawowe	Kierownik ds. Obsługi Klienta
2	PR i marketing - podstawowe	
3	Zapewnienie bezpieczeństwa fizycznego - pomocnicze	
4	Zapewnienie bezpieczeństwa technicznego - pomocnicze	
5	Rekrutacja pracowników - pomocnicze	
6	Szkolenia pracowników - pomocnicze	
7	Zarządzanie budżetem firmy - pomocnicze	

8	Zarządzanie danymi - pomocnicze	
9	Doradztwo prawne - podstawowe	
10	Nadzór nad wykonywaniem procesów - zarządczy	
11	Remonty i inwestycje - pomocnicze	
12	Zaopatrzenie - pomocnicze	
13	Reprezentacja klienta - podstawowe	
14	Zarządzanie kadrą (zwolnienia, awanse) - pomocnicze	

Krok 3: Teraz, proszę skupić się wyłącznie na wybranych 4 procesach. Wykorzystując metodę „burzy mózgów” proszę opisać/rozrysować działania, jakie należy podjąć aby zrealizować dany proces (można rozrysować sobie proces na kartce / innym środowisku do rysowania). na kartce).

- obsługa klienta
    - umawianie klientów - osobiście, telefonicznie i internetowo
    - kontakt z klientem
    - doradztwo prawne (udzielanie rad i wskazówek)
    - obsługa prawna klienta (wykonywanie zadań z dziedziny prawa; nie tylko porady, ale też podjęcie działań prawnych, np. organizacja postępowań zakupowych, tworzenie formuł rozliczeniowych, negocjacje i zawieranie umów między klientem a drugim podmiotem (m. in. fuzje i przejęcia), reprezentacja klienta w sądzie i przed innymi urzędami)
- zapewnienie bezpieczeństwa technicznego
    - zabezpieczenie komputerów przenośnych
    - zabezpieczenie telefonów służbowych
    - zabezpieczenie sieci wewnątrz kancelarii
    - zabezpieczenie bazy danych

    - zabezpieczenie serwera
    - współpraca z firmą informatyczną
    - współpraca z zaufanym dostawcą usług chmurowych
- PR i marketing
    - strona internetowa
    - social media
        - Facebook
        - Instagram
        - Twitter
        - YouTube
    - wywiady do gazet, radia i telewizji
    - logo firmy - rozpoznawalność kancelarii
    - newsletter
    - blog
- zarządzanie danymi
    - otrzymywanie i przechowywanie CV kandydatów
    - przechowywanie umów z pracownikami
    - przechowywanie umów z klientami
    - przechowywanie dokumentacji klienta
    - archiwizacja danych
    - niszczenie dokumentacji
    - przechowywanie umów z usługodawcami (firma informatyczna, sprzątająca, catering)
    - przechowywanie informacji niejawnych (poufnych) od strony rządowej
    - przechowywanie faktur

Krok 4: Następnie proszę o wypisanie wszystkich możliwych zasobów/aktywów informacyjnych wykorzystywanych w ramach każdego z 4 realizowanych procesów. Proszę wypisać zarówno aktywa/zasoby podstawowe jak i wspierające.

[przykład: aktywa podstawowe – CV kandydata do pracy; aktywa wspierające – Folder na Google Drive gdzie umieszczane są CV].

[Proszę pamiętać o tym, że aktywa należy rozumieć szeroko].

Proces 1 (obsługa klienta) – Aktywa:

Lp.	AKTYWA
1	dokumentacja klienta
2	serwer
3	strona internetowa
4	programy koordynujące pracę
5	poczta elektroniczna
6	umowy
7	szafa pancerna
8	system CRM
9	drukarka
10	telefon
11	komputer
12	chmura
13	projekty umów między klientem a drugim podmiotem

Proces 2 (zapewnienie bezpieczeństwa technicznego) – Aktywa:

Lp.	AKTYWA
1	antywirus
2	komputer
3	internet
4	drukarki
5	Firewall
6	IDS/IPS
7	serwer
8	telefon
9	umowy
10	poczta elektroniczna
11	informatyk
12	niszczarki
13	strona internetowa
14	routery
15	kable

16	chmura
17	hasła do social media
18	hasła pracowników

Proces 3 (PR i marketing) – Aktywa:

Lp.	AKTYWA
1	strona internetowa
2	informatyk
3	komputer
4	internet
5	poczta elektroniczna
6	social media - Facebook, Instagram, Twitter, YouTube
7	baza danych osób z newslettera
8	kamera
9	aparat
10	gazeta
11	radio

12	telewizja
13	umowy
14	serwer
15	ulotki
16	wizytówki
17	osoba odpowiedzialna za marketing i PR
18	broszury informacyjne
19	system CRM
20	ogłoszenia o działalności firmy
21	logo firmy
22	hasła do social media

Proces 4 (zarządzanie danymi) – Aktywa:

Lp.	**AKTYWA**
1	CV
2	poczta elektroniczna
3	baza danych klientów

4	komputer
5	serwer
6	baza danych pracowników
7	chmura
8	umowy
9	szafa pancerna
10	CRM
11	drukarka
12	niszczarka
13	programy koordynujące pracę
14	baza danych współpracujących podmiotów
15	faktury

Krok 5: Za pomocą poniższej macierzy proszę o określenie związku pomiędzy aktywami/zasobami podstawowymi a wspierającymi. Celem jest zidentyfikowanie, które zasoby/aktywa podstawowe wykorzystują jakie zasoby /aktywa wspierające

AKTYWA PODSTAWOWE	CV	Faktury	Dokumentacja klienta	Umowy	Baza danych klientów	Baza danych współpracujących podmiotów	Baza danych pracowników	Projekty umów między klientem a drugim podmiotem	Ulotki	Broszury informacyjne	Ogłoszenia o działalności firmy	Wizytówki	Logo firmy	Baza danych osób z newslettera	Hasła pracowników	Hasła social media
AKTYWA WSPIERAJĄCE																
Folder na chmurze	+	+	zbyt duże ryzyko	zbyt duże ryzyko		+	+	+	+	+		+	+	+		
Serwer	+	+	+	+	+	+	+	+	+	+		+	+	+	+	+
Szafa pancerna	+	+	+	+				+								
Drukarki	+	+	+	+				+	+	+		+	+			
Niszczarki	+	+	+	+				+								
Strona internetowa									+	+	+	+	+	+		
Programy koordynujące pracę		+	+	+	+	+	+	+	+	+	+	+	+	+		
Poczta elektroniczna	+	+	+					+	+	+	+		+	+		
System CRM			+		+			+						+		
Telefon			+		+	+	+	+	+	+	+					+
Komputer	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
Antywirus	+	+	+	+	+	+	+	+						+	+	+
Internet	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
IDS/IPS	+	+	+	+	+	+	+	+						+	+	+
Firewall	+	+	+	+	+	+	+	+						+	+	+

Informatyk	+	+	+	+	+	+	+	+	+	+	+	+	+	+		
Routery	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
Kable	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
Social media - Facebook, Instagram, Twitter, YouTube									+	+	+	+	+			+
Kamera											+					
Aparat									+	+	+	+				
Gazeta											+		+			
Radio											+					
Telewizja											+		+			
Osoba odpowiedzialna za marketing i PR									+	+	+	+	+	+		+

Krok 6. Proszę ocenić wartość wcześniej zidentyfikowanych aktywów/zasobów podstawowych biorąc pod uwagę kontekst funkcjonowania podmiotu w tym np. uregulowania prawne.

[Wskazówka: określając wartość zasobów proszę wziąć pod uwagę cele funkcjonowania firmy].

AKTYWA PODSTAWOWE	WARTOŚĆ
CV	do użytku wewnętrznego
Faktury	ściśle chronione
Dokumentacja klienta	ściśle chronione
Umowy	ściśle chronione
Bazy danych klientów	do użytku wewnętrznego
Baza danych współpracujących podmiotów	do użytku wewnętrznego
Baza danych pracowników	do użytku wewnętrznego
Projekty umów między klientem a drugim podmiotem	do użytku wewnętrznego
Ulotki	publicznie dostępne
Broszury informacyjne	publicznie dostępne
Ogłoszenia o działalności firmy	publicznie dostępne
Wizytówki	publicznie dostępne
Baza danych osób z newslettera	do użytku wewnętrznego
Logo firmy	publicznie dostępne
Hasła pracowników	ściśle chronione
Hasła social media	ściśle chronione

Krok 7: Proszę zastanowić się nad otoczeniem zewnętrznym firmy – z jakimi podmiotami firma wchodzić będzie w interakcje.

Lp.	Interesariusze
1	Rząd
2	Sąd
3	Prezes URE
4	Przedsiębiorstwa energetyczne
5	Odbiorcy przemysłowi
6	Szkoły wyższe
7	Dostawca prądu
8	Dostawca usług chmurowych
9	Dostawca internetu
10	Firma informatyczna
11	Firma sprzątająca
12	Instytucje państwowe (np. ZUS, Urząd Skarbowy)
13	Sklepy elektroniczne
14	Inne kancelarie prawne

ZADANIE 2 - OCENA RYZYKA

Krok 1: Proszę wrócić do 4 wybranych wcześniej procesów i zidentyfikować maksymalnie dużo zagrożeń, które mogą wpłynąć negatywnie ich przebieg i na wykorzystywane do ich realizacji aktywa (na integralność, poufność, dostępność). Proszę być kreatywnym i wskazać możliwie dużo zdywersyfikowanych źródeł zagrożeń (np. związanych z obszarem osobowym, technologicznym, fizycznym itd.). Scenariusze funkcjonowania podmiotów mają być źródłem inspiracji, należy się nimi posiłkować, ale nie traktować jako wyczerpującego materiału ograniczającego w zadaniu. Proszę także brać pod uwagę wcześniej wskazane informacje jak np. to z jakimi interesariuszami wchodzimy w interakcje.

1 proces [Obsługa klienta] – lista zagrożeń:

- awaria sieci telefonicznej
- awaria sieci Internet
- choroba sekretarki
- wyciek terminarza przez przypadkowe wysłanie
- wyciek terminarza przez atak hakerski
- zainfekowana skrzynka pocztowa (wysyłanie spamu)
- zgubienie telefonu służbowego przez pracownika
- zgubienie komputera przenośnego służbowego przez pracownika
- kradzież sprzętu służbowego
- awaria sprzętu służbowego
- zainfekowanie sprzętu służbowego
- kradzież dokumentacji klienta
- modyfikacja dokumentacji klienta
- zgubienie dokumentacji klienta
- dostęp do dokumentacji klienta przez nieodpowiednie osoby
- nieumyślne zniszczenie dokumentacji klienta (plików na serwerze oraz form papierowych)
- zalanie sprzętu
- awaria serwera
- włamanie do serwera
- wyciek danych klienta z systemu

- przechwytywanie danych klienta podczas umawiania się na spotkanie przez stronę internetową
- przekupienie sekretarki przez konkurencje - udostępnianie dokumentacji klienta, jego danych
- podsłuch spotkań z klientami przez osoby trzecie
- podsłuch telefoniczny
- podszycie pod klienta przez konkurencje w celu infiltracji firmy (np. podłożenie podsłuchu)
- pożar - utrata dokumentacji klienta
- zalanie serwerowni i archiwum - lokalizacja kancelarii w obszarze zalewowym
- awaria prądu
- upadek działalności dostawcy Internetu

2 proces [Zapewnienie bezpieczeństwa technicznego] – lista zagrożeń:

- zgubienie komputera przenośnego służbowego przez pracownika
- zgubienie telefonu służbowego przez pracownika
- kradzież sprzętu służbowego
- zainfekowanie sprzętu służbowego (np. wchodzenie pracowników na zainfekowane strony, pobieranie zainfekowanych plików, aplikacji)
- zainfekowanie serwera
- zainfekowanie chmury
- przyklejenie hasła dostępu na biurku pracownika
- pozostawienie odblokowanego komputera z pełnym dostępem do danych
- włamanie do kancelarii i kradzież sprzętu
- nieumyślne zniszczenie sprzętu służbowego
- awaria sieci Internet
- awaria firewall
- awaria antywirusa
- awaria IDS/IPS
- awaria sprzętu służbowego
- atak typu DDoS lub DoS
- wyciek bazy danych
- dostęp do bazy danych przez osoby trzecie (np. atak SQL injection)
- nieumyślne zniszczenie baz danych

- awaria serwera kancelarii
- zalanie kancelarii - awaria sprzętu, serwera
- pożar kancelarii
- choroba informatyka
- przekupienie informatyka przez konkurencje
- upadek firmy informatycznej
- nieprawidłowe wdrożenie rozwiązań typu firewall, antywirus, IDS/IPS
- przechwytywanie ruchu między pracownikiem pracującym zdalnie a serwerem
- ataki sieciowe
- wyciek danych z chmury
- awaria serwerów, na których są umieszczone dane z chmury
- zawieszenie działalności dostawcy usług chmurowych
- upadek działalności dostawcy Internetu
- tworzenie zbyt prostych haseł
- nieumyślne wyłączenie prądu w serwerowni
- awaria prądu (problem u dostawcy)
- awaria systemu operacyjnego
- brak aktualizacji systemów sprzętu służbowego
- nieumyślne zniszczenie kabli
- ataki na komputery

3 proces [PR i marketing] – lista zagrożeń:

- zgubienie komputera przenośnego służbowego przez pracownika
- zgubienie telefonu służbowego przez pracownika
- kradzież sprzętu służbowego
- zainfekowanie sprzętu służbowego (np. wchodzenie pracowników na zainfekowane strony, pobieranie zainfekowanych plików, aplikacji)
- zainfekowanie serwera
- zainfekowanie chmury
- przyklejenie hasła dostępu na biurku pracownika
- nieumyślne zniszczenie sprzętu służbowego

- awaria sieci Internet
- awaria sprzętu służbowego
- wyciek bazy danych (negatywny wpływ na wizerunek firmy)
- wyciek dokumentacji klienta (negatywny wpływ na wizerunek firmy)
- awaria serwera kancelarii
- zalanie kancelarii - awaria sprzętu, serwera
- pożar kancelarii
- choroba informatyka
- upadek firmy informatycznej
- wyciek danych z chmury (negatywny wpływ na wizerunek firmy)
- awaria serwerów, na których są umieszczone dane z chmury (baza danych z newslettera)
- zawieszenie działalności dostawcy usług chmurowych
- upadek działalności dostawcy Internetu
- tworzenie zbyt prostych haseł do social media
- nieumyślne wyłączenie prądu w serwerowni
- awaria prądu (problem u dostawcy)
- awaria systemu operacyjnego
- zainfekowana skrzynka pocztowa (wysyłanie spamu w newsletterze)
- manipulowanie wypowiedziami pracowników kancelarii w wywiadach (przedstawienie fragmentu wypowiedzi “wyrwanego” z kontekstu negatywnie rzutującego na wizerunek firmy)
- niepoprawna wypowiedź pracownika firmy w wywiadach (negatywny wpływ na wizerunek firmy)
- zainfekowanie strony internetowej
- niszczenie banerów firmy (np. przez kiboli z pobliskiego stadionu)
- choroba osoby odpowiedzialnej za marketing i PR
- zainfekowany blog
- podszywanie się pod kancelarię na social mediach i niszczenie wizerunku firmy
- wystawianie negatywnych opinii przez konkurencję
- kradzież projektów marketingowych
- nieumyślne zniszczenie projektów marketingowych
- zgubienie projektów marketingowych

4 proces [Zarządzanie danymi] – lista zagrożeń:

- zgubienie komputera przenośnego służbowego przez pracownika
- zgubienie telefonu służbowego przez pracownika
- kradzież sprzętu służbowego
- zainfekowanie sprzętu służbowego (np. wchodzenie pracowników na zainfekowane strony, pobieranie zainfekowanych plików, aplikacji)
- zainfekowanie serwera
- zainfekowanie chmury
- przyklejenie hasła dostępu na biurku pracownika
- pozostawienie odblokowanego komputera z pełnym dostępem do danych
- włamanie do kancelarii i kradzież sprzętu
- nieumyślne zniszczenie sprzętu służbowego (niszczenie danych na dysku)
- awaria sieci Internet
- awaria firewall
- awaria antywirusa
- awaria IDS/IPS
- awaria sprzętu służbowego
- wyciek bazy danych
- dostęp do bazy danych przez osoby trzecie (np. atak SQL injection)
- nieumyślne zniszczenie baz danych
- awaria serwera kancelarii
- zalanie kancelarii
- pożar kancelarii
- choroba informatyka
- przekupienie informatyka przez konkurencje
- upadek firmy informatycznej
- nieprawidłowe wdrożenie rozwiązań typu firewall, antywirus, IDS/IPS
- przechwytywanie ruchu między pracownikiem pracującym zdalnie a serwerem
- ataki sieciowe
- wyciek danych z chmury (CV, faktury, projekty umów)
- awaria serwerów, na których są umieszczone dane z chmury

- zawieszenie działalności dostawcy usług chmurowych
- upadek działalności dostawcy Internetu
- nieumyślne wyłączenie prądu w serwerowni
- awaria prądu (problem u dostawcy)
- awaria systemu operacyjnego
- nieumyślne zniszczenie kabli
- ataki na komputery
- awaria poczty elektronicznej
- nieumyślne zniszczenie umów, CV, faktur, itd.
- kradzież dokumentów
- dostęp do dokumentów przez osoby nieupoważnione
- modyfikacja dokumentów
- zgubienie dokumentów
- nieprawidłowa archiwizacja danych
- nieprawidłowe zniszczenie danych
- przekupienie sprzątaczki przez konkurencje

Krok 2: Proszę wybrać 10 zidentyfikowanych zagrożeń i dokonać oceny ryzyka. Wybór konkretnych wartości w ocenie powinien być udokumentowany i wyjaśniony w postaci odpowiedniego komentarza.

Uwaga! Przy ocenie podatności proszę wykazać się kreatywnością i dokonać pewnych teoretycznych założeń (jak również informacji ze scenariusza). Wybór także proszę uzasadnić umieszczając konkretny komentarz.
Np. podatność dla laptopa pracownika oceniona będzie wysoko bowiem zakładamy, że nie ma na nim antywirusa, ani innego zabezpieczenia.
Scenariusze funkcjonowania podmiotów mają być źródłem inspiracji, należy się nimi posiłkować, ale nie traktować jako wyczerpującego materiału ograniczającego w zadaniu.

ID	ZASÓB	ZAGROŻENIE	P	UZASADNIENIE (P)	PoD	UZASADNIENIE PoD	S	UZASADNIENIE S	WYNIK
1	dane wrażliwe klientów; wizerunek firmy; pieniądze	podsłuch telefoniczny	3	Bliskość Ambasady Stanów Zjednoczonych Ameryki i Ambasady Federacji Rosyjskiej oraz informacje o przypadkach podsłuchu telefonicznego w innych kancelariach obsługujących klientów z sektora energetycznego w ostatnim roku.	2	Korzystanie z szyfrowanych komunikatorów.	3	Możliwość infiltracji polskiej gospodarki energetycznej, skompromitowanie firmy, długotrwała utrata klientów. Obowiązek zapłaty odszkodowania dla klienta za wyciek danych.	18
2	dane klientów i firmy; pieniądze	przekupienie sekretarki przez konkurencje	1	Brak tego typu działań wśród tego typu kancelarii w ostatnich latach.	2	Przy odpowiedniej kwocie sekretarka może działać dla konkurencji w sposób trudny do wykrycia.	3	Utrata klientów, wizerunku oraz danych klientów i firmy. Obowiązek zapłaty odszkodowania dla klienta za wyciek danych.	6
3	sprzęt; dane klientów i firmy	brak aktualizacji systemów sprzętu służbowego	1	Pracownicy są zdyscyplinowani w tej kwestii. Dodatkowo przypomina o tym informatyk. Część aktualizacji wykonuje się automatycznie.	1	Informatyk pilnuje, aby system nie był zbyt przestarzały.	3	Zainfekowanie komputerów, telefonów (na Windowsa i Androida jest więcej wirusów, więc szansa jest większa). Rozprzestrzenianie się złośliwego oprogramowania na sprzęty innych pracowników. Może to spowodować utratę, wyciek lub modyfikację danych.	3
4	wszelkie dane rozpowszechnione w firmie; wizerunek firmy	tworzenie zbyt prostych haseł	1	Pracownicy są uświadomieni w tej kwestii. Nigdy nie nastąpiły włamanie na konto pracownika lub konto firmowe na social mediach.	2	Przy ustawianiu hasła wymagana jest długość 10 znaków, w tym znaków specjalnych, cyfr, dużych i małych liter. Podatność średnia, bo pracownik może użyć np. kombinacji swojego imienia i roku urodzenia z jednym znakiem specjalnym.	3	Złamanie hasła daje dostęp do różnych danych firmy, wykluczając dane ściśle chronione, ale dalej to jest poważny incydent. Ponadto złamanie hasła na social media może negatywnie wpłynąć na wizerunek firmy.	6
5	wizerunek firmy; pieniądze	niszczenie banerów firmy	3	W pobliżu znajduje się Stadion Miejski Legii Warszawa, z którego po meczach wychodzą kibole, którzy mogą pod wpływem emocji niszczyć mienie publiczne.	3	Kancelaria nie ma wpływu na kiboli oraz na wprowadzenie dodatkowych zabezpieczeń banerów.	2	Może to negatywnie wpłynąć na wizerunek firmy oraz jej rozpoznawalność. Kancelaria poniesie niewielkie straty finansowe.	18
6	wizerunek firmy	podszywanie się pod kancelarię na social mediach i niszczenie wizerunku firmy	2	Jedna z kancelarii w Warszawie miała z tego tytułu kłopoty ok. 8 lat temu.	3	Nie możemy zapobiec tego typu działaniu. Możemy mu jedynie przeciwdziałać kiedy już wystąpi.	2	Może to negatywnie wpłynąć na wizerunek firmy. Może skutkować utratą potencjalnych klientów. Stali klienci są informowani o incydencie.	12

7	dane wrażliwe klientów, firmy i aplikantów; wizerunek firmy; pieniądze	nieprawidłowe zniszczenie danych	3	Każdy pracownik może zniszczyć dane w sposób nieprawidłowy. Incydent wystąpił w naszej firmie w ostatnim roku.	1	Po ostatnim wystąpieniu incydentu, pracownicy sprawdzają siebie nawzajem pod kątem niszczenia danych.	3	Incydent może spowodować wypłynięcie ważnych danych z firmy. Kancelaria będzie zmuszona wypłacić odszkodowanie. Wpłynie to też na jej wizerunek.	9
8	dane wrażliwe klientów, firmy; wizerunek firmy; pieniądze	dostęp do dokumentów przez osoby nieupoważnione	1	Pracownicy otrzymali ścisłe instrukcje postępowania z dokumentami. Jeśli odchodzą od biurka, muszą je chować do szuflady zamykanej na klucz, który zabierają ze sobą. Monitor pracownika wygasza się automatycznie po 5 sekundach.	1	Nad zabezpieczeniem firmy czuwa informatyk, a szafę pancerną może otworzyć tylko osoba, która zna szyfr. Ponieważ pracownicy pracują w przestrzeni typu open space, nie jest trudno wykryć osobę nieupoważnioną, która próbuje dostać się do jakichś zasobów.	3	Incydent może spowodować wypłynięcie ważnych danych z firmy. Kancelaria będzie zmuszona wypłacić odszkodowanie. Wpłynie to też na jej wizerunek.	3
9	sprzęt; wszelkie dane (za wyjątkiem tych w chmurze); pieniądze	zalanie kancelarii	3	Firma znajduje się na terenie zalewowym. Ponadto ze względu na drastycznie zmieniające się warunki klimatyczne, jest większe prawdopodobieństwo powodzi.	1	Z doświadczenia ostatnich lat wynika, że wały przeciwpowodziowe są skuteczne. Dodatkowo nasza firma znajduje się na półpiętrze. Ponieważ kancelaria ma siedzibę w biurowcu, jest praktycznie niemożliwe zalanie przez firmę zajmującą lokal powyżej. Nie mają pralek, pryszniców i wanien, czyli najczęstszych przyczyn zalania.	3	Zniszczenie dokumentacji i sprzętu. Dodatkowo kancelaria poniesie duże straty finansowe.	9
10	wszelkie dane rozpowszechnione w firmie; sprzęt; pieniądze	zgubienie telefonu służbowego przez pracownika	3	Incydent wystąpił w ciągu ostatniego roku w kancelarii.	3	Nie ma systemu zarządzania urządzeniami mobilnymi. Firma nie ma dużego wpływu na ten incydent.	3	Incydent może spowodować wyciek danych wrażliwych klientów i firmy. Skutkuje to stratą finansową - wypłata odszkodowań oraz zakup nowego sprzętu. Negatywnie wpłynie też na wizerunek firmy.	27

*”wszelkie dane rozpowszechnione w firmie” to projekty umów, bazy danych, i inne dane przechowywane elektronicznie, natomiast “wszelkie dane” obejmują także umowy i dokumentację klienta, a więc dane niedostępne w formie elektronicznej i przechowywane jedynie w formie papierowej w szafach pancernych.

P = prawdopodobieństwo

Pod - podatność

S = skutek

Krok 3: Wynik oceny ryzyka proszę porównać ze skalą. Tam gdzie ryzyko jest nieakceptowalne proszę zaproponować strategię dalszego działania.

ID	ZAGROŻENIE	WYNIK	STRATEGIA DZIAŁANIA
1	podsłuch telefoniczny	duże	transfer ryzyka - zgłoszenie możliwości wystąpienia podsłuchu telefonicznego prowadzony przez wrogi wywiad do polskich służb specjalnych oraz korzystanie z szyfrowanych komunikatorów
5	niszczenie banerów firmy	duże	unikanie ryzyka - umieszczanie banerów w większej odległości od stadionu
6	podszywanie się pod kancelarię na social mediach i niszczenie wizerunku firmy	średnie	transfer ryzyka - wynajęcie agencji PR
7	nieprawidłowe zniszczenie danych	średnie	redukowanie ryzyka - szkolenia z bezpieczeństwa danych dla pracowników
9	zalanie kancelarii	średnie	transfer ryzyka - ubezpieczenie firmy, kopie dokumentów przechowywane w ściśle strzeżonym magazynie (poza miasto, monitoring, dobre zabezpieczenia na klucz i szyfr)
10	zgubienie telefonu służbowego przez pracownika	duże	redukowanie ryzyka - szkolenia pracowników, wprowadzenie szyfrowania dysków na wszystkich urządzeniach przenośnych i systemu zarządzania urządzeniami mobilnymi

Dla sytuacji w której ryzyko jest nieakceptowalne, a decyzja o działaniu polega na zastosowaniu zabezpieczeń, proszę o opisanie owych zabezpieczeń.

ZADANIE 3 - POLITYKI

POLITYKA BEZPIECZEŃSTWA INFORMACJI KANCELARII PRAWNEJ

CEL

Celem polityki bezpieczeństwa informacji, zwanej dalej polityką, jest ochrona danych i aktywów informacyjnych firmy przy użyciu jak najlepszych praktyk.

DEKLARACJA KIEROWNICTWA

Kierownictwo (skład w załączniku 1a) rozumie wagę informacji oraz zobowiązuje się do rygorystycznego spełnienia wszystkich wymogów zawartych w niniejszej polityce oraz zapewnienia środków służących do utrzymania bezpieczeństwa informacji. Kierownictwo zobowiązuje się do regularnego przeglądania, aktualizowania i doskonalenia polityki.

ZAKRES

Polityka skierowana jest do wszystkich pracowników kancelarii. Musi być zaakceptowana również przez obecnych (załącznik 1b do niniejszej do polityki), a także przyszłych interesariuszy.

DEFINICJE

Bezpieczeństwo - stan, w którym informacje są zabezpieczone przed nieuprawnionym odczytem, modyfikacją lub usunięciem, a aktywa przed nieautoryzowanym dostępem. Natomiast obydwa mają zapewniony ciągły dostęp dla osób, które są upoważnione.
Pracownik kancelarii (zwany dalej pracownikiem) - osoba związana z kancelarią umową o pracę.
Informacje - dane firmy, klientów, pracowników w formie elektronicznej oraz papierowej.
Urządzenia mobilne - elektroniczne urządzenia przenośne z dostępem do Internetu (laptop, smartfon, tablet).
Praca zdalna - wykonywanie obowiązków pracowniczych poza siedzibą firmy.
Incydent - naruszenie lub groźba naruszenia bezpieczeństwa.
Podatność - każda okoliczność działająca na korzyść wystąpienia incydentu.
Analiza ryzyka - oszacowanie prawdopodobieństwa danego incydentu wraz z konsekwencjami jego wystąpienia po uwzględnieniu podatności.

Bezpieczeństwo techniczne - stan, w którym zapewnione jest utrzymanie właściwego funkcjonowania urządzeń wykorzystywanych w kancelarii.

KLUCZOWE WYTYCZNE

1. Każdy pracownik ma obowiązek klasyfikować informacje oraz postępować zgodnie z wytycznymi dotyczącymi ich ochrony (załącznik 1c).
2. Każdy pracownik korzystający z komputera stacjonarnego w firmie ma obowiązek postępowania zgodnie z regulaminem dotyczącym korzystania z komputera (załącznik 1d).
3. Każdy pracownik korzystający z urządzeń mobilnych ma obowiązek postępowania zgodnie z regulaminem dotyczącym korzystania z urządzeń mobilnych (załącznik 1e).
4. Każdy pracownik pracujący zdalnie ma obowiązek postępowania zgodnie z regulaminem dotyczącym pracy zdalnej (załącznik 1f).
5. Każdy pracownik pracujący w przestrzeni typu open space ma obowiązek postępowania zgodnie z regulaminem dotyczącym pracy w przestrzeni typu open space (załącznik 1g).
6. Każdy pracownik ma obowiązek udziału w szkoleniach z bezpieczeństwa podnoszących jego kompetencje w tym zakresie oraz zapoznania się z harmonogramem szkoleń w załączniku 1h.
7. Każdy pracownik ma obowiązek zgłaszania incydentów i podatności zgodnie z regulaminem (załączniku 1i).
8. Kancelaria zobowiązuje się do okresowego przeprowadzania analizy ryzyka zgodnie z zasadami (załącznik 1j).
9. Osoba odpowiedzialna za bezpieczeństwo techniczne ma obowiązek postępowania zgodnie z regulaminem (załącznik 1k).

ZNAJOMOŚĆ POLITYKI I KONSEKWENCJE JEJ NARUSZENIA

1. Każdy pracownik ma obowiązek zapoznania się z niniejszą polityką oraz ze wszystkimi jej załącznikami, które go dotyczą, a także potwierdzić to stosownym oświadczeniem.
2. Każdy pracownik ma obowiązek przestrzegania polityki. W razie jej naruszenia, równoważnego z nieprzestrzeganiem obowiązków pracowniczych, mogą zostać wyciągnięte konsekwencje wypływające z Kodeksu pracy.
3. W sytuacji nieuregulowanej polityką, należy zgłosić się do jednej osób z załącznika 1a.

WŁAŚCICIEL

Właścicielem niniejszej polityki jest Jan Kowalski.
Polityka bezpieczeństwa informacji v.1.5.3. jest zgodna z obowiązującymi przepisami prawnymi, standardami i wytycznymi.

ZAŁĄCZNIK 1E DO POLITYKI BEZPIECZEŃSTWA INFORMACJI KANCELARII PRAWNEJ
REGULAMIN DOTYCZĄCY KORZYSTANIA Z URZĄDZEŃ MOBILNYCH

CEL

Celem regulaminu dotyczącego korzystania z urządzeń mobilnych, zwanego dalej regulaminem, jest zapewnienie bezpieczeństwa informacji znajdujących się na nich, a także bezpieczeństwa samych urządzeń.

ZAKRES

Regulamin skierowany jest do wszystkich pracowników kancelarii, którzy korzystają z urządzeń mobilnych.

DEFINICJE

Informatyk - osoba zatrudniona w kancelarii, odpowiedzialna za wdrażanie bezpieczeństwa technicznego.
Konta związane z firmą - konta, na których znajdują się informacje lub dane związane z firmą.
Uwierzytelnianie dwuetapowe - weryfikacja użytkownika złożona z dwóch etapów: wpisanie hasła i kodu OTP przesłanego inną drogą komunikacji.
OTP - jednorazowy kod wykorzystywany przy każdej próbie zalogowania się, wysyłany na maila lub numer telefonu.
Ważne dokumenty - dokumenty o szczególnie dużym znaczeniu dla funkcjonowaniu firmy i utrzymania jej reputacji.
Informacje związane z firmą - dane firmy, klientów, pracowników w formie elektronicznej.
System zarządzania urządzeniami mobilnymi - program umożliwiający kontrolę wyłączenia, włączenia oraz lokalizacji urządzenia mobilnego.
Niezaufane źródła - strony, co do których nie ma pewności czy są bezpieczne.

KLUCZOWE WYTYCZNE

1. Pracownik ma obowiązek dbania o bezpieczeństwo informacji znajdujących się na urządzeniach mobilnych, w szczególności:
    - zgłoszenie się do informatyka w celu szyfrowania dysku urządzenia
    - pozastawianie zgaszonego ekranu po odejściu od urządzenia (niezależnie od okresu nieobecności przy urządzeniu)
    - tworzenie min. 10-znakowych różnych haseł, w tym znaków specjalnych, cyfr, dużych i małych liter do zalogowania się na komputer i kont związanych z firmą
    - korzystanie z 2FA (uwierzytelnianie dwuetapowe) z OTP przy logowaniu na konta związane z firmą
    - nieprzechowywanie haseł w widocznym miejscu
    - zadbanie o tzw. “czysty pulpit”, czyli umieszczanie ważnych dokumentów w innych miejscach urządzenia niż pulpit

- zabezpieczenie katalogów zawierających informacje związane z firmą hasłami

2. Pracownik ma obowiązek dbania o bezpieczeństwo urządzeń mobilnych, w szczególności:
    - zabezpieczenie przed kradzieżą - zgłoszenie się do informatyka w celu włączenia urządzenia do systemu zarządzania urządzeniami mobilnymi
    - zgłoszenie się do informatyka w celu zainstalowania antywirusa
    - niepozostawianie urządzenia bez opieki w miejscach publicznych
    - nieotwieranie linków oraz niepobieranie plików, aplikacji z niezaufanego źródła
    - zachowanie ostrożności przy korzystaniu z urządzenia
    - aktualizowanie systemu operacyjnego oraz aplikacji

WŁAŚCICIEL

Właścicielem niniejszego regulaminu jest Grzegorz Brzęczyszczykiewicz.
Regulamin dotyczący korzystania z urządzeń mobilnych v.1.1.3. jest zgodny z obowiązującymi przepisami prawnymi, standardami i wytycznymi.

ZADANIE 4 - AUDYT

Kancelaria prawna - audyt

1. Polityka “czystego pulpitu” - obserwacja.
2. Poprawne niszczenie dokumentów - sprawdzanie zawartości w koszu na śmieci.
3. Okresowe przeprowadzanie analizy ryzyka - prośba o pokazanie ostatniej analizy ryzyka.
4. Zgłaszanie incydentów - rozmowa z pracownikami i analiza dokumentacji.
5. Przekupienie sekretarki przez konkurencję - socjotechnika.
6. Aktualizacja systemów sprzętu służbowego - sprawdzenie wszystkich (lub pewnej ilości losowo wybranych) urządzeń pod kątem ostatnich aktualizacji oraz rozmowa z informatykiem.
7. Sprawdzenie znajomości polityki bezpieczeństwa u pracowników - rozmowa z pracownikami.
8. Sprawdzenie, po jakim czasie uruchamiają się wygaszacze ekranu - obserwacja.
9. Sprawdzenie, czy szafa pancerna jest zamknięta - doświadczalnie.
10. Próba odtworzenia danych z kopii - doświadczalnie.
11. Pracownicy mają obowiązek wkładania dokumentów do szuflad i zamykania ich na klucz, kiedy odchodzą z biurka - obserwacja.