Arkusz analizy ryzyka

Wyjaśnienie oznaczeń:

P – prawdopodobieństwo, że zagrożenie się zmaterializuje w skali 1 (niskie) – 3 (wysokie)
przy jego określaniu bierzemy pod uwagę już istniejące zabezpieczenia, które obniżają to prawdopodobieństwo

S – negatywny skutek w skali 1(mały) – 3 (duży) jaki incydent (materializacja zagrożenia) wywrze na osobach, których prawa zostaną naruszone w jego wyniku
inaczej: waga incydentu, stopień naruszenia praw w wyniku utraty dostępności, integralności lub poufności przetwarzanych danych

R (ryzyko) = P x S

Każdy szacunek (przyjęcie takich a nie innych wartości P i S) należy uzasadnić. Uzasadnienie załączyć do dokumentacji wraz z arkuszem analizy.

Podjęcie decyzji po oszacowaniu (wyliczeniu) ryzyk:

R pomiędzy 1 a 3 – ryzyko akceptowalne

R = 9 – ryzyko bezwzględnie wymagające redukcji poprzez wprowadzenie dodatkowych zabezpieczeń lub rezygnację z wykonywania czynności powodujących ryzyko

R pomiędzy 4 a 6 – wymaga podjęcia świadomego wyboru – czy ma zostać zaakceptowane czy poddane redukcji

Każdą decyzję trzeba uzasadnić. Uzasadnienie załączyć do dokumentacji.

Data przeprowadzenia analizy: __ __ / __ __ / __ __ __ __

Zagrożenie	**Opis zagrożenia**	**P**	**S**	**R**	**Możliwe zabezpieczenia**
Phishing, cybersquatting (podrabianie stron) Może spowodować wejście na stronę zawierającą złośliwy kod.	• Mail z prośbą o zalogowanie się (pod pretekstem weryfikacji danych lub informowanie o próbie włamania na konto) do „podróbki" strony, np. bankowej, lub pseudo konta gmail i w rezultacie przejęcie hasła lub wykonanie złośliwego kodu. • Zachęcanie do zalogowania się do podrobionej strony o „wiarygodnym" adresie www. Zamiast logować się do www.mbank.pl logowanie byłoby w www.rnbank.pl				• Sprawdzone systemy antywirusowy i antyspamowy • Higiena pracy (brak pośpiechu, koncentracja)
Instalacja i działanie szkodliwego oprogramowania	Szkodliwe oprogramowanie (backdoory, exploity, exploitpaki, keyloggery). *Najczęściej instalowane są poprzez otwarcie „zainfekowanego" załącznika z maila lub poprzez kliknięcie na*				• Stosowanie zasady kasowania wiadomości o treści podejrzanej lub nieadekwatnej do oczekiwań bądź prowadzonej działalności, zwłaszcza od nieznanych nadawców • Stosowanie zasady nieotwierania załączników przy braku pewności co do źródła i spodziewanej zawartości • Sprawdzone systemy antywirusowy i antyspamowy

	zarażoną stronę. Maile takie zachęcają do otwarcia załącznika lub kliknięcia na hiperlink (mail z fakturą do opłacenia, mail z DHL o przesyłce, mail z rzekomym pismem urzędowym). W efekcie możemy zarazić nasz komputer lub wiele komputerów w sieci. Mogą instalować się po odwiedzeniu podejrzanych stron internetowych. Działające szkodliwe oprogramowanie może wywołać różnorodne skutki: • Przejęcie konta pocztowego do wysyłki spamu • Użycie przejętych komputerów do kopania kryptowalut • Użycie przejętych komputerów do ataków DOS • Użycie przejętych komputerów do śledzenia haseł użytkowników celem uzyskania dostępu do systemów i plików • Użycie przejętych komputerów do uzyskania pełnego dostępu do danych (kradzież)				• Korzystanie ze sprawdzonych dostawców poczty elektronicznej • Korzystanie z opcji bezpieczeństwa zapewnianych przez system operacyjny i program pocztowy, nie wyłączanie tych opcji, nie obniżanie domyślnego poziomu bezpieczeństwa • Nieodwiedzanie podejrzanych (głównie z uwagi na treść) stron internetowych, w szczególności związanych z hazardem, pornografią itp.
Podrzucone nośniki danych	Atakujący pozostawia w biurze specjalnie przygotowany pendrive z zainstalowanym samouruchamiającym się szkodliwym programem. W wielu przypadkach z CIEKAWOŚCI ludzie sprawdzają jego zawartość wkładając go do portu USB. W wyniku tego uruchamiają nieświadomie szkodliwe oprogramowanie (backdoory, exploity, exploitpaki, keyloggery).				• Sprawdzony system antywirusowy • Stosowanie zasady niepodłączania do komputera urządzeń nieznanego pochodzenia
Ataki telefoniczne	• Intruz przedstawia się jako „serwisant Orange lub Netii" naprawiający usterkę i prosi o wejście na określoną stronę internetową w ramach testowania łącza internetowego • Intruz przedstawia się jako inżynier Microsoftu lub programista dostawcy oprogramowania. Podsyła „aktualizację" lub prosi o udostępnienie pulpitu				• Stosowanie zasady ignorowania telefonów dotyczących konserwacji sprzętu lub oprogramowania od osób, których tożsamości nie można z całą pewnością ustalić.
Łamanie haseł	Łamanie haseł metodami słownikowymi i siłowymi (*brute force*): • do poczty • do routera				• Polityka haseł (patrz niżej)
Łatwo dostępne, łatwe lub standardowe hasła	• Ujawnianie haseł • Nieprawidłowe przechowywanie (karteczki, pliki) • Stosowanie domyślnych haseł producenta				**Polityka haseł:** • długość hasła - 12 znaków • hasło zawiera duże, małe litery cyfry lub znaki specjalne • częstotliwość zmiany hasła – 60 dni

	• Stosowanie słownikowych lub popularnych haseł, np. Grazynka1, qwerty, 12345678
	• Stosowanie jednego hasła do wielu systemów
					• mechanizm wymuszenia zmiany hasła
					• uwierzytelnianie za pomocą kodu PIN / biometryczne
					• uwierzytelnianie do
					  ○ aplikacji,
					  ○ systemu operacyjnego
					  ○ dysku sieciowego
					  ○ poczty
					  ○ smartfona, tabletu

Ataki na sprzęt - Włamania za pośrednictwem niepotrzebnych usług (np. telnet na routerze)	Atakujący wykorzystuje do włamania usługi sieciowe Zagrożenie dla nast. Usług: • DHCP • DNS • SSH • RDP • PING/Traceroute • http/https • Java (porty 8080, 8443) • telnet • email (IMAP/POP3/SMTP) • FTP *Router posiada często włączone wszystkie możliwe usługi, mimo iż nie wszystkie z nich są potrzebne. Każda z tych usług jest obsługiwana przez oprogramowanie, które może zawierać błędy.*				• Włączone tylko te usługi, które są niezbędne do działania danego środowiska
Ataki na oprogramowanie - Wykorzystanie znanych dziur w nieaktualizowanym oprogramowaniu	Atak z wykorzystaniem znanych dziur w niezaktualizowanym oprogramowaniu Zagrożenie dla systemów/programów • Windows • Przeglądarki www • MS Office • Adobe *Istniejące błędy oprogramowania pozwalające na przełamanie zabezpieczeń są upubliczniane po tym, jak producent oprogramowania przygotuje odpowiednią łatę lub aktualizację. Jeżeli nie zainstalujemy tych aktualizacji, narażamy się na atak, np. zdalny dostęp do systemu lub wykonanie złośliwego kodu (instalacja backdoora, exploita, ransomeware)*				• Włączone aktualizacje automatyczne, unikanie odkładania aktualizacji na później • Informatycy cyklicznie sprawdzają stosowane systemy i programy pod kątem ich aktualności
Podsłuch	• podsłuch danych przesłanych drogą mailową				• szyfrowanie poczty wysyłanej (PGP/GPG, S/MIME)

	• podsłuch podczas korzystania z formularzy kontaktowych				• szyfrowanie połączeń internetowych (SSL/TLS) • szyfrowanie plików wysyłanych mailowo
Włamanie do sieci poprzez WIFI	Uzyskanie dostępu do komputera poprzez włamanie się do sieci bezprzewodowej				• Stosowanie dobrze zabezpieczonej sieci WiFi o dobrym standardzie szyfrowania • Stosowanie silnych haseł dostępu do sieci • Odseparowanie wifi dla gości/klientów od sieci, w której pracuje komputer przetwarzający dane
Atak ransomeware	Ransomeware - Program do szyfrowania plików. Instaluje się z maili lub z hiperlinków w mailach lub poprzez odwiedziny zainfekowanej strony. Odszyfrowanie wymaga zapłaty 500 USD. Bardzo groźny				• Systemy antywirusowy i antyspamowy • Kopie bezpieczeństwa kluczowych danych

Nieuprawniony dostęp lub włamanie do pomieszczeń	Dostęp do:
	• Budynku / mieszkania
	• Pomieszczeń biurowych
	• Archiwów
	• Miejsc przechowywania kopii bezpieczeństwa
	
	Może skutkować:
	• dostępem do danych w wersji papierowej
	• dostępem do plików lub aplikacji lub baz danych
	• zainstalowaniem nieautoryzowanych urządzeń do dostępu do sieci wewnętrznej
	• kradzieżą komputerów, nośników
					• kontrola nad kluczami
					• ograniczona liczba kopii kluczy
					• bezpieczne przechowywanie kluczy
					• formalne ograniczenie dostępu do pomieszczeń osobom nieupoważnionym (zakaz wstępu)
					• rozmieszczenie komputerów /drukarek /xero ograniczające dostęp osób nieupoważnionych
					• Zabezpieczenie dostępu do pomieszczeń
					  ○ drzwi zamykane na klucz
					  ○ drzwi antywłamaniowe
					• Zabezpieczenie dokumentacji / danych w pomieszczeniach
					  ○ zamknięte niemetalowe szafy
					  ○ zamknięte metalowe szafy
					  ○ sejf
					  ○ sejf ogniotrwały
					  ○ skrytki na klucze
					• Polityka czystego biurka
					• Systemy alarmowe / zabezpieczenia antywłamaniowe
					  ○ system alarmowy
					  ○ kraty
					  ○ rolety
					• Ochrona fizyczna obiektu / pomieszczeń
					  ○ firma ochroniarska (zdalny monitoring systemu alarmowego)
					  ○ monitoring wizyjny w obrębie obiektu i otoczeniu

Kradzież / zagubienie sprzętu i nośników poza biurem	Kradzież / zagubienie: • laptopów • smartfonów, • pendrive • dysków wymiennych				**Procedury:** • Regulamin użytkowania komputerów przenośnych • Procedura zabezpieczenia sprzętu mobilnego **Zabezpieczenia:** • Szyfrowanie dysków laptopów (bitlocker, Veracrypt, oprogramowanie systemowe)

					• Stosowanie szyfrowanych dysków przenośnych • Stosowanie szyfrowanych pendrive • Uwierzytelnianie (hasło, odcisk palca) do urządzeń typu smartfon/tablet • Programy/usługi do zdalnego blokowania/czyszczenia smartfonów, tabletów i laptopów
Awarie / uszkodzenia elementów IT	Awarie: • komputera (w tym w szczególności dysku komputera) • routera				• wykonywanie kopii zapasowych • cykliczna wymiana sprzętu na nowszy
Błąd / awaria oprogramowania	Awarie: • systemu operacyjnego • aplikacji • poczty				• wykonywanie kopii zapasowych • włączony okresowy auto-zapis dokumentów • używanie wyłącznie sprawdzonego i legalnego oprogramowania
Pożar / eksplozja	• Pożar obiektu / pomieszczenia				**Zabezpieczenia:** • gaśnice • sejf ogniotrwały • system PPOŻ • używanie materiałów niepalnych • czujnik dymu
Zalanie	• Zalanie pomieszczenia (powódź, zalanie z rur)				• składowanie dokumentacji papierowej na podwyższeniu • digitalizacja dokumentów nie wymagających przechowywania w oryginale
Awaria zasilania	• skoki napięcia • przerwy w dostawie zasilania • Może skutkować brakiem dostępu do danych, jak też awarią sprzętu.				• UPS podtrzymujący zasilanie komputera • Agregat prądotwórczy
Brak / błędy w wykonywaniu kopii bezpieczeństwa	• doraźne lub za rzadkie wykonywanie kopii • błędy podczas procesu wykonywania kopi • niemożność odtworzenia kopii ze względu na zmiany w oprogramowaniu				• wykonywany jest backup aplikacji / plików / konfiguracji / licencji /haseł • backup jest zabezpieczony przed ransomeware • kopie zapasowe przechowywane są w innym miejscu • testuje się możliwość odtworzenia kopii • stosuje się sprawdzone (np. zawarte w systemie) oprogramowanie do wykonywania kopii
Nieprawidłowe / brak procedur niszczenia nośników z danymi	• wyrzucenie uszkodzonych nośników bez ich zniszczenia • wyrzucanie dokumentów papierowych na śmietnik lub • wyrzucenie niezniszczonych HD, pendrive, DVD				• niszczarki • niszczenie/czyszczenie nośników przed utylizacją • firma niszcząca dokumenty
Nieprawidłowe / brak procedur napraw w serwisach zewnętrznych	• naprawa sprzętu z nośnikami bez umowy lub bez standardu bezpiecznej naprawy				• usuwanie nośnika danych (dysku) przed naprawą, o ile możliwe • określanie zasad poufności danych w postaci umowy • korzystanie z profesjonalnych firm oferujących określony standard usługi

Pomyłki i błędy	• pomyłkowe udostępnienie danych • wysłanie do złego odbiorcy, błąd w adresie • nieumyślne usunięcie danych				• stosowanie i regularne przeglądanie elektronicznych książek adresowych, unikanie wpisywania adresów e-mail „z palca” • wykonywanie kopii zapasowych • stosowanie standardowych klauzul (*disclaimers*) w stopce maila, informujących o poufności informacji oraz obowiązku usunięcia wiadomości w przypadku jej nieuprawnionego otrzymania • sprawdzanie tożsamości osób, którym dane są przekazywane
Brak aktualnej dokumentacji (instrukcji) sprzętu i oprogramowania	• Brak instrukcji obsługi sprzętu i oprogramowania • Brak instrukcji instalacji i konfiguracji • *Zagrożenie związane z możliwymi trudnościami w odtworzeniu środowiska i zarządzania nim, gdy np. odejdzie informatyk lub będzie on niedostępny podczas krytycznej awarii*				• staranne, bezpieczne przechowywanie wszelkiej dokumentacji sprzętu i oprogramowania • unikanie przechowywania dokumentacji wyłącznie na sprzęcie, którego dotyczy (w razie awarii będzie ona niedostępna) – wykonywanie kopii lub drukowanie
Nieprawidłowe / brak umowy gwarancyjnej lub wsparcia serwisowego	• zapomniany termin przedłużenia umowy • nieokreślenie standardu udzielanego wsparcia (w szczególności maksymalnych terminów jego udzielenia) • pomylenie czasu reakcji z czasem naprawy • brak umowy				• stosowanie umów o określonym standardzie usług (SLA) • preferowanie umów bezterminowych lub sporządzenie harmonogramu przedłużeń umów • uważna lektura umów przed ich zawarciem
Upadek firmy outsourcingowej lub dostawczej	• ryzyko braku zastępstw, np. dla hostingodawcy poczty, dla wsparcia do zakupionej aplikacji, informatyka				• weryfikacja kondycji dostawcy przed zawarciem umowy • utrzymywanie bazy alternatywnych dostawców
Zgubienie/kradzież dokumentów papierowych poza biurem	• Pozostawienie w środkach komunikacji publicznej, restauracji, innym miejscu publicznym lub nienadzorowanym • Kradzież w wyniku włamania do samochodu • Kradzież w wyniku napaści				• Ograniczenie liczby dokumentów wynoszonych poza miejsce pracy • Stosowanie zasady niepozostawiania dokumentów bez nadzoru (zaparkowany samochód, szatnia)
Przekazanie danych (wykonanych tłumaczeń) osobie nieuprawnionej	• Przekazanie wykonanego tłumaczenia innej osobie niż zleceniodawca (członkowi rodziny, osobie obcej) • Przekazanie wykonanego tłumaczenia innemu zleceniodawcy, w wyniku pomyłki				• Weryfikacja tożsamości na etapie zlecania i odbioru pracy • Utrzymywanie listy zleceniodawców zawierającej dane umożliwiające ustalenie tożsamości (np. nr dow. os.) niezależnie od repertorium (*dane usuwane po odbiorze pracy*)
Nieudzielenie wymaganych prawem informacji o przetwarzaniu danych	• Nieokreślony lub nieszczelny proces udzielania informacji skutkujący możliwością, że osoba, której dane dotyczą nie zostanie prawidłowo poinformowana				• Stosowanie standardowych formularzy papierowych zlecenia usługi, zawierających niezbędne informacje • Uwzględnienie wymaganych informacji w szablonach umów • Zawarcie wymaganych informacji w formularzach internetowych
wymyślaj dalej ☺	•				•
	•				•