Arkusz analizy ryzyka

P-Prawdopodobieństwo incydentu (skala od 1 do 3), S-Skutki wystąpienia incydentu (skala od 1 do 3), R-Ryzyko wystąpienia incydentu (skala od 1 do 9), Formuła: R=P*S

Zagrożenie	Opis zagrożenia	P	S	R	Zabezpieczenie
Phishing, cybersquatting (podrabianie stron)	• 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. • Zachęcanie do zalogowania się do podrobionej strony o „wiarygodnym" adresie www. Zamiast logować się do www.mbank.pl logowanie byłoby w www.rnbank.pl	1	1	1	**Procedura:** • Szkolenia personelu • Polityka Ochrony Danych Osobowych w PWSTE w Jarosławiu **Zabezpieczenie:** • Systemy antywirusowy i antyspamowy • Sewery proxy i bramki filtrujące
Nakłanianie do wykonania czynności	• Mail z dyspozycją podjęcia określonej czynności • Fax/mail z fakturą od rzekomego „dostawcy" z informacją o zmianie numeru konta bankowego do opłacenia faktur	1	1	1	**Procedura:** • Szkolenia personelu • Polityka Ochrony Danych Osobowych w PWSTE w Jarosławiu
Instalacja szkodliwego oprogramowania / działanie szkodliwego oprogramowania	Szkodliwe oprogramowanie (backdoory, exploity, exploitpaki, keyloggery). *Najczęściej instalowane są poprzez otwarcie „zainfekowanego" załącznika z maila lub poprzez kliknięcie na zarażoną stronę. Maile takie zachęcają do otwarcia załącznika lub kliknięcia na hiperlink. W efekcie możemy zarazić nasz komputer lub wiele komputerów w sieci* *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 wewnętrznej sieci i kopiowania danych i baz danych (kradzież)* *Szkodliwe oprogramowanie:* *Wirusy i trojany – instalują się często z nielegalnym oprogramowaniem. Zawierają ukrytą funkcjonalność, działają na szkodę użytkownika.* *Backdoory - Instalują się z maili lub z hiperlinków w mailach.*	1	2	2	**Procedura:** • Szkolenia personelu • Polityka Ochrony Danych Osobowych w PWSTE w Jarosławiu **Zabezpieczenie:** • Systemy antywirusowy i antyspamowy • Sewery proxy i bramki filtrujące

PR

	Po uruchomieniu umożliwiają intruzowi ponowny dostęp i stałą kontrolę nad komputerem. Taki komputer-zombie może być użyty do wszelkich zachcianek intruza. *Keyloggery - Programy przechwytujące hasła wpisywane na klawiaturze przez użytkownika i oddające je intruzowi.* *Exploity / exploitpaki - Oprogramowanie wykorzystujące znane luki w systemach. Uruchomiony pozwala na przejęcie systemu przez intruza.*				
Podrzucone nośniki danych	Atakujący pozostawia w biurze lub w dziale księgowości specjalnie przygotowany pendrive z zainstalowanym samouruchamiającym się szkodliwym programem. W wielu przypadkach pracownicy sprawdzają jego zawartość wkładając go do portu USB. W wyniku tego uruchamiają nieświadomie szkodliwe oprogramowanie (backdoory, exploity, exploitpaki, keyloggery).	2	1	2	**Procedura:** • Szkolenia personelu • Polityka Ochrony Danych Osobowych w PWSTE w Jarosławiu **Zabezpieczenie:** • Blokada portów USB na stacjach roboczych • Dopuszczenie do użycia wyłącznie zakwalifikowanych pendrive
Ataki telefoniczne	• Intruz podający się za „naszego informatyka" prosi o podanie hasła pod pretekstem sprawdzania lub naprawy naszego systemu informatycznego • 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	1	1	1	**Procedura:** • Szkolenia personelu • Polityka Ochrony Danych Osobowych w PWSTE w Jarosławiu
Łamanie haseł	Łamanie haseł metodami słownikowymi i siłowymi (brute force) : • do baz danych • do serwera • do aplikacji www • do poczty • do windows na stacjach roboczych • do routera • do firewalla	2	1	2	**Procedura:** • Instrukcja zarządzania systemami informatycznymi – wykaz zabezpieczeń RODO • Szkolenia personelu **Zabezpieczenia:** • Testy penetracyjne
Łatwo dostępne, łatwe lub standardowe hasła	• Ujawnianie haseł • Nieprawidłowe przechowywanie (karteczki, pliki) • Stosowanie domyślnych haseł producenta • Stosowanie słownikowych lub popularnych haseł, np. Grazynka1, qwerty, 12345678 • Stosowanie jednego hasła do wielu (często wszystkich) systemów	1	1	1	**Procedura:** • Instrukcja zarządzania systemami informatycznymi – wykaz zabezpieczeń RODO • Szkolenia personelu **Zabezpieczenia:** • długość hasła - 8 znaków • hasło zawiera duże, małe litery cyfry lub znaki specjalne • częstotliwość zmiany hasła – 32 dni • mechanizm wymuszenia zmiany hasła

					• uwierzytelnianie do
					  ○ aplikacji,
					  ○ stacji roboczych
					  ○ dysku sieciowego
					  ○ sieci
					  ○ poczty
					• Testy penetracyjne

Ataki na sprzęt - Włamania do urządzeń nieaktualizowanych	Ataki na urządzenia sieciowe oraz inne, które działają dzięki umieszczonemu na nich oprogramowaniu (firmware/ strowniki) Zagrożenie dla nast. elementów: • routery • switche • access pointy • firewall • macierz • dysk NAS • drukarki i skanery *Brak aktualizacji tego oprogramowania skutkuje podatnością na włamania, kradzież danych, zakłócanie pracy.*	1	1	1	**Procedura:** • Instrukcja zarządzania systemami informatycznymi – wykaz zabezpieczeń RODO **Zabezpieczenia:** • Testy penetracyjne • Sondy IPS/IDS
Ataki na sprzęt - Włamania do urządzeń nieodpowiednio skonfigurowanych	Ataki na błędnie skonfigurowany sprzęt lub sprzęt działający z ustawieniami fabrycznymi. Zagrożenie dla nast. elementów: • routery • switche • access pointy • firewall • macierz • dyski NAS • drukarki i skanery *Błędy konfiguracyjne popełniane przez administratorów mogą ułatwiać hackerom włamanie się do sieci lub urządzenia. Powodem jest najczęściej brak profesjonalnej wiedzy u osób konfigurujących urządzenia. Przykładem jest np. pozostawienie domyślnych haseł lub dostępu do strony konfiguracyjnej routera z poziomu Internetu.*	1	2	2	**Procedura:** • Instrukcja zarządzania systemami informatycznymi – wykaz zabezpieczeń RODO **Zabezpieczenia:** • Zmiana domyślnych haseł na urządzeniach • Zmiana domyślnej nazwy konta administratora w urządzeniu • Testy penetracyjne
Ataki na sprzęt - Włamania z użyciem niezabezpieczonych interfejsów lokalnych	Atakujący wpina się do urządzeń IT przez ich niezabezpieczone porty konfiguracyjne (USB, Ethernet lub COM - szeregowe) Zagrożenie dla nast. elementów: • routery • switche	1	1	1	**Procedura:** • Instrukcja zarządzania systemami informatycznymi – wykaz zabezpieczeń RODO **Zabezpieczenia:** • Dostęp do portów fizycznych (gniazd - np. szeregowy, USB, Ethernet) zabezpieczono hasłem, aby przypadkowa osoba, która podłączy do nich swój

	• firewalle • macierze • serwery • drukarki i skanery *Administratorzy często pozostawiają te porty niezabezpieczone, co powoduje ryzyko wpięcia się do powyższych urządzeń i ich skonfigurowania przez hakera.*				komputer nie mogła zmienić konfiguracji. • Umieszczenie krytycznych elementów infrastruktury w zamykanych na klucz szafach serwerowych • Kontrola dostępu do pomieszczeń serwerowni i punktów dystrybucyjnych sieci • Testy penetracyjne
Ataki na sprzęt - Włamania za pośrednictwem niepotrzebnych usług (np. telnet na routerze)	Atakujący wykorzystuje do włamania usługi sieciowe, których działanie w danym środowisku nie jest wymagane Zagrożenie dla nast. Usług: • DHCP • DNS • SSH • http • telnet • FTP • SMTP • SNMP *Urządzenia sieciowe posiadają często włączone wszystkie możliwe usługi sieciowe (DHCP, DNS, SSH, HTTP, telnet, FTP), mimo iż nie wszystkie z nich są potrzebne w danym środowisku. Każda z tych usług jest obsługiwana przez oprogramowanie, które może zawierać błędy.*	1	1	1	**Procedura:** • Instrukcja zarządzania systemami informatycznymi – wykaz zabezpieczeń RODO **Zabezpieczenia:** • Wyłączenie niepotrzebnych serwisów (ogranicza ilość dziur i możliwość przechwycenia / podsłuchania ruchu lub haseł.) • Włączone tylko te usługi, które są niezbędne do działania danego środowiska • Monitorowanie aktywnych usług • Skanery podatności (stosowany jest system wykrywania słabości i zagrożeń) • Security Information and Event Managment (analityczny system do wykrywania zagrożeń • Testy penetracyjne
Ataki na oprogramowanie - Wykorzystanie znanych dziur w nieaktualizowanym oprogramowaniu	Atak z wykorzystaniem znanych dziur w niezaktualizowanym oprogramowaniu Zagrożenie dla programów • Systemy operacyjne na stacjach roboczych • Systemy serwerowe • Przeglądarki www • Wordpress, Drupal, <inne silniki webowe>, <sklepy internetowe>, • Dedykowany CMS • Adobe • Flash • Java • (podaj inne aplikacje niewymienione) *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*	1	2	2	**Procedura:** • Instrukcja zarządzania systemami informatycznymi – wykaz zabezpieczeń RODO **Zabezpieczenia:** • Stosowane jest darmowe/komercyjne oprogramowanie do inwentaryzacji zainstalowanego oprogramowania na stacjach roboczych (serwerach) oraz do kontroli procesu aktualizacji (patche / łatki) • Aktualizacja oprogramowania zgodnie z zaleceniami producentów oraz opinią rynkową co do bezpieczeństwa i stabilności nowych wersji (np. aktualizacje, service pack-i, łatki) • Skanery podatności (stosowany jest system wykrywania słabości i zagrożeń) • Security Information and Event Managment (analityczny system do wykrywania zagrożeń) • Sondy IPS/IDS • Testy penetracyjne

	wykonanie złośliwego kodu (instalacja backdoora, exploita, ransomeware)				
Podsłuch	• podsłuch danych przesłanych drogą mailową • podsłuch danych podczas korzystania z aplikacji webowych • podsłuch podczas korzystania z formularzy kontaktowych • podsłuch podczas zdalnego dostępu do sieci wewnętrznej przez Internet	1	1	1	**Procedura:** • Polityka Ochrony Danych Osobowych w PWSTE w Jarosławiu **Zabezpieczenia:** • szyfrowanie poczty wysyłanej (SSL) • szyfrowanie połączeń internetowych SSL/VPN • szyfrowanie plików (7zip) wysyłanych mailowo • Ograniczenie fizycznego dostępu do miejsc, gdzie znajdują się nienadzorowane gniazdka sieciowe (np. sale konferencyjne, korytarze) • Dezaktywacja nieużywanych gniazd sieciowych przez wypięcie przewodu lub wyłączenie portu na switchu • Testy penetracyjne
Ataki na oprogramowanie - Włamania z wykorzystaniem luk typu zero day	Zero-day to błędy w oprogramowaniu, do których autor nie przygotował jeszcze poprawek / aktualizacji. Informacje o nich są sprzedawane i wykorzystywane przez intruzów.	1	1	1	**Procedura:** • Instrukcja zarządzania systemami informatycznymi – wykaz zabezpieczeń RODO **Zabezpieczenia:** • Oprogramowanie antywirusowe • Sondy IPS/IDS • Testy penetracyjne
Ataki na oprogramowanie - Włamania z wykorzystaniem najczęstszych błędów programistycznych	*Programiści pisząc programowanie często popełniają te same, znane błędy.* *Przykładowo: możliwość wpisania ujemnej liczby sztuk w formularzu zamówienia, możliwość odgadnięcia numeru zamówienia innego klienta i wpisanie go w pasku adresu przeglądarki w celu wyświetlenia szczegółów.*	1	1	1	**Procedura:** • Instrukcja zarządzania systemami informatycznymi – wykaz zabezpieczeń RODO **Zabezpieczenia:** • Sondy IPS/IDS • Testy penetracyjne
Włamania z wykorzystaniem API (interfejsów programistycznych)	*Niektóre aplikacje pozwalają na zdalne zarządzanie nimi przez specjalnie zaprojektowane funkcje/usługi sieciowe. Np. baza danych może pozwalać na podłączenie się do niej administratorowi w celu wykonania prac naprawczych lub backupu. Dostęp ten odbywa się przy użyciu domyślnych loginów i haseł, co stanowi zagrożenie.*	1	1	1	**Procedura:** • Instrukcja zarządzania systemami informatycznymi – wykaz zabezpieczeń RODO **Zabezpieczenia:** • Zmiana domyślnych loginów i haseł • Wyłączenie zdalnego dostępu, gdy nie jest wymagany • Testy penetracyjne
Ataki na oprogramowanie - Namierzanie wersji testowych (np. strona www)	*Niektóre aplikacje posiadają swoje kopie utrzymywane do celów testowych. Są one często gorzej zabezpieczone i łatwiej jest się do nich włamać, a mogą zawierać również krytyczne dane ze środowiska produkcyjnego. Przykładem może być kopia serwera wykonana w celu przetestowania nowej wersji aplikacji. Często udaje się je namierzyć wpisując np. zamiast adresu www.strona.pl adres test.strona.pl .*	1	2	1	**Procedura:** • Instrukcja zarządzania systemami informatycznymi – wykaz zabezpieczeń RODO **Zabezpieczenia:** • Zmiana domyślnych loginów i haseł • Stosowanie tych samych zasad bezpieczeństwa, co do systemów produkcyjnych • Testy penetracyjne
Skanowanie sieci i usług	*Udostępniane w Internecie serwery, urządzenia sieciowe i aplikacje oraz serwisy www mogą być namierzane przez intruzów poprzez skanowanie adresów IP. Polega to na*	2	1	1	**Procedura:** • Procedura zabezpieczenia systemu informatycznego **Zabezpieczenia:**

PQ

	próbach łączenia się z wszystkimi znanymi usługami w celu sprawdzenia, które z nich są dostępne w naszej sieci i w jakiej wersji. Dzięki temu możliwe jest znalezienie usług nieaktualnych i zawierających błędy.				• Firewalle • Sondy IPS/IDS • Wyłączanie niepotrzebnych usług na urządzeniach sieciowych i serwerach
Włamanie do sieci poprzez WIFI	Uzyskanie dostępu do sieci wewnętrznej poprzez włamanie się do sieci bezprzewodowej	1	1	1	**Z Procedura:** • Instrukcja zarządzania systemami informatycznymi – wykaz zabezpieczeń RODO **Zabezpieczenia:** • Odseparowanie wifi dla gości/klientów od sieci wewnętrznej • Stosowanie odpowiednich standardów szyfrowania • Stosowanie haseł dostępowych

Włamanie z sieci zewnętrznej do sieci wewnętrznej	Włamania z zewnątrz poprzez nieodpowiednio zabezpieczone i skonfigurowane punkty styku z Internetem oraz udostępnione w Internecie serwery i aplikacje.	2	1	2	**Procedura:**
					• Instrukcja zarządzania systemami informatycznymi – wykaz zabezpieczeń RODO
					
					Zabezpieczenia:
					• Sewery proxy i bramki filtrujące
					  ○ skan niebezpiecznej zawartości
					• Firewall / NG Firewall / UTM do ochrony dostępu do sieci komputerowej
					  ○ firewall sprzętowy
					  ○ firewall programowy
					• system IDS/IPS do ochrony dostępu do sieci komputerowej
					• Skanery podatności (stosowany jest system wykrywania słabości i zagrożeń)
					• Testy penetracyjne

Nieuprawniony dostęp do sieci z użyciem hakerskiego urządzenia	Możliwość wpięcia hakerskiego urządzenia do łatwo dostępnych urządzeń sieciowych wewnątrzorganizacyjnych, celem uzyskania dostępu do sieci przez to urządzenie z zewnątrz. Możliwość uruchomienia tzw. wrogiego access pointa w celu przechwycenia klientów sieci bezprzewodowej. Zagrożenie dla nast. elementów: • gniazdka sieciowe w korytarzach, w sali konferencyjnej • skanery, drukarki na korytarzach • switche w miejscach dostępnych	1	2	1	**Procedura:** • Instrukcja zarządzania systemami informatycznymi – wykaz zabezpieczeń RODO **Zabezpieczenia:** • Okablowanie i elementy sieci są fizycznie zabezpieczone przed ingerencją osób postronnych • Blokada portów USB na stacjach roboczych • Dezaktywacja nieużywanych gniazd sieciowych poprzez wypięcie przewodu lub wyłączenie portu na switchu
Atak ransomeware	Ransomeware - Program do szyfrowania plików. Instaluje się z maili lub z hiperlinków w mailach lub poprzez odwiedziny zainfekowanej strony. Są też znane przypadki infekcji poprzez sieć lokalną. Odszyfrowanie wymaga zapłaty np. 500 USD. Bardzo groźny	2	1	1	**Procedura:** • Instrukcja zarządzania systemami informatycznymi – wykaz zabezpieczeń RODO • Szkolenia personelu • Polityka Ochrona Danych Osobowych w PWSTE w Jarosławiu **Zabezpieczenia:** • Systemy antywirusowy i antyspamowy • Kopie bezpieczeństwa kluczowych danych zabezpieczone przed szyfrowaniem przez ransomeware • Sewery proxy i bramki filtrujące ○ blokada ruchu na podstawie bazy reputacji

PR

					○ blokada dostępu do określonych stron
ATAKI MAN-IN-THE-MIDDLE	Zmuszenie komputerów w sieci lokalnej do komunikowania się za pośrednictwem komputera intruza. Umożliwia przechwytywanie i podsłuchiwanie ruchu w sieci.	1	1	1	**Procedura:** • Instrukcja zarządzania systemami informatycznymi – wykaz zabezpieczeń RODO **Zabezpieczenia:** • Systemy antywirusowe • Sondy IPS/IDS • Systemy SIEM • Testy penetracyjne
Eskalacja uprawnień	• Zwiększenie uprawnień użytkownika przez wykorzystanie błędów programistycznych • Przejęcie uprawnień użytkownika zaawansowanego • Przejęcie uprawnień administratora • Przejęcie uprawnień systemowych • Przejęcie innych poświadczeń (certyfikaty elektroniczne, pliki cookies z identyfikatorami sesji)	1	1	1	**Procedura:** • Instrukcja zarządzania systemami informatycznymi – wykaz zabezpieczeń RODO • Polityka Ochrony Danych Osobowych w PWSTE w Jarosławiu **Zabezpieczenia:** • Systemy SIEM • Regularny przegląd logów i uprawnień • Monitorowanie logowania na konta administracyjne • Testy penetracyjne
Atak DOS / DDOS	Atak na system komputerowy lub usługę sieciową w celu uniemożliwienia działania. Atak dotyczy głownie stron i aplikacji www. Np. wypełnienie i wysłanie kilka milionów razy formularza kontaktowego (za pomocą skryptu) i spowodowanie zapełnienia dysku. *Zmasowany atak pojedynczego atakującego (DOS) lub z wielu komputerów jednocześnie (DDOS) na jakąś stronę www lub na portal, aby ją przeciążyć i „zakorkować"*	1	3	3	**Procedura:** • Procedura zabezpieczenia systemu informatycznego **Zabezpieczenia:** • WAF (Web application firewall) • Firewall • Mechanizm captcha (kod z obrazka do przepisania w formularzu) • Systemy SIEM • Testy penetracyjne
Nieuprawniony dostęp lub włamanie do pomieszczeń	Dostęp do: • Budynków • Pomieszczeń biurowych • Archiwów • Serwerowni • 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	1	3	3	**Procedury:** • Polityka Ochrony Danych Osobowych w PWSTE w Jarosławiu **Zabezpieczenia:** • kontrola kluczy zapasowych / kontrola wydawania kluczy • praca personelu sprzątającego w godzinach pracy i w obecności osób upoważnionych • rozmieszczenie komputerów /drukarek /xero ograniczające dostęp osób nieupoważnionych • dostęp osób nieupoważnionych w obecności osoby upoważnionej • zabezpieczenie dostępu do pomieszczeń (drzwi zamykane na klucz)/ drzwi zamykane na kod • zabezpieczenie dostępu do serwerowni (drzwi zamykane na klucz) • zabezpieczenie dostępu do archiwum (drzwi zamykane na klucz) • zabezpieczenie dokumentacji / danych w pomieszczeniach (zamknięte niemetalowe szafy / zamknięte metalowe szafy) • ochrona fizyczna obiektu / pomieszczeń (ochrona własna) • system kontroli dostępu

					• monitoring wizyjny w obrębie obiektu i otoczeniu
Kradzież / zagubienie sprzętu i nośników poza organizacją	Kradzież / zagubienie: • laptopów • smartfonów, • pendrive • dysków wymiennych	2	1	2	**Procedury:** • Polityka Ochrony Danych Osobowych w PWSTE w Jarosławiu • Instrukcja zarządzania systemami informatycznymi -wykaz zabezpieczeń RODO **Zabezpieczenia:** • Hasła na komputerach przenośnych • Stosowanie hasłowanych dysków przenośnych • Stosowanie hasłowanych pendrive
Nieuprawniony dostęp do infrastruktury IT oraz do programów	• brak kontroli nad dostępem do serwera, plików, programów, komputerów • nadane zbyt wysokie uprawnienia użytkownikom • dostęp osób nieupoważnionych do kopii bezpieczeństwa • łatwy dostęp osób nieupoważnionych do danych prezentowanych na monitorach, drukarkach, kserokopiarkach • niezabezpieczona praca zdalna użytkowników lub serwisu IT	1	1	1	**Procedury:** • Polityka Ochrony Danych Osobowych PWSTE w Jarosławiu • Instrukcja zarządzania systemami informatycznymi- wykaz zabezpieczeń RODO • Szkolenie personelu **Zabezpieczenia:** • szyfrowanie baz danych, aby hacker lub przypadkowy użytkownik nie „widział" danych w bazie • zarządzanie uprawnieniami – profile użytkowników • minimalizacja uprawnień • konta firmowe odseparowane od prywatnych • separacja sieci wewnętrznej od sieci przeznaczonej dla gości • uwierzytelnianie użytkowników z zewnątrz poprzez akceptację wybranych adresów IP • blokada logowania się po kilku błędnie podanych hasłach • zahasłowane wygaszacze ekranu aktywowane po 15 minutach nieaktywności użytkownika • ustawienie monitorów uniemożliwiające wgląd w dane osób postronnych • polityka czystego ekranu • filtry polaryzacyjne na monitorach • drukarki wyposażone w kontrolę wydruków (PIN)
Udostępnianie danych osobom nieupoważnionym z sieci publicznej (przez internet)	• dostęp do danych osobowych poprzez stronę www bez logowania się • dostęp do danych osobowych poprzez stronę www po zalogowaniu się (użytkownik może przeglądać dane osobowe innych użytkowników) • dostęp do katalogów udostępnionych pod publicznym adresem IP plików z danymi osobowymi lub kopii bezpieczeństwa (bez logowania się) • udostępnianie plików zaindeksowanych przez roboty google na skutek braku komend chroniących katalogi webowe przez taką indeksacją • przesłanie lub wydawanie informacji osobie	1	3	3	**Procedura** • Polityka Ochrony Danych Osobowych w PWSTE w Jarosławiu **Zabezpieczenia** • Uwierzytelnianie dostępu do zasobów • Testy penetracyjne

PR

	nieupoważnionej				
Awarie / uszkodzenia elementów IT	Awarie: • dysków • stacji roboczych • urządzeń sieciowych/routerów • drukarek / skanerów • serwera	1	3	3	**Procedury:** • Instrukcja zarządzania systemami informatycznymi- wykaz zabezpieczeń PWSTE w Jarosławiu **Zabezpieczenia:** • redundancja serwera • macierz DS. 3400, V3700 • system do inwentaryzacji sprzętu • plan ciągłości działania
Błąd / awaria oprogramowania	Awarie: • programu kadrowo-płacowego • poczty • aplikacji www (np. wordpressa) • bazy danych	1	1	1	**Procedury:** • Instrukcja zarządzania systemami informatycznymi – wykaz zabezpieczeń PWSTE w Jarosławiu **Procedury:** • Zabezpieczenia techniczne **Zabezpieczenia:** • Wirtualizacja
Pożar / eksplozja	• Pożar obiektu • Pożar serwerowni • Pożar serwera • Zniszczenie serwerowni (np. wybuch gazów technicznych)	1	3	3	**Procedury:** • Zabezpieczenia techniczne **Zabezpieczenia:** • gaśnice • system PPOŻ • czujnik dymu w serwerowni
Zalanie	• Zalanie serwerowni • Zalanie archiwum (powódź, zalanie z rur) • Zalanie pomieszczenia kadr	1	1	1	**Procedury:** • Zabezpieczenia techniczne **Zabezpieczenia:** • składowanie dokumentacji papierowej na podwyższeniu, w szafach metalowych
Przegrzanie / zbyt duża wilgotność	• wysoka temperatura w serwerowni • wysoka wilgotność w archiwum	1	3	3	**Procedury:** • Zabezpieczenia techniczne

PR

					Zabezpieczenia: • powiadamianie administratora systemu informatycznego o alertach temperatury • monitoring środowiskowy w serwerowni - czujnik temperaturowy • monitoring środowiskowy w archiwum - czujniki wilgotności
Awaria zasilania	• skoki napięcia • przerwy w dostawie zasilania	1	1	1	**Procedury:** • Zabezpieczenia techniczne **Zabezpieczenia:** • sieć stabilizowana • UPS podtrzymujący zasilanie serwera • UPS na kluczowych elementów systemu IT • Agregat prądotwórczy • Redundantna linia zasilania
Nieuprawniona modyfikacja / usunięcie	• niezamierzone lub pomyłkowe zmodyfikowanie / usunięcie danych • sfałszowanie danych przez osoby z wewnątrz lub zewnątrz organizacji	1	3	3	**Procedury:** • Instrukcja zarządzania systemami informatycznymi- wykaz zabezpieczeń PWSTE w Jarosławiu **Zabezpieczenia:** • Rozliczalność operacji o kluczowe programy/systemy logują operacje tworzenia, zmiany, usuwania rekordu, wglądu w dane, eksportu danych o każdy użytkownik programu/systemu posiada swój indywidualny login
Nieuprawnione kopiowanie danych	• kopiowanie danych z katalogów, dysków, baz, programów • kserowanie i robienie zdjęć przez pracownika lub przez osobę obcą	1	1	1	**Procedury:** • Instrukcja zarządzania systemami informatycznymi- wykaz zabezpieczeń PWSTE w Jarosławiu • Polityka Ochrony Danych Osobowych w PWSTE w Jarosławiu **Zabezpieczenia:** • Rozliczalność operacji o kluczowe programy/systemy logują operacje tworzenia, zmiany, usuwania rekordu, wglądu w dane, eksportu danych o każdy użytkownik programu/systemu posiada swój indywidualny login
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	1	1	1	**Procedury:** • Instrukcja zarządzania systemami informatycznymi- wykaz zabezpieczeń PWSTE w Jarosławiu

PR

					Zabezpieczenia: • wykonywany jest backup serwerów / aplikacji / plików / konfiguracji / licencji /haseł • backup jest zabezpieczony przed ransomeware • kopie zapasowe przechowywane są poza serwerownią • testowanie możliwości odtworzenia kopii • niszczenie/czyszczenie nośników przed utylizacją
Nieprawidłowe / brak procedur niszczenia nośników z danymi –	• wyrzucenie uszkodzonych nośników bez ich zniszczenia • wyrzucanie dokumentów papierowych na śmietnik lub pozostawienie dokumentów w miejscu publicznym • wyrzucenie niezniszczonych , HD, pendrive, DVD	1	2	2	**Procedury:** • Polityka Ochrony Danych Osobowych w PWSTE w Jarosławiu **Zabezpieczenia:** • fizyczne niszczenie sprzętu
Nieprawidłowe / brak procedur napraw w serwisach zewnętrznych	• naprawa sprzętu z nośnikami bez umowy lub bez standardu bezpiecznej naprawy	1	1	1	**Procedury:** • Polityka Ochrony Danych Osobowych w PWSTE w Jarosławiu
Nieprzestrzeganie procedur	• świadome naruszenie pisemnych lub ustnych procedur np. niewylogowywanie się z systemu, przekazywanie haseł osobom nieupoważnionym, naruszenie polityki czystego ekranu lub czystego biurka • naruszenia powyżej wskazane na skutek braków w inteligencji lub z powodów niewiedzy	2	1	2	**Procedury:** • Szkolenia personelu • Polityka Ochrony Danych Osobowych w PWSTE w Jarosławiu
Pomyłki i błędy administratorów, użytkowników	• udostępnienia katalogów i dysków, serwerów ftp, aplikacji z danymi do powszechnego dostępu przez sieć publiczną –z powodu „ułatwienia pracy" administratorów systemów • łatwe logowanie się do baz i programów „login admin, hasło admin1" • dostęp do programów testowych (z prawdziwymi danymi osobowymi) bez logowania • pomyłkowe udostępnienie, wysłanie do złego odbiorcy, błędne zabezpieczenia	1	3	3	**Procedury:** • Instrukcja zarządzania systemami informatycznymi- wykaz zabezpieczeń PWSTE w Jarosławiu • Szkolenia personelu • Polityka Ochrony Danych Osobowych w PWSTE w Jarosławiu
Błędy projektowe / konfiguracyjne	• błędy programistów prowadzące do udostępniania danych z tworzonych lub administrowanych programów • niezabezpieczenie danych w katalogach i bazach webowych i przed indeksacją robotów google	1	1	1	**Zabezpieczenie** • Instrukcja zarządzania systemami informatycznymi –wykaz zabezpieczeń w PWSTE w Jarosławiu • Zabezpieczenie baz i katalogów webowych przed indeksacją wyszukiwarek
Brak aktualnej	• Brak instrukcji, opisów, dokumentacji technicznej sprzętu	1	2	2	**Procedury:**

dokumentacji (instrukcji, opisów, dokumentacji technicznej sprzętu i oprogramowania)	i oprogramowania • Brak instrukcji instalacyjnych i konfiguracyjnych środowiska lub oprogramowania *Zagrożenie związane z możliwymi trudnościami w odtworzeniu środowiska i zarządzania nim, gdy np. odejdzie pracownik IT lub będzie on niedostępny podczas krytycznej awarii*				• Procedury przywracania
Nieprawidłowe / brak umowy o współpracy	Nieprecyzyjnie określone odpowiedzialności we współpracy, co stwarza ryzyko braku zabezpieczeń	1	1	1	**Zabezpieczenia:** • Umowa powierzenia • Pisemne upoważnienia dla podmiotu współpracującego z jasnymi warunkami bezpiecznej pracy z danymi powierzonymi
Nieprawidłowe / brak umowy gwarancyjnej lub wsparcia serwisowego	*Należy uwzględnić, że umowy wymagają przedłużania, czas reakcji nie oznacza czasu naprawy*	1	1	1	**Zabezpieczenie** • stosowane są Umowy powierzenia • Instrukcja zarządzania systemami informatycznymi- wykaz zabezpieczeń PWSTE w Jarosławiu
Upadek firmy outsourcingowej lub dostawczej	• brak zastępstw, np. dla hostingodawcy poczty, dla wsparcia do zakupionej aplikacji • Utrata usługi / aplikacji, którą świadczy pomiot przetwarzający	1	1	1	**Zabezpieczenie** • Redundancja firmy / osoby
Awaria łączy telekomunikacyjnych	Krytyczne dla administratora świadczącego usługi wymagające „internetu", usługi chmurowe, ISP oraz dostawcy platform SaaS	1	3	3	• Redundancja łączy

PR