Polityka Bezpieczeństwa Informacji SRP

Wyciąg z Polityki bezpieczeństwa informacji przetwarzanych na stacjach roboczych SRP

Załącznik 2.16 do Polityki Bezpieczeństwa Informacji SRP - wyciąg

Właściciel	Minister właściwy ds. informatyzacji			
Tryb zatwierdzenia:	Dokument zatwierdza Dyrektor departamentu w ministerstwie właściwym ds. informatyzacji odpowiedzialnego za eksploatację i utrzymanie SRP			
Stan	Zatwierdzony		Daty obowiązywania	
Założenia	Dokument stanowi wyciąg z Załącznika 2.16 do Polityki Bezpieczeństwa Informacji SRP			
Adresaci	Interesariusze wnioskujący o dostęp do SRP			
Historia dokumentu	Wersja	Data	Autor	Opis zmian
	1.0	21.01.2020	WUS MC	Utworzenie dokumentu na podstawie wer. 2.2 załącznika 2.16 PBI SRP

Spis treści

1. Cel

Celem niniejszego opracowania jest określenie wymagań oraz dopuszczalnych warunków i zasad bezpieczeństwa informacji przetwarzanych w pomieszczeniach i na stacjach roboczych w lokalizacjach uprawnionych interesariuszy zewnętrznych łączących się za pośrednictwem dedykowanej sieci oraz aplikacji Źródło do Systemu Rejestrów Państwowych.
Bezpieczeństwo informacji rozumiane jest jako zachowanie takich właściwości informacji i systemu informacyjnego, jak:

- poufność – właściwość polegająca na tym, że informacja nie jest udostępniana ani ujawniana nieautoryzowanym podmiotom (osobom, podmiotom lub procesom),
- integralność – właściwość polegająca na zapewnieniu dokładności i kompletności,
- dostępność – właściwość bycia dostępnym i użytecznym na żądanie autoryzowanego podmiotu,
- rozliczalność - właściwość systemu pozwalająca przypisać określone działanie w systemie do podmiotu oraz umiejscowić je w czasie,
- niezaprzeczalność – zdolność do udowodnienia, że wystąpiły deklarowane zdarzenia lub działania oraz, że wywołał je dany podmiot,
- autentyczność – właściwość polegająca na tym, że podmiot jest tym, za kogo się podaje,
- niezawodność – właściwość oznaczająca spójne, zamierzone zachowanie i skutki.

2. Realizacja polityki

2.1 Wymagania dotyczące podłączania infrastruktury interesariuszy zewnętrznych do SRP

Zalecanym sposobem podłączenia infrastruktury interesariuszy zewnętrznych systemu (np.: gmin) jest wykorzystanie dedykowanej wydzielonej sieci teleinformatycznej będącej w gestii służb podległych Ministrowi właściwemu ds. wewnętrznych i administracji z zachowaniem pełnej separacji stacji roboczych systemu umiejscowionych w lokalizacjach uprawnionych interesariuszy od innych sieci.

W sieci lokalnej interesariuszy również wymagana jest separacja sieci dostępowej do SRP od innych sieci urzędu.

2.2 Wymagania dotyczące ochrony fizycznej pomieszczeń

2.2.1 Wymagania minimalne wynikające z przepisów prawa

Interesariusze SRP mają obowiązek zapewnić poziom ochrony fizycznej pomieszczeń, w których są zlokalizowane stacje robocze przeznaczone do przetwarzania informacji w systemie - zgodny z aktualnymi przepisami dotyczącymi ochrony danych osobowych oraz wewnętrznymi przepisami obowiązującymi w instytucji interesariusza (np. Polityka Bezpieczeństwa Informacji w Urzędzie Gminy).

2.2.2 Zalecenia właściciela systemu

Lokalizacja obiektu i pomieszczenia do przetwarzania informacji w systemie	
Minimalne zabezpieczenia	Zalecane zabezpieczenia
• Pomieszczenia powinny zapewniać takie rozmieszczenie sprzętu oraz dokumentów, aby uniemożliwić dostęp do informacji osobom nieupoważnionym np.: poprzez stosowanie zabezpieczeń fizycznych w postaci wygradzania stanowiska, stosowania, rolet, żaluzji itp.	• Pomieszczenia powinny zapewniać takie rozmieszczenie sprzętu oraz dokumentów, aby uniemożliwić dostęp do informacji osobom nie upoważnionym i nie powinny być pomieszczeniami przechodnimi.

• Pomieszczenia powinny być zlokalizowane w miejscach gdzie ryzyko wystąpienia powodzi, pożaru, oraz katastrof i aktów terroru jest zminimalizowane.	• Pomieszczenia powinny być wyposażone w system alarmowy, czujki wilgoci oraz dymu z funkcją powiadomienia do służby ochrony lub jednostek straży pożarnej, policji.
Kontrola dostępu do pomieszczeń	
Minimalne zabezpieczenia	Zalecane zabezpieczenia
• Kontrola dostępu do pomieszczeń realizowana jest metodami organizacyjno-proceduralnymi (np. książka pobrań kluczy). • Dostęp do pomieszczeń mogą mieć tylko osoby upoważnione do przetwarzania danych przez administratora danych (ADO). Inne osoby mogą przebywać w pomieszczeniach jedynie w obecności osób upoważnionych, za ich wiedzą i zgodą.	• Zastosowanie systemu elektronicznej kontroli dostępu. Urządzenia automatycznej kontroli dostępu winny być nadzorowane całodobowo przez służbę ochrony i okresowo powinna być wykonywana kontrola logów urządzenia. • Dostęp do pomieszczeń mogą mieć tylko osoby upoważnione do przetwarzania danych przez administratora danych (ADO). Inne osoby mogą przebywać w pomieszczeniach jedynie w obecności osób upoważnionych, za ich wiedzą i zgodą po odnotowaniu danych osób nieupoważnionych w książce osób nieuprawnionych.
Zabezpieczenie drzwi i okien	
Minimalne zabezpieczenia	Zalecane zabezpieczenia
• Drzwi znajdujące się wewnątrz budynku w strefie ograniczonego dostępu (bądź dozorowanej), powinny być wyposażone w co najmniej 1 zamek atestowany (klasa C). • Drzwi znajdujące się wewnątrz budynku w strefie ogólnodostępnej niedozorowanej powinny alternatywnie: o spełniać wymagania klasy 2 zgodnie z normą PN-EN14351-1+A1:2010 lub,	• Drzwi znajdujące się wewnątrz budynku w strefie ograniczonego dostępu (bądź dozorowanej) powinny być zabezpieczone przed wyważeniem i wyposażone w co najmniej 1 zamek atestowany (klasa C). • Drzwi znajdujące się wewnątrz budynku w strefie ogólnodostępnej niedozorowanej powinny spełniać wymagania co najmniej klasy 2 zgodnie z normą PN-EN14351-1+A1:2010 oraz być wyposażone w co najmniej jeden zamek atestowany (klasa C).

○ być zabezpieczone przed wyważeniem (podważeniem) oraz być wyposażone w co najmniej 1 zamek atestowany (klasa C). • Drzwi, do których dostęp jest z zewnątrz budynku, powinny: ○ spełniać wymagania co najmniej klasy 2 zgodnie z normą PN-EN14351-1+A1:2010, ○ posiadać co najmniej jeden zamek atestowany (klasa C) lub, ○ w pomieszczeniach powinien być zainstalowany system alarmowy z funkcją powiadamiania. • Okna pomieszczeń zlokalizowanych na parterze lub ostatniej kondygnacji (jeśli jest swobodny dostęp do dachu) o ile nie są zabezpieczone kratami, powinny być oklejone folią antywłamaniową lub powinny być w nich zastosowane szyby o wzmocnionej odporności na zbicie.	• Drzwi, do których dostęp jest z zewnątrz budynku powinny spełniać wymagania co najmniej klasy 3 zgodnie z normą PN-EN14351-1+A1:2010. • Otwory okienne pomieszczeń zlokalizowanych na parterze lub ostatniej kondygnacji (o ile jest swobodny dostęp do dachu) powinny być okratowane lub posiadać okna spełniające wymagania co najmniej klasy 2 zgodnie z normą PN-EN14351-1+A1:2010 z szybą klasy P4.

2.3 Wymagania dotyczące zabezpieczeń nośników informacji

Mając na uwadze kategorię przetwarzanych danych osobowych oraz zagrożenia związane z przetwarzaniem informacji w systemie, należy zastosować adekwatne środki bezpieczeństwa w stosunku do zidentyfikowanych zagrożeń.

Nośniki informacji	
Minimalne zabezpieczenia	Zalecane zabezpieczenia
• Dokumenty i nośniki informacji zawierające dane osobowe należy przechowywać w miejscu uniemożliwiającym dostęp do nich osobom nieupoważnionym (np. w zamykanych na klucz szafkach,	• Informacje przechowywane na elektronicznych oraz papierowych nośnikach powinny być składowane w szafach wyposażonych w co najmniej 1 zamek atestowany (klasa A).

szufladach) – patrz pkt 2.5 Polityka czystego biurka i czystego ekranu. • Karty kryptograficzne służące do logowania, należy składować w szafach wyposażonych w co najmniej 1 zamek. Zakazane jest przechowywanie wraz z kartą kodu PIN do karty oraz kodu PUK. • Do likwidacji wydruków dokumentów i nośników informacji powinny być stosowane niszczarki zgodne z normą DIN66399 o stopniu tajności 1 lub instytucja powinna posiadać stosowną umowę na niszczenie dokumentów z firmą zewnętrzną.	• Karty kryptograficzne służące do logowania, powinny być składowane w metalowych szafach wyposażonych w co najmniej 1 zamek atestowany (klasa A) lub sejfach. Zakazane jest przechowywanie wraz z kartą kodu PIN do karty oraz kodu PUK. • Do likwidacji wydruków dokumentów i nośników informacji powinno się stosować niszczarki klasy DIN 2 zgodnie z normą DIN66399 o stopniu tajności 2.

2.4 Wymagania dotyczące oprogramowania, konfiguracji i zabezpieczeń stacji roboczych

2.4.1 Wymagania dotyczące oprogramowania

Lp.	Rodzaj	Implementacja	Uwagi
1	System operacyjny	Zalecane oprogramowanie to: Microsoft Windows 8, 8.1, Microsoft Windows 10.	System operacyjny musi być wspierany przez producenta w zakresie poprawek i aktualizacji zabezpieczeń oraz wspierać sterowniki urządzeń peryferyjnych niezbędnych do pracy. Data i godzina systemowa musi być zgodna z rzeczywistą. Z tego względu niezalecane jest stosowanie systemu Windows w wersji 7 i wcześniejszych.
2	JAVA	Java SE 8 Runtime Environment (JRE) w wersji aktualnej.	Niezbędna do uruchamiania appletów w przeglądarce internetowej.
3	Oprogramowanie antywirusowe	Udostępnione przez właściciela systemu na	Oprogramowanie powinno posiadać aktualne definicje i bazy antywirusowe.

		dedykowanym serwerze.	
4	Czytnik PDF	Acrobat Reader lub inny.	W wersji aktualnej.
5	Przeglądarka Internetowa	Mozilla Firefox, Internet Explorer, Microsoft Edge, Google Chrome.	Należy stosować aktualne wersje przeglądarek zawierające wszystkie poprawki bezpieczeństwa udostępnione przez producenta. Stacja robocza musi mieć zainstalowane dodatki umożliwiające uruchamianie apletów języka Java, dla wszystkich wykorzystywanych typów przeglądarek.
6	Sterowniki urządzeń peryferyjnych	Oprogramowanie niezbędne do obsługi, kart, czytników kart kryptograficznych i drukarek.	Sterowniki do obsługi kart powinny być zainstalowane zarówno w systemie jak i przeglądarce internetowej (dot. Mozilla Firefox). Przed zainstalowaniem sterowników, należy upewnić się, że przeglądarki są już zainstalowane.

2.4.2 Wymagania dotyczące konfiguracji i zabezpieczeń

Konta i hasła	
Minimalne zabezpieczenia	Zalecane zabezpieczenia dodatkowe
• Uruchomienie komputera wymaga podania hasła. • Każdemu użytkownikowi komputera należy założyć oddzielne konto. • Wbudowane konto administratora należy używać tylko w przypadku wykonywania czynności administratora. • Konta użytkownika nie mogą mieć uprawnień administratora o ile nie jest to wymagane przy bieżącej pracy. • Długość nazwy użytkownika nie mniej niż 6 znaków.	• Długość hasła konta administratora lub użytkownika z uprawnieniami administratora nie mniej niż 14 znaków (hasło złożone co najmniej: 1 duża litera, 1 cyfra i znak specjalny), okres ważności hasła nie dłuższy niż 30 dni. • Długość hasła konta użytkownika nie mniej niż 12 znaków (hasło złożone co najmniej: 1 duża litera, 1 cyfra i znak specjalny), okres ważności hasła nie dłuższy niż 30 dni. • Zastąpienie logowania tradycyjnego (login i hasło) logowaniem z użyciem

<table>
<tr><td>

- Długość hasła konta administratora lub użytkownika z uprawnieniami administratora nie mniej niż 12 znaków (hasło złożone co najmniej 1 duża litera, 1 cyfra i znak specjalny), okres ważności hasła nie dłuższy niż 30 dni.
- Długość hasła konta użytkownika nie mniej niż 8 znaków (hasło złożone co najmniej 1 duża litera, 1 cyfra i znak specjalny), okres ważności hasła nie dłuższy niż 30 dni.

</td><td>

kart mikroprocesorowych, czytników cech biometrycznych, kluczy bezprzewodowych.

- Długość nazwy użytkownika nie mniej niż 8 znaków.
- Należy wprowadzić stosowne regulacje sankcjonujące sposoby przechowywania nazw użytkowników i haseł oraz zabraniające udostępnia ich innym osobom.

</td></tr>
<tr><td colspan="2">Ustawienia BIOS/UEFI</td></tr>
<tr><td>Minimalne zabezpieczenia</td><td>Zalecane zabezpieczenia dodatkowe</td></tr>
<tr><td>

- Wejście i zmiana ustawień BIOS/UEFI wymaga podania hasła.
- Wyłączona jest możliwość uruchamiania systemu z sieci lub innych nośników niż dysk twardy komputera.
- Długość hasła BIOS/UEFI nie mniej niż 8 znaków (co najmniej 1 duża litera i 1 cyfra).

</td><td>

- Długość hasła BIOS/UEFI nie mniej niż 10 znaków (co najmniej 1 duża litera i 1 cyfra).

</td></tr>
<tr><td colspan="2">Ochrona antywirusowa</td></tr>
<tr><td>Minimalne zabezpieczenia</td><td>Zalecane zabezpieczenia dodatkowe</td></tr>
<tr><td>

- Istnieje obowiązek zainstalowania oprogramowania antywirusowego na stacjach roboczych dostępowych do aplikacji ŹRÓDŁO w ramach dedykowanej sieci SRP. Instrukcja instalacji oraz pakiet instalacyjny tego oprogramowania antywirusowego znajdują się na stronie: http://pomocny.obywatel.gov.pl/av. Strona ta jest dostępna w ramach dedykowanej sieci SRP. W celu pobrania oprogramowania, adres należy wprowadzić w przeglądarce internetowej na stanowisku podłączonym do SRP.

</td><td></td></tr>
</table>

• Oprogramowanie antywirusowe instalowane na stacjach przetwarzających dane działające w czasie rzeczywistym. • Ustawienie oprogramowania zapewniające pełne skanowanie antywirusowe stacji co najmniej 1 raz w tygodniu. • Bieżąca aktualizację sygnatur przez administratora za pośrednictwem udostępnionego serwera aktualizacji.	
Dyski i urządzenia przenośne	
Minimalne zabezpieczenia	Zalecane zabezpieczenia dodatkowe
• Przenośne pamięci flash oraz dyski przenośne, które będą służyły do wynoszenia informacji poza obręb pomieszczenia muszą być wyposażone w oprogramowanie lub rozwiązanie sprzętowe umożliwiające szyfrowanie danych z użyciem hasła dostępowego nie krótszego niż 8 znaków (hasło złożone co najmniej 1 duża litera, 1 cyfra i znak specjalny) lub w czytnik identyfikacji biometrycznej. • Dane składowane na dysku stacji roboczej przenośnej muszą być umieszczone w obszarze podlegającym szyfrowaniu lub być szyfrowane. • Należy wdrożyć regulacje zapewniające prawidłowe posługiwanie się oraz prowadzić ewidencję obsługi dysków przenośnych bądź pamięci flash. • Nośniki nie są wynoszone po za obręb pomieszczenia lub muszą być wyposażone w rozwiązanie sprzętowe umożliwiające szyfrowanie danych z użyciem hasła dostępowego nie krótszego niż 8 znaków	• W przypadku stosowania dysków twardych umieszczonych w wyjmowanych kieszeniach muszą być one wyposażone w zamknięcie na kluczyk i zamknięte gdy znajduje się w nich dysk. Po zakończonej pracy zalecane jest usunięcie dysku i jego dalsze przechowywanie w zabezpieczonej szafie. • Partycja lub dysk stacji przenośnej, na której są składowane dane jest w całości zaszyfrowany. • Stacje przenośne w miejscach korzystania, należy zabezpieczyć linką antykradzieżową przymocowaną do stałego elementu wyposażenia (o ile jest to możliwe).

(hasło złożone co najmniej 1 duża litera, 1 cyfra i znak specjalny) uniemożliwiające skorzystanie z danych po max 5 próbach nieudanego podania hasła do odblokowania nośnika.	
Rozmieszczenie sprzętu	
Minimalne zabezpieczenia	Zalecane zabezpieczenia dodatkowe
• Stacja powinna być ustawiona w miejscu uniemożliwiającym do niej dostęp osobom nieupoważnionym – patrz pkt 2.5 Polityka czystego biurka i czystego ekranu. • Wymagane jest takie ustawienie drukarki aby nie było możliwości podejrzenia bądź pobrania wydruków przez osoby nieuprawnione. • Wymagane jest takie ustawienie monitora aby nie było możliwości podejrzenia danych przetwarzanych na ekranie przez osoby nieuprawnione – patrz pkt 2.5 Polityka czystego biurka i czystego ekranu. • W przypadku stanowisk roboczych mobilnych wymagane jest stosowanie filtrów prywatyzacyjnych zabezpieczających przed możliwością podejrzenia danych przetwarzanych na ekranie przez osoby nieuprawnione.	• Zalecane jest stosowanie filtrów prywatyzacyjnych zabezpieczających przed możliwością podejrzenia danych przetwarzanych na ekranie przez osoby nieuprawnione.
Usuwanie danych	
Minimalne zabezpieczenia	Zalecane zabezpieczenia dodatkowe
• Po skasowaniu danych należy opróżnić „kosz” systemowy.	• Do usuwania danych należy używać wyspecjalizowanego oprogramowania. • Ustawić opcję automatycznego czyszczenia „kosza” systemowego.
Aktualizacja systemu operacyjnego i innego oprogramowania	

Minimalne zabezpieczenia	Zalecane zabezpieczenia dodatkowe
• Cykliczne aktualizowanie systemu operacyjnego i oprogramowania przez administratora z zastosowaniem nośników wymiennych lub za pośrednictwem udostępnionego serwera aktualizacji (opcja). • Włączenie automatycznych aktualizacji systemu oraz oprogramowania zgodnie z zaleceniami producentów (opcja pobierz aktualizacje i zdecyduj kiedy/które zainstalować).	
Kopie bezpieczeństwa	
Minimalne zabezpieczenia	Zalecane zabezpieczenia dodatkowe
• Składowanie kopii bezpieczeństwa powinno odbywać się w innym budynku bądź pomieszczeniach w odpowiednio zabezpieczonej szafie.	
Zasilanie awaryjne	
Minimalne zabezpieczenia	Zalecane zabezpieczenia dodatkowe
• Stacje powinny być wyposażone w urządzenia podtrzymujące zasilanie (UPS) umożliwiające automatyczne bezpieczne zamknięcie stacji w przypadku wyczerpania się akumulatora lub powinny być dołączone do zasilania gwarantowanego obiektu. • W przypadku pracy na zasilaniu bateryjnym stan baterii stacji przenośnej ma umożliwić bezpieczne zamknięcie systemu po zaniku zasilania sieciowego.	
Inne zabezpieczenia	
Minimalne zabezpieczenia	Zalecane zabezpieczenia dodatkowe

• Wymagane jest ustawienie czasu automatycznego uruchamiania wygaszacza ekranu na max 5 minut, wznowienie pracy wymaga podania hasła, zalecane jest także blokowanie stacji przy każdorazowym opuszczeniu stanowiska.	

2.4.3 Stosowanie jako stacji roboczych komputerów przenośnych oraz maszyn wirtualnych

Sprzęt komputerowy przenośny może być używany do pracy z SRP, ale ze względu na zwiększone ryzyko związane z utratą danych podczas przenoszenia sprzętu, stosowanie tego rozwiązania jest **NIEZALECANE** i powinno być ograniczone tylko do uzasadnionych przypadków.

Zabezpieczenia przenośnych stacji roboczych muszą uwzględniać wytyczne pkt 2.4.2.

Maszyny wirtualne mogą być używane do pracy z SRP, ale stosowanie tego rozwiązania jest **NIEZALECANE** i powinno być ograniczone tylko do uzasadnionych przypadków.

Zabezpieczenia serwerów/stacji udostępniających maszyny wirtualne oraz zabezpieczenia systemu udostępnianego z wykorzystaniem maszyny wirtualnej muszą być co najmniej na poziomie minimalnym opisującym stanowiska robocze SRP. Dodatkowe zabezpieczenia dla maszyn wirtualnych:

- uprawnienia do katalogu oraz dostęp do folderu udostępnianego musi zostać ograniczony tylko do użytkowników maszyny wirtualnej;
- uprawnienia do katalogu oraz dostęp do folderu udostępnianego powinien uniemożliwiać skopiowanie pliku maszyny innej osobie niż administrator;
- stosowanie maszyn wirtualnych na dyskach przenośnych bądź pamięciach typu flash **nie jest zalecane.** W przypadku konieczności stosowania takiego rozwiązania zalecane jest szyfrowanie w całości nośników maszyn wirtualnych z użyciem hasła dostępowego nie krótszego niż 10 znaków (hasło złożone co najmniej: 1 duża litera, 1 cyfra i znak specjalny) uniemożliwiające skorzystanie z danych po max 3 próbach nieudanego podania hasła do odblokowania nośnika.

2.5 Polityka czystego biurka i czystego ekranu

W celu zapobieżenia ujawnieniu, zniszczeniu lub kradzieży informacji systemu zawartych na dokumentach papierowych oraz nośnikach danych wprowadza się politykę „czystego biurka". Dla zabezpieczenia informacji przechowywanych na serwerach, stacjach roboczych oraz urządzeniach mobilnych wprowadza się politykę „czystego ekranu".
Podstawowe zasady:

1. Chronione nieużywane informacje systemu należy przechowywać w sejfie, zamykanej szafie lub zamykanej szufladzie.
2. Stanowisko pracy, powinno być tak zaplanowane, aby żadna osoba postronna nie mogła podglądać chronionych informacji niezależnie od ich formy.
3. Opuszczając pokój (niezależnie na jak długo) należy zamknąć drzwi na klucz, lub zablokować dostęp do pomieszczenia aktywując inne dostępne zabezpieczenia oraz schować do zamykanej szafy lub szuflady wszelkie istotne dokumenty i nośniki informacji (płyty, taśmy, dyski przenośne, itp.).
4. Każdorazowe odejście od komputerowego stanowiska pracy powinno zostać poprzedzone zamknięciem sesji lub zablokowaniem komputera za pomocą mechanizmu blokowania ekranu i klawiatury przy użyciu hasła, tokenu lub innego mechanizmu uwierzytelniania użytkownika lub innych dostępnych zabezpieczeń, w tym mechanicznych.
5. Po zakończeniu pracy wszystkie dokumenty i nośniki informacji systemu istotne z punktu widzenia bezpieczeństwa informacji należy przechowywać w zamykanych, zabezpieczonych i w miarę możliwości ognioodpornych szafach. Nie powinny pozostać niezabezpieczone, gdyż w razie kradzieży, katastrofy naturalnej lub aktu terroru mogłyby dostać się w niepowołane ręce, zostać uszkodzone lub zniszczone.
6. Po zakończeniu pracy należy zamknąć wszystkie aktywne sesje oraz wylogować się z systemu lub aktywować oprogramowanie blokujące klawiaturę i wygaszacz ekranu zabezpieczony hasłem.
7. Nie należy pozostawiać nawet na chwilę bez opieki wydruków oraz kopiowanych dokumentów, które zostały wykonane na kserokopiarkach i drukarkach, tzn.: należy odebrać je z urządzenia w taki sposób, aby żadna osoba postronna nie mogła się zapoznać z ich zawartością.

2.6 Zgłaszanie zdarzeń wskazujących na naruszenie bezpieczeństwa informacji w systemie

Każdy pracownik instytucji będącej interesariuszem Systemu Rejestrów Państwowych realizujący w nim zadania ma obowiązek dbać o bezpieczeństwo informacji w systemie zgodnie

z dokumentami polityk bezpieczeństwa informacji, oraz reagować na zdarzenia, które mogą wskazywać na wystąpienie incydentu bezpieczeństwa informacji i informować o zdiagnozowanych słabościach systemu.

Szybka reakcja stanowi podstawowy element skutecznego ograniczenia następstw takich zdarzeń, dlatego nie należy zwlekać z podejmowaniem działań niezależnie od okoliczności. Obsługa incydentów związanych z bezpieczeństwem informacji jest realizowana priorytetowo w stosunku do innych zgłoszeń, a w przypadku incydentów związanych z naruszeniem bezpieczeństwa informacji prawnie chronionych (np. dane osobowe) przepisy prawa wymagają reakcji we wskazanym okresie od wykrycia incydentu oraz informowania osób, w których kompetencji znajduje się nadzór nad przestrzeganiem przepisów dotyczących bezpieczeństwa informacji (Inspektor Ochrony Danych, Administrator Danych).

Zdarzenia, które wiążą się lub mogą wiązać się z naruszeniem bezpieczeństwa informacji to, m.in. naruszenie dowolnego atrybutu bezpieczeństwa systemu (m.in.: poufność, integralność, dostępność, autentyczność) w wyniku umyślnych lub nieumyślnych działań, w szczególności:

- dostęp do systemu osoby nieposiadającej upoważnienia do przetwarzania danych,
- włamanie do systemu lub jego dowolnego komponentu,
- połączenie wydzielonej infrastruktury systemu z dowolną siecią zewnętrzną bez zgody właściciela biznesowego systemu,
- nieuprawnione pozyskanie informacji,
- udostępnienie danych z systemu osobom nieuprawnionym,
- utrata aktywu/zasobu systemu (komputer przenośny, pendrive, dysk, płyta CD z danymi, telefon, dokument, itp.),
- destrukcja danych i oprogramowania systemu,
- próba sabotażu lub sabotaż systemu skutkujący niedostępnością,
- piractwo, kradzież oprogramowania systemu lub oprogramowania wspomagającego (np. licencjonowane oprogramowanie bazy danych),
- oszustwo i fałszerstwo danych systemu,
- szpiegostwo dotyczące danych zawartych w systemie oraz danych dotyczących systemu,
- ujawnienie lub podejrzenie ujawnienia osobom trzecim haseł dostępowych do dowolnych komponentów systemu,
- długotrwała niedostępność systemu lub jego dowolnego komponentu,
- wykrycie szkodliwego oprogramowania w dowolnym komponencie systemu, np.:
    - wirusy komputerowe,
    - makrowirusy,
    - robaki,
    - konie trojańskie,
    - bomby logiczne,
    - rootkity,

- programy szpiegujące,
- programy reklamowe,
- keyloggery.

Uprawniony interesariusz lub każdy z użytkowników systemu ma obowiązek zgłosić zdarzenia mogące wskazywać na wystąpienie incydentu w obszarze bezpieczeństwa informacji SRP bezpośrednio **w systemie ITSM** dostępnym pod adresem: https://pomoc.coi.gov.pl lub w przypadku braku takiej możliwości: na adres poczty elektronicznej: service_desk_itsm@coi.gov.pl lub telefonicznie na nr.: (42) 25 35 499.

W treści zgłoszenia przekazuje następujące informacje:

- imię i nazwisko oraz dane kontaktowe,
- stanowisko w systemie (np.: lokalny administrator systemu),
- miejsce wystąpienia incydentu bezpieczeństwa (np. pomieszczenie do przetwarzania danych SRP w urzędzie gminy),
- opis incydentu bezpieczeństwa zawierający informacje:
  - na czym polega incydent i czy dotyczy bezpieczeństwa danych prawnie chronionych (danych osobowych, informacji niejawnych, tajemnicy przedsiębiorstwa),
  - jakiego elementu systemu (aplikacji) dotyczy,
  - dotyczące daty i godziny wystąpienia lub wykrycia incydentu,
  - na temat wpływu incydentu na elementy systemu,
  - czy incydent nadal trwa lub czy występuje okresowo w sposób powtarzalny,
- wstępną ocenę realnych lub potencjalnych skutków incydentu bezpieczeństwa (oszacowanie szkód),
- podjęte dotychczas działania.

Jeśli osoba zgłaszająca posiada dodatkowe informacje techniczne w postaci konfiguracji sprzętowej, systemu operacyjnego, adresacji sieciowej urządzeń i innych znanych jej kwestii technicznych - dane te powinny być niezwłocznie przekazane po nawiązaniu kontaktu bezpośrednio do linii wsparcia „bezpieczeństwo” w uzgodnionym bezpiecznym kanale komunikacyjnym, przy czym przekazanie danych inicjuje pracownik linii wsparcia „bezpieczeństwo”.

Pracownik service desk może żądać od osoby zgłaszającej incydent bezpieczeństwa informacji uzupełnienia opisu w systemie ITSM jeśli przekazane informacje nie pozwalają na podjęcie dalszych działań.

Niezależnie, czy w toku dalszych działań zgłoszone zdarzenie zostanie sklasyfikowane jako incydent bezpieczeństwa lub inne zdarzenie - service desk informuje o tym osobę zgłaszającą. Osoba zgłaszająca jest również informowana za pośrednictwem systemu ITSM o rozwiązaniu incydentu.

Osoba zgłaszająca ma obowiązek ponadto:

- poinformować o zaistniałym zdarzeniu swojego bezpośredniego przełożonego,

- współpracować z komórką odpowiedzialną za bezpieczeństwo informacji ministerstwa właściwego ds. informatyzacji lub podmiotu realizującego zadania na rzecz ministerstwa właściwego ds. informatyzacji w przedmiotowym obszarze oraz w razie potrzeby realizować przekazane wytyczne i zalecenia,
- zabezpieczyć miejsce zdarzenia, istotne dane lub urządzenia teleinformatyczne do czasu podjęcia dalszych działań przez komórki organizacyjne odpowiedzialne za bezpieczeństwo informacji. Zabezpieczenie to należy realizować m.in. poprzez:
  - bezzwłoczne zanotowanie wszystkich istotnych szczegółów dotyczących zdarzenia,
  - archiwizację wiadomości lub innych informacji dotyczących zdarzenia np. komunikatów z systemu antywirusowego,
  - zabezpieczenie „zrzutów" ekranowych lub zdjęć obrazujących wystąpienie zdarzenia wskazującego na naruszenie bezpieczeństwa informacji,
  - zabezpieczenie urządzenia, nośnika informacji (np.: dokument papierowy, płyta CD z danymi systemu lub dotyczącymi systemu) jak również innego dowodu wskazującego na możliwość naruszenia bezpieczeństwa informacji.

Zabrania się działań mogących spowodować utrudnienia w wyjaśnieniu przyczyn incydentu bezpieczeństwa informacji w tym niszczenia, usuwania, ukrywania, modyfikowania informacji i materiałów zawierających dane związane z przedmiotowym incydentem.

2.7 Audyt wewnętrzny bezpieczeństwa informacji systemu

Gestor SRP zapewnia realizację audytów bezpieczeństwa informacji SRP.

Audyt bezpieczeństwa ma na celu ocenę zgodności i dostarczenie informacji, czy Polityka Bezpieczeństwa Informacji jest adekwatna do konieczności zapewnienia wysokiego poziomu bezpieczeństwa SRP i informacji w nim przetwarzanych, wynikającego m.in. z przepisów prawa i niniejszej PBI oraz, czy postanowienia niniejszej Polityki dotyczące rozwiązań organizacyjnych i technicznych bezpieczeństwa są skutecznie wdrożone i utrzymywane.

Audyt wewnętrzny bezpieczeństwa SRP realizowany jest przez każdego z interesariuszy mającego interakcje z systemem i oddziaływującego na niego.

Audyt wewnętrzny bezpieczeństwa SRP prowadzony jest w sposób cykliczny i planowy corocznie, zgodnie z wewnętrznymi regulacjami (regulaminami, procedurami) interesariuszy w zakresie audytu wewnętrznego, z uwzględnieniem tego, że kryterium audytu jest PBI SRP i jej postanowienia. Zakres audytu obejmuje kwestie bezpieczeństwa SRP i danych w nim przetwarzanych.

Wyniki audytu są udokumentowane w postaci Raportu z audytu i zawierają opis i ocenę zgodności stanu zastanego z postanowieniami PBI SRP oraz zalecenia w zakresie osiągnięcia pełnej zgodności z postanowieniami PBI SRP.

Kierownictwo jednostek organizacyjnych interesariuszy systemu zapewnia niezależność, obiektywność i bezstronność procesu audytu oraz ochronę wyników audytu.

2.8 Nadzór i kontrola nad podmiotami korzystającymi z udostępniania danych w SRP

2.8.2 Nadzór i kontrola w oparciu o przepisy Ustawy z dnia 24 września 2010r. o ewidencji ludności

Zgodnie z Ustawą z dnia 24 września 2010 r. o ewidencji ludności (Dz. U. 2010 nr 217 poz. 1427) Wojewoda jest organem wyższego stopnia w stosunku do organów gmin wydających rozstrzygnięcia administracyjne na podstawie ustawy.

Wojewoda sprawuje nadzór nad działalnością organów gmin w zakresie realizacji obowiązków określonych w ustawie.

Minister właściwy do spraw wewnętrznych i administracji sprawuje nadzór nad działalnością wojewody w zakresie realizacji obowiązków określonych w ustawie. Sprawowanie nadzoru polega na przeprowadzaniu kontroli, w tym na badaniu:

- prawidłowości prowadzonych przez wojewodę postępowań administracyjnych,
- terminowości załatwiania spraw z zakresu spraw określonych w ustawie,
- kształtowaniu jednolitej polityki w zakresie realizacji obowiązków określonych w ustawie i kontroli wykonywania ustalonych sposobów postępowania.

Kontrola ta jest wykonywana na zasadach określonych w ustawie z dnia 15 lipca 2011 r. o kontroli w administracji rządowej (Dz. U. 2011 nr 185 poz. 1092).

Kontrola podmiotów korzystających z udostępniania danych w drodze weryfikacji

Minister właściwy do spraw informatyzacji może przeprowadzać kontrolę podmiotów, które korzystają z dostępu do danych za pomocą udostępniania danych w drodze weryfikacji, w zakresie spełniania przez te podmioty warunków, o których mowa w art. 46 ust. 2 pkt 1 lub art. 48 ust.1.

2.8.3 Kontrola w oparciu o przepisy Ustawy z dnia 6 sierpnia 2010r. o dowodach osobistych

Kontrola podmiotów korzystających z udostępniania danych w trybie ograniczonej teletransmisji

Minister właściwy do spraw informatyzacji może przeprowadzać kontrole podmiotów wymienionych w art. 68 ust. 4 pkt 2 w zakresie spełniania przez te podmioty wymogów określonych w art. 68 ust. 3.

2.9 Audyt sieci przyłączeniowej interesariusza

Właściciel sieci dostępowej do systemu SRP w Ministerstwie właściwym ds. wewnętrznych i administracji może przeprowadzić audyt dotyczący przestrzegania zasad integracji z siecią dostępową SRP.

2.10 Odpowiedzialność z tytułu naruszenia zasad bezpieczeństwa

Decyzja o odebraniu dostępu do rejestru PESEL i rejestru mieszkańców za pomocą urządzeń teletransmisji uprawnionemu interesariuszowi może zostać podjęta w przypadku, gdy nie spełniony jest przynajmniej jeden z poniższych warunków:

- interesariusz posiada urządzenia lub systemy teleinformatyczne przeznaczone do komunikowania się pomiędzy uprawnionymi podmiotami a rejestrem PESEL, umożliwiające identyfikację osoby uzyskującej dane z rejestru, zakres oraz datę ich uzyskania,
- interesariusz posiada zabezpieczenia techniczne i organizacyjne właściwe dla przetwarzania danych osobowych, w szczególności uniemożliwiające dostęp osób nieuprawnionych do przetwarzania danych osobowych i wykorzystanie danych niezgodnie z celem ich uzyskania,
- uzyskanie danych przez interesariusza tą drogą jest uzasadnione specyfiką lub zakresem wykonywanych zadań albo prowadzonej działalności.

Odebranie uprawnień może nastąpić w drodze decyzji administracyjnej wydanej przez Ministra właściwego ds. informatyzacji z rygorem natychmiastowej wykonalności, w oparciu o **Art.51 Ustawy z dnia 24 września 2010 r. o ewidencji ludności**.

Decyzję o odebraniu dostępu do danych zawartych w Rejestrze Dowodów Osobistych w trybie pełnej teletransmisji uprawnionemu interesariuszowi może zostać podjęta w przypadku, gdy nie spełniony jest co najmniej jeden z poniższych warunków:

- interesariusz posiada i stosuje mechanizmy umożliwiające identyfikację i rejestrację osób uzyskujących dostęp do danych oraz rejestrujących zakres udostępnionych danych i datę udostępnienia danych;
- interesariusz posiada i stosuje zabezpieczenia techniczne i organizacyjne chroniące przed uzyskaniem dostępu do danych przez inne osoby i podmioty.

Odebranie uprawnień może nastąpić w drodze decyzji administracyjnej wydanej przez Ministra właściwego ds. informatyzacji z rygorem natychmiastowej wykonalności, w oparciu o **Art. 67 (tryb pełnej teletransmisji) i Art.71 (tryb ograniczonej teletransmisji) Ustawy z dnia 6 sierpnia 2010 r. o dowodach osobistych**.

2.11 Postanowienia końcowe

W przypadku naruszenia bezpieczeństwa danych osobowych z winy użytkownika systemu odpowiedzialność ponosi użytkownik zalogowany do systemu w czasie, gdy dane te zostały pobrane z SRP.