Fundusze Europejskie dla Rozwoju Społecznego | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | PARP Grupa PFR

Rekomendacja nr 1/2026
Rady Programowej ds. kompetencji
z dnia 19.05.2026 r.

Warszawa, 19 maja 2026 r.

Rekomendacja została przygotowana w oparciu o „Ekspertyzę dotyczącą kompetencji pracowników z sektora MŚP w obszarze cyberbezpieczeństwa”, autorstwa Pawła Zegarowa (NASK-PIB) i została wykonana w ramach projektu finansowanego ze środków Ministerstwa Cyfryzacji.

Spis treści

REKOMENDACJA

REKOMENDACJA NR 1/2026 RADY PROGRAMOWEJ DS. KOMPETENCJI

Z 19.05.2026 r.

Rodzaj rekomendacji: kompetencje przedsiębiorców i ich pracowników w zakresie cyberbezpieczeństwa w przedsiębiorstwach, w szczególności w sektorze mikro, małych i średnich przedsiębiorstw.

I. Rekomendacja została wydana uchwałą Rady Programowej ds. kompetencji – Uchwała nr 3/2026 z dnia 19.05. 2026 r.

II. Opis wybranych obszarów kompetencji.

Mając na uwadze dynamiczny rozwój technologii informacyjno-komunikacyjnych, postępującą cyfryzację procesów biznesowych, stale rosnącą liczbę zgłaszanych i obsługiwanych incydentów cyberbezpieczeństwa przez CSIRT NASK, a także strategiczne znaczenie sektora mikro, małych i średnich przedsiębiorstw dla polskiej gospodarki, konieczne jest systemowe rozwijanie kompetencji przedsiębiorców oraz ich pracowników w zakresie cyberbezpieczeństwa.

Wzmacnianie kompetencji w zakresie cyberbezpieczeństwa jest szczególnie istotne **wśród osób niebędących specjalistami IT**, ponieważ to one najczęściej obsługują kluczowe procesy operacyjne, a także stanowią pierwszą linię kontaktu z potencjalnymi zagrożeniami w sektorze mikro, małych i średnich przedsiębiorstw.

W niniejszej rekomendacji przedstawiono wybrane kompetencje w zakresie cyberbezpieczeństwa o charakterze międzysektorowym, czyli takie, które znajdują zastosowanie w wielu sektorach gospodarki.

Kompetencje te dotyczą następujących obszarów:

A. Rozpoznawanie oszustw komputerowych – Blok 1,
B. Cyberhigiena – Blok 2,
C. Wzmacnianie odporności na socjotechniki wykorzystywane przez cyberprzestępców – Blok 3,
D. Bezpieczeństwo danych i informacji – Blok 4,
E. Podstawy reagowania na incydenty -Blok 5.

Obszar A: „**Rozpoznawanie oszustw komputerowych**” obejmuje szeroki zakres kompetencji związanych z **umiejętnością identyfikacji najczęściej występujących oszustw komputerowych**, w szczególności tych, które bazują na manipulacji użytkownikiem (**phishingu, smishingu, vishingu**), a nie na zaawansowanych metodach technicznych.

Obszar B: „**Cyberhigiena**” obejmuje szeroki zakres kompetencji związanych z **umiejętnością bezpiecznego korzystania z narzędzi cyfrowych** w codziennej pracy, w szczególności z poczty elektronicznej, systemów online, urządzeń końcowych oraz usług chmurowych.

Obszar C: „**Wzmacnianie odporności na socjotechniki wykorzystywane przez cyberprzestępców**” obejmuje szeroki zakres kompetencji związanych z **umiejętnością rozumienia mechanizmów manipulacji psychologicznej, rozpoznawania i neutralizowania prób wpływu**, których celem jest skłonienie użytkownika do podjęcia niekorzystnych działań.

Obszar D: „**Bezpieczeństwo danych i informacji w codziennej pracy**” obejmuje szeroki zakres kompetencji związanych z **umiejętnością bezpiecznego przetwarzania, przechowywania, udostępniania i ochroną informacji** wykorzystywanych w bieżącej działalności przedsiębiorstwa.

Obszar E: „**Podstawy reagowania na incydenty**” obejmuje szeroki zakres kompetencji związanych z **rozpoznawaniem zdarzeń naruszających bezpieczeństwo oraz podejmowaniem właściwych, uporządkowanych działań ograniczających skutki incydentu** na poziomie użytkownika i przedsiębiorstwa.

III. Analiza trendów rynkowych oraz obowiązujących aktów prawnych z punktu widzenia potrzeb kompetencyjnych opisanych w dalszej części dokumentu.

Obszar A: „Rozpoznawanie oszustw komputerowych”.

Jak wynika z raportu CERT Polska za rok 2024, w Polsce odnotowano 600 990 zgłoszeń, z których 103 449 zostało zakwalifikowanych jako potwierdzone incydenty cyberbezpieczeństwa. Około 95% z nich stanowiły oszustwa komputerowe, głównie związane z wyłudzaniem danych dostępowych i podszywaniem się pod zaufane podmioty. Oznacza to, że dominującym mechanizmem cyberataków jest manipulacja użytkownikiem. Raport: https://cert.pl/raporty/raport-roczny-2024/.

Mając na uwadze dynamiczny rozwój technologii informacyjno-komunikacyjnych, a także stały wzrost liczby incydentów cyberbezpieczeństwa obsługiwanych przez CSIRT NASK, systemowe rozwijanie kompetencji w zakresie szeroko rozumianego cyberbezpieczeństwa wśród przedsiębiorców i pracowników przedsiębiorstw z sektora MŚP wydaje się priorytetem. Rozwój tych kompetencji jest kluczowy zarówno z perspektywy operacyjnej i strategicznej.

Obszar B: „Cyberhigiena”.

Z raportu DESI z 2024 roku wynika, że Polska znajduje się na 3 miejscu od końca wśród krajów Unii Europejskiej pod względem poziomu podstawowych umiejętności cyfrowych. Raport: DESI indicators - Digital Decade DESI visualisation tool. Oznacza to, że znaczny odsetek polskich przedsiębiorców i pracowników z sektora MŚP nie posiada podstawowych umiejętności cyfrowych. Wynik ten bezpośrednio przekłada się na większe ryzyko wystąpienia incydentów cyberbezpieczeństwa, które potencjalnie mogą prowadzić do strat finansowych, reputacyjnych, przerwania ciągłości działania i upadku przedsiębiorstw.

Obszar C: „Wzmacnianie odporności na socjotechniki wykorzystywane przez cyberprzestępców”.

Wraz ze stałym wzrostem liczby incydentów cyberbezpieczeństwa widoczna jest również zmiana charakteru zagrożeń. Rozwój narzędzi wykorzystujących sztuczną inteligencję umożliwia cyberprzestępcom zarówno prowadzenia masowych, jak i precyzyjnie wymierzonych cyberataków. Analiza incydentów wykazuje, że skuteczność cyberataków w dużej mierze opiera się na wykorzystaniu szeroko rozumianych podatności psychologicznych użytkowników. Trend ten znajduje potwierdzenie w analizach ENISA, które wskazują, że czynnik ludzki pozostaje kluczowym elementem każdego systemu cyberbezpieczeństwa.

Obszar D: „Bezpieczeństwo danych i informacji w codziennej pracy”.

Dane są kluczowym zasobem przedsiębiorstw zarówno z perspektywy operacyjnej, jak i strategicznej. Postępująca cyfryzacja i stopniowe przenoszenie wszystkich procesów biznesowych do świata cyfrowego powodują, że przetwarzanie informacji odbywa się w sposób rozproszony. Bezpieczeństwo danych nie jest wyłącznie zagadnieniem technicznym, ale także kompetencyjnym.

Obszar E: „Podstawy reagowania na incydenty”.

Zdolność do szybkiego rozpoznania incydentu cyberbezpieczeństwa jest istotnym elementem odporności przedsiębiorstwa. Warto podkreślić, że reagowanie na incydenty nie ogranicza się wyłącznie do aspektu technicznego. Proces ten obejmuje szereg elementów związanych z komunikacją. W środowisku przedsiębiorstw w sektorze MŚP, w którym procesy są mniej sformalizowane rola świadomego pracownika jest szczególnie istotna.

A. Zapotrzebowanie na kompetencje/kwalifikacje w wybranych obszarach kompetencji.

A.1. Kompetencja/kwalifikacja: „Wzmacnianie bezpieczeństwa cyfrowego w środowisku pracy w MŚP”.

Czy kompetencja/kwalifikacja jest włączona do Zintegrowanego Systemu Kwalifikacji?

NIE

Krótka charakterystyka kompetencji:

Kompetencja „Wzmacnianie bezpieczeństwa cyfrowego w środowisku pracy w MŚP” przeznaczona jest dla przedsiębiorców oraz pracowników sektora mikro, małych i średnich przedsiębiorstw, którzy w codziennej pracy korzystają z poczty elektronicznej, systemów online, bankowości elektronicznej oraz narzędzi komunikacji cyfrowej.

Celem uzyskania kompetencji jest rozwinięcie wiedzy i umiejętności umożliwiających: identyfikowanie i analizowanie oszustw komputerowych; stosowanie zasad cyberhigieny w środowisku pracy, w szczególności w zakresie bezpiecznego korzystania z urządzeń, systemów, sieci oraz ochrony dostępu i danych; rozpoznawanie i analizowanie mechanizmów manipulacji psychologicznej wykorzystywanych w atakach socjotechnicznych oraz podejmowanie decyzji ograniczających podatność na tego typu zagrożenia; bezpieczne przetwarzanie, przechowywanie oraz udostępnianie danych i informacji w działalności przedsiębiorstwa; identyfikowanie incydentów cyberbezpieczeństwa oraz podejmowanie podstawowych działań ograniczających ich skutki w środowisku pracy.

W trakcie usługi rozwojowej uczestnicy nabywają wiedzę, umiejętności i kompetencje społeczne, uporządkowane w pięć bloków, wyznaczonych przez pięć zdefiniowanych obszarów, w zakresie:

- ✓ rodzajów oszustw komputerowych, elementów ostrzegawczych w komunikacji elektronicznej, realnych scenariuszy oszustw komputerowych oraz komunikowania zagrożeń i dzielenia się wiedzą, opracowanych w ramach Bloku 1 - Identyfikowanie i analizowanie oszustw

komputerowych w MŚP;

- ✓ zasad cyberhigieny, zarządzania hasłami i dostępem, bezpieczeństwa urządzeń
  i oprogramowania, korzystania z sieci, tworzenia kopii zapasowych oraz reagowania na nieprawidłowe działania, opracowanych w ramach Bloku 2 - Stosowanie zasad cyberhigieny w codziennej pracy z narzędziami cyfrowymi;
- ✓ mechanizmów socjotechnik wykorzystywanych w atakach, faz ataków socjotechnicznych, nawyków decyzyjnych zwiększających odporność na socjotechniki, technik manipulacji psychologicznej oraz asertywnego reagowania na próby nacisku lub wpływu w sytuacjach niepewności lub podwyższonego ryzyka ataku, opracowanych w ramach Bloku 3 - Stosowanie zasad bezpiecznego przetwarzania, przechowywania i udostępniania danych w codziennej pracy;
- ✓ rodzajów danych i informacji w przedsiębiorstwie, zasad bezpiecznego przetwarzania i przechowywania danych, zapobiegania wyciekom danych, zasad odpowiedzialności i zgodności z przepisami o ochronie danych oraz wsparcia współpracowników
  w stosowaniu zasad bezpiecznego przetwarzania i przechowywania danych, opracowanych w ramach Bloku 4 - Stosowanie zasad bezpiecznego przetwarzania, przechowywania i udostępniania danych w codziennej pracy;
- ✓ zdarzeń mogących stanowić incydent cyberbezpieczeństwa, podstawowych działań ograniczających skutki incydentu cyberbezpieczeństwa, działań ograniczających ryzyko ponownych incydentów oraz działań zgodnych z dobrymi praktykami w zakresie współpracy z pracownikami w sytuacji kryzysowej, opracowanych w ramach Bloku 5 - Rozpoznawanie incydentów cyberbezpieczeństwa oraz podejmowanie podstawowych działań ograniczających ich skutki.

BLOK 1 - IDENTYFIKOWANIE I ANALIZOWANIE OSZUSTW KOMPUTEROWYCH W MŚP.

Efekty uczenia się i kryteria weryfikacji:

1.1. Charakteryzuje najczęściej występujące rodzaje oszustw komputerowych.

Kryteria weryfikacji:

a. wyjaśnia pojęcia phishing, smishing i vishing oraz wskazuje różnice między nimi,

b. rozróżnia oszustwa komputerowe masowe i ukierunkowane, z uwzględnieniem ich charakterystycznych cech,

c. wskazuje najczęstsze cele oszustw komputerowych w przedsiębiorstwach, w tym wyłudzanie danych, środków finansowych oraz dostępu do systemów,

d. opisuje aktualne trendy w oszustwach komputerowych, w tym złośliwe wykorzystanie sztucznej inteligencji,

e. wyjaśnia konsekwencje oszustw dla funkcjonowania przedsiębiorstwa (finansowe, operacyjne, reputacyjne),

f. komunikuje współpracownikom informacje o rozpoznanych zagrożeniach związanych z oszustwami komputerowymi.

1.2. Rozpoznaje elementy ostrzegawcze w komunikacji elektronicznej.

Kryteria weryfikacji:

a. wskazuje cechy charakterystyczne fałszywych stron logowania i płatności,

b. ocenia wiarygodność linków i załączników w komunikacji elektronicznej za pomocą dostępnych narzędzi,

c. identyfikuje cechy wiadomości phishingowych,

d. wyjaśnia mechanizm Business Email Compromise (BEC) i identyfikuje typowe schematy wykorzystania,

e. wskazuje kanały komunikacji w przedsiębiorstwach z sektora MŚP, które są wykorzystywane przez cyberprzestępców do realizacji oszustw komputerowych,

f. dzieli się wiedzą, informacjami, umiejętnościami w rozpoznawaniu elementów ostrzegawczych w komunikacji elektronicznej z innymi pracownikami.

1.3. Analizuje realne scenariusze oszustw komputerowych.

Kryteria weryfikacji:

a. omawia scenariusz oszustwa komputerowego, które polega na przejęciu dostępu do poczty elektronicznej, wskazując jego przebieg oraz możliwe skutki,
b. omawia scenariusz oszustwa komputerowego, które polega na wyłudzeniu pieniędzy wykorzystując fałszywą fakturę,
c. omawia scenariusz oszustwa komputerowego, które polega na podszywaniu się pod przełożonego lub współpracownika,
d. wskazuje dominujące typy oszustw komputerowych w przedsiębiorstwach w sektorze MŚP,
e. identyfikuje główne przyczyny podatności przedsiębiorstw w sektorze MŚP,
f. dzieli się wnioskami z analiz scenariuszy oszustw komputerowych z innymi pracownikami.

BLOK 2 - STOSOWANIE ZASAD CYBERHIGIENY W CODZIENNEJ PRACY Z NARZĘDZIAMI CYFROWYMI I URZĄDZENIAMI KOŃCOWYMI W MŚP.

Efekty uczenia się i kryteria weryfikacji:

2.1. Rozumie zasady cyberhigieny.

Kryteria weryfikacji:

a. definiuje pojęcie cyberhigiena oraz jej rolę w bezpieczeństwie organizacji,
b. wymienia podstawowe zasady bezpiecznego korzystania z narzędzi cyfrowych,
c. omawia rolę użytkownika w systemie cyberbezpieczeńtwa,
d. wskazuje najczęstsze błędy użytkowników prowadzące do incydentów,
e. wyjaśnia rolę użytkownika jako pierwszej linii obrony,
f. reaguje na zaobserwowane działania współpracowników zwiększające ryzyko incydentu cyberbezpieczeństwa.

2.2. Stosuje zasad bezpiecznego zarządzanie hasłami i dostępem.

Kryteria weryfikacji:

a. tworzy hasła spełniające zasady bezpieczeństwa,
b. rozróżnia hasła silne i słabe,
c. stosuje zasadę unikalności haseł,
d. wyjaśnia rolę menedżerów haseł,
e. omawia korzyści związane z wykorzystywaniem uwierzytelniania wieloskładnikowego (MFA),
f. reaguje na zaobserwowane działania współpracowników wskazujące na sytuacje naruszenia zasad bezpiecznego zarządzania hasłami w środowisku pracy.

2.3. Stosuje zasady bezpieczeństwa urządzeń i oprogramowania.

Kryteria weryfikacji:

a. wyjaśnia znaczenie aktualizacji systemów i aplikacji,
b. stosuje blokadę ekranu i zabezpieczenia biometryczne,
c. rozpoznaje ryzyko instalacji nieznanych aplikacji,
d. wskazuje skutki braku aktualizacji dla cyberbezpieczeństwa,
e. weryfikuje i ogranicza uprawnienia aplikacji do niezbędnego zakresu aplikacji,
f. reaguje na zaobserwowane działania współpracowników wskazujące na sytuacje nieprawidłowego korzystania z urządzeń i oprogramowania w środowisku pracy.

2.4. Stosuje zasady bezpiecznego korzystania z sieci.

Kryteria weryfikacji:

a. wskazuje ryzyka związane z korzystaniem z publicznych sieci WiFi,
b. odróżnia sieć publiczną od prywatnej,
c. wskazuje korzyści stosowania VPN,
d. rozpoznaje sytuacje wymagające unikania korzystania z publicznych sieci WiFi,
e. rozpoznaje podejrzane sieci publiczne WiFi,
f. informuje współpracowników o zidentyfikowanych zagrożeniach związanych z korzystaniem z publicznych sieci Wi-Fi.

2.5. Stosuje podstawowe zasady tworzenia kopii zapasowych.

Kryteria weryfikacji:

a. definiuje pojęcie kopii zapasowej,
b. wyjaśnia cel tworzenia kopii zapasowej,
c. wskazuje dane wymagające kopii zapasowej z punktu widzenia, funkcjonowania przedsiębiorstwa,
d. omawia skutki braku kopii zapasowej,
e. wyjaśnia różnicę pomiędzy kopią zapasową lokalną i chmurową,
f. reaguje na sytuacje braku kopii zapasowej lub ryzyka utraty danych w środowisku pracy.

BLOK 3 - ROZPOZNAWANIE I NEUTRALIZOWANIE TECHNIK MANIPULACJI PSYCHOLOGICZNEJ STOSOWANYCH W CYBERATAKACH.

Efekty uczenia się i kryteria weryfikacji:

3.1. Charakteryzuje mechanizmy socjotechniczne wykorzystywane w cyberatakach.

Kryteria weryfikacji:

a. definiuje pojęcie socjotechniki w cyberbezpieczeństwie,
b. rozróżnia ataki techniczne i socjotechniczne, wskazując ich charakterystyczne cechy,
c. identyfikuje przykłady złośliwego wykorzystania sztucznej inteligencji, ze szczególnym uwzględnieniem deepfake,
d. identyfikuje najczęstsze kanały ataków socjotechnicznych,
e. wyjaśnia cele ataków socjotechnicznych,
f. wskazuje rolę użytkownika jako potencjalnego celu ataku socjotechnicznego,
g. reaguje na próby wywierania presji lub manipulacji w środowisku pracy.

3.2. Rozpoznaje fazy ataku socjotechnicznego.

Kryteria weryfikacji:

a. omawia istotę etapu rozpoznawania (rekonesansu) potencjalnego celu ataku,

b. identyfikuje działania charakterystyczne dla etapu budowania relacji z potencjalnym celem ataku,
c. rozróżnia etapy budowania zaufania i wywierania presji,
d. opisuje skutki udanego ataku socjotechnicznego dla funkcjonowania przedsiębiorstwa w sektorze MŚP,
e. rozróżnia phishing masowy i ukierunkowany,
f. wykorzystuje asertywność w kontaktach z osobami wywierającymi wpływ lub nacisk w celu uzyskania informacji.

3.3. Buduje nawyki decyzyjne zwiększające odporność na socjotechniki.

Kryteria weryfikacji:

a. omawia wpływ stresu na proces podejmowania decyzji,
b. omawia wpływ autorytetu na proces podejmowanie decyzji,
c. wyjaśnia wpływ heurystyk na proces podejmowania decyzji,
d. analizuje konsekwencje ulegania błędom poznawczym,
e. unika działania pod wpływem impulsu,
f. analizuje komunikat przed udzieleniem odpowiedzi i podjęciem działań,
g. konsultuje z pracownikami decyzje w sytuacjach niepewności lub podwyższonego ryzyka.

3.4. Rozpoznaje techniki manipulacji psychologicznej stosowane w atakach socjotechnicznych.

Kryteria weryfikacji:

a. identyfikuje komunikaty wywołujące presję czasu lub konieczność natychmiastowego działania,
b. omawia wpływ emocji na proces podejmowania decyzji,
c. identyfikuje komunikaty, które mają na celu podszywanie się pod przełożonego lub instytucję publiczną,
d. rozpoznaje komunikaty wywołujące posłuszeństwo wobec autorytetu,
e. identyfikuje cechy charakterystyczne komunikatów, które zawierają obietnice nagrody,
f. informuje współpracowników o rozpoznanych próbach manipulacji w komunikacji

elektronicznej.

BLOK 4 - STOSOWANIE ZASAD BEZPIECZNEGO PRZETWARZANIA, PRZECHOWYWANIA I UDOSTĘPNIANIA DANYCH W CODZIENNEJ PRACY.

Efekty uczenia się i kryteria weryfikacji:

4.1. Charakteryzuje rodzaje danych i informacji w przedsiębiorstwie.

Kryteria weryfikacji:

a. rozróżnia kategorie danych, w tym dane osobowe i finansowe,
b. definiuje dane wewnętrzne w kontekście funkcjonowania przedsiębiorstwa,
c. omawia skutki ujawnienia poszczególnych kategorii danych,
d. wyjaśnia na czym polega przypisywanie poziomów poufności danych w przedsiębiorstwie,
e. identyfikuje dane krytyczne dla ciągłości działania przedsiębiorstwa,
f. reaguje na zidentyfikowane zagrożenia zwracając uwagę współpracownikom na konieczność właściwego postępowania z danymi.

4.2. Stosuje zasady bezpiecznego przetwarzania i przechowywania danych.

Kryteria weryfikacji:

a. wyjaśnia dlaczego powinno przetwarzać się tylko dane niezbędne,
b. analizuje skutki nieuzasadnionego kopiowania danych,
c. rozpoznaje ryzyko przechowywania danych na przenośnych nośnikach pamięci oraz lokalnych dyskach,
d. stosuje szyfrowanie plików,
e. korzysta z bezpiecznych platform transferu danych,
f. reaguje na sytuacje nieprawidłowego przetwarzania lub przechowywania danych w środowisku pracy.

4.3. Zapobiega wyciekom danych.

Kryteria weryfikacji:

a. identyfikuje sytuacje mogące prowadzić do wycieku danych,

b. rozpoznaje ryzyko korzystania z prywatnych urządzeń w celach służbowych,
c. stosuje zasadę czystego biurka oraz blokowania komputera,
d. zgłasza podejrzenie wycieku danych do przełożonego i współpracowników,
e. zabezpiecza hasła oraz dane uwierzytelniające przed widocznością,
f. wspiera współpracowników w stosowaniu zasad zapobiegających wyciekom danych.

4.4. Postępuje zgodnie z zasadą odpowiedzialności i zgodności z przepisami o ochronie danych.

Kryteria weryfikacji:

a. rozróżnia zakres odpowiedzialności pracownika i pracodawcy w obszarze ochrony danych,
b. wyjaśnia konsekwencje prawne naruszeń przepisów w obszarze ochrony danych,
c. rozpoznaje przypadki nieautoryzowanego dostępu do danych,
d. stosuje zasady obiegu i przetwarzania dokumentów,
e. wspiera innych pracowników w bezpiecznych praktykach dotyczących przetwarzania i przechowywania danych.

BLOK 5 - ROZPOZNAWANIE INCYDENTÓW CYBERBEZPIECZEŃSTWA ORAZ PODEJMOWANIE PODSTAWOWYCH DZIAŁAŃ OGRANICZAJĄCYCH ICH SKUTKI.

Efekty uczenia się i kryteria weryfikacji:

5.1. Identyfikuje zdarzenia mogące stanowić incydent cyberbezpieczeństwa.

Kryteria weryfikacji:

a. rozróżnia pojęcia podatności i incydentu cyberbezpieczeństwa,
b. identyfikuje przykłady naruszeń poufności, integralności i dostępności,
c. wskazuje konsekwencje infekcji złośliwym oprogramowaniem dla przedsiębiorstwa,
d. odróżnia incydent techniczny od błędu użytkownika,
e. identyfikuje najczęściej występujące rodzaje incydentów cyberbezpieczeństwa w przedsiębiorstwach z sektora MŚP,
f. informuje innych pracowników o zaobserwowanych nieprawidłowościach.

5.2. Podejmuje podstawowe działania ograniczające skutki incydentu cyberbezpieczeństwa.

Kryteria weryfikacji:

a. wskazuje działania podejmowane bezpośrednio po wykryciu incydentu cyberbezpieczeństwa,
b. zabezpiecza dowody i zachowuje podejrzaną wiadomość lub plik
c. omawia procedurę poinformowania właściwego CSIRTu o incydencie cyberbezpieczeństwa,
d. identyfikuje rodzaj zagrożonych danych,
e. omawia zasadę minimalizacji dalszego ryzyka,
f. działa zgodnie z dobrymi praktykami i współpracuje z pracownikami w sytuacji kryzysowej, pomimo presji czasu.

5.3. Stosuje działania ograniczające ryzyko ponownych incydentów.

Kryteria weryfikacji:

a. analizuje przyczyny najczęściej występujących incydentów cyberbezpieczeństwa w przedsiębiorstwach z sektora MŚP,
b. wskazuje działania usprawniające procedury bezpieczeństwa w przedsiębiorstwie,
c. przekazuje informacje współpracownikom o wnioskach wynikających z incydentu cyberbezpieczeństwa,
d. współpracuje z pracownikami w celu wdrażania działań zapobiegających incydentom,
e. wskazuje zasady cyberhigieny zmniejszają ryzyko przyszłych incydentów.

Szacowana skala niedoboru kompetencji/kwalifikacji (liczba osób)

6 500 000 osób

Usługa rozwojowa wspierająca zdobycie kompetencji/kwalifikacji
Minimalne wymagania dotyczące usługi

Usługa musi być realizowana przez podmiot spełniający wymagania określone w Rozporządzeniu Ministra Funduszy i Polityki Regionalnej z dnia 28 lipca 2023 r. w sprawie rejestru podmiotów świadczących usługi rozwojowe (Dz.U. z 2023 r. poz. 1686). Usługa musi być realizowana zgodnie z wymogami określonymi w wyżej

wymienionym Rozporządzeniu oraz określonymi w niniejszej rekomendacji minimalnymi wymaganiami dotyczącymi usługi.

Minimalne warunki w zakresie kompetencji osób przystępujących do usługi:

Brak

Maksymalna liczebność grupy szkoleniowej:

15 osób

Minimalny czas trwania usługi:

Usługa jest realizowana dla pracowników sektora mikro, małych i średnich przedsiębiorstw, wykonujących zróżnicowane zadania. Szkolenie trwa 56 godzin i składa się z niezależnych modułów, które mogą być elastycznie łączone w zależności od potrzeb uczestników
oraz specyfiki stanowiska pracy. Modułowa organizacja szkolenia pozwala na delegowanie pracowników na krótsze, jedno- lub dwudniowe bloki szkoleniowe, co ogranicza wpływ na bieżące funkcjonowanie przedsiębiorstwa. Natomiast, w odniesieniu do właścicieli oraz osób zarządzających w sektorze mikro, małych i średnich przedsiębiorstw zalecamy szkolenie w formie spójnego programu obejmujące wszystkie bloki. Usługa trwa:

- Blok 1 – 8 godzin,
- Blok 2 – 16 godzin,
- Blok 3 – 8 godzin,
- Blok 4 – 16 godzin,
- Blok 5 – 8 godzin.

Minimalne wymagania w zakresie zasobów:

- sala wykładowa spełniająca standardy jakości w zakresie realizacji usług szkoleniowych, dostosowana do liczby uczestników usługi,
- sprzęt komputerowy dla trenera z dostępem do internetu,
- sprzęt komputerowy dla uczestników z dostępem do internetu,

- oprogramowanie umożliwiające prezentowanie treści, realizację zadań, ćwiczeń i weryfikację umiejętności oraz komunikację zdalną,
- rzutnik, ekran,
- materiały dla uczestników usługi.

Minimalne wymagania w zakresie kompetencji trenera:

Trener powinien posiadać kompetencje spełniające wymogi określone w §6

rozporządzenia Ministra Funduszy i Polityki Regionalnej z dnia 28 lipca 2023 r. w sprawie rejestru podmiotów świadczących usługi rozwojowe (Dz.U. z 2023 r. poz. 1686)
oraz dodatkowo powinien posiadać:

- doświadczenie w zakresie tematyki usługi: minimum 2 lata doświadczenia w zakresie cyberbezpieczeństwa,
- doświadczenie w zakresie realizacji usług rozwojowych: doświadczenie w prowadzeniu szkoleń - minimum 100 godzin.

Minimalne wymagania w zakresie sposobu oraz metod realizacji usługi:

W trakcie realizacji usługi powinny być wykorzystywane metody pozwalające na rozwój umiejętności, w szczególności case study, ćwiczenia do samodzielnego lub grupowego wykonania przez uczestników usługi. Usługa musi zostać zakończona weryfikacją nabytych przez uczestników usługi efektów uczenia się, przeprowadzoną zgodnie ze standardami określonymi w rozporządzeniu Ministra Funduszy i Polityki Regionalnej z dnia 28 lipca 2023 r. w sprawie rejestru podmiotów świadczących usługi rozwojowe (Dz.U. z 2023 r. poz. 1686).

Rekomenduje się, żeby walidacja efektów uczenia została przeprowadzona z wykorzystaniem:

- testu wiedzy w formie ustnej lub pisemnej (elektronicznej),
- zadań praktycznych w warunkach symulowanych,
- zadań decyzyjnych,
- wywiadu walidacyjnego,
- obserwacji w warunkach symulowanych lub odgrywania ról, umożliwiającej ocenę

zachowań uczestnika w zakresie komunikacji z innymi pracownikami.

Rekomendowana forma realizacji usługi:

Stacjonarna

Potencjalni uczestnicy usług rozwojowych

Osoby odpowiedzialne lub osoby, które w codziennej pracy korzystają z narzędzi komunikacji elektronicznej, którym przedsiębiorca zamierza powierzyć odpowiedzialność za:

- obsługę poczty elektronicznej i komunikację z klientami,
- realizację płatności i operacji finansowych z wykorzystaniem bankowości internetowej,
- realizację zamówień,
- administrację biurową,
- nadzór nad procesami organizacyjnymi w przedsiębiorstwie.

Dodatkowe uwagi

Brak

Załączniki:

Załącznik nr 1 – Szacowany koszt wdrożenia rekomendacji