Poradnik dla użytkowników:

Jak poszerzyć wiedzę

o bezpieczeństwie informacji

czerwiec 2006 r.

Spis treści

Streszczenie

Świadomość ryzyka i dostępnych zabezpieczeń to pierwsza linia obrony bezpieczeństwa systemów i sieci informacyjnych. Niniejszy Poradnik zawiera praktyczne wskazówki dla państw członkowskich na temat tego, jak można poszerzać wiedzę o bezpieczeństwie informacji w różnych grupach docelowych, w szczególności wśród użytkowników prywatnych i MŚP. Dokument niniejszy skierowany jest do państw członkowskich Unii Europejskiej w celu wykorzystania przy realizacji inicjatyw i programów podnoszenia świadomości na temat bezpieczeństwa informacji.

Poradnik dla użytkowników: Jak poszerzyć wiedzę o bezpieczeństwie informacji ilustruje główne procesy konieczne do zaplanowania, zorganizowania i przeprowadzenia inicjatyw mających na celu uwrażliwienie na bezpieczeństwo informacji – planowanie i ocenę, realizację i zarządzanie, ewaluację i dostosowanie. Każdy proces jest analizowany, określa się w nim działania i relacje zależne od upływu czasu. Przedstawiony model procesu zawiera podstawę dla rozpoczęcia działań związanych z określaniem zakresu i planowaniem, jak również z realizacją i oceną każdego programu. Poradnik ma również na celu zapewnienie spójnego i szerokiego zrozumienia przez użytkowników głównych procesów i działań.

Etap planowania i oceny uznawany jest za najistotniejszy w osiągnięciu sukcesu jakiegokolwiek programu. Na potrzeby użytkowników identyfikuje się i opisuje kluczowe działania. W Poradniku szczególny nacisk położono na znaczenie określenia celów i założeń inicjatyw, zdefiniowanie grup docelowych, stworzenie planu przekazywania informacji oraz pomiar skuteczności programów podnoszenia świadomości. Ponadto w Poradniku wzięto pod uwagę, że przyjęcie w stosunku do inicjatyw edukacyjnych podejścia polegającego na zmianie zarządzania ma ogromne znaczenie, jako że pozwala na zasypanie przepaści pomiędzy konkretną kwestią a reakcją człowieka na potrzebę zmian.

Zamieszczono również szablony i wzory sugerowanych narzędzi w celu wsparcia użytkowników na różnych etapach kampanii zwiększających wiedzę. Są to, między innymi, szablon przedstawienia zdobytego doświadczenia, wzór harmonogramu prac i szablon przedstawienia danych o grupie docelowej.

W Poradniku wskazano również przeszkody w zrealizowaniu zamierzeń i praktyczne wskazówki na temat tego, jak je przezwyciężyć podczas etapu planowania i wdrażania programu. Poradnik dodatkowo opisuje główne czynniki osiągnięcia sukcesu każdej inicjatywy dotyczącej bezpieczeństwa informacji. Na przykład, przed wdrożeniem (lub zmianą) programu podnoszącego świadomość i sformułowaniem przekazu konieczne jest określenie punktu odniesienia dotyczącego obecnego stanu rzeczy, jako że zwielokrotni to wpływ poprzez zwiększenie liczby osób otrzymujących przekaz.

ENISA ma nadzieję, że niniejszy Poradnik stanie się dla państw członkowskich wartościowym narzędziem w przygotowywaniu i wdrażaniu inicjatyw i programów mających na celu podniesienie świadomości. Zapewnianie bezpieczeństwa informacji jest samo w sobie dużym wyzwaniem, a zwiększanie świadomości i wiedzy wśród wybranych odbiorców docelowych to istotny krok w kierunku spełnienia tego wyzwania.

Wstęp

W dzisiejszym zautomatyzowanym świecie, w życiu prywatnym i w pracy technologie ICT (Information Communication Technologies) są bezcenne w codziennej działalności zarówno dla osób prywatnych, jak i przedsiębiorstw. Jednocześnie coraz więcej osób i przedsiębiorstw zagrożonych jest naruszeniem bezpieczeństwa informacji. Wynika to z niedociągnięć w nowych i istniejących technologiach oraz z konwergencji, wzrastającego użycia stałych łączy oraz ciągłego, gwałtownego przyrostu liczby użytkowników w państwach członkowskich. Takie naruszenia bezpieczeństwa mogą być związane z technologiami informatycznymi, na przykład poprzez działanie wirusów komputerowych, lub też warunkowane społecznie, na przykład poprzez kradzież wyposażenia. W czasie, kiedy wszyscy coraz bardziej polegamy na informacji cyfrowej, liczba zagrożeń rośnie. Znaczna liczba obywateli może być nieświadoma narażenia na zagrożenia bezpieczeństwa.

Przy zaawansowaniu i szybkim rozprzestrzenianiu się tych niebezpieczeństw dzisiejsze rozwiązania dotyczące bezpieczeństwa informacji jutro są już przestarzałe. Krajobraz bezpieczeństwa podlega ciągłym zmianom. Większość analityków jest zdania, że we wszelkich systemach bezpieczeństwa informacji czynnik ludzki jest najsłabszym ogniwem. W takim przypadku jedynie wyraźna zmiana w sposobie myślenia użytkowników albo kulturze organizacyjnej może skutecznie zredukować naruszenia bezpieczeństwa informacji.

W całej Europie występują znaczne braki w świadomości na temat bezpieczeństwa. Na przykład prywatni użytkownicy w wielu państwach członkowskich mogą być nieświadomi tego, że ich komputery osobiste mogą być kontrolowane bez ich wiedzy przez hakerów planujących oszustwo z wykorzystaniem tożsamości elektronicznej lub atak DoS (Denial of Service).

Europejska Agencja Bezpieczeństwa Sieci i Informacji (ENISA) doradza i udziela pomocy państwo członkowskim w osiąganiu lepszego zrozumienia zagadnienia podnoszenia świadomości na temat bezpieczeństwa w celu propagowania bezpiecznego i odpowiedzialnego korzystania z ICT.

Zakres

ENISA ma świadomość, że wiedza o zagrożeniach i dostępnych zabezpieczeniach jest pierwszą linią obrony bezpieczeństwa systemów i sieci informacyjnych. Stąd też celem niniejszego Poradnika jest przedstawienie praktycznych porad dla państw członkowskich w celu przygotowania i wdrożenia inicjatyw edukacyjnych dotyczących bezpieczeństwa informacji. Podane informacje zawierają porady na temat tego, jak krok po kroku stworzyć podstawę skutecznej i odpowiednio dopasowanej kampanii edukacyjnej mającej na celu zwiększenie świadomości. Poradnik niniejszy oparty jest na badaniach i analizach wykorzystanych przez pracowników ENISA oraz na informacjach powszechnie dostępnych lub przedstawionych Agencji przez odpowiednie organizacje państw członkowskich UE. Skierowany jest do państw członkowskich UE w celu wykorzystania przy realizacji kampanii podnoszenia świadomości na temat bezpieczeństwa informacji.

Założenia

Przy pomocy niniejszego Poradnika ENISA pragnie:

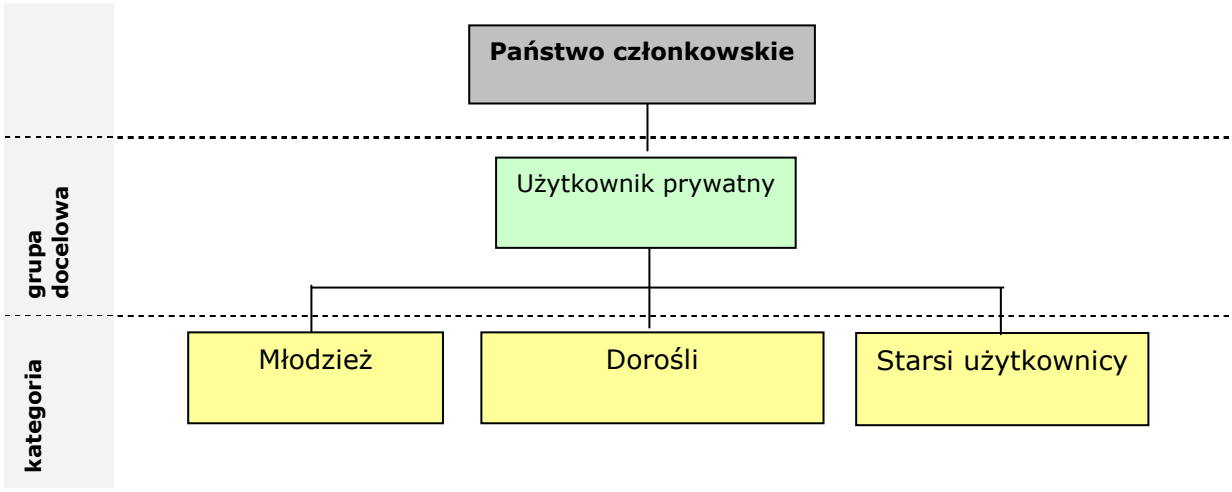
- zilustrować przykładową strategię planowania, organizowania i przeprowadzania inicjatyw mających na celu uwrażliwienie na bezpieczeństwo informacji;

- wskazać potencjalne zagrożenia związane z inicjatywami podnoszenia świadomości w celu uniknięcia takich trudności w przyszłych programach;
- przedstawić zasady oceny skuteczności programów podnoszących świadomość;
- przedstawić zasady przekazywania informacji;
- zaprezentować szablony i narzędzia przeznaczone do użycia jako punkty wyjściowe przez zespół odpowiedzialny za podnoszenie świadomości;
- przyczynić się do rozwoju kultury bezpieczeństwa informacji w państwach członkowskich poprzez zachęcanie użytkowników do przejawiania odpowiedzialnych zachowań i w konsekwencji podejmowania bezpieczniejszych działań.

Docelowi odbiorcy

Niniejszy Poradnik skierowany jest do konkretnych grup docelowych, dla których można zorganizować inicjatywy edukacyjne: do użytkowników prywatnych oraz małych i średnich przedsiębiorstw (MŚP).

Użytkownicy prywatni: obywatele w różnym wieku i o różnych umiejętnościach technicznych, którzy wykorzystują ICT na potrzeby prywatne poza miejscem pracy. Tę grupę użytkowników można podzielić na trzy kategorie:



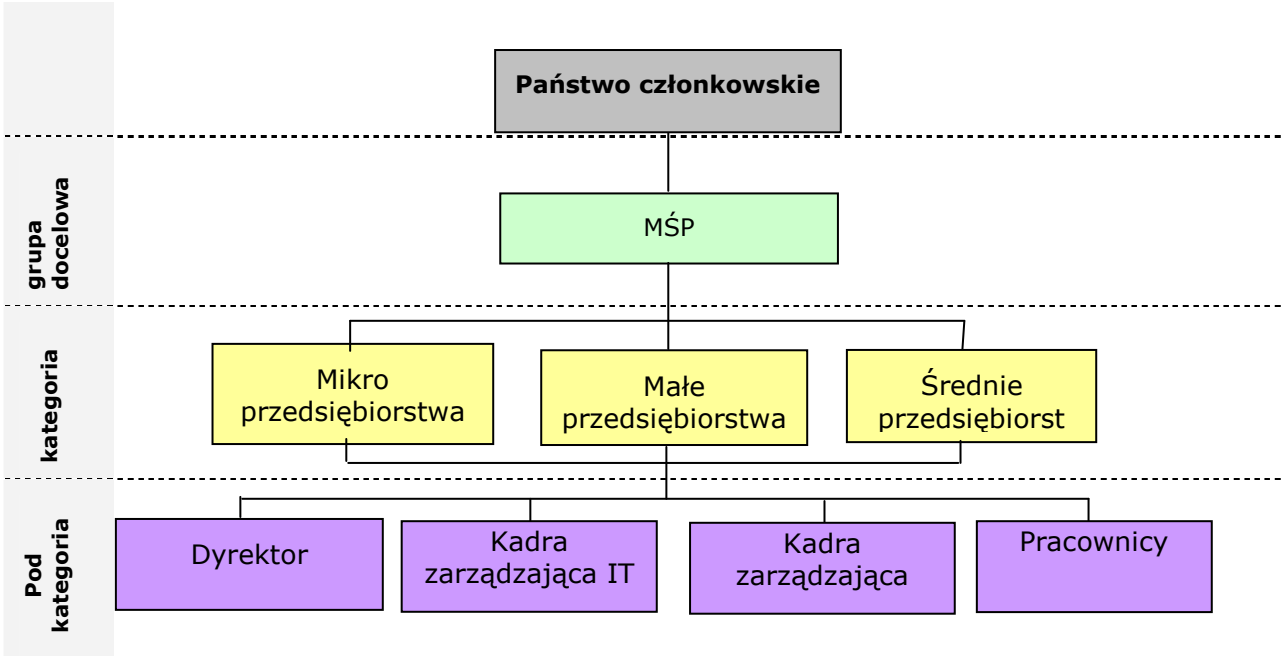
Młodzież – zazwyczaj w wieku 7-15 lat – osoby, które dorosły w otoczeniu ICT, a poziom ich wiedzy podyktowany jest w znacznym stopniu stopniem rozwoju infrastruktury w każdym z państw członkowskich. Obywatele ci są godni zaufania ze względu na ich młody wiek, mają ogromny potencjał przyswajania wiedzy i często eksperymentują z technologiami.

Dorośli – obywatele urodzeni po latach 50-tych XX w., powyżej 16 roku życia – grupa, która częściowo dorastała w otoczeniu technologii ICT. Zakres umiejętności i znajomości ICT wśród tych użytkowników jest prawdopodobnie najbardziej zróżnicowany w porównaniu z innymi grupami, jako że sięga od całkowitej niewiedzy do ogromnego zasobu umiejętności. Obywatele ci mogą mieć lub nie mieć dzieci i pracować w różnorakich zawodach.

Starsi użytkownicy – obywatele urodzeni w latach 50-tych XX w lub wcześniej, którzy nie dorastali w otoczeniu ICT. Ich poziom umiejętności jest niski lub żaden i chociaż zazwyczaj nie orientują się w zagadnieniach technicznych, dość swobodnie korzystają z usług (na przykład usług elektronicznych z telefonów komórkowych). Jako że nie

dorastali w otoczeniu ICT, mogą mieć większe wątpliwości albo wręcz być nieufni wobec nowych technologii.

MŚP: pracodawcy i pracownicy z mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw (firm). Za średnie przedsiębiorstwa Komisja Europejska uznaje firmy zatrudniające do 250 pracowników, za małe przedsiębiorstwa – do 50 pracowników, zaś za mikroprzedsiębiorstwa – do 10 pracowników[1]. Klasyfikacja rodzajów przedsiębiorstw w zależności od wielkości może być różna w poszczególnych państwach członkowskich. Ta grupa docelowa ma ogromne znaczenie, jako że stanowi 99% przedsiębiorstw w UE i zapewnia 65 mln miejsc pracy. Tę grupę użytkowników można podzielić na trzy



Mikroprzedsiębiorstwa – przedsiębiorstwa zatrudniające do 10 osób, których roczny obrót i/lub roczny bilans nie przekracza 2 mln euro. Ta grupa obywateli zazwyczaj nie posiada własnych specjalistów ds. IT czy bezpieczeństwa. W konkretnych państwach członkowskich wartości liczbowe mogą się różnić – na przykład w Wielkiej Brytanii mikroprzedsiębiorstwo składa się zazwyczaj z najwyżej 5 osób.

Małe przedsiębiorstwa – przedsiębiorstwa zatrudniające do 50 osób, których roczny obrót i/lub roczny bilans nie przekracza 10 mln euro. Państwa członkowskie stosują różne definicje małych przedsiębiorstw czy firm. Małe przedsiębiorstwo może mieć własnego specjalistę ds. IT, ale raczej nie ma specjalisty ds. bezpieczeństwa.

Średnie przedsiębiorstwa – przedsiębiorstwa zatrudniające mniej do 250 osób, których roczny obrót nie przekracza 50 mln euro i/lub roczny bilans nie przekracza 43 mln euro. Państwa członkowskie stosują różne definicje średnich przedsiębiorstw czy

[1] *Rekomendacja 2003/361/WE*, Dz.U. L 124 z dn. 20.05.2003, str. 36. Więcej informacji na temat definicji MŚP można znaleźć pod adresem: http://europa.eu.int/comm/enterprise/enterprise_policy/sme_definition/index_en.htm

firm. Średnie przedsiębiorstwa mają zazwyczaj własnego specjalistę ds. IT i mogą mieć pracownika, który posiada wiedzę na temat bezpieczeństwa.

W każdej z trzech kategorii grupy docelowej można wyróżnić cztery podkategorie użytkowników:

Dyrektor / Właściciel – osoba podejmująca kluczowe decyzje w zakresie inwestowania w bezpieczeństwo.

Kadra zarządzająca IT – grupa pracowników technicznych, którzy nie muszą być specjalistami w zakresie bezpieczeństwa, ale muszą rozumieć i wdrażać protokoły bezpieczeństwa informacji.

Kadra zarządzająca – pracownicy często niezorientowani w kwestiach technicznych, którzy jednakże muszą być tak wyszkoleni, by rozumieli wagę bezpieczeństwa informacji. Umożliwi im to wdrożenie właściwych strategii bezpieczeństwa i kontroli w obszarach ich działań.

Pracownicy (szeregowi) – największa liczba użytkowników w grupie docelowej i prawdopodobnie najistotniejsza, jako że, jak sugerują badania, większość naruszeń bezpieczeństwa informacji wywołana jest błędem popełnionych przez człowieka.

Dla celów niniejszego poradnika mikroprzedsiębiorstwa oraz małe i średnie przedsiębiorstwa występują jako jedna całość (MŚP), jako że te trzy kategorie traktowane są często w państwach członkowskich jako jedna. We wszelkich inicjatywach podnoszących świadomość bezpieczeństwa zastosować można różne metody określania profilu docelowych grup obywateli. Na przykład kampania może być skierowana do użytkowników dobranych pod względem grupy wiekowej, warunków społeczno-demograficznych, lokalizacji geograficznej czy wykonywanego zawodu. Kampanię można również skierować do takich grup jak instytucje, organizacje pozarządowe, uniwersytety lub, jak w przypadku tego Poradnika, użytkowników prywatnych czy MŚP.

ENISA

Europejska Agencja Bezpieczeństwa Sieci i Informacji (ENISA) jest agencją Unii Europejskiej stworzoną w celu usprawnienia funkcjonowania unijnego Rynku Wewnętrznego poprzez doradzanie i udzielanie pomocy państwom członkowskim, organom unijnym i środowisku przedsiębiorców w osiąganiu wysokiego i wydajnego poziomu bezpieczeństwa sieci i informacji. ENISA ogrywa również rolę centrum wiedzy dla państw członkowskich i instytucji unijnych, wspomagającego wymianę informacji i współpracę.

Dane kontaktowe

Isabella Santa

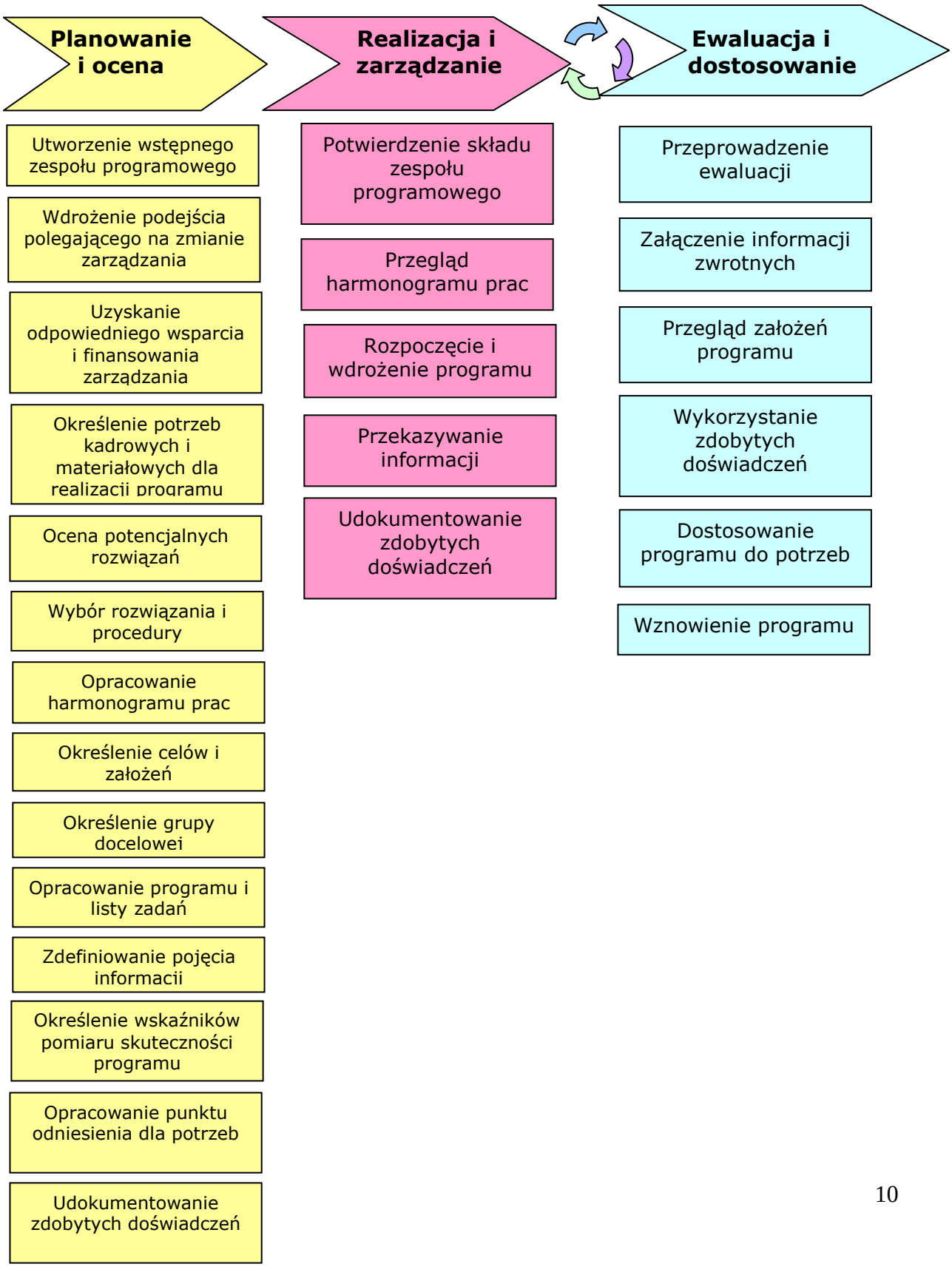
e-mail: awareness@enisa.europa.eu Internet http://www.enisa.europa.eu

Ogólna strategia realizowania inicjatyw i programów edukacyjnych

Niniejsza część ilustruje główne procesy konieczne do zaplanowania, zorganizowania i przeprowadzenia inicjatyw mających na celu uwrażliwienie na bezpieczeństwo informacji – planowanie i ocenę, realizację i zarządzanie, ewaluację i dostosowanie. Każdy proces

został zanalizowany w celu określenia działań i relacji zależnych od upływu czasu. Przedstawiony model procesu zawiera podstawę do rozpoczęcia działań związanych z określaniem zakresu i planowaniem, jak również z realizacją i oceną każdego programu, a także działań mających na celu zapewnienie spójnego i szerokiego zrozumienia głównych procesów i działań.

Przedstawiono tu również szablony i narzędzia mające pomóc użytkownikom lepiej zrozumieć sposoby wdrażania strategii realizowania inicjatyw i programów edukacyjnych.



Etap I
Planowanie i Ocena

Utworzenie wstępnego zespołu programowego

Aby rozpocząć proces planowania programu poszerzania wiedzy, należy utworzyć zespół. Jego głównym celem jest planowanie i organizowanie inicjatywy poprzez realizację zadań przewidzianych w pierwszym etapie.

Wdrożenie podejścia polegającego na zmianie zarządzania

Bardzo istotne jest wdrożenie w inicjatywie poszerzającej wiedzę podejścia polegającego na zmianie zarządzania, ponieważ pomaga to zniwelować różnicę między określoną kwestią, a ludzką reakcją na konieczność zmiany, nawet w przypadku zmian kulturowych.

Wykorzystanie głównych zasad zmiany zarządzania (np. kierowane informacje, uczestnictwo, szkolenie i ewaluacja) pomaga w wypełnieniu założeń inicjatywy dotyczącej poszerzania wiedzy; stanowią one także stabilną podstawę dla przyszłych lub uzupełniających programów.

Zmianami należy zarządzać całościowo, co ma na celu zagwarantowanie połączenia wysiłków, a także prawdziwe i trwałe korzyści wywołane zmianą. Aby wesprzeć programy poszerzania wiedzy, ważne jest ustalenie zmian w kwestii następujących zasad:

- Rozpoznanie głównych osób zainteresowanych i zaangażowanie ich w podejmowanie decyzji, planowanie, wdrażanie i ewaluację.
- Ustalenie w porozumieniu z głównymi osobami zainteresowanymi wyraźnego celu dla punktów końcowych zmiany.
- Wyraźny podział ról, obowiązków i odpowiedzialności.
- Połączenie i zintegrowanie kluczowych elementów zmiany.
- Zarządzanie ryzykiem i reagowanie na przeszkody we wdrożeniu zmiany.
- Zapewnienie kierownictwa na wszystkich etapach procesu wdrażania zmiany.
- Przekazywanie informacji w sposób otwarty, szczery, jasny i punktualny.
- Zezwolenie na elastyczność podejść w zależności od potrzeb różnych osób zainteresowanych.
- Zasoby, wsparcie i zarządzanie zmianą.
- Wspieranie poprzez szkolenia i rozwój w celu zapewnienia zmian w zachowaniu i kulturze.
- Wyciąganie wniosków z poprzednich i obecnych doświadczeń, tworzenie możliwości dla zmian i świętowania osiągnięć.

Uzyskanie odpowiedniego wsparcia i finansowania zarządzania

Uzyskanie dla programu poszerzania wiedzy odpowiedniego wsparcia i finansowania zarządzania jest chyba jednym z najważniejszych aspektów całej inicjatywy. Istotne jest budowanie między osobami podejmującymi decyzję porozumienia co do tego że program ten jest ważny i wart finansowania. W tym momencie istotna jest kwestia pojęcia zarządzania osobami zainteresowanymi. Jeżeli główne osoby zainteresowane nie pojmują konieczności wdrożenia programów poszerzania wiedzy informacji i nie wspierają założeń i celów, inicjatywa nie posunie się do przodu.

Ważne jest zwiększenie wiedzy osób zainteresowanych odnośnie do wartości i kwestii, które należy ująć, a także zaangażowanie wszystkich osób w czasie trwania programu. Program nie powiedzie się, jeżeli nie otrzyma potrzebnego wsparcia ze strony osób zapewniających środki i osób, które będą korzystały z jego wyników. Dlatego też bardzo ważne jest utworzenie koalicji w zakresie interesów i wspierania programu. W żadnym projekcie, programie lub inicjatywie nie należy lekceważyć znaczenia zarządzania osobami zainteresowanymi.

W zależności od organizacji czy instytucji może istnieć (lub nie) konieczność solidnego zabezpieczenia finansowego inwestycji. Jednakże więcej członków ścisłego kierownictwa przekonuje się o korzyściach płynących z programu poszerzania wiedzy, kiedy widzą wyniki czarno na białym.

Szersza i wyraźniej zdefiniowana współpraca lub partnerstwo, na przykład w ramach inicjatyw prywatno-publicznych lub między państwami członkowskimi, może powodować maksymalne zwiększenie potencjalnego zasięgu każdej kampanii. Partnerstwo publiczno-prywatne może być bardzo skuteczną metodą realizowania kampanii, szczególnie jeśli każda organizacja może wykorzystać swoją siłę i zasoby. Przy opracowywaniu wspólnego programu ważne jest posiadanie kodeksów postępowania (zakresu działań) i wytycznych dotyczących projektów. Proces organizowania publiczno-prywatnego partnerstwa powinien obejmować utworzenie grupy nadzorującej, zespołu zarządzania projektem, grupy roboczej (i grupy medialnej) i zespołów ds. podprojektów.

Analiza kosztów i korzyści

Aby wdrożyć skuteczny program poszerzania wiedzy, konieczne jest złożenie formalnego wniosku o fundusze potrzebne na wsparcie inicjatywy. Główne wydatki będzie ponosił zespół ds. programu poszerzania wiedzy w zakresie bezpieczeństwa informacji. Jeśli organizacja posiada już personel z odpowiednim doświadczeniem, osoby te będą potrzebne, aby wesprzeć inicjatywę. W przeciwnym razie do wydatków trzeba będzie doliczyć pensję kierownika i powiązane koszty, a także koszty związane z rozwojem, produkcją i dostarczaniem materiałów edukacyjnych. Wydatki obejmują ponadto wszelkie koszty dodatkowej obsady etatów, wynikające z oddelegowania części pracowników do zespołu ds. programu poszerzania wiedzy, a także opłaty związane z zakupem materiałów edukacyjnych poszerzających wiedzę, odbyciem szkoleń poza organizacją itp. Typowe części składowe kosztu można podsumować następująco:

1. Pracujący na pełnym lub niepełnym etacie kierownik programu bezpieczeństwa informacji i zastępcy (pensje i dodatki plus potencjalne koszty rekrutacji).
2. Materiały edukacyjne (umowy na dostarczanie usług przez specjalistów z firm Gartner i IsecT itp.), jeśli materiały takie nie zostały uprzednio nabyte.
3. Materiały promocyjne (przedmioty związane z danym tematem, na przykład wygaszacze ekranu, długopisy, plakaty, podkładki pod mysz, quizy z nagrodami itp.).
4. Drukowanie (w przypadku materiałów, które nie są rozsyłane elektronicznie).

Suma kosztów pozycji 1-4 stanowi wysokość budżetu potrzebnego do realizacji programu.

Ustalenie korzyści wynikających z programu

W celu uzyskania odpowiedniego wsparcia i finansowania zarządzania bardzo istotne jest ustalenie korzyści wynikających z programu.

IsecT Ltd., firma konsultingowa w zakresie technik informacyjnych, specjalizująca się w bezpieczeństwie informacji, twierdzi, że: „Bezpieczeństwo informacji jest trochę jak hamulce przy rowerze: owszem, spowalniają jazdę, ale też sprawiają, że można bezpiecznie jechać z większą prędkością." Innymi słowy, bezpieczeństwo informacji stanowi podstawę działań w dzisiejszym coraz bardziej połączonym i technologicznie złożonym świecie. Program poszerzania wiedzy bezpieczeństwa informacji:

1. Stanowi główny punkt i siłę napędową dla wielu działań poszerzających wiedzę, szkoleniowych i edukacyjnych związanych z bezpieczeństwem informacji. Niektóre z nich mogą już istnieć w danej organizacji, ale może potrzebna jest ich lepsza koordynacja i zwiększenie skuteczności.
2. Przekazuje ważne i zalecane wytyczne lub praktyki potrzebne do zabezpieczenia zasobów informacji.
3. Przekazuje odpowiednim osobom zarówno ogólne, jak i konkretne informacje na temat zagrożeń dla bezpieczeństwa informacji i kontroli tego bezpieczeństwa.
4. Uwrażliwia poszczególne osoby na ich obowiązki w zakresie bezpieczeństwa informacji.
5. Motywuje poszczególne osoby do stosowania zalecanych wytycznych lub praktyk.
6. Tworzy silniejszą kulturę bezpieczeństwa, charakteryzującą się głębokim zrozumieniem i zaangażowaniem w bezpieczeństwo informacji.
7. Pomaga zwiększać spójność i skuteczność istniejących mechanizmów kontrolujących bezpieczeństwo informacji i potencjalnie stymuluje wdrożenie opłacalnych mechanizmów kontrolnych.
8. Pomaga zmniejszyć liczbę i rozmiar naruszeń bezpieczeństwa informacji, redukując w ten sposób koszty bezpośrednio (np. dane uszkodzone przez wirusy) i pośrednio (np. mniejsza potrzeba badania i rozwiązywania problemu naruszeń). Są to główne finansowe korzyści płynące z programu.

Określenie potrzeb kadrowych i materiałowych dla realizacji programu

Na tym etapie procesu konieczne jest ustalenie potrzeb kadrowych i materiałowych. Logicznym pierwszym posunięciem jest rozejrzenie się za odpowiednimi zasobami w organizacji. Personel działów technik informacyjnych, komunikacji, szkolenia i rozwoju prawdopodobnie posiada doświadczenie i przygotowanie najbardziej odpowiednie dla programu poszerzania wiedzy.

Porady i doświadczenie kolegów i/lub państw członkowskich, stosujących programy poszerzania wiedzy, szkoleniowe i edukacyjne, mogą okazać się bardzo cenne pod względem materiałów i doświadczenia. Ponadto konsultowanie się z nimi służy celom zarządzania osobami zainteresowanymi, ponieważ może pomóc w uzyskaniu ich wsparcia dla wprowadzania programu w przyszłości. Nie angażowanie osób i specjalistów z innych krajów może nastawić ich przeciwko programowi.

W Internecie znajduje się szeroki wybór informacji dostępnych zarówno bezpłatnie, jak i za opłatą. Bardzo pomocne będzie szybkie przeszukanie zasobów związanych z takimi pojęciami jak „poszerzanie wiedzy o bezpieczeństwie" lub „poszerzanie wiedzy o bezpieczeństwie informacji". Istnieje wiele bezpłatnych forów dotyczących konkretnie poszerzania wiedzy o bezpieczeństwie. Zapisanie się do któregoś z nich może być użyteczne, ponieważ członkowie uzyskują dostęp do zasobów archiwalnych.

Łatwo jest zgromadzić dużą ilość informacji na temat produktów i usług, ważne jest jednak, aby zbierać te informacje w sposób zorganizowany i systematyczny, co ułatwi przeprowadzenie pozostałych działań.

Po zgromadzeniu informacji należy przeprowadzić dokładną analizę wewnętrznych i zewnętrznych zasobów. Trzeba położyć nacisk na ustalenie elementów, które mogą być przydatne dla celów programu i odpowiadają jego potrzebom. Typową reakcją jest odrzucenie informacji, które wydają się być nieodpowiednie, należy jednak postępować z rozwagą. Łatwo jest przeoczyć przydatne zasoby, które nie zostały w pełni opisane, lub, w przypadku usług handlowych, są nieodpowiednio promowane.

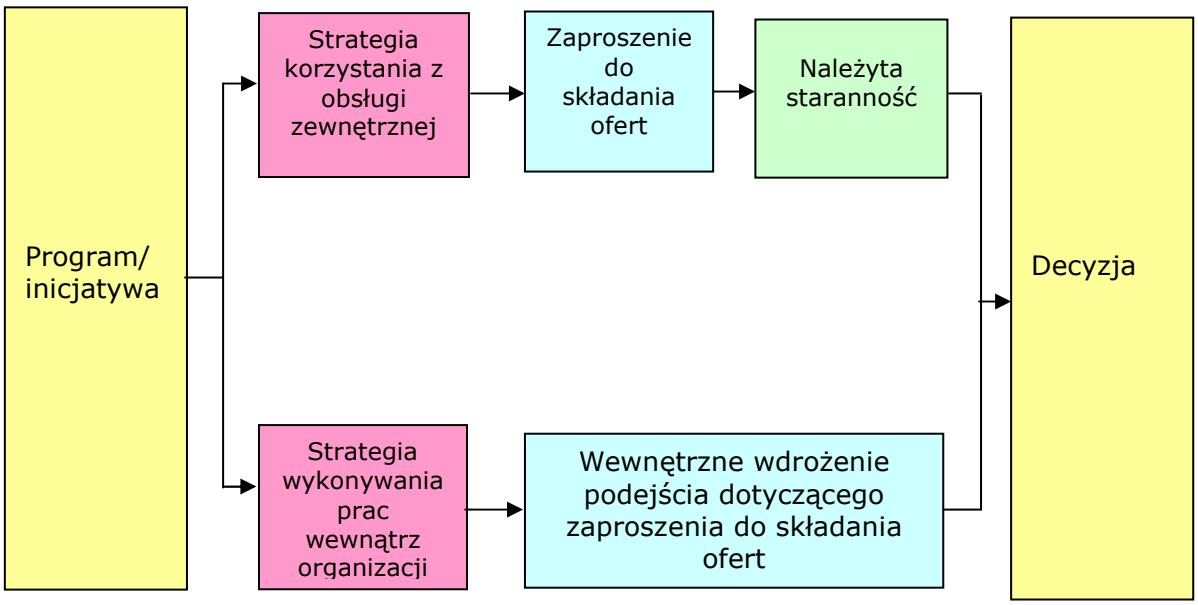
Ostatnia część tego etapu polega na sporządzeniu krótkiej listy potencjalnych rozwiązań. Ich ocena będzie elementem kolejnego kroku.

Ocena potencjalnych rozwiązań

Podczas oceniania potencjalnych rozwiązań najważniejsze jest czy dany program poszerzania wiedzy będzie wykonywany wewnątrz organizacji, czy zostanie zlecony na zewnątrz. Obecnie coraz częściej korzysta się ze zlecania wykonania usług na zewnątrz. Organizacje i instytucje lepiej rozpoznają obszary działalności w których górują i obszary, którymi skutecznie mogą się zająć partnerzy zewnętrzni. Niesie to ze sobą konieczność podjęcia decyzji, czy skorzystać z obsługi zewnętrznej, ustalenia co można zlecić na zewnątrz, określenia charakteru tej relacji i dokonania wyboru partnerów, którzy nie będą stanowili zagrożenia dla powodzenia programów i inicjatyw w przyszłości.

Proces przedstawiony poniżej obrazuje najlepsze praktyki dotyczące podejmowania decyzji w zakresie wykonywania prac wewnątrz organizacji lub korzystania z obsługi zewnętrznej. Zalecane jest stosowanie tego samego podejścia dotyczącego zaproszenia do składania ofert, nawet jeśli praca zostanie wykonana w organizacji, ponieważ jest ono rygorystyczne i pomoże zespołowi w odpowiednim zorganizowaniu wymagań.

Proces podejmowania decyzji o wykonaniu prac wewnątrz lub korzystaniu z obsługi zewnętrznej



Kompletny proces ewaluacji i oceny oparty jest na tradycyjnym postępowaniu przetargowym:

1. Przygotowanie formalnego zaproszenia do składania ofert, zawierającego dokładne wymagania, określone na podstawie dwóch pierwszych kroków w tym procesie. Konieczne jest ustalenie składu zespołu do spraw programu, określenie pożądanego doświadczenia i cech, a także ról, obowiązków i struktury sprawozdawczości. Należy

ustalić procedury i strategie dotyczące programu i nadać im formalny charakter. Dotyczy to także podejścia do cotygodniowych sprawozdań ze stanu działań, sprawozdawczości finansowej i zarządzania publikacjami.
2. Wysłanie zaproszenia do składania ofert do podmiotów, które mogą stanąć do przetargu, wraz z określeniem terminu udzielenia odpowiedzi.
3. Opracowanie odpowiedzi otrzymanych od stających do przetargu i udzielenie im odpowiedzi z zachowaniem terminów bez ujawniania tożsamości pytającego.
4. Po upłynięciu terminu należy odrzucać dalsze propozycje i rozpocząć systematyczną ewaluacje i ocenę ofert za pomocą sporządzonej uprzednio listy kontrolnej.
5. Należy skupić się na najważniejszych wymaganiach; może to prowadzić do natychmiastowego wykluczenia niektórych stających do przetargu, jeżeli nie spełniają oni tych warunków.
6. Należy przejrzeć dodatkowe oferty złożone przez stających do przetargu, ponieważ mogą one zawierać pożyteczne i cenne pomysły, które zostały poprzednio przeoczone. Mogą one także pomóc w podjęciu ostatecznej decyzji w przypadku gdy ocena kilku ofert jest podobna
7. Należy zwrócić uwagę na jakość ofert i załączone do nich przykładowe systemy poszerzania wiedzy lub materiały, ponieważ są to istotne wskaźniki profesjonalizmu i jakości stających do przetargu.
8. Należy obliczyć wyniki stających do przetargu (suma wyników dla każdego kryterium pomnożonych przez wskaźnik przypisany do danego kryterium, a następnie podzielona przez maksymalny możliwy wynik i pomnożona przez 100%.)
9. Jeżeli podjęto decyzję, aby zlecić wykonanie programu (lub jego części) na zewnątrz, w procesie przetargu należy zapewnić udział specjalistów ds. zamówień, ponieważ są oni w stanie zagwarantować, że proces będzie sprawiedliwy.
10. Jeżeli praca zostanie wykonana wewnątrz organizacji, podejmowanie decyzji dotyczących programu na forum komisji może przyczynić się do zwiększenia integracji i przejrzystości.

Podczas formalizowania wymagań, co przedstawiono w punkcie 1 powyżej, należy wziąć pod uwagę sposób przeprowadzania ewaluacji skuteczności programu.

Zaproszenie do składania ofert powinno zawierać dokładne wymagania. Przykładowe zaproszenie do składania ofert znajduje się w Załączniku I. Ponadto bardzo ważne na tym etapie jest ustalenie i sformalizowanie procedur i strategii, w tym cotygodniowej sprawozdawczości itp. Szablon cotygodniowego sprawozdania ze stanu realizacji programu dostępny jest w Załączniku II.

Wybór rozwiązania i procedury

Końcowy wynik ewaluacji mógł nie wyłonić zwycięzcy przetargu, a spowodować podjęcie decyzji o pozostawieniu niektórych części programu wewnątrz organizacji i zleceniu wykonania innych części jednemu lub wielu zewnętrznym wykonawcom. Część etapu selekcji wiąże się z negocjacjami; może też wymagać dalszego sprecyzowania budżetu, cen i warunków, a także rezultatu prac i ich ram czasowych.

W końcu dochodzi do podjęcia decyzji, wystawione zostaje zlecenie zakupu i podpisana umowa.

Opracowanie harmonogramu prac

Po dokonaniu wyboru rozwiązania i wyznaczeniu zespołu zalecane jest opracowanie harmonogramu prac. Na obecnym etapie harmonogram prac będzie zawierał jedynie

główne działania, do których zostaną określone potrzebne zasoby, ramy czasowe i etapy realizacji prac. Po opracowaniu programu harmonogram prac zostanie przeanalizowany.

Istotne jest przygotowanie harmonogramu prac określającego działania, zasoby, ramy czasowe i ważne etapy realizacji prac. Aby efektywnie zarządzać pracami zalecane jest korzystanie z odpowiedniego narzędzia. Przykładowy harmonogram prac znajduje się w Załączniku III.

Określenie celów i założeń

Bardzo ważne jest, aby przygotowania do każdego programu poszerzania wiedzy rozpoczynać od ustalenia, co chce się osiągnąć. Należy zauważyć, że jeśli nie ustali się wyraźnych założeń, próba zaplanowania i zorganizowania programu może powodować problemy, a ewaluacja programu będzie po prostu niemożliwa. Poniżej zamieszczono serię pytań pomocnych w ustaleniu celów i założeń programu.

Uwaga na temat różnicy między celami a założeniami:
Aby uniknąć mylenia tych dwóch terminów, należy pamiętać, że cele to pojęcie szerokie, natomiast założenia - wąskie. Cele to ogólne zamiary; założenia są precyzyjne. Cele są niematerialne; założenia – namacalne. Cele są abstrakcyjne; założenia – konkretne. Cele nie mogą być potwierdzone jako takie, natomiast założenia mogą.
Mówi się, że: "Cel jest miejscem, które chcemy osiągnąć. Założenia to kroki potrzebne by tam dotrzeć."

Aby ustalić, jaki rezultat próbuje się osiągnąć poprzez inicjatywę dotyczącą poszerzania wiedzy, należy dokładnie rozważyć następujące podstawowe pytania:

1. Czy obecnie w organizacji stosowany jest jakikolwiek program dotyczący bezpieczeństwa informacji, czy dla organizacji jest to nowa inicjatywa? Być może żaden program dotyczący bezpieczeństwa informacji nie jest stosowany, ale czy wdrożone są inne programy poszerzania wiedzy, które mogłyby zostać wykorzystane jako sprawdzony wzór lub punkt wyjścia?
2. Czy program będzie skupiony jedynie na poszerzaniu wiedzy czy będzie obejmował także szkolenie i edukację, lub ich połączenie?
3. Jakie konkretne kwestie program ma obejmować? Jakie powiązane tematy mogłyby także zostać uwzględnione?
4. Jak często program będzie kierowany do poszczególnych osób? Czy częstotliwość ta jest odpowiednia, aby uwrażliwić pracowników na zagadnienia związane z bezpieczeństwem informacji?
5. Jaki poziom informacji (i szczegółów) stanowiłby wartościowe źródło informacji dla odbiorców docelowych? Czy powinien być szczegółowy czy wystarczy powierzchowny zarys?
6. Po udzieleniu odpowiedzi na powyższe pytania należy rozważyć dodatkowe kwestie:
7. Czy celem jest „uświadomienie” pracownikom kwestii dotyczących bezpieczeństwa? Czy też celem programu jest zmiana zachowania pracowników, spowodowana zwiększeniem świadomości? Eksperci są zgodni co do tego, że świadomość jest z pewnością wartościowa sama w sobie, ale nie powinna być celem ostatecznym. Plan programu powinien być kontynuowany poza zwykłe zwiększanie świadomości.

8. Czy celem jest ogólne poszerzenie wiedzy na temat bezpieczeństwa, uzyskanie określonych informacji (i ewentualne przeprowadzenie szkoleń) dotyczących konkretnych problemów, czy też połączenie tych dwóch celów? Czy lista konkretnych problemów lub tematów jest stała, czy też będzie rozwijana na przestrzeni nadchodzących miesięcy i lat? Odpowiedzi na te pytania pomogą ustalić czy zaplanowanie jednorazowego programu jest wykonalne, czy też konieczna jest inicjatywa długoterminowa, aby uniknąć przeciążenia i/lub zastraszenia członków grupy docelowej.
9. Z powyższym pytaniem wiąże się kolejna kwestia: czy program poszerzania wiedzy ma być stale stosowany, czy też ma to być jednorazowa kampania lub podobna krótkotrwała akcja, dotycząca określonego zagadnienia? Oba podejścia mają swoje zalety w odpowiednich okolicznościach, jednakże są sytuacje, w których konieczne jest podejście połączone.
10. W jaki sposób inicjatywa będzie zarządzana? Jako zintegrowana część organizacji? Czy zarządzanie inicjatywą zostanie zlecone na zewnątrz? Czy zostanie utworzony zespół zajmujący się projektem? Kto będzie odpowiedzialny za zarządzanie? Jakie kwalifikacje/doświadczenie posiadają członkowie zespołu w zakresie bezpieczeństwa informacji i poszerzania wiedzy/prowadzenia szkoleń/działań edukacyjnych na temat bezpieczeństwa? Jakie będą role i obowiązki poszczególnych osób?

Warto podkreślić, że należy mieć realistyczne podejście co do czasu i wysiłku potrzebnych do zaplanowania i wdrożenia programu!

Określenie grup docelowych

Bardzo istotne jest określenie konkretnych odbiorców, do których skierowana jest inicjatywa dotycząca poszerzania wiedzy. Następujące pytania pomogą określić grupy docelowe:

1. Do kogo ma dotrzeć program poszerzania wiedzy?
2. Czy potrzeby danych grup docelowych są takie same, czy też mają one różne potrzeby w zakresie informacji? Czy istnieją grupy wymagające skrajnie różnych informacji?
3. Czy zasoby wiedzy danych grup docelowych są takie same, czy też mają one różne zasoby wiedzy?
4. Jaka forma przekazywania informacji powinna być używana do dostarczania wiadomości stanowiących część programu poszerzania wiedzy?
5. Jak dane grupy docelowe postrzegają kulturę bezpieczeństwa informacji? Czy kwestia ta jest traktowana poważnie, czy też nie jest uważana za bardzo istotną? Czy członkowie grup docelowych widzieli kiedykolwiek zalecane wytyczne lub praktyki dotyczące bezpieczeństwa informacji? Jeżeli tak, to czy są one utrzymywane i uaktualniane, czy też muszą być opracowane i promowane przez program poszerzania wiedzy?

Bardzo ważne jest określenie konkretnych odbiorców, do których skierowany jest program poszerzania wiedzy. Aby uzyskać te informacje, zalecane jest zastosowanie odpowiedniego narzędzia. Szablon przedstawienia danych o grupie docelowej znajduje się w Załączniku IV.

Opracowanie programu i listy zadań

Oczywiste jest, że dobra organizacja programów poszerzania wiedzy i zarządzanie nimi wymagają dużo wysiłku. Dlatego też konieczne jest skupienie wysiłku na zaprojektowaniu programu, następnie na rozwijaniu planu aby utworzyć program, i w końcu na skutecznym zarządzaniu zapewniającym realizację przewidywanych korzyści.

Jeżeli lista tematów związanych z bezpieczeństwem informacji jest długa, zalecane jest zaplanowanie programu w postaci odrębnych części rozłożonych w czasie. Pozwoli to na skoncentrowanie wysiłków na określonych tematach w sposób zrozumiały dla każdej grupy odbiorców docelowych, a nie powodujący przeciążenia lub nieporozumień. Na przykład w przypadku problemu wirusów konieczne jest, aby każda osoba, która korzysta z komputera podłączonego w jakikolwiek sposób do sieci, posiadała podstawową wiedzę na temat wirusów. Podczas wyjaśniania zagadnienia wirusów można jednocześnie przedstawić takie tematy, jak zarządzanie konfiguracją, dostęp do sieci lub systemów itd.

Jednakże najlepiej nie omawiać powiązanych tematów zbyt szczegółowo. Można poinformować odbiorców docelowych, że zagadnienia te zostaną omówione później. W ten sposób buduje się oczekiwanie na dalszy wysiłek w późniejszym czasie, co stanowi element inicjatywy dotyczącej poszerzania wiedzy na temat kolejnych zagadnień związanych z bezpieczeństwem informacji. Przeprowadzanie dalszych działań jest ważne dla zachowania wiarygodności programu.

Po opracowaniu pełnej listy tematów, które należy uwzględnić w trakcie realizacji programu ważna jest ewaluacja każdego z nich i uporządkowanie według znaczenia. Prostą metodą ewaluacji zagadnień jest przypisanie każdemu z nich wagi, na przykład: 3 = zasadnicze, 2 = ważne i, w końcu, 1 = przydatne. Pomoże to skoncentrować się na najważniejszych tematach i umożliwi sprecyzowanie i dopracowanie wymagań programu poszerzania wiedzy. To z kolei ułatwia opracowanie planu związanego z danym programem.

Zdefiniowanie pojęcia informacji

Informacje są kluczowe dla programu poszerzania wiedzy. Efektywne zarządzanie informacjami ma decydujące znaczenie dla powodzenia programu. Sprawni kierownicy wykorzystują potrzebne zasoby, aby zagwarantować, że osoby zaangażowane w program lub których program dotyczy, otrzymają potrzebne im informacje (tj. wiadomości) we właściwym czasie i w odpowiedni sposób. Dla członków każdej inicjatywy lub programu, bądź też osób zainteresowanych, decydujące znaczenie ma zapewnienie terminowego i odpowiedniego podawania i dystrybucji informacji dotyczących programu. Informacje dotyczące tego zagadnienia i przedstawione poniżej zamieszczono na płycie CD wydanej przez ENISA, Information Package: Raising Awareness in Information Security – Insight and Guidance for Member States2 [Pakiet informacji: poszerzanie wiedzy na temat bezpieczeństwa informacji – analiza i wskazówki dla państw członkowskich].

Skuteczne przekazywanie informacji

Po przeanalizowaniu wielu kampanii przeprowadzonych w kilku państwach członkowskich można wyodrębnić kilka punktów kluczowych, widocznych w przypadku każdego kraju podejmującego inicjatywę poszerzania wiedzy w zakresie bezpieczeństwa informacji.

Poniżej przedstawiono niektóre najistotniejsze zalecenia dotyczące skutecznej kampanii.

[2] *Information Package: Raising Awareness in Information Security – Insight and Guidance for Member States* [Pakiet informacji: poszerzanie wiedzy na teamt bezpieczeństwa informacji – analiza i wskazówki dla państw członkowskich], ENISA, grudzień 2005 r., str. 47 – 58.

Kwestie podstawowe

- Należy dotrzeć do jak najszerszego kręgu odbiorców. W zwiększeniu zasięgu wiadomości przydatne jest uwzględnienie kryteriów mnożnikowych.
- Nie należy wpadać w panikę lub być zbyt negatywnie nastawionym do sytuacji. Jeżeli konieczne jest szczegółowe omówienie zagadnień lub zagrożeń, często łatwiej jest odbiorcom je zrozumieć, kiedy są przedstawione w kontekście rzeczywistych doświadczeń.
- Celem każdej inicjatywy dotyczącej poszerzania wiedzy powinna być pozytywna zmiana zachowania grupy docelowej w związku z bezpieczeństwem.
- Przekazywana wiadomość, używane kanały i nadawca wiadomości muszą mieć istotny wpływ i być wiarygodne, w przeciwnym wypadku grupa docelowa może być mniej skłonna do wysłuchania.
- Grupy docelowe uzyskują informacje z różnych źródeł. Aby skutecznie do tych grup dotrzeć, konieczne jest posłużenie się więcej niż jednym kanałem przekazywania informacji.
- Należy zapewnić elastyczność i możliwość dostosowania inicjatywy, ponieważ czynniki zewnętrzne często mogą zmieniać sytuację.

Wiadomość

- Należy przekazać właściwą zawartość wiadomości odpowiednim odbiorcom i za pomocą najskuteczniejszych kanałów przekazywania wiadomości. Zwiększy to atrakcyjność informacji i przekona odbiorców do wykonania działań, szczególnie jeśli wiadomość odpowiada zainteresowaniom i potrzebom grupy docelowej. Wiadomość może i powinna być dostosowana do wiedzy lub technicznych zdolności grupy docelowej. Należy zgromadzić określone dane, pomocne w projektowaniu skutecznej kampanii.
- Wiadomość powinna być dynamiczna, aktualna dla grupy docelowej i spójna. Często dobre efekty przynoszą przesłania typu „10 najlepszych rad", ze względu na zwięzłość informacji i łatwą czytelność/dostępność.
- Każda wiadomość w swojej najprostszej formie, stanowiąca część inicjatywy dotyczącej poszerzania wiedzy, powinna określać ryzyko i zagrożenia, przed którymi stają użytkownicy, dlaczego są one istotne, co należy zrobić, a czego nie, i wreszcie jak się przed nimi zabezpieczać.
- Wiadomość powinna przyciągać uwagę. Grupa docelowa styka się na rynku z tak dużą ilością informacji, że wiadomość należy dostarczyć w twórczy sposób, aby została ona łatwiej zauważona. Pomocne jest także stosowanie głównych i stałych tematów i haseł.
- Wartość dodana.
- Jeśli jest to możliwe, należy pozwolić grupie docelowej na wyrażenie opinii na temat kampanii, co pomoże ulepszyć ją lub kolejne inicjatywy.
- Planowanie i przeprowadzenie kampanii to połowa wysiłku. Ewaluacja kampanii dotyczącej przekazywania informacji (wobec wskaźników, założeń dotyczących wyników itp.) powinna być przeprowadzana także po to, aby informować o skuteczności kampanii i określić zdobyte doświadczenia pomocne w ulepszeniu przyszłych inicjatyw. Do obserwowania skuteczności można wykorzystać takie wskaźniki jak: liczba odwiedzających na stronie internetowej, liczba pobrań lub zamówień publikacji lub też liczba artykułów prasowych.
- Ewaluację wpływu różnych kampanii na poszerzanie wiedzy grupy docelowej można także przeprowadzić poprzez badania jakościowe (np. grupy dyskusyjne, rozmowy) i/lub ilościowe (np. kwestionariusze, sondaże obejmujące różne zagadnienia). Więcej informacji znajduje się w części dotyczącej ewaluacji programu.

- Przykłady dobrych praktyk i konkretnych inicjatyw dotyczących poszerzania wiedzy mogą dostarczyć organizacje takie jak ENISA i inne państwa o podobnej charakterystyce użytkowników.

Strategia przekazywania informacji może być skonstruowana w sposób uwydatniający kolejne kroki głównego procesu w każdej skutecznej inicjatywie poszerzającej wiedzę.

Główny proces	Opis
Określenie celów i założeń inicjatywy i określenie grupy docelowej	• Należy zadać pytania dotyczące powodów podejmowania kampanii, kluczowych kwestii, którymi trzeba się zająć i dlaczego, a także czy dana organizacja jest w stanie zająć się tymi kwestiami. • Nie należy działać na podstawie przypuszczeń. Jeśli jest to możliwe, należy zgromadzić dane i zastosować takie metody jak grupy dyskusyjne. • Należy ustalić wskaźniki do pomiaru wyników kampanii i do pomocy w opracowywaniu zdobytych doświadczeń.
Nawiązać współpracę, jeśli jest to konieczne	• Należy nawiązać współpracę z inną organizacją, jeżeli nie posiada się możliwości dostępu do planowanych odbiorców, brakuje potrzebnych zasobów lub jeżeli w zakresie informowania o bezpieczeństwie informacji odbiorcy ufają innej organizacji. • Należy upewnić się, że istnieje wspólna wiadomość, a także wspólne poglądy i opinie.
Stworzenie wspólnej wiadomości dla określonej grupy docelowej	• Konieczne jest wyznaczenie określonej grupy, której członkowie mają podobne interesy i priorytety, ponieważ ogół społeczeństwa ma różnorodne interesy, kompetencje i doświadczenia. Ponieważ różni odbiorcy kładą nacisk na różne zagrożenia (co często jest wynikiem osobistych doświadczeń), wiadomość należy kierować do konkretnej grupy. • Należy zadać pytania dotyczące tego co zauważą odbiorcy albo co przyciągnie ich uwagę, dlaczego coś będzie dla nich ważne (dostosowanie do potrzeb i zainteresowań odbiorców) i co zrobią.
Szczegółowy opis wiadomości	• Konieczne jest zrozumienie odbiorców w zakresie poziomu ich wiedzy w danej kwestii, ich potrzeb, zagadnień, którymi są zainteresowani, skąd czerpią informacje i jakie informacje chcieliby otrzymać. • Zawartość rzeczywistej wiadomości musi spowodować trzy rzeczy: przyciągnąć uwagę odbiorców, uwrażliwić ich na zagrożenie i dostarczyć im informacje lub poinformować, gdzie można je znaleźć. • Należy upewnić się, że wiadomość jest jak najbardziej neutralna, na przykład nie powinna ona dyskryminować mniejszości.
Testowanie wiadomości	• Należy rozpocząć kampanię i przeprowadzić ewaluację wyników lub reakcji. Ewaluacja (ilościowa mi jakościowa) może być wykonana za pomocą takich metod jak: grupy dyskusyjne, rozmowy, kwestionariusze lub sondaże obejmujące różne zagadnienia.

Najskuteczniejszym sposobem dostarczenia wiadomości stanowiącej część inicjatywy poszerzającej wiedzę jest wykorzystanie mnożników, które mogą pomóc w przekazaniu wiadomości jak najszerszemu kręgowi odbiorców w grupie docelowej.

Do pomocy w dostarczeniu wiadomości będących częścią inicjatywy można wykorzystać kilku partnerów lub organów wspomagających. Mogą to być:

1. Programy edukacyjne dla osób dorosłych
2. Banki
3. Przedsiębiorstwa
4. Domy kultury
5. Szkoły przygotowawcze
6. Sklepy komputerowe
7. Niezależne agencje
8. Organy przemysłowe (związki, stowarzyszenia)
9. Instytucje
10. Dostawcy usług internetowych
11. Czołowe akademie
12. Biblioteki
13. Lokalne organizacje handlowe
14. Media
15. Organizacje pozarządowe
16. Stowarzyszenia rodziców i nauczycieli
17. Uniwersytety

Kanały komunikacji

Poniższa matryca przedstawia niektóre z głównych dostępnych kanałów pomocnych w podnoszeniu świadomości obywateli w ramach inicjatywy związanej z bezpieczeństwem informacji. W tabeli wymieniono tylko wybrane zalety i wady, a zatem nie należy traktować jej jako wyczerpującej wskazówki.

Kanał	Zalety	Wady
Broszura lub czasopismo	✓ Łatwiej jest sprecyzować treść i format wiadomości. ✓ Umożliwiają grupie docelowej ostrożne przestudiowanie treści. ✓ Można dotrzeć do wybranych odbiorców.	❖ Nie są stałym źródłem informacji, gdyż można je zgubić. ❖ Mogą być atrakcyjne tylko dla wybranej grupy docelowej.
Komiks	✓ Atrakcyjny dla pewnych grup docelowych, takich jak młodzież. ✓ Treść wiadomości może mieć bardziej abstrakcyjny charakter.	❖ Trudno jest umieścić w nim bardziej szczegółowe wiadomości. ❖ Może przemawiać wyłącznie do wybranej grupy docelowej.
Nauka na odległość - Szkolenie z wykorzystaniem komputerów - Szkolenie internetowe	✓ Umożliwia szkolenie obejmujące obszary geograficznie rozproszone. ✓ Treść wiadomości może być bardziej szczegółowa.	❖ Stworzenie programów szkoleniowych może być kosztowne. ❖ Wybór tego kanału zakłada, że osoby odbywające szkolenie posiadają już pewną wiedzę techniczną.
Szkolnictwo - Pakiet edukacyjny - Materiały do nauki	✓ Dobry sposób na dotarcie do dużej liczby dzieci. ✓ Istnieją wcześniej utworzone kanały, którymi można rozprowadzać	❖ Czas spędzany w szkole już teraz ma bardzo dużą wartość, a programy nauczania są przepełnione. ❖ Nauczyciele mogą nie mieć

	materiały.	odpowiedniej wiedzy, aby przekazać wiadomość. ❖ Zaplecze komputerowe może nie pozwalać na realizację pewnych działań, np. ćwiczeń z zakresu instalowania oprogramowania antywirusowego.
E-mail	✓ Stosunkowo tani kanał umożliwiający dotarcie do masowych odbiorców. ✓ Umożliwia grupie docelowej przetrawienie informacji w dogodnym dla niej czasie.	❖ Wiadomość może zostać zignorowana z powodu dużej liczby e-maili i spamu. ❖ Niezbędna jest znajomość adresów e-mailowych.
Wydarzenie - Targi - Posiedzenie - Seminarium - Konferencja	✓ Umożliwia dotarcie do bardzo zróżnicowanych odbiorców na drodze ostrożnego wyboru miejsc i tematyki. ✓ Ma większe szanse na zainteresowanie odbiorców dzięki interaktywnemu charakterowi kanału.	❖ Planowani odbiorcy mogą nie przybyć na miejsce wydarzenia. ❖ Nie jest to kanał proaktywny, w przypadku którego istnieje grupa docelowa, której udziału w wydarzeniu można się spodziewać.
Ulotka informacyjna	✓ Może zawierać dużo informacji. ✓ Opłacalna w produkcji.	❖ Istnieje potrzeba zorganizowania kanałów dystrybucji, poprzez które ulotki docierałyby do właściwych odbiorców. ❖ Nie jest to stałe źródło informacji, gdyż można zgubić materiały.
E-biuletyn	✓ Ma podobne zalety do e-maila.	❖ Nie jest to kanał proaktywny, gdyż zazwyczaj wymaga od użytkowników zarejestrowania się. ❖ Wybór tego kanału zakłada, że osoba odbywająca szkolenie ma już pewną wiedzę techniczną.
Gazeta	✓ Masowy obieg połączony z dogłębną penetracją rynku. W oparciu o koszty przypadające na tysiąc osób, gazety są zazwyczaj niedrogim, opłacalnym środkiem dostarczania wiadomości do szerokiej rzeszy odbiorców. ✓ Reklama w gazecie może	❖ Czynnik nieładu. W obrębie danej gazety istnieje duża konkurencja o uwagę czytelników. Gazety zazwyczaj przepełnione są reklamami różnych rozmiarów i w różnych stylach, promujących wiele produktów i usług. ❖ Gdy zamierza się dotrzeć wyłącznie do określonego

	zawierać tyle szczegółowych informacji, ile potrzeba, a nawet przedstawiać obrazy lub znaki graficzne.	wycinka społeczeństwa, może okazać się, że gazety tracą zbyt dużą część obiegu. ❖ Gazety mają krótki żywot. Często czyta się je w biegu, bez możliwości zagłębienia się w treść.
Telefon	✓ Umożliwia bezpośredni kontakt z grupą docelową. ✓ Ma większe szanse na zainteresowanie odbiorców z powodu interaktywnego charakteru kanału.	❖ Może być stosunkowo drogi. ❖ Potrzebne są numery telefonu grupy docelowej.
Plakat	✓ Może przyciągać uwagę z powodu rozmiaru i formatu. ✓ Informacje mogą być ogólnie dostępne, gdy umieszczone są na murach.	❖ W przypadku obszernego materiału informacyjnego można nie zauważyć wiadomości.
Radio	✓ Największą zaletą radia jest duża częstotliwość (docieranie do tych samych odbiorców wiele razy) za rozsądna cenę. ✓ Muzyczne formatowanie stacji pomaga w określeniu grup interesu i pewnych kategorii demograficznych. Zatem można wybrać konkretny rodzaj odbiorców, do których chce się dotrzeć.	❖ Radio jest wysoce skomercjalizowane. ❖ Nie można pokazać i zademonstrować tematu. ❖ Program radiowy pozbawiony jest stałego charakteru wiadomości drukowanej. ❖ Z powodu formatowania i specjalizacji odbiorców pojedyncza stacja rzadko może zaoferować szeroki zasięg rynkowy.
Wygaszacze ekranu	✓ Umożliwiają umieszczenie informacji na komputerze, dzięki czemu istnieje prawdopodobieństwo, że użytkownicy zobaczą je.	❖ Wymagają opracowania. ❖ Niedoświadczeni użytkownicy mogą nie potrafić zainstalować wygaszasz. ❖ Nie dociera do osób, które nie mają komputera.
SMS	✓ Treść wiadomości można dostarczyć bezpośrednio do grupy docelowej, zapewniając widoczność.	❖ Potrzeba współpracy z dostawcą usług telekomunikacyjnych. ❖ Skuteczny kanał, jeśli chodzi o ostrzeganie grupy docelowej przed niebezpieczeństwami, ale mało skuteczny jeśli chodzi o pogłębianie wiedzy - z

		powodu ograniczonej treści.
Szkolenie	✓ Ma większe szanse na zainteresowanie odbiorców dzięki interaktywnemu charakterowi kanału. ✓ Treść wiadomości może być bardziej szczegółowa i opracowana pod kątem indywidualnego klienta.	❖ Nie jest to kanał proaktywny, w przypadku którego istnieje grupa docelowa, której udziału w wydarzeniu można się spodziewać. ❖ W rzeczywistości nie może dotrzeć do masowych odbiorców z powodu stosowanych środków i logistyki.
TV	✓ Duży wpływ na odbiorców; łącząc obraz, dźwięk i ruch, może przyciągać uwagę i ułatwiać zapamiętywanie. ✓ Telewizja jest najbliższa modelowi bezpośredniej komunikacji spośród wszystkich środków przekazu. ✓ Osobista wiadomość przekazana przez organ władzy może być bardzo przekonywająca. ✓ Można zademonstrować treść wiadomości. ✓ Telewizja umożliwia wybór odbiorców dzięki różnym programom. Umożliwia też elastyczność planowania w różnych programach i o różnych porach dnia oraz zwrócenie uwagi na zasięg lub częstotliwość.	❖ Koszt – wymogi budżetowe są stosunkowo wysokie. ❖ Chociaż jest możliwość wyboru programów, istnieje ryzyko, że najbardziej popularne programy zostaną wysprzedane.
Wideo - DVD - CD	✓ Umożliwia twórczą swobodę przy tworzeniu wiadomości. ✓ Profesjonalizm kanału, o ile jest on właściwie wykorzystany, mógłby wzmocnić przekaz wiadomości.	❖ Może nie dotrzeć do osób nie obeznanych z najnowszą technologią.
Strona internetowa	✓ Może być aktualizowana i dzięki temu odzwierciedlać zmiany. ✓ Może zawierać treści przeznaczone dla zróżnicowanych odbiorców.	❖ Może nie dotrzeć do osób nie obeznanych z najnowszą technologią. ❖ Wybór tego kanału zakłada, że osoba odbywająca szkolenie posiada już pewną wiedzę techniczną.

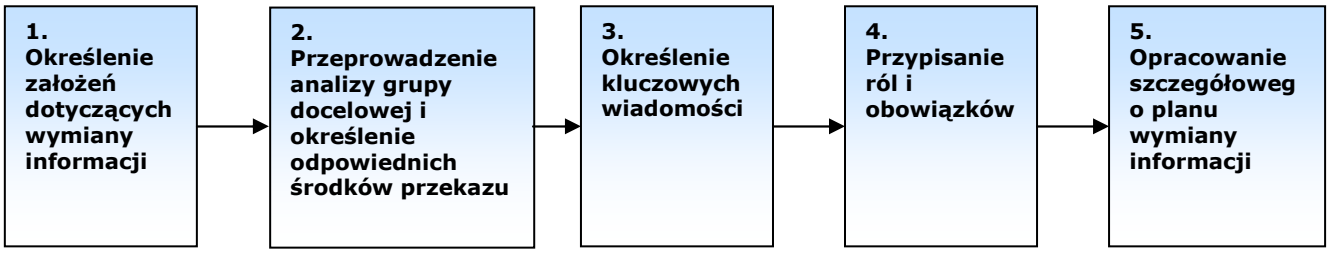
	✓ Zapewnia łatwą łączność z innymi informacjami.	❖ Nie jest to kanał proaktywny i – biorąc pod uwagę bogactwo stron i informacji dostępnych w Internecie – wiadomość może być pominięta.

Wskazówki dotyczące planowania wymiany informacji

Niniejsza część przedstawia proces i podejście, jakie państwa członkowskie mogą zastosować w celu opracowania wyczerpującego Planu Wymiany Informacji. Zaprezentowane szablony i narzędzia przeznaczone są do użycia jako punkty wyjściowe przez zespół odpowiedzialny za podnoszenie świadomości.

Proces

Opracowanie konkretnego planu wymiany informacji jest kluczowym krokiem w kierunku zapewnienia skutecznej zmiany w postępowaniu grupy docelowej. Zalecany jest proces pięcioetapowy, który został przedstawiony w formie diagramu poniżej.



Kluczowe cechy charakterystyczne procesu

- Cele wymiany informacji narzucają wybór działań.
- Analiza grupy docelowej pomaga w uszeregowaniu zainteresowanych grup docelowych pod względem ważności i umożliwia określenie celów i wymogów związanych z wymianą informacji.
- Kluczowe wiadomości muszą być dostosowane do problemów i obaw charakterystycznych dla różnych grup docelowych.
- Plan wymiany informacji obejmuje opis wiadomości, środków przekazu i częstotliwości przekazywania informacji grupom docelowym. Wybór terminu przekazywania konkretnych wiadomości jest tak zaprojektowany, aby wspierać realizację głównych punktów programu podnoszenia świadomości.
- Zasięganie opinii grupy docelowej jest niezbędne, aby utrzymać jakość, spójność i skuteczność przekazywania informacji.

Określenie celów wymiany informacji

Powiadamianie na temat bezpieczeństwa informacji powinno skutecznie angażować, zajmować i informować wszystkie kluczowe grupy docelowe, aby wspierać owocne podnoszenie świadomości. Wymiana informacji może mieć na celu:

- promowanie wizji bezpieczeństwa sieci i informacji oraz płynących z niego korzyści dla całego społeczeństwa;

- aktywne zaangażowanie wszystkich zidentyfikowanych grup docelowych;
- umożliwienie zainteresowanym grupom docelowym zrozumienia zagadnień dotyczących bezpieczeństwa informacji oraz tego, z czym te zagadnienia będą się dla nich wiązały;
- umożliwienie członkom grup docelowych zadawania pytań i poruszania kwestii budzących obawy;
- gromadzenie energii i nabieranie rozmachu, aby wspierać tworzenie nowego środowiska edukacyjnego.

Analiza grupy docelowej i określenie kanału

Określenie różnych grup docelowych i odpowiednie zaangażowanie ich ma decydujące znaczenie dla osiągnięcia sukcesu.

Społeczeństwo stanowi zróżnicowaną grupę jednostek o rozbieżnych zainteresowaniach, poziomach kompetencji i priorytetach. Dlatego też trudno jest znaleźć zagadnienia i wiadomości, które będą odpowiednie dla każdego. A zatem zazwyczaj konieczne jest określenie konkretnych grup docelowych o podobnych zainteresowaniach i priorytetach. ENISA określiła pewną liczbę grup docelowych dla państw członkowskich w ramach inicjatywy podnoszenia świadomości. Gdy tylko zespół odpowiedzialny za podnoszenie świadomości określi różne grupy docelowe, należy przeprowadzić badania, aby:

- poznać poziom znajomości kwestii związanych z bezpieczeństwem informacji, jaki reprezentuje każda grupa.
- dowiedzieć się, jaki poziom znajomości odpowiednich rozwiązań reprezentuje każda grupa.
- poznać cele, dla których każda z grup korzysta z ICT.
- poznać kluczowe obawy każdej z grup.
- dowiedzieć się, gdzie obecnie każda grupa uzyskuje informacje.

Przykład wzorcowych kroków, jakie można podjąć, przeprowadzając analizę grupy docelowej, jest przedstawiony poniżej.

Wzorcowe kroki podejmowane w ramach analizy grupy docelowej

Określenie grup docelowych	Grupy docelowe to te, na które mają wpływ lub które wpływają na poziom świadomości zagadnień związanych z bezpieczeństwem informacji.
Zrozumienie sytuacji	Grupa docelowa może obawiać się wpływu na jej organizację, utraty kontroli, itd.
Ocena poziomu świadomości	Wystawienie ocen H (wysoka), M (średnia), L (niska) odzwierciedlających poziom świadomości zagadnień związanych z bezpieczeństwem informacji i znajomości rozwiązań reprezentowany przez każda grupe docelowa.
Określenie pożądanych działań	Określenie działań, jakie każda grupa docelowa powinna podjąć, aby zająć się kluczowymi problemami.

Korzyści wynikające z przeprowadzenia wnikliwej analizy grupy docelowej

- Potrzeba informacji i działań będzie lepiej rozumiana.
- Będzie możliwe dogłębne zrozumienie wpływu problemów związanych z bezpieczeństwem informacji i działań niezbędnych do rozwiązania tych problemów.
- Można opracować plan wymiany informacji, aby upewnić się, że członkowie grupy docelowej otrzymują właściwe informacje we właściwym czasie we właściwy sposób.
- Zespół odpowiedzialny za podnoszenie świadomości będzie znał poziom świadomości każdej grupy docelowej i będzie mógł nim zarządzać.

Gdy tylko analiza grupy docelowej jest gotowa, można określić odpowiednie cele wymiany informacji i właściwe kanały. Poniższa matryca ilustruje sposób realizacji tych zadań.

Cele wymiany informacji*

Grupa docelowa	Podnoszenie świadomości	Umożliwienie zrozumienia	Poszerzenie wiedzy	Zaangażowanie w rozwiązania
Grupa 1		✓	✓	✓
Grupa 2	✓	✓	✓	✓
Grupa 3	✓	✓		
Grupa 4	✓	✓	✓	✓
Grupa 5	✓	✓		
Grupa 6	✓	✓		
Grupa 7	✓			
*Wyłącznie wzorcowe cele i rodzaje kanałów	Strona internetowa E-mail Biuletyn Publikacje	Prezentacje Posiedzenia Konferencje	Warsztaty Posiedzenia	Warsztaty Seminaria Notatki

Odpowiedni kanał*

Określenie kluczowych informacji

Informacja i grupa docelowa są ściśle powiązane; wzajemnie na siebie oddziałują. Informacja może skupiać się na radzeniu sobie z określonym rodzajem ryzyka, na przykład na zagrożeniach dla prywatności, lub na konkretnej technologii, na przykład na telefonach komórkowych. Odbiorcy z małym doświadczeniem w dziedzinie bezpieczeństwa informacji prędzej zidentyfikują i zrozumieją wiadomość, która odnosi się do tego, jak korzystają lub współpracują z ICT. Na przykład: sformułowanie „Korzystając ze swojego telefonu komórkowego powinieneś wziąć pod uwagę następujące kwestie…" jest bardziej skuteczne niż ogólna informacja o ochronie prywatności. Wiadomości mogą również dotyczyć wielorakich grup docelowych, co zilustrowano poniżej.

	Grupa docelowa 1	Grupa docelowa 2	Grupa docelowa 3	Grupa docelowa 4	Grupa docelowa 5	Grupa docelowa 6	
Znaczenie kopii zapasowych	✓	✓	✓	✓	✓	✓	✓
Ochrona danych osobowych w czasie korzystania z Internetu (zakupy, korzystanie z usług bankowych, głosowanie)	✓	✓	✓	✓	✓	✓	✓
Zagwarantowanie, że dzieci czerpią korzyści z Internetu	✓			✓	✓		
Jak nie być wykrywalnym dla osób dokonujących próby włamania się przez Bluetooth	✓	✓		✓	✓		
…	✓	✓				✓	✓
…	✓	✓		✓	✓		
…	✓	✓		✓	✓		
…	✓	✓	✓	✓	✓		
…	✓	✓	✓	✓	✓	✓	✓
…	✓	✓		✓	✓		

Tylko przykłady

Przypisanie ról i obowiązków

Każdy członek zespołu odpowiedzialnego za podnoszenie świadomości (jak również partnerzy) odegrają rolę w wymianie informacji, pełniąc funkcję agentów wymiany informacji. Dlatego należy przydzielić konkretne role i obowiązki członkom zespołu, aby zagwarantować dobrą koordynację wydarzeń, które prawdopodobnie będą miały miejsce w różnych departamentach i organizacjach. Poniżej zilustrowano podział ról.

Grupa	Role i obowiązki
Członkowska Grupa Zainteresowana	• Zatwierdzenie Planu Wymiany Informacji • Zagwarantowanie odpowiedniego rozpowszechnienia informacji • Zagwarantowanie odpowiedniego sponsoringu na wszystkich poziomach • Prowadzenie organizacji odpowiedzialnej za rozpowszechnianie informacji
Sponsor	• Wspieranie strategii wymiany informacji oraz odpowiednie sponsorowanie projektów przez firmy • Aktywne wspieranie Forum Podnoszenia Świadomości w celu zagwarantowania zgodności ze sponsoringiem wykonawczym
Zespół odpowiedzialny za podnoszenie świadomości	• Kierownictwo i opracowanie strategii i planu wymiany informacji • Koordynowanie treści zebranych od odpowiednich ekspertów w ramach programu • Opracowanie i w niektórych przypadkach przekazywanie treści informacji w oparciu o działaniami zawarte w planie wymiany informacji • Zagwarantowanie realizacji wszystkich wymaganych działań związanych z wymianą informacji zgodnie z planem

Opracowanie szczegółowego planu wymiany informacji

Gdy tylko założenia wymiany informacji, kanały, kluczowe wiadomości, role i obowiązki zostaną szczegółowo określone, zespół odpowiedzialny za podnoszenie świadomości będzie miał odpowiednie warunki do przygotowania szczegółowego planu wymiany informacji. Opracowanie i realizacja docelowej strategii wymiany informacji i planów przygotowanych pod kątem konkretnych odbiorców umożliwi rozpoznanie i podniesienie poziomu świadomości wśród określonych grup docelowych. Plan wymiany informacji pomaga w zaangażowaniu grup docelowych w sposób zorganizowany i zmniejsza prawdopodobieństwo przeoczenia kluczowych osób zainteresowanych. Plany wymiany informacji zazwyczaj powstają co rok (aktualizacje mają miejsce zgodnie z wymogami) i umożliwiają koordynację wszystkich wydarzeń organizowanych dla wszystkich grup docelowych. Dzięki planowi zmniejsza się również prawdopodobieństwo dwukrotnie wykonanej pracy na skutek nieskoordynowanego planowania. Przykład ilustrujący fragment planu wymiany informacji jest pokazany poniżej.

Docelowi odbiorcy	Potrzeby odbiorców	Wiadomość	Kanał	Właściciel	Założenia	Wybór terminu/ częstotliwość	Narzędzie do gromadzenia informacji zwrotnych
Kto będzie odbiorcą wiadomości	Potrzeby odbiorców dotyczące wymiany informacji	Treść informacji	Postać, w jakiej wiadomość zostanie przesłana	Kto jest odpowiedzialny za realizację tej wymiany informacji	Co zamierzamy osiągnąć dzięki tej wymianie informacji	wymiana informacji na temat wydarzenia powinna mieć miejsce	Przy pomocy jakiego narzędzia będą gromadzone informacje zwrotne
Starsi użytkownicy	Poziom wiedzy jest niski albo żaden Ponieważ mieszkańcy nie korzystali w młodości z ICT, mogą być bardziej	Ochrona danych osobowych w czasie korzystania z Internetu	Dostarczanie informacji przy użyciu rozwiązań związanych z opieką zdrowotną Informacje przy współpracy z zakładem ubezpieczeń społecznych	Zespół odpowiedzialny za podnoszenie świadomości	Poszerzenie wiedzy na temat zagadnienia i dostępnych rozwiązań	Podczas Krajowego Tygodnia Ludzi Starszych	Adres e-mail Nr telefonu

Określenie wskaźników pomiaru powodzenia programu

Skuteczność programu pogłębiania wiedzy i jego zdolność do zwiększania bezpieczeństwa informacji są mierzalne. Potrzeba świadomości bezpieczeństwa jest powszechnie uznawana, lecz niewiele publicznych czy prywatnych organizacji próbowało określić ilościowo wartość programów podnoszących świadomość.

Ocena kampanii lub programu jest niezbędna, aby poznać ich skuteczność oraz aby wykorzystać te dane jako wskazówkę pomocną w dostosowaniu inicjatywy tak, aby przyniosła jeszcze większe owoce. Warto zauważyć, że wskaźnika ewaluacji nie można powszechnie stosować w odniesieniu do wszystkich grup docelowych, gdyż potrzeby i warunki są bardzo zróżnicowane. W niniejszej części nacisk położony jest na wskaźniki służące do ewaluacji kampanii skierowanych do użytkowników prywatnych i w mniejszym stopniu do MŚP, gdyż są to najbardziej prawdopodobne grupy docelowe, do których skierowane są kampanie na rzecz bezpieczeństwa informacji. Jednakże niewielkim nakładem pracy można dostosować przedstawione wskaźniki tak, aby odpowiadały potrzebom innych grup docelowych.

Podstawową różnicą pomiędzy użytkownikami prywatnymi a MŚP jest to, że programy poszerzające wiedzę na temat bezpieczeństwa informacji, skierowane do tej drugiej grupy powinny skupiać się na potrzebie opracowania i wdrożenia strategii bezpieczeństwa informacji, jak również proponować sposoby dostosowania się do strategii obowiązującej wewnątrz organizacji. Odnosi się to również do instytucji publicznych i firm prywatnych różnej wielkości[3].

[3] W celu znalezienia dalszych informacji *i wskazówek dotyczących strategii bezpieczeństwa informacji, zobacz SANS Security Policy na stronie http://www.sans.org/resources/policies/.*

Inaczej wygląda sytuacja w przypadku organów publicznych, które nigdy nie będą w stanie opracować jakiegokolwiek rodzaju strategii bezpieczeństwa informacji dla użytkowników prywatnych. Dlatego też organy powinny skupić się na opracowaniu „zalecanych wskazówek" lub „najlepszych praktyk" w związku z bezpieczeństwem informacji i promować je w społeczeństwie.

Kategorie pomiaru

Ogólnie rzecz biorąc, są cztery główne kategorie, w oparciu o które należy mierzyć świadomość bezpieczeństwa:

- Ulepszenie procesu.
- Odporność na ataki.
- Wydajność i skuteczność.
- Wewnętrzna ochrona.

Świadomość bezpieczeństwa można mierzyć, stosując i dostosowując wskaźniki proponowane przez firmę Gartner tak, aby odpowiadały potrzebom użytkowników prywatnych i MŚP. Podstawowe wskaźniki opisane są poniżej.

1. Ulepszenie procesu

Kategoria ta dotyczy opracowania, rozpowszechnienia i rozmieszczenia zalecanych wskazówek bezpieczeństwa, jak i szkolenia z zakresu świadomości bezpieczeństwa. Wskaźniki ewaluacji obejmują następujące kwestie:

1. Czy organ publiczny lub publiczno-prywatna inicjatywa opracowała zalecane wskazówki dotyczące bezpieczeństwa dla społeczeństwa? Czy wskazówki te są przejrzyste i zwięzłe? (Oczekiwana odpowiedź: tak.)
   Dla MŚP: Czy MŚP opracowało ogólną strategię bezpieczeństwa dla swojej organizacji? Czy jest ona czytelna i zwięzła? (Oczekiwana odpowiedź: tak.)
2. Czy zalecane wskazówki dotyczące bezpieczeństwa są zatwierdzone przez odpowiedni organ? Czy inicjatywa ta jest odpowiednio sponsorowana? (Oczekiwana odpowiedź: tak.)
   Dla MŚP: Czy ogólna strategia bezpieczeństwa jest zatwierdzona na najwyższych poziomach organizacji? (Oczekiwana odpowiedź: tak.)
3. Jaki procent badanych osób wie, że zalecane wskazówki dotyczące bezpieczeństwa istnieją? Ile osób widziało lub przeczytało je? (Oczekiwana zmiana: wzrost.)
   Dla MŚP: Jaki procent pracowników MŚP wie, że istnieje strategia bezpieczeństwa? Ile osób zapoznało się z nią? (Oczekiwana zmiana: wzrost.)
4. Jaki procent osób jest pewien, że rozumie zalecane wskazówki dotyczące bezpieczeństwa? (Oczekiwana zmiana: wzrost.)
   Dla MŚP: Jaki procent pracowników wykazał w wyniku zautomatyzowanych badań lub innych procesów, że rozumie strategię bezpieczeństwa? (Oczekiwana zmiana: wzrost.)
5. Jaki procent osób zna właściwą procedurę, którą należy wdrożyć na wypadek jakiegoś incydentu lub wie, do kogo można się zwrócić? (Oczekiwana zmiana: wzrost.)
   Dla MŚP: Jaki procent pracowników wie, do kogo się zwrócić lub jaką procedurę należy wdrożyć na wypadek incydentu? (Oczekiwana zmiana: wzrost.)
6. Ile średnio czasu ma dany organ/inicjatywa na rozesłanie masowego e-maila ostrzegawczego po zidentyfikowaniu nowego zagrożenia lub na umieszczenie ostrzeżeń na często odwiedzanych stronach internetowych? (Oczekiwana zmiana: spadek.)

Dla MŚP: Jaki jest średni czas na rozesłanie ostrzegawczego e-maila do wszystkich pracowników firmy po zidentyfikowaniu nowego zagrożenia ? (Oczekiwana zmiana: spadek.)

7. Czy opracowano i rozlokowano program szkoleniowy podnoszący świadomość? (Oczekiwana odpowiedź: tak.)
   Dla MŚP: Czy opracowano szkolenie podnoszące świadomość? (Oczekiwana odpowiedź: tak.)
8. Jaki procent osób uczestniczył w szkoleniu? (Oczekiwana zmiana: wzrost.)
   Dla MŚP: Jaki procent pracowników uczestniczył w szkoleniu? (Oczekiwana zmiana: wzrost.)
9. Jak często aktualizowana jest treść szkolenia podnoszącego świadomość? (Oczekiwana zmiana: wzrost.)
   Dla MŚP: Jaki średnio upłynął czas, od kiedy pracownik przeszedł szkolenie podnoszące świadomość? (Oczekiwana zmiana: spadek.)
   Dla MŚP: Czy miało miejsce zerwanie umowy za niestosowanie się do strategii bezpieczeństwa? Ile było takich przypadków? (Oczekiwana zmiana: spadek.)
   Dla MŚP: Czy jest program wewnętrznych i zewnętrznych audytów bezpieczeństwa? (Oczekiwana odpowiedź: tak.)
   Dla MŚP: Czy wewnętrzne i zewnętrzne audyty bezpieczeństwa wykazują poprawę w zakresie stosowania się do strategii bezpieczeństwa? (Oczekiwana odpowiedź: tak.)

2. Odporność na ataki

Ta kategoria dotyczy rozpoznania wydarzenia związanego z bezpieczeństwem informacji i odporności na atak.

Wskaźnik ewaluacji obejmuje następujące kwestie:

1. Jaki procent badanych osób rozpoznaje scenariusz wydarzenia związanego z bezpieczeństwem informacji w czasie badań? (Oczekiwana zmiana: wzrost.)
2. Jaki procent badanych osób pada ofiarą wybranego scenariusza? (Oczekiwana zmiana: spadek.)
3. Jaki procent użytkowników nie przeszedł testu na ujawnienie swojego hasła dostępu? (Oczekiwana zmiana: spadek.)
   Dla MŚP: Jaki procent administratorów IT lub personelu helpdesk nie potrafiła zaprezentować niewłaściwej próby zmiany hasła dostępu? (Oczekiwana zmiana: spadek.)
4. Jaki procent użytkowników uruchomił „testowego wirusa”? (Oczekiwana zmiana: spadek.)

3. Wydajność i skuteczność

Kategoria ta skupia się na wydajności i skuteczności w odniesieniu do incydentów związanych z bezpieczeństwem.

Wskaźnik ewaluacji obejmuje następujące kwestie:

1. Jaki procent incydentów związanych z bezpieczeństwem, których doświadczyły osoby, wynikał głównie z postępowania człowieka? (Oczekiwana zmiana: spadek.)
2. Jaki procent czasu przestoju spowodowany był takimi incydentami związanymi z bezpieczeństwem? (Oczekiwana zmiana: spadek.)

Dla MŚP: Jaki procent wydatków zwiazanych z bezpieczeństwem i/lub procent dochodu stanowią wydatki MŚP na podnoszenie świadomości bezpieczeństwa? (Oczekiwana zmiana: spadek.)

4. Wewnętrzna ochrona

Ta kategoria dotyczy tego, jak dobrze dana osoba chroniona jest przed potencjalnymi zagrożeniami.

Wskaźnik ewaluacji obejmuje następujące kwestie:

1. Jaki procent oprogramowania i sprzętu komputerowego dana osoba zakupiła, mając na względzie bezpieczeństwo? (Oczekiwana zmiana: wzrost.)
   Dla MŚP: Jaki procent oprogramowania, partnerów i dostawców MŚP sprawdzono pod kątem bezpieczeństwa (w tym świadomości bezpieczeństwa)? (Oczekiwana zmiana: wzrost.)
2. Jaki procent szczególnie chronionych danych osoby jest pod odpowiednią ochroną? (Oczekiwana zmiana: wzrost.)
   Dla MŚP: Jaki procent danych szczególnie chronionych MŚP jest „odpowiednio" chroniony, uwzględniając świadomość administratorów? (Oczekiwana zmiana: wzrost.)
3. Jaki procent szczególnie chronionych danych osoby nie jest chroniony zgodnie z zalecanymi wskazówkami? (Oczekiwana zmiana: spadek.)
   Dla MŚP: Jaki procent danych szczególnie chronionych MŚP nie jest chroniony zgodnie ze standardami bezpieczeństwa firmy? (Oczekiwana zmiana: spadek.)
4. Jaki procent badanego systemu danej osoby miał zainstalowane uciążliwe oprogramowanie typu spyware? (Oczekiwana zmiana: spadek.)
5. Jaki procent oprogramowania stanowiły programy pirackie? (Oczekiwana zmiana: spadek.)

Opracowanie linii odniesienia do ewaluacji

W poprzednim akapicie przedstawiono wskaźniki oceny skuteczności programu podnoszącego świadomość. Jednakże aby móc korzystać z tych wskaźników, należy określić poziom bieżących potrzeb. Jeśli uprzednio oceni się sytuację, możliwe jest dostrzeżenie korzyści wynikających z programu podnoszącego świadomość. Ewaluacje zapewniają doskonałą możliwość oceny, które składniki miały najwyższy poziom sukcesu oraz które były mniej owocne.

Ankiety i wieloaspektowe badania zapewniają możliwość ewaluacji skuteczności programów. Ze względu na to, że przyszła ewaluacja będzie porównana z tą linią odniesienia, ważne jest, aby zauważyć, że podobne ankiety i badania powinny być ponownie użyte w przyszłych etapach inicjatywy.

Ankiety i wieloaspektowe badania zapewniają możliwość ewaluacji skuteczności programów. Próbka ankiety dotyczącej świadomości dostępna jest w Załączniku V.

Udokumentowanie zdobytych doświadczeń

Ukończywszy wszystkie kroki w ramach pierwszego etapu, należy przeznaczyć czas na opisanie i udokumentowanie doświadczeń zdobytych dotychczas w programie. Można

skorzystać z następującego procesu jako pomocy w określeniu, udokumentowaniu i przedstawieniu zdobytych doświadczeń. Jednak nie chodzi tu o to, by sugerować, że zdobyte doświadczenia mogą być udokumentowane wyłącznie w wyniku procesu grupowego.

W zależności od środowiska i okoliczności programu powinien istnieć środek, przy pomocy którego poszczególni członkowie zespołu programowego mogą sporządzać notatki i opowiadania i przedstawiać je wyznaczonej osobie w celu „wyszlifowania" i złożenia ich w przechowalni lub bazie danych. Taki proces należy określić i udokumentować w wyniku Kroku 1 procedury.

Najważniejsze kwestie

Ustalając podstawowe zasady na początku spotkania, należy zająć się kwestią tego, czym jest posiedzenie dotyczące zdobytego doświadczenia i jak powinna wyglądać konstruktywna krytyka. Poniżej przedstawiono kilka wskazówek dotyczących konstruktywnej krytyki:

- Zdobyte doświadczenie jest zorientowane na zarządzanie programem, a nie na produkt pracy.
- Przykłady przypadków są najbardziej skutecznym sposobem, aby przedstawić swoje uwagi.
- Krytyka powinna być konstruktywna i dotyczyć procesu, a nie osoby. Zachęca się uczestników do tego, aby wyrażali swoje opinie w sposób życzliwy.
- Jeśli nie można w żaden sposób rozwiązać, poprawić, złagodzić jakiegoś problemu lub mieć na niego wpływu, nie należy omawiać go.
- Indywidualne przygotowanie do spotkania przyspiesza proces.
- Należy pamiętać, że jest to forum przeznaczone zarówno do przedstawiania uwag krytycznych, jak i pochwał; nie należy ani jednych, ani drugich odbierać zbyt osobiście, ponieważ jest to praca zespołowa.

Posiedzenie sprawozdawcze poświęcone zdobytym doświadczeniom może w rzeczywistości dawać możliwość osiągnięcia kilku celów organizacyjnych:

- Omówienie alternatywnych stanowisk w sprawie bieżących procesów i ulepszenie bieżącego programu.
- Pokazanie personelowi, że jego uwagi są cenione i wysłuchiwane.
- Podniesienie morale zespołu.
- Możliwość wykorzystania zdobytego doświadczenia w przygotowaniu przyszłych programów o podobnych celach.

Doskonała okazja do krytyki i wzrostu

Niektórzy członkowie personelu mają bardzo zdecydowane poglądy na temat tego, jak pewne części programu są zarządzane. Takie forum jest doskonałą okazją do tego, aby umożliwić im przedstawienie swoich opinii, przekazać pomysły innym i omówić różne podejścia do bieżących procesów. Jeśli spotkanie to jest właściwie prowadzone przez mediatora, może stanowić forum, na którym członkowie zespołu dają upust swoim frustracjom w pozytywny i konstruktywny sposób oraz przedstawiają swoje opinie na temat tego, jak można ulepszyć procesy na przyszłość.

Kierownik programu lub lider zespołu musi skutecznie zarządzać oczekiwaniami przedstawionymi na spotkaniu i znaleźć równowagę pomiędzy pozytywnymi aspektami omawianych kwestii a rzeczywistością harmonogramu programu. W przeciwnym razie istnieje ryzyko, że sesja sprawozdawcza przyniesie skutek przeciwny do zamierzonego i

że spadnie morale zespołu. Należy wziąć pod uwagę to, że wśród członków zespołu może istnieć ciche przekonanie, że wszelkie określone ulepszenia zostaną wdrożone w bieżącym programie. Jeśli nie ma wystarczająco dużo czasu, aby zrealizować którąś z zalecanych zmian (zdobyte doświadczenia) w bieżącym programie, należy powiadomić o tym zespół.

Może zdarzyć się, że zespół określił sposób, dzięki któremu mógłby ulepszyć proces, lecz na tym etapie programu wdrożenie nowej procedury kosztowałoby po prostu zbyt dużo czasu i wysiłku (przypadek, w którym lekarstwo jest gorsze od choroby).

Doświadczenia zdobyte w dziedzinie zarządzania programem obejmują zarówno pozytywne, jak i negatywne wrażenia. Równie ważne jest udokumentowanie tych rozwiązań, które sprawdziły się i które należy powtórzyć w przyszłym programie, jak i zapisanie tego, co się nie powiodło lub może się nie powieść oraz jak można temu zapobiec lub zmierzyć się z tym w przyszłości.

Wskazówki dotyczące posiedzeń poświęconych konstruktywnej krytyce

- Należy rozważyć wprowadzenie limitów czasowych na posiedzeniu. Tego typu posiedzenia mogą być owocne, lecz czasochłonne. Ustalenie limitów czasowych dla poszczególnych wypowiedzi może pomóc zachować pewne pozory porządku nawet w środowisku dosyć niezorganizowanym lub posiadającym luźną formę.
- Należy rozważyć możliwość polecenia członkom zespołu, aby przynieśli na spotkanie udokumentowane pomysły, które już przemyśleli. Jeśli dochodzi do przestoju w rozmowie, należy być przygotowanym na to, aby poruszyć kwestię trudności z poprzednim programem i rozwiązań, jakie zastosowano. Doskonałym punktem wyjściowym do poszukiwania potencjalnych ulepszeń są wszelkie notatki ze spotkania lub sprawozdanie z poruszonych problemów.
- Jeśli poszczególne osoby nie zapiszą zdobytych doświadczeń, gdy rozważają je, doświadczenia te prawdopodobnie pozostaną niewykorzystane.
- Należy zachęcać członków zespołu, aby prowadzili dzienniki w czasie trwania programu. Można odwoływać się do nich, aby przygotować się do posiedzeń. Zachęca się członków zespołu, aby umieszczali komentarze w dziennikach z dbałością , gdyż w pewnym momencie dziennik może stać się częścią dokumentacji programu.
- Należy rozważyć dodanie części poświęconej zdobytym doświadczeniom do bieżących raportów, aby można było wrócić i z łatwością zidentyfikować doświadczenia pod koniec etapu lub programu.
- Należy strategicznie zaplanować czas, w którym zdobyte doświadczenia zostaną zebrane. Zazwyczaj najlepszym czasem na określenie zdobytych doświadczeń pomocnych w ulepszeniu zarządzania programem jest koniec programu, koniec etapu programu, realizacja większego zadania, przyjęcie lub zwolnienie personelu oraz czas po omówieniu ewaluacji działania. Są to okresy, w których doskonale pamięta się wszelkie procesy, które można by ulepszyć. Częstotliwość tych sprawozdawczych posiedzeń zależy od wielkości i złożoności programu.
- W przypadku długotrwałych lub złożonych programów może zachodzić potrzeba okresowych sesji sprawozdawczych, natomiast w przypadku mniejszych programów może zachodzić potrzeba tylko jednorazowej sesji. Przed zgromadzeniem personelu, należy określić proces kontroli przedstawiania zdobytych doświadczeń i objaśnić ten proces w czasie szkolenia zespołu. Na przykład, czy jest konieczne zorganizowanie spotkania i nadanie formalnego charakteru zdobytym doświadczeniom, zanim doświadczenia te zostaną przedłożone kierownictwu programu lub czy poszczególne osoby mogą

przedstawić zdobyte doświadczenia ad hoc? Wiele zależy od doświadczenia personelu i opinii kierownika programu.

- Należy rozważyć możliwość przeprowadzania wywiadów z innymi zespołami lub zaproszenia innych zespołów na sesję sprawozdawczą w celu określenia pokrywających się doświadczeń, doświadczeń z zakresu wymiany informacji lub integracji.

Ważne jest, aby określić, udokumentować i przedstawić zdobyte doświadczenia. Użycie narzędzia zalecane jest, aby skutecznie zarządzać pracą. Szablon formularza, w którym przedstawia się zdobyte doświadczenia, jest dostępny w Załączniku VI.


Etap II
Realizacja i Zarządzanie

Etap II - Realizacja i zarządzanie

- Utworzenie wstępnego zespołu programowego
- Wdrożenie podejścia polegającego na zmianie zarządzania
- Uzyskanie odpowiedniego wsparcia i finansowania zarządzania
- Określenie potrzeb kadrowych i materiałowych dla realizacji programu
- Ocena potencjalnych rozwiązań
- Wybór rozwiązania i procedury
- Opracowanie harmonogramu prac
- Określenie celów i założeń
- Określenie grupy docelowej
- Opracowanie programu i listy zadań
- Zdefiniowanie pojęcia informacji
- Określenie wskaźników pomiaru skuteczności programu
- Opracowanie punktu odniesienia dla potrzeb oceny

- Potwierdzenie składu zespołu programowego
- Przegląd harmonogramu prac
- Rozpoczęcie i wdrożenie programu
- Przekazywanie informacji
- Udokumentowanie zdobytych doświadczeń

- Przeprowadzenie ewaluacji
- Załączenie informacji zwrotnych
- Przegląd założeń programu
- Wykorzystanie zdobytych doświadczeń
- Dostosowanie programu do potrzeb
- Wznowienie programu

Potwierdzenie składu zespołu programowego

Drugi etap programu polega na realizacji. Każdy członek zespołu, którego zadaniem jest podnoszenie świadomości, będzie ogrywał konkretną rolę w kontekście realizacji i zarządzania inicjatywą. Przed rozpoczęciem programu, należy potwierdzić skład zespołu, który będzie odpowiadał zarówno za realizację, jak i za zarządzanie.

Przegląd harmonogramu prac

Przed rozpoczęciem programu, należy zaktualizować harmonogram prac i określić główne punkty programu tak, aby odpowiadały celom i założeniom, jak również wymogom budżetowym.

Rozpoczęcie i wdrażanie programu

Praca wykonywana zgodnie z powyżej wskazanymi krokami oraz z tymi, które zostały wskazane na poprzednim etapie może wydawać się bardzo powolna i zbiurokratyzowana, jednak cały ten czas poświęcony na opracowanie wymogów, rozwiązań i dopracowanie wyników zaowocuje sprawniejszą i skuteczniejszą realizacją.

Gdy już mamy dobrze opracowany plan, jak również odpowiednie zasoby pozwalające na wprowadzenie go, czas na zwrócenie się o pomoc do kolegów z firmy i do wybranych zewnętrznych dostawców w celu opracowania i wprowadzenia programu dla uzyskania korzyści płynących ze zwiększonej świadomości na temat bezpieczeństwa.

Przekazywanie informacji

Podnoszenie świadomości na temat przekazywania informacji wybranym grupom docelowym. Obecnie jest odpowiedni czas na wdrożenie planu przekazywania informacji. Jednocześnie należy zwrócić uwagę na równie istotny element, jakim jest gromadzenie informacji zwrotnych otrzymywanych w ramach programu. Informacje zwrotne są bardzo ważne i należy uwzględnić je przy realizacji kolejnych etapów przekazywania informacji.

Udokumentowanie zdobytych doświadczeń

W związku z tym, że program został już rozpoczęty i trwa jego realizacja, duże znaczenie ma gromadzenie doświadczeń zdobytych podczas tego drugiego etapu. Procedurę dopełnioną pod koniec etapu I należy powtórzyć. Ciekawe mogłoby być porównanie rozwoju programu z perspektywy zdobytych doświadczeń.


Etap III
Ewaluacja i dostosowanie

Etap III - Ewaluacja i dostosowanie

- Utworzenie wstępnego zespołu programowego
- Wdrożenie podejścia polegającego na zmianie zarządzania
- Uzyskanie odpowiedniego wsparcia i finansowania zarządzania
- Określenie potrzeb kadrowych i materiałowych dla realizacji programu
- Ocena potencjalnych rozwiązań
- Wybór rozwiązania i procedury
- Opracowanie harmonogramu prac
- Określenie celów i założeń
- Określenie grupy docelowej
- Opracowanie programu i listy zadań
- Zdefiniowanie pojęcia informacji
- Określenie wskaźników pomiaru skuteczności programu
- Opracowanie punktu odniesienia dla potrzeb oceny

- Potwierdzenie składu zespołu programowego
- Przegląd harmonogramu prac
- Rozpoczęcie i wdrożenie programu
- Przekazywanie informacji
- Udokumentowanie zdobytych doświadczeń

- Przeprowadzenie ewaluacji
- Załączenie informacji zwrotnych
- Przegląd założeń programu
- Wykorzystanie zdobytych doświadczeń
- Dostosowanie programu do potrzeb
- Wznowienie programu

Przeprowadzenie ewaluacji

Zgodnie z tym, co zostało powiedziane w związku z etapem I, skuteczność programu podnoszącego świadomość oraz jego zdolność do poprawy bezpieczeństwa informacji może, mimo pewnych przeciwnych twierdzeń, zostać zmierzona.

Punkt odniesienia wskazany przed rozpoczęciem programu stanowi obraz początkowej sytuacji w ramach grup docelowych. Kwestionariusze uzupełniające i wielotematyczne badania ankietowe pozwalają śledzić postęp w podnoszeniu świadomości.

Załączenie informacji zwrotnych

Informacje zwrotne uzyskane przy przekazywaniu informacji programowych, powinny zostać rozważone pod kątem ulepszenia przyszłych działań związanych z przekazywaniem informacji. Informacje te powinny być połączone z wynikami uzyskanymi z przeprowadzonej ewaluacji.

Przegląd założeń programu

Założenia programu należy ponownie rozważyć w kontekście skuteczności. Co udało się zespołowi osiągnąć? Czy zrealizowano potencjalne korzyści? Jeżeli tak, to z pewnością jest powód do zadowolenia. Jeżeli nie, co należy zrobić aby osiągnąć wyznaczone wyniki? Czy może należałoby zmienić założenia? Ponowne rozważenie założeń pozwala na przeprowadzenie poważnej oceny.

Wykorzystanie zdobytych doświadczeń

Należy poddać ewaluacji doświadczenia zdobyte dzięki programowi podnoszenia świadomości. Które z tych doświadczeń mogą mieć wpływ na podniesienie efektywności i skuteczności programu w przyszłości? Należy zwrócić szczególną uwagę na wyciąganie wniosków zarówno z doświadczeń pozytywnych, jak i negatywnych, a następnie wprowadzić je w życie.

Dostosowanie programu do potrzeb

Dzięki wiedzy i zrozumieniu wynikającym z doświadczeń zdobytych począwszy od rozpoczęcia programu, możliwe jest dostosowanie programu do potrzeb tak, aby zwiększyć jego skuteczność. Każde działanie i zadanie prowadzone w ramach programu może podlegać koniecznym modyfikacjom. Modyfikacje należy wprowadzać w taki sposób, aby zachować w niezmienionej formie cele i założenia programu.

Wznowienie programu

Teraz, kiedy na podstawie zdobytych doświadczeń program został dostosowany do potrzeb, kolejnym krokiem jest wznowienie programu, uzupełniając zadania z etapu II. Jest to idealna sytuacja do uzupełnienia dodatkowych elementów lub wzmocnienia tych, które były realizowane w ramach poprzedniego etapu.

Przeszkody w osiągnięciu odpowiedniego poziomu skuteczności

Wdrożenie skutecznego programu podnoszenia świadomości bezpieczeństwa informacji może okazać się trudnym zadaniem. Nawet najlepiej zaplanowane programy mogą napotkać na pewne przeszkody. Jednakże zrozumienie niektórych z nich może pozwolić na przezwyciężenie ich podczas etapu planowania i wdrażania programu.

Ogólne

1. Wdrażanie nowej technologii

W sytuacji, gdy wdrażana jest nowa technologia, często konieczna jest zmiana sposobu postępowania lub poziomu zrozumienia. Czasami technologia rozwija się w szybszym tempie lub niezależnie od programu mającego na celu podnoszenie świadomości. Może mieć miejsce taka sytuacja, że zespół nie jest ani na bieżąco z aktualnym stanem wiedzy, ani nie jest odpowiednio poinformowany na temat możliwości edukacyjnych. Z tego właśnie powodu tak ważne jest, aby w ramach programu kładziono nacisk na wewnętrzny przepływ informacji, jak również zapewnienie istnienia strategii postępowania w sytuacjach nadzwyczajnych lub strategii przekazywania informacji w sytuacji kryzysowej.

2. Jeden dla wszystkich

W przypadku niektórych programów podnoszących świadomość na temat bezpieczeństwa informacji nie udało się dokonać odpowiedniej segmentacji odbiorców, w wyniku czego wiadomości nie są dostarczane, a ich treść nie jest znana. Użytkownicy technologii informacji każdego dnia otrzymują setki wiadomości z różnych źródeł. Bardzo ważne jest aby dokonać odpowiedniej segmentacji odbiorców i dopilnować, aby otrzymywali oni tylko te informacje, których potrzebują. Strategia „jedna dla wszystkich" może być łatwiejsza do opracowania i wdrożenia, ale za to nie będzie skuteczna.

3. Zbyt wiele informacji

Przekazywanie zbyt wielu informacji jest dość często powtarzającym się błędem. Społeczeństwo wyznacza pewną granicę co do ilości akceptowanych informacji z każdego źródła. Jeżeli odbiorcy są stale zasypywani nadmiarem wiadomości, istnieje duże prawdopodobieństwo odwrócenia ich uwagi. Nawet jeżeli podjęto konieczne kroki w celu dokonania segmentacji odbiorców i przesyłania im odpowiednich wiadomości, nie zmienia to faktu, że zbyt wiele informacji to zawsze zbyt wiele informacji. Program podnoszenia świadomości nie musi zostać zrealizowany w bardzo krótkim czasie. Należy poczekać na ujawnienie się potrzeb odbiorców i znalezienie odpowiedniej równowagi.

4. Brak organizacji

Wielu programom podnoszenia świadomości nie udaje się opracować spójnego procesu i strategii przekazywania wiadomości użytkownikom. W sytuacji gdy styl, temat i sposób przekazania nie jest spójny, trudno jest przyciągnąć uwagę użytkownika, a użytkownikowi dowiedzieć się, czego może się spodziewać. Spójność przekazywania informacji jest kluczowym elementem. Pozwoli to także na określenie tożsamości programu i zbudowanie relacji z odbiorcami.

5. Zaniechanie

Dość częstym zjawiskiem w przypadku programów podnoszących świadomość bezpieczeństwa informacji jest to, że rozpoczynane są z wielkim zapałem, który z czasem gaśnie przynosząc w rezultacie słabe wyniki. W przypadku wielu programów nie udaje się ustanowić i utrzymać regularnego przepływu informacji. Bardzo ważne jest, aby użytkownicy regularnie otrzymywali przypomnienia o kluczowych wiadomościach. Oprócz tego w przypadku wielu programów widoczne jest zjawisko zaniechania podejmowania dalszych działań w stosunku do

odbiorców, jak również proszenia ich o informacje zwrotne. Bardzo ważne jest słuchanie odbiorców i dostosowywanie programu do ich potrzeb.

6. Przekazanie wiadomości do odpowiednich odbiorców

Przekazanie odpowiedniej wiadomości odpowiednim odbiorcom jest często prawdziwym wyzwaniem. Dotyczy to w szczególności dużych społeczeństw. Tytułem przykładu: nawet jeżeli lokalna władza opracowała dobrą strategię przekazywania informacji konkretnym odbiorcom, dostarczanie odpowiednich wiadomości odpowiednim odbiorcom jest nadal bardzo trudne. Grupy e-mailowe opierające się na indywidualnych kryteriach mogą być w takiej sytuacji pomocne, jednak nie rozwiązują problemu.

W niektórych przypadkach, mimo że konkretni odbiorcy zostali zidentyfikowani, zadanie polegające na dowiedzeniu się, kto należy do grupy tych odbiorców może okazać się bardzo trudne. Przykładem może być sytuacja, w której konieczne jest przesłanie wiadomości do konkretnej części odbiorców. Tytułem przykładu, rodzice mogą zostać zidentyfikowani na podstawie rejestrów szkolnych, jednak istnieje małe prawdopodobieństwo, że listy są kompletne, bo mogą nie uwzględniać takich informacji jak ta, że dziecko mieszka tylko z jednym z rodziców. Wyzwaniem jest opracowanie najlepszego rozwiązania dotyczącego identyfikacji i prowadzenia listy, które umożliwiałoby przekazywanie odpowiednich wiadomości odpowiednim rodzicom. Jest to trudne zadanie.

7. Brak zasobów

Brak zasobów wynika na ogół z braku odpowiedniego zarządzania. Bez wsparcia zarządzania trudno jest zapewnić odpowiednie zasoby, a bez odpowiednich zasobów skuteczność programu podnoszenia świadomości na temat bezpieczeństwa jest ograniczona.

8. Brak odpowiedzi na pytanie „dlaczego”

W przypadku wielu programów podnoszących świadomość nie udaje się poinformować użytkowników o tym, dlaczego bezpieczeństwo jest ważne. Wszystkie pozostałe aspekty są uwzględnione, ale niestety informacje, które mogłyby w największym stopniu przyczynić się do zmiany zachowania użytkowników są pomijane. W przypadku użytkowników, którzy rozumieją dlaczego pewne zachowania są ryzykowne istnieje większe prawdopodobieństwo zmiany tych zachowań. Na przykład jeżeli przekazane zostaną wskazówki dotyczące procesu wprowadzania nowego hasła wraz z bardziej rygorystycznymi i złożonymi zasadami, użytkownicy najprawdopodobniej uznają nowy proces za nic więcej, jak tylko niedogodność. Jednak jeżeli wraz z informacją na temat nowego hasła podane zostaną informacje o tym, że hasła są łamane i wykorzystywane w niewłaściwych celach, jak również informacje na temat wpływu takich działań, użytkownicy będą bardziej skłonni do przyjęcia i korzystania z nowych wskazówek.

9. Inżynieria społeczna

Inżynieria społeczna niekoniecznie musi wpływać na wdrażanie programu podnoszącego świadomość, ale może mieć wpływ na jego skuteczność. Poruszenie tej kwestii ma duże znaczenie ponieważ dotyczy „ludzkiego ogniwa”, które program podnoszący świadomość ma wzmocnić. Inżynieria społeczna polega na wykorzystywaniu naturalnej ludzkiej skłonności do pomagania innym, a także

wykorzystywania naiwności ludzkiej w celu uzyskania informacji, które byłyby trudne do uzyskania innym sposobem. Większość ludzi wierzy, że nikt celowo nie oszukuje ani nie manipuluje społeczeństwem. Niemniej jednak w rzeczywistości inżynieria społeczna jest jedną z najbardziej powszechnych form ataku.

Atakujący wybierają często tę metodę, ponieważ jest zadziwiająco łatwa i nie zabiera dużo czasu. Dlaczego atakujący mieliby poświęcać wiele godzin na złamanie hasła, jeżeli mogą bezpośrednio skontaktować się z daną osobą, podając się za helpdesk banku lub innej instytucji i oszukując łatwowierną osobę uzyskują informacje szczególnie chronione? Jednymi z najczęściej wykorzystywanych metod inżynierii socjalnej są: podawanie się za inną osobę, pochlebstwo i pozorowanie pilnej sytuacji, jak również zgoda osoby trzeciej. Bardzo duże znaczenie ma opracowanie i wdrożenie strategii edukacyjnej dotyczącej tego zagadnienia. Niestety, zgodnie z opinią Grangera, Stevena i Berga, uznanych ekspertów w dziedzinie bezpieczeństwa informacji i inżynierii społecznej, zjawisko inżynierii socjalnej jest taką formą ataku, która może oszukać nawet najbardziej dbających o bezpieczeństwo użytkowników.

Charakterystyczne dla MŚP

Poniżej opisane zostały niektóre przeszkody, na które głównie napotykają MŚP. Jednakże omawiane tendencje mogłyby być powszechnie stosowane w przypadku programów podnoszących świadomość na temat bezpieczeństwa kierowanych do innych grup docelowych.

1. **Zmiana długo wypracowywanych zachowań**

   W wielu organizacjach środki bezpieczeństwa wdrażane są z opóźnieniem. A w związku z tym, że środki bezpieczeństwa nie są wprowadzane od początku, użytkownicy mają całe miesiące, tygodnie czy nawet lata na nabranie złych nawyków. Powoduje to, że wyzwanie polegające na wdrażaniu programu podnoszącego świadomość na temat bezpieczeństwa informacji jest jeszcze trudniejsze. Nie chodzi tylko o poinformowanie użytkowników, ale także o to, aby sami użytkownicy odzwyczaili się od złych nawyków, które mogli sobie wyrobić. Ponadto tacy użytkownicy mają większe trudności w zrozumieniu wartości, jaką przedstawia bezpieczeństwo. Ich zdaniem organizacje przez wiele lat świetnie prowadziły swoją działalność bez stosowania środków bezpieczeństwa. Obecnie wymogi odnoszące się do bezpieczeństwa są postrzegane jako niepotrzebne zmiany, które utrudniają życie.

2. **„Bezpieczeństwo jest problemem działu technologii, a nie moim...”**

   Wielu użytkowników uważa, że za bezpieczeństwo odpowiada wyłącznie dział IT. Ograniczają oni swoją rolę do niezbędnego minimum zgodności i to raczej w celu utrzymania pracy, niż z powodu wyrażania chęci uczestniczenia w takim rozwiązaniu. Stosowanie się do polityki jest dobrym początkiem, niemniej jednak pozostaje jeszcze wiele do zrobienia. Ważne jest aby użytkownicy zrozumieli, że personel IT nie może sam zajmować się bezpieczeństwem informacji.

3. **Brak wsparcia ze strony rządzących**

   Uzyskanie wsparcia jest jednym z najbardziej istotnych aspektów programu podnoszenia świadomości na temat bezpieczeństwa informacji i jednocześnie

stanowi największe wyzwanie. Aby wiadomości na temat bezpieczeństwa były skuteczne, muszą być wspierane odgórnie . Nawet jeżeli wielu menedżerów wyraża chęć wspierania inicjatyw na rzecz bezpieczeństwa, często nie znajduje to odzwierciedlenia w praktyce. Jest tak, ponieważ menedżerowie mają własne obowiązki i zadania. Ich podstawowym celem jest osiągnięcie założeń przedsiębiorstwa i dlatego często ciężko jest im znaleźć czas na zagadnienia związane z bezpieczeństwem, niezależnie od tego, jak duże w ich opinii znaczenie ma bezpieczeństwo.

Główne czynniki decydujące o skuteczności

Główne czynniki odpowiedzialne za skuteczność każdego programu podnoszącego świadomość na temat bezpieczeństwa są następujące:

- przed wdrożeniem lub wznowieniem programu podnoszącego świadomość konieczne jest określenie punktu odniesienia dotyczącego obecnego stanu rzeczy;
- programy podnoszące świadomość na temat bezpieczeństwa informacji nie będą skuteczne, jeżeli nie dotrą do docelowej grupy odbiorców;
- w celu rozpowszechnienia informacji należy wykorzystywać organizacje pozarządowe, instytucje, banki, biblioteki, lokalne przedsiębiorstwa handlowe, domy kultury, sklepy komputerowe, instytucje edukacyjne i programy kształcenia dla osób dorosłych, szkoły i organizacje skupiające rodziców i nauczycieli;
- rozgłos ma podstawowe znaczenie w kampanii na rzecz podnoszenia świadomości, ponieważ zwiększa wpływ podnosząc liczbę osób, do których dociera wiadomość.
- należy współpracować na poziomie publicznym oraz na płaszczyźnie prawnej

W przypadku programów skierowanych do MŚP należy pamiętać, że:

- programy podnoszące świadomość na temat bezpieczeństwa informacji skierowane do MŚP nie będą skuteczne, jeżeli będą sprzeczne z kulturą organizacyjną lub nie będą wspierane przez kadrę kierowniczą wyższego szczebla.
- budowanie stałego wsparcia dla programów skierowanych dla MŚP wymaga przedstawienia tego, jak bardzo wysiłki mające na celu podniesienie świadomości na temat bezpieczeństwa są skuteczne.

Wskaźniki omawiane w niniejszym poradniku są w stanie pokazać, czy program podnoszący świadomość na temat bezpieczeństwa zakończył się sukcesem czy porażką.

Wnioski

Obywatele europejscy są coraz bardziej mobilni i coraz częściej korzystają z Internetu. Dlatego też wymagają możliwości pewnego i bezpiecznego połączenia niezależnie od miejsca i czasu. Ta nowa tendencja daje nowe możliwości wspólnotom europejskim. Jednakże zwiększanie częstotliwości przesyłania informacji typu push-and-pull pociąga za sobą pewne konsekwencje, których rozwiązanie należy do obowiązków rządów.

Każdy system jest tak mocny, jak najsłabszy z jego elementów. Błąd człowieka może osłabić nawet najbardziej rygorystyczny program bezpieczeństwa informacji. Świadomość zagrożeń i dostępnych środków bezpieczeństwa jest podstawowym elementem w kontekście bezpieczeństwa systemów i sieci informacyjnych.

ENISA ma nadzieje, że niniejszy Poradnik dostarczy państwom członkowskim cennego narzędzia pomocnego przy opracowywaniu i wdrażaniu inicjatyw i programów mających na celu podnoszenie świadomości. Zapewnienie bezpieczeństwa informacji jest ogromnym wyzwaniem. Pierwszym krokiem do osiągnięcia jego celu jest zwiększenie świadomości grupy docelowej.

Źródła

Pakiet informacyjny: podnoszenie świadomości na temat bezpieczeństwa informacji. Wskazówki dla państw członkowskich.

http://www.enisa.europa.eu//deliverables/index_en.htm

Program budowania świadomości na temat bezpieczeństwa - CyberGuard

http://www.gideonrasmussen.com/article-01.html

NIST 800-50 program szkoleniowo-edukacyjny na temat bezpieczeństwa

Publikacja NIST dostarcza szczegółowych wskazówek na temat opracowywania, rozwijania, wdrażania i prowadzenia programu szkoleniowo-edukacyjnego na rzecz podnoszenia świadomości w ramach programu bezpieczeństwa IT.

http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf

Uwagi dotyczące podnoszenia świadomości na temat bezpieczeństwa (Security Awareness Tips) - Gideon T. Rasmussen

http://www.gideonrasmussen.com/sectips/

Zestaw środków pomagających w podnoszeniu świadomości na temat bezpieczeństwa (Security Awareness Toolbox) - The Information Warfare Site

Zestaw środków pomagających w podnoszeniu świadomości na temat bezpieczeństwa zawiera wiele przydatnych dokumentów i linków.

http://www.iwar.org.uk/comsec/resources/sa-tools/

Sekcja „Czytelnia” organizacji SANS dotycząca podnoszenia świadomości na temat bezpieczeństwa

http://www.sans.org/rr/whitepapers/awareness/

Strona poświęcona polityce bezpieczeństwa organizacji SANS

http://www.sans.org/resources/policies/

Strona internetowa Uniwersytetu w Arizonie poświęcona świadomości bezpieczeństwa

http://security.arizona.edu/awareness.html

System zarządzania polityką bezpieczeństwa firmy NoticeBored i materiały dotyczące podnoszenia świadomości na temat bezpieczeństwa

http://www.noticebored.com/html/white_papers.html i http://www.isect.com/

Human Firewall Council

http://www.humanfirewall.com/

Zbiór zasobów dotyczących świadomości na temat cyberbezpieczeństwa (Cybersecurity Awareness Resource Library)

http://www.educause.edu/CybersecurityAwarenessResourceLibrary/8762

ITSafe Service - inicjatywa rządu Wielkiej Brytanii dotyczącą bezpieczeństwa IT

http://www.itsafe.gov.uk/

Wirtualna Platforma Szkoleniowa (Virtual Training Environment) firmy CERT

https://www.vte.cert.org/vtelibrary.html

Skuteczne strategie dotyczące podnoszenia świadomości na temat bezpieczeństwa

http://techrepublic.com.com/5100-10878_11-5193710.html#

Program budowania świadomości na temat bezpieczeństwa – Stawianie czoła zagrożeniom zaczynając od środowiska firmy (Addressing the Threat From Within)

Gideon T. Rasmussen

http://www.gideonrasmussen.com/article-01.html

Centrum Bezpieczeństwa Internetowego CIS (Center for Internet Security)

http://www.cisecurity.org/resources.html

Stowarzyszenie ds. bezpieczeństwa systemów informacyjnych (Information Systems Security Association)

http://www.issa.org/

Komunikaty amerykańskiego CERT na temat cyberbezpieczeństwa

Wskazówki na temat powszechnych kwestii związanych z bezpieczeństwem skierowane dla użytkowników-amatorów.

http://www.us-cert.gov/cas/tips/index.html

Praktyczny poradnik na temat cyberbezpieczeństwa dla małych przedsiębiorstw

http://www.us-cert.gov/reading_room/CSG-small-business.pdf

Bezpieczeństwo sieci domowej

Daje prywatnym użytkownikom ogólny ogląd zagrożeń związanych z bezpieczeństwem w Internecie, jak również odpowiednich środków zaradczych, szczególnie w kontekście tzw. „always-on" (nieustannego połączenia z Internetem) lub szerokopasmowego dostępu do sieci (takiego jak na przykład modemy kablowe i DSL).

http://www.us-cert.gov/reading_room/home-network-security/

Organizacja National Cyber Security Alliance (NCSA) na rzecz podnoszenia świadomości na temat cyberbezpieczeństwa i kształcenia użytkowników, małych przedsiębiorstw i instytucji edukacyjnych.

http://www.staysafeonline.org/

Grupa Yahoo na rzecz podnoszenia świadomości na temat bezpieczeństwa prowadzi forum, na którym omawiane są metodologie programowe mające na celu podnoszenie świadomości.

http://groups.yahoo.com/group/security-awareness/

The Society for the Policing of Cyberspace (POLCYB)

http://www.polcyb.org/index.htm

Podnoszenie świadomości obywateli na temat bezpieczeństwa informacji: praktyczny poradnik eAware, 2003.

ZAŁĄCZNIKI – SZABLONY I WZORY

Załącznik I – Wzór zaproszenia do składania ofert

Stowarzyszenie <XYZ>, nowa organizacja w <nazwa miasta> poszukuje konsultanta lub konsultantów do pomocy przy początkowym uruchomieniu, wdrażaniu oraz analizie ewentualnych programów podnoszenia świadomości bezpieczeństwa informacji. Zob. związaną z tym „Umowę o usługach", która następuje zwykle po przedstawieniu ofert przy założeniu, że klient znalazł odpowiadającego mu konsultanta, z którym chce podpisać umowę.

Sytuacja

Stowarzyszenie <XYZ> zostało założone w dniu <data>, aby pomóc kilku istniejącym grupom władz lokalnych w <nazwa miasta> oraz promować i koordynować <rodzaj działalności> na tym obszarze. <Nazwa miasta> to miasto, którego liczba mieszkańców wynosi 17,500. Obecnie, <XYZ> ma status organizacji non profit i zwolnionej z podatku, na której czele stoi zarząd, ale nie zatrudnia ona pracowników ani nie posiada powierzchni biurowej. Maksymalny budżet na pracę konsultantów w wysokości <podać wartość> został uzgodniony na początku.

Zadania do realizacji

Należy kontynuować rozwój Stowarzyszenia oraz planować jego przyszłą pracę wraz z przedstawicielami organizacji członkowskich w celu określenia wspólnych potrzeb, jakimi organizacja <XYZ> powinna się zająć oraz uzgodnienia, w jaki sposób przygotować kampanię mającą na celu budowanie świadomości. W szczególności należy:

- opracować plan pracy oparty na uzgodnionych celach i założeniach;

- przygotować biuletyn <XYZ> i opublikować pierwsze numery;

- opracować roczne plany budżetowe <XYZ> na kampanię na następne trzy lata;

- przygotować działania w celu zbadania skuteczności kampanii;

- opracować metodologię przedstawiania zdobytego doświadczenia, informacji zwrotnych oraz załączania ich do zaktualizowanego harmonogramu prac.

Kampania ta powinna zacząć się w dniu <data> oraz zakończyć nie później niż w dniu <data>.

Jak złożyć ofertę

Zainteresowani konsultanci powinni przedstawić <wpisać nazwisko osoby> z <XYZ> następujące dokumenty/informacje nie później niż do dnia <wpisać datę>. Aby uzyskać więcej informacji, należy skontaktować się z <wpisać nazwiska właściwych osób>.

1. Ofertę uwzględniającą Państwa kwalifikacje (lub kwalifikacje zespołu konsultantów) i przedstawiającą sposoby wykonania wyżej wymienionych zadań
2. Ostateczne wyliczenie opłat, jakie będą pobierane oraz kosztów, które zostaną poniesione
3. Życiorysy wszystkich konsultantów, którzy uczestniczyliby w projekcie
4. Nazwiska, numery telefonów oraz osoby kontaktowe w trzech organizacjach pozarządowych będących Państwa klientami w ciągu ostatnich 18 miesięcy, z którymi możemy się skontaktować jako z osobami dającymi referencje
5. Rozmowy z finalistami odbędą się w tygodniu <wpisać datę>.

Załącznik II – Szablon tygodniowego sprawozdania

Tygodniowe sprawozdania z postępu w realizacji

DATA

PROJEKT / PROGRAM

Osoby i organizacja

Zadania wykonane w zeszłym tygodniu

Zadania zaplanowane na przyszły tydzień

Zagrożenia

Zdarzenia / sytuacje, które mogą wpłynąć na nasze plany i działania

Opis	Źródło	Dotkliwość możliwych strat	Prawdopodobieństwo	Plan(y) mające na celu zmniejszenie strat

Problemy

Zdarzenia / sytuacje, które już wpływają na nasze plany i działania

Opis	Źródło	Dotkliwość strat	Prawdopodobieństwo	Plan(y) mające na celu zmniejszenie strat

Prognoza na przyszły tydzień

Lokalizacja osób i ich działania (dotyczące urlopów / szkoleń / warsztatów / innych zobowiązań klientów etc.)

Dzień	Rano	Po południu
Poniedziałek		
Wtorek		
Środa		
Czwartek		
Piątek		

Załącznik III – Wzór harmonogramu prac

Działania **Wymienić każde działanie, przedstawić krótki opis tego działania i wszystkich działań podrzędnych (główny cel itp.)**	**Data rozpoczęcia planowanych działań**	**Data ukończenia planowanych działań**	**Wyniki działań** **Przedstawić wyniki każdego wymienionego działania**
I. Planowanie i ocena			
- Utworzenie wstępnego zespołu programowego	kwiecień 2006	kwiecień 2006	- zespół utworzony
- Wdrożenie podejścia polegającego na zmianie sposobu zarządzania	kwiecień 2006	kwiecień 2006	- zasady programu ustalone
- Uzyskanie odpowiedniego wsparcia i finansowania zarządzania	kwiecień 2006	czerwiec 2006	- wyraźne wsparcie systemu zarządzania i zatwierdzenie budżetu
- Określenie potrzeb kadrowych i materiałowych dla realizacji programu	maj 2006	maj 2006	- krótka lista kadr i materiałów
- Ocena potencjalnych rozwiązań	maj 2006	czerwiec 2006	- decyzja, czy wykonać w firmie czy zlecić wykonanie na zewnątrz - lista opcji uszeregowana pod względem ważności - polityka programu i procedury - szablony sprawozdań dla programu - funkcje i obowiązki
- Wybór rozwiązania i	lipiec 2006	lipiec 2006	- umowa podpisana

procedury			
- Opracowanie harmonogramu prac	czerwiec 2006	czerwiec 2006	- harmonogram prac
- Określenie celów i założeń	czerwiec 2006	lipiec 2006	- cele i założenia programu formalnie określone i uzgodnione
- Określenie grupy docelowej	czerwiec 2006	lipiec 2006	- grupy docelowe określone i potrzeby udokumentowane
- Opracowanie programu i listy zadań	czerwiec 2006	lipiec 2006	- program opracowany
- Zdefiniowanie pojęcia informacji	czerwiec 2006	lipiec 2006	- wiadomość ustalona - wiadomość szczegółowo opisana - wiadomość wypróbowana - partnerzy w wymianie informacji - kanały informacyjne wybrane - szczegółowy plan wymiany informacji - mechanizm informacji zwrotnych
- Określenie wskaźników pomiaru skuteczności programu	czerwiec 2006	lipiec 2006	- wskaźnik oceny
- Opracowanie punktu odniesienia dla potrzeb oceny	czerwiec 2006	lipiec 2006	- ocena bieżącej sytuacji
- Udokumentowanie zdobytych doświadczeń	lipiec 2006	lipiec 2006	- zdobyte doświadczenia nagrane
II. Realizacja i zarządzanie			
Potwierdzenie składu zespołu	sierpień 2006	sierpień 2006	- skład zespołu potwierdzony

programowego			
Przegląd harmonogramu prac	sierpień 2006	sierpień 2006	- ostateczny harmonogram prac
Rozpoczęcie i wdrożenie programu	październik 2006	styczeń 2007	-
Przekazywanie informacji	październik 2006	styczeń 2006	- plan przekazywania informacji wdrożony
Udokumentowanie zdobytych doświadczeń	styczeń 2007	styczeń 2007	- zdobyte doświadczenia nagrane
III. Ewaluacja i dostosowanie			
Przeprowadzenie ewaluacji	luty 2007	marzec 2007	- wyniki ankiet
Załączenie informacji zwrotnych	luty 2007	marzec 2007	- informacje zwrotne
Przegląd założeń programu	luty 2007	marzec 2007	- cele programu
Wykorzystanie zdobytych doświadczeń	marzec 2007	kwiecień 2007	- doświadczenia zaktualizowane
Dostosowanie programu do potrzeb	marzec 2007	kwiecień 2007	- zaktualizowany harmonogram prac
Wznowienie programu	maj2007		

Załącznik IV – Szablon przedstawienia danych o grupie docelowej

Grupa docelowa			
Definicja			
Kategoria		**Cele, potrzeby**	
Podkategoria		**Wiedza**	
Wielkość		**Kanał informacyjny**	
Lokalizacja			

Przykład / Zalecenia	

Załącznik V – Wzór kwestionariusza na temat świadomości bezpieczeństwa informacji – do użytku przez organ publiczny

[*Nazwa organizacji*] prowadzi badania, które ułatwią określenie sposobów pogłębiania wiedzy obywateli [*nazwa wspólnoty*] na tematy związane z bezpieczeństwem informacji. Będziemy wdzięczni, jeśli zgodzą się Państwo poświęcić 10 minut swojego czasu na udzielenie odpowiedzi na kilka krótkich pytań dotyczących bezpieczeństwa informacji.

1. W jaki sposób łączą się Państwo z Internetem:

a.___ połączenie dial-up

b.___ łącze ADSL (szerokopasmowe)

c.___ Internet w firmie

2. Gdzie korzystają Państwo ze swojego komputera (prosimy zaznaczyć wszystkie odpowiedzi, które Państwa dotyczą):

a.___ dom

b.___ biuro

c.___ miejsca publiczne (szkoła, biblioteka itp.)

d.___ kafejka internetowa

e.___ centrum telefoniczne/internetowe

f.___ inne (prosimy sprecyzować) _____

3. Zdaniem wielu, bezpieczeństwo oznacza ochronę przed niepożądanymi działaniami. Przyjmując taką definicję, prosimy wskazać w skali od 1 do 5, jakie znaczenie ma dla Państwa bezpieczeństwo Waszego sprzętu technologicznego i, co za tym idzie, informacji, np. komputera, urządzeń zewnętrznych, danych itp., przy czym 1 oznacza największe znaczenie, a 5 - najmniejsze.

1 2 3 4 5

Duże Średnie Bardzo małe

4. Co z wymienionych poniżej stanowi, Państwa zdaniem, największe zagrożenie dla technologii informacyjnej? Można zaznaczyć kilka odpowiedzi:

a._____ wirusy i robaki

b._____ spam i inne niepożądane e-maile

c._____ hakerzy

d._____ czyny nieuczciwej konkurencji

e._____ złośliwe oprogramowanie (np. spyware)

f._____ wadliwy sprzęt komputerowy

Inne_____

5. Czy są Państwo świadomi, że [*organ publiczny*] oceni potencjalne zagrożenia dla technologii informacyjnej oraz, że informacje na ten temat mogłyby pomóc Państwu opracować plan mający na celu ochronę przed tymi zagrożeniami?

Tak, zdaję sobie z tego sprawę.

Nie, nie jestem tego świadom.

6. Prosimy wskazać, w skali od 1 do 5, poziom Państwa wiedzy na temat działań, jakie można podjąć w celu ochrony Waszego sprzętu i danych, przy czym 1 oznacza najwyższy poziom wiedzy, a 5 – najniższy:

1 2 3 4 5

Najwyższy Średni Najniższy

7. Czy mają Państwo zainstalowany którykolwiek z poniższych środków ochrony komputera i danych elektronicznych. Można zaznaczyć kilka odpowiedzi.

a._____ Oprogramowanie antywirusowe, które jest regularnie aktualizowane

b._____ Zapora sieciowa (firewall)

c._____ Blokada antyspamowa

d._____ Hasła zapewniające skuteczną ochronę

e._____ Regularne tworzenie kopii zapasowych

f._____ Zaktualizowana wyszukiwarka internetowa z kodowaniem

g._____ Inne, prosimy

sprecyzować_____

8. Który z przedstawionych poniżej sposobów informowania o ochronie przed potencjalnymi zagrożeniami byłby, według Państwa, najlepszy? Mówiąc inaczej, najszybciej przyswoją Państwo informacje na temat bezpieczeństwa informacji przedstawione:

a._____ w radiu

b._____ w reklamach telewizyjnych

c._____ na łamach lokalnej prasy

d._____ w listach przychodzących do domu

e._____ podczas spotkań z sąsiadami/mieszkańcami miasta

f. _____ na plakatach

g._____ w inny sposób, prosimy sprecyzować

_____

Dziękujemy bardzo za wzięcie udziału w ankiecie. Mamy nadzieję, że udzielone przez Państwa odpowiedzi dostarczą informacji, które pozwolą zwiększyć świadomość społeczeństwa na temat znaczenia bezpieczeństwa informacji.

Jeżeli chcieliby Państwo otrzymać dodatkowe informacje na temat bezpieczeństwa informacji, prosimy zaznaczyć poniżej:

_____ TAK

_____ NIE

Załącznik VI – Szablon przedstawienia zdobytego doświadczenia

<table>
<tr><td rowspan="2">ZDOBYTE DOŚWIADCZENIE</td><td>NR ZBIORU</td><td>Strona z</td></tr>
<tr><td colspan="2">KATEGORIA (główna / alternatywna)</td></tr>
<tr><td>TYTUŁ/PRZEDMIOT:</td><td colspan="2">SŁOWA KLUCZOWE:</td></tr>
<tr><td>OPIS WYDARZENIA:</td><td colspan="2"></td></tr>
<tr><td>ZDOBYTE DOŚWIADCZENIA:</td><td colspan="2"></td></tr>
<tr><td>ZALECENIA:</td><td colspan="2"></td></tr>
</table>

ZAŁĄCZNIKI:			ODNIESIENIA:	
ZŁOŻONE PRZEZ:	PROJEKT/BIURO:	ORGANIZACJA /FIRMA:	LOKALIZACJA:	DATA ZDARZENIA:
NR TELEFONU:	ADRES E-MAIL:	SPECJALIZACJA:	BUDYNEK/SALA:	DATA ZŁOŻENIA: