dr inż. Tomasz Klasa

Zachodniopomorska Szkoła Biznesu
- Akademia Nauk Stosowanych

dr inż. Adrian Kapczyński

Politechnika Śląska

UX jako jeden z elementów związanych z zapewnieniem bezpieczeństwa informacji w świetle wymagań dyrektywy NIS-2

Streszczenie:

Bezpieczeństwo informacji staje się jednym z największych wyzwań dla organizacji wszystkich typów i różnych wielkości. Źródłem wyzwań jest nie tylko ogólna sytuacja geopolityczna czy pojawianie się licznych nowych podatności w narzędziach informatycznych o lawinowo rosnącej złożoności, ale także sami użytkownicy tych rozwiązań. Dyrektywa NIS-2 wprowadza szereg nowych obowiązków związanych z cyberbezpieczeństwem, których skuteczna realizacja będzie uzależniona od zdolności dopasowania się z wdrażanymi rozwiązaniami do potrzeb nie tylko samej organizacji jako całości, ale też poszczególnych osób ją tworzących. Z tego powodu zasadne wydaje się wykorzystanie podejścia UX podczas projektowania zmian wynikających z dyrektywy NIS-2.

Słowa kluczowe:

UX, bezpieczeństwo informacji, dyrektywa NIS-2

WPROWADZENIE

Gwałtowny rozwój technologii teleinformatycznych oraz napięta sytuacja geopolityczna powodują, że wydłuża się lista czynników wpływających na ogólny stan cyberbezpieczeństwa organizacji.

Do wielu znanych od lat typów incydentów dołączają nie tylko coraz bardziej wyrafinowane modele ataków motywowanych gospodarczo lub politycznie, ale też problemy wynikające z lawinowo rosnącej złożoności oprogramowania. Odpowiedzią na nie są coraz bardziej rozbudowane mechanizmy zabezpieczeń - zarówno techniczne, jak i organizacyjne. Implementowane są silniejsze algorytmy szyfrowania, rozbudowane systemy kontroli uprawnień czy procedury z precyzyjnym podziałem obowiązków i odpowiedzialności.

Wszystkie te działania powodują dalszy wzrost złożoności systemu, obciążając użytkowników dodatkowymi czynnościami lub generując dodatkowe obciążenie infrastruktury teleinformatycznej. Wielu problemów można jednak uniknąć albo znacznie ograniczyć ich skutki, projektując warstwę interakcji użytkownika z systemem informatycznym w sposób dostosowany do wymogów bezpieczeństwa informacji. Identyfikacja błędów popełnianych przez użytkownika za pomocą adekwatnych walidacji wsparta czytelnymi informacjami zwrotnymi może skutecznie zabezpieczyć przed wystąpieniem wielu znanych problemów, ale nie jest rozwiązaniem kompletnym. Zabezpieczają przed ne-

gatywnymi konsekwencjami, ale w wyniku podjęcia dodatkowych działań w odpowiedzi na wykryte nieprawidłowości. Jednocześnie korzystając z zasad UX i reguł projektowania interfejsów użytkownika można wyeliminować szereg warunków sprzyjających występowaniu tych nieprawidłowości.

Celem niniejszej publikacji jest systematyzacja rozważań na temat związku między UX, a bezpieczeństwem informacji postrzeganym z perspektywy dyrektywy NIS-2.

Niniejszy artykuł powstał w oparciu o pogłębioną analizę literatury, w ramach której przeprowadzono systematyczny przegląd źródeł naukowych i technicznych, poddając je krytycznej ocenie i finalnie syntezie. Pozwoliło to na kompleksowe przedstawienie przedmiotowego problemu i sformułowanie wniosków opartych na ugruntowanych podstawach teoretycznych.

W pierwszej kolejności zostanie przybliżony obszar tematyczny związany z bezpieczeństwem informacji oraz dyrektywą NIS-2, a następnie zaprezentowana zostanie relacja między UX, a bezpieczeństwem informacji.

BEZPIECZEŃSTWO INFORMACJI

Bezpieczeństwo informacji to stan będący efektem szeregu działań chroniących informacje i systemy informacyjne przed "nieautoryzowanym dostępem, wykorzystaniem, ujawnieniem, zakłóceniem, modyfikacją lub zniszczeniem"[1]. Zgodnie z §3542 tej normy, bezpieczeństwo informacji stanowi kombinację trzech podstawowych obszarów bezpieczeństwa, realizowanych w postaci rozwiązań sprzętowo-programowych:

- Poufność (w tym prywatność),
- Integralność (w tym niezaprzeczalność),
- Dostępność.

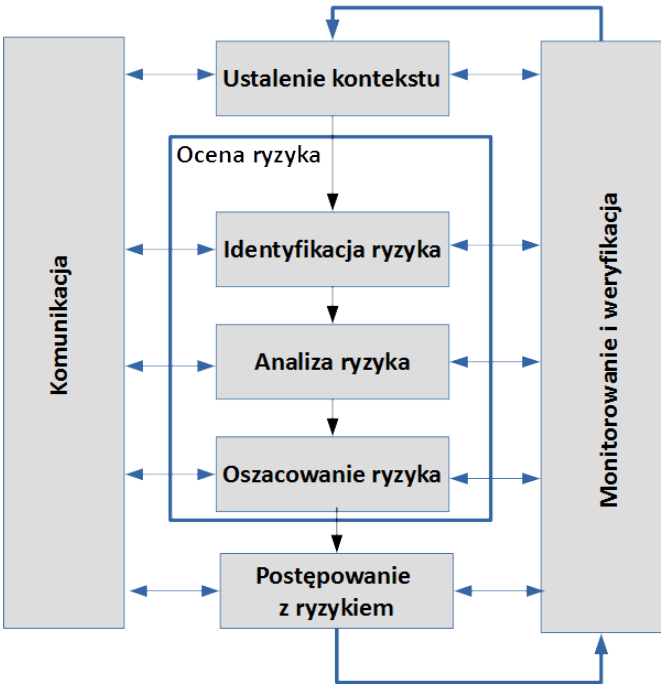
Bezpieczeństwo nie jest czynnością ani procesem, a rezultatem osiąganym w efekcie uporządkowanego postępowania ze znanymi zagrożeniami, których główne przykłady wymieniono w przytoczonej definicji. Zagrożenia nie są powiązane z charakterystyką posiadanych zasobów - jest to każda uogólniona, potencjalna możliwość naruszenia, uszkodzenia zasobów[2], „okoliczność lub zdarzenie, które może potencjalnie wpłynąć na działania organizacji, jej zasoby, członków, inne organizacje, lub państwo poprzez nieautoryzowany dostęp, zniszczenie, wyjawienie lub modyfikację informacji albo odmowę obsługi w ramach systemu informatycznego"[3]. Słowo "potencjalnie" ma w tej definicji równie duże znaczenie - podkreśla, że nie jest istotne, jak duże są szanse na zrealizowanie się danego zagrożenia. Sam fakt jego istnienia sprawia, że należy zweryfikować, jaki może mieć wpływ na stan bezpieczeństwa danego systemu czy organizacji. Oceny tej dokonuje się poprzez identyfikację podatności posiadanych zasobów na dane zagrożenie, definiowanej jako „związek trzech składowych: wrażliwości systemu lub błędu, dostępu napastnika do luki, możliwości wykorzystania luki przez

1 United States Code. 2006. Title 44, Chapter 35, Subchapter III. 2006.

2 ISO/IEC15408-1:2009. Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model.

3 NIST. 2012. Guide for Conducting Risk Assessments, NIST Special Publication 800-30. Gaithersburg : National Institute of Standards and Technology, 2012.

atakującego”[4]. To oznacza ocenę cech własnych zasobu pod kątem wrażliwości na określone rodzaje zagrożeń, które mogą być skutkiem założeń projektowych lub błędów w implementacji. Każda istniejąca podatność, która w określony sposób może być użyta, tworzy scenariusz wpływający negatywnie na poziom bezpieczeństwa systemu. Skala tego wpływu będzie różna w zależności od skutków, ale też prawdopodobieństwa zrealizowania się tego scenariusza. W celu utrzymania pożądanego poziomu bezpieczeństwa należy podjąć stosowne środki zaradcze wobec podatności, których wpływ powoduje przekroczenie akceptowalnego poziomu bezpieczeństwa systemu lub organizacji. Zwykle są to działania polegające na wdrożeniu zabezpieczeń technicznych lub organizacyjnych.



Rys. 1. Proces zarządzania ryzykiem

Źródło: (ISO/IEC31000:2009, 2009)[5].

Mnogość i różnorodność zagrożeń, a także złożoność budowanych systemów informacyjnych sprawiają, że identyfikowanie podatności i ocena ich wpływu na poziom bezpieczeństwa powinny być wykonywane w usystematyzowany sposób. Do tego celu stosuje się opisany w normie ISO 27001 proces zarządzania bezpieczeństwem, który opiera się o proces zarządzania ryzykiem[6]. Proces ten rozpoczyna się ustaleniem kontekstu (zebranie informacji o systemie i organizacji, w której jest wdrożony oraz celach do osiągnięcia). Następnie identyfikuje się i analizuje ryzyka, by na podstawie szacowanego poziomu ryzyka dobrać adekwatne środki zaradcze (sposób postępowania z ryzykiem). Rezultaty każdego z tych etapów podlegają stałej kontroli i monitorowaniu. Ponadto, na każdym z tych etapów bardzo ważne jest skuteczne komunikowanie użytkownikom zidentyfikowanych problemów oraz przyjętego postępowania.

4 U.S. Air Force Software Protection Initiative. 2009. The Three Tenets of Cyber Security, 2009.

5 ISO/IEC31000:2009. 2009. Risk management - Principles and guidelines, 2009.

6 J.w.

Wyróżnia się cztery rodzaje postępowania z ryzykiem[7],[8]:

- akceptacja,
- unikanie,
- przeniesienie – jego przypadkiem szczególnym jest dzielenie ryzyka wyróżnione w NIST jako odrębny rodzaj postępowania z ryzykiem,
- ograniczenie.

Akceptacja oznacza przyjęcie aktualnego poziomu ryzyka – jako akceptowalnego lub ze względu na brak możliwości jego ograniczenia. Przeniesienie jest przekazaniem częściowej odpowiedzialności za skutki danego ryzyka na inny podmiot, w ramach umowy dwustronnej. Przykładem takiego postępowania z ryzykiem może być np. Polisa ubezpieczeniowa. Unikanie polega na podjęciu działań, które redukują prawdopodobieństwo zrealizowania się danego ryzyka, np. przez wprowadzenie warunków, które nie sprzyjają lub wręcz uniemożliwiają wystąpienie danego zdarzenia. Z kolei ograniczenie oznacza redukowanie skutków zrealizowania się ryzyka, np. poprzez zmniejszenie zasięgu lub czasu oddziaływania.

ZMIANY WYNIKAJĄCE Z KONIECZNOŚCI IMPLEMENTACJI DYREKTYWY NIS-2

Dyrektywa NIS-2 (ang. Network and Information Systems Directive 2) to przepisy mające na celu zwiększenie poziomu cyberbezpieczeństwa w państwach członkowskich UE[9].

Głównym celem dyrektywy jest wzmocnienie odporności w zakresie cyberbezpieczeństwa poprzez wprowadzenie stosownych środków zarządzania ryzykiem w podmiotach funkcjonujących we wskazanych w dyrektywie sektorach gospodarki. Lista sektorów obejmuje między innymi:

a. sektor energetyczny (wytwarzanie i dystrybucja energii elektrycznej; wydobycie, magazynowanie i transport ropy naftowej, gazu ziemnego i węgla, itp.,
b. sektor transportu (lotniczego, kolejowego, wodnego i drogowego,
c. sektor bankowy i finansowy (banki i inne podmioty z nimi powiązane, w tym firmy inwestycyjne oraz giełdy papierów wartościowych),
d. sektor medyczny (szpitale, producenci leków i wyrobów medycznych, dostawcy usług cyfrowych w sektorze zdrowia i inne),
e. inne sektory gospodarki, w których funkcjonują przedsiębiorstwa wodociągowe i kanalizacyjne; dostawcy usług dostępu do Internetu; organy administracji rządowej i samorządowej czy podmioty zajmujące się zbieraniem, transportowaniem, przetwarzaniem i unieszkodliwianiem odpadów.

Warto zauważyć, iż dyrektywa NIS-2 wprowadza dwie kategorie podmiotów:

7 NIST. 2012. Guide for Conducting Risk Assessments, NIST Special Publication 800-30. Gaithersburg : National Institute of Standards and Technology, 2012.

8 ISO27005:2011. 2011. Information technology - Security techniques - Information security risk management, 2011.

9 Transforming NIS2 Challenges into Strategic Opportunities, Cisco White Paper, 2023. https://www.cisco.com/c/dam/global/EMEA-Security/EU_NIS2_white_paper_0801241.pdf [data dostępu 2024.11.05].

- Podmioty kluczowe, które świadczą usługi o zasadniczym znaczeniu dla utrzymania krytycznych funkcji społecznych lub gospodarczych,
- Podmioty ważne, których zakłócenie działalności może mieć znaczący wpływ na społeczeństwo lub gospodarkę.

Zakres wymagań w zakresie cyberbezpieczeństwa różni się w zależności od kategorii.

Wśród kluczowych celów przedmiotowej dyrektywy jest obowiązek raportowania incydentów, co ma dać pełny obraz zmaterializowanych zagrożeń, a także pozwolić na skuteczne i szybkie reagowanie na incydenty. Zapisy w dyrektywie promują współpracę między państwami członkowskimi oraz wymianę informacji na temat zagrożeń, które wystąpiły w danym kraju.

Konieczność implementacji NIS-2 wymusza następujące zmiany:

- Przeprowadzanie kompleksowych ocen ryzyka.
- Zarządzanie ryzykiem związanym z dostawcami.
- Wdrażanie właściwych środków bezpieczeństwa (prewencyjnych, detekcyjnych i korygujących), w tym: kontroli dostępu oraz ochrony sieci i systemów.
- Opracowanie planów reagowania na incydenty oraz zapewnienie ciągłości działania.
- Zapewnienia odpowiednich zasobów niezbędnych do realizacji szkoleń w zakresie cyberbezpieczeństwa.

Każda z ww. zmian wiąże element ludzki, techniczny oraz organizacyjny. Taki splot jest naturalnym środowiskiem dla działań w zakresie UX, o czym stanowi kolejny punkt artykułu.

ROLA UX W BEZPIECZEŃSTWIE INFORMACJI

Termin UX (ang. User eXperience) dot. ukierunkowanego na doświadczenia człowieka (użytkownika) projektowanie produktu, np. aplikacji. Celem nie jest samo osiągnięcie zamierzonej funkcjonalności czy opracowanie ładnego interfejsu, a kompleksowo przemyślana forma interakcji z użytkownikiem, dostosowana do jego potrzeb i możliwości[10]. Pozwala na opracowywanie nie tylko systemów informacyjnych, ale też fizycznych produktów. Klasycznym przykładem ze świata motoryzacji było umieszczanie zestawu narzędzi i trójkąta ostrzegawczego w klapie bagażnika m.in. w Mercedesach i BMW (lata 80/90 XXw.). W razie awarii ułatwiało to przeprowadzenie naprawy – potrzebne narzędzia nie były schowane na dnie bagażnika, pod wszystkimi walizkami.

Koncepcja UX może znaleźć zastosowanie nie tylko podczas projektowania konkretnego produktu w postaci rzeczy lub programu. Trzy etapy procesu zarządzania ryzykiem (a także bezpieczeństwem) opierają się na interakcjach z ludźmi:

- Komunikacja
- Postępowanie z ryzykiem
- Monitorowanie

Skuteczność komunikacji z użytkownikami wpływa na efektywność postępowania z ryzykiem,

10 C. Badura, UXUI Design Zoptymalizowany. Nie tylko dla designerów, Helion, Gliwice, 2022.

np. przez kształtowanie świadomości użytkowników o konsekwencjach określonych działań. Same działania zaradcze, jeśli nie zostaną dostosowane nie tylko do oczekiwań w zakresie bezpieczeństwa, ale także do możliwości użytkowników oraz ich zadań i sposobu ich wykonywania (a nawet warunków, w jakich są realizowane) mogą się okazać nie tylko nieefektywne, ale wręcz stworzyć szereg nowych problemów[11],[12]. W rezultacie nieadekwatne działania mogą doprowadzić do wzrostu ryzyka, choć celem ich wprowadzenia było jego ograniczenie.

Jako główne źródła ryzyka w organizacjach od dawna wskazuje się m.in.[13],[14],[15]:

- utrata komunikacji,
- współdzielenie informacji,
- złożoność systemu (im większa, tym wyższe prawdopodobieństwo błędów),
- rozbudowana łączność (liczne kanały komunikacyjne),
- błędy w zarządzaniu hasłami (słabe hasła lub niewłaściwe ich przechowywanie),
- błędy oprogramowania,
- brak kontroli danych wejściowych

Są to czynniki, w których udział człowieka ma wręcz kluczowe znaczenie. Błędy w oprogramowaniu popełniają ludzie, rozbudowane systemy sprawiają problemy ludziom bardziej niż innym programom. Cyklicznie powtarzane analizy stale wskazują, że głównym źródłem incydentów są osoby bezpośrednio lub pośrednio związane z organizacją[16],[17]. To z kolei oznacza, że jednym z głównych narzędzi poprawy bezpieczeństwa (poprzez ograniczenie ryzyka) może być zastosowanie technik UX, choć zwykle myśli się o nich w kontekście poprawy użyteczności produktu, zapewnienia przewagi nad konkurencją czy po prostu zwiększenia sprzedaży.

Spośród czterech rodzajów postępowania z ryzykiem wymienionych w punkcie pierwszym niniejszego artykułu, techniki UX mogą znaleźć zastosowanie do:

- Ograniczenia ryzyka
- Unikania ryzyka

W przypadku unikania ryzyka, powszechnie stosuje się walidacje dla wartości wprowadzanych przez użytkowników oraz rozwiązania uniemożliwiające wprowadzenie niepoprawnej wartości. Dotyczy to na przykład wprowadzania daty czy wyboru wartości ze zbioru (np. podczas rezerwacji wizyty u lekarza). Nie są to techniki nowe i jako takie nie stanowią o faktycznym użyciu UX. Za pomocą UX

11 M. Mannan, P. C. van Oorschot, Security and Usability: The Gap in Real-World Online Banking, NSPW, 2007 https://www.nspw.org/papers/2007/nspw2007-mannan.pdf [data dostępu 2024.11.05].

12 F. Di Nocera, G. Tempestini, M. Orsini, Usable Security: A Systematic Literature Review, Information 2023, 14(12), 641; https://doi.org/10.3390/info14120641 [data dostępu 2024.11.05].

13 Kakareka, A. 2009. Chapter "23". [book auth.] J. Vacca. Computer and Information Security Handbook. s.l. : Morgan Kaufmann Publications. Elsevier Inc., 2009, p. 393.

14 Alawamleh, M. and Popplewell, K. 2010. Risk Sources Identification in Virtual Organisation. [book auth.] K. Popplewell, et al. Enterprise Interoperability IV. Making the Internet of the Future for the Future of Enterprise. New York : Springer London Dordrecht Heidelberg, 2010.

15 An Introduction to the FAIR Materiality Assessment Model, FAIR Institute, 2023. https://1616664.fs1.hubspotusercontent-na1.net/hubfs/1616664/An%20Introduction%20to%20the%20FAIR%20Materiality%20Assessment%20Model.pdf. [data dostępu 2024.11.05].

16 Contos, B. 2006. Enemy at the Water Cooler: Real-Life Stories of Insider Threats and Enterprise Security Management Countermeasures. s.l. : Syngress, 2006.

17 PWC. 2023. Global State of Information Security Survey 2023. Global State of Information Security Survey. [Online] 2023. https://www.pwc.com/gx/en/issues/risk-regulation/global-risk-survey.html [data dostępu 2024.11.05].

można dobrać odpowiedni dla konkretnego zastosowania sposób realizacji konkretnej walidacji czy wyboru wartości. W zależności od adresata (kim jest użytkownik) i warunków eksploatacji systemu konieczne może być zastosowanie innej formy informacji zwrotnej lub innego rodzaju selekcji wartości ze zbioru.

W przypadku ograniczania ryzyka, gdy celem jest ograniczenie skutków zaistniałego problemu, jednym z głównych zastosowań UX będzie dobór skutecznych środków dystrybucji informacji o zaistniałym problemie, by inne osoby mogły jak najszybciej zareagować w sposób przewidziany w polityce bezpieczeństwa. Dobór właściwej formy i środków komunikacji w zależności od kontekstu i bieżących uwarunkowań może mieć kluczowe znaczenie dla skuteczności powiadomienia o incydencie, wpływając na czas reakcji i skalę strat. Drugim z kluczowych zastosowań UX w obszarze ograniczania ryzyka będzie dopasowanie technik monitorowania stanu bezpieczeństwa, które wymagają bezpośredniego zaangażowania użytkownika. Pozyskiwanie informacji bezpośrednio od ludzi niejednokrotnie jest koniecznością, choć powoduje obciążenie dodatkowymi zadaniami i jest podatny na nieprecyzyjne informacje zwrotne. Za pomocą technik UX można zaprojektować pozyskiwanie danych w sposób ograniczający uciążliwość wynikającą z dodatkowych czynności, a jednocześnie wykrywający niespójności lub luki w przekazywanych danych.

Choć celem nadal pozostaje utrzymanie określonego poziomu bezpieczeństwa, podejście UX pozwala zrealizować je z uwzględnieniem perspektywy człowieka jako użytkownika - w tym jednostkowych ograniczeń, preferencji, szczególnych zdolności.

WYBRANE PRZYKŁADY UŻYCIA ROZWIĄZAŃ UX JAKO ODPOWIEDZI NA ZMIANY WYNIKAJĄCE Z DYREKTYWY NIS-2

W niniejszym artykule skupiono uwagę na relację między UX a bezpieczeństwem informacji, stąd warto przedstawić wybrane przykłady użycia rozwiązań UX jako odpowiedzi na zmiany wynikające z dyrektywy NIS-2.

Konkretnych przykładów użycia rozwiązań UX w rozwiązaniach z zakresu bezpieczeństwa informacji można podać bardzo dużo tu jednak chodzi konkretnie o te, które mają związek ze zmianami wynikającymi z dyrektywy NIS-2. W poprzedniej części artykułu zwrócono uwagę na kilka podstawowych zmian, które muszą wprowadzić podmioty z związku z koniecznością dostosowania organizacji do wymogów przedmiotowej dyrektywy, a wśród nich bardzo ważne są zmiany związane z “Wdrażaniem właściwych środków bezpieczeństwa (prewencyjnych, detekcyjnych i korygujących), w tym: kontroli dostępu oraz ochrony sieci i systemów” oraz “Zapewnienia odpowiednich zasobów niezbędnych do realizacji szkoleń w zakresie cyberbezpieczeństwa”. W dalszej części opracowania przyjrzymy się tym dwóm obszarom, formułując przykłady użycia.

W nawiązaniu do obszaru pierwszego, dotyczącego środków bezpieczeństwa, warto podkreślić kluczową rolę zarządzania tożsamością i dostępem. W dyrektywie NIS-2 podkreśla się znaczenie silnego uwierzytelniania. Wysokie doświadczenie użytkownika może sprawić, że proces uwierzytel-

niania będzie przyjazny dla użytkownika, np. poprzez wykorzystanie biometrii lub powiadomień typu push zamiast kodów jednorazowych dostarczanych poprzez aplikację mobilną lub krótką wiadomość tekstową (SMS). Uwierzytelnianie ściśle związane jest z autoryzacją i tu znajdziemy kolejny przykład użycia: interfejsy do zarządzania uprawnieniami powinny być intuicyjne i łatwe w użytkowaniu, umożliwiając administratorom nadawanie, modyfikowanie oraz usuwanie uprawnień[18].

W zakresie obszaru szkoleń z zakresu cyberbezpieczeństwa: dyrektywa NIS-2 wymaga podnoszenia wiedzy z zakresu cyberbezpieczeństwa, w praktyce stawiając wymóg ciągłego podnoszenia świadomości i umiejętności pracowników w zakresie ochrony informacji. Platforma zdalnej edukacji z dobrym UX może pomóc w spełnieniu wymogów dyrektywy i znacznie zwiększyć zaangażowanie uczestników szkolenia. Grywalizacja: systemy punktowe, odznaki za osiągnięcia i rankingi, mogą zachęcać uczestników do częstej interakcji. Mikronauczanie, które opiera się na dostarczaniu krótkich, skoncentrowanych na wybranym zagadnieniu pigułek wiedzy, umożliwia skuteczne przyswajanie informacji w krótkim czasie, co jest szczególnie cenne w dynamicznych środowiskach pracy.

Dostosowywanie materiałów szkoleniowych do uwarunkowań w zakresie pełnionych obowiązków w organizacji przez danego pracownika, ale także posiadanych doświadczeń i indywidualnych preferencji uczenia się, oferuje "doświadczenie edukacyjne", które jest odpowiednie i angażujące. Ponadto warto podkreślić to, iż intuicyjny oraz responsywny interfejs umożliwiający naukę na różnych urządzeniach oraz interaktywne elementy, np. symulacje scenariuszy zagrożeń, mogą znacząco podnieść efektywność szkoleń. Wreszcie, platforma e-learningowa z zaawansowanymi funkcjami analitycznymi pozwala na monitorowanie postępów i identyfikację obszarów wymagających dodatkowej uwagi, co podnosi skuteczność realizowanych procesów szkoleniowych i tym samym przyczynia się do budowania kultury bezpieczeństwa w organizacji, zgodnie z ideą dyrektywy NIS-2.

Na koniec warto zauważyć, iż przedstawione powyżej (wybrane) przykłady nie stanowią zamkniętego katalogu. Interesującym przykładem użycia jest zastosowanie prostych, zrozumiałych oraz adaptacyjnych formularzy zgłoszeniowych podejrzeń naruszenia bezpieczeństwa.

Bardzo ciekawym przedmiotem analizy jest rola inkluzywnych interfejsów użytkownika, które uwzględniają wymagania WCAG (Web Content Accessibility Guidelines) w systemach zarządzania bezpieczeństwem informacji.

WNIOSKI

Dyrektywa NIS-2 wprowadza szereg nowych obowiązków w zakresie cyberbezpieczeństwa. Skuteczność ich implementacji będzie w znacznej mierze zależna od uwzględnienia perspektywy adresata, czyli użytkownika. Realizacja cyklicznych szkoleń, jeśli nie zostanie odpowiednio przygotowana i dostosowana do odbiorców, stanie się tylko dodatkowym obciążeniem, w którym udział wiele osób będzie ograniczać. Tym samym aktualizacja wiedzy będzie nieefektywna, co doprowadzi do wzrostu ryzyka pomimo wdrożenia zmian wynikających z NIS-2.

18 W. Fallatah, S. Furnell, Y. He, Refining the Understanding of Usable Security, Lecture Notes in Computer Science ((LNCS,volume 14045)), 2023.

Ze względu na duży wpływ samych użytkowników na skuteczność wdrożenia zmian wprowadzanych dyrektywą NIS-2, na podstawie opisanej w niniejszym artykule wstępnej analizy aplikowalności technik UX w zarządzaniu cyberbezpieczeństwem, wskazane wydaje się przeprowadzenie pogłębionych badań w zakresie wykorzystania istniejących technik UX w obszarze rozwiązań zastosowanych w związku z wymogami dyrektywy NIS-2. Drugim ważnym obszarem wymagającym dalszej weryfikacji jest problem dostępności w świetle wymagań dyrektywy NIS-2, który można próbować rozwiązać za pomocą projektowania opartego o UX.

BIBLIOGRAFIA

Alawamleh, M. and Popplewell, K. 2010. Risk Sources Identification in Virtual Organisation. [book auth.] K. Popplewell, et al. Enterprise Interoperability IV. Making the Internet of the Future for the Future of Enterprise. New York : Springer London Dordrecht Heidelberg, 2010.

C. Badura, UXUI Design Zoptymalizowany. Nie tylko dla designerów, Helion, Gliwice, 2022.

Transforming NIS2 Challenges into Strategic Opportunities, Cisco White Paper, 2023 https://www.cisco.com/c/dam/global/EMEA-Security/EU_NIS2_white_paper_0801241.pdf [data dostępu 2024.11.05].

Contos, B. 2006. Enemy at the Water Cooler: Real-Life Stories of Insider Threats and Enterprise Security Management Countermeasures. s.l. : Syngress, 2006.

F. Di Nocera, G. Tempestini, M. Orsini, Usable Security: A Systematic Literature Review, Information 2023, 14(12), 641; https://doi.org/10.3390/info14120641 [data dostępu 2024.11.05].

W. Fallatah, S. Furnell, Y. He, Refining the Understanding of Usable Security, Lecture Notes in Computer Science ((LNCS,volume 14045)), 2023.

An Introduction to the FAIR Materiality Assessment Model, FAIR Institute, 2023 https://1616664.fs1.hubspotusercontent-na1.net/hubfs/1616664/An%20Introduction%20to%20the%20FAIR%20Materiality%20Assessment%20Model.pdf [data dostępu 2024.11.05].

ISO/IEC15408-1:2009. Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model.

ISO27005:2011. 2011. Information technology - Security techniques - Information security risk management, 2011.

ISO/IEC31000:2009. 2009. Risk management - Principles and guidelines, 2009.

Kakareka, A. 2009. Chapter „23”. [book auth.] J. Vacca. Computer and Information Security Handbook. s.l. : Morgan Kaufmann Publications. Elsevier Inc., 2009, p. 393.

M. Mannan, P. C. van Oorschot, Security and Usability: The Gap in Real-World Online Banking, NSPW, 2007 https://www.nspw.org/papers/2007/nspw2007-mannan.pdf [data dostępu 2024.11.05].

NIST. 2012. Guide for Conducting Risk Assessments, NIST Special Publication 800-30. Gaithersburg : National Institute of Standards and Technology, 2012.

PWC. 2023. Global State of Information Security Survey 2023. Global State of Information Security Survey. [Online] 2023. https://www.pwc.com/gx/en/issues/risk-regulation/global-risk-survey.html [data dostępu 2024.11.05].

United States Code. 2006. Title 44, Chapter 35, Subchapter III, 2006.

U.S. Air Force Software Protection Initiative. 2009. The Three Tenets of Cyber Security, 2009.

UX AS ONE OF FACTORS IN INFORMATION SECURITY ASSURANCE IN LIGHT OF NIS-2 DIRECTIVE

Summary:

Information security becomes one of the biggest challenges to organizations no matter of their size and type. They originate not only from general geopolitical situation or appearance of numerous vulnerabilities in software tools of rapidly growing complexity, but also from the users of these tools. The NIS-2 directive introduces a number of new requirements connected with cybersecurity. Their successful implementation will depend on the ability to adapt with introduced solutions not only to the needs of the organization as a whole, but also to individuals it consists of. Because of that it seems reasonable to adapt UX-based approach to design of solutions based on requirements of NIS-2 directive.

Keywords:

UX, information security, NIS-2 directive