GRYWALIZACJA, GRY WIDEO, FILMY INTERAKTYWNE, SYMULACJE PHISHINGOWE – NAJNOWSZE TRENDY W SZKOLENIACH Z ZAKRESU PODNOSZENIA ŚWIADOMOŚCI CYBERBEZPIECZEŃSTWA

5.01.2017

- Cyberprzestępcy coraz częściej ukierunkowują swoje działania w nieświadomych pracowników a nie w zabezpieczenia technologiczne
- Inwestycje w zabezpieczenia IT i szkolenia cyberspecjalistów są równie ważne jak szkolenia pracowników w zakresie świadomości cyberzagrożeń
- Przyszłe rozwiązania szkoleniowe będą oparte przede wszystkim o zasady i elementy gier oraz symulacje wideo. Pozwolą na skuteczne nabywanie, rozwijanie i utrwalanie niezbędnych umiejętności w zakresie obrony przed cyberatakami
- Wiele czynników ma wpływ na jakość szkoleń i kształtowanie kultury cyberbezpieczeństwa

Nowe technologie cyfrowe oraz usługi internetowe, w tym przede wszystkim urządzenia i aplikacje mobilne, rozwiązania w chmurze oraz media społecznościowe znacząco usprawniły sposób funkcjonowania współczesnych organizacji. Z drugiej strony, obok niewątpliwych korzyści biznesowych, przyniosły nowe zagrożenia bezpieczeństwa IT. Aby się przed nimi uchronić, organizacje inwestują w najnowsze technologie zabezpieczeń i szkolenia specjalistów bezpieczeństwa IT. Niestety, często nie dostrzegają faktu, że współczesne cyberataki stają się coraz mniej techniczne. I – co najgorsze – wykorzystują najmniej chronioną część organizacji – nieświadomych pracowników. Jak wynika z raportu PhishMe[1] z 2016 roku, przeważająca część cyberataków jest skuteczna, ponieważ pracownicy ulegają różnym formom ataków socjotechnicznych. Na przykład, klikają w fałszywe linki lub załączniki w wiadomościach phishingowych, zawierające jakąś formę złośliwego oprogramowania. Dotyczy to nawet 91% cyberataków.

Rys. 1: Kadr filmu animowanego pt. „Phishing Beware" (źródło: ISQ)

[1] Enterprise Phishing Susceptibility and Resiliency Report, https://phishme.com/enterprise-phishing-susceptibility-report

Socjotechnika jest potężnym narzędziem w rękach cyberprzestępców. Każdy z nas może ulec różnym formom manipulacji, perswazji lub oszustwa, zarówno w świecie realnym, jak i cyfrowym. Jednak w tym drugim dużo łatwiej podszyć się pod zaufaną osobę lub znaną markę i wyłudzić od pracownika poufne informacje albo skłonić pracownika do działań, które pozwolą atakującemu na ominięcie technicznych zabezpieczeń systemów IT. Bardzo często wystarczy e-mail lub telefon do nieświadomego pracownika, żeby zdobyć potrzebne informacje.

> SOCJOTECHNIKA JEST POTĘŻNYM NARZĘDZIEM W RĘKACH CYBERPRZESTĘPCÓW

W cyberprzestrzeni pojawia się coraz więcej zagrożeń socjotechnicznych i są one coraz bardziej wyrafinowane. Cyberprzestępcy wykorzystują najrozmaitsze odmiany technik tzw. wpływu społecznego (tzw. reguły Cialdiniego)[2]. Przykładem jest reguła autorytetu, stosowana z powodzeniem w atakach phishingowych. Wykorzystuje ona fakt, że ludzie bardzo często bezwarunkowo spełniają prośby osób uznanych za autorytet, np. zajmujących wysokie stanowiska w organizacji lub ekspertów w danej dziedzinie. Technika ta jest skutecznie stosowana np. w atakach typu CEO fraud, czyli oszustwach „na dyrektora generalnego", w których, w celu wyłudzenia pieniędzy lub informacji, atakujący w e-mailu lub przez telefon, podszywa się pod menadżera wysokiego szczebla w organizacji.

Nieświadomi zagrożeń socjotechnicznych pracownicy są najbardziej na nie podatni i to ich nieostrożność, naiwność lub ignorancja potrafi zniweczyć najbardziej zaawansowane zabezpieczenia techniczne. Stanowią więc oni jeden z krytycznych elementów bezpieczeństwa IT organizacji i dlatego wymagają szkolenia zarówno z podstaw bezpieczeństwa IT, jak i z rozpoznawania zagrożeń socjotechnicznych. Szkolenia powinny stać się jednym z priorytetów inwestycyjnych w cyberbezpieczeństwo organizacji.

Aby przekonać się, w jakim stopniu pracownicy danej organizacji są odporni na różne formy ataków socjotechnicznych, wystarczy wykonać tzw. **testy socjotechniczne**. Można to zrobić korzystając np. z usług tzw. **zespołów Red Team**. Zespoły te, wykorzystując tzw. **etyczny hacking** (ang. *ethical hacking*) zajmują się profesjonalnie testowaniem bezpieczeństwa systemów IT. Wykonują one kontrolowane ataki, sprawdzające zabezpieczenia techniczne, fizyczne a także podatność pracowników w danej organizacjina zagrożenia socjotechniczne. Testowanie poziomu odporności pracowników na takie zagrożenia jest przeprowadzane za pomocą symulowanych ataków phishingowych, rozmów telefonicznych (poprzez podszywanie się pod pracownika organizacji) albo poprzez podrzucenie w organizacji przenośnych urządzeń pamięci masowej (np. pendrivów, kart SD).

Szkolenie pracowników w zakresie rozpoznawania zagrożeń socjotechnicznych jest ogromnym wyzwaniem. Eksperci ds. bezpieczeństwa IT wiedzą, jak trudno jest przekonać pracowników do stosowania trudnych do odgadnięcia haseł lub robienia zapasowych kopii dokumentów. Natomiast, z punktu widzenia pracowników, szkolenia z zakresu podnoszenia świadomości cyberbezpieczeństwa są postrzegane często jako zbyt długie, zbyt techniczne a w rezultacie – mało interesujące[3].

[2] Robert B. Cialdini, „Wywieranie wpływu na ludzi. Teoria i praktyka", Wyd. GWP, 2013
[3] https://usa.ingrammicro.com/cms/media/Documents/ingrammicro/s/security/cyber-security-awareness.pdf

Jak zatem należy przeprowadzić szkolenie, które zainteresuje i zmotywuje pracowników do stosowania chociażby minimalnych środków zabezpieczeń? Takie, które skutecznie przygotuje ich do przeciwstawienia się atakom socjotechnicznym. Takie, które pokaże jak rozpoznać manipulację, ucząc wzmożonej czujności i ostrożności np. podczas klikania w linki lub załączniki w wiadomościach e-mailowych, nie udzielania poufnych informacji przez telefon czy nie korzystania z pendrivów z niezaufanych źródeł? Ponadto, jak przeprowadzić takie szkolenia na dużą skalę? Faktem jest, że na tego typu szkolenia kwalifikuje się praktycznie każdy pracownik każdej organizacji. Dotyczy to często nie kilkudziesięciu osób, ale kilkuset czy nawet kilku tysięcy pracowników poszczególnych organizacji.

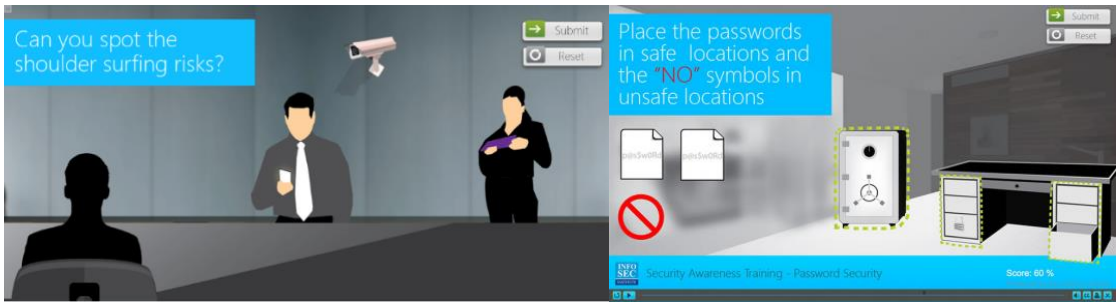
W ostatnich latach, rynek szkoleń i programów w zakresie podnoszenia świadomości bezpieczeństwa IT, bardzo intensywnie się rozwija. Pojawiły się nowe formy szkoleń, coraz bardziej interesujące z punktu widzenia ich uczestników. W ofercie wielu firm znajdują się szkolenia wykorzystujące grywalizację (ang. *gamification*), „poważne" gry (ang. *serious games*), filmy interaktywne, symulacje phishingowe (ang. *phishing simulations*) a także znacznie ulepszone jakościowo formy dotychczasowych rozwiązań szkoleniowych (biuletyny, infografiki, itp.).

> WIELE RÓŻNYCH FIRM ABY UATRAKCYJNIĆ FORMUŁĘ SZKOLEŃ, WPROWADZA DO NICH ELEMENTY GIER

Grywalizacja. Wiele różnych firm, aby uatrakcyjnić formułę szkoleń, wprowadza do nich grywalizację, czyli elementy gier, żeby uzyskać większe zaangażowanie uczestników. Typowe dla gier elementy, takie jak: współzawodnictwo, satysfakcja z postępów i rozwiązanych problemów (przejście kolejnych poziomów gry) a także punktacja, osiągnięty wynik, wizja wygranej oraz nagrody, wyjątkowo silnie motywują i angażują uczestnika do czynnego udziału w szkoleniu. Jednym z przykładów takich rozwiązań jest opracowana przez firmę Digital Guardian platforma DG Data Defender[4]. To tak naprawdę odwrócona idea tradycyjnych rozwiązań ochrony przed wyciekami informacji (ang. *Data Loss Prevention*, DLP), połączona z grywalizacją. Zamiast, jak w przypadku technologii DLP, identyfikowania i raportowania zachowań pracowników niezgodnych z przyjętymi w organizacji zasadami bezpieczeństwa IT, wprowadza ona system nagradzania pracowników za ich przestrzeganie. W tej **korporacyjnej grze z nagrodami**, każde poprawne zachowanie związane z bezpieczeństwem IT (np. szyfrowanie wiadomości zawierających poufne dane lub zgłaszanie wiadomości phishingowych) jest punktowane i umieszczane w tabeli wyników, widocznych przez wszystkich pracowników w organizacji. W ustalonych odstępach czasu, liderzy gry są premiowani kartami podarunkowymi np. do sklepu internetowego. Ten rodzaj szkolenia zakłada, że promowanie pozytywnego podejścia i nagradzania pracowników jest dużo bardziej motywujące niż egzekwowanie przestrzegania procedur, które często odnosi niestety przeciwny skutek.

Innym przykładem, opartym na grywalizacji, jest program podnoszenia świadomości SecurityIQ AwareEd[5], opracowany przez INFOSEC Institute. Program składa się z wielu poziomów trudności i zawiera ćwiczenia, które wymagają od uczestnika realizowania podobnych działań jak w grach wideo, takich jak np. wybranie właściwych elementów w danym scenariuszu czy „upuszczenie" ich na właściwe miejsce (Rys. 2). Program ten umożliwia generowanie szczegółowych raportów z postępów szkolenia.

[4] https://digitalguardian.com/blog/gamification-data-loss-prevention-educating-and-enabling-employees-dlp
[5] INFOSEC Institute, Security IQ, http://resources.infosecinstitute.com/gamification-of-security-awareness-campaigns-2/



Rys. 2: Ćwiczenia z programem SecurityIQ AwareEd (źródło: INFOSEC Institute)

Wśród rozwiązań opartych o grywalizację jest gra on-line Cybersecurity Lab[6], dostępna na stronie NOVA Labs. Tutaj gracze mogą rozwinąć świadomość cyberzagrożeń dzięki kolejnym rozgrywkom, w których wzmacniają elementy zabezpieczeń hipotetycznej sieci społecznościowej. Poszczególne rozgrywki dotyczą różnych wyzwań, np. tworzenia „silnych" haseł lub przeciwstawiania się zagrożeniom socjotechnicznym. Innym przykładem szkoleń wykorzystujących grywalizację są warsztaty CyberSafety Games[7], organizowane przez Kaspersky Lab. Uczestnicy warsztatów, prowadzonych z wykorzystaniem zasad gry, są zapoznawani z cyberzagrożeniami oraz zachowaniami sprzecznymi z zasadami bezpieczeństwa IT. Gra uwzględnia charakterystyczne cechy środowiska pracy szkolonych pracowników i sytuacje znane im z miejsca ich pracy. Grywalizacja jest także z powodzeniem stosowana w szkoleniach menadżerów wyższego szczebla w zakresie podejmowania decyzji dotyczących cyberbezpieczeństwa oraz uświadamiania. Do tego rodzaju szkoleń zaliczają się tzw. **gry biznesowe (strategiczne)**. Należy do nich np. gra planszowa KIPS Game[8] opracowana przez Kaspersky Lab oraz interaktywna symulacja Game of Threats[9] firmy PwC. Obie gry zdobyły już uznanie w środowiskach korporacyjnych.

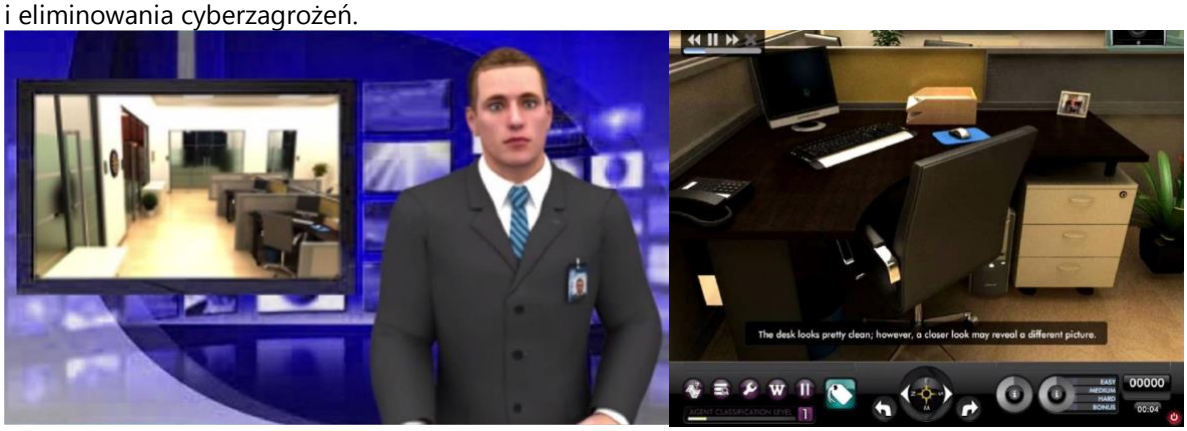
Gry poważne. Wśród rozwiązań szkoleniowych, coraz większe zainteresowanie wzbudzają tzw. „poważne" gry, czyli edukacyjne gry wideo, wykorzystywane już z powodzeniem w edukacji z zakresu medycyny, biznesu i wojskowości. Gry tego typu mają wiele ważnych cech, potęgujących proces uczenia i przyswajania wiedzy. Przede wszystkim jest to wizualizacja, która przykuwa uwagę a tym samym maksymalizuje koncentrację uczestnika gry. Ponadto, istotne jest rozbudzane stopniowo zainteresowanie i „realistycznie" przedstawione problemy

> EDUKACYJNE GRY WIDEO SĄ JUŻ Z POWODZENIEM WYKORZYSTYWANE W SZKOLENIACH Z MEDYCYNY, BIZNESU I WOJSKOWOŚCI

[6] NOVA Labs, Cybersecurity Lab, http://www.pbs.org/wgbh/nova/labs/lab/cyber/
[7] CyberSafety Games, https://www.kaspersky.pl/dla-korporacji/cybersecurity-awareness
[8] KIPS, Kaspersky Interactive Protection Simulation, https://www.kaspersky.com/enterprise-security/security-awareness
[9] PWC, Game of Threats, https://www.pwc.com/us/en/financial-services/cybersecurity-privacy/game-of-threats.html

do rozwiązania a także wzmożone zaangażowanie, które wynika z przypisania gracza do kluczowej roli w podejmowaniu decyzji. Wszystkie te czynniki pozwalają na lepsze zrozumienie przedstawionych zagadnień, łatwiejsze ich opanowanie i zapamiętanie.

W zakresie uświadamiania z zakresu cyberbezpieczeństwa, „poważne" gry dopiero pojawiają się na rynku. Jednym z przykładów są mini-gry z serii Info-Sentinel[10] firmy MAVI Interactive (Rys. 3) oraz gry przygodowe Agent Surfire[11] tej samej firmy. Na początku, gracz uczestniczy w szkoleniu typu "wskaż i kliknij" a następnie kontynuuje ćwiczenia poprzez udział w scenariuszu "złap hackera". Trening dotyczy ponad setki różnych wyzwań, które pomagają uczestnikowi gry wzmocnić umiejętności w zakresie wykrywania i eliminowania cyberzagrożeń.



Rys. 3: Kadry gry Info-Sentinel (źródło: MAVI Interactive)

Interaktywne filmy wideo. Inną interesującą formą narzędzi edukacyjnych, wykorzystywanych w podnoszeniu świadomości cyberbezpieczeństwa, są interaktywne fabularne filmy szkoleniowe. Do przykładów należą, dostępne on-line, filmy: „An Awareness Story"[12], wyprodukowany przez Deutsche Telecom oraz „Targeted Attack: the Game"[13] firmy Trend Micro. Filmy tego typu angażują widza w realistyczną fabułę, dając mu możliwość wpływu na jej przebieg. Na przykład, w filmie „An Awareness Story", scenariusz filmu zakłada, że rozwój wydarzeń doprowadzi do udanego bądź nieskutecznego ataku socjotechnicznego. Rolą widza jest, w ustalonych momentach akcji filmu, podejmowanie decyzji (zob. Rys. 4), które pozwolą bohaterom filmu przeciwstawić się różnym formom manipulacji a tym samym obronić się przed atakiem socjotechnicznym. Pomyślny finał filmu zależy od właściwych wyborów widza. Dobrze zagrany, sugestywny i działający na emocje film potrafi skutecznie dotrzeć do świadomości widza oraz lepiej zrozumieć i utrwalić właściwe zachowania przedstawione w scenariuszu.

> SUGESTYWNY FILM POTRAFI SKUTECZNIE DOTRZEĆ DO ŚWIADOMOŚCI WIDZA I OSIĄGNĄĆ OCZEKIWANY EFEKT SZKOLENIOWY

[10] MAVI Interactive, "Info-Sentinel", http://maviinteractive.com/video_info_sentinel.asp
[11] MAVI Interactive, "Agent SurfFire", http://maviinteractive.com/video_insider_threat.asp
[12] Deutsche Telecom, „An Awareness Story", http://eisas.enisa.fak11.uni-muenchen.de/Telekom/Bluffpl.html
[13] Trend Micro, "Targeted Attack: the Game", http://targetedattacks.trendmicro.com/index.html

Rys. 4: Kadry z filmu szkoleniowego z zagrożeń socjotechnicznych pt. „An Awareness Story" (źródło: Deutsche Telecom)

Symulacje phishingowe. W ostatnich latach pojawiły się także dedykowane rozwiązania szkoleniowe z zakresu różnych form phishingu. Są to platformy symulacyjno-szkoleniowe, których celem jest zredukowanie częstotliwości, z jaką pracownicy klikają w linki w wiadomościach phishingowych. Wśród rozwiązań tego typu, znajdziemy oferty firm m.in. MediaPro[14], PhishMe[15], Know4Be[16] czy PhishLine[17]. Każda z nich oferuje własne rozwiązanie w tym zakresie ale podstawowa koncepcja działania jest taka sama. W ramach przeprowadzanych w organizacji ćwiczeń, wiadomości phishingowe są wysyłane do pracowników. Pracownicy, którzy klikną w fałszywy link, umieszczony w wiadomości e-mailowej (zamiast kliknąć „zgłoś phishing"), automatycznie stają się uczestnikami szkolenia komputerowego (ang. *Computer-Based Training*, *CBT*) z zakresu zagrożeń phishingowych.

Firmy oferujące powyższe rozwiązania, będąc na bieżąco z nowymi trendami w wiadomościach phishingowych, mogą szybko dostosować taktykę swoich programów szkoleniowych do nowych zagrożeń. W celu osiągnięcia wysokiej skuteczności w rozpoznawaniu zagrożeń phishingowych przez pracowników, symulacje przeprowadzane są cyklicznie a uzyskane statystyki potwierdzają efektywność takiego podejścia. Oferty firm różnią się szczegółami rozwiązań, np. proponują adaptacyjny symulator phishingu, który z każdym kolejnym szkoleniem wysyła wiadomości phishingowe o różnym stopniu trudności. Inne dostarczają zautomatyzowanego reagowania na zgłoszone maile phishingowe. Jeszcze inne proponują usługi typu Red Teaming, z zakresu testowania różnych technik ataków socjotechnicznych, w tym wysyłanie wiadomości SMS, połączenia telefoniczne (tj. atak typu vishing, od ang. *voice phishing*) czy podrzucenie pendrivów.

Inne formy edukacyjne: biuletyny, infografiki, plakaty, quizy, komiksy, filmy animowane. Pomimo coraz większej różnorodności i zaawansowania rozwiązań, dostępnych na rynku szkoleń, warto zauważyć, że nie powinno się rezygnować z tradycyjnych form edukacji i środków

> INFOGRAFIKI I PLAKATY SĄ SKUTECZNE W SZYBKIM DOTARCIU DO DUŻEJ LICZBY PRACOWNIKÓW

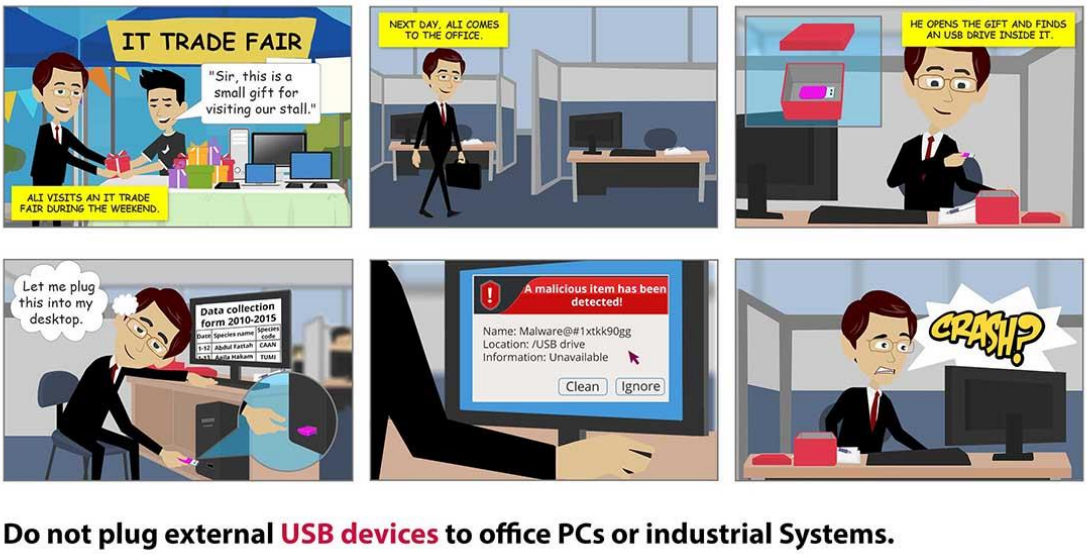
[14] MediaPro, https://www.mediapro.com/security-awareness-program/anti-phishing/
[15] PhishMe, https://phishme.com/product-services/simulator-2/
[16] Know4Be, https://www.knowbe4.com/products/enterprise-security-awareness-training/
[17] PhishLine, https://www.phishline.com/methods/

przekazu aby realizować kompleksowe programy uświadamiające. Z pewnością, wysokiej jakości infografiki czy plakaty mogą być skutecznym sposobem na szybkie dotarcie do dużej liczby pracowników a nie wymagają aż tak dużego nakładu pracy, jak opracowanie gry czy nakręcenie filmu. Nieskomplikowany przekaz, zawierający atrakcyjną grafikę, pobudzający wyobraźnię i zapadający w pamięć rysunek, może być skuteczny w przedstawieniu podstawowych elementów cyberbezpieczeństwa. Na przykład, ENISA proponuje zestawy plakatów[18], przedstawiających ostrzeżenia dotyczące cyberzagrożeń (Rys. 5).

Rys. 5: Plakaty uświadamiające z zakresu cyberzagrożeń (źródło: ENISA)

[18] Innovative tools for creating an engaging user awareness programme, ENISA, https://www.enisa.europa.eu/media/multimedia/material/illustrations

Skuteczny i szybki efekt w podnoszeniu świadomości można także uzyskać dostarczając prostej historii, przedstawionej w postaci komiksu, dotyczącej np. zagrożenia, jakie może spowodować użycie pendriva z niepewnego źródła (Rys. 6).



Rys. 6: Komiks dotyczący zagrożenia wynikającego z użycia zainfekowanego pendriva (źródło: ISQ)[19]

Podobny efekt uświadamiający można osiągnąć za pomocą krótkich, ciekawych animowanych filmów uświadamiających, które proponuje np. platforma cyfrowa NOVA Labs[20]. Również infografiki, jakie opracowuje np. Fundacja Bezpieczna Cyberprzestrzeń, mogą być bardzo pomocne w czerpaniu przystępnych informacji na temat np. bezpiecznego korzystania z Internetu i nowych technologii (Rys. 7).

[19] ISQ, http://isqworld.com/security-awareness-training-samples/
[20] NOVA Labs, http://www.pbs.org/wgbh/nova/labs/videos/#cybersecurity

Rys. 7: Infografika dotycząca Bezpiecznych Zakupów Świątecznych (źródło: Fundacja Bezpieczna Cyberprzestrzeń)

Natomiast, do sprawdzenia znajomości nabytej wiedzy można wykorzystać różne, dostępne on-line, quizy, np. The Weakest Link: A User Security Game[21]. Niezależnie od wyboru narzędzia uświadamiającego, niewątpliwą zaletą takich uproszczonych form edukacji jest ich łatwa dostępność, darmowość (ewentualnie niewysoki koszt), dzięki czemu mogą być one wykorzystane w każdej organizacji „od zaraz" w rozpoczęciu procesu uświadamiania.

Metody socjotechniczne stale ewoluują i stają się coraz bardziej wyrafinowane a przez to wyjątkowo skuteczne. Prawie dwie dekady minęły od pierwszej publikacji książki pt. „Sztuka podstępu. Łamałem ludzi, nie hasła" Kevina Mitnicka. Powszechny dostęp do cyfrowych technologii spowodował, że tytuł książki Mitnicka coraz bardziej odzwierciedla działania współczesnych cyberprzestępców, którzy coraz częściej ukierunkowują swoje działania w nieświadomych użytkowników a nie w zabezpieczenia technologiczne.

Do skutecznej ochrony organizacji przed cyberzagrożeniami potrzebne są zatem inwestycje zarówno w najnowsze technologie zabezpieczeń i szkolenia cyberspecjalistów[22], jak również w edukację pracowników. Pracownicy, posiadający podstawową wiedzę z zakresu cyberzagrożeń, którzy nie ulegną manipulacji, właściwie rozpoznając atak a także w porę zgłoszą go do działów bezpieczeństwa IT, mogą uchronić firmę przed poważnymi stratami, zarówno finansowymi, jak i wizerunkowymi, które mogłyby doprowadzić nawet do upadłości firmy.

Uświadamianie pracowników i tworzenie tzw. kultury cyberbezpieczeństwa (ang. *Cybersecurity Culture*) organizacji jest procesem stopniowym i długofalowym, zwłaszcza w złożonym i dynamicznym środowisku korporacyjnym. Niestety, nie ma tutaj prostych rozwiązań i efekty nie będą natychmiastowe. Większość pracowników zignoruje lub zapomni ostrzeżenia o zagrożeniach podanych na wykładzie lub zawartych w biuletynie, gdy nadejdzie moment zastosowania dostarczonych informacji i właściwej reakcji na atak socjotechniczny.

Jak spowodować, żeby szkolenia były naprawdę skuteczne, takie po których pracownik faktycznie

> TWORZENIE KULTURY CYBERBEZPIECZEŃSTWA ORGANIZACJI JEST PROCESEM STOPNIOWYM I DŁUGOFALOWYM

[21] IS Decisions, https://www.isdecisions.com/user-security-awareness/
[22] https://www.cybsecurity.org/pl/cyberpoligony-nowa-generacja-szkolen-dla-specjalistow-bezpieczenstwa-it/

zastosuje środki zabezpieczeń IT i będzie potrafił przeciwstawić się atakom socjotechnicznym? Ma na to wpływ wiele czynników. Jednym z nich jest z pewnością pomysłowość w sposobie przekazywania wiedzy i metody, które zaangażują szkolonego pracownika do czynnego udziału w szkoleniu. W tym zakresie, powstają nowe formy szkoleń, w tym rozwiązania oparte o grywalizację oraz gry wideo, które wprowadzają elementy rozrywki do procesu szkoleń. Już teraz, za najbardziej przyszłościowe i jednocześnie najpotężniejsze narzędzie edukacyjne, uważane są „poważne" gry wideo, które rozwiną się jeszcze bardziej, dzięki wprowadzeniu rzeczywistości rozszerzonej i wirtualnej (ang. *Augmented and Virtual Reality*).

Każdy z nas ma swój unikalny sposób uczenia się i przyswajania wiedzy ale istnieje ponoć prawidłowość[23], według której dorosły człowiek uczy się 10% z tego, co czyta, 20% z tego, co słyszy, 30% z tego, co widzi, 50% z tego, co zarówno widzi i słyszy, natomiast aż 90% z własnych działań. Dlatego uczenie się poprzez ćwiczenia i samodzielne rozwiązywanie problemów jest najlepszym sposobem zdobywania wiedzy i umiejętności. Pomimo powyższej reguły, stosowanie różnorodnych środków przekazu, w tym profesjonalnie opracowanych plakatów, podcastów czy filmów, może bardzo pozytywnie wpłynąć na proces przyswajania wiedzy.

Kolejnym istotnym elementem szkoleń jest przystępność informacji i jej wysoka jakość. Dlatego, w tworzeniu i przeprowadzaniu szkoleń, bardzo ważna jest rola ekspertów w dziedzinie bezpieczeństwa IT, np. etycznych hackerów, którzy znają szczegóły techniczne zagrożeń a dzięki doświadczeniu, wytłumaczą i pokażą jak należy się zabezpieczyć. Równocześnie trzeba pamiętać, że cyberbezpieczeństwo staje się dziedziną coraz bardziej interdyscyplinarną. Przygotowanie szkoleń, zwłaszcza w odniesieniu do sfery podatności na zagrożenia użytkowników, wymaga wspólnych wysiłków nie tylko specjalistów bezpieczeństwa IT, ale również ekspertów innych nauk, w tym m.in. psychologicznych, społecznych i zarządzania.

Zwłaszcza, kluczowa może okazać się rola psychologów w przygotowaniu odpowiedniego przekazu informacji. Z pewnością, zapadający w pamięć obraz z plakatu lub filmu i zapamiętane podczas szkolenia emocje, mają dużą szansę wpisać się na trwałe w umysły pracowników i przyczynić się do zwiększenia ich odporności na zagrożenia. Do emocji, które skutecznie mogą zostać wykorzystane podczas szkolenia, należą zarówno te pozytywne, np. nagroda za postępy, jak i negatywne, np. doświadczenie strachu w wyniku skasowania lub zaszyfrowania plików podczas symulowanego ataku ransomware.

Oprócz powyższych czynników, mających zasadniczy wpływ na efektywność szkoleń, niewątpliwie optymalizacja czasu szkoleniowego jest kwestią, której nie można pominąć. Ważne jest przecież, żeby nie znużyć uczestnika i nie zniechęcić go do nauki.

[23] Gordon Dryden, Jeanette Vos, „Rewolucja w uczeniu", Wyd. Zysk i S-ka, 2011.

Według raportu SANS[24] [12], największymi przeszkodami w skutecznym funkcjonowaniu programu podnoszeniu świadomości pracowników w zakresie bezpieczeństwa IT, są przede wszystkim 1) słaba komunikacja wewnątrz organizacji w tym zakresie, 2) czas poświęcony temu zagadnieniu i 3) brak zaangażowania pracowników w ten proces. Jednym z bodźców, motywującym organizacje do zmiany tej sytuacji, będzie na pewno wprowadzenie unijnego Rozporządzenia o Ochronie Danych Osobowych (RODO) w maju 2018 roku, które, miejmy nadzieję, skutecznie wpłynie na odpowiedzialne podejście do ochrony danych w organizacjach. **Jednak, przede wszystkim, budowanie dobrej atmosfery, zachęcanie pracowników do zaangażowania się w proces tworzenia cyberbezpiecznego środowiska pracy są kluczem do skuteczności programów uświadamiających i kształtowania kultury cyberbezpieczeństwa organizacji.**

Autor: Elżbieta Nowicka

Kierownik Projektu
Fundacja Bezpieczna Cyberprzestrzeń

Śledź na:
TT: @cybsecurity_org
Facebook: @FundacjaBezpiecznaCyberprzestrzen

[24] SANS, Security Awareness Report, https://securingthehuman.sans.org/media/resources/STH-SecurityAwarenessReport-2017.pdf