Co-funded by the Erasmus+ Programme of the European Union

Moduł treningowy InCyT

Bezpieczeństwo informacji dla pracowników **Część 4, Tydzień 7** **Moduł: Inżynieria społeczna**	
Zajęcia edukacyjne	❑ **Webinar** ❑ **Ćwiczenia** ❑ **Warsztaty** ❑ **Prezentacja** ❑ **Inne**
Odpowiedzialni za zajęcia	• David Sommer • Ileana Hamburg
Cele aktywności edukacyjnej	1. Techniki ataków socjotechnicznych 2. Znaczenie szkoleń z zakresu inżynierii społecznej 3. Jak chronić się przed atakami typu Phishing 4. Inżynieria społeczna w ujęciu interdyscyplinarnym
Umiejętności do zdobycia	• **TS3 Bezpieczeństwo sieci** • **TS4 Testy penetracji (luki w zabezpieczeniach)** • **SS3 Analiza poznawcza i behawioralna**
Czas trwania okresu edukacyjnego	2 tygodnie
Wymagania wstępne	***Co jest wymagane?*** • Dostęp do Internetu • Przeglądarka internetowa • MS Office365

Krótka informacja o module

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

Opis
Inżynieria społeczna jest ważnym i bardzo częstym zagrożeniem dla bezpieczeństwa informacji. Moduł ten wyjaśnia w skrócie cykl życia inżynierii społecznej, jak dochodzi do ataku i jak można mu zapobiec. W szczególności opisany jest phishing, jako jeden z najpopularniejszych ataków socjotechnicznych. Wiele firm stosuje rozwiązania techniczne, aby zapobiegać atakom, ale środki technologiczne są mało skuteczne, jeśli personel nie jest odpowiednio przeszkolony. Jest to jeden z celów tej jednostki. Uczniowie mogą uzyskać informacje na temat tych aspektów czytając odpowiedni tekst, oglądając webinaria i rozwiązując ćwiczenia we własnym tempie. Wszystkie te dokumenty znajdują się na cyfrowej interaktywnej platformie projektu. Uczestnicy mogą sprawdzić swoje odpowiedzi na ćwiczeniach samooceny. Odpowiedzi na inne ćwiczenia powinny być zapisywane na odpowiednim forum dyskusyjnym i omawiane z mentorem na wspólnym spotkaniu organizowanym raz w tygodniu. Uczniowie mogą współpracować z innymi uczniami i mentorem, szczególnie podczas spotkań. Będą wspierani w tworzeniu e-portfolio ważnego dla refleksji i oceny szkolenia.

Treść materiałów dydaktycznych

Czym jest inżynieria społeczna?

Inżynierię społeczną można zdefiniować jako manipulowanie ludźmi, najczęściej przy użyciu metod psychologicznych, w celu uzyskania dostępu do danych, dokumentów i informacji, do których atakujący nie powinien mieć dostępu. Różne formy inżynierii społecznej można było spotkać już wiele lat temu, ale ze względu na coraz szersze zastosowanie technologii w głównych aspektach biznesu i życia, zagrożenia rosną i stają się złożonym procesem trudnym do powstrzymania. Inżynieria społeczna jest obecnie jednym z głównych zagrożeń dla bezpieczeństwa informacji i stanowi skuteczną formę cyberprzestępczości. Potencjalne reperkusje udanego ataku społecznego mogą być bardzo niebezpieczne dla ludzi i organizacji. Na przykład w 2019 roku phishing, forma przestępstwa inżynierii społecznej, był odpowiedzialny za wiele naruszeń danych, więcej niż jakikolwiek inny rodzaj ataku.

Wiele ataków inżynierii społecznej spowodowały, że organizacje straciły znaczne kwoty pieniężne. Na przykład w 2020 r. straty w USA wyniosą 4,2 mld dolarów, jak podaje FBI (Abbate, 2020).

Firmy mogą doznać zakłóceń w działalności - utrata produktywności, spadek morale pracowników i trudności w odzyskaniu przez organizację sprawności. Proces ten może mieć konsekwencje, często zwalnia się zespół reagowania na incydenty, należy dostarczyć oprogramowanie zabezpieczające, które pomoże zapobiec przyszłym atakom, a pracownicy muszą zostać przekwalifikowani. Firmy,
w przypadku ataku socjotechnicznego, mogą również doznać uszczerbku na reputacji, ponieważ

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

klienci nie są przekonani, że organizacja potrafi się zabezpieczyć.

Znaczenie szkoleń z zakresu inżynierii społecznej

Ochrona przed inżynierią społeczną jest trudna, ponieważ taktyki stosowane przez atakujących opierają się na zachowaniach jednostek, a jeśli pracownicy nie mają odpowiedniego przeszkolenia w zakresie rozpoznawania ataków inżynierii społecznej, ryzyko stania się ofiarą jest ogromne.

Szkolenie z zakresu inżynierii społecznej może być włączone do programów świadomości bezpieczeństwa i daje pracownikom wiedzę i narzędzia potrzebne do rozpoznania tego typu ataków i ochrony zarówno siebie, jak i swojej organizacji (Weßelmann, 2008).

Ze względu na znaczenie szkolenia z zakresu inżynierii społecznej w minimalizowaniu zagrożeń, wiele organizacji, w szczególności MŚP, które mają mniejsze zasoby, powinno otrzymać pomoc w potraktowaniu szkolenia z zakresu świadomości cybernetycznej, w tym inżynierii społecznej, bardzo poważnie i zaoferować swoim pracownikom możliwość skorzystania z niego (Mimecast Contributing Writer, 2021).

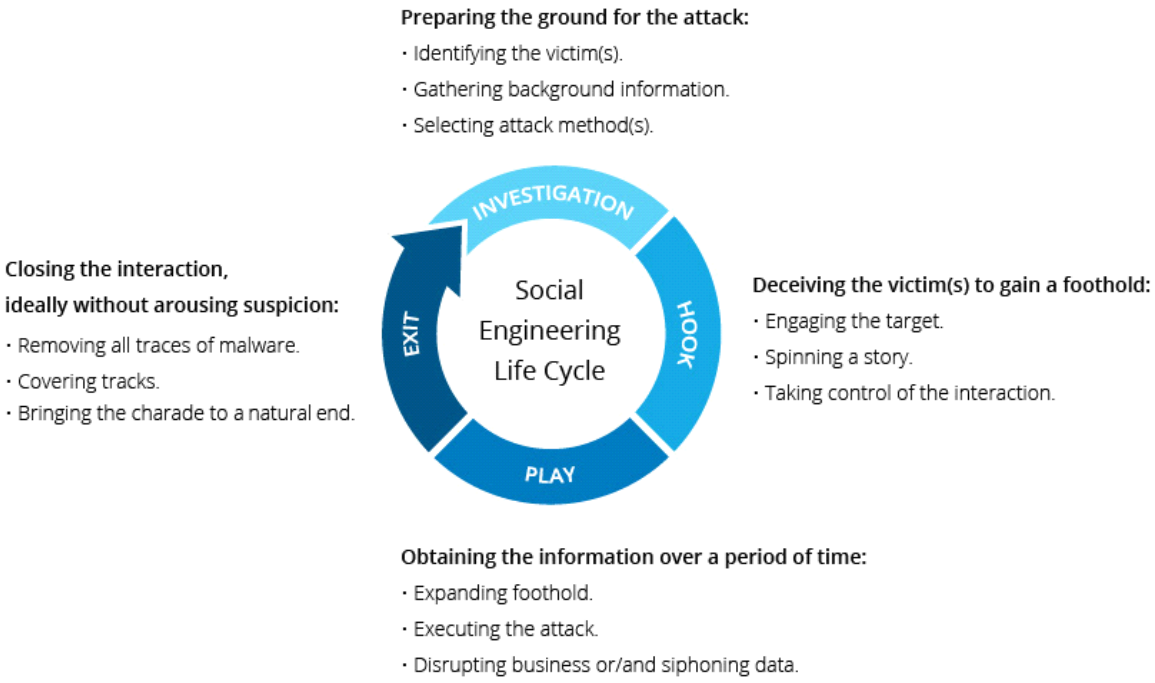
Do 2022 roku planuje się na przykład, że 60% dużych organizacji będzie rozważać świadomość bezpieczeństwa (Gartner Magic Quadrant for SAT 2019).

Cykl życia ataku socjotechnicznego

Często ataki socjotechniczne są przeprowadzane w kilku etapach. Atakujący najpierw bada ofiarę, aby zebrać niezbędne informacje, takie jak punkty wejścia i słabe protokoły bezpieczeństwa, które są potrzebne do ataku. Następnie, atakujący stara się zdobyć zaufanie ofiary i dostarczyć bodźców do działań, które zazwyczaj nie są praktykami bezpieczeństwa, takich jak udostępnienie wrażliwych informacji lub udzielenie dostępu do krytycznych zasobów. Rysunek 1 wyjaśnia cykl życia ataku.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union



Rysunek 1: Cykl trwania ataku (https://www.iacpcybercenter.org/resource-center/what-is-cyber-crime/cyber-attack-lifecycle/)

Inżynieria społeczna jest szczególnie niebezpieczna, ponieważ opiera się bardziej na błędach ludzkich, a nie na lukach w oprogramowaniu i systemach operacyjnych. Przewidzenie błędów popełnianych przez legalnych użytkowników, ich identyfikacja i powstrzymanie jest trudniejsze niż w przypadku włamania opartego na złośliwym oprogramowaniu.

Techniki ataku socjotechnicznego

Ataki socjotechniczne mają różne formy i mogą być przeprowadzane wszędzie tam, gdzie zaangażowana jest interakcja międzyludzka. Najczęstsze formy cyfrowych ataków socjotechnicznych są następujące:

Baiting

Ataki typu baiting (przynęta) starają się osiągnąć ciekawość ofiary. Wciągają użytkowników w pułapkę kradnąc ich dane osobowe lub infekując ich systemy złośliwym oprogramowaniem. Najczęściej forma przynęty wykorzystuje fizyczne nośniki do rozprzestrzeniania złośliwego oprogramowania. Na przykład, zainfekowane złośliwym oprogramowaniem pendrive'y, w widocznych miejscach, gdzie jest pewność, że potencjalne ofiary je zobaczą (np. łazienki, windy, parking docelowej firmy). Przynęta ma autentyczny wygląd, np. etykietę przedstawiającą ją jako listę płac firmy. Ofiary podnoszą przynętę i wkładają ją do komputera w pracy lub w domu, co

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

powoduje automatyczną instalację szkodliwego oprogramowania w systemie. Ataki z wykorzystaniem przynęty nie muszą być przeprowadzane w świecie fizycznym. Internetowe formy przynęty polegają na kuszących reklamach prowadzących do złośliwych stron, które zachęcają użytkowników do pobrania zainfekowanej złośliwym oprogramowaniem aplikacji.

Scareware

Ofiarami stają się fałszywe alarmy i fikcyjne zagrożenia. Użytkownicy myślą, że ich system jest zainfekowany złośliwym oprogramowaniem i muszą instalować oprogramowanie, które przynosi korzyści tylko atakującemu lub samo jest złośliwym oprogramowaniem. Scareware jest uważane za oprogramowanie zwodzące, nieuczciwe oprogramowanie skanujące. Powszechnym przykładem scareware są legalnie wyglądające banery popup we własnej przeglądarce podczas surfowania po Internecie z tekstem takim jak: "Twój komputer może być zainfekowany szkodliwymi programami spyware". Oferuje on albo instalację narzędzia (często zainfekowanego złośliwym oprogramowaniem), albo kieruje ofiarę na złośliwą stronę, gdzie własny komputer zostanie zainfekowany. Scareware jest również dystrybuowane za pośrednictwem wiadomości e-mail typu spam, w których użytkownicy są zachęcani do zakupu bezwartościowych/szkodliwych usług.

Pretexting

Atakujący uzyskuje informacje poprzez serię kłamstw. Oszustwo jest często inicjowane przez sprawcę, który udaje, że potrzebuje wrażliwych informacji od ofiary, aby wykonać krytyczne zadanie. Atakujący zwykle zaczyna od zdobycia zaufania ofiary, podszywając się pod współpracowników, policję, urzędników bankowych i podatkowych lub inne osoby, które mają prawo wiedzieć. Atakujący zadaje pytania, które są wymagane do potwierdzenia tożsamości ofiary, dzięki czemu zbiera ważne dane osobowe. Za pomocą tego oszustwa można zdobyć wiele ważnych informacji i zapisów, tj. numery ubezpieczenia społecznego, osobiste adresy i numery telefonów, bilingi, daty urlopów pracowników, zapisy bankowe, a nawet informacje dotyczące bezpieczeństwa zakładu fizycznego.

Phishing

Jest to jeden z najpopularniejszych typów ataków socjotechnicznych; oszustwa phishingowe (wyłudzenia) to wiadomości e-mail i kampanie wiadomości tekstowych mające na celu wywołanie u ofiar ciekawości lub strachu i zachęcenie ich do podania poufnych informacji, kliknięcia linków do złośliwych stron internetowych lub otwarcia załączników zawierających złośliwe oprogramowanie. Przykładem może być wiadomość e-mail wysłana do użytkowników usługi online, która ostrzega ich o naruszeniu polityki wymagającym natychmiastowego działania, np. o wymaganej zmianie hasła. Zawiera on link do nieautentycznej strony internetowej - o niemal identycznym wyglądzie jak jej legalna wersja - a użytkownik wprowadza swoje aktualne dane uwierzytelniające i nowe hasło. Informacje te są wysyłane do atakującego. Ponieważ identyczne

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

lub prawie identyczne wiadomości są wysyłane do wielu użytkowników w kampaniach phishingowych, ich wykrywanie i blokowanie jest łatwiejsze dla serwerów pocztowych mających dostęp do platform współdzielenia zagrożeń.

Spear phishing

Jest to szczególna forma ataku phishingowego, ponieważ atakujący wybiera konkretne osoby lub przedsiębiorstwa. Atakujący dostosowują swoje wiadomości do cech, stanowisk pracy i kontaktów swoich ofiar, aby ich atak był mniej widoczny. Spear phishing wymaga większego wysiłku od sprawcy (osoby popełniającej czyn zabroniony), a jego przygotowanie może zająć tygodnie i miesiące. Znacznie trudniej jest wykryć takie ataki i mają one większy współczynnik sukcesu. Przykładowo, scenariusz spear phishingu zakłada atakującego, który jako konsultant IT (istniejącej) organizacji wysyła e-mail do jednego lub kilku pracowników. Jest on podpisany dokładnie tak, jak zwykle robi to konsultant, a odbiorcy myślą, że jest to autentyczna wiadomość. Wiadomość wymaga od ofiar zmiany hasła i dostarcza im link, który przekierowuje je na złośliwą stronę, gdzie atakujący kradnie ich dane uwierzytelniające.

Wykrywanie Phishingu

Oszuści (osoby prowadzące nieuczciwe interesy) wykorzystują pocztę elektroniczną lub wiadomości tekstowe, aby oszukać osoby do przekazania ich danych osobowych. Próbują wykraść hasła, numery kont lub numery ubezpieczenia społecznego. Jeśli zdobędą te informacje, mogą uzyskać dostęp do poczty elektronicznej, banku lub innych kont. Oszuści przeprowadzają tysiące ataków phishingowych jak co dzień - i często są one skuteczne. Oszuści często aktualizują swoją taktykę, ale istnieją pewne znaki, które pomagają ofiarom rozpoznać phishingowy e-mail lub wiadomość tekstową, takie jak następujące:

- Phishingowe e-maile i wiadomości tekstowe mogą wyglądać, jakby pochodziły od firmy, którą znasz lub której ufasz. Wyglądają na pochodzące z banku, firmy obsługującej karty kredytowe, portalu społecznościowego, strony internetowej lub aplikacji do płatności online albo sklepu internetowego.
- Wiadomości e-mail i SMS-y phishingowe często opowiadają historię, aby oszukać ofiary do kliknięcia na link osoby lub otwarcia załącznika. Mogą powiedzieć, że zauważyli jakąś podejrzaną aktywność lub próby logowania, twierdzą, że jest problem z kontem lub informacjami o płatności, mówią, że osoba musi potwierdzić pewne dane osobowe, zawierają fałszywą fakturę, chcą, aby osoba kliknęła link, aby dokonać płatności, mówią, że osoba kwalifikuje się do zarejestrowania się do zwrotu rządowego itp.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Rysunek 2: Przykład phishingu (https://www.verified.org/articles/scams/netflix-phishing-emails)

Rysunek 2 przedstawia rzeczywisty przykład phishingu.

- E-mail wygląda jak od firmy, którą osoba znała, mogła i zaufała: Netflix. Użyto w nim nawet logo i nagłówka Netflixa.
- W mailu jest napisane, że własne konto jest wstrzymane z powodu problemu z rozliczeniem.
- Email ma ogólne powitanie "Hi Dear". Jeśli osoba ma konto w firmie, to prawdopodobnie nie użyłaby tak generycznego powitania.
- E-mail zaprasza osobę do kliknięcia na link, aby zaktualizować swoje dane dotyczące płatności.

Ten e-mail może wyglądać na prawdziwy, ale nie jest. Oszuści, którzy wysyłają e-maile takie jak ten, nie mają nic wspólnego z firmami, za które się podszywają. E-maile phishingowe mogą mieć realne konsekwencje dla osób, które podają oszustom swoje informacje. Mogą też zaszkodzić reputacji firm, za które się podszywają.

Ochrona przed phishingiem

Własne filtry antyspamowe potrafią utrzymać wiele wiadomości phishingowych z dala od własnej skrzynki odbiorczej. Jednak oszuści zawsze próbują przechytrzyć filtry antyspamowe, więc warto dodać dodatkowe warstwy ochrony.

Metody ochrony:

- Aby chronić własny komputer za pomocą oprogramowania zabezpieczającego, oprogramowanie powinno być aktualizowane automatycznie, aby radzić sobie

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

z zagrożeniami bezpieczeństwa.

- Aby chronić własny telefon komórkowy, oprogramowanie powinno być aktualizowane automatycznie
- W celu ochrony własnych kont należy stosować uwierzytelnianie wieloczynnikowe

Dodatkowe dane uwierzytelniające do zalogowania się na własne konto można pogrupować na:

- Kod dostępu uzyskuje się poprzez aplikację uwierzytelniającą lub klucz bezpieczeństwa.
- Skan własnego odcisku palca, siatkówki oka lub twarzy.

Wieloczynnikowe uwierzytelnianie utrudnia oszustom logowanie się na inne konta, jeśli uda im się zdobyć odpowiednią nazwę użytkownika i hasło. Ważne jest, aby chronić własne dane poprzez tworzenie kopii zapasowych, które nie są podłączone do sieci domowej. Pliki z własnego komputera powinny być kopiowane na zewnętrzny dysk twardy lub do magazynu w chmurze. Również dane z własnego telefonu powinny być kopiowane.

Postępowanie w przypadku podejrzenia ataku phishingowego

- Jeśli przychodzi e-mail lub SMS z prośbą o kliknięcie w link lub otwarcie załącznika, zapytaj: Czy mam konto w tej firmie lub znam osobę, która się ze mną skontaktowała?
- Jeśli odpowiedź brzmi "Nie", może to być oszustwo typu phishing. Należy przejrzeć wskazówki w Jak rozpoznać phishing, poszukać oznak oszustwa phishingowego, zgłosić wiadomość, a następnie ją usunąć.
- Jeśli odpowiedź brzmi "Tak", skontaktuj się z firmą, korzystając z numeru telefonu lub prawdziwej strony internetowej, nie umieszczając informacji w wiadomości e-mail, ponieważ załączniki i linki mogą zainstalować szkodliwe złośliwe oprogramowanie.

Odpowiedź na wiadomość phishingową

Istnieją konkretne kroki, które należy podjąć w oparciu o utracone informacje

- Uruchom skanowanie.
- Jeśli otrzymasz phishingową wiadomość e-mail lub SMS, zgłoś to.

Inżynieria społeczna w ujęciu interdyscyplinarnym

Dzisiejszy usieciowiony świat oraz intensywne korzystanie z Internetu i technologii są katalizatorami ataków socjotechnicznych. Zabezpieczenia systemowe są pomocne w łagodzeniu niektórych ataków inżynierii społecznej, ale to nie wystarcza. Przestępczość

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

internetowa Federalnego Biura Śledczego podkreśliła, że zwiększone wykorzystanie inżynierii społecznej i schematów oszustw z wykorzystaniem biznesowej poczty elektronicznej spowodowało miliardy dolarów strat w ciągu ostatnich kilku lat (Abbate, 2020). Ponownie metody hakerów, konieczne jest zastosowanie podejścia interdyscyplinarnego, aby zrozumieć to zjawisko i wszystkie jego złożoności, zwłaszcza w kontekście tego, jak wpływa na przedsiębiorstwa. W przeglądach literatury podkreśla się perspektywy z różnych dyscyplin: informatyki, psychologii, biznesu i etyki. Rysunek 3 ilustruje to spojrzenie (Washo, 2021).

Dyscyplina technologii informacyjnej

Inżynieria społeczna nie może być omawiana, jeśli nie w kontekście rzeczywistych systemów informatycznych i ich wykorzystania w biznesie. Obrony techniczne mogą być stosowane jako forma ograniczania ryzyka, a strategie kontroli są zalecane do stosowania. Wieloczynnikowe uwierzytelnianie jest powszechnym i często skutecznym sposobem potwierdzania przez organizacje, że osoba uzyskująca dostęp do systemów rzeczywiście powinna mieć ten dostęp. Na przykład, proces logowania za pomocą nazwy użytkownika i hasła jest jednym ze sposobów uwierzytelnienia użytkownika. Dodatkowym czynnikiem może być użycie logowania przez wirtualną sieć prywatną (VPN) w celu dalszej weryfikacji użytkownika.

Dyscyplina psychologii

Inżynieria społeczna jest związana z podstępem, więc psychologiczne podejście do zrozumienia tej koncepcji jest ważne, aby zrozumieć myśli i zachowania zarówno atakującego, jak i ofiary. Zastosowanie metod psychologicznych jest ważne dla inżynierii społecznej, ponieważ są one wykorzystywane do wspierania zabezpieczeń takich jak zapory sieciowe i systemy używane do identyfikacji intruzów (Bullee, Montoya, Pieters, Junger, & Hartel, 2018). Cała sieć informatyczna w danej firmie jest tylko tak silna, jak indywidualny użytkownik danego systemu. W rzeczywistości zachowanie i działania pracowników są jedną z wiodących przyczyn naruszeń danych.

Perspektywa biznesowa

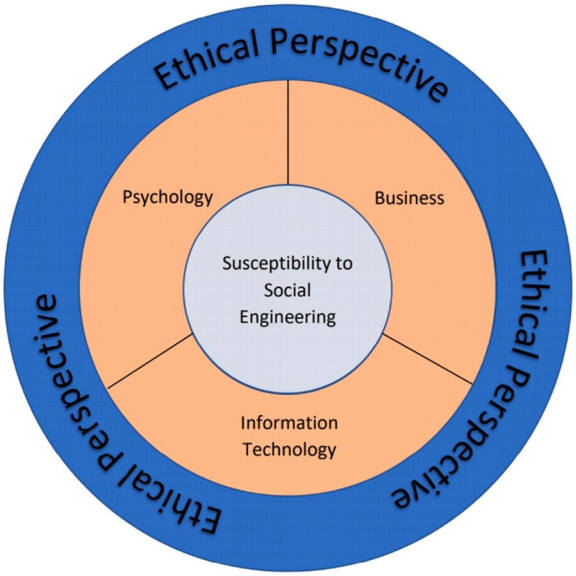
Inżynieria społeczna ma wpływ na wiele rodzajów firm i ma implikacje dla sposobu, w jaki organizacje są zorganizowane i zarządzane. Temat ten można rozpatrywać z perspektywy biznesowej, aby określić czynniki wpływające na ataki inżynierii społecznej. Ten punkt widzenia jest korzystny, jeśli dotyczy następujących obszarów działalności: szkolenia i rozwój, udokumentowane polityki, procedury audytu wewnętrznego, budżety i kultura

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

organizacyjna. Niedobór w każdym z tych obszarów może przyczynić się do ataków.

Perspektywa etyczna

Etyka jest ważna w kontekście inżynierii społecznej i związanych z nią badań na ten temat. Idea manipulowania innym człowiekiem narusza wiele zasad etycznych. W przypadku wystąpienia socjotechniki, traktowanie ofiar może być różne, ale często nie są one wystarczająco traktowane, co pozwala na przeprowadzenie ataku. Niestety, cechy zwykle spotykane u idealnych pracowników, takie jak zaufanie, chęć zadowolenia innych, takich jak kierownicy, klienci, współpracownicy i goście, oraz gotowość do posłuszeństwa wobec autorytetu, są zwykle tymi samymi cechami, które czynią jednostkę podatną na inżynierię społeczną (Mouton, Malan, Kimppa, & Venter, 2015).



Rysunek 3: Inżynieria społeczna w ujęciu interdyscyplinarnym (Washo, 2021)

Przegląd literatury z różnych dyscyplin wyjaśnia potrzebę zintegrowanego podejścia do badania złożonego tematu inżynierii społecznej. Każda dyscyplina dostarcza informacji o tym, jak rozumieć i interpretować temat, chronić się przed różnymi rodzajami ataków oraz zrozumieć wpływ inżynierii społecznej zarówno z punktu widzenia człowieka, jak i organizacji. Jednak interpretacja tematu przez każdą z dyscyplin jest użyteczna tylko wtedy, gdy jest rozpatrywana w kontekście pozostałych dyscyplin.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

Pytania:

Pytania Forum dyskusyjne, na które należy odpowiedzieć z krótkim uzasadnieniem. Odpowiedzi zostaną omówione z mentorem podczas sesji mentorskich

1. Jak rozpoznać Phishing: tj. Phishingowe e-maile i wiadomości tekstowe często opowiadają historię, aby skłonić ofiary do kliknięcia na link lub otwarcia załącznika.
2. Jak chronić się przed atakami Phishingowymi
3. Proszę wymienić kilka dyscyplin związanych z Inżynierią społeczną i krótko wyjaśnić te powiązania

Załączniki:

1. Prezentacje
2. Filmy wideo

Odnośniki:

Abbate, P., (2020). Internet Crime Report 2020
URL: (https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf)

Bullee, J., Montoya, L., Pieters, W., Junger, M., HYPERLINK "http://refhub.elsevier.com/S2451-9588(21)00074-9/sref14"&HYPERLINK "http://refhub.elsevier.com/S2451-9588(21)00074-9/sref14" Hartel, P. (2018). On the anatomy of social engineering attacks: A literature-based dissection of successful attacks. HYPERLINK "http://refhub.elsevier.com/S2451-9588(21)00074-9/sref14"Journal of Investigative Psychology and Offender Profiling, 15HYPERLINK "http://refhub.elsevier.com/S2451-9588(21)00074-9/sref14"(1), 20HYPERLINK "http://refhub.elsevier.com/S2451-9588(21)00074-9/sref14"–45.

Lee, T. (2020). Hire the Right Teachers for the Better Security Awarness. URL: https://www.gartner.com/smarterwithgartner/hire-the-right-teachers-for-better-security-awareness

Mimecast Contributing Writer (2021). Social Engineering Awarness Training for Emploeyees. URL: https://www.mimecast.com/blog/what-is-social-engineering/

Mouton, F., Malan, M., Kimppa, K., & Venter, H. (2015). Necessity for ethics in social engineering research. Computers & Security, 55, 114–127. https://doi.org/10.1016/j.HYPERLINK "https://doi.org/10.1016/j.cose.2015.09.001"cose.2015.09.001

Washo, A. (2021). An interdisciplinary view of social engineering: A call to action for research. URL: https://www.researchgate.net/publication/353448049_An_interdisciplinary_view_of_social_engineering_A_call_to_action_for_research

Weßelmann, B. (2008). Maßnahmen gegen Social Engineering: Training muss Awareness-Maßnahmen ergänzen. In: Datenschutz und Datensicherheit. DuD. 601–604.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.