Cyberdefence 24

aut. Andrzej Kozłowski 12.09.2017

EDUKACJA PODSTAWĄ SYSTEMU CYBERBEZPIECZEŃSTWA [ANALIZA]

Człowiek pozostaje najsłabszym elementem systemu cyberbezpieczeństwa i jednocześnie – najczęstszym obiektem ataków. Niezbędna jest więc systematyczna edukacja za pomocą specjalistycznych szkoleń, skierowanych zarówno do pracowników sektora prywatnego i publicznego. W innym wypadku, liczba zaawansowanych, globalnych, udanych ataków będzie stale rosnąć, stwarzając coraz większe zagrożenie finansowe oraz wizerunkowe.

Choć sieci komputerowe bazują na zaawansowanych technologiach, to błąd człowieka jest jedną z najczęstszych przyczyn udanych ataków cyberprzestępców. Kevin Mitnick, nazywany „najsłynniejszym hakerem na świecie" napisał w książce „Sztuka podstępu", że w rzeczywistości łamał ludzi, a nie hasła. Doskonale obrazuje to również aktualny mechanizm działania cyberprzestępców.

Fot. Eneas De Troya/Kevin Mitnick/CC 2.0

Do podobnych wniosków prowadzą badania przeprowadzone przez jedną z największych brokersko-doradczych firm Willis Towers Watson. Wynika z nich, że około 90 proc. udanych włamań było możliwe

dzięki błędom popełnionym przez człowieka lub niewłaściwemu, nieodpowiedzialnemu zachowaniu[1]. Dyrektorzy firm zbyt często skupiają się na inwestycjach jedynie w usprawnienia technologiczne, zapominając o edukacji wśród swoich pracowników.

Dlatego też tak istotne jest codzienne przestrzeganie tzw. cyberhigieny, czyli wykonywanie czynności takich jak używanie skomplikowanych haseł, aktualizowanie oprogramowania czy zaniechanie otwierania załączników z nieznanych źródeł. Według ekspertów, w tym brytyjskiej agencji GCHQ zajmujące się wywiadem radioelektronicznym pozwoli to na zatrzymanie nawet 90 proc. ataków hakerskich. Oczywiście, dokładna skala zatrzymanych ataków zależy od wielu innych czynników, jednak bez wątpienia stwierdzić można, że znacząca część ataków mogłaby zostać udaremniona już na etapie rozsądnej polityki bezpieczeństwa, znanej i stosowanej przez szeregowych pracowników

W 2015 roku Pentagon ucierpiał wskutek ataku phishingowego, za którym prawdopodobnie stali rosyjscy hakerzy. Udało się wykraść dane osobowe prawie 4 tysięcy pracowników wojskowych i cywilnych. Udany phishing był też przyczyną jednej z najbardziej spektakularnych operacji. W 2014 roku północnokoreańscy hakerzy zaatakowali Sony Pictures Entertainment, doprowadzając do wstrzymania emisji komedii poświęconej przywódcy Korei Północnej.

Fot. David B. Gleason/Wikimedia (CC BY-SA 2.0)

W przeciągu tylko sierpnia 2017 roku doszło do prawie 30 olbrzymich wycieków danych. Do Internetu przeniknęły między innymi odcinki popularnego serialu fantasy Gra o Tron, dane medyczne ponad miliona Brytyjczyków czy 100 tys. rekordów holenderskich kierowców. Wyciekowi danych nie potrafił też zapobiec włoski bank UniCredit. W jego wyniku ucierpiało ponad 400 tys. klientów. Na początku września z firmy Equifax wykradziono dane ponad 140 milionów Amerykanów. Dane te wystawiono na sprzedaż na forum cyberprzestępczym.

Czytaj więcej: Ogromy wyciek danych w Stanach Zjednoczonych. 150 milionów osób zagrożonych

Przykłady te pokazują znaczenie regularnego szkolenia pracowników, w szczególności w zakresie ochrony przed phishingiem i otwieraniem złośliwych załączników. Problem ten dostrzegają państwa

oraz instytucje międzynarodowe. Między innymi Europejska Agencja ds. Bezpieczeństwa Sieci i Informacji (ENISA), która na swojej stronie zamieszcza wiele materiałów poświęconych odpowiedniej edukacji pracowników[2].

Podobnie postępują władze poszczególnych państw, umieszczając kwestie zwiększania świadomości bezpieczeństwa na liście swoich priorytetów. Według rządu Wielkiej Brytanii pierwszą linię obrony w cyberprzestrzeni mają stanowić właśnie brytyjscy obywatele, świadomi czyhających na nich zagrożeń. Na ten problem zwracają uwagę w Polsce Krajowe Ramy Polityki Cyberbezpieczeństwa na lata 2017-2022 . Należy to ocenić pozytywnie, ponieważ do tej pory kwestia edukacji społeczeństwa w naszym kraju przez długi okres czas nie była traktowany z należytą powagą[3].

Firma LogicalTrust w ramach wygodnej platformy e-learningowej Securityinside proponuje atrakcyjne formy nauki o cyberzagrożeniach, przeznaczone dla osób poszukujących sposobów na zwiększenie bezpieczeństwa firm i instytucji. Za rozwiązaniem stoi solidne przygotowanie merytoryczne oraz zrozumienie potrzeb biznesowych. Eksperci LogicalTrust posiadają ponad 10-letnie doświadczenie, poparte licznymi przeprowadzonymi testami bezpieczeństwa instytucji finansowych, telekomunikacyjnych oraz rządowych. Jej przedstawiciele występują na konferencjach branżowych takich jak Secure, SEMAFOR, Confidence, OWASP, czy Internet Banking Security. Firma angażuje się też w popularyzację wiedzy na temat bezpieczeństwa wśród szeregowych internautów, m.in. prowadząc strony z informacjami na temat kolejnych ataków czy przygotowując publicznie dostępne quizy i kampanie edukacyjne.

W celu uatrakcyjnienia edukacji, firma LogicalTrust przygotowała platformę on-line pozwalającą na zaprezentowanie przystępnych formatów i atrakcyjnych wizualnie filmów. Umożliwia to skuteczniejsze zwiększenie świadomości pracowników z zakresu zagadnień bezpieczeństwa IT.

Program szkoleniowy zaprezentowany przez LogicalTrust obejmuje następując zagadnienia: hasła, kwestie phishingu, bezpieczeństwo urządzeń mobilnych, fałszywe załączniki, wycieki informacji i sieci bezprzewodowe.

Pomimo coraz nowszych i zaawansowanych metod uwierzytelnia, wciąż dominującym sposobem na zabezpieczenie swoich zasobów jest stosowanie haseł. Użytkownicy popełniają jednak w tym procesie liczne błędy, przez co narażają się na utratę cennych danych czy nawet pieniędzy. Pierwsza przyczyna leży w zbyt prostych hasłach, które albo nawiązują do osobistych informacji, które łatwo można wyśledzić w Internecie, albo do najprostszych, łatwych do zapamiętana formułek jak „123456789” czy „qwerty”. Coroczne rankingi najpopularniejszych haseł od lat potwierdzają ten negatywny trend[4].

Często użytkownicy dążą do uzyskania prostych i wygodnych rozwiązań, pozostawiając bezpieczeństwo na dalszym planie. Dlatego LogicalTrust stawia na wyjaśnienie znaczenia silnego hasła oraz na aspekt praktyczny, czyli jak tworzyć i zapamiętywać liczne, skomplikowane hasła. Wbrew pozorom, stworzenie trudnego do złamania, a łatwego do zapamiętania hasła nie wymaga nadmiernego wysiłku.

Drugim elementem programu jest ochrona przed phishingiem.

Lekcja omawia problem pozyskiwania poufnych danych uwierzytelniających użytkownika, takich jak login i hasło, za pomocą fałszywych wiadomości e-mail oraz stron WWW. Uczy się zwracać uwagę na drobne elementy, które pozwolą zidentyfikować fałszywkę oraz nie dopuścić do przekazania poufnych danych atakującemu. CERT Polska w swoim raporcie o stanie bezpieczeństwa polskiego Internetu z 2016 zwraca uwagę na zagrożenie związane z podszywaniem się pod m.in. firmy komornicze, operatorów telekomunikacyjnych czy kancelarie komornicze[5].

Trzecim elementem szkolenia jest bezpieczeństwo urządzeń mobilnych. Już w 2014 roku, liczba ich użytkowników przekroczyła liczbę użytkowników laptopów, dlatego też ich zabezpieczenie jest tak istotne. Dzisiaj służą nam one do przelewów bankowych, jako forma identyfikacji oraz umożliwiają dostęp do danych na Facebooku czy poczcie elektronicznej. Jednocześnie jednak, wraz z liczbą dostępnych urządzeń, pojawią się nowe, coraz bardziej zaawansowane, złośliwe programy.

Fot. domena publiczna / pixabay CC0

W 2016 roku według Kaspersky Lab odnotowano pojawienie się ponad 8 milionów różnego rodzaju złośliwego oprogramowania. To 3 razy więcej niż w 2015 roku[6]. Szkolenie SecurityInside oferuje sposoby rozpoznania złośliwych aplikacji.

Czwarty element szkolenia SecurityInside uwzględnia sposoby zwalczania fałszywych załączników. Bardzo często ta forma wykorzystywana jest w atakach phishingowych i spearphishingowych, gdzie hakerzy wysyłają zainfekowane pliki w spreparowanych wiadomościach. Szkolenie pokazuje, jak rozpoznać zainfekowany załącznik, wyjaśnia, dlaczego instalacja programu antywirusowego nie oznacza stuprocentowej ochrony, ale też przedstawia kroki, które należy podjąć, jeżeli nieumyślnie otworzymy niebezpieczny plik.

Następne elementy szkolenia oferowane przez LogicalTrust obejmują przeciwdziałanie wyciekowi danych i informacji. Podczas analizy zagrożeń problem ten jest często pomijany, a eksperci skupiają się na zagrożeniach pochodzących z zewnątrz. Tymczasem pracownicy danego podmiotu działający „z wewnątrz" ujawniający dane są bardzo częstym źródłem przecieków.

Najbardziej znane nazwiska w tym kontekście to Edward Snowden czy Bradley Manning, którzy ujawnili chronione dane władz USA. To samo zagrożenie dotyczy jednak firm czy instytucji prywatnych. W ramach oferty szkolenia eksperci z LogicalTrust będą dążyć do identyfikacji najpopularniejszych źródeł wycieku poufnych informacji oraz informować o potencjalnych skutkach

ujawnienia nieistotnych danych. Jak można wykorzystać takie dane opisał wspomniany już Kevin Mitnick na łamach swojej książki. Pozyskiwanie informacji, które z punktu widzenia osób, które je ujawniały były nieistotne, umożliwiały mu dokonanie włamań do licznych instytucji i przedsiębiorstw.

Czytaj też: Największy sukces rosyjskiego wywiadu: Edward Snowden?

Ostatni punkt szkolenia obejmuje sieci bezprzewodowe i ich bezpieczną konfigurację. Sieć Wi-Fi wykorzystywana jest przez pracowników na co dzień, nie tylko w domu czy biurze, ale i w kawiarniach, na dworcach czy w centrach miast. Często jednak użytkownicy zapominają o podstawowych środkach bezpieczeństwa, podczas łączenia się z nową siecią. Za każdym razem, robiąc zakupy online przy pomocy karty kredytowej, zlecając przelewy bankowe czy logując się do swojej skrzynki pocztowej są przecież narażeni na przechwycenie wpisywanych danych uwierzytelniających przez cyberprzestępców, potrafiących podszyć się pod pozornie bezpieczną sieć publiczną. Z tego powodu LogicalTrust przygotowało propozycję lekcji również w tym zakresie.

Czytaj też: Świadomość zagrożenia, to fundament cyberbezpieczeństwa [ANALIZA]

Z oferty szkoleń LogicalTrust skorzystały już takie firmy jak Credit Agricole, Getin Bank, Szkoła Głowna Handlowa, czy PLAY. Platforma e-learningowa to narzędzie służące do monitorowania edukacji nawet większych grup pracowników – wszystkie moduły szkoleń umożliwiają pomiar efektów prowadzonych zajęć, co pozwala błyskawicznie ocenić ich skuteczność.

Fot.Գեղամ Վարդանյան/Wikipedia Commons/ CC 4.0

Wszystko wskazuje na to, że w przyszłości, wraz ze wzrostem zastosowania technologii informatycznych, zakres zagrożeń dla pracowników instytucji państwowych i prywatnych będzie rosnąć. Kluczowym elementem cyberbezpieczeństwa pozostanie jednak człowiek. Z tego względu kluczowe znaczenie ma i będzie jego odpowiednia edukacja. Pozwala ona na znaczące zmniejszenie ryzyka utraty danych, czy nawet poważnych strat finansowych.

Dla naszych czytelników firma LogicalTrust przygotowała 10% rabat na usługę e-learningu: Kod: CEGEEPHAE. Rabat obowiązuje do 31 października.

Artykuł przygotowano we współpracy Redakcji Defence24.pl i firmy LogicalTrust.

---

[1] Effective Cybersecurity Strategy Rests on People, Not Just Technology, http://www.insurancejournal.com/news/national/2017/03/01/443270.htm

[2] Information Security awareness material, https://www.enisa.europa.eu/media/multimedia/material

[3] Krajowe ramy polityki cyberbezpieczenstwa rzeczypospolitej polskiej na lata 2017-2022, http://m.mc.gov.pl/files/krajowe_ramy_polityki_cyberbezpieczenstwa_rzeczypospolitej_polskiej_na_lata_2017_-_2022.pdf

[4] The world's most common passwords revealed: Are you using them?, http://www.telegraph.co.uk/technology/2017/01/16/worlds-common-passwords-revealed-using/

[5] *Krajobraz bezpieczeństwa polskiego Internetu w 2016 roku*, https://www.cert.pl/news/single/krajobraz-bezpieczenstwa-polskiego-internetu-2016-roku/

[6] *Report: 2016 saw 8.5 million mobile malware attacks, ransomware and IoT threats on the rise*, http://www.techrepublic.com/article/report-2016-saw-8-5-million-mobile-malware-attacks-ransomware-and-iot-threats-on-the-rise/