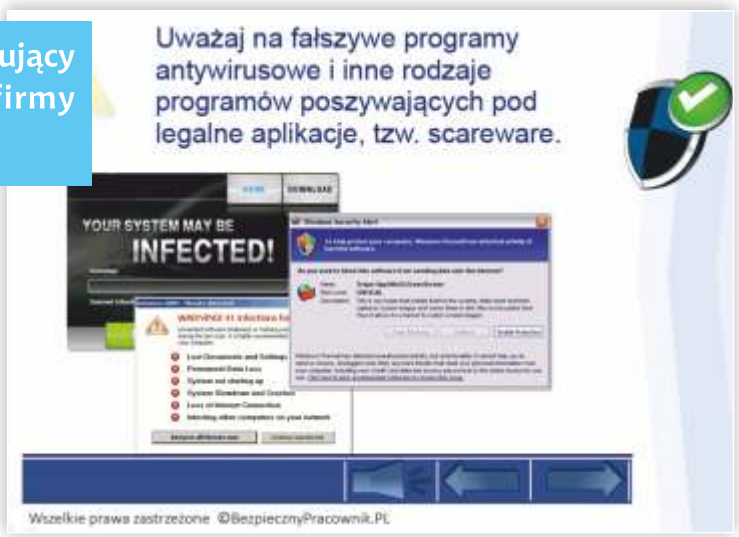
Szkolenia e-learningowe
Security Awareness

Obecnie zdecydowana większość incydentów bezpieczeństwa w systemach informatycznych jest rezultatem wykorzystania najsłabszego elementu - użytkowników. Zabezpieczenia techniczne nie mogą skutecznie ochronić systemów bez jednoczesnego przeszkolenia pracowników w zakresie bezpieczeństwa eksploatacji.
Każdy pracownik firmy powinien być przygotowany na zagrożenia wynikające z korzystania z usług internetowych. Wiedza i umiejętności pracowników powinny być regularnie odświeżane i aktualizowane. Jednakże w praktyce nie jest możliwe organizowanie tradycyjnych, stacjonarnych szkoleń dla wszystkich pracowników firmy. Rozwiązaniem są nowoczesne szkolenia e-learningowe z dziedziny "Security awareness".

Pracownicy świadomi zagrożeń, znający i stosujący zasady bezpieczeństwa stanowią dla firmy najskuteczniejszą metodę ochrony!



Oferowane w interaktywnej formie e-learningowej szkolenie Security Awareness to:

- Lekcje opracowane w języku polskim w sposób zrozumiały dla każdego pracownika.
- Treść materiałów szkoleniowych i metody przekazu dostosowane do mentalności i kultury polskich organizacji.
- Przykłady praktyczne opracowane na podstawie doświadczeń z rzeczywistych audytów bezpieczeństwa w polskich przedsiębiorstwach.
- Opracowana w ciekawy sposób, animowana forma szkolenia sprawia, że uczestnicy z dużym zaangażowaniem biorą udział w zajęciach.
- Materiał pokrywa wszystkie istotne zagrożenia, na jakie narażeni są pracownicy firm korzystający z Internetu.
- Materiały kursu e-learning są regularnie aktualizowane o nowe zagrożenia Internetu.
- Zajęcia kładą nacisk na praktyczne umiejętności rozpoznawania zagrożeń i podejmowania właściwych zachowań.
- Materiał podzielony na krótkie 5-10 minutowe lekcje. Pracownicy mogą odbywać zajęcia z dowolnego miejsca,
- Ścieżka audio nagrana przez zawodowego aktora.
- Interaktywne lekcje e-learningowe dostosowują projekcje materiału do preferencji, zdolności i umiejętności osób uczących się.
- Intuicyjny interfejs graficzny umożliwia odbycie szkolenia bez wstępnego przygotowania.
- Wbudowany w kurs e-learning interaktywny system podpowiedzi sprawia, że każda osoba bez względu na wykształcenie odbywa szkolenie z pełnym zrozumieniem prezentowanych pojęć i terminów.

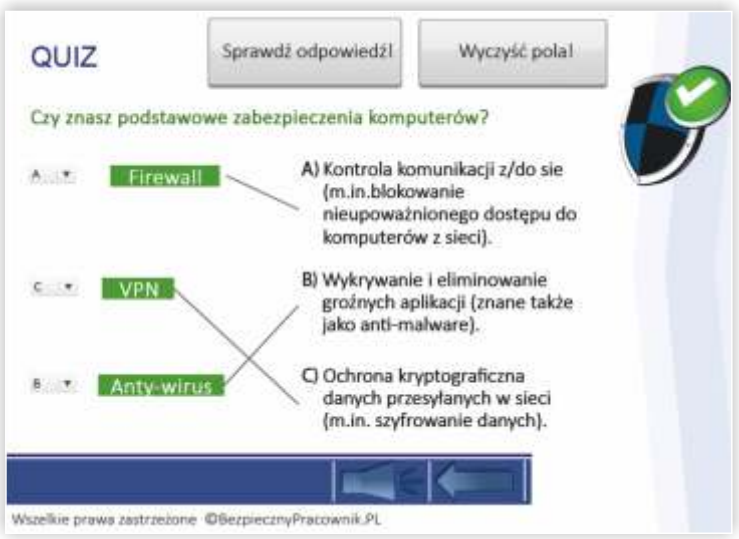
- Dzięki animacjom, quizom i pytaniom kontrolnym osoby uczące się biorą czynny udział w zajęciach e-learningowych.
- Adaptacyjny program nauczania na bieżąco dostosowuje prezentowany materiał do stanu wiedzy osób uczących się - w razie problemów z przyswajaniem wiedzy w sposób dynamiczny dodawane są lekcje uzupełniające.
- Uczestnicy zajęć sami decydują o tempie projekcji szkolenia - w dowolnym momencie mogą przerwać i później powrócić do kursu, jak również zapoznać się z wcześniej prezentowanym materiałem.
- Na życzenie materiał szkolenia może być rozszerzany i dostosowywany do specyficznych potrzeb.
- Firmy posiadają aktualne informacje na temat stanu i postępów kształcenia wszystkich swoich pracowników.

Edukacja pracowników redukuje ryzyko i zapobiega zagrożeniom, które nie mogą być zaadresowane za pomocą sprzętu ani oprogramowania.

Dla banków i instytucji finansowych:

Wymagania dotyczące zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w bankach określa „Rekomendacja D" wydana przez Komisję Nadzoru Finansowego. W 2013 roku została dokonana aktualizacja Rekomendacji (z 2002 r.), która wynika ze znacznego rozwoju technologicznego oraz systematycznego wzrostu znaczenia obszaru technologii informacyjnej dla działalności banków, jak również z pojawienia się nowych zagrożeń w tym zakresie. Utrzymanie bezpieczeństwa jest możliwe przez zastosowanie odpowiednich środków ochrony oraz rozwijanie kultury bezpieczeństwa informacji w skali całej organizacji poprzez tzw. program Security Awareness.

Sekcja: Podział obowiązków, Punkt: 5.4
- Bank powinien stosować adekwatne formy szkoleń, zapewniać właściwe materiały, jak również prowadzić różnorodne akcje edukacyjne mające na celu podniesienie kultury bezpieczeństwa informacji.



Sekcja: Architektura infrastruktury teleinformatycznej, Punkt: 9.7
- W ramach prowadzenia edukacji pracowników bank powinien uwzględniać m.in. zagrożenia związane z korzystaniem z urządzeń mobilnych, korzystaniem z własnego sprzętu informatycznego w celach zawodowych oraz korzystaniem ze sprzętu służbowego w celach prywatnych, publikowaniem przez pracowników informacji dotyczących banku w Internecie (w szczególności na portalach społecznościowych) oraz z atakami socjotechnicznymi (…)

CC Otwarte Systemy Komputerowe Sp. z o.o.

ul. Rakowiecka 36, 02-532 Warszawa
tel. +48 22 646-68-73; fax +48 22 606-37-80
e-mail: office@cc.com.pl

Więcej informacji znajdziecie Państwo w Internecie, na stronach:
http://www.cc.com.pl/

Kontakt:
Dział Techniczny: tech@cc.com.pl
Dział Handlowy: sales@cc.com.pl