Razem możemy WIĘCEJ

Partner merytoryczny:

ZAUFANA TRZECIA STRONA.PL

WARSZTAT

Cyberbezpieczeństwo w banku spółdzielczym – jak bronić się przed atakami na banki i ich klientów

Organizowane przez:

Krajowy Związek Banków Spółdzielczych

Data:

2 grudnia 2019 r.

Miejsce:

Centrum Konferencyjne Ogrodowa 58 przy ul. Ogrodowej 58 w Warszawie.

09:30 – 10:00	**Rejestracja uczestników**
10:00 – 12:00	**Wykład cz. I**
12:00 – 12:15	**Przerwa kawowa**
12:15 – 14:15	**Wykład cz. II**
14:15 – 15:00	**Lunch**

PROGRAM:

1. **Studium przypadku ataku na bank spółdzielczy.**

W opisywanym incydencie sprawcy za pomocą manipulacji doprowadzili pracownicę banku do przekazania im 30 000 PLN. Przedstawimy metody działania sprawców i wskazówki, jak przeciwdziałać takim atakom.

2. **Studium przypadku ataku na klienta banku spółdzielczego.**

W tej analizie ataku pokażemy, jak przejmując kontrolę nad komputerem jednego z klientów banku sprawcy doprowadzili do kradzieży znacznej sumy środków z konta klienta. Zastanowimy się nad mechanizmami umożliwiającymi wczesne wykrywanie analogicznych ataków.

3. **Ataki „na prezesa".**

W tym module przedstawionych zostanie kilka prawdziwych ataków na polskie firmy, w których przestępcy, pisząc emaile lub dzwoniąc, skutecznie podszyli się pod przełożonych, by nakłonić podwładnych do zrealizowania przelewów pod zmyślonymi pretekstami. Pokazujemy, jak obronić się przed takim podstępem.

4. **Ataki na procesy finansowe**.

W tym module opisujemy wiele różnych ataków, które polegały na modyfikacji procesu płatności poprzez podszycie się pod dostawcę i zmianę sposobu płatności lub rachunku, na który miał trafić przelew. Wskazanie, jak zorganizować firmowe procesy, by były odporne na to zagrożenie.

5. **Złośliwe oprogramowanie**.

W tym module omówione zostaną historie użytkowników, którzy zarazili swoje komputery i pokazane będą skutki takich infekcji. Wytłumaczony zostanie sposób, w jaki doszło do incydentu i co można robić, by ograniczyć takie ryzyko na swoim komputerze.

6. **Bezpieczeństwo aplikacji mobilnych.**

W tej części pokazane zostaną ryzyka czające się w sklepach z aplikacjami na smartfony. Tłumaczymy, jak odróżnić dobrą aplikację od niebezpiecznej i pokazujemy, jakie mogą być skutki zainfekowania smartfona.

7. **Fałszywe strony banków.**

W tym module zademonstrowane będą liczne przykłady ataków na klientów bankowości elektronicznej wraz ze wskazaniem, jak wyglądają fałszywe witryny banków, jak wygląda proces oszustwa krok po kroku wraz z informacją, jak można rozpoznać atak przestępców.

8. **Ataki Dotpay/PayU**.

W tej części szkolenia pokazany zostanie najczęściej obecnie spotykany mechanizm internetowego oszustwa, wykorzystujący fałszywe witryny pośredników szybkich płatności. Opowiadamy o wielu wariantach tego oszustwa, jednocześnie ucząc, jak uniknąć oddania danych swojego rachunku bankowego przestępcom.

9. **Jak nie zostać słupem**.

To moduł, w którym przedstawione zostaną techniki używane przez przestępców do rekrutowania osób, których rachunki bankowe zostaną użyte do przestępstwa. Ostrzegamy przed zbyt dobrymi ofertami pracy i opowiadamy o konsekwencjach, które czekają na mniej uważne ofiary.

10. **Bezpieczne transakcje na Allegro i OLX.**

W tym module opisane będą najpopularniejsze scenariusze oszustwa w ww. serwisach. Pokazujemy, jak można paść ofiarą wyłudzenia zarówno jako kupujący, jak i sprzedający. Radzimy także, jak weryfikować oferty.

11. **Bezpieczny Facebook.**

To moduł omawiający najpopularniejsze oszustwa w tym serwisie - konkursy, fałszywe wiadomości czy wyłudzenia kodów BLIK. Na przykładzie prawdziwych historii pokazujemy, jak łatwo można paść ofiarą przestępców i uczymy, jak rozpoznać, że rozmawiamy ze złodziejem.

12. **Jak rozpoznać złośliwego emaila.**

Ten moduł poświęcamy nauce rozpoznawania złośliwych wiadomości. Na licznych przykładach pokazane zostaną krok po kroku, jakie elementy warto zweryfikować i na co zwrócić uwagę, by odróżnić wiadomość prawdziwą od fałszywej.

13. **Jak rozpoznać załącznik**.

W tej części pokazujemy, jak mogą wyglądać złośliwe załączniki nawet, gdy udają niewinne dokumenty z programów biurowych. Na przykładach uczymy, na co zwracać uwagę i w co nie klikać, by nie zarazić swojego komputera.

INFORMACJA O OSOBIE PROWADZĄCEJ:

Dominik Rozdziałowski

Doświadczony trener, uznany prelegent wielu branżowych konferencji. Biegły Sądowy z pięciu dziedzin przy Sądzie Okręgowym w Kielcach. Wieloletni funkcjonariusz pionu do walki z przestępczością gospodarczą, następnie Naczelnik Wydziału do Walki z Cyberprzestępczością Komendy Wojewódzkiej Policji w Kielcach. Absolwent Wyższej Szkoły Ekonomii i Prawa na kierunku Informatyka w ekonomii oraz Wyższej Szkoły Handlowej w Kielcach na kierunku elektronika i telekomunikacja. Posiada niezwykle szerokie doświadczenie w zwalczaniu cyberprzestępczości oraz duży talent do edukowania słuchaczy w przystępny i atrakcyjny sposób. Jego prezentacje zyskują bardzo dobre oceny na największych polskich konferencjach poświęconych bezpieczeństwu.