CYBERBEZPIECZEŃSTWO

BEZPIECZEŃSTWO

Bezpieczeństwo jest to stan systemu informatycznego, w którym poziom ryzyka jego aplikacji jest zredukowany do akceptowalnego poziomu, poprzez zastosowanie odpowiednich środków.

CYBERTERRORYZM

- Ośmieszenie
- Zdobycie informacji zastrzeżonych
- Wyłączenie systemów informacyjnych
- Fizyczne uszkodzenie

RODZAJE ATAKÓW

- Phishing
- Man in the middle; sniffin i spoofing
- Socjotechnika
- Deface
- Smishing
- Wirusy i pokrewne
- Błąd oprogramowania

PHISHING

odnosi się do procesu zbierania (kradzieży) danych przez przestępców.

PHISHING

W typowym ataku phishingowym cyberprzestępca tworzy **prawie idealną replikę strony WWW** dowolnej instytucji lub portalu.

Następnie przy użyciu **technik spamowych** wysyłane są wiadomości e- mail imitujące prawdziwą korespondencję wysyłaną przez różne instytucje.

Wszystkie takie wiadomości mają jeden cel: **nakłonienie odbiorców do kliknięcia zawartego w liście odsyłacza.**

Stworzone przez phisherów odsyłacze kierują użytkowników bezpośrednio do fałszywej strony WWW, na której "schwytana ryba" wprowadza poufne informacje

odblokuj-aliegro.80.pl

kartki internetowe wypracowania, sciagi darmowe domeny darmowe liczniki na strone www

allegro

Aby odblokować Twoje konto w Allegro wyślij SMS o treści SKT na nr 73070
z numeru telefonu przypisanego do Twojego konta.

Lub zeskanuj kod:

Ponieważ wykryto włamanie, powyższy krok jest niezbędny do zweryfikowania czy jesteś właścicielem konta.
(Koszt wysłania wiadomości SMS wg. stawki operatora (0,55PLN))
Po wysłaniu wiadomości wpisz kod do formularza i kliknij "Odblokuj Konto" aby odblokować Twoje konto allegro.

Podaj Kod SMS:

Kod SMS:

Odblokuj konto

Drogi Uzytkowniku

Ta wiadomosc zostala do Ciebie automatycznie, przez system rozpoznawania niebezpieczenstw platformy allegro.

Dnia 29-04-2015 wykryto nieautoryzowany dostep do Twojego konta w portalu. W zwiazku z wykrytym niebezpieczenstwem Twoje konto zotalo tymczasowo zawieszone.
Aby odbokowac swoje konto przejdz pod adres : http://odblokuj.allegro.pl?6846713

Grupa Allegro Sp. z o.o.
ul. Grunwaldzka 182
60-166 Poznan

Poczta Polska

Kurier nie dostarczył przesyłkę do numeru zgłoszenia **RR6536886973PL** na adres **05.07.2015**, ponieważ nikt w tym czasie. Proszę zobaczyć informacje na temat wysyłki, drukowania i iść na pocztę, aby otrzymać pakiet.

Zobacz informacje

Uwaga

Jeżeli przesyłka nie dotrze w ciągu 7 dni roboczych Poczta Polska będzie miała prawo do ubiegania się koszty utrzymania przesyłka 50 zł za jeden dzień. Dziękujemy za korzystanie z naszych usług dostawy. Życząc miłego dnia Twoja Poczta Polska.

Phishing z wykorzystaniem mediów społecznościowych to rodzaj ataku przeprowadzany za pośrednictwem takich platform, jak Instagram, LinkedIn, Facebook lub Twitter. **Celem takiego ataku jest kradzież danych osobowych lub przejęcie kontroli nad kontem w mediach społecznościowych.**

PHISHING METODY OCHRONY

FORMA – niechlujna

TREŚĆ – alarmująca, nakazowa, ofertowa

NADAWCA – nieznany, podszywający się

ODNOŚNIKI - inna nazwa, inne miejsce docelowe

Smishing = atak przez SMS

17:33

[redacted]

Aktywny(a) teraz

[redacted]

Jesteście znajomymi na Facebooku

Mieszka w: Tymowa, Tarnow, Poland

Pracuje w: Straż Pożarna

16:41

Hej Katarzyna jak masz chwile możesz odebrać sobie bon na zakupy do Rosmann na stronie przezent-rossman.24.eu To nowa akcja świąteczna sklepu i można wygrać 2000zł, ale zostało już tylko kilka sztuk do zgarniecia, powodzenia!

Aa

[redacted]

Aktywny(a) teraz

[redacted]

Jesteście znajomymi na Facebooku

Mieszka w: Kraków

22:19

mam pytanie moze ty znasz tego chlopaka na zdjeciu , wypisuje do mnie i twierdzi ze zna ciebie ? znasz go

http://facebok-profile65241445996.5v.pl

Naciśnij i przytrzymaj ☺, aby zareagować

18:33

[redacted]

[redacted]

Jesteście znajomymi na Facebooku

Mieszka w: Bochnia

adwokat w: Kancelaria Adwokacka

06.12, 18:42

Hej Katarzyna! Przeczytaj zanim usuną przechwycone-zdjecia.eu

06.12, 19:07

Wirus uwaga nie klikać

Aa

SOCJOTECHNIKA

Zestaw metod mających na celu uzyskanie niejawnych informacji przez cyberprzestępcę.

Hackerzy często wykorzystują niewiedzę bądź łatwowierność użytkowników systemów informatycznych, aby pokonać zabezpieczenia odporne na wszelkie formy ataku.

Wyszukują przy tym najsłabszy punkt systemu bezpieczeństwa, którym najczęściej jest człowiek.

METODY ATAKU SOCJOTECHNICZNEGO

- Z pozoru nieszkodliwa informacja
- Czasem wystarczy po prostu poprosić
- Budowanie zaufania
- Może pomóc?
- Potrzebuję pomocy
- Współczucie, wina i zastraszenie

JAK WYGLĄDA ATAK?

Udawanie pracownika tej samej firmy.

Udawanie przedstawiciela dostawcy, firmy partnerskiej lub agencji rządowej.

Udawanie kogoś, kto ma władzę.

Udawanie nowego pracownika proszącego o pomoc.

Udawanie przedstawiciela producenta systemu operacyjnego zalecającego pilną aktualizację.

Oferowanie pomocy w razie wystąpienia jakiegoś problemu.

Podrzucenie w okolicach stanowiska pracy ofiary dyskietki lub płyty CD-ROM zawierającej niebezpieczny kod.

Używanie wewnętrznej terminologii i żargonu w celu zbudowania zaufania.

Podrzucenie dokumentu lub pliku w pomieszczeniu poczty wewnętrznej firmy, aby dotarł do miejsca przeznaczenia jako korespondencja wewnętrzna.

ATAK- ZNAKI OSTRZEGAWCZE

- Odmowa podania numeru zwrotnego.
- Nietypowa prośba.
- Okazywanie posiadania władzy.
- Podkreślanie pilności sprawy.
- Grożenie konsekwencjami niepodporządkowania się prośbie.
- Okazywanie niechęci w przypadku zadawania pytań.
- Wymienianie wielu nazwisk.
- Komplementy lub pochlebstwa.
- Flirtowanie.

MAN-IN-THE-MIDDLE

- Przerwanie przesyłania danych – informacja nie dociera do odbiorcy

- Przechwycenie danych – informacja dochodzi do odbiorcy, ale odczytuje ją również strona trzecia

- Modyfikacja danych – informacja zostaje przejęta, zmodyfikowana i w fałszywej postaci dostarczona do odbiorcy

MAN-IN-THE-MIDDLE

Każde podłączenie niezaufanego sprzętu do komputera może skutkować atakiem MIM

Ataki MIM:

Kopiowanie numeru

konta bankowego

Atak na karty zbliżeniowe

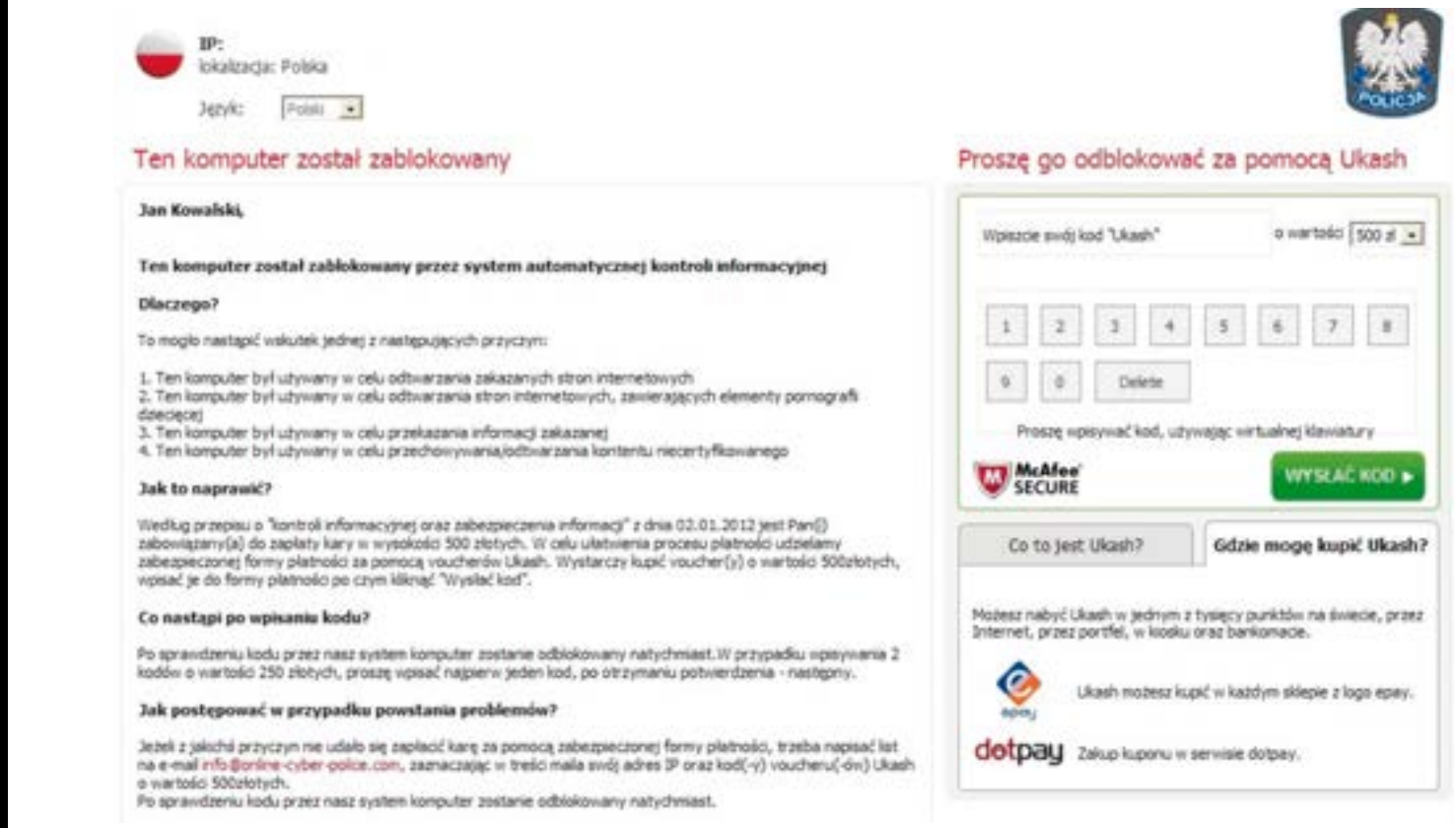
MAN-IN-THE-MIDDLE – JAK SIĘ CHRONIĆ?

Inne kanały komunikacyjne	Potwierdzenie wiadomości	Bezpieczny podpis	Zdrowy rozsądek
• Telefon • Kontakt bezpośredni	• E-mail zwrotny	• Algorytmy komputerowe zapewniające tożsamość nadawcy	• Publiczna infrastruktura jest niebezpieczna

DEFACE

- „Oczernienie” jest typowym atakiem na stronę internetową zmieniającą jej wygląd zewnętrzny. Zwykle jest skutkiem ataku osób mniej obeznanych technicznie, nowicjuszy w świecie hackerskim.

WIRUSY I POKREWNE



WIRUSY I POKREWNE – METODY OCHRONY

- Antywirusy
- Firewalle (Zapory)
- Poprawki systemowe