TEMAT:

CYBERBEZPIECZEŃSTWO CZ.2

Botnet

Grupa komputerów zainfekowanych szkodliwym oprogramowaniem, które umożliwia atakującemu kontrolę nad nimi.

Komputer zombie

Komputery wchodzące w skład botnetu.

Właściciel urządzenia nie jest świadomy, że jest on wykorzystywany przez kogoś innego np. do rozsyłania spamu lub przeprowadzania ataków w sieci.

Podsłuch sieciowy (ang. Sniffing)

Przechwytywanie danych transmitowanymi w sieci.

Przykłady:
- dane osobowe
- dane logowania
- dane do e-usług

Podręcznik Rys. 10.1. str. 154

Phishing – typ oszustwa internetowego

Cel – wyłudzenie od użytkownika jego danych

Poprzez:
- bank
- urząd
- pocztę
- podmiot świadczący e-usługę

Phishing – jak to działa

Phishing - przykład

From: Kundenservice DHL Logistik [mailto:stegnitz@silometal.sk]
Sent: Wednesday, May 20, 2015 9:56 AM
To:
Subject: Obecny stan przesyłki DHL

Sledzenie trasy przesyłki DHL

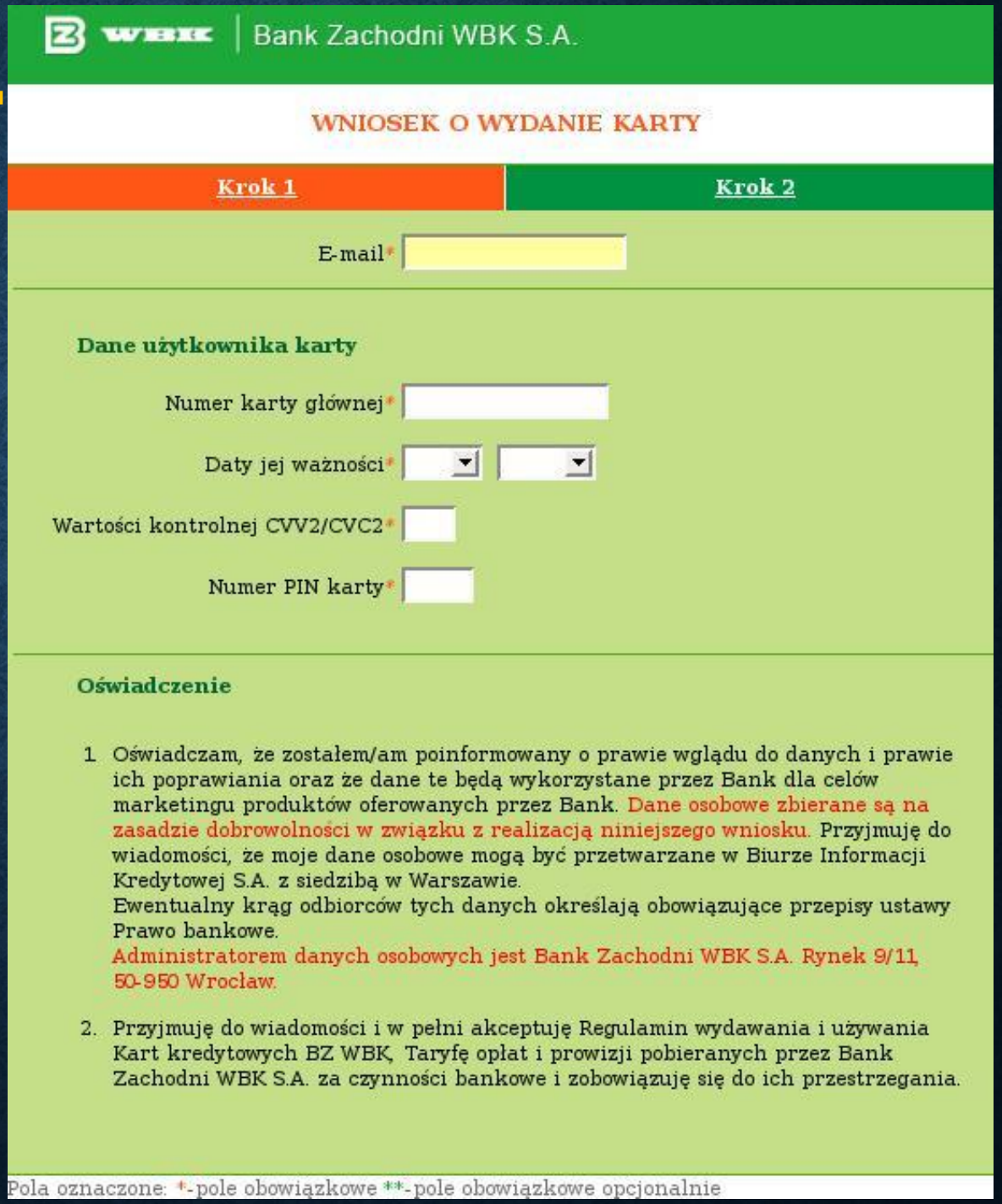
DHL Sendungsverfolgung

Numer przesyłki	49177414936436
Produkt / serwis	DHL RETOURE
Status od środa, 20.05.2015 07:55:19	Przesyłka jest przygotowywana w początkowym centrum pakowania.
Doreczono do	Przesyłka zwrotna do nadawcy

http://www.cetil.com.uy/4if30oexj8y
Kliknij, aby śledzić łącze

Sprawdź informacje od odbiorcy
(ZIP Format)

Phishing – przykład



Bank Zachodni WBK S.A.

WNIOSEK O WYDANIE KARTY

Krok 1 | Krok 2

E-mail*

Dane użytkownika karty

Numer karty głównej*

Daty jej ważności*

Wartości kontrolnej CVV2/CVC2*

Numer PIN karty*

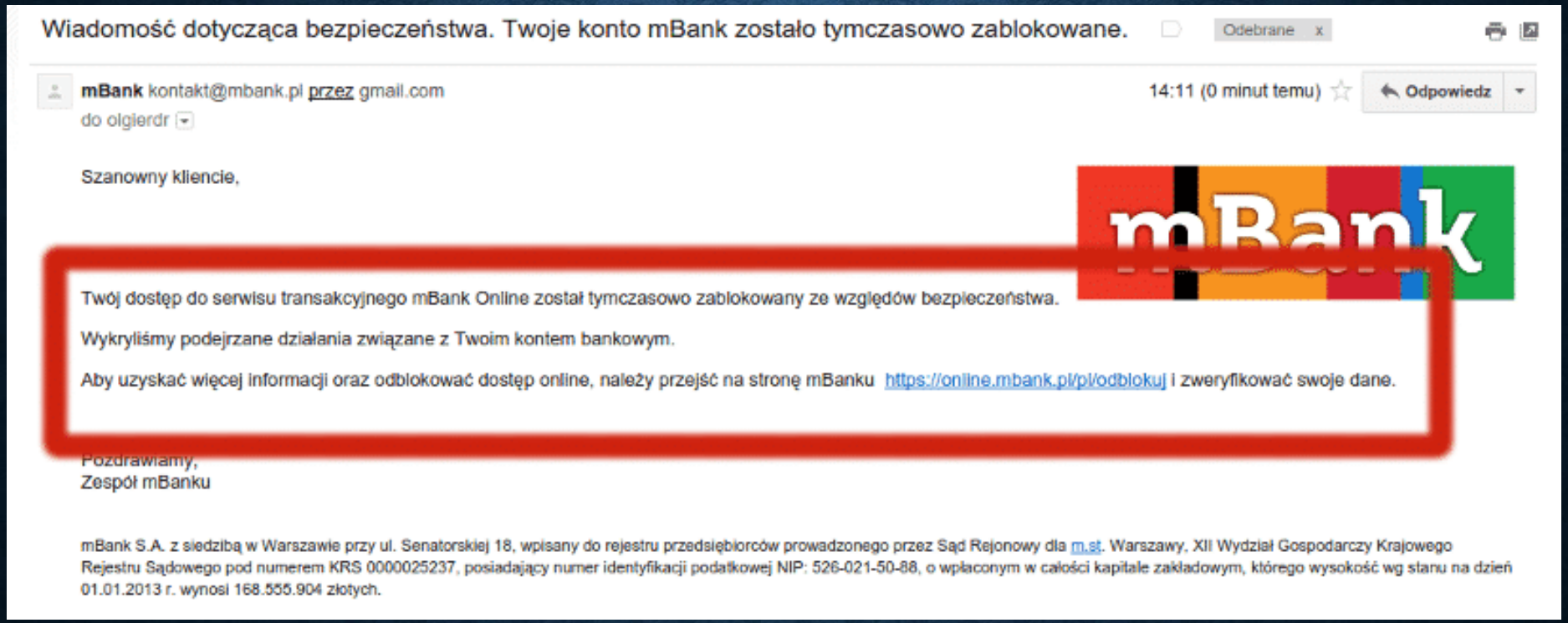
Oświadczenie

1. Oświadczam, że zostałem/am poinformowany o prawie wglądu do danych i prawie ich poprawiania oraz że dane te będą wykorzystane przez Bank dla celów marketingu produktów oferowanych przez Bank. Dane osobowe zbierane są na zasadzie dobrowolności w związku z realizacją niniejszego wniosku. Przyjmuję do wiadomości, że moje dane osobowe mogą być przetwarzane w Biurze Informacji Kredytowej S.A. z siedzibą w Warszawie.
   Ewentualny krąg odbiorców tych danych określają obowiązujące przepisy ustawy Prawo bankowe.
   Administratorem danych osobowych jest Bank Zachodni WBK S.A. Rynek 9/11, 50-950 Wrocław.

2. Przyjmuję do wiadomości i w pełni akceptuję Regulamin wydawania i używania Kart kredytowych BZ WBK, Taryfę opłat i prowizji pobieranych przez Bank Zachodni WBK S.A. za czynności bankowe i zobowiązuję się do ich przestrzegania.

Pola oznaczone: *-pole obowiązkowe **-pole obowiązkowe opcjonalnie

Phishing - przykład



Wiadomość dotycząca bezpieczeństwa. Twoje konto mBank zostało tymczasowo zablokowane. Odebrane x

mBank kontakt@mbank.pl przez gmail.com 14:11 (0 minut temu) Odpowiedz

do olgierdr

Szanowny kliencie,

Twój dostęp do serwisu transakcyjnego mBank Online został tymczasowo zablokowany ze względów bezpieczeństwa.

Wykryliśmy podejrzane działania związane z Twoim kontem bankowym.

Aby uzyskać więcej informacji oraz odblokować dostęp online, należy przejść na stronę mBanku https://online.mbank.pl/pl/odblokuj i zweryfikować swoje dane.

Pozdrawiamy,
Zespół mBanku

mBank S.A. z siedzibą w Warszawie przy ul. Senatorskiej 18, wpisany do rejestru przedsiębiorców prowadzonego przez Sąd Rejonowy dla m.st. Warszawy, XII Wydział Gospodarczy Krajowego Rejestru Sądowego pod numerem KRS 0000025237, posiadający numer identyfikacji podatkowej NIP: 526-021-50-88, o wpłaconym w całości kapitale zakładowym, którego wysokość wg stanu na dzień 01.01.2013 r. wynosi 168.555.904 złotych.

Phishing - przykład

From: <bzwbk@bzwbk.pl>
Date: 14 maja 2008 02:12:43 GMT+02:00
To: <webmaster@kaspersky.pl>
Subject: **Uaktywnij konto BZ WBK 24**
Reply-To: <bzwbk@bzwbk.plz>

Uaktywnij konto BZ WBK 24

Aby uaktywnic konto BZ WBK 24, nalezy kliknac ponizsze lacze i wprowadzic Numer karty na wyswietlonej stronie w celu potwierdzenia BZ WBK 24.

Kliknij tutaj, aby uaktywnic konto

http://host217-36-231-196.in-addr.btopenworld.com/aspnet_client/system_web/1_1_4322/SmartNav.htm

BZ WBK 24 mozesz rów ta BZ WBK 24 pod adresem https://www.ce

Dziekujemy za korzysta
Zespól BZ WBK 24.

Ataki sieciowe

Atak typu DoS (odmowa dostępu)

Atak typu DDoS (rozproszona odmowa dostępu)

Podręcznik str. 155

Ataki cyberbprzestępców:

- pojedynczy użytkownicy

- instytucje (szpitale, firmy, państwa itp.)

Jak zwiększyć swoje bezpieczeństwo?

1.Urządzenia komputerowe i oprogramowanie:

1. Podczas codziennej pracy nie korzystaj z konta administratora
2. Stosuj silne hasła
3. Zainstaluj firewall (zaporę sieciową)
4. Pobieraj aktualizację z zaufanych źródeł
5. Regularnie aktualizuj oprogramowanie (systemu, aplikacji)
6. Smartfony (blokada ekranu itp.)

2. Przeglądarka internetowa przechowuje:

- historię przeglądania

- pliki tymczasowe (pliki zapisane na komputerze - fragmenty stron, grafika itp.)

- pliki cookie (ciasteczka) – (pliki zapisane na komputerze – podstrony, sklepy internetowe – koszyki, statystyki stron i odwiedzający stronę)

Przeglądarka internetowa przechowuje:

- dane do uzupełniania formularzy (adres, numer karty płatniczej)

- hasła i inne dane logowania

Wniosek:
Przeglądarka przechowując dane ułatwia pracę, ale...?
Wyczyść dane przeglądania!

3. Szyfrowanie danych:

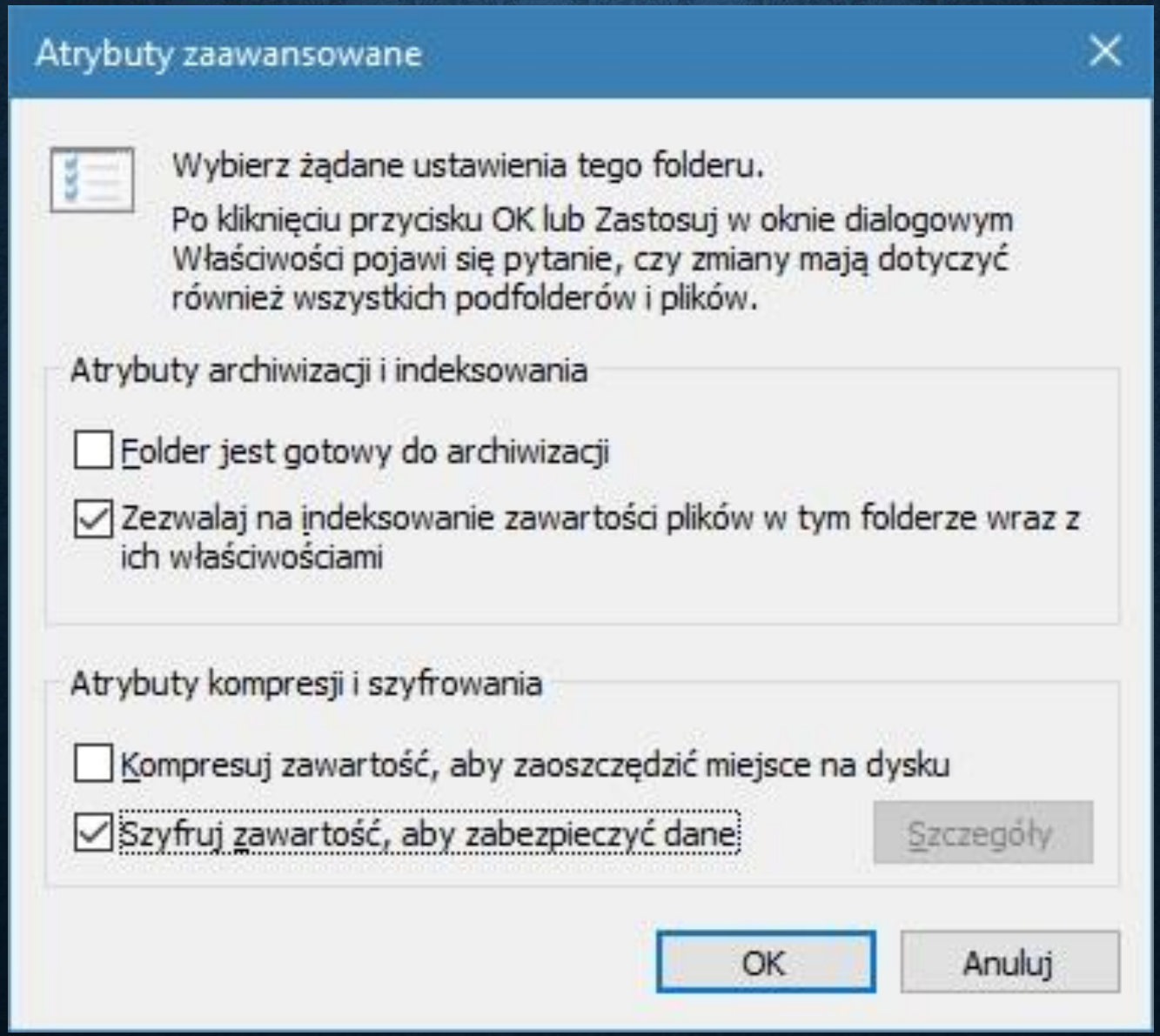
Zabezpieczyć:

- dyski komputera

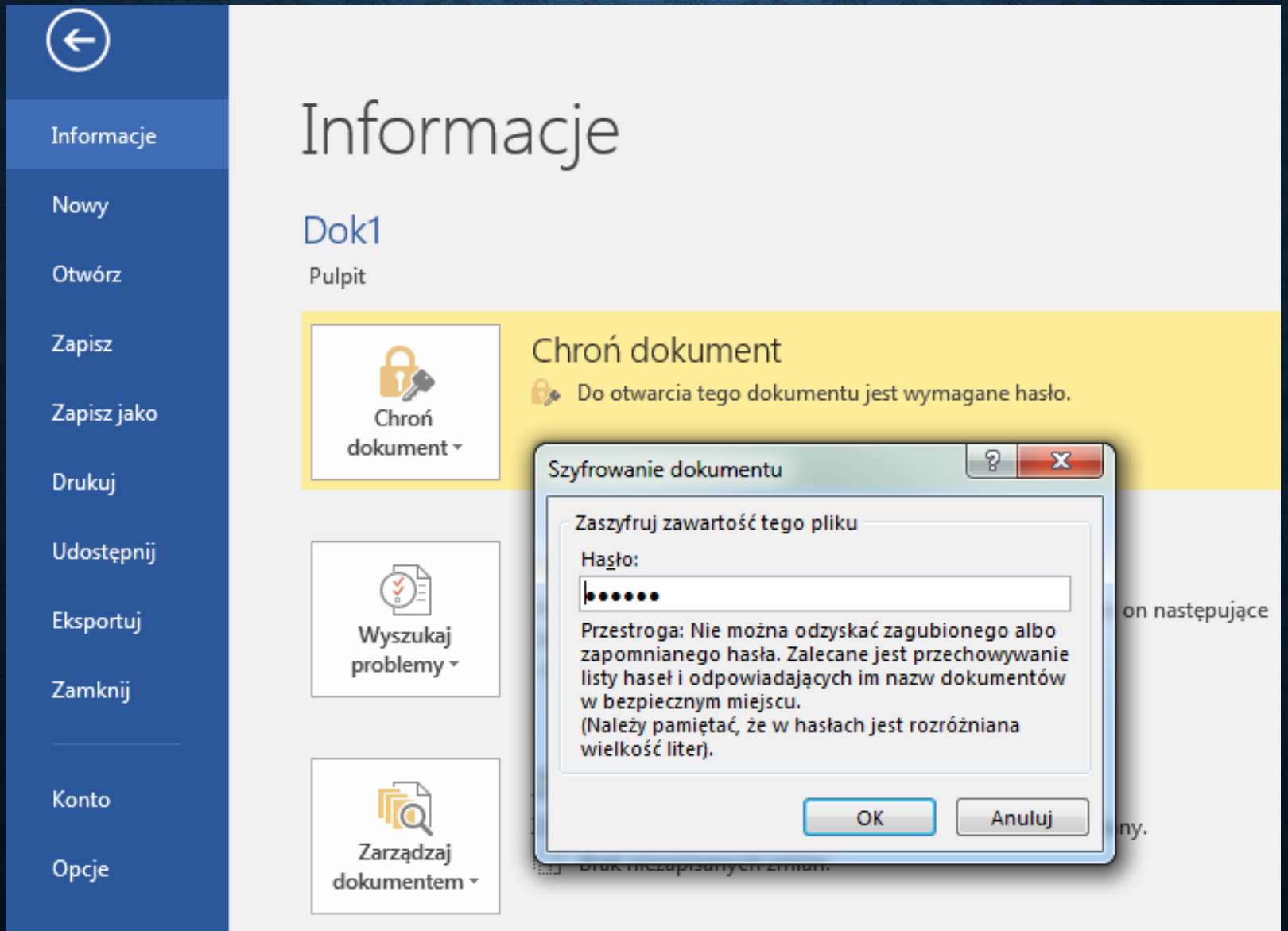
- pliki

- katalogi

Szyfrowanie plików, folderów



Szyfrowanie plików MS Office od wersji 2007:



4. Korzystanie z e-usług:

Procedura potwierdzająca tożsamość:

- **kilkustopniowe uwierzytelnianie** (login, hasło, kod PIN)

- **token** (wygenerowany kod otrzymywany przez SMS przy transakcji)

- **wykorzystanie danych biometrycznych** (np. skanowanie linii, tęczówki oka, twarzy, rozpoznawaniu mowy)

- **szyfrowanie danych** - protokół https://

5. Postępowanie w przypadku ataku:

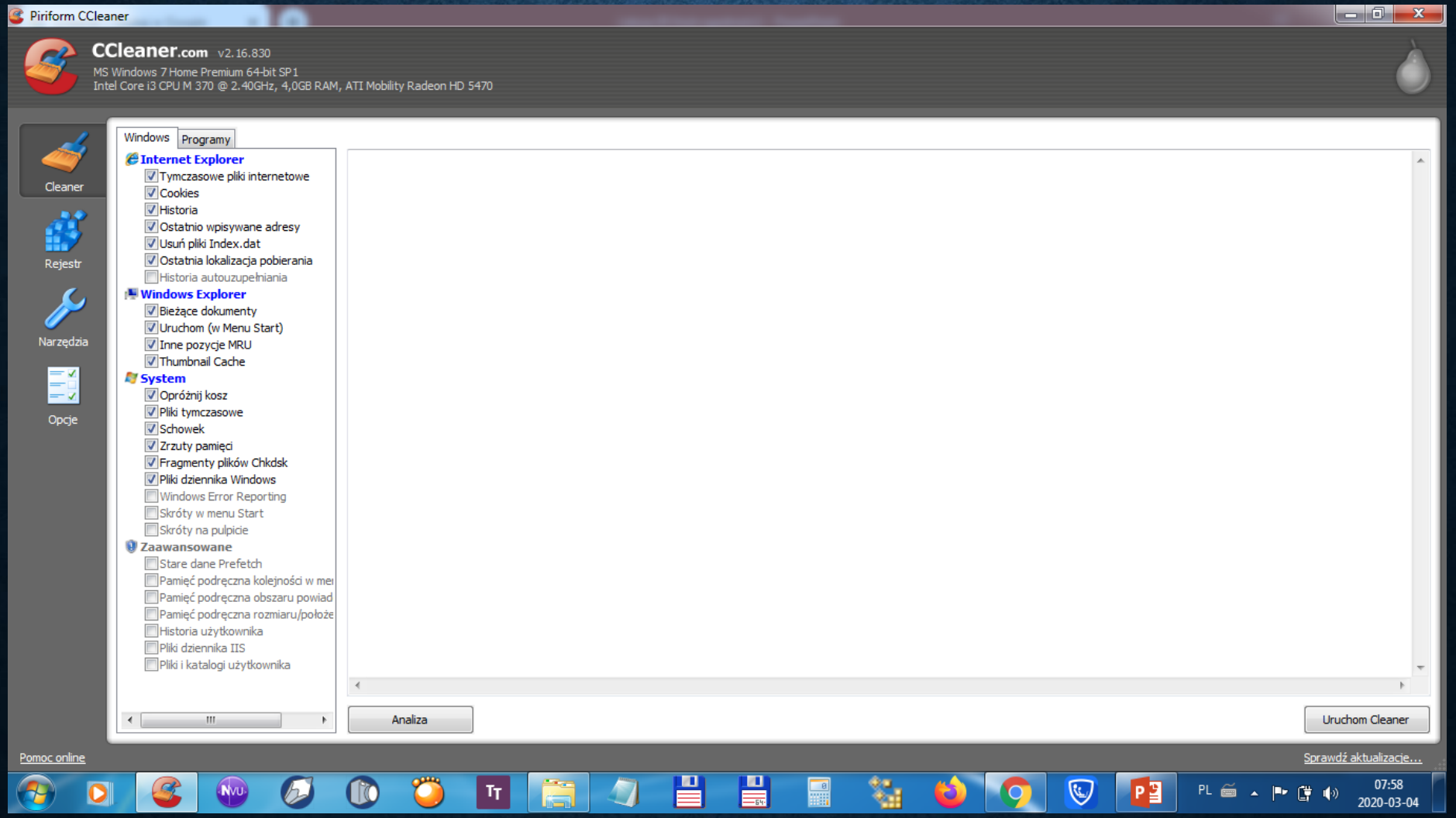
- skontaktuj się z usługodawcą, administratorem

- Policja

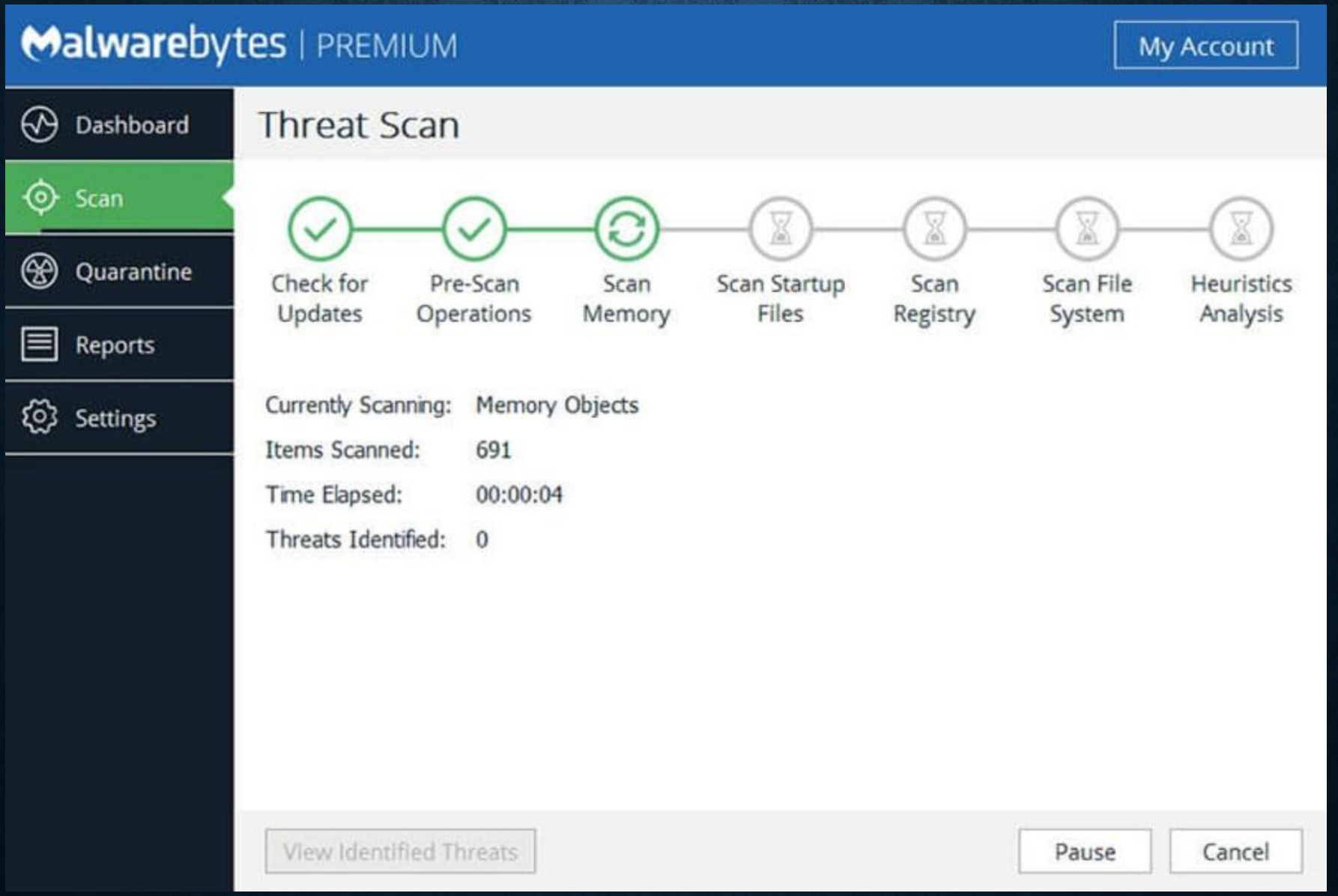
- CERT (Computer Emergency Response Team) – Zespół działający przy NASK - na stronie zgłaszać ataki!

Liczba zgłaszanych przypadków CERT:
- 2016r. – 1926 zgłoszeń
- 2017r. – 3182 zgłoszeń

Program Ccleaner



Program Malware



Program antywirusowe