Nr 4 - Kwiecień 2013

# CIP focus

RCB
Rządowe Centrum Bezpieczeństwa

foto FBC

## Mikko Hyppönen:

# Jeszcze wszystkiego nie widzieliśmy

Wywiad z Dyrektorem ds. badań w F-Secure. ekspertem w dziedzinie bezpieczeństwa komputerowego, jednym z 50 najważniejszych ludzi Internetu

- **str. 7**

Foto: http://www.publicdomainpictures.net - Per Kratochvil

# Cyber-EXE POLSKA 2013

Po udanym ćwiczeniu Cyber-EXE Polska 2012 organizatorzy utwierdzili się w przekonaniu, że inicjatywa systematycznego przeprowadzania ćwiczeń z ochrony w cyberprzestrzeni powinna być kontynuowana. Jeszcze przed ogłoszeniem końcowego raportu z zeszłorocznego ćwiczenia rozpoczęto dyskusje do kogo skierowana powinna być kolejna edycja. Zdecydowanym faworytem został sektor finansowy, a w szczególności banki.

- str. 12

**W NUMERZE:**




## Narodowy Program Ochrony Infrastruktury Krytycznej

26 marca 2013 r. Rada Ministrów przyjęła Narodowy Program Ochrony Infrastruktury Krytycznej, którego głównym celem jest stworzenie warunków do poprawy bezpieczeństwa infrastruktury krytycznej kraju.

**POBIERZ**

# Drodzy Czytelnicy,

Przede wszystkim chcielibyśmy rozpocząć od podzielenia się dobrymi wiadomościami. Mamy przyjemność zakomunikować Wam, że w dniu 26 marca Rada Ministrów przyjęła Narodowy Program Ochrony Infrastruktury Krytycznej (NPOIK). Oznacza to, że przewidziane w ustawie o zarządzaniu kryzysowym działania mogą w końcu wejść w życie. Dla nas oznacza to oczywiście mnóstwo pracy, ale jesteśmy podekscytowani nowymi wyzwaniami, które nas czekają.

W programie znajdziecie większość informacji niezbędnych w dyskusji o infrastrukturze krytycznej, jej identyfikacji i ochronie, celach i wiodących zasadach Programu, podziale odpowiedzialności, sposobie i mechanizmach wymiany informacji, podstawach oceny ryzyka i szeroko pojętej współpracy. Zachęcamy Was zatem do lektury NPOIK.

Szczególnie zainteresować Was może, jak podeszliśmy do tematu ochrony teleinformatycznej. Odpowiedź na to pytanie znajdziecie w rozdziale 2.8 Załącznika nr 2 do NPOIK.

Ten numer zaczynamy od krótkiego podsumowania zdarzeń jeszcze z zeszłego roku. Warto ponownie uzmysłowić sobie tendencję rozwoju złośliwego oprogramowania na świecie tym bardziej, że jest coraz bardziej wyrafinowane.

Najsłabszym ogniwem ciągle pozostaje jednak użytkownik, o czym będzie przypominał w serii swoich artykułów poświęconych bezpieczeństwu przesyłania danych w sieci Internet Emil Wróbel z Rządowego Centrum Bezpieczeństwa. W pierwszym z nich skupia się na protokole HTTPS.

Z kolei Mirosław Maj z Fundacji Bezpieczna Cyberprzestrzeń spotkał się z Mikko Hyppönenen, jednym z najbardziej znanych ekspertów IT i nie omieszkał zadać mu kilku pytań. Wywiad został podzielony na dwie części. Pierwszą znajdziecie na stronach Fundacji, a drugą u nas.

W dalszej części CIIP focusa przedstawiamy kolejne fazy budowy zespołu reagowania na incydenty komputerowe, których omawianie rozpoczęliśmy w numerze 2 naszego Informatora (wszystkie etapy skrótowo są przedstawione także w Załączniku nr 2 do NPOIK).

Na koniec proponujemy Wam lekturę dwóch artykułów wzajemnie powiązanych. Najpierw Mirosław Maj przedstawi ogólne założenia kolejnych ćwiczeń z ochrony w cyberprzestrzeni, których tegoroczna edycja skupiać się będzie na sektorze finansowym, a następnie Kamil Kiliński z banku Citi Handlowy wprowadzi Was w świat standardów stosowanych w bankowości, sposobów certyfikacji na zgodność z nimi, a także przedstawi kilka cennych porad jak przeprowadzić ten proces sprawnie.

*Redakcja CIIP focus*




## NEWS

### Ataki na systemy SCADA i słabości tych systemów w ocenie CERT-ICS

W 2012 roku systemy nadzoru infrastruktury krytycznej były wielokrotnie atakowane. Amerykański CERT dla infrastruktury krytycznej CERT-ISC (Industrial Control System) odnotował prawie 200 takich ataków. 40% z nich dotyczyło systemów energetycznych, a 15% systemów nadzoru wodociągów. Odnotowano też kilkadziesiąt słabości systemowych dotyczących systemów SCADA.
Więcej: http://bit.ly/YZyLCo

### Analiza ataków na systemy SCADA

Firma TrendMicro przeprowadziła badania związane z atakami na systemy SCADA. Ich wyniki przedstawiła na znanej konferencji o bezpieczeństwie Black Hat Europe oraz w specjalnie wydanym raporcie. Do przeprowadzenia testów wykorzystano technologię honeypot. Większość ataków na systemy pochodziło z USA. 2% z nich pochodziło z komputerów zlokalizowanych w Polsce i związane one były między innymi z próbami nieautoryzowanego dostępu.
Więcej: http://bit.ly/ZUjqGU

### Systemy korporacyjne atakowane średnio raz na 3 minuty

Zdaniem specjalistów firmy FireEye systemy informatyczne przedsiębiorstw atakowane są średnio raz na 3 minuty. Podstawowym celem ataków stały się systemy firm technologicznych. Coraz częściej pojawiają się ataki dedykowane, a zaawansowanie funkcji złośliwego kodu jest coraz większe.
Więcej: http://bit.ly/YPlXT1
[pełny raport]: http://bit.ly/XpV0GO
(wymagana rejestracja)

Jeśli nie zaznaczono inaczej, fotografie pochodzą z serwisu:
http://www.publicdomainpictures.net

# PRZEGLĄD NAJWAŻNIEJSZYCH WYDARZEŃ 2012 ROKU

*Mirosław Maj*
*Fundacja Bezpieczna Cyberprzestrzeń*

**Minął już wprawdzie czas podsumowań roku 2012, niemniej jednak warto jeszcze raz obejrzeć się za siebie i spojrzeć na wydarzenia sprzed kilkunastu miesięcy z perspektywy największych zagrożeń związanych z działaniem złośliwego oprogramowania. W szczególności dlatego, że jest na co spoglądać. Niektóre z nazw złośliwego kodu na stałe zadomowią się w słowniku najbardziej istotnych zagrożeń internetowych.**

Rok 2012 to między innymi sieciowe konflikty na poziomie międzynarodowym, ataki ukierunkowane, haktywizm. Z mijającego roku wszyscy powinni zapamiętać takie wirusy, jak Flame i Gauss. Haktywiści uruchamiali coraz to nowe operacje, z czego w Polsce z pewnością zapamiętamy wydarzenia z drugiej połowy stycznia, związane z konfliktem społecznym wokół ACTA i uciążliwe ataki na serwisy rządowe oraz przemówienie „Baśki" na stronie Prezesa Rady Ministrów. Później, w ciągu roku wielokrotnie słyszeliśmy o poważnych atakach, które nie omijały także największych firm, czyli takich, jak Sony, Oracle, Adobe, Microsoft czy Google. Doniesienia te obalały mity na temat bezpieczeństwa niektórych systemów. Skutecznie zrobił to na przykład wirus Flashback, który w kwietniu zainfekował ponad 700 000 komputerów obsługiwanych przez system MacOS X. Wyznawcy poglądu „mam Maca, więc jestem bezpieczny" musieli zrewidować swoje poglądy.

Prawdziwym majstersztykiem w tworzeniu złośliwego kodu był pakiet wirusowy Flame. Lista jego funkcjonalności jest długa. Są to głównie funkcje szpiegowskie i z pewnością, biorąc pod uwagę cele jego ataku, wirus ten wpisuje się w kategorie „wojny cybernetyczne". Istnieją też opracowania pokazujące jego podobieństwo do wcześniejszych wirusów Stuxnet i Duqu. A wiele śladów wskazuje na rządy Izraela i Stanów Zjednoczonych jako jego autorów. Wirus działał od roku 2010, a kiedy pojawiły się pierwsze doniesienia o jego wykryciu, dość szybko znikł z komputerów swoich ofiar. Co ciekawe, w historii o Flame jest też wątek polski. Zdaniem KasperskyLab część infrastruktury, która służyła do zarządzania znajdowała się w Polsce[1]. Co jednak najważniejsze, to fakt, że począwszy od Stuxnet'a, przez Flame'a, Duqu i późniejszego Gaussa, pojęcie „wojen cybernetycznych" z pozycji terminu w literaturze przeszło do świata realnego. Do powyższego zestawienia można dodać kasowanie danych na 30 000 komputerów światowego giganta w wydobyciu ropy naftowej – Saudi Aramco, czyli coś, co znamy pod nazwą wirusa Shamoon.

Omawiając najważniejsze wydarzenia roku 2012 nie można pominąć sprawy dynamicznego wzrostu zagrożeń dla platform mobilnych. A właściwie należałoby uczciwie stwierdzić, że chodzi przede wszystkim o system Android. Powodem tego jest oczywiście jego niezwykła popularność (około 70% udziału w rynku), ale chyba jeszcze bardziej słabych mechanizmów weryfikacji oprogramowania, które pojawia się w Android Market. To sytuacja zupełnie inna niż w przypadku dwóch innych systemów – iOS i Windows Phone/Mobile. Tam kontrola jest znacznie bardziej restrykcyjna. Efekt jest widoczny gołym okiem. Wirusy na iOS i Windows Phone/Mobile łącznie oscylują wokół 1% wszystkich wirusów na platformy mobilne. Natomiast wirusy na Android mają mniej więcej taki sam udział procentowy w liczbie wirusów ogółem, jaki jest udział systemu Android w rynku. Żeby uprzytomnić skalę zjawiska warto przywołać statystyki wspominanego już

[1] „Dach płonie: walka z serwerami kontroli Flame'a" - http://www.viruslist.pl/weblog.html?weblogid=794

## NEWS

### Raport kwartalny amerykańskiego ICS-CERT

Raport zawiera informacje szczególnie istotne dla operatorów infrastruktury krytycznej. Opisane są najbardziej popularne ataki w ostatnim okresie, najczęściej spotykane słabości dla poszczególnych kategorii procesów związanych z zarządzaniem systemami teleinformatycznymi, materiały uświadamiające oraz zestawienie alertów i rekomendacji związanych z zagrożeniami.
Więcej: http://1.usa.gov/XgEHdb

### Mapa źle skonfigurowanych urządzeń sieciowych

Przy wykorzystaniu powszechnie używanego oprogramowania do wykrywania słabości systemowych zbudowany został botnet ze źle skonfigurowanych urządzeń sieciowych. Kontrowersyjny projekt, który nieznany haker przedstawia jako czysto edukacyjny, doprowadził do powstania mapy zagrożonych urządzeń. Szczególnie zagrożone regiony świata to amerykańskie wschodnie wybrzeże i obszar Unii Europejskiej. Haker bardzo szczegółowo przedstawił wyniki swojej pracy.
Więcej: http://bit.ly/15VkU5t

### Problem obsługi słabości systemowych dla systemów SCADA

Opracowanie na temat problemów jakie najczęściej występują przy obsłudze słabości systemowych systemów SCADA oraz ich znaczenia w kontekście innych elementów zapewnienia bezpieczeństwa np.: poprawnego projektowania systemów. W artykule zaproponowano podejścia do zarządzania tym procesem oraz przedstawiono ocenę działania instytucji z nim powiązanych np.: ICS-CERT.
Więcej: http://ubm.io/Zdv3IR

### Wyniki badania dotyczącego bezpieczeństwa systemów SCADA

SANS przygotował raport na temat bezpieczeństwa systemów SCADA. Wynika z niego między innymi, że 70% operatorów tych systemów jest świadomych ryzyka związanego z ich funkcjonowaniem. Niestety 1/3 z nich podejrzewa, że mogło dojść do skutecznego ataku na ich systemy. Jako najpoważniejsze zagrożenia podają: zaawansowany malware (np.: Stuxnet), zagrożenia z wewnątrz organizacji oraz akty haktywizmu.
Więcej: http://bit.ly/W1Loz8

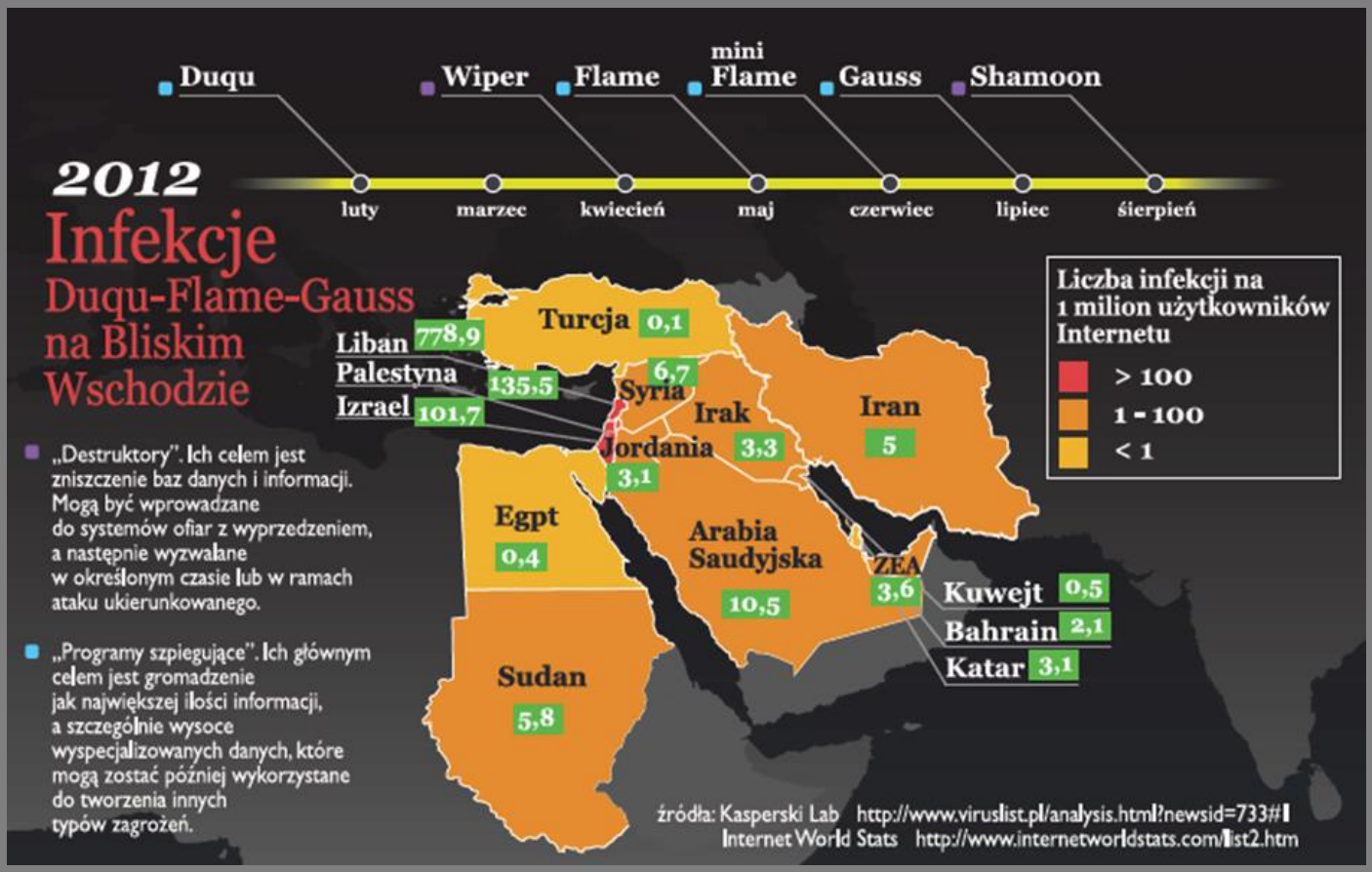



foto IDG

KasperskyLab mówiące o tym, że w 2012 roku odnotowano około 35 000 wirusów na Android. Krótko mówiąc - po blisko 10 latach ustawicznego „wywoływania wilka z lasu", biorąc pod uwagę systematyczne przewidywania co do wzrostu zagrożeń związanych z telefonami komórkowymi, wilk z lasu w końcu wyszedł.

Nie obyło się w 2012 roku również bez dużych wycieków danych osobowych. Co prawda nie były one tak spektakularnie jak w 2011 roku, kiedy to atak na Sony skończył się wyciekiem danych o 70 milionach użytkownikach, ale wpadki – najpierw LinkedIn (6,4 mln rekordów), a później Dropbox (8 mln rekordów), podtrzymały złą passę.

W 2012 roku kolejny raz potwierdziło się istotne zagrożenie związane z korzystaniem z Javy. W sierpniu pojawiły się masowe infekcje związane z krytyczną dziurą w Java oraz równie powszechne związane z Adobe Flash Player.

Oprócz spektakularnych problemów z powszechnie używanym oprogramowaniem warto wspomnieć jeszcze o dwóch ciekawych przypadkach dotyczących sprzętu. Pierwszy z nich to pojawienie się na „rynku" urządzenia wartego 50$, dzięki któremu można otworzyć 4 miliony drzwi w kilku tysiącach hoteli na całym świecie, wliczając w to takie sieci hotelowe jak Hyatt, Mariott czy Holiday Inn. Co prawda to zagrożenie trochę „z innej beczki", ale dobrze uzmysławia skomplikowanie i kosztowność procesu łatania systemów po wykryciu ich słabości. W tym przypadku łatwo sobie wyobrazić jak bardzo kosztowne byłoby „załatanie" tej dziury w porównaniu do łatania dziur w oprogramowaniu. Drugi ciekawy przypadek to historia z Brazylii, gdzie ofiarą padło 4,5 mln właścicieli modemów. Wszystko to poprzez jedną dziurę w modemowym firmware'rze i nielegalnej sieci 40 serwerów DNS.

Większość przytoczonych zagrożeń jest na tyle ciekawa, że warto im przyjrzeć się bliżej. Dlatego do niektórych z nich z pewnością wrócimy w kolejnych numerach CIIP focus.


Foto: http://www.publicdomain... Petr Kratochvil

# BEZPIECZEŃSTWO DANYCH W SIECI INTERNET

## Część I - protokół HTTPS

*Emil Wróbel*
*Zespół Informatyki i Łączności RCB, Absolwent Wydziału Cybernetyki WAT*

**Dostęp do globalnej sieci stał się naszą codziennością. Wiele osób nie wyobraża sobie już funkcjonowania w świecie bez Internetu. Usługi świadczone drogą elektroniczną to przede wszystkim wygoda załatwiania codziennych spraw oraz ich dostępność praktycznie z każdego miejsca na Ziemi. Niestety powszechność tego typu rozwiązań prowadzi również do wzrostu liczby zagrożeń czyhających na użytkowników.**

Niniejszy artykuł chciałbym poświęcić zagadnieniu ochrony danych przesyłanych pomiędzy klientem a serwerem na przykładzie najpopularniejszego scenariusza, czyli wymiany danych za pomocą protokołu HTTP (ang. Hypertext Transfer Protocol) używanego m. in. do serwowania zawartości stron internetowych oraz zbierania danych przesyłanych przez użytkowników. Artykuł jest początkiem serii, w której będę poruszał kwestie związane z szeroko rozumianym pojęciem bezpieczeństwa w sieci.

### Twoje dane podane na talerzu

Wiele osób nie zdaje sobie sprawy, że podczas codziennego surfowania w Internecie naraża się na niebezpieczeństwo wycieku prywatnych danych. W normalnych warunkach wszystkie informacje są przesyłane za pomocą nieszyfrowanego protokołu HTTP. Jeśli nie podejmiemy żadnych działań w celu zabezpieczenia kanału komunikacyjnego, cała nasza aktywności w sieci jest dostępna dla potencjalnych atakujących. Ma to znaczenie zwłaszcza w rozległych sieciach korporacyjnych, gdzie jeden zainfekowany komputer może zbierać dane o wielu użytkownikach bez ich wiedzy, wykorzystując proste techniki podsłuchu np. *ARP spoofing*[1].

[1] Rodzaj ataku sieciowego polegający na podszywaniu się pod inny komputer za pomocą odpowiednio spreparowanych pakietów ARP służących do identyfikacji adresów MAC karty sieciowej na podstawie adresu IP. Po wykonaniu udanego ataku najczęściej cała komunikacja przechodzi przez komputer atakującego pozwalając na dostęp do przesyłanych treści.

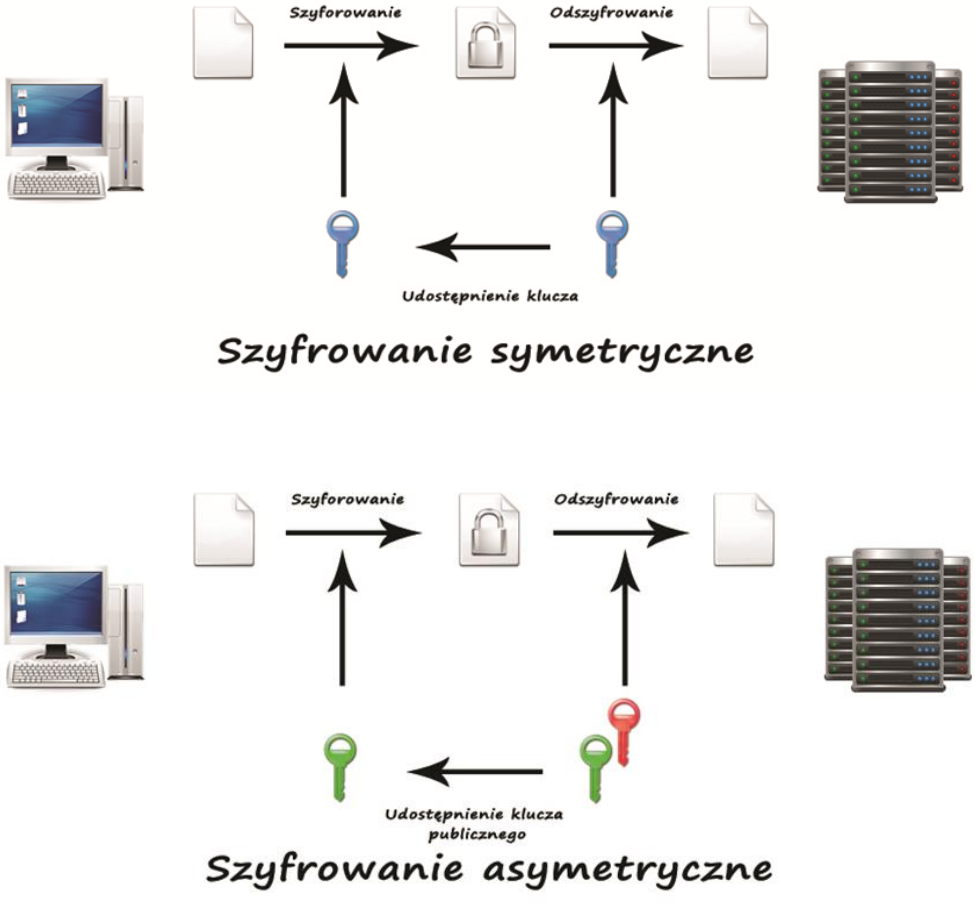
Sytuacja wygląda znacznie gorzej, gdy stajemy się celem bardziej ukierunkowanego ataku, mającego wydobyć od nas określony rodzaj informacji np. dane kary kredytowej, hasło chroniące dokumenty firmowe, czy konto w systemie bankowym. W tym momencie pojawia się naturalna potrzeba ochrony wrażliwych danych przesyłanych za pomocą sieci przed dostępem osób nieupoważnionych.

### Kilka słów o zabezpieczeniach

Zdecydowanie najbardziej rozpowszechnionym mechanizmem zapewniającym bezpieczeństwo komunikacji w Internecie jest powstały w 1994 roku protokół SSL (ang. Secure Sockets Layer) oraz stosowana obecnie jego późniejsza implementacja TLS (ang. Transport Layer Security). Rozwiązanie to ma przede wszystkim zapewnić poufność i integralność danych dzięki zastosowaniu odpowiednich technik kryptograficznych oraz pozwolić na weryfikację tożsamości serwera i klienta.

W standardzie SSL/TLS wykorzystywane są algorytmy kryptograficzne działające zarówno na bazie szyfrowania symetrycznego, jak i asymetrycznego. Pierwsze z nich charakteryzuje wykorzystanie tego samego pakietu danych zwanego kluczem do zaszyfrowania wiadomości oraz późniejszego jej odczytania. Jego alternatywą jest rozwiązanie posiadające dwa takie zestawy: klucz publiczny stosowany do zabezpieczenia wiadomości oraz sparowany z nim klucz prywatny pozwalający na jej odszyfrowanie. Algorytm asymetryczny jest wykorzystywany w pierwszej fazie komunikacji w celu ustalenia wspólnego klucza sesji. Dalsza komunikacja jest szyfrowana za pomocą algorytmu symetrycznego, ponieważ działa on zdecydowanie szybciej i nie powoduje istotnych narzutów czasowych transmisji danych.

Protokół ten posiada również mechanizmy chroniące przed przypadkową lub celową utratą integralności danych. Są to mechanizmy MAC (ang. Message Authentication Codes) oraz stosowany




Zasada działania szyfrowania symetrycznego i asymetrycznego

Atak typu man in the middle

w TLS – HMAC (ang. Keyed Hash Message Authentication Codes). Służą one do obliczenie funkcji skrótu przesyłanych danych, w celu weryfikacji zgodności wysłanych i odebranych pakietów. HMAC stosuje dodatkowo szyfrowanie w celu lepszej ochrony przed ujawnieniem przesyłanej zawartości.

Istotnym elementem standardu jest także możliwość weryfikacji tożsamości drugiej strony dzięki wykorzystaniu certyfikatów. Pełna autoryzacja jest możliwa tylko w przypadku zastosowania certyfikatów kwalifikowanych, wystawianych przez zewnętrzne podmioty, do których obie strony mają zaufanie tzw. CA (ang. Certification Authority).

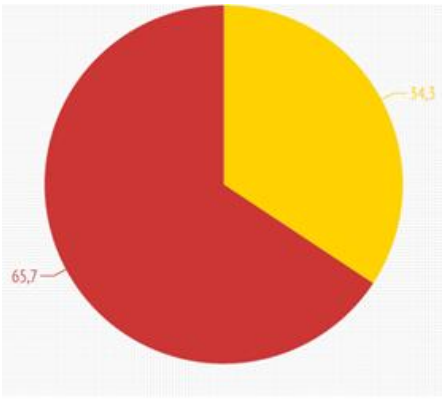
**HTTPS = HTTP + SSL/TLS**

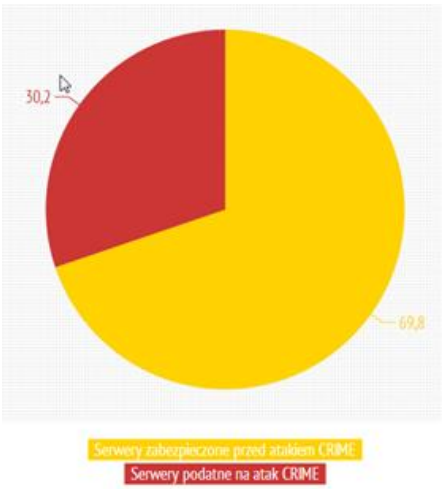
SSL/TLS działający w warstwie prezentacji *modelu OSI*[1] może zostać wykorzystany jako mechanizm zabezpieczenia protokołów warstwy aplikacji (m.in FTP, SMTP), jednak najczęściej występuje w popularnym i mającym szerokie zastosowanie protokole HTTPS (ang. Hypertext Transfer Protocol Secure). Popularność tego rozwiązania zawdzięczamy przede wszystkim jego pochodzeniu – został on opracowany przez firmę Netscape Comunications, której flagowy produkt, czyli przeglądarka Netscape Navigator posiadała w połowie lat 90-tych około 80% udziału rynku przeglądarek internetowych. Standard HTTPS szybko zyskał uznanie społeczności, dostawców serwerów WWW, a nawet konkurencji firmy Netscape, dzięki czemu błyskawicznie wyparł inne rozwiązania np. protokół S-HTTP.

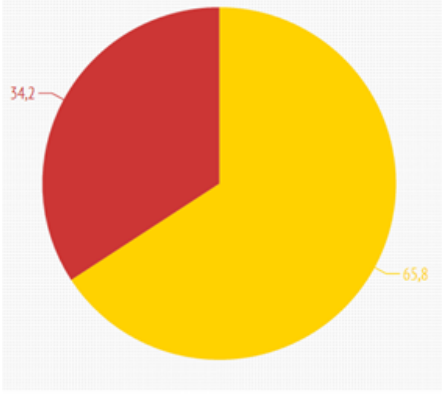
### Pozorne bezpieczeństwo

Ataki na witryny zabezpieczone poprzez protokół HTTPS są szczególnie niebezpieczne, ponieważ użytkownik przekonany o własnym bezpieczeństwie nie zdaje sobie sprawy z możliwych zagrożeń. Najpopularniejsze ataki wykorzystują luki istniejące w samym protokole lub nieuwagę użytkownika poprzez serwowanie mu spreparowanych stron lub przechwycenie komunikacji i zmianę protokołu na niezabezpieczony HTTP.

Jak wynika z raportu Trustworth Internet Movement z marca 2013 r. podstawowym zagrożeniem dla bezpieczeństwa jest stosowanie, pomimo dostępności nowszych wersji tego standardu, protokołu TLS w wersji 1.0, dla którego istnieją rozpoznane podatności oraz wykorzystanie niedostatecznych technik kryptograficznych.




Z danych zaprezentowanych w raporcie wynika, że aż 65,7 % stron działających w oparciu o protokół HTTPS jest podatnych na atak BEAST[1], natomiast 30,2% witryn wykazuje wrażliwość na atak CRIME[2]. Do tego 34.2 % stron korzysta z algorytmów szyfrowania opartych na 128 bitowym kluczu, który nie zapewnia pełnego bezpieczeństwa kryptograficznego.

Drugi rodzaj ataku łączący w sobie techniki z obszaru informatyki i socjotechniki polega na przekonaniu użytkownika do przesłania wrażliwych danych za pomocą podrobionej lub zmodyfikowanej witryny. Do ataku może dojść m.in. w momencie, gdy witryna przełącza nas ze standardowego protokołu HTTP na jego bezpieczną wersję np. podczas uwierzytelniania. Sygnał taki może zostać przechwycony przez komputer kontrolujący komunikację pomiędzy nami, a serwerem, do którego chcemy się połączyć i kontynuując komunikację z oryginalnym serwerem będzie serwowało użytkownikowi dane w postaci niezabezpieczonej.

### Co robić?

Sytuacja nie jest beznadziejna. Stosowanie aktualnych wersji przeglądarek internetowych, które wspierają nowsze wersje protokołu TLS oraz stosowanie krótkich sesji może uchronić nas przed utratą wrażliwych danych i wszelkimi tego konsekwencjami. Bezpieczeństwo w Internecie zależy przede wszystkim od użytkowników i ich zdolności oceny potencjalnych zagrożeń, a zabezpieczenie komunikacji pomiędzy klientem a serwerem odgrywa jedną z podstawowych ról w tym procesie.

Drugi artykuł tej serii poświęcony będzie bezpieczeństwu przechowywania haseł – zapraszam do zapoznania się z nim w kolejnym numerze CIIP Focus.

[1] Opracowany przez Open Systems Interconnection standard opisujący strukturę komunikacji sieciowej w postaci 7 warstwowego modelu oraz zależności komunikacyjnych pomiędzy warstwami.

[1] Atak wykorzystujący podatność protokołu SSL 3.0 i TLS 1.0. Wykorzystuje kod JavaScript w celu ustalenia tzw. wektora inicjalizującego ułatwiając przejęcie ciastka sesyjnego tworzonego podczas logowania do serwisu oraz przejęcie kontroli nad kontem użytkownika.

[2] Atak wykorzystujący podatność kompresji danych protokołu TLS. Polega on na wyszukiwaniu różnic rozmiarów skompresowanych sfabrykowanych odpowiednio zapytań w celu odnalezienia klucza sesyjnego, opierając się na zasadzie, że zmniejszenie rozmiaru przesyłanego pakietu oznacza lepsze dopasowanie do wzorca i możliwość dokonania redukcji jego rozmiaru.

## MIKKO HYPÖNNEN DLA FBC i CIIP focus:

# ZAGROŻENIA DLA INFRASTRUKTURY KRYTYCZNEJ I MIĘDZYNARODOWE KONFLIKTY W INTERNECIE

**Z Mikko Hypponenem rozmawia Mirosław Maj z Fundacji Bezpieczna Cyberprzestrzeń.**

**Mirosław Maj: Chciałbym, abyśmy porozmawiali o cyber wojnach. W mojej opinii są trzy główne modele przygotowania się do cyber wojny: amerykański, chiński, rosyjski. Czy Ty się z tym zgadzasz i czy możesz powiedzieć, który według Ciebie jest najbardziej skuteczny?**

Mikko Hypponen: Całkiem sporo wiemy o tym co robią Chińczycy i jakie formy przygotowań przyjmują, znamy sporo szczegółów i sytuacji. Wiemy trochę o tym, co robią Amerykanie - oni są mniej widoczni od Chińczyków, ale wiemy, że inwestują w nowe technologie ataków i coś w tym celu robią. Natomiast nie wiemy zupełnie nic o tym co robią Rosjanie. Rosyjski program cyber wojny jest dla mnie wielką zagadką. Musimy jednak założyć, że coś na pewno robią.

Nigdy nie spotkałem się z żadnym programem szpiegowskim zrobionym przez Rosjan. Ataki DDoS, które miały miejsce w Estoni i Gruzji mogły być przeprowadzone na skutek nacisków rządu rosyjskiego, ale nikt nigdy tego nie udowodnił ani się do tego nie przyznał. Rząd rosyjski nie wykonał bezpośrednio żadnego ruchu. Dlatego Rosja jest wielką tajemnicą.

Ale masz rację, że są to trzy różne mechanizmy cyber wojenne. Chiny działają schematycznie i standardowo – zajmują się szpiegostwem, atakami APT itp. Amerykanie nie używają emaili, mają nowoczesne technologie, super komputery, i zaawansowane techniki. Wszystko odbywa się na bardzo wysokim poziomie i przy olbrzymich inwestycjach finansowych. Mają zupełnie inny system od Chińczyków. Natomiast Rosjanie? To mnie zastanawia i niepokoi, ponieważ naprawdę nie wiem co oni robią.

**MM: Jak myślisz, ile my widzimy, z tego co w rzeczywistości te kraje robią? Ile z tego co widzimy jest prawdą, a ile propagandą? Wszyscy znamy raport Madiant, ale kto wie o tym, że chiński rząd ciągle mówi o atakach na ich rządowe strony internetowe ze strony Amerykanów. Nikt tego nie zauważa.**

MH: Ja zauważam, ale zgadzam się z Tobą, że generalnie tego się nie zauważa. Oczywiście, że w tym jest dużo propagandy. Oni chcą się pokazać jako wielce poszkodowanych przez agresorów. To jest także propaganda wewnątrz państwa. Chiński rząd pokazuje swoim obywatelom, że są narażeni na cyber agresję ze świata a chińscy oficerowie muszą bronić obywateli przed cyber atakami.

**MM: No tak, ale z punktu widzenia reszty świata, każdy wie przede wszystkim o agresjach ze strony**

Mikko Hyppönen foto: FBC

Mikko Hyppönen – dyrektor ds. badań w F-Secure. Ekspert w dziedzinie bezpieczeństwa komputerowego, publicysta. Pisał dla magazynów takich, jak: Scientific American, Wired czy The New York Times. Od 1990 roku, Hyppönen pomagał w egzekwowaniu prawa w Stanach Zjednoczonych, Europie i Azji w przypadkach cyberprzestępstw, doradza rządom w dziedzinie bezpieczeństwa komputerowego. W 2011 roku znalazł się na 61. miejscu listy Top 100 Światowych Myślicieli sporządzonej przez Foreign Policy. Został również uznany przez PC Word za jednego z 50 najważniejszych ludzi Internetu. Polecamy również wystąpienia Hyppönena na platformie TED.

**chińskiego rządu. Mam inne pytanie - jak myślisz, co będzie następnym Stuxnet'em? W którym kierunku i jak daleko podąży rozwój wirusów? Już teraz to wygląda bardzo kompleksowo i trudno sobie wyobrazić następny krok w tej ewolucji.**

MH: Tak naprawdę, to nie mamy pojęcia. Po prostu tego nie wiemy. Jedna myśl, która przychodzi mi do głowy to wynik analizy komunikatu amerykańskiego senatu, który ostrzega amerykańskie firmy, aby nie kupowały produktów Huawei i ZTE, ponieważ są blisko powiązane z chińskim rządem. Ok, ale co by się stało, gdyby chiński senat wydał ostrzeżenie o nie kupowaniu produktów CISCO, Juniper, Microsoft, ponieważ są związane z amerykańskim rządem, co w rzeczywistości jest prawdą? I tu nasuwa mi się na myśl Intel. Jak myślisz gdzie oni produkują procesory?

**MM: Indonezja?**

MH: Nie

**MM: Chiny?**

MH: Nie.

**MM: Naprawdę w USA?**

MH: Tak. I oczywistym jest, że mogliby to produkować gdzie indziej taniej, ale tego nie robią. Z pewnych względów robią to w USA. Nie sądzę, aby takie działanie było przypadkowe.

**MM: Na mapie operacji „Red October" wydaje się, że Polska wygląda bardzo dobrze, że nic tu się nie dzieje. Z naszego krótkiego badania wynika, że ta pewność pochodzi z co najwyżej 5 % całości danych, które trzeba by było przeanalizować aby być pewnym. A jakie jest według Ciebie prawdopodobieństwo, że faktycznie były infekcje i Polska nie powinna być zaznaczona na biało na tej mapie? Na ile na ocenę tego wpływa fakt, że w czasie ataku były przygotowane specjalne pliki, które miały posłużyć bezpośrednio do ataku na polskich użytkowników?**

MH: Jest wysoce prawdopodobne, że są infekcje i w Polsce. Wyniki które znamy pochodzą tylko z 3 serwerów ze wszystkich 35, w dodatku monitorowanych tylko przez kilka tygodni. Więc fakt, że na trzech serwerach nie odnotowano ruchu związanego z Polską to dobra wiadomość, ale nie znaczy, że nie było skutecznych ataków na Polskę. Mogły iść innymi serwerami lub mogły nastąpić w innym czasie. Tego nie wiadomo. Jest to bardzo prawdopodobne, że infekcje były. Jednak zupełnie nie przypominam sobie, abym słyszał o ukierunkowanych atakach na Polskę ze specjalnie stworzonymi plikami w języku polskim.

**MM: W operacji „Red October" była poruszona sprawa katyńska. Jeden z plików nosił nazwę „Katyn_-_opinia_Rosjan.xls". Katyń to jest nasz narodowy dramat związany z mordem polskich oficerów przez Sowietów. Teoretycznie po nazwie pliku można by się dowiedzieć co Rosjanie sądzą o polskiej tragedii w Katyniu. To dobrze dobrany element typu social engineering. Twórcy musieli być dobrze zorientowani w naszych wzajemnych relacjach co w pewien sposób potwierdza przypuszczenie o ich pochodzeniu z tej części świata.**

MH: I tu wracamy do wcześniejszego tematu ataków z Chin, Rosji i USA, jak już mówiłem, my nie widzimy bezpośredniej aktywności Rosji. Odnotowujemy dużą aktywność Chin i mam pewne obawy, że część z niej wcale tak na prawdę nie pochodzi z Chin tylko właśnie z Rosji.

**MM: Czy myślisz, że to kwestia współpracy czy raczej coś innego?**

MH: Myślę, że się podszywają. Każdy wie, że Chiny to robią, więc jeśli ktoś inny chce zaatakować, to używa chińskich serwerów, lub chińskiej wersji Worda do przygotowania plików aby wyglądało, że to Chiny. Sprytne, prawda?

**MM: Zgadzam się. Mam jeszcze inne pytanie. Kiedy cofamy się w czasie i patrzymy na złośliwe kody napisane w nawiązaniu do infrastruktury krytycznej, to mamy coś co dotyka jej symbolicznie – jak wirus Czarnobyl i coś co dotyka rzeczywiście jak Stuxnet. I oczywiście poziom potencjalnego zniszczenia przez te wirusy jest drastycznie odmienny. Ale tak w ogóle to osobiście mam wrażenie, że dotychczas tylko w niewielkim stopniu doświadczyliśmy skutków tego jaki jest potencjał w złośliwym oprogramowaniu atakującym infrastrukturę krytyczną. Czy Ty zgadzasz się z tą opinią?**

MH: Tak, zgadzam się. Jeszcze wszystkiego nie widzieliśmy. Jeśli będzie coś dużego, to będziemy o tym wiedzieli. Żyjemy w czasach głębokiego pokoju. Większość obecnych konfliktów jest w krajach, które się dopiero rozwijają, np. Afganistanie. Co wiemy o infrastrukturze teleinformatycznej Afganistanu? Jest bardzo słaba. Dlatego trudno tam o poważne zniszczenia. Jeśli weźmiemy np. taki kraj jak Iran, to tam nie ma wojny i nie ma ataków, ale jeśli np. USA wypowie Iranowi wojnę to aktywność znacznie się zwiększy i można się wtedy spodziewać ataków na wodę, elektryczność, transport.

**MM: To lekko przerażająca wizja, ale niestety prawdziwa. No cóż pozostaje nam robić swoje i pracować nad lepszym zabezpieczeniem infrastruktury krytycznej. Mikko, bardzo dziękuję za rozmowę**.

MH: Również dziękuję.

foto: FBC

# ZASADY TWORZENIA ZESPOŁU REAGOWANIA

## D A L S Z E  K R O K I

*Mirosław Maj*
*Fundacja Bezpieczna Cyberprzestrzeń*

**Niniejszy artykuł jest kolejnym artykułem dotyczącym zespołów CERT. W szczególności jest on kontynuacją artykułu przedstawiającego cztery pierwsze kroki związane z tworzeniem zespołu CERT, który ukazał się w drugim numerze biuletynu CIIP focus.**

W pierwszym artykule na temat tworzenia zespołów typu CERT omówione zostały cztery początkowe kroki z ośmioetapowego procesu tworzenia takiego zespołu. W niniejszym artykule przedstawione zostaną pozostałe cztery kroki.

Opisaliśmy dotychczas następujące kroki :

1. Poparcie tworzenia zespołu CERT przez zarząd.
2. Stworzenie planu strategicznego.
3. Zebranie istotnych informacji dla działania CERT.
4. Wizja CERT.

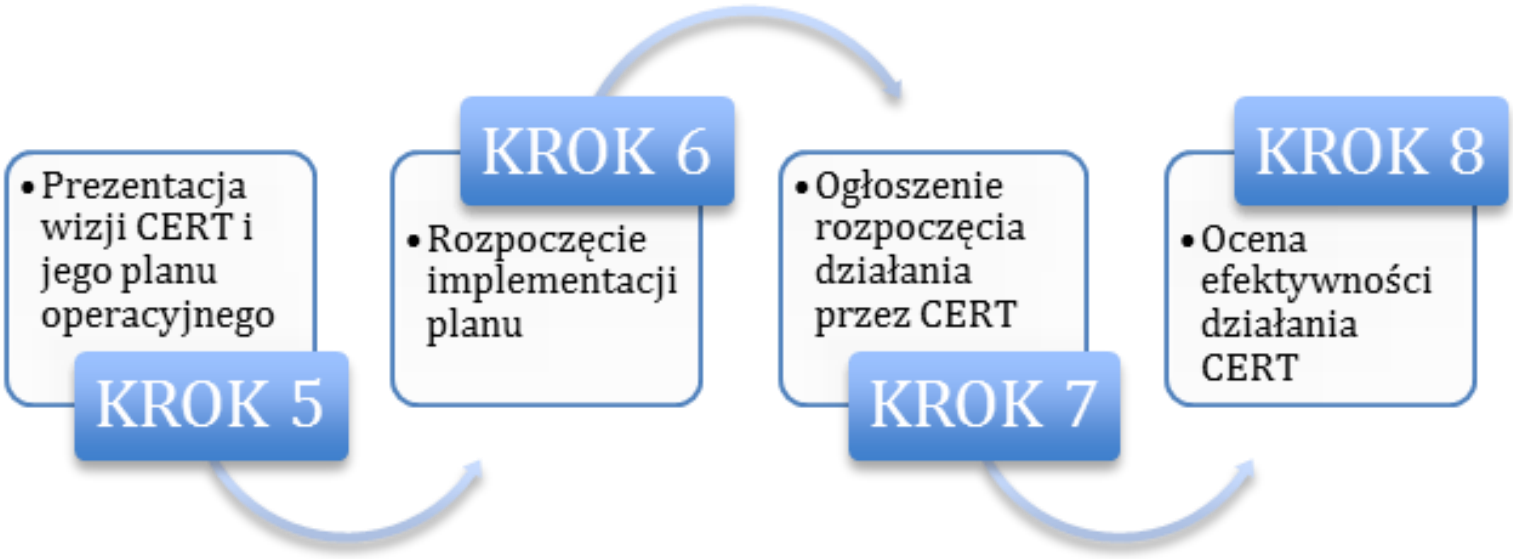
Pozostałe cztery kroki to:

5. Prezentacja wizji CERT i jego planu operacyjnego.
6. Rozpoczęcie implementacji planu.
7. Ogłoszenie rozpoczęcia działania przez CERT.
8. Ocena efektywności działania CERT.

Jak widać, chociażby po nazwach tych działań, w drugiej części całości procesu mamy już do czynienia z działaniami operacyjnymi, związanymi z budową zespołu. To zasadnicza zmiana w stosunku do części pierwszej, w której głównie dumaliśmy nad stworzeniem zespołu i zbieraliśmy wsparcie dla naszej idei.

### KROK 5
### PREZENTACJA WIZJI I PLANU OPERACYJNEGO

W sytuacji kiedy jest już znana i wstępnie zaakceptowana wizja zespołu oraz dokładny plan jego działania to warto tymi informacjami podzielić się z pozostałymi członkami organizacji. De facto chodzi tu nie tylko o kadry zarządzające, ale i o odbiorców naszych usług czyli naszą grupę docelową. tzw. *constituency.* To nic, że właściwie zarówno i wizja i plan powstały w oparciu o dane zebrane w kroku trzecim (zbieranie istotnych informacji dla działania CERT). Po tym zebraniu dane przeszły proces transforma-



cji w konkretny plan i warto zadać sobie pytanie, czy nie wystąpił tu efekt „głuchego telefonu" i za chwilę nie będziemy świadczyć usług lub działać według zasad nie do końca oczekiwanych przez tych, którym CERT ma służyć.

Proces ten tylko z pozoru może się wydawać prosty. Prawda jest taka, że o ile nie jest problemem stworzenie komunikatu i poproszenie o materiał zwrotny, o tyle jest nim z pewnością otrzymanie odpowiedzi. Dlatego trzeba zrobić wszystko, aby było to zadaniem prostym dla odpytywanego. Dobrą formą jest stworzenie i wykorzystanie formularza online, w którym dodatkowo ograniczymy otwarte pytania. Daje to dość sporą szansę na pozyskanie informacji. Jeśli do tego dodamy jeszcze pismo przewodnie od szefa organizacji, wskazujące na wagę komentarzy i uwag, o które prosimy, to powinien być to już zupełnie udany proces.

## KROK 6
## ROZPOCZĘCIE IMPLEMENTACJI PLANU

Jeśli w zespole odpowiedzialnym za tworzenie CERT-u mamy specjalistów technicznych, którzy narzekają na nadmiar teoretyzowania, w tej fazie wkraczamy w etap, który ich bardzo zadowoli. Być może część z nich będzie pochodzić z rekrutacji wewnętrznej lub zewnętrznej, która jest elementem tej fazy.

Najbardziej technicznym przedsięwzięciem jest zakup i implementacja sprzętu oraz budowa infrastruktury sieciowej. Oczywistym jest, że przy każdej z tych czynności obowiązują najwyższe standardy zapewnienia bezpieczeństwa. Zakładamy jednak, że osobom które zaangażowaliśmy do tego projektu nie będziemy musieli tego szczególnie tłumaczyć. To zresztą będzie pierwszy realny test ich wiedzy i umiejętności z tego zakresu.

Kolejnym bardzo ważnym zadaniem fazy implementacji planu jest przygotowanie się do procesu obsługi incydentów. Do tego zadania należy podejść od dwóch stron. Od strony zadań własnych oraz postępowania przez członków naszego *constituency*. Zadania własne to przygotowanie procedur i zasad działania, które odzwierciedlają nasze usługi, a w szczególności tę najważniejszą, czyli obsługę incydentów. W praktyce należy wziąć listę tego co ustaliliśmy, że będziemy robić i punkt po punkcie opisać jak będziemy to robić. Jaka będzie interakcja z usługobiorcą. Natomiast dla odbiorców naszych *usług* trzeba przygotować mniej lub bardziej szczegółowe wytyczne i materiały wspomagające, aby wiedzieli jak z nich skorzystać. Leży to jak najbardziej w naszym własnym interesie. Wiadomo - klient świadomy to mniej problemów dla nas w świadczeniu usługi. Doskonałym materiałem wspomagającym przeprowadzenie tej fazy są dostępne materiały przygotowane przez ENISA (European Network Information Security Agency), a w szczególności „Good Practice Guide for Incident Management"[1]. W materiale tym można też odnaleźć odniesienie do konkretnych ćwiczeń dla członków zespołów CERT, które mogą być pomocne przy realizacji zadania np.: ćwiczenia z budowy infrastruktury dla CERT[2], czy przygotowywania procedury obsługi incydentów[3].

## KROK 7
## OGŁOSZENIE ROZPOCZĘCIA DZIAŁANIA PRZEZ CERT

Nadszedł długo oczekiwany moment ogłoszenia, że nasz CERT rozpoczyna swoją działalność. Nie powinno to mieć jednak wiele wspólnego z „fanfarami". To ważny moment, który będzie bardzo wpływał na jakość dalszych relacji z usługobiorcami. Jest to wyjątkowa okazja, aby dotrzeć do nich z ważnymi informacjami. Dlatego informując o powstaniu i rozpoczęciu działalności trzeba pamiętać o:

1. Wysłaniu tego komunikatu przez możliwie najwyższej ustawioną w hierarchii kadrę zarządzającą. Jeśli jest to sam prezes dużej organizacji, to można informację podzielić na tę o charakterze strategicznym - „CERT powstał i działa", wysłaną przez prezesa i informację uzupełniającą - wysłaną przez upoważnioną przez prezesa inną osobę (np.: szefa CERT-u lub jego przełożonego).
2. Przekazaniu informacji na temat misji zespołu.
3. Przekazaniu podstawowych informacji dotyczących kontaktu z zespołem, jak godziny jego pracy i kanały komunikacji (telefon, email, system online).
4. Przekazaniu informacji o zakresie usług oferowanych przez CERT.
5. Przekazaniu informacji na temat postępowania w przypadku najczęściej występujących przypadków, które powinny być zgłaszane do CERT.

## KROK 8
## OCENA EFEKTYWNOŚCI DZIAŁANIA CERT

Ostatnim krokiem w całym procesie tworzenia CERT jest sprawdzenie jak działa nasz pomysł na CERT. Jest to krok, który jest potrzebny w praktyce dla wszystkich. Dla kadry zarządzającej, aby zweryfikować słuszność decyzji związanej z powołaniem zespołu. Dla odbiorców, aby byli świadomi, że CERT pełni funkcje pomocnicze i wspierające a jego priorytetem jest dostosowanie się do realnych potrzeb. Wreszcie dla samych członków zespołu, aby mieli poczucie dobrze realizowanej misji i weryfikowali wyniki swojej codziennej pracy. Minimalny okres po jakim warto dokonać oceny to kwartał. W praktyce okazuje się to najczęściej zbyt szybko i okres „rozliczeniowy" wydłużany jest do jednego roku.

Nie ma prostego sposobu na wymierną ocenę CERT-u. Zespoły, które istnieją (a jest ich na świecie kilkaset) bardzo różnią się od siebie. Dlatego warto od samego początku, już w fazie tworzenia zespołu, opracować zestaw mierników, który nam posłuży do oceny. Mierniki te można generalnie podzielić na te bezpośrednio odwołujące się do operacyjnych czynności zespołu, np.: liczba obsłużonych incydentów, liczba wykrytych incydentów (coraz częściej stosowany miernik, wraz z rozwojem proaktywnego podejścia do wykrywania incydentów), odsetek pozytywnie obsłużonych incydentów, liczba wydanych raportów technicznych i uświadamiających, komunikatów ostrzegających przed zagrożeniami itp. Druga grupa to mierniki odwołujące się do pewnego rodzaju badań nad jakością funkcjonowania zespołu. Do tego posłużyć mogą ankiety przeprowadzane z odbiorcami usług czy konsultacje i wnioski zebrane w ich trakcie.

Szczególną formą materiału służącą ocenie działania zespołu jest ankieta/badanie, które odnosi się do zasadni-

[1] http://www.enisa.europa.eu/activities/cert/support/incident-management

[2] http://www.enisa.europa.eu/activities/cert/support/exercise/exercise-4

[3] http://www.enisa.europa.eu/activities/cert/support/exercise/exercise2

| | |
|---|---|
| Dates of the control | |
| Controller | |
| Incident (reference no.) | |
| Was the procedure followed in handling the incident? | |
| Were all possible parties involved in the resolution of the incident? | |
| Did everybody fulfil the tasks according to his or her role in the team? | |
| Was the incident correctly classified? (compare the classification with other similar incidents) | |
| Was disclosure policy followed during incident handling? (and was the information exchanged correctly classified) | |
| Remarks | |
| Control rank (high / medium / low – score) | |
| Explanation of the control rank | |
| Things to improve | |

Formularz oceny jakości obsługi incydentów

źródło: ENISA Good Practice Guide for Incident Response

czej funkcji usługowej CERT-u, czyli badanie samego procesu obsługi incydentu. Można do tego wykorzystać formularz, który zawiera podstawowe pytania dotyczące tego procesu. Stanowi on swoistą, bardzo praktyczną listę kontrolną.

**PODSUMOWANIE**

Osiem kroków prowadzących do stworzenia zespołu typu CERT wydaje się procesem żmudnym i w niektórych przypadkach biurokratycznym. Warto jednak rzetelnie przez nie przejść, aby mieć pewność, że zrobiliśmy wszystko aby zespół działał poprawnie i zarówno jego członkowie jak i klienci byli zadowoleni, a wynik ich wspólnej pracy w sposób widoczny pozytywnie wpłynął na poziom bezpieczeństwa teleinformatycznego organizacji lub całego obszaru działania CERT-u.

Foto: http://www.publicdomainpictures.net - Anna Langova

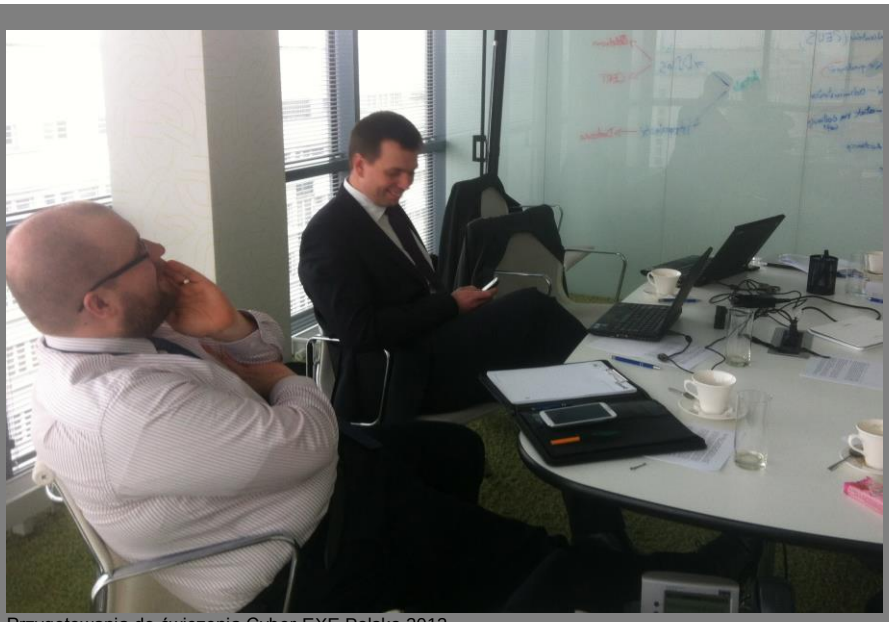
# CYBER-EXE POLSKA 2013

*Mirosław Maj*
*Fundacja Bezpieczna Cyberprzestrzeń*

Foto: http://www.publicdomainpictures.net GeorgeHodan

**Po udanym ćwiczeniu Cyber-EXE Polska 2012, o którym wielokrotnie pisaliśmy na łamach „CIIP focus", mieliśmy mocne przekonanie, że inicjatywa organizacji ćwiczeń z ochrony w cyberprzestrzeni powinna być kontynuowana. Jeszcze przed ogłoszeniem końcowego raportu z zeszłorocznego Cyber-EXE zaczęliśmy zastanawiać się, kiedy warto by zorganizować następne ćwiczenie. Zresztą pytanie brzmiało – nie tylko kiedy, ale też jakie to ma być ćwiczenie i kto powinien wziąć w nim udział?**

Powtórzenie ćwiczeń w gronie uczestników Cyber-EXE 2012 nie wchodziło w rachubę. Cykl przygotowań związany z organizacją ćwiczenia wskazywałby na to, że zespół projektowy powinien po podsumowaniu ćwiczenia z 2012 roku praktycznie od razu przystąpić do organizacji nowego. Nie było to możliwe. Chociażby dlatego, że po ćwiczeniu warto poświęcić odpowiednią ilość czasu na gruntowne zapoznanie się z wnioskami i wdrożenie rekomendacji. Wymaga to z pewnością dużo pracy i czasu. Wiemy, że obydwaj główni uczestnicy ćwiczeń, tzn. Gaz-System SA i PSE SA poważnie podeszli do wyników ćwiczenia i włożyli dużo pracy w to, aby z nich w pełni skorzystać. Jednoczesna praca przy kolejnych ćwiczeniach byłaby w związku z tym bardzo utrudniona.



Przygotowania do ćwiczenia Cyber-EXE Polska 2013.
Od prawej Jakub Teska (PKO BP) oraz Cezary Piekarski (Deloitte)

Dlatego w sytuacji, w której postanowiliśmy, aby z kolejną edycją czekać tylko rok, było jasne, że trzeba rozważyć przeprowadzenie ćwiczenia dla innego sektora. Co zresztą ma głęboki sens w postaci angażowania wielu sektorów do proaktywnych działań na rzecz poprawy bezpieczeństwa. Rozważania na temat tego jaki powinien to być sektor nie były długie ani trudne. Zdecydowanym faworytem był sektor finansowy, a w szczególności banki. Jego znaczenie dla funkcjonowania gospodarki i możliwości świadczenia podstawowych usług dla obywateli są oczywiste.

Pierwsza okazja do przetestowania tego pomysłu pojawiła się już w październiku 2012 r. w czasie I Kongresu Business Continuity Management. W trakcie Kongresu Maciej Pyznar (RCB) i Mirosław Maj (FBC) przedstawili przebieg ćwiczenia i pierwsze, jeszcze nieoficjalne wnioski. Na koniec prezentacji przedstawili też pomysł przeprowadzenia następnej edycji Cyber-EXE w roku 2013 dla sektora finansowego. Na reakcję nie trzeba było długo czekać. Instytucją, która zainteresowała się wsparciem takiej koncepcji była firma Deloitte Advisory sp. z o.o., a pierwsze konsultacje z potencjalnymi uczestnikami ćwiczenia miały pozytywny przebieg. Przystąpiono do uzgodnień dotyczących organizacji ćwiczenia. Podjęto decyzję o tym, że w 2013 r. zorganizowane zostanie ćwiczenie Cyber-EXE Polska dla sektora finansowego. Oficjalnym organizatorem ćwiczenia została Fundacja Bezpieczna Cyberprzestrzeń, a silnego wsparcia w organizacji udzielą

jej Rządowe Centrum Bezpieczeństwa i wspomniana już firma Deloitte Advisory sp. z o.o.

W tej chwili przygotowania do ćwiczenia idą pełną parą. Mamy za sobą 5 spotkań, w których wzięło udział już kilkanaście organizacji. Zawiązał się ścisły zespół projektowy, który ma za zadanie ustalić szczegółowe cele ćwiczenia, zarys scenariusza i skonstruować ostateczną grupę podmiotów uczestniczących w ćwiczeniu. O szczegółach scenariusza ćwiczenia rzecz jasna informować nie będziemy. Nawet członkowie zespołu projektowego nie mogą opowiadać o nim swoim współpracownikom w bankach. Możemy tylko zapewnić, że ćwiczenie będzie przebiegało najprawdopodobniej w dwóch ścieżkach, a zdarzenia które zaistnieją, będą odnosić się do najbardziej realnych zagrożeń dla sektora finansowego, zarówno w warstwie świadczenia usług detalicznych jaki i usług świadczonych pomiędzy członkami tego sektora. Trochę więcej być może zdradzają cele ćwiczenia. Celem głównym jest *zbadać zdolność i przygotowanie organizacji do identyfikacji zagrożeń w obszarze bezpieczeństwa teleinformatycznego, odpowiedzi na nie oraz współpracy w ramach sektora bankowego w odniesieniu do zaleceń Rekomendacji D Komisji Nadzoru Finansowego ze stycznia 2013 r., dotyczącej zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w bankach*. Jak widać chcemy aby ćwiczenie miało jak najbardziej praktyczny charakter stąd konkretne odesłanie do jednego z najważniejszych dla banków dokumentów z zakresu bezpieczeństwa teleinformatycznego, a mianowicie Rekomendacji D KNF. Zalecenia zawarte w tym dokumencie wejdą w życie 31 grudnia 2014 r. co oznacza, że banki czeka wiele pracy. Zakładamy, że udział w ćwiczeniu Cyber-EXE Polska 2013 może być dla nich bardzo pożyteczny i pomocny w wypełnieniu rekomendacji wydanych w styczniu tego roku.

Oprócz celu głównego przygotowane też zostały cele szczegółowe. Pierwszym z nich jest to, aby *sprawdzić zdolność do reakcji organizacji na atak teleinformatyczny*. Zeszłoroczne ćwiczenia pokazały, że niezależnie od tego jak bardzo organizacja jest przygotowana na taki atak, zawsze istnieje możliwość poprawy tego procesu. Zresztą dojrzałe organizacje w sposób systematyczny sprawdzają swoje plany i procedury działania. W przypadku teleinformatyki zazwyczaj te kontrole dotyczą klasycznych przypadków związanych z ciągłością działania – takich jak kłopoty z dostawą prądu czy katastrofa naturalna zmuszająca do uruchomienia awaryjnej procedury. Tym razem będziemy mieli do czynienia z atakiem teleinformatycznym i wydaje się, że jest to atrakcyjna perspektywa z punktu widzenia kontroli własnego przygotowania właśnie na ten rodzaj ataku.

Zakładamy, że ostatecznie w ćwiczeniu weźmie udział kilkanaście podmiotów. Ćwiczenie jest skierowane nie tylko do banków komercyjnych, ale również do innych bardzo ważnych instytucji sektora finansowego. Dlatego stanie się ono doskonałą okazją do *zidentyfikowania zależności i współzależności pomiędzy organizacjami i regulatorami rynku finansowego a innymi podmiotami.* Krótko mówiąc będziemy szukali synergii wynikającej z takiej współpracy. W szczególny sposób będziemy chcieli *sprawdzić komunikację między bankami oraz regulatorami i innymi podmiotami rynku finansowego.* Rzecz dotyczyć będzie przede wszystkim sprawdzania czy występuje i jak wygląda wymiana informacji o zagrożeniach i czy informacje te są przydatne i są wykorzystywane w praktyce.

Przed nami jeszcze wiele miesięcy przygotowań. Kilkanaście spotkań, prace w grupach roboczych i przygotowywanie szczegółowego scenariusza ćwiczenia. Punkt po punkcie, minuta po minucie. Wszystko po to, aby w drugiej połowie października, w ciągu jednego dnia przeprowadzić całodzienne ćwiczenie. Doświadczenia i rezultaty związane z organizacją Cyber-EXE Polska 2012 przekonały nas, że warto podjąć wysiłek. Mamy przekonanie, że doświadczenia metodyczne z zeszłego roku pozwolą nam na przygotowanie sprawnego i jeszcze lepszego ćwiczenia. Po pierwszej edycji, oprócz pracy nad wnioskami i rekomendacjami dla uczestników, wykonaliśmy jeszcze sporo pracy związanej z wyciągnięciem wniosków i przygotowaniem zaleceń związanych z organizacją ćwiczenia. Dotyczą one każdego z etapów ćwiczenia – jego identyfikacji, przygotowania, przeprowadzenia i podsumowania. Temat ćwiczenia z pewnością będzie systematycznie poruszany na łamach CIIP focus, dlatego serdecznie zachęcamy do śledzenia przygotowań, a potencjalnych uczestników do dołączenia do nas, gdyż jest jeszcze na to czas.


W trakcie I-go Kongresu BCM Maciej Pyznar (RCB) i Mirosław Maj (FBC) przedstawiali ideę organizacji ćwiczeń Cyber-EXE Polska dla sektora finansowego.

# Standard(owy) na BANK

*Kamil Kiliński*
*Citi Handlowy*

**Standard** – ustalone powszechnie obowiązujące kryterium, które określa najbardziej pożądane cechy np. wytwarzanego przedmiotu czy ludzkiego zachowania (norma kulturowa). Standard to czasem także podstawowa, najprostsza wersja produktu.[1]

W technice standard to zestaw parametrów, który zapewnia odpowiedni poziom jakości, **bezpieczeństwa**, wygody lub zgodności z innymi wytworami techniki (np. ISO nazwa standardu).

**Na każdym kroku, jako konsumenci, jesteśmy „bombardowani" różnymi standardami – czy to w przemyśle spożywczym czy w bankowości internetowej. Można śmiało zaryzykować stwierdzenie - dzisiejszy świat to świat standardów.**

Od kilku lat standardy stały się sztandarowym narzędziem porządkującym działania na wielu płaszczyznach. Od produkcji po konsumpcję. Nie wszystkie z tych standardów zrozumiałe są dla przeciętnego konsumenta. Konsument jednak nie potrzebuje ich zrozumieć by oczekiwać usług na najwyższym poziomie bezpieczeństwa. Na przykład klient banku oczekuje nie tylko produktów, ale również najwyższej jakości świadczonych przez bank usług. Banki tę jakość mogą zapewnić, właśnie poprzez wdrożenie standardów. Kolejnym elementem przemawiającym za stosowaniem standardów w codziennych rozwiązaniach jest duża konkurencja. Najlepszym tego przykładem jest sieć Internet, miejsce dynamicznego rozwoju pod względem stosowanych rozwiązań dla klientów. To, co jeszcze kilka lat temu wydało się niemożliwe, dziś otrzymujemy w standardzie. Jeszcze kilka lat temu, kiedy Internet rodził się w polskiej rzeczywistości, nikomu nie przyszło na myśl, że banki wprowadzą standard w zakresie obsługi klientów za pomocą bankowości elektronicznej. Dziś wydaje się to naturalną drogą – codziennością zarówno dla dostawców jak i odbiorców usług bankowych.

Ze standardami nieodzownie wiążą się normy. Dobry standard wymaga dobrego gruntu. I ten grunt zapewniają nam normy. Krajową jednostką normalizacyjną jest Polski Komitet Normalizacyjny (PKN) który stoi na czele wszystkich komitetów technicznych opracowujących normy. Należy podkreślić, że PKN nie jest odpowiedzialny za treść norm i nie jest urzędem tworzącym przepisy techniczne, nadzoruje jedynie zgodność procesów opracowywania norm z przepisami wewnętrznymi PKN. Zatwierdzenie projektu przez PKN jest formalnym stwierdzeniem tej zgodności i nadaniem projektowi statusu **normy krajowej**. Pomimo iż od 2003 roku nieprzestrzeganie postanowień PKN nie jest już naruszeniem prawa (normy stały się całkowicie dobrowolne) banki dążą do ich wdrażania.

Na świecie normalizacją zajmuje się Międzynarodowa Organizacja Normalizacyjna (ang. *International Organization for Standardization* – ISO). Jest ona odpowiedzialna za szereg norm, które wykorzystywane są przez organizacje zarówno państwowe jak i prywatne w codziennych pracach.

Również bankowość internetowa dopracowała się swoich norm bezpieczeństwa, nie tylko w zakresie transakcji elektronicznych czy systemu informatycznego, ale całego systemu informacji.

Coraz więcej Polaków korzysta z bankowości internetowej. W naszym kraju, według danych ZBP za IV kwartał 2012, już 20,8 mln[2] klientów indywidualnych ma podpisaną umowę umożliwiającą korzystanie z bankowości internetowej. Aktywnych użytkowników jest jednak mniej, ich liczbę szacuje się na ok. 11,4 mln. W Polsce odsetek klientów korzystających z bankowości online wynosi ok. 25%. Daje nam to 20 miejsce w Europie[3].

Dane statystyczne stanowiące ilustrację skali popytu i podaży oraz wskazujące

[1] Wikipedia
[2] Raport Bankowość Internetowa i Płatności Bezgotówkowe. Podsumowanie IV kwartału 2012 r. – http://www.zbp.pl/photo/konf19-03-13/raportIVkw2012.pdf
[3] Bankowość elektroniczna – Polsce daleko do czołówki w PRNews (Dostęp: 2011-12-16).

na duży potencjał rozwoju bankowych usług elektronicznych nasuwają pytanie, w jaki sposób banki dziś zapewniają bezpieczeństwo użytkownikom korzystającym z bankowości internetowej? Odpowiedzią są normy opracowane na potrzeby ujednolicenia zasad bezpieczeństwa informacji. Warte uwagi są normy zgrupowane jako ISO 27000.

**ISO 27000**

• ISO/IEC 27000 „Technika informatyczna - Techniki bezpieczeństwa - Systemy Zarządzania Bezpieczeństwem Informacji - Omówienie i słownictwo" – stanowi wprowadzenie do innych norm z tej grupy. Porządkuje definicje podstawowych pojęć związanych z bezpieczeństwem informacji.

• ISO/IEC 27001 „Technika informatyczna - Techniki bezpieczeństwa - Systemy Zarządzania Bezpieczeństwem Informacji - Wymagania" – określa specyfikację wymagań dla Systemów Zarządzania Bezpieczeństwem Informacji na zgodność z którą mogą być wydawane certyfikaty.

• ISO/IEC 27002 „Technika informatyczna - Techniki bezpieczeństwa - Praktyczne zasady zarządzania bezpieczeństwem informacji" – opisuje zbiór najlepszych praktyk związanych z budowaniem, użytkowaniem i rozwijaniem Systemu Zarządzania Bezpieczeństwem Informacji.

• ISO/IEC 27003 „Technika informatyczna - Techniki bezpieczeństwa - Porady i wskazówki dotyczące implementacji Systemu Zarządzania Bezpieczeństwem Informacji" – norma pomocna w procesie tworzenia i wdrażania Systemu Zarządzania Bezpieczeństwem Informacji.

• ISO/IEC 27004 „Technika informatyczna - Techniki bezpieczeństwa - Wskaźniki i pomiar w bezpieczeństwie informacji" – mierzenie i raportowanie efektywności Systemu Zarządzania Bezpieczeństwem Informacji.

• ISO/IEC 27005 „Technika informatyczna - Techniki bezpieczeństwa - Zarządzanie ryzykiem bezpieczeństwa informacji" – norma wzorowana na normie BS 7799-3. Prezentuje efektywne zarządzanie ryzykiem bezpieczeństwa informacji w systemach teleinformatycznych.

• ISO/IEC 27006 „Technika informatyczna - Techniki bezpieczeństwa - Wymagania dla jednostek prowadzących audyt i certyfikację Systemów Zarządzania Bezpieczeństwem Informacji" – dokument określa wymagania, jakie muszą spełniać instytucje wydające certyfikaty na zgodność z normą ISO/IEC 27001.

• ISO/IEC 27007 „Technika informatyczna - Techniki bezpieczeństwa - Wytyczne do audytów Systemów Zarządzania Bezpieczeństwem Informacji" – norma opisująca zagadnienia związane z prowadzeniem audytów i procesem certyfikacji SZBI.

• ISO/IEC 27011 „Technika informatyczna - Techniki bezpieczeństwa - Wytyczne w zakresie bezpieczeństwa informacji dla instytucji branży telekomunikacyjnej" – standard uzupełnia normy ISO/IEC 27001 i 27002 o dodatkowe wytyczne dla przemysłu telekomunikacyjnego.

• ISO/IEC 27799 „Informatyka medyczna - Wytyczne w zakresie wprowadzania normy ISO/IEC 17799 w sektorze medycznym" – wytyczne oraz wskazówki przy wdrażaniu normy ISO/IEC 17799 w sektorze medycznym.

Wśród ww. norm na szczególną uwagę zasługuje norma ISO 27001 opisująca wymagania dla Systemów Zarządzania Bezpieczeństwem Informacji. Składa się ona z dwóch głównych części: normy podstawowej, która zawiera definicję modelu zarządzania bezpieczeństwem informacji oraz załącznika A, zawierającego opis zabezpieczeń, które należy stosować w celu ograniczenia ryzyka.

Załącznik A jest obligatoryjny, zawiera jedenaście obszarów, mających wpływ na bezpieczeństwo informacji w organizacji:

1. polityka bezpieczeństwa
2. organizacja bezpieczeństwa informacji
3. zarządzanie aktywami
4. bezpieczeństwo zasobów ludzkich
5. bezpieczeństwo fizyczne i środowiskowe
6. zarządzanie systemami i sieciami
7. kontrola dostępu
8. pozyskiwanie, rozwój i utrzymanie systemów informatycznych
9. zarządzanie incydentami związanymi z bezpieczeństwem informacji
10. zarządzanie ciągłością działania
11. zgodność

Norma ta obejmując swoim zasięgiem zarówno obszary związane z bezpieczeństwem fizycznym, teleinformatycznym jak i prawnym, stanowi kompleksowe podejście do bezpieczeństwa informacji. Zaletą tej normy jest zwrócenie uwagi na problemy i zagrożenia bez wskazywania szczegółowych rozwiązań technicznych do zaimplementowania. Decyzja dotycząca rozwiązań technicznych pozostaje po stronie banku i powinna być poparta analizą potrzeb, ryzyka oraz możliwościami organizacji.

Pierwsze przymiarki do wdrożenia normy ISO 27001 Citi Handlowy rozpoczął w roku 2008. Wszystko zaczęło się od budowania świadomości wśród najwyższych managerów. Zadania tego podjął się dyrektor Departamentu Bezpieczeństwa Systemów Informatycznych (DBSI). W serii spotkań poświęconych tematowi, wraz z pracownikami departamentu przedstawiał czym jest norma ISO 27001, oraz korzyści płynące z jej wdrożenia. Jednym z najważniejszych argumentów przemawiających do menagerów była realna możliwość wykorzystania normy i stosowania jej w codziennych działaniach.

Rozpoczynając pracę nad wdrożeniem normy ISO 27001 w Citi Handlowy przyświecały słowa guru bezpieczeństwa Bruce'a Schneiera *Bezpieczeństwo to nie produkt, to proces*[1]. Hasło to stało się podstawą budowania świadomości, również na niższych szczeblach organizacji. Zrozumienie czym jest norma ISO 27001 i jakie korzyści daje organizacji jest niewątpliwie najważniejszym czynnikiem sukcesu. Brak zrozumienia korzyści płynących z ISO 27001 często prowadzi do sytuacji, w której ludzie skupieni są jedynie na realizacji swoich jednostkowych działań i nie angażują się w realizację całego projektu. Dlatego element budowania świadomości i przydatności takiej certyfikacji uważam za najważniejszy we wdrażaniu normy ISO 27001.

Zarząd dał „zielone światło" na wprowadzenie normy i maszyna ruszyła. Co ważne obszar bezpieczeństwa teleinformatycznego w Citi Handlowy od samego początku opierał się na międzynarodowych normach i standardach. Stanowiło to też doskonałą bazę podczas budowania obecnego, opartego o normy ISO, systemu zarządzania organizacji. Działania takie jak: opracowanie mapy proce-

[1] http://www.schneier.com/crypto-gram-0005.html

sów, budowa dokumentacji systemowej czy wdrożenie dokumentacji funkcjonowały w organizacji od lat.

Kolejnym etapem było powołanie komitetów oraz grup roboczych w poszczególnych obszarach organizacji tak, aby zapewnić spójność we wdrażaniu normy. DBSI będący liderem projektu wdrażania normy ISO 27001, został koordynatorem wszystkich działań. DBSI jest komórką, której główne działania koncentrują się na zapewnieniu bezpieczeństwa informacji. Jako najlepiej rozumiejąca ten obszar, będąca jednocześnie mentorem dla innych była najlepiej przygotowana do takich działań. Zarówno zaangażowanie w projekt, pełne zrozumienie mechanizmu działania normy jak i świadomość płynących z jej wdrożenia korzyści pozwala na stwierdzenie, że wybór DBSI i połączenie roli lidera i koordynatora było rozwiązaniem, które sprawdziło się doskonale. Poszczególne działania wynikające z harmonogramu prac omawiano na spotkaniach komitetów, o postępach prowadzonych prac na bieżąco informowany był Zarząd.

Certyfikacja ISO 27001 w Citi Handlowy przebiegała zgodnie z ustalonym procesem audytowym, podzielonym na trzy fazy:

**Faza 1: Przegląd dokumentacji**

**(faza określana również mianem gap analysis)**

Pierwszym krokiem na drodze wdrażania standardu ISO 27001 był przegląd dokumentacji procesów stosowanych w Citi Handlowy. Citi Handlowy posiadał szereg dokumentów opisujących procesy wewnątrz organizacji, w tym m.in. dokument regulujący bezpieczeństwo informacji. Dojrzałość procesów działających w innych obszarach była niewątpliwie dużym wsparciem dla wdrażania normy ISO 27001, a tym samym ważnym elementem w mapowaniu punktów normy ISO 27001 z Polityką Bezpieczeństwa Informacji i określeniu brakujących elementów. Można, więc powiedzieć, że zaawansowanie wszystkich procesów w Citi Handlowy pozwoliło nie tylko na efektywne, ale i sprawne zmapowanie Polityki Bezpieczeństwa Informacji z punktami normy ISO 27001.

**Faza 2: Audyt**

Citi Handlowy od samego początku miał jasno sprecyzowane oczekiwania w stosunku do audytorów. Oczekiwano niezależnego przeglądu systemu kontroli wewnętrznej. Audytorzy wskazywali obszary, które będą poddane próbie, koncentrując się na obserwacji danego obszaru.

Audytorzy rozpoczęli swoje działania od sprawdzenia dokumentacji. Kontrola ta miała na celu ocenę czy organizacja w pełni przygotowana jest do certyfikacji czy też wymagane są dalsze działania doskonalące na potrzeby późniejszego audytu. Drugim elementem sprawdzającym przygotowanie organizacji do przeprowadzenia audytu były wywiady z wybranymi osobami. Kolejnym elementem były czynności audytowe.

**Faza 3: Końcowe obserwacje**

Przedyskutowanie obserwacji poczynionych w trakcie audytu było ostatnim krokiem na drodze do uzyskania certyfikacji. W przypadku braku niezgodności[1] – co oczywiście jest najbardziej pożądaną sytuacją – droga do certyfikacji zostaje od razu otwarta. W sytuacji wystąpienia niezgodności dyskusja skupia się głównie na nich. W przypadku małych niezgodności, wydanie certyfikatu możliwe jest dopiero po trzymiesięcznym okresie naprawczym. Jeśli natomiast zaobserwowane zostaną duże niezgodności odstępuje się od wydania certyfikatu.

Na koniec kilka ważnych czynników, bez których osiągnięcie celu, jakim jest wdrożenie i uzyskanie certyfikatu[2] ISO 27001 byłoby bardzo trudne lub wręcz niemożliwe:

Zaangażowanie kierownictwa organizacji oraz wszystkich pracowników – bez tego czynnika nie można mówić o sukcesie wdrożenia ISO 27001. Na wdrożenie ISO 27001 pracują wszyscy pracownicy.

Jasno sprecyzowany zakres zarządzania bezpieczeństwem informacji - bez ograniczania go wyłącznie do jednego obszaru (np. tylko biuro lub system informatyczny), uwzględniając charakter działalności organizacji.

Szkolenie pracowników - w jaki sposób można zastosować normę ISO 27001 w codziennej pracy.

Uwzględnienie wszystkich form informacji – także nieelektronicznych - którymi są np. dokumentacja papierowa, nagrania rozmów telefonicznych czy notatki.

Wszystkich korzyści płynących z posiadania Certyfikatu ISO 27001 nie sposób wymienić. Najważniejszymi były: identyfikacja ryzyk biznesowych i ich minimalizacja dostosowanie do prawodawstwa RP i UE, ochrona zasobów firmy – zwiększenie bezpieczeństwa wewnętrznego, a także minimalizacja ryzyka niedostarczenia produktu, czyli niewykonanie usługi. Nie bez znaczenia były też prestiż oraz zwiększenie wartości marki banku. To tylko nieliczne przykłady.

*Kamil Kiliński - Od ponad 13 lat zajmuje się zagadnieniami ochrony informacji. Doświadczenie zdobywał w firmach z branży telekomunikacyjnej, medialnej oraz finansowej. Prowadził projekty na poziomie międzynarodowym w branży telekomunikacyjnej oraz finansowej. Odpowiadał za wykonywanie audytów bezpieczeństwa, analiz ryzyka, testów penetracyjnych. Definiował standardów w zakresie technicznych oraz organizacyjnych środków ochrony informacji. Brał czynny udział w analizie trendów oraz zagrożeń informacji. Projektował oraz wdrażał systemy zabezpieczeń w branży telekomunikacyjnej oraz finansowej.*

***Skontaktuj się z nami, wyraź opinię, zaproponuj temat – CIIP focus***

[1] tak było w przypadku City Handlowy

[2] Citi Handlowy jako jedyna instytucja finansowa w Polsce został podwójnie certyfikowany dokumentami o międzynarodowym znaczeniu - certyfikatem ISO 27001 w zakresie bezpieczeństwa oraz certyfikatem BS 25999 dotyczącym ciągłości biznesu. Niezależni Audytorzy uznali nasze procedury za zgodne z najwyższymi międzynarodowymi standardami.