Nr 6 – grudzień 2013

CIP focus

RCB
Rządowe Centrum Bezpieczeństwa

CYBER-EXE POLSKA 2013

www.publicdomainpictures.net

FUNDACJA bezpieczna cyberprzestrzeń

RCB
Rządowe Centrum Bezpieczeństwa

W numerze:

Szanowni Czytelnicy,

wydanie kolejnego numeru CIIP focusa zbiega się w czasie ze Świętami Bożego Narodzenia i końcem roku. Czas podsumowań i życzeń.

Przedstawiamy zatem na kartach biuletynu streszczenie z kolejnego ćwiczenia z cyklu Cyber – EXE Polska. Tegoroczne przeprowadzone zostały dla sektora bankowego. Opowiadają o nich Mirek Maj (moderator główny) i Maciek Pyznar (ewaluator). Z duchem minionych świąt wracamy jednak do wirusa STUXNET. Rozmawiamy o nim z Genadijem Reznikovem z białoruskiej firmy VirusBlokAda, która jako pierwsza go wykryła.

Rok 2014 przyniesie nowe wyzwania w sektorze IT. Nowym technologiom będą towarzyszyły nowe zagrożenia. Życzymy Państwu osiągniecia wysokiego poziomu bezpieczeństwa systemów IT w Państwa organizacjach. Nie chcemy jednak by na życzeniach skończyła się nasza pomoc. Zachęcamy zatem do lektury szczególnie dwóch ostatnich artykułów. W pierwszym z nich dr inż. Janusz Cendrowski w kompleksowy sposób omawia splendor norm dotyczących bezpieczeństwa informacji. W drugim Emil Wróbel wyjaśnia czym są ataki typu SQL Injection i jak się przed nimi bronić.

Zapraszamy do kontaktu – ciip-focus@rcb.gov.pl

Redakcja

NEWS NEWS NEWS

Chińczycy przyłapani na ataku na amerykański system uzdatniania wody

APT 1 to zespół, który wg ustaleń firmy Mandiant stanowi część chińskiej armii. Został przyłapany przez amerykańskiego badacza z Trend Micro na próbach włamania do systemów komputerowych odpowiedzialnych za sterowanie systemami obsługi stacji uzdatniania wody. Do przyłapania Chińczyków na gorącym uczynku wykorzystano system honeypotów imitujących prawdziwe systemy. Obserwacja działań atakujących wg badaczy nie pozostawia wątpliwości, że atak nie był przypadkowy i atakujący dobrze wiedzieli co jest ich celem.

http://bit.ly/JAVDav

Jak wyglądają botnety?

Bardzo ciekawą wizualizację botnetów można obejrzeć w serwisie globe.cyberfeed.net. Obracający się glob prezentuje wykryte botnety. Dodatkowo pojawiają się informacje jak dużo następuje połączeń botnetowych na sekundę, jak dużo zainfekowano maszyn w ciągu ostatniej doby i kraje gdzie botnetów jest najwięcej. Być może wykorzystanie praktyczne serwisu nie jest jego najsilniejszą stroną, ale z pewnością to doskonały materiał uświadamiający skalę naruszeń bezpieczeństwa w sieci.

http://globe.cyberfeed.net/

NEWS NEWS NEWS

Podręcznik ENISA dotyczący mitygacji ataków na ICS

Agencja ENISA wydała kolejną publikację. Tym razem dotyczy ona tematu najlepszych praktyk związanych z radzeniem sobie z atakami skierowanymi na systemy komputerowej kontroli procesów przemysłowych. W dokumencie znajduje się omówienie najbardziej rekomendowanych praktyk bezpieczeństwa zarówno postrzeganych jako działania techniczne jak i działania organizacyjne. Wiele z nich odnosi się do usług jakie świadczą dedykowane dla sektora infrastruktury krytycznej zespoły CERT-owe. O usługach tych pisaliśmy w poprzednim numerze „CIIP focus" w artykule poświęconym ICS-CERT.

http://bit.ly/1kh2jc4

Nauka wyniesiona z ataków na systemy SCADA

Kolejna publikacja aktywnej na polu ochrony IK Agencji ENISA. Tym razem opracowanie „Czy możemy się czegoś nauczyć na podstawie incydentów na systemy SCADA?". Pytanie retoryczne, aczkolwiek lektura wskazuje na to, że doświadczania te są podobne do tych mówiących o atakach na inne systemy. Niemniej jednak to treściwa lektura porządkująca proces obsługi incydentów związanych ze SCADA, ze szczególnym uwzględnieniem technicznego procesu zbierania i analizy śladów ataku. W dokumencie znajduje się też szczegółowa rozpiska zadań przypisanych odpowiednim stanowiskom związanym z techniczną i organizacyjną obsługą systemów SCADA.

http://bit.ly/J4PYZL

Projekt „SHINE" odsłania słabości systemów SCADA

Wydaje się, że systemy nadzorowania IK powinny być głęboko ukryte przed oczami Internautów. Tymczasem w ramach projektu SHINE codziennie wykrywanych jest od 2 000 do 8 000 tego typu systemów. W ciągu półtora roku trwania projektu wykryto ponad 1 000 000 systemów SCADA dostępnych przez Internet. W ocenie twórców projektu około 30% tych systemów może posiadać słabości pozwalające na przejęcie kontroli nad nimi. Większość wykrytych systemów dostępnych jest przez najbardziej popularne protokoły sieciowe, takie jak http, telnet, ftp czy SNMP. Trzeba przyznać, że dane brzmią przerażająco.

http://ubm.io/19cfWHA

Stuxnet wykryty w rosyjskiej elektrowni atomowej

W tym numerze dużo piszemy znowu o Stuxnecie publikując wywiad z przedstawicielem firmy VirusBlokAda. Właściwie od początku było wiadomo, że Stuxnet zaatakował nie tylko swoje podstawowe cele w Iranie. Naturą wirusa jest to, że nie do końca można kontrolować jego propagację. Dlatego co chwila dowiadujemy się o tym, że infekcje pojawiły się w różnych miejscach. Eugene Kaspersky wyjawił, że infekcje miały miejsce również na terytorium Rosji. Jest to raczej sensacja natury medialnej, ponieważ wiadomo że wirus miał kod dostosowany do specyficznej instalacji i tam mógł być tylko skuteczny. Ciekawsza jest informacja Kasperskiego, że budżet stworzenia tego typu wirusa to koszt minimum 10 mln $. To by potwierdzało angażowanie się w działania tego typu struktur państwowych.

http://bit.ly/19SdPD2

Podsumowanie, wnioski, rekomendacje

CYBER – EXE Polska 2013

Kiedy powstawał raport z poprzedniego ćwiczenia Cyber-EXE Polska 2012 (raport do pobrania ze strony www.cyberexepolska.pl w zakładce „Media") zaczęliśmy się zastanawiać jak powinno wyglądać następne ćwiczenie, a przede wszystkim kogo dotyczyć. Krytyczne znaczenie technologii informatycznych dla sektora finansowego w połączeniu ze szczególną rolą tego sektora dla indywidualnych odbiorców sprawiło, że już wtedy był on naszym „faworytem". Pozostało tylko zorganizować resztę.

Maciej Pyznar

Rządowe Centrum Bezpieczeństwa

Mirosław Maj

Fundacja Bezpieczna Cyberprzestrzeń

Jedną z najważniejszych rzeczy na początku organizacji ćwiczenia, poza zdecydowaną chęcią jego przeprowadzenia, jest zebranie grupy organizacyjnej. W grupie powinni się znaleźć partnerzy, którym zależy na przeprowadzeniu ćwiczenia, a jednocześnie mogą wnieść wkład merytoryczny, metodyczny lub logistyczny. Pierwszym partnerem został Deloitte, który już podczas prezentacji raportu z ćwiczeń Cyber-EXE Polska 2012 wyraził gotowość do wsparcia kolejnej edycji ćwiczeń (z czego skwapliwie skorzystaliśmy). Byłoby błędem nie skorzystanie z pomocy organizacji o takim potencjale i doświadczeniu. Oczywistym partnerem w organizacji kolejnego ćwiczenia było również RCB, które w kraju ma największe doświadczenie w organizacji ćwiczeń z udziałem dużej liczby podmiotów z różnych sektorów gospodarki i administracji. Wydaje się, że te doświadczenia poprzez zaangażowanie przedstawicieli RCB w organizację Cyber-EXE Polska 2013, były w jeszcze większym stopniu wykorzystane niż rok wcześniej. O tym, że RCB chętnie wspiera wszelkie inicjatywy mające na celu podniesienie bezpieczeństwa państwa wiadomo od dawna. Był to zatem oczywisty wybór i nie po raz pierwszy RCB podjęło się roli partnera organizacyjnego.

Grupa organizacyjna składała się ostatecznie z trzech podmiotów: Fundacji Bezpieczna Cyberprzestrzeń jako organizatora ćwiczenia oraz Deloitte Advisory Sp. z o.o. i RCB jako partnerów organizacyjnych.

Od czasu zawiązania się grupy ruszyły zasadnicze przygotowania do organizacji ćwiczenia Cyber-EXE Polska 2013. Zgodnie z wypracowaną w poprzedniej edycji metodyką rozpoczęła się faza identyfikacji, w której przede wszystkim pracuje się nad stworzeniem ostatecznej grupy podmiotów biorących udział w ćwiczeniu. Zarówno chęć uczestnictwa z ich strony jak i istotność występowania danego podmiotu w ćwiczeniu, ma decydujące znaczenie w formowaniu listy uczestników. W związku z tym, że adresatem ćwiczenia miał być sektor finansowy pierwsza faza przygotowań skoncentrowała się na określeniu celów ćwiczenia oraz pozyskaniu jego uczestników. W sformułowaniu celów ćwiczenia bardzo pomocna okazała się Rekomendacja D Komisji Nadzoru Finansowego dotycząca zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w bankach wydana w styczniu 2013 r., która w naturalny sposób pomogła wyznaczyć ramy i zakres tematyczny Cyber-EXE Polska 2013 r. W oczywisty sposób była ona katalizatorem decyzji banków o uczestniczeniu w ćwiczeniu, dlatego że łatwo można było sobie wyobrazić bardzo praktyczne wykorzystanie doświadczeń z ćwiczenia w realizacji zaleceń KNF, co jest jednym z głównych zadań dla środowiska bankowców w roku 2014.

Ostatecznie celem głównym ćwiczenia było zbadanie zdolności i przygotowania 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. Poza celem ogólnym konieczne stało się sformułowanie celów szczegółowych. Rekomendacja D zawiera listę 22 rekomendacji. Oczywistym więc było, że ćwiczenie nie obejmie swym zakresem wszystkich. Zdecydowano, że będzie dotyczyło:

1.Sprawdzenia zdolności reakcji organizacji na atak teleinformatyczny: sprawdzenia istniejących planów i procedur zarządzania, identyfikacji potrzeb ich uzupełnienia, aktualizacji lub stworzenia nowych, sprawdzenia współpracy i komunikacji wewnątrz organizacji.

2.Zidentyfikowania zależności i współzależności pomiędzy organizacjami i regulatorami rynku finansowego a innymi podmiotami.

3.Sprawdzenia komunikacji między bankami oraz regulatorami i innymi podmiotami rynku finansowego: sprawdzenia czy występuje wymiana informacji o zagrożeniach, sprawdzenia jakości i przydatności wymienianych informacji.

Jeśli chodzi o uczestników to wszyscy organizatorzy podjęli działania w celu skompletowania listy. Najskuteczniejszą i najczęściej wykorzystywaną formą zachęty do udziału w ćwiczeniu były bezpośrednie rozmowy organizatorów z potencjalnie zainteresowanymi podmiotami. Ostatecznie do Cyber-Exe Polska przystąpiło 6 banków, które stanowiły reprezentatywną dla sektora grupę, tak pod względem ich typów, formy własności, jak i udziału w świadczeniu usług drogą elektroniczną. Warto w tym miejscu wspomnieć również o tym, że ćwiczenie zdecydowały się objąć patronatem: Komisja Nadzoru Finansowego, Ministerstwo Finansów, Narodowy Bank Polski oraz Związek Banków Polskich.

Podmioty te wystąpiły również w charakterze bezpośrednich obserwatorów ćwiczenia, a ich przedstawiciele byli obecni na ćwiczeniu i mogli bezpośrednio obserwować jego przebieg i na

gorąco omawiać swoje spostrzeżenia.

Ustalenie celów i uczestników ćwiczenia zamknęło fazę identyfikacji. Mniej więcej od marca rozpoczęła się najważniejsza faza przygotowania ćwiczenia – faza planowania. To jej wynikiem miał być scenariusz. Nie będziemy odkrywać kuchni pracy nad scenariuszem. W każdym razie po kilkunastu spotkaniach uczestników ćwiczenia, organizatora i partnerów ćwiczenia udało się zbudować scenariusz składający się z dwóch wątków. Pierwszy z nich to atak DDoS, zaś drugi to dedykowany atak na wrażliwe dane uczestniczących banków, który był odpowiednikiem ataku wykonanego zgodnie z typowym zagrożeniem APT (Advanced Persistant Threat). Ważnym elementem fazy planowania było również ustalenie organizacyjnych i technicznych zasad przeprowadzenia ćwiczenia, w tym przydzielenie ról związanych z zarządzaniem ćwiczeniem oraz opracowanie instrukcji. Metoda pracy w mniejszych zespołach, wypracowana w czasie zeszłorocznego ćwiczenia, sprawdziła się i tym razem. W szczególności dużo pracy czekało członków grupy „SCENARIUSZ". Natomiast nowością, a tym samym dużym wyzwaniem, była organizacja ćwiczenia również w warstwie medialnej, o czym obszerniej poniżej.

Inaczej niż w poprzednim ćwiczeniu Cyber-EXE Polska zorganizowana została wymiana informacji pomiędzy moderatorem ćwiczenia a jego uczestnikami. Wprowadzony został moderator bankowy, który miał przekazywać wprowadzenia ze scenariusza i czuwać nad przebiegiem ćwiczenia wewnątrz instytucji. Oczywiście skomplikowało to organizację ćwiczenia i ograniczyło wpływ moderatora głównego na przebieg ćwiczenia wewnątrz ćwiczącej instytucji, ale pozwoliło spełnić jeden z podstawowych postulatów uczestników – konieczność zachowania poufność wrażliwych dla nich informacji związanych z reakcją na incydenty zaplanowane w scenariuszu. Moderator bankowy prawdopodobnie i tak musiałby zostać wprowadzony, gdyż w porównaniu do zeszłorocznego Cyber-EXE inaczej wyglądał również model przeprowadzenia ćwiczenia. Właściwie poprawnie byłoby napisać modele, gdyż uczestnicy zdecydowali się przeprowadzić je na trzy różne sposoby:

1) Zespołowe ćwiczenie sztabowe – w ramach którego uczestnicy są zorganizowani w zespół uprzednio powiadomiony o terminie, ogólnym zakresie oraz planowanym czasie trwania ćwiczenia. Zespół przebywa potencjalnie w jednym pomieszczeniu, a komunikacja między nimi ma charakter otwarty.

2) Model częściowej symulacji – w którym uczestnicy otrzymują informację o zbliżającym się ćwiczeniu, swoim udziale w nim, ale nie otrzymują dodatkowych informacji o samym scenariuszu, przedmiocie ćwiczenia czy oczekiwanej roli. Potencjalnie uczestnicy przebywają przy swoich stanowiskach pracy realizując również inne, codziennie obowiązki służbowe.

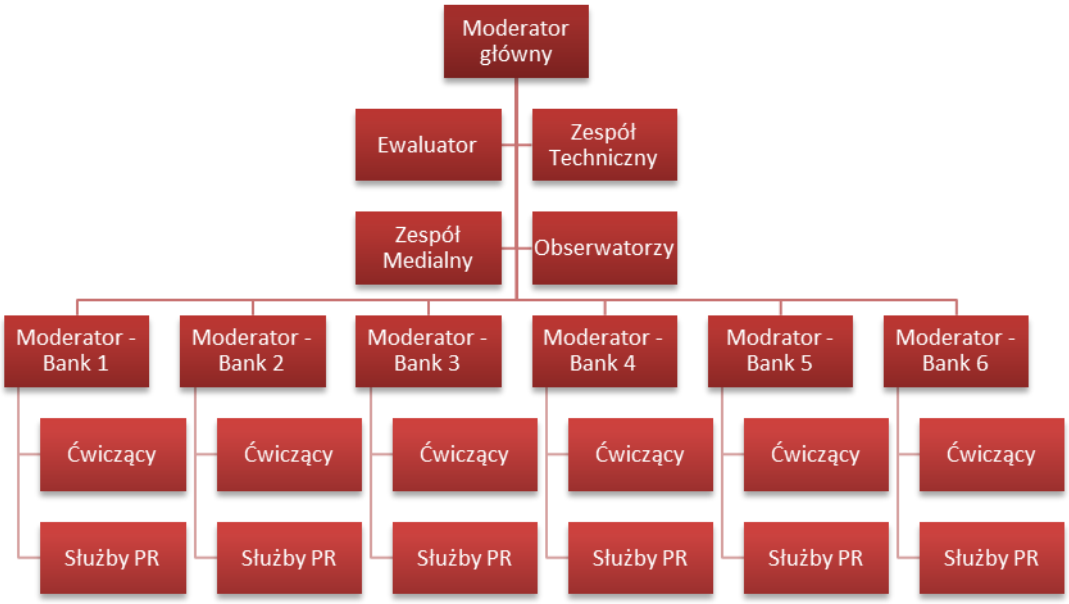
3) Model pełnej symulacji – w którym uczestnicy otrzymują informację o ćwiczeniach już w trakcie samego wydarzenia (np. w formie informacji dołączonych do „zdarzeń" – „UWAGA TO TYLKO ĆWICZENIE"). Grupa uczestników nie jest zdefiniowana i będzie się dynamicznie rozszerzać zależnie od przebiegu ćwiczenia w danej organizacji.

Kolejną nowością było włączenie do ćwiczenia służb prasowych uczestniczących banków – nie od dziś bowiem wiadomo, że „zła prasa" może bardzo zaszkodzić płynności finansowej banków. Reakcje służb prasowych banków w przypadku ataków teleinformatycznych uwzględnionych w scenariuszu jest niezwykle istotna i czasami ma krytyczne znaczenie, gdyż w dużym stopniu kształtuje odbiór sytuacji przez klientów banku, a tym samym ich reakcje, które mogą się na przykład skończyć masowym przenoszeniem kont z jednego banku do drugiego w wyniku dużego poziomu niezadowolenia.

Komunikacja medialna była prowadzona za pomocą platformy CISKOM. Jest to strona internetowa składająca się z dwóch części. W pierwszej, ukazują się informacje, które w sytuacji realnej byłyby przekazywane przez media (TV, radio, prasa, agencje informacyjne, portale internetowe i portale społecznościowe itp.). Za informacje na tej części platformy odpowiada występująca przy moderatorze głównym ćwiczenia grupa symulująca pracę mediów (osoby te w trakcie ćwiczenia „udają" dziennikarzy) oraz niezadowolonych klientów banków. Druga część strony internetowej jest miejscem, gdzie służby prasowe/PR podmiotów ćwiczących powinny prezentować swoje komunikaty i informacje oraz wszelką aktywność medialną w związku z daną sytuacją kryzysową.

Poprzednia edycja ćwiczenia Cyber-EXE Polska 2012 udowodniła, że ćwiczenie powinno mieć swoją „bazę", czyli miejsce gdzie w przyjaznych warunkach może się spotykać zespół planistyczny, gdzie wykuwa się scenariusz oraz podejmowane są istotne dla przebiegu ćwiczenia decyzje. Taką bazę w tegorocznej edycji ćwiczenia udostępnił Deloitte. W siedzibie Deloitte zorganizowano również Centrum Koordynacji Ćwiczenia

Struktura organizacyjna ćwiczenia



(CKC), gdzie 29 października moderator główny, wysyłając pierwsze wprowadzenie, rozpoczął ćwiczenie Cyber-EXE Polska 2013.

Przez następne 8 godzin wszyscy w CKC byli bardzo zajęci. Moderator główny, przy dużym wsparciu ewaluatora ćwiczenia i dodatkowego eksperta przekazywał kolejne wprowadzenia, podgrywał instytucje, które nie brały czynnego udziału w ćwiczeniu, a także zewnętrzne w stosunku do banków systemy teleinformatyczne, symulował również, przewidzianego w scenariuszu, szantażystę. Moderatorzy bankowi przekazywali wprowadzenia i koordynowali przebieg ćwiczenia wewnątrz swoich organizacji (czyt. czuwali, by ćwiczenie nie wymknęło się spod kontroli), podgrywali wewnętrzne systemy teleinformatyczne i co godzinę raportowali moderatorowi głównemu o sytuacji w organizacji. Zespół medialny pisał artykuły, pogrywał niezadowolonych klientów, dzwonił do rzeczników prasowych ćwiczących, odpowiadał na komunikaty medialne ćwiczących. Zespół techniczny wizualizował na podstawie raportów sytuację w ćwiczeniu oraz czuwał nad poprawnym działaniem wszystkich użytych urządzeń. Ewaluator wspomagał moderatora głównego, zbierał wnioski do raportu i przedstawiał sytuację w ćwiczeniu obserwatorom. Ćwiczenie było obserwowane przez przedstawicieli instytucji, które mu patronowały. Przygotowany został dla nich specjalny, dwugodzinny program, który obejmował: przedstawienie celów, sposobu przeprowadzenia oraz scenariusza ćwiczenia, wizytę w centrum kontroli ćwiczenia, relacje z przebiegu ćwiczenia, pokaz warstwy medialnej poprzez portal CISKOM.

Obserwatorzy przebywali w sali obok CKC, gdzie prowadzili ożywioną dyskusję na temat działań, które mogliby podjąć w przypadku zdarzeń proponowanych w scenariuszu ćwiczenia. W tym samym czasie Cyber-EXE Polska 2013 było już bardzo zaawansowane i tylko skupione twarze moderatorów bankowych zdradzały jak intensywnie przebiega ono wewnątrz ćwiczących organizacji. Około 16.00 moderator główny zaczął wygaszać ćwiczenie tzn. wysłał informację o konieczności dokończenia otwartych spraw i raczej ostudzenia zapału ćwiczących. Z ulgą odetchnęli zwłaszcza moderatorzy bankowi, ale i zespół medialny ocierał pot z czoła po intensywnych ośmiu godzinach pracy.

Teraz czas na opracowanie raportu, wyciągnięcie wniosków i wprowadzenie ewentualnych zmian. Już teraz serdecznie zapraszamy czytelników do lektury raportu, którego premiera planowana jest na 22 stycznia 2014 r.

W ćwiczeniu CEP13 bardzo ważną część stanowiły działania w warstwie medialnej na platformie CISKOM. Na zdjęciu przedstawicielki zespołu medialnego. Od lewej: Anna Adamkiewicz (RCB) Katarzyna Madej (RCB) Joanna Makowska (Deloitte), Adrianna Maj (FBC).

VirusBlokAda: STUXNET to praca zespołowa

Z Genadijem Reznikovem z białoruskiej firmy VirusBlokAda, która jako pierwsza wykryła wirusa Stuxnet i poddała go analizie, rozmawiamy o tym jak wykryto Stuxneta, jakie były pierwsze analizy i kto mógł być odpowiedzialny za jego przygotowanie.

CIIP focus: Jak w ogóle doszło do tego, że VirusBlokAda wykrył wirusa Stuxnet? W Jaki sposób weszliście w jego "posiadanie"?

Genady Reznikov: Jeden z naszych partnerów prowadzących sprzedaż naszych produktów w Iranie napisał do nas, że w Iranie pojawił się jakiś wirus, który nie jest rozpoznawany przez żaden z programów antywirusowych. Dodatkowo zaczął narzekać, że na niektórych z komputerów na których działało nasze oprogramowanie zaczął pojawiać się windowsowy „blue screen". Konieczne więc było abyśmy zajęli się sprawą. Poprosiliśmy, aby zorganizował nam zdalny dostęp do komputerów, na których pojawia się problem. Nasi specjaliści pracując z Mińska uruchomili na tych komputerach opracowany przez nas „anty-rootkit". W ten sposób znaleźliśmy nieprawidłowości w systemie Windows i pozyskaliśmy próbki złośliwego oprogramowania do dalszej analizy.

CIIP focus: Jak duży zespól nad tym pracował? Ile czasu zajęła analiza?

GR: Pracowało nad tym dwóch ludzi przez kilka dni. W tym czasie wykonali oni kilka szczegółowych analiz. Między innymi znaleźli lukę dotyczącą przetwarzania plików LNK (pliki LNK są jednym z rodzajów skrótów, które odwołują się do innych plików, wraz z możliwością dołączenia parametrów uruchomienia innego programu w systemie operacyjnym – przyp.red.), przebadali różne wersje systemu Windows w kontekście występowania podatności na atak, a także zbadali funkcje sterowników, w tym metody ukrywania się złośliwego kodu. Część szczegółowych badań odłożyliśmy do czasu otrzymania odpowiedzi z Microsoft i Realtek, których to dotyczyły podatności.

CIIP focus: Ile sami wywnioskowaliście na temat geograficznego i technicznego celu ataku?

GR: Niewiele. To, że miało to być skierowane na Iran bardziej wynikało z relacji naszego partnera oraz szeroko dyskutowane w mediach irański program atomowy i problemy, które jego dotyczą.

CIIP focus: Jednym z ważniejszych elementów siły Stuxneta było to, że wykorzystywał zaufane certyfikaty. Jak mogło dojść do ich przejęcia?

GR: Z naszego punktu widzenia te certyfikaty mogły być skradzione lub ktoś z dostępem do nich po prostu podpisał i autoryzował wirusa.

CIIP focus: Czy zdawaliście sobie sprawę z wagi swojego odkrycia?

GR: Tak, ponieważ to był zupełnie nowy wirus, więc jak tylko informacja o nim pojawiła się w bazie naszego antywirusa, informacje o wykorzystywaniu luk zostały wysłane do firmy Microsoft, a informacje o wykorzystaniu certyfikatów do Realtek. Po tym jak nie otrzymaliśmy żadnej odpowiedzi w ciągu trzech tygodni - próbki zostały wysłane do laboratorium firmy Kaspersky.

CIIP focus: Powszechnie wskazuje się na USA i Izrael jako twórców Stuxneta. Czy Wy sami prowadziliście jakieś dociekania na ten temat, które by to potwierdzały lub temu zaprzeczały?

GR: Mam swoją opinię na temat pochodzenia twórców wirusów. Nie mam wątpliwości, że stworzenie Stuxneta to była praca zespołowa, a w zespole byli ludzie, dla których rosyjski jest językiem ojczystym. Do tego aby dokładnie określić jakie kraje za tym stały trzeba by przeanalizować wiele wydarzeń jakie miały miejsce w różnych krajach, nie tylko w Stanach Zjednoczonych i Izraelu. Zaznaczam jednak, że to moje prywatne zdanie.

CIIP focus: Czy jest trend wskazujący na pojawianie się coraz większej liczby wirusów nastawionych na ataki na systemy SCADA?

GR: Logika wskazuje na to, że pojawia się coraz więcej szkodliwych programów, które za zadanie mają zakłócić działanie systemów kontroli i sterowania procesami przemysłowymi.

CIIP focus: Na koniec powiedz proszę kilka słów o tym czym się zajmuje VirusBlokAda? Czy badania złośliwego kodu to stały fragment Waszej pracy?

GR: Nasza firma zlokalizowana na Białorusi zajmuje się ochroną informacji przed złośliwym oprogramowaniem. Jesteśmy jedynym białoruskim podmiotem, który to robi. Mamy własny program antywirusowy. Został on stworzony w 1997 r. Posiadamy wszystkie niezbędne licencje i certyfikaty wydane w Republice Białorusi, aby to robić. Dotyczy to również norm jakości ISO.

CIIP focus: Czym było wykrycie Stuxneta dla Waszej firmy? Czy nastąpiła wyraźna zmiana po tym fakcie?

GR: Czym było? Mówiąc szczerze - trudno odpowiedzieć. Tak, trzeba przyznać że byliśmy bardzo zadowoleni, że udało nam się zapobiec zakażeniu na masową skalę tym wirusem w naszym kraju. Jakiejś szczególnej zmiany nie odczuliśmy. No może jedynie jesteśmy wskazywani palce, jako ci którzy znaleźli Stuxneta.

CIIP focus: Bardzo dziękuję za rozmowę i podzielenie się z nami tymi ciekawymi informacjami dotyczącymi Stuxneta.

GR: Ja również dziękuję.

Polskie Normy dotyczące bezpieczeństwa informacji wykorzystanie w ochronie teleinformatycznej infrastruktury krytycznej

INFORMACJA W NORMIE

dr inż. Janusz Cendrowski

Narodowy Program Ochrony Infrastruktury Krytycznej, opublikowany w tym roku przez Rządowe Centrum Bezpieczeństwa w załączniku drugim zaleca wykorzystanie Polskiej Normy PN–ISO/IEC 17799 [1] w celu zabezpieczenia systemów teleinformatycznych wchodzących w skład infrastruktury krytycznej. Wymieniono 11 obszarów, w których norma przedstawia zalecenia w zakresie bezpieczeństwa informacji. Należy się zgodzić z zaleceniem stosowania tej normy, tym bardziej że jest szeroko stosowana na świecie, ale wypada podkreślić, iż istnieje jeszcze wiele innych Polskich Norm dotyczących bezpieczeństwa informacji. Niniejsze opracowane jest poświęcone ich krótkiemu omówieniu.

Charakterystyka norm

Na świecie istnieje bardzo wiele technicznych Norm Międzynarodowych, Europejskich i Narodowych regulujących prawie wszystkie dziedziny techniki, technologii i produkcji. To jak wiele jest tych dziedzin świadczy fakt, że tylko w skład Polskiego Komitetu Normalizacyjnego wchodzi 315 Komitetów Technicznych (www.pkn.pl/kt/), z których każdy zajmuje się inną dziedziną. Normy dotyczące ochrony informacji są opracowywane głównie przez KT nr 182 „Ochrona informacji w systemach teleinformatycznych". Normy są sumą doświadczeń w tych dziedzinach, których dotyczą i powstają w wyniku szerokich konsultacji specjalistów danej dziedziny. Przykładowo podkomisja SC27 wchodząca w skład ISO/IEC JTC1, która ustanawia Normy Międzynarodowe dotyczące ochrony informacji gromadzi przedstawicieli 50 państw–członków i 18 państw–obserwatorów z całego świata (http://bit.ly/1cT3Vpa). Jedne normy są ogólne, inne są szczegółowe i rozwijają zagadnienia przedstawione skrótowo w normach ogólnych (będzie to szerzej opisane w kontekście rodziny norm 270xx). Zasadą jest pełne uregulowanie pewnego obszaru w serii (rodzinie) norm i przedstawienie przykładów, które mogą mieć treść informacyjną. Przykładowo podpisowi cyfrowemu jest poświęcony szereg następujących Norm Międzynarodowych (dla części z nich ustanowiono Polskie Normy), ale każda w innym obszarze a mianowicie:

a) Norma [2] – dotyczy podpisów cyfrowych z odtwarzaniem wiadomości opartych na faktoryzacji liczb całkowitych,
b) Norma [3] – dotyczy podpisów cyfrowych z odtwarzaniem wiadomości opartych na logarytmach dyskretnych
c) Norma [4] – dotyczy podpisów cyfrowych z załącznikiem opartych na faktoryzacji liczb całkowitych,
d) Norma [5] dotyczy podpisów cyfrowych z załącznikiem opartych na logarytmach dyskretnych.
e) Norma [6] dotyczy zastosowania algorytmów na krzywych eliptycznych w podpisach cyfrowych.

Normy Międzynarodowe są obojętne technologicznie, nie preferują żadnego konkretnego producenta systemów, urządzeń, czy też technologii. Mogą jednak zawierać opisy konkretnych algorytmów np. kryptograficznych, funkcji skrótu, ale jako załączniki informacyjne a nie normalizacyjne. Trochę inne podejście jest stosowane w normach krajowych. Przykładowo w normach NIST serii FIPS takie algorytmy jak AES, 3DES czy SHA-2 zostały uznane za standardy kryptograficzne.

Z drugiej strony nomy są obciążone wadami wynikającymi z trybu ich powstawania. Najważniejszą jest opóźnienie w stosunku do aktualnego rozwoju techniki. Wynika to z długiego czasu aktualizowania norm (w SC27 jest to z reguły 5 lat), który jest pochodną określonej procedury, uwzględniającej wiele etapów dyskusji, uzgodnień i wprowadzania poprawek. Z tym związana jest okresowa niespójność norm. Jeśli normy są merytorycznie związane, to aktualizacja jednej powinna spowodować aktualizację drugiej. Z reguły nie ma jednak możliwości, aby to zrobić jednocześnie i musi upłynąć kilka lat zanim będzie miała miejsce nowelizacja normy związanej.

Potrzeba norm w ochronie infrastruktury krytycznej

Nasuwa się pytanie, czy normy dotyczące ochrony informacji mają zastosowanie w ochronie systemów ICT wchodzących w skład infrastruktury krytycznej w tym samym, czy większym stopniu niż pozostałych systemów ICT. Z uwagi na fakt, że pewne systemy ICT zostały do tej infrastruktury zaliczone wypływa wniosek, że bardzo istotne jest zachowanie ich dostępności, niezawodności działania, poufności przetwarzanych danych (w kontekście udostępniania tylko użytkownikom uprawnionym), ich integralności czasie przechowywania, przesyłania i przetwarzania, oraz zachowania innych atrybutów bezpieczeństwa. A więc wszelkie wsparcie merytoryczne w tej dziedzinie takie jak przepisy prawa, normy, dobre praktyki, specjalistyczna wiedza i doświadczenie, które służą wyborowi właściwych zabezpieczeń jest jak najbardziej potrzebne.

Jaki jest powód wykorzystywania norm dotyczących bezpieczeństwa informacji, a nie tylko wiedzy i doświadczenia specjalistów? Można tu wymienić dwa powody, przy czym każdy w innym obszarze zastosowania.

1. Normy bardzo szczegółowe, dotyczące mechanizmów kryptograficznych (protokołów, algorytmów, trybów ich stosowania) służą projektantom systemów kryptograficznych. Bardzo wiele systemów aplikacyjnych bazuje na gotowych bibliotekach (interfejsach do urządzeń szyfrujących) implementujących SSL/TLS IPSEC, SSLVPN itp., ale w niektórych obszarach (np. w obszarze ochrony informacji niejawnych) zawsze będzie potrzeba opracowania własnych rozwiązań, które będą później certyfikowane. A więc mechanizmy kryptograficzne należy zaimplementować samodzielnie albo implementacje gotowych kodów źródłowe (open source) należy sprawdzić pod kątem zgodności z normami.

2. Normy dotyczące opracowania i wdrożenia SZBI, pomocne

w opracowaniu polityki bezpieczeństwa czy przeprowadzeniu szacowania ryzyka powinny służyć osobie odpowiedzialnej w organizacji (organie administracji, organizacji gospodarczej, instytucji użyteczności publicznej) za bezpieczeństwo informacji do zarządzania systemem bezpieczeństwa. Nie należy bowiem w obszarze bezpieczeństwa informacji polegać tylko na wysoko, ale wąsko wyspecjalizowanych informatykach. Tego rodzaju pracownicy są niezbędni, ale zawsze będą dążyli do ukierunkowania swojej pracy na obszary, które są im najlepiej znane, w których posiadają wiedzę udokumentowaną certyfikatami (bezpieczeństwo sieciowe, bezpieczeństwo baz danych i systemów operacyjnych, audyty bezpieczeństwa i testy penetracyjne, prowadzenie projektów informatycznych, a w ich ramach zarządzanie zmianą i konfiguracją itp). Pozostawią poza swoim obszarem zainteresowania pozostałe dziedziny zwłaszcza te nietechniczne, a związane z organizacją bezpieczeństwa. Dlatego tak ważna jest rola pracownika, który powinien objąć swoją uwagą wszystkie obszary zarządzania bezpieczeństwem informacji. NPOIK nazywa takiego pracownika „Kierownikiem bezpieczeństwa informacji". Warto zauważyć, że w obszarach ochrony informacji niejawnych i ochrony danych osobowych Ustawodawca powołał podobne role, a więc odpowiednio Pełnomocnika Ochrony i Administratora Bezpieczeństwa Informacji.

Polskie normy w zakresie bezpieczeństwa informacji

Komitet Techniczny nr 182 „Ochrona danych w systemach teleinformatycznych" Polskiego Komitetu Normalizacyjnego do tej pory opracował łącznie 34 Polskie Normy dotyczące ochrony informacji. Największa grupę (21 sztuk) stanowią szczegółowe normy poświęcone *kryptograficznym i niekryptograficznym technikom i mechanizmom zabezpieczeń*. W ich skład wchodzą m.in. normy dotyczące podpisów cyfrowych, technik uwierzytelnienia i PKI. *Kryteriom oceny bezpieczeństwa oraz metodyce testów bezpieczeństwa* poświęcone są 3 normy, szkoda że dwie z nich, będące implementacją Wspólnych Kryteriów (Common Criteria) [7] i [8] są nieaktualne i brak środków na ich nowelizację oraz ustanowienie trzeciej normy z tej serii. Dwie Polskie Normy powstały w obszarze *Aspektów bezpieczeństwa w zarządzaniu tożsamością, w biometrii oraz ochronie danych osobowych*. Po jednej Polskiej Normie opracowano w obszarach *Usług i aplikacji wspierających wdrożenie celów stosowania zabezpieczeń i zabezpieczeń* oraz *Terminologii*. Natomiast obszar, który jest najbardziej interesujący z punktu widzenia projektowania i wdrażania systemów zabezpieczeń w systemach teleinformatycznych, a mianowicie *Systemy zarządzania bezpieczeństwem informacji* (dalej SZBI) zapełnia 6 Polskich Norm – szczegóły w tabeli poniżej.

Wypada dodać, że nie tylko KT nr 182 opracowuje normy dotyczące bezpieczeństwa informacji. Inny Komitet Techniczny - KT nr 172 ds. „Identyfikacji Osób, Podpisu Elektronicznego, Kart Elektronicznych oraz Powiązanych z nimi Systemów i Działań" wydaje szereg Polskich Norm dotyczących kart elektronicznych (nieprawidłowo nazywanych „inteligentnymi" lub „chipowymi"), które maja szerokie zastosowanie w usługach uwierzytelnienia podmiotów i danych.

Inny Komitet Techniczny - KT nr 302 „Zastosowania Informatyki w Ochronie Zdrowia" wydał bardzo ważna normę PN–EN ISO 27799:2010 [11] do której odwołuje się 8 rozporządzeń Ministra Zdrowia, wykonawczych do Ustawy z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia, (Dz.U. nr 113, poz 657). Rozporządzenia te wymagają ponadto opracowania SZBI zgodnie z przepisami Ustawy z dnia 17.02.2005 o informatyzacji podmiotów publicznych (Dz.U. Nr 64, poz. 565) a więc zgodnie z dalej opisanym rozporządzeniem w sprawie Krajowych Ram Interoperacyjności. Rozporządzenia te będą istotne dla systemów, które powstają głównie w ramach platformy P1.

Również bardzo istotną norma jest dwuczęściowa PN–ISO/IEC 20000 [9] i [10] ustanowiona przez KT nr 171 ds. „Sieci Komputerowych i Oprogramowania", która zawiera wymagania i zalecenia w zakresie *dostarczenia zarządzanych usług o jakości akceptowalnej przez klientów*. Regulacje tej normy, zwłaszcza w zakresie zarządzania bezpieczeństwem informacji, łączą się z normami rodziny 27000 dotyczącymi SZBI,

Numer	Nazwa
PN–I–13335–1:1999	Technika informatyczna – Wytyczne do zarządzania bezpieczeństwem systemów informatycznych – Pojęcia i modele bezpieczeństwa systemów informatycznych
PN–ISO/IEC 17799:2007[1]	Technika informatyczna – Techniki bezpieczeństwa – Praktyczne zasady zarządzania bezpieczeństwem informacji
PN–ISO/IEC 27001:2007	Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania
PN–ISO/IEC 27005:2010	Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji
PN–ISO/IEC 27006:2009	Technika informatyczna – Techniki bezpieczeństwa – Wymagania dla jednostek prowadzących audyt i certyfikację systemów zarządzania bezpieczeństwem informacji
PN–ISO/IEC 27000:2012	Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Przegląd i terminologia

ustanawianymi przez KT nr 182.

Dodatkowe informacje o Polskich Normach i formach zakupu jest oczywiście dostępna na portalu www.pkn.pl

Normy rodziny 27000

Normy serii 27000 dotyczące ochrony informacji w zakresie SZBI tworzą strukturę hierarchiczna, która została przedstawiona na rysunku nr 1.

Najbardziej ogólną normą tej rodziny jest ISO/IEC 27000, której polskim odpowiednikiem jest PN–ISO/IEC 27000:2011 [12]. Zawiera ona krótkie omówienie wszystkich pozostałych norm tej rodziny, definicje i skróty w nich stosowane. Te ostatnie, w polskiej wersji tej normy, można uważać za najbardziej aktualne i uzgodnione w szerokim gronie specjalistów.

Dwie następne w hierarchii, to najważniejsze, z punktu widzenia organizacji potrzebujących wymagań i wytycznych w zakresie bezpieczeństwa informacji, normy ISO/IEC 27001 i ISO/IEC 27002, których polskimi odpowiednikami są [13] i wspomniana już [1].

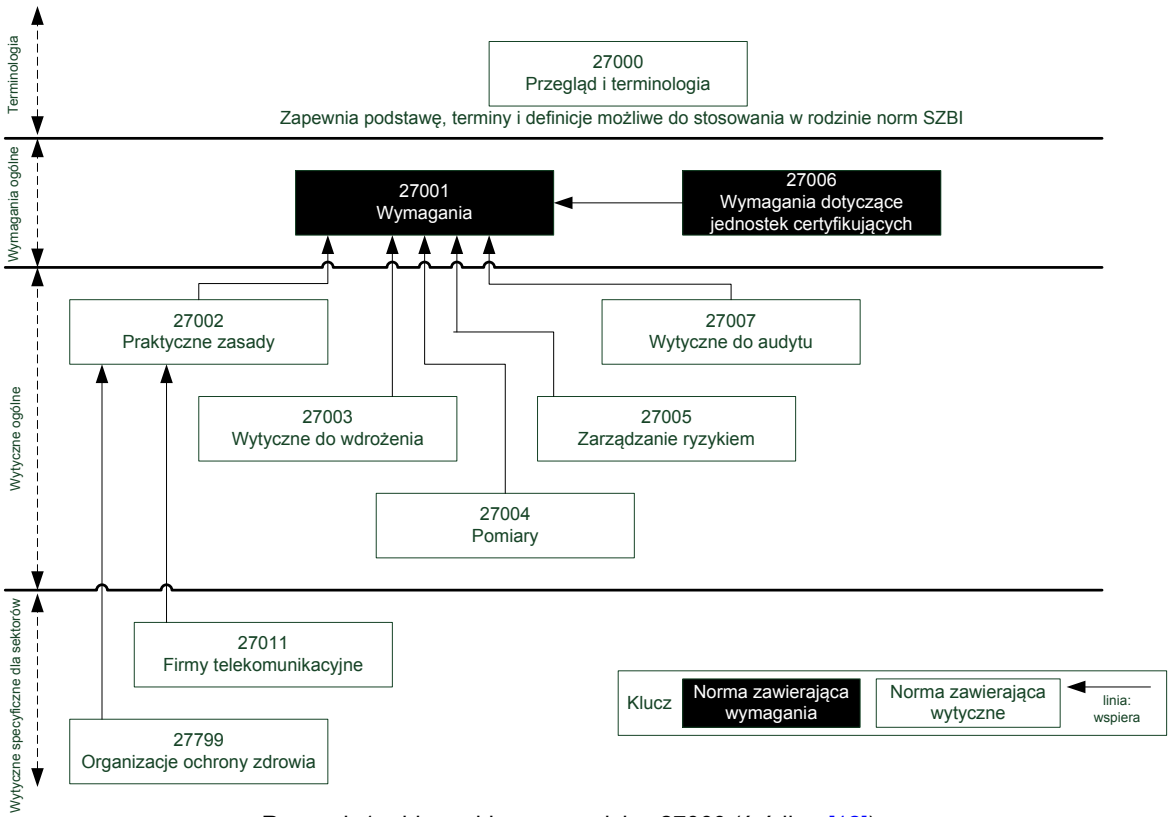
Norma [1], zawierająca zalecenia w zakresie zarządzania bezpieczeństwem informacji została omówiona w dokumencie NPOIK. Polska Norma PN–ISO/IEC 27001:2007 jest z nią tematycznie bardzo związana ale nie zawiera opcjonalnych zaleceń, ale restrykcyjne wymagania w dwóch dziedzinach:

1. Opracowania, implementacji, monitorowania i udoskonalenia Systemu Zarządzania Bezpieczeństwem Informacji, które to wymagania są wymienione w głównej części normy;

2. Wdrożenia celów zabezpieczeń i zabezpieczeń wymienionych w załączniku A normy, które to zabezpieczenia są uogólnieniem rozdziałów normy [1] w takich obszarach jak:
a. Polityka bezpieczeństwa;
b. Organizacja bezpieczeństwa informacji;
c. Zarządzanie aktywami;
d. Bezpieczeństwo zasobów ludzkich;
e. Bezpieczeństwo fizyczne i środowiskowe;
f. Zarządzanie systemami i sieciami;
g. Kontrola dostępu;
h. Zarządzanie ciągłością działania;
i. Pozyskiwanie, rozwój i utrzymanie systemów informatycznych;
j. Zarządzanie incydentami związanymi z bezpieczeństwem informacji;
k. Zgodność z wymaganiami prawnymi i własnymi standardami

Istotność normy PN-ISO/IEC 27001 polega na tym, że służy jako podstawa do wdrożenia SZBI w każdym podmiocie publicznym zgodnie z § 20 rozporządzenia w sprawie Krajowych Ram Interoperacyjności [14]. Rozporządzenie zakłada również wykorzystanie norm [1] i [15]. Zgodnie z § 23 dla systemów teleinformatycznych podmiotów realizujących zadania publiczne należy wdrożyć systemy SZBI nie później niż w dniu ich pierwszej istotnej modernizacji przypadającej po wejściu w życie rozporządzenia.

Dla infrastruktury krytycznej ma to kapitalne znaczenie, gdyż oznacza pełne i kompleksowe podejście do wdrażania bezpieczeństwa informacji. Pewnym dysonansem, na który trzeba zwrócić uwagę, jest fakt, że ww. rozporządzenie wiąże wdrożenie SZBI z wdrożeniem systemu teleinformatycznego podczas gdy norma wyraźnie wymaga, aby zakres SZBI obejmował całą lub część organizacji. Być może podejście Ustawodawcy można wytłumaczyć tym, że część informacji w podmiotach publicznych (zwłaszcza administracji publicznej) należy do obszaru informacji niejawnych i nie może być formalnie objęta wymaganiami normy PN–ISO/IEC 27001 skoro regulują ją przepisy o ochronie informacji niejawnych, a w zakresie



Rysunek 1 – hierarchia norm rodziny 27000 (źródło - [12])

ochrony systemów teleinformatycznych dodatkowo zaleceniami ABW i SKW.

Wiele organizacji posiadających i zarządzających systemami ICT wchodzącymi w skład infrastruktury krytycznej nie jest podmiotami publicznymi tylko firmami komercyjnymi i nie podlegają przepisom ww. rozporządzenia. Z drugiej strony tego rodzaju firmy często wdrażają SZBI i certyfikują je, doceniając pozytywny wpływ takiego wdrożenia na bezpieczeństwo informacji biznesowych (formalnie tajemnicy przedsiębiorstwa) oraz na podniesienie swojej konkurencyjności.

Kolejna Polska Norma - PN–ISO/IEC 27005:2011 [15] jest z kolei przewodnikiem po zarządzaniu ryzykiem w bezpieczeństwie informacji. Opisuje poszczególne etapy zarządzania ryzykiem przedstawione schematycznie na rysunku nr 2 i formułuje w tym zakresie szereg zaleceń, jak te etapy realizować. Przedstawia strategie postępowania z ryzykiem, a więc: redukowanie ryzyka, zachowanie ryzyka, unikania ryzyka, transfer ryzyka.

Warto odnotować, że oprócz tej normy inny Komitet Techniczny - KT nr 6 ds. „ Systemów Zarządzania" ustanowił dwie inne normy dotyczące zarządzania ryzykiem: PKN–ISO Guide 73 [16] oraz PN–ISO 31000:2012 [17]. W odróżnieniu od normy PN–ISO/IEC 27005:2001 pierwsza jest norma terminologiczną, a druga zawiera zalecenia bardziej ogólne dedykowane do zarządzania ryzykiem biznesowym, operacyjnym itp. Uwzględnia ona systemy informacyjne, ale nie koncentruje się na nich.

Oczekiwane zmiany i postulaty

Wypada jeszcze dodać, że w związku z pojawieniem się w SC27 nowych norm międzynarodowych lub nowych wersji norm już istniejących, KT nr 182 przygotował w tym roku projekty następujących nowych Polskich Norm:

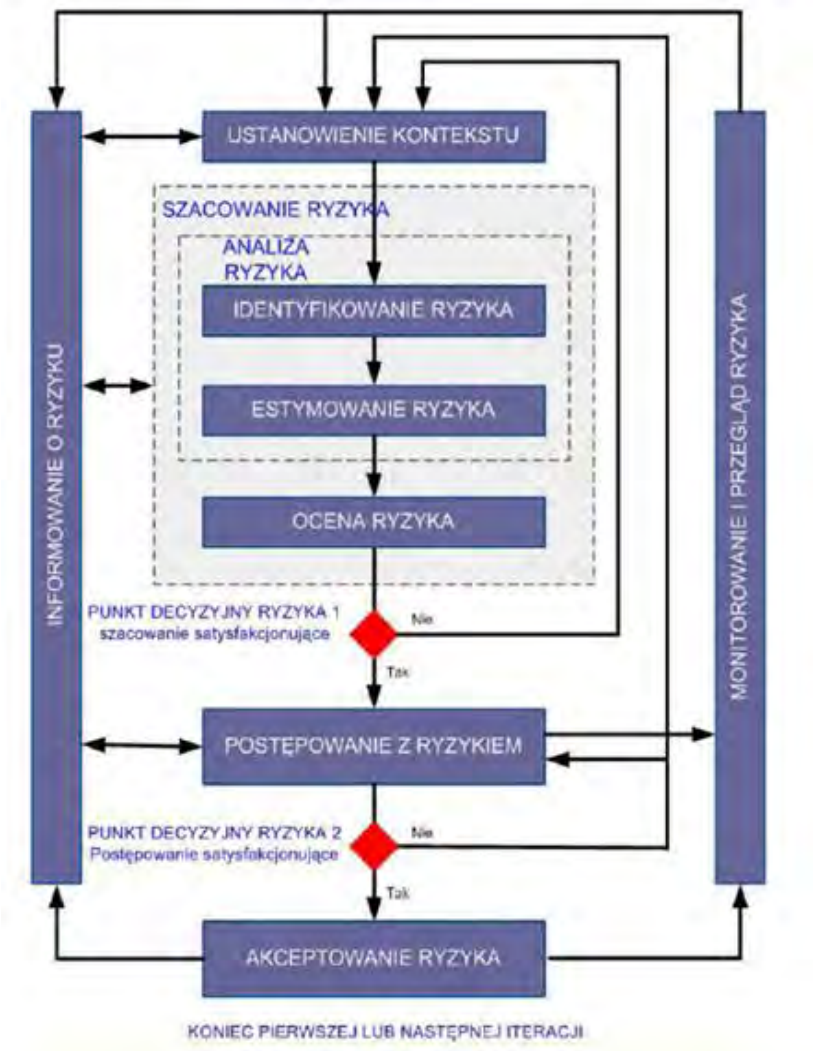
a. Pr PN–ISO/IEC 27006 Technika informatyczna – Techniki bezpieczeństwa – Wymagania dla jednostek prowadzących audyt i certyfikację systemów zarządzania bezpieczeństwem informacji (dostosowanie do zmian, które wprowadzono w ISO/IEC 27006:2011),

b. Pr PN–ISO/IEC 27005 Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji (dostosowanie do zmian, które wprowadzono w ISO/IEC 27006:2011),

c. Pr PN–ISO/IEC 27013 Technika informatyczna – Techniki bezpieczeństwa – Wytyczne do zintegrowanego wdrożenia ISO/IEC 27001 oraz ISO/IEC 20000–1 (norma nowa na podstawie ISO/IEC 27013).

Natomiast w KT nr 171 powstaje projekt Pr PN–ISO/IEC 20000–1, nowej w stosunku do [9] w związku ze zmianami w normie źródłowej, a mianowicie pojawieniu się nowej wersji ISO/IEC 20000:2011.

Co ważniejsze, jeszcze w tym roku oczekuje się ustanowienie przez ISO/IEC JTC1 SC27 nowych wersji ISO/IEC 27001 i ISO/IEC 27002. W niniejszym artykule brak miejsca na omó-



Proces zarządzania ryzykiem w bezpieczeństwie informacji (źródło - [15])

wienie zmian, warto jednak podkreślić, że są one bardzo znaczące, a osoby zajmujące się wdrożeniem lub audytem systemów SZBI będą musiały zmienić częściowo swoje podejście do budowania SZBI, bardziej uwzględniając uwarunkowania biznesowe w szacowaniu ryzyka. Ponadto niezbędne będzie dla tych specjalistów szczegółowe zapoznanie się z nową normą ISO/IEC 27002, na podstawie której zostały opracowane wymagania załącznika nr A do normy. Tu zmiany poszły jeszcze dalej niż w części głównej normy.

Na zakończenie warto wskazać, jakie potrzeby istnieją w zakresie normalizacji, które by korelowały z infrastrukturą krytyczną. Niewątpliwie ważną kwestią dla infrastruktury krytycznej jest zapewnienie ciągłości działania i odtwarzanie po katastrofie. Istnieje Polska Norma PN–ISO/IEC 24762 [18], która jednak jest normą szczegółową w zakresie usług odtwarzania. Potrzeba natomiast przede wszystkich norm ogólnych, które zawierałyby zalecenia i wymagania w zakresie opracowywania polityki ciągłości, analizy wpływu, budowania i testowania planów BCP/DRP.

W tym kontekście warto byłoby podjąć inicjatywę opracowania polskich odpowiedników norm ISO/IEC 22301 [19], ISO/IEC 22301 [20] oraz ISO/IEC 22313 [21].

Podsumowanie

Które z wymienionych norm są istotne dla systemów teleinformatycznych wchodzących w skład infrastruktury krytycznej? Można zaryzykować stwierdzenie, że kierownik bezpieczeństwa informacji powinien poznać je wszystkie. Następnie na podstawie PN-ISO/IEC 17799 powinien wypracować pierwszą politykę bezpieczeństwa informacji, aby stworzyć podstawę do dalszych działań. Gdy polityka już się przyjmie w organizacji, to można opracowywać i wdrażać (samodzielnie bądź z pomocą firm zewnętrznych) System Zarządzania Bezpieczeństwem Informacji biorąc za podstawę wymagania PN-ISO/IEC 27001. W pierwszym etapie opracowania będzie potrzeba posiłkowania się PN-ISO/IEC 27005 w celu opracowania metodyki szacowania ryzyka. Koniec wdrożenia SZBI celowo jest zakończyć opracowaniem planów ciągłości działania i odtwarzania po katastrofie a tu zacząć trzeba od normy [21].

Dr inż. Janusz Cendrowski, uczestniczy w tworzeniu Polskich Norm od roku 1994, aktualnie reprezentuje Asseco Poland w KT nr 182 w PKN

Bibliografia

[1] PN–ISO/IEC 17799:2007 Technika informatyczna – Techniki bezpieczeństwa – Praktyczne zasady zarządzania bezpieczeństwem informacji

[2] ISO/IEC 9796–2:2010 Information technology – Security techniques – Digital signature schemes giving message recovery – Part 2: Integer factorization based mechanisms

[3] ISO/IEC 9796–3:2006 Information technology – Security techniques – Digital signature schemes giving message recovery – Part 3: Discrete logarithm based mechanisms

[4] ISO/IEC 14888–2:2008 Information technology – Security techniques – Digital signatures with appendix – Part 2: Integer factorization based mechanisms

[5] ISO/IEC 14888–3:2006 Information technology – Security techniques – Digital signatures with appendix – Part 3: Discrete logarithm based mechanisms

[6] ISO/IEC 14888–3:2006/Amd 1:2010 Elliptic Curve Russian Digital Signature Algorithm, Schnorr Digital Signature Algorithm, Elliptic Curve Schnorr Digital Signature Algorithm, and Elliptic Curve Full Schnorr Digital Signature Algorithm

[7] PN–ISO/IEC 15408–1:2002 Technika informatyczna – Techniki zabezpieczeń – Kryteria oceny zabezpieczeń informatycznych – Wprowadzenie i model ogólny

[8] PN ISO/IEC 15408–3: 2002 Technika Informatyczna – Techniki zabezpieczeń – Kryteria oceny zabezpieczeń informatycznych – Wymagania uzasadnienia zaufania do zabezpieczeń

[9] PN–ISO/IEC 20000–1:2007 – Technika informatyczna – Zarządzanie usługami – Część 1: Specyfikacja;

[10] PN–ISO/IEC 20000–2:2007 – Technika informatyczna – Zarządzanie usługami – Część 2: Reguły postępowania.

[11] PN–EN ISO 27799:2010 [11] Informatyka w ochronie zdrowia – Zarządzanie bezpieczeństwem informacji w ochronie zdrowia z wykorzystaniem ISO/IEC 27002

[12] PN–ISO/IEC 27000:2011 Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Przegląd i terminologia

[13] PN–ISO/IEC 27001:2007 Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania

[14] Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych Dz.U. z 2012 poz. 526.

[15] PN–ISO/IEC 27005:20011Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji

[16] PKN–ISO Guide 73:2012 Zarządzanie ryzykiem – Terminologia

[17] PN–ISO 31000:2012P Zarządzanie ryzykiem – Zasady i wytyczne

[18] 24762] PN-ISO/IEC 24762:2010 Technika informatyczna - Techniki zabezpieczeń - Wytyczne dla usług techniki teleinformatycznej odtwarzania po katastrofie

[19] ISO 22300:2012 Societal security – Terminology

[20] ISO 22301:2012 Societal security – Business continuity management systems – Requirements

[21] ISO 22313:2012 Societal security – Business continuity management systems – Guidance

Raport ENISA za rok 2012 na temat najpoważniejszych incydentów w sieciach operatorów telekomunikacyjnych.

INCYDENTY W TELEKOMACH

Europejska Agencja Bezpieczeństwa Sieci i Informacji (ENISA) opublikowała raport dotyczący incydentów zgłoszonych do ENISA w 2012, które wynikały z realizacji zapisów tzw. Artykułu 13a. Na początku warto zwrócić uwagę, że to już drugi raport od momentu wprowadzenia obowiązku zgłaszania takich przypadków w europejskiej dyrektywie telekomunikacyjnej. Ten obowiązek dotyczy operatorów telekomunikacyjnych, którzy muszą raportować do krajowych władz regulujących rynek telekomunikacyjny.

W 2012 roku do Agencji zgłoszono 51 takich przypadków (dotyczyły one roku 2011), zaś w tym roku tych przypadków było 79. Jednak przyrost nie jest tak dynamiczny jak wskazują te liczby, ponieważ jest on mocno uwarunkowany liczbą krajów, które raportowały. W zeszłym roku było ich 20, zaś w tym już 28. Nie wszystkie raportujące kraje odnotowały poważne incydenty. Tych, które odnotowały było tylko 18. Nie znamy jednak szczegółów co do tego, który z krajów raportował, a który nie. Który i ile miał incydentów i jakie to były incydenty. Wszelkie szczegóły objęte są tajemnicą. Jeśli chodzi o Polskę to należy podejrzewać, że znaleźliśmy się w gronie krajów nieraportujących. Dlaczego? Otóż implementacja artykułu 13a dyrektywy telekomunikacyjnej w polskim prawodawstwie nastąpiła dopiero w listopadzie 2012 r. Odpowiednie zapisy znalazły się w nowym Prawie Telekomunikacyjnym, które weszły w życie w styczniu tego roku, a wzór formularza informującego o naruszeniu bezpieczeństwa lub integralności sieci (swoją drogą integralność jest jedną z cech bezpieczeństwa, więc przy okazji może warto usunąć ten błąd definicyjny) opracowano dopiero 19 marca b.r. Trudno więc przypuszczać, żeby ktoś wcześniej zdecydował się na takie zgłoszenia do Urzędu Komunikacji Elektronicznej. Obecnie „na mocy art. 175a ust.1 ustawy z dnia 16 listopada 2012 r. o zmianie ustawy – Prawo telekomunikacyjne (Dz. U. nr 171, poz. 1800, z późn. zm.) przedsiębiorcy telekomunikacyjni obowiązani są niezwłocznie informować prezesa UKE o naruszeniu bezpieczeństwa lub integralności sieci lub usług, które miało istotny wpływ na funkcjonowanie sieci lub usług, o podjętych działaniach zapobiegawczych i środkach naprawczych oraz podjętych działaniach, o których mowa w art. 175 i art. 175c“[1].

Tak jak to już było wspomniane na początku, raportowanie odbywa się do krajowych władz regulujących. W Polsce jest to wzmiankowane UKE. Zgodnie z przyjętym schematem UKE powinno się dzielić tymi danymi z ENISA oraz swoimi odpowiednikami w innych krajach, w sytuacji kiedy naruszenie bezpieczeństwa ma charakter transgraniczny i obowiązkowo raz na rok przekazywać ENISA dane zbiorcze. To co powinno się raportować określane jest jako „incydenty naruszające bezpieczeństwo, które miały znaczący wpływ na ciągłość świadczenia usług teleinformatycznych”.

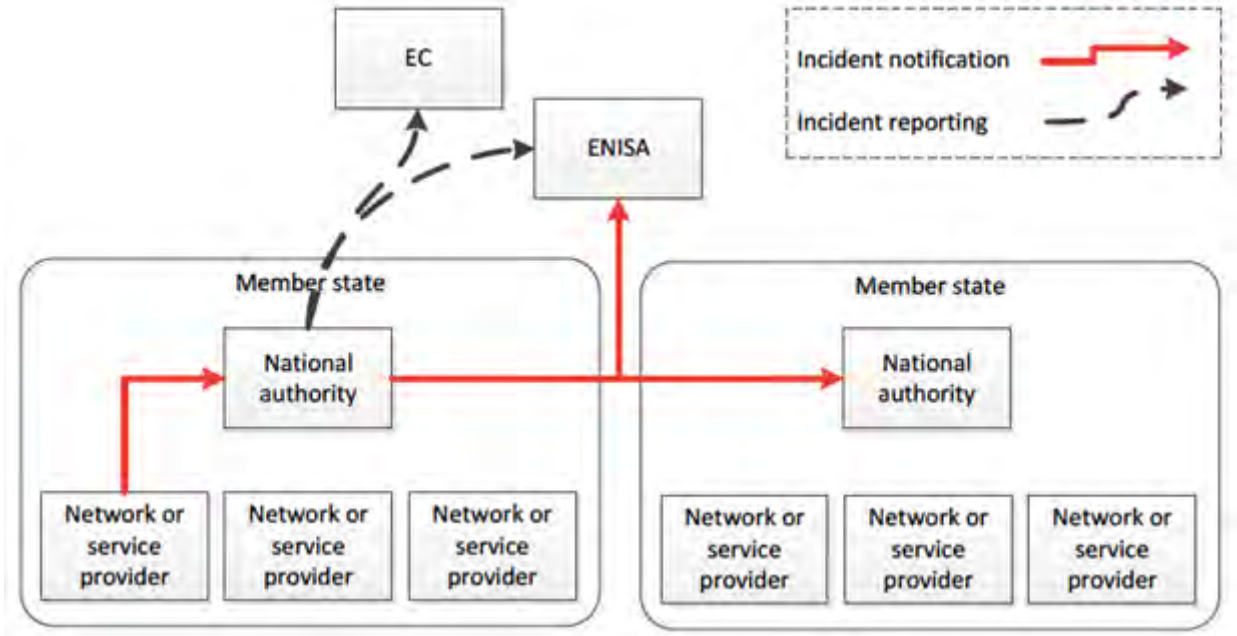
Co w praktyce zawiera raport? Jakie przypadki są zgłaszane? Przyjrzyjmy się kilku zanonimizowanym przypadkom:

- Przy przejściu ze świadczenia usług w oparciu o sieć tymczasową na sieć docelową, usługi głosowe VoIP były niedostępne dla 400 tys. użytkowników;
- Aktualizacja jednego z głównych ruterów była błędna, co spowodowało wyłączenie ruchu IP i w konsekwencji niedostępność wielu serwisów, w tym połączenia alarmowego 112. Incydent doprowadził do awarii trwającej 17 godzin i dotyczył 3 mln użytkowników;
- Sieć światłowodowa została przecięta przy okazji kradzieży kabla. Incydent spowodował niedostępność usług telefonii stacjonarnej przez 10 godzin dla 70 tys. użytkowników i kablowej sieci internet dla 90 tys. użytkowników;
- Seria ataków DDoS (Distributed Denial of Service, skierowana na usługę DNS (Domain Name Service) spowodowała niedostępność sieci Internet przez 1-2 godziny dla 2,5 mln użytkowników;
- Operator telekomunikacyjny zaimplementował aktualizacje systemowe dla HLR (Home Location Register), co spowodowało awarię i w konsekwencji niedostępności mobilnej telefonii i usługi dostępu do sieci Internet. Incydent dotyczył połowy klientów operatora i trwał przez 8 godzin.

Jak widać z powyższych przypadków zgłoszenia w dużej mierze dotyczą problemów wynikających z sytuacji nie wywołanych działaniem intencjonalnym. Nie mniej jednak i takie występują, o czym świadczy przypadek ataków DDoS na system DNS. W raporcie pojawia się 5 głównych przyczyn incydentów: awaria systemu (76%), błąd u dostawcy zewnętrznego (13%), złośliwe działanie (8%), zjawiska naturalne (6%), których swoją drogą usuwanie trwa najdłużej – średnio 36 godzin i błędy ludzkie (6%). Co ciekawe w tej kategorii nastąpiła dość istotna zmiana w stosunku do roku poprzedniego, w którym błędy u dostawców zewnętrznych dotyczyły co trzeciego przypadku (33%). Dla tych, którzy zastanawiają się co się kryje za dość ogólnym pojęciem „awaria systemu” podpowiadam, że autorzy raportu wskazują takie podkategorie jak: awaria sprzętu, „dziury” w oprogramowaniu, awarie ruterów i switchy czy kłopoty lokalnego IXP (Internet eXchange Point).

Przypatrzmy się bliżej temu jakie straty powodują zgłoszone incydenty. 50% z nich doprowadza do zakłócenia działania sieci telefonicznej lub sieci Internet. W tych przypadkach pokaźna jest liczba odbiorców usług, których awaria dotyka. Jest to średnio 1,8 mln użytkowników i jest to znaczący wzrost w stosunku do roku 2011, kiedy ta liczba wynosiła 400 tys. Jak

Schemat raportowania incydentów związanych z art. 13a q.



piszą autorzy – w 37% incydent nie powoduje kłopotów z dostępnością numeru alarmowego 112, choć może istotniejsze jest podkreślenie, że w 63% powoduje. Natomiast warto zwrócić uwagę, że rzadko kiedy awaria dotyczy znaczącej grupy klientów danego operatora. Średnio jest to około 10% tzw. „bazowych użytkowników" i tylko w przypadku mobilnego Internetu, który trudno uznać nadal za usługę krytyczną, jest to 16%.

Biorąc pod uwagę profil naszego biuletynu – nas najbardziej interesują przypadki, które są związane z atakami komputerowymi. Nie jest ich dużo, ale jest czemu się przyjrzeć. W naturalny sposób odnajdujemy je w kategorii działanie złośliwe (dla przypomnienia – to 8% przypadków). Jeśli sięgniemy do statystyk pokazujących szczegółowe przyczyny incydentów to znajdziemy tam informację, że „cyber attacks" były przyczyną 6 incydentów i jest to VI miejsce wśród przyczyn. Warto jednak zwrócić uwagę, że jeżeli rozważania ograniczymy do ataków na sieć Internet to cyberataki są drugą najczęstszą przyczyną incydentów. We wszystkich kategoriach jako przyczyna incydentu zdecydowanie dominuje awaria sprzętu. To zresztą jest chyba najlepszą charakterystyką tego jak cały obowiązek zgłaszania incydentów rozumieją operatorzy. Zdecydowanie koncentrują się oni na awariach sprzętowych i programowych. Intencjonalne działanie nie stanowi dla nich chyba najważniejszej kategorii. To refleksja pojawiająca się przy czytaniu raportu, ale nie tylko. Podobne wnioski wyciągam z rozmów z przedstawicielami ISP, którzy jednoznacznie twierdzą, że przypadki cyberataków, które odnotowują w swojej sieci na swoich ważnych klientów nie rozpoznają jako ich problem. Nie twierdzę, że powinni, ale ciekawe jest to, że w ten sposób w raporcie pomija się całą masę przypadków niedostępności bardzo ważnych usług, takich chociażby jak serwisy e-commerce czy serwisy e-banking. Jeśli odnotowujemy brak dostępności usługi VoIP, to dlaczego pomijane są inne? Wydaje się, że jest to ciekawy temat do dalszej dyskusji.

W swoim raporcie ENISA podaje również kryteria jakie powinny obowiązywać w przypadku zgłaszania incydentów. Dzięki temu operatorzy telekomunikacyjni i narodowi regulatorzy rynku telekomunikacyjnego mają podpowiedź jak rozpatrywać swoje przypadki. Zgodnie ze wskazówkami zgłaszany powinien być każdy z incydentów, który powoduje przerwę w świadczeniu usługi dłuższą niż 8 godzin (nawet jeśli dotyczy

Przyczyny powstawania incydentów naruszających bezpieczeństwo (źródło ENISA Annual Incidents Report 2012)

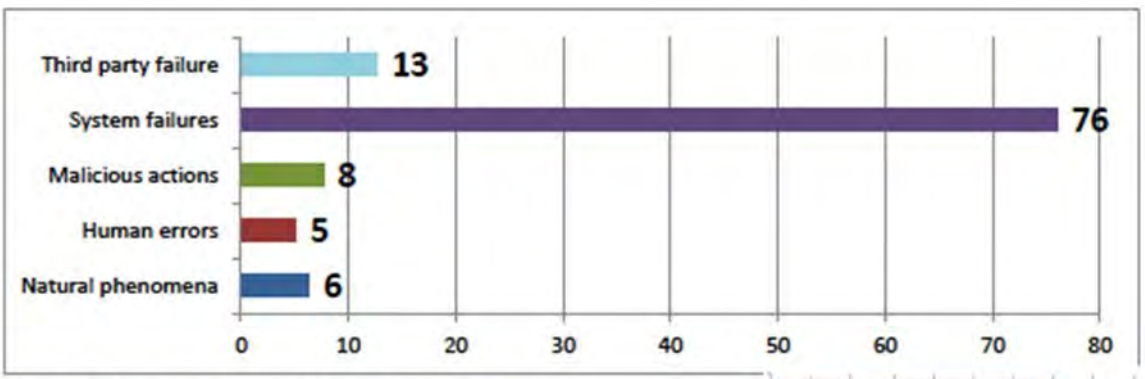
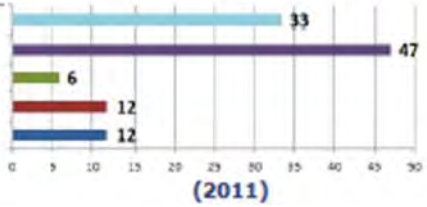
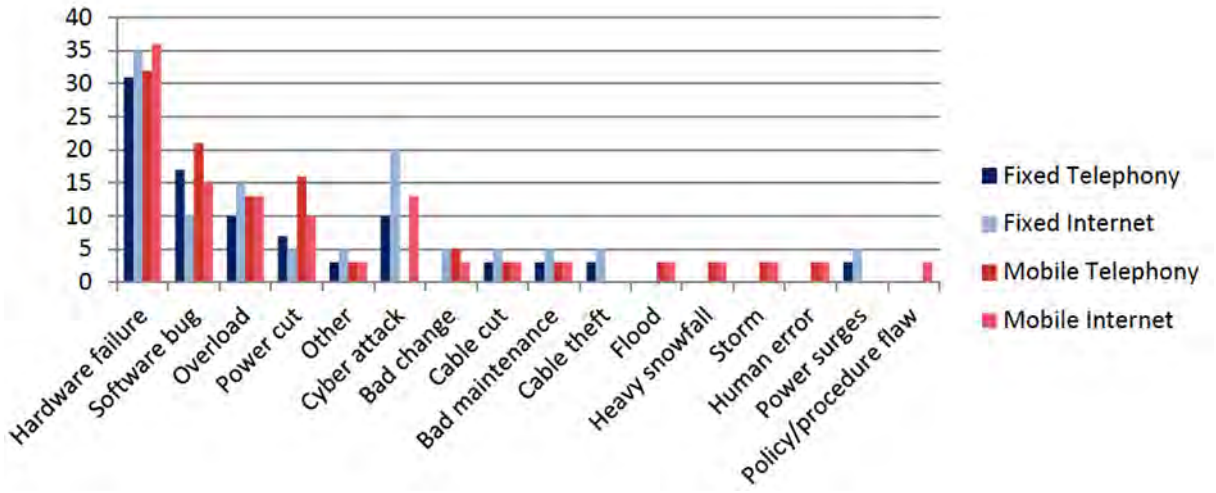


Figure 9 Incidents per root cause category (percentage).





Szczegółowe przyczyny incydentów w odniesieniu do poszczególnych serwisów (źródło ENISA Annual Incidents Report 2012)

tylko 1% użytkowników) lub dotyczy więcej niż 15% użytkowników tego serwisu (nawet jeśli trwa tylko 1 godzinę). To są bazowe kryteria dla tych dwóch cech (czas trwania i zasięg oddziaływania). Występują one również w kombinacji długości trwania awarii i jej zasięgu, a odpowiednią tabelę przedstawiającą te kombinacje można znaleźć w raporcie.

Takie a nie inne kryteria spowodowały, że do ENISA zostało zgłoszonych 79 przypadków. Czy to dużo czy mało? Bardzo trudno odpowiedzieć na to pytanie. Chyba za krótkie są doświadczenia wszystkich „graczy" tej układanki, aby uznać, że raporty z poszczególnych krajów osiągnęły standardowy, docelowy kształt. Część tej dyskusji miała miejsca pod koniec września tego roku w Atenach, w trakcie konferencji jaką zorganizowała ENISA, w trakcie której raport był po raz pierwszy prezentowany (2nd ENISA International Conference on Cyber Crisis Cooperation and Exercises).

Podsumowując raport warto przywołać kilka ważnych kwestii. Incydenty bezpieczeństwa w sieciach operatorów telekomunikacyjnych są nadal postrzegane głównie jako problemy z dostępnością spowodowaną awariami. Zapewne potrzeba jeszcze 2-3 raportów, aby jasno wypracować kryteria i wprowadzić wspólne zrozumienie problematyki wśród państw członkowskich. Ważne jest też aby państwa członkowskie aktywnie uczestniczyły w tej wymianie doświadczeń. No i przede wszystkim warto przypomnieć cel całego przedsięwzięcia. Mimo tego, że w 89% przypadków zgłaszający twierdzili, że ich awarie miały negatywny wpływ na sieci innych, połączonych z nimi operatorów, to wydaje się że podstawowym celem i praktycznym rezultatem będzie wynik pracy analitycznej Agencji. Jak zapewniają autorzy raportu ENISA w tej chwili przygotowuje rekomendacje wynikające ze zgłoszonych przypadków.

fragment dyskusji z serwisu Twitter dotyczące raportu ENISA. Marnix Dekker jest pracownikiem ENISA, jednym z autorów raportu.

BEZPIECZEŃSTWO DANYCH W SIECI INTERNET

Część III - SQL Injection

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

Koniec roku zawsze sprzyja refleksji i podsumowaniu mijającego okresu - niebawem pojawią się różnego rodzaju opracowania analizujące ostatnie dwanaście miesięcy - także w kwestii szeroko rozumianego bezpieczeństwa IT. Przeglądając dane z kilku ostatnich lat można zaobserwować systematyczny wzrost liczby ataków na serwisy internetowe z wykorzystaniem zautomatyzowanych technik, bazujących na dobrze znanych lukach w zabezpieczeniach. Doskonale w ten trend wpisują się ataki typu SQL Injection, które nadal okazują się skuteczne, pomimo szeregu dobrych praktyk i mechanizmów ochrony przed nimi.

Uwaga! Zaprezentowane w tym artykule przykłady zawierają celowe niedociągnięcia, które nie wpływają na ich merytoryczny przekaz, a jedynie mają zapobiegać wykorzystaniu ich wprost przez osoby niedoświadczone.

1. Kilka słów o wstrzykiwaniu

W szerokim rozumieniu zbiór technik code injection (ang. wstrzykiwanie kodu) polega na odpowiednim spreparowaniu danych wejściowych aplikacji w taki sposób, aby możliwe stało się wykonanie nadmiarowych operacji przekazanych wewnątrz tych danych. W tym artykule zostanie szerzej opisana technika, w której do przeprowadzenia ataku wykorzystywane są zapytania języka SQL (Structured Query Languge), stosowanego praktycznie we wszystkich popularnych systemach bazodanowych. Warto wspomnieć, że atak nie jest najczęściej ukierunkowany na samą bazę danych, ale na aplikację, której luki zabezpieczeń pozwalają na przesłanie tych zapytań.

Ataki SQL Injection są, w pewnym stopniu niesłusznie, uważane za mało wyrafinowaną technikę przełamywania zabezpieczeń, głównie ze względu na stosunkowo mały zasób wiedzy jaki jest wymagany do skutecznego wykorzystania podatności. W ciągu ostatnich 10 lat, czyli od początku kariery SQL Injection wielu specjalistów z dziedziny zabezpieczeń miało okazję przekonać się, że mogą one jednak stanowić poważne zagrożenia dla bezpieczeństwa informacji w ich organizacjach.

Głównym celem ataków SQL Injection są formularze na stronach WWW, ale ataki tego typu mogą być wykonywane również poprzez adresy URL oraz pliki cookies. Coraz częściej techniki te są łączone z innymi rodzajami ataków w celu zwiększenia ich skuteczności.

2. Rodzaje ataków

Żadna klasyfikacja nie pozwala na pełne oddanie charakteru danego zjawiska, jednak sensowe wydaje się pogrupowanie ataków SQL Injection wg. kryterium przewidywanego rezultatu, pozostawiając nieco na uboczu techniczne aspekty drogi do jego osiągnięcia. Stosując powyższą metodę możemy wyróżnić ataki ukierunkowane na:

- Uzyskanie dostępu do informacji - to najpopularniejszy i zarazem najprostszy w realizacji rodzaj ataku. Zaliczyć tu należy nie tylko pobranie zawartości tabel, ale również uzyskiwanie struktury danych lub informacji o samej bazie tzw. database fingerprinting. Zwykle bywają one skuteczne ze względu na zbyt szeroki zakres uprawnień użytkownika - nadal funkcjonuje błędne przekonanie, że konta z prawami odczytu nie stanowią poważnego zagrożenia dla bezpieczeństwa aplikacji. Informacje zdobyte w ten sposób, stanowią często podstawę do dalszych ataków.

Przykład 1: UNION SELECT - dodanie dodatkowego członu zapytania zwracającego zawartość chronioną przed użytkownikiem. W tego typu atakach ważna jest zgodność liczby kolumn oraz formatu danych. Tak więc kiepsko zabezpieczona wyszukiwarka produktów może umożliwić zdobycie danych na temat klientów sklepu np.

```
SELECT nazwa, cena, opis FROM produkt WHERE nazwa = $parametr
```

Preparując odpowiednio wartość zmiennej $paramert otrzymujemy zapytanie

```
SELECT nazwa, cena, opis FROM produkty WHERE nazwa = nazwa UNION SELECT login, NULL, haslo FROM uzytkownicy
```

pozwalające nam na pobranie dodatkowych informacji, które nigdy nie powinny zostać ujawnione. W przypadku, gdy hasła nie były odpowiednio zabezpieczone (zainteresowanych tym tematem odsyłam do poprzedniego artykuły tej serii) to przestępca może uzyskać dostęp do kont wszystkich klientów.

Przykład 2: Database fingerprinting z wykorzystaniem sqlli-

ISTOTNE NA ATAKI TYPU SQL INJECTION

Czerwiec 2013: Grupa hackerów RedHack włamała się na rządową turecką stronę ioi.gov.tr. Twierdzili oni, że byli w stanie skasować rachunki obywateli.

Styczeń 2013: Po wykryciu luki pozwalającej na przeprowadzenie SQL Injection w popularnym frameworku Ruby on Rails duński rząd zdecydował się na zamknięcie zintegrowanego systemu uwierzytelniania DigiD, pozbawiając obywateli dostępu do wielu usług e-Gov.

Lipiec 2012: Włamanie do serwisu Yahoo. Udostępnione zostały loginy i niezabezpieczone hasła 450 000 użytkowników usługi Yahoo Voices. Wykorzystano technikę typu "UNION SELECT".

Czerwiec 2012: Wyciek danych z jednego z największych serwisów społecznościowych LinkedIn. Skuteczny atak SQL Injection przyczynił się do ujawnienia danych 6,5 miliona użytkowników.

SQL INJECTION A POLSKIE PRAWO

Szerokim echem odbił się w mediach branżowych wyrok Sądu Rejonowego w Głogowie z dnia 11 sierpnia 2008 r. dotyczący przełamywania zabezpieczeń przy użyciu SQL Injection. Wykorzystana została tam przytoczona w tym artykule technika ominięcia uwierzytelniania za pomocą wprowadzenia ciągu znaków "OR 1 = 1" . Sprawa zyskała rozgłos przede wszystkim ze względu na wyrok uniewinniający. Decyzja sądu spowodowała pojawienie się wielu wątpliwości dotyczących prawnej ochrony podmiotów przed atakami typu SQL Injection. Wyrok ten nadal żyje w świadomości wielu osób, jednak od tamtej pory kodeks karny został zmieniony m. in. w związku z dostosowywaniem polskiego prawa do Konwencji Rady Europy o Cyberprzestępczości i obecnie dokonywanie tego typu nieautoryzowanych testów penetracyjnych nie jest dozwolone.

te_version() - przedstawione powyżej zapytanie możemy równie dobrze wykorzystać w celu zdobycia informacji o wersji bazy danych w celu późniejszego wykorzystania znanych exploitów.

```
SELECT nazwa, cena, opis FROM produkty WHERE nazwa =
nazwa UNION SELECT NULL, NULL, sqllite_version()
```

• Ominięcie uwierzytelniania - wykorzystywane jest wszędzie tam gdzie uzyskanie dostępu do aplikacji wymaga potwierdzenia tożsamości np. za pomocą loginu i hasła.

Przykład 3: OR 1 = 1 - popularna technika pozwalająca na zmianę warunków logicznych zapytania, tak aby zracało ono zawszę wartość PRAWDA.

```
SELECT count(*) FROM uzytkownik WHERE login = $login
AND haslo = $haslo
```

Znów dokonując odpowiedniej modyfikacji wartości parametrów wprowadzanych przez użytkownika za pomocą formularza możemy otrzymać zapytanie dające nam dostęp do chronionej treści.

```
SELECT count(*) FROM uzytkownik WHERE login = 'admin'
AND haslo = 'cokolwiek' OR 1 = 1
```

Zapytanie takie pomimo, że nie zostanie spełniony założony przez autora programu warunek pozwoli atakującemu uzyskać dostęp do aplikacji.

• Zmiana integralności danych - czyli najprościej mówiąc dokonywanie nieautoryzowanej zmiany lub usunięcie informacji. Technika skuteczna może być wszędzie tam gdzie użytkownik posiada wysoki poziom uprawnień do całej bazy np. wszelkiego typu popularne systemu CMS.

Przykład 4: Taxonomy Timer - atak na system Drupal - wykryta kilka lat temu luka pozwalała na wykonanie dowolnego kodu SQL przekazywanego do systemu za pomocą adresu URL. Treść zapytania:

```
SELECT * FROM $taxonomy_timer_defaults WHERE ttid =
$arg3
```

Wywołanie odpowiednio spreparowanego adresu URL powodowało wykonanie zapytania, które pozwalało np. usunąć tabelę z naszej bazy:

```
http://www.example.com/admin/taxonomy_timer/delete/1;
DROP TABLE tabela;
```

```
SELECT * FROM taxonomy_timer_defaults WHERE ttid = 1;
DROP TABLE tabela;
```

• Odmowę dostępu do usługi - w systemach posiadających skuteczne mechanizmy ochrony serwera WWW przed atakiem DoS (Denial of Service) alternatywą może okazać się zaatakowanie bazy danych, tak aby to jej przeciążenie spowodowało niedostępność usługi. W tym celu wstrzykuje się kod SQL powodujący wykonywanie skomplikowanych obliczeń matematycznych lub zapytania blokujące dostęp rekordów na czas ich wykonania.

• Zdalne wykonanie poleceń - niektóre silniki bazodanowe mają funkcje pozwalające na wywoływanie operacji w systemie operacyjnym lub systemie plików. Przykładem może być tutaj xp_cmdshell z Microsoft SQL Servera. Nieprawidłowa konfiguracja tego elementu może stworzyć zagrożenie nie tylko dla bazy danych, ale również dla całego systemu.

3. Walcz z niechlujstwem!

Ze smutkiem muszę stwierdzić, że większość udanych ataków SQL Injection, które miałem okazję przeanalizować, nie zakończyłaby się sukcesem, gdyby nie zaniedbania twórców serwisów internetowych na różnych etapach ich budowy. Jak wspomniałem we wstępie tego artykułu od kilku lat istnieją skuteczne mechanizmy zabezpieczania aplikacji przed tego typu atakami. Podsumowując ten artykuł chciałbym wspomnieć o kilku podstawowych aspektach, które powinny zostać uwzględnione przy tworzeniu serwisów internetowych.

A. Odseparuj dane publiczne od chronionych

B. Dbaj o zasadę minimalnych uprawnień

C. Pamiętaj o aktualizacjach

C. Nigdy nie ufaj danym wprowadzanym przez użytkowników

D. Sprawdź poprawność wprowadzonych informacji przed wysłaniem zapytania do bazy

E. Dokonaj sanityzacji - oczyszczenia danych wejściowych z potencjalnie niebezpiecznych zapisów

F. Buduj bezpieczne zapytania bazodanowe z wykorzystaniem aktualnych zaleceń

Fotoradar SQL Injection :-)

źródło: http://i.imgur.com/RmfbEsZ.jpg