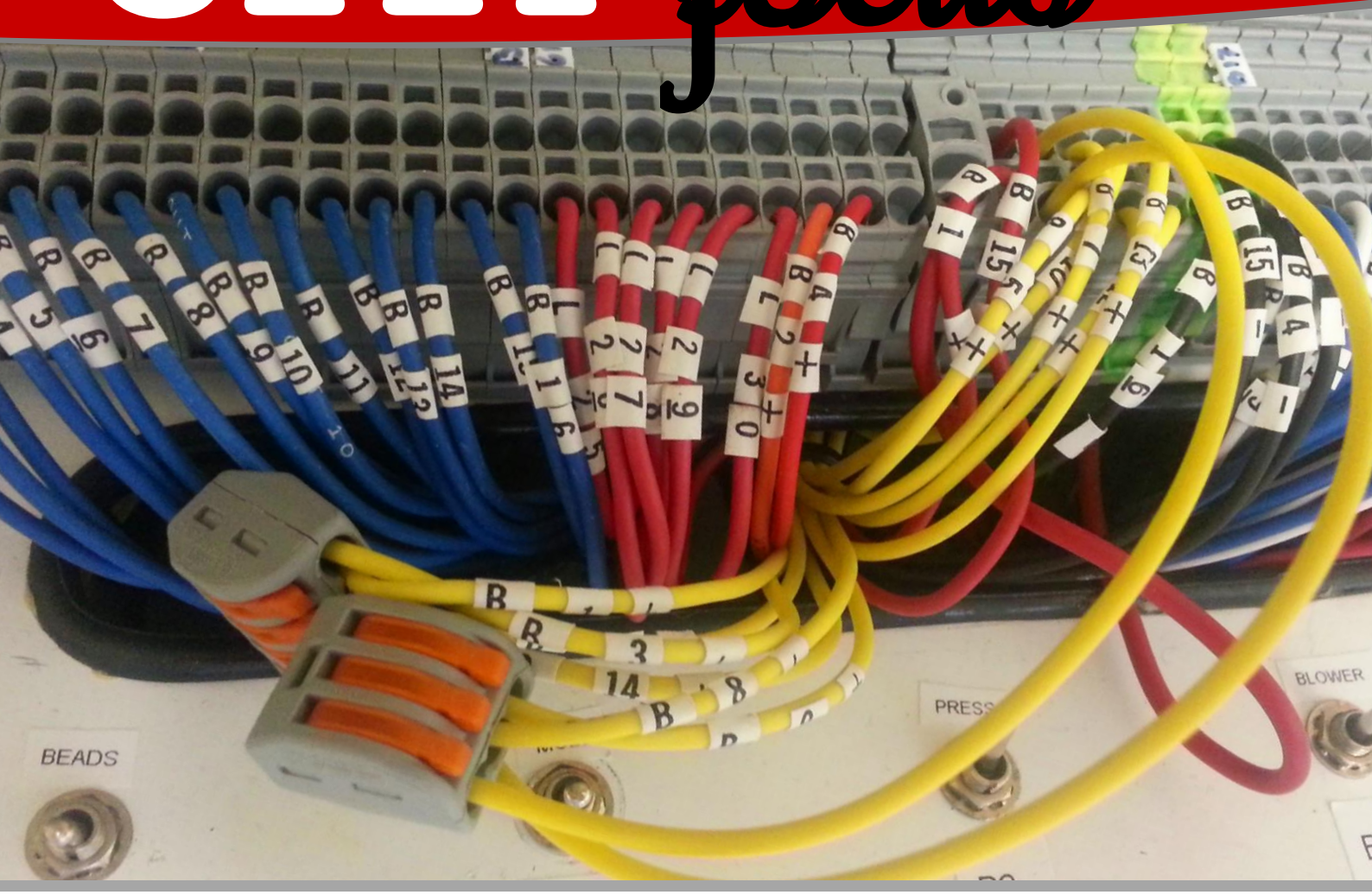
Nr 5 – lipiec 2013

CIP focus

RCB
Rządowe Centrum Bezpieczeństwa



W NUMERZE:

Drodzy Czytelnicy,

Drodzy Czytelnicy!

Po raz kolejny mamy przyjemność zaprosić Państwa do lektury biuletynu CIIP focus. Wierzymy, że wśród Was są już stali czytelnicy, którzy z przyjemnością sięgają po publikowane w nim artykuły. Czego możecie oczekiwać tym razem?

Zaczynamy od małej monografii Gaussa. Wirus Gauss nie jest czymś nowym, ale ze względu na to jaką rolę odegrał jakiś czas temu, warto do niego powrócić. Jako złośliwy kod związany bardzo silnie z tematyką „state sponsored attacks", z pewnością budzi zainteresowanie wielu specjalistów. Warto przeczytać o najważniejszych „dokonaniach" Gaussa. W skomasowanej formie przedstawia je w swoim artykule Mirosław Maj z FBC. Swoją drogą ciekawe, kto powinien zajmować się takimi atakami. Czy specjalny CERT dedykowany dla ochrony TIK? Ten interesujący temat, ten sam autor podejmuje w artykule o CERT-ach dla infrastruktury krytycznej.

Artur Barankiewicz z Orange Polska opisuje natomiast historię i najważniejsze zagadnienia związane z atakami DDoS. Wielu polskich administratorów niestety przeszło w tym roku przyśpieszony kurs dotyczący tych ataków. Jest okazja, aby wiedzę sobie usystematyzować.

Trzeci artykuł, na który szczególnie chcielibyśmy zwrócić uwagę, to artykuł Krzysztofa Silickiego – polskiego przedstawiciela w Radzie Zarządzającej ENISA. ENISA od dłuższego czasu konsekwentnie i wartościowo wzbogaca literaturę dotyczącą ochrony infrastruktury krytycznej. Krzyszto Silicki dokonał przeglądu tych materiałów. Oprócz tych ściśle związanych z ochroną TIK, przywołał kilka pozycji odnoszących się do zasad budowy współpracy publiczno-prywatnej, czy dobrych praktyk związanych z wymianą informacji. To doskonała lektura dla nas wszystkich, gdyż wiele jest jeszcze do zrobienia w Polsce w tej dziedzinie. A jak pokazał autor – „dobre praktyki" są. Nic tylko czytać i stosować.

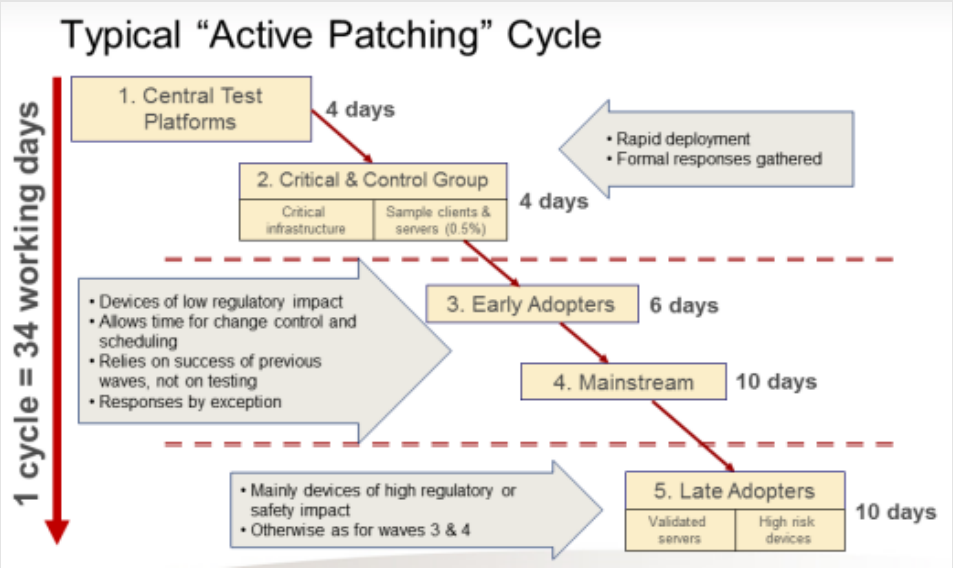
Elementarza bezpieczeństwa nigdy za wiele, dlatego Emil Wróbel z RCB wziął na warsztat hasła. Przypomina o ich krytycznym znaczeniu i zasadach bezpiecznego stosowania. Wydaje się, że to temat przewałkowany, ale proszę zrobić prosty, uczciwy test korzystając z "hasłowego BHP". Wynik może nie być bardzo optymistyczny, dlatego mimo wszystko namawiamy do lektury.

Oprócz wspomnianych artykułów znajdziecie Państwo jak zwykle ciekawe newsy dotyczące TIK. W biuletynie jest też relacja z konferencji światowych CERT-ów, w trakcie której przeprowadziliśmy krótki, ale mamy nadzieję, że ciekawy, wywiad z Damirem Rajnovicem.

Życząc przyjemnej lektury jak zwykle zachęcamy do kontaktu z redakcją. Państwa opinie i sugestie dotyczące przyszłych numerów CIIP focus będą dla nas bardzo cenne!

Redakcja CIIP focus

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



Astra-Zeneca Illustration from "SCADA and ICS Patching: On the Horns of a Dilemma" presentation. Source: Joakim Moby, Astra-Zeneca, ISA Expo 2006

NEWS

Stacje ładowania samochodów elektrycznych można zhackować

W dziesięciominutowej prezentacji lider izraelskiego oddziału Projektu OWASP wyjaśnia, czym w praktyce są stacje ładowania samochodów elektrycznych i dlaczego narażone one są na ataki komputerowe.

Więcej: http://youtu.be/d484G5MghM4

Analiza ataków na systemy SCADA

Taki tytuł nosi raport opublikowany przez Trend Micro Inc. To kompletny raport, w którym autorzy prezentują podstawy konieczne do zrozumienia tematu określonego w tytule. Można w nim znaleźć informacje o metodach wykorzystywania systemów ICS/SCADA, dlaczego te systemy narażone są na zagrożenia, w jakiej działają architekturze etc. Badacze TM zbudowali i uruchomili honeypot, aby dokładnie rozpoznać źródła ataków na systemy SCADA. Systemy te, będąc pułapką na atakujących, w ciągu 28 dni zebrały informacje o 39 atakach z 14 krajów. W ten sposób powstało zestawienie, w którym czołowe miejsca jako kraje atakujące zajęły Chiny i USA. Na mapie źródeł zagrożeń znajduje się też Polska. Raport kończy się zestawem rekomendacji.

Więcej: http://bit.ly/ZUjqGU

Łatanie dziur w systemach SCADA

Łatanie dziur (ang. patching) w systemach automatyki przemysłowej to jedno z największych wyzwań. Zmiana oprogramowania ze względów bezpieczeństwa staje dość często w szranki z koniecznością utrzymania stabilności działania systemu. Tym trudnym problemem zajmuje się w swoim artykule Eric Byres. Prezentuje w nim między innymi rekomendacje EEI (Edison Electric Institute) z tego zakresu oraz bardzo praktyczny schemat (po lewej) implementacji zmian w systemie, który został opracowany przez firmę Astra-Zeneca.

Więcej: http://bit.ly/182rIPT

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

G A U S S

kolejny przedstawiciel bliskowschodniej cyber-inwazji

Mirosław Maj
Fundacja Bezpieczna Cyberprzestrzeń

Kiedy inżynierowie firmy Kaspersky Lab, w trakcie badań wykonywanych na zlecenie ITU (International Telecommunication Unit) po raz pierwszy zaczęli analizować złośliwy kod, który sami później nazwali wirusem Gauss, nie przykuł on ich szczególnej uwagi. Wydawało się, że wirus był już znany, a jego „szczepionka" zaimplementowana w wielu programach antywirusowych. Dopiero po pewnym czasie wykryli oni, że kod zawiera trochę więcej niż powszechnie się wydawało. Dzięki temu odkryli nowe, niezwykle interesujące moduły. Wirus Gauss dołączył do tria Stuxnet, Flame i Duqu, tworząc wraz z nimi kwartet, który na początku bieżącej dekady dokonał skutecznej inwazji na cyber-ziemie Bliskiego Wschodu.

Lagrange ponownie przegrywa z Gaussem

Kurt Godel, Johann Carl Friedrich Gauss i Joseph-Louis Lagrange to trzej matematycy, którzy „umieszczeni" zostali w kodzie wirusa. Ich nazwiskami nazwane zostały niektóre z modułów wirusa. Badacze uznali, że najważniejszy z tych modułów to moduł Gauss, bo on właśnie odpowiadał za funkcje wskazane jako najważniejsze dla działania wirusa. Chodzi o funkcje szpiegowskie, związane z kradzieżą danych. Lagrange po raz drugi przegrał rywalizację z Gaussem. Pierwszy raz, kiedy jego prace nad Zasadniczym Twierdzeniem Algebry poszły w zapomnienie, a pierwszeństwo matematycznego dowodu związanego z tym twierdzeniem przypadło właśnie Gaussowi. Nowy złośliwy kod ostatecznie nazwano Gaussem, a Kaspersky Lab nadał mu swoją oficjalną nazwę – Trojan.Win32.Gauss.

Kolejne dzieło „nieznanych sprawców"

„Godel", „Lagrange" i „Gauss" to jednak tylko wirtualni wykonawcy przestępczego działania. Twórcy wirusa pozostają nieznani, podobnie zresztą jak twórcy pozostałych przedstawicieli „bliskowschodniego" kwartetu. Można stwierdzić z dużym prawdopodobieństwem, że są to ci sami twórcy, albo jako to niektórzy określają – pochodzą z tej samej „stajni". Liczba podobieństw pomiędzy poszczególnymi kodami jest wystarczająco duża, aby postawić taką tezę. Stuxnet i Duqu posiadają tę samą platformę Tilded. Podobnie jak Flame i Gauss posiadają platformę nazwaną na bazie tego pierwszego – Flame. Moduł infekcji USB ze Stuxneta został wykorzystany w Flame i Gauss. Takich podobieństw jest znacznie więcej. Dostatecznie dużo, aby uznać je za nieprzypadkowe. Ciekawe też są operacyjne koincydencje, np.: Gauss rozpoczął swoją aktywną penetrację komputerów najprawdopodobniej we wrześniu 2011 roku, czyli dokładnie w czasie, kiedy badacze z węgierskiego CrySys Lab wykryli Duqu. Wiele faktów świadczy o tym, że twórcy wspomnianych wirusów bardzo uważnie śledzą postępy prac związanych z ich wykrywaniem i reagują, a to nowymi wersjami broni ze swojego arsenału, a to „samozagładą" części tego arsenału. Sam wirus został stworzony najprawdopodobniej chwilę wcześniej, około połowy 2011 roku. Wykryto go mniej więcej rok później - w czerwcu 2012 roku. Wtedy też nastąpiły pierwsze, głębsze analizy. Wykrycie nastąpiło w czasie wspomnianych już prac w ramach projektu ITU. Projekt dotyczył analizy Flame'a. Właśnie z Flame'em Gauss ma najwięcej wspólnego. Tak jak już to było wspomniane – przede wszystkim obydwa wirusy bazują na tej samej platformie. Obydwa wirusy mają też podobne fragmenty kodu i podobne mechanizmy komunikacji z serwerami nadzorującymi. Chociaż Gauss jest mniej zaawansowanym i skomplikowanym kodem. Nie zmienia to faktu, że niektóre jego elementy nadal pozostają nieznane. Przede wszystkim związane z metodami infekcji.

NEWS

ICS-CERT Monitor

Publikacja amerykańskiego ICS-CERT zawiera informacje o zagrożeniach związanych z systemami automatyki przemysłowej. W publikacji można między innymi przeczytać o systematycznych atakach na jedną z amerykańskich stacji kompresji gazu. W raporcie znajdują się również informacje o incydentach jakie trafiły do ICS-CERT w pierwszym półroczu 2013 r. (w tym szczegółowe statystyki o źródłach zgłoszeń). „Monitor" zawiera także wiele informacji o charakterze edukacyjnym oraz dokładne zestawienie alertów i porad publikowanych przez ICS-CERT.

Więcej: http://1.usa.gov/18m1M4v

OWASP SCADA Security Project

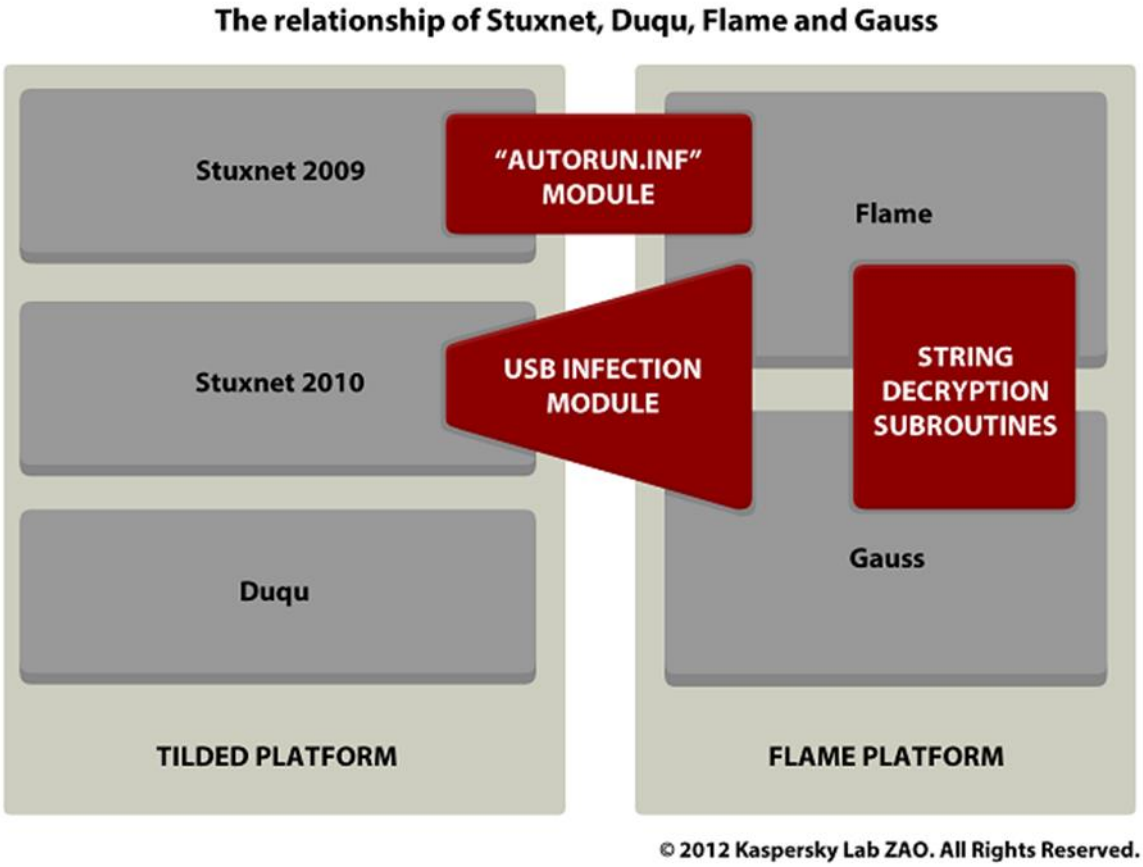
OWASP (Open Web Application Security Project) to projekt, którego głównym celem jest praca nad poprawą oprogramowania z punktu widzenia jego bezpieczeństwa. W szczególności w kontekście web-aplikacji. W projekcie OWASP SCADA Security, chodzi o uwzględnienie aspektu bezpieczeństwa web-aplikacji w całościowym bezpieczeństwie systemów automatyki przemysłowej. Autorzy projektu stawiają sobie za cel zebranie informacji na temat wszystkich potencjalnych metod poprawy bezpieczeństwa systemów ICS (Industrial Control System) i stworzenie rekomendacji z tego zakresu. Warto obserwować postępy w realizacji projektu.

Więcej: http://bit.ly/155Vy3p

Systemy SCADA pilnują bezpieczeństwa swojego otoczenia

Naukowcy z North Carolina State University opracowali algorytm wykrywania i izolowania urządzeń, które stanowią zagrożenie dla swoich „sąsiadów". Algorytm ten polega na stałej obserwacji sieciowych sąsiadów i wykrywaniu ich niebezpiecznego zachowania, a w konsekwencji izolowaniu ich od reszty komponentów sieci, aby wyeliminować migrację zagrożenia na inne obiekty. System nie jest sterowany centralnie, a za wykrycie i podjęcie reakcji odpowiadają poszczególne urządzenia w sieci, które „opiekują" się swoimi „sąsiadami".

Więcej: http://bit.ly/12yf9by



Rysunek – Podobieństwa w budowie wirusów Stuxnet, Duqu, Flame i Gauss

Command & Control w drogerii w Pradze i hotelu w Oslo

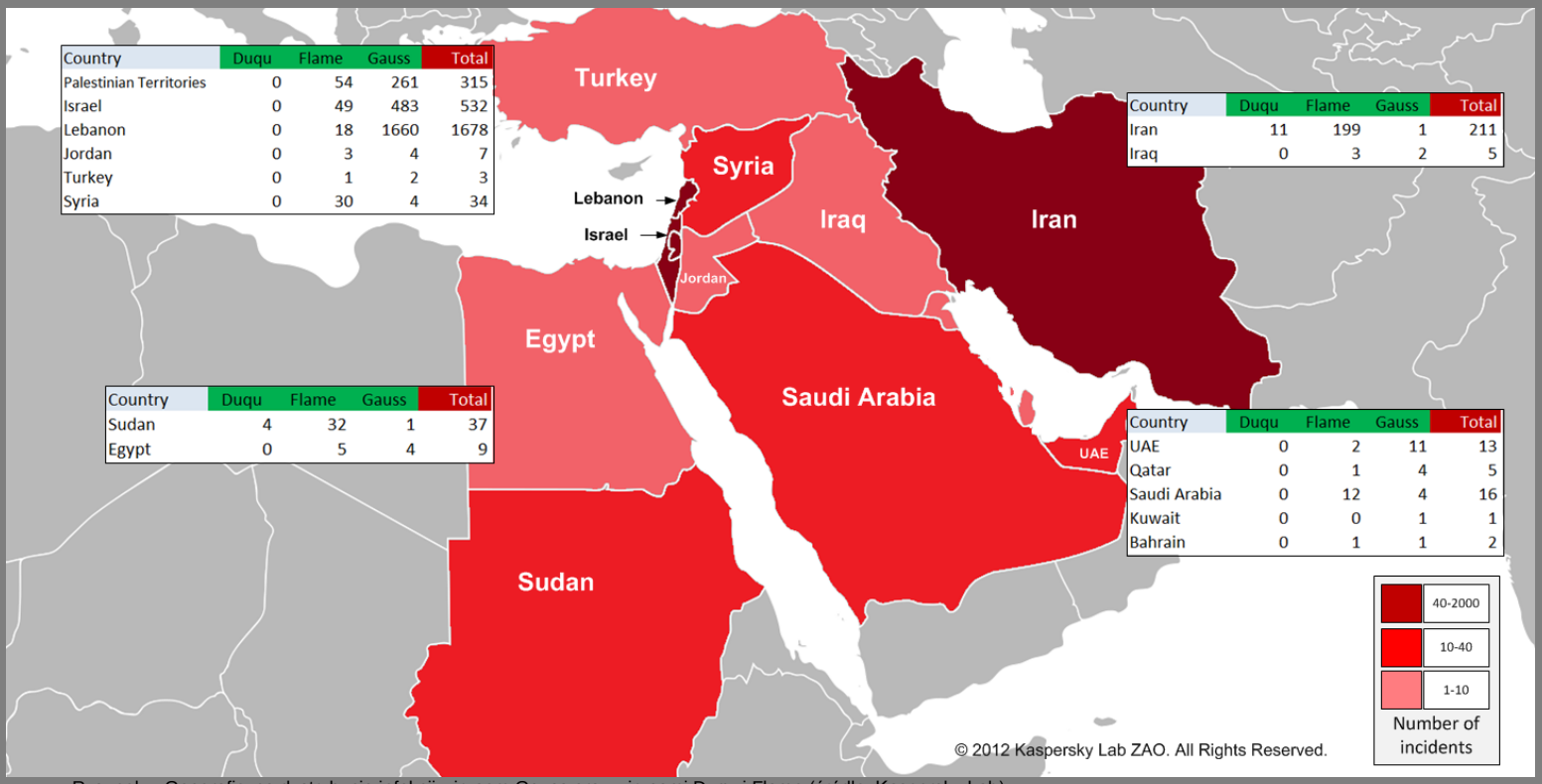
Miesiąc po wykryciu i pierwszych analizach Gaussa przestały działać serwery pełniące funkcję command&control (C2). Zainfekowane komputery przeszły w stan uśpienia i oczekiwania na możliwość ponownego połączenia z serwerami zarządzającymi. Z tymi serwerami też jest zresztą związana ciekawa historia. Do ich obsługi zarejestrowano 6 domen. Swoją drogą zdecydowanie mniej niż dla Flame'a, którego obsługiwało około 100 domen. Rejestratorami okazali się: niewielki hotel w Oslo przy Prinsensgate i drogeria w Pradze na ulicy Antala Staska. To rzecz jasna sfałszowane dane, które nadają się jedynie do „turystyki informatycznej" odwiedzając stolice Norwegii i Czech.

Libańskie banki celem ataku

Prawdziwy jest natomiast obszar działania Gaussa, który czyni go wyjątkowym w odniesieniu do Stuxneta, Duqu i Flame'a. Tu pierwsze miejsce na liście zajmuje Liban, gdzie nastąpiło blisko 2/3 wszystkich infekcji. Prawie 20% z nich miało miejsce na terytorium Izraela i około 10% w Palestynie. Pozostałe kraje to pojedyncze przypadki, w większości kraje bliskowschodnie, ale także USA i Niemcy. Nie do końca wiadomo ile było wszystkich infekcji. Kaspersky Lab. Badający wirusa odnotował ich około 2,5 tysiąca. Są to jednak dane pochodzące tylko i wyłącznie z systemu monitoringu firmy Kaspersky. Badacze przypuszczają, że wszystkich infekcji było najprawdopodobniej kilkadziesiąt tysięcy. Stawia to Gaussa na drugiej pozycji co do liczby infekcji, w rywalizacji z przywoływanymi tu wielokrotnie pozostałymi wirusami.

Co właściwie robił i jak działał Gauss?

Wirus Gauss to kod napisany w języku C++. Z punktu widzenia taksonomii złośliwego oprogramowania, specjaliści najbardziej skłonni są uznać go za tzw. konia trojańskiego. W praktyce należałoby jednak podkreślić, że najważniejsze funkcje wirusa to funkcje szpiegujące. Gauss koncentrował się w swoim działaniu na przechwytywaniu danych i rzecz jasna odsyłaniu ich do „zainteresowanych". W ten sposób wykradał trzy rodzaje danych: dane związane z przeglądarką internetową, ustawienia konfiguracyjne i to, co najczęściej się podkreśla wspominając tego wirusa – dane autoryzacyjne do libańskich banków. W pierwszej kategorii pozyskiwane były takie dane jak hasła do przeglądarek, historia przeglądarek, ciasteczka (ang. cookies), zaszyte hasła. W kontekście pozyskiwania informacji o konfiguracji systemowej, głównie chodziło o informacje o sterownikach i strukturze folderów. Co ciekawe, twórcy sami popełnili błąd (a może zrobili to intencjonalnie, w sytuacji kiedy nie ma to większej wartości rozpoznawczej) i zdradzili miejsce składowania kodu wirusa na swoim komputerze, pozostawiając w kodzie odwołania do folderów systemowych takich jak d:\projects\gauss, d:\projects\gauss_for_macis_2 oraz c:\documentsandsettings\flamer\desktop\gauss_white_1. Zresztą ten ostatni katalog z nazwą „white", interpretuje się jako odwołanie do Libanu, gdyż nazwa tego państwa ma swoje źródło w semickim słowie oznaczającym właśnie „biały". Natomiast jeśli chodzi o ataki bankowe, to przedmiotem zainteresowania było sześć libańskich banków: Bank of Beirut, Byblos Bank, Credit Libanais, BLOM Bank, Banque Libano-Française oraz Fransabank. Nie wiadomo na ile udana była ta część przedsięwzięcia. Libańscy klienci e-bankowości to nie duża grupa, a dodatkowo przedstawiciele wspomnianych banków właściwie jednym chórem odpowiadają, że w ich przypadku do niczego złego nie doszło. Gauss posiadał też ciekawą funkcję przechowywania skradzionych informacji w ukrytym pliku na nośnikach USB, właśnie poprzez możliwość infekcji styku USB. Ta słabość opisana jest w ramach słabości



Rysunek – Geograficzna dystrybucja infekcji wirusem Gauss oraz wirusami Duqu i Flame (źródło: Kaspersky Lab)

CVE-2010-2568 (http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2568) i badaczom znana była już dzięki analizie Flame'a.

Jak już wspomniano, Gauss jest klasycznym przykładem wirusa kontrolowanego przez serwer command&control (C2). Do tej kontroli wykorzystano tylko 6 domen i kilku serwerów. Ciekawa jest tu funkcjonalność load-balancingu dla serwerów przechwytujących dane. Zakładając duży wolumen skutecznie prowadzonej akcji szpiegującej i przesyłanie danych do tylko kilku serwerów, taki balans ruchu być może był nawet koniecznością, a z pewnością jest dobrą optymalizacją zarządzania tym ruchem.
Właściwie jedynym poważnym, nierozpoznanym obszarem funkcjonowania wirusa, pozostaje sposób w jaki dochodziło do infekcji Gaussem. W kodzie nie wykryto funkcji samopropagacji wirusa. Niewykluczone, że badacze mieli do czynienia ze słabością typu „zero-day" i stąd to niepowodzenie.
Na koniec opisu funkcji wirusa warto wspomnieć o dość dziwnej funkcji jaką jest instalacja czcionki Pallida Narrow. Absolutnie brak pomysłów na interpretację celu, jakim kierowali się twórcy wirusa decydując się na tę funkcję. W praktyce wyszło na to, że jej przydatność sprowadziła się do tego, że Kaspersky Lab i CrySys Lab utworzyły proste serwisy sprawdzające istnienie tej czcionki na komputerze i wskazujące w ten sposób na możliwość infekcji Gaussem (https://www.securelist.com/en/blog/724/Online_Detection_of_Gauss, http://gauss.crysys.hu/).

Kto jest autorem?

Powszechnie uznaje się, że Gauss to, podobnie jak Stuxnet, Duqu i Flame, wirus określany jako „state sponsored", czyli, że w jego przygotowanie zaangażowane były służby niektórych państw. Najbardziej podejrzani to duet Stany Zjednoczone – Izrael. Powiązania technologiczne z innymi wirusami „state sponsored" wskazują na taką możliwość. Z drugiej strony pojawienie się takiej funkcji jak moduł odpowiadający za atak na klientów kilku banków, jest zupełnie niespójny z celami ataków sponsorowanych przez państwo. Trudno sobie wyobrazić takie potrzeby rządów, w Waszyngtonie i Tel Awiwie, jak kradzież pieniędzy z kont bankowych. Dlatego niektórzy komentatorzy wskazują na możliwość innego źródła tego ataku. Na przykład Stephen Bryen z portalu technologysecurity.wordpress.com spekuluje, czy Gauss nie jest dziełem autorów rosyjskich. Wątek ataku bankowego oraz zaangażowanie w analizę firmy Kaspersky Lab, przez niektórych postrzeganą jako mającą bardzo dobre relacje z administracją na Kremlu, traktuje jako argumentyprzemawiające za taką teorią. Wydaje się to trochę naciąganą interpretacją, niemniej jednak tak długo jak nie pojawią się fakty przybliżające nas do prawdy w tej sprawie, nie należy wykluczać żadnych możliwości.

Źródła:
1.Gauss: Nation-state cyber-surveillance meets banking Trojan - http://www.securelist.com/en/blog?weblogid=208193767
2. Who is behind the gauss virus? - http://technologysecurity.wordpress.com/2012/08/13/who-is-behind-the-gauss-virus/
3. Gauss: Abnormal Distribution - http://www.securelist.com/en/analysis/204792238/

ATAKI DDoS

Artur Barankiewicz

kierownik Wydziału Analiz i Strategii Bezpieczeństwo Systemów Teleinformatycznych Infrastruktura IT i Bezpieczeństwo Teleinformatyczne *Orange Polska*

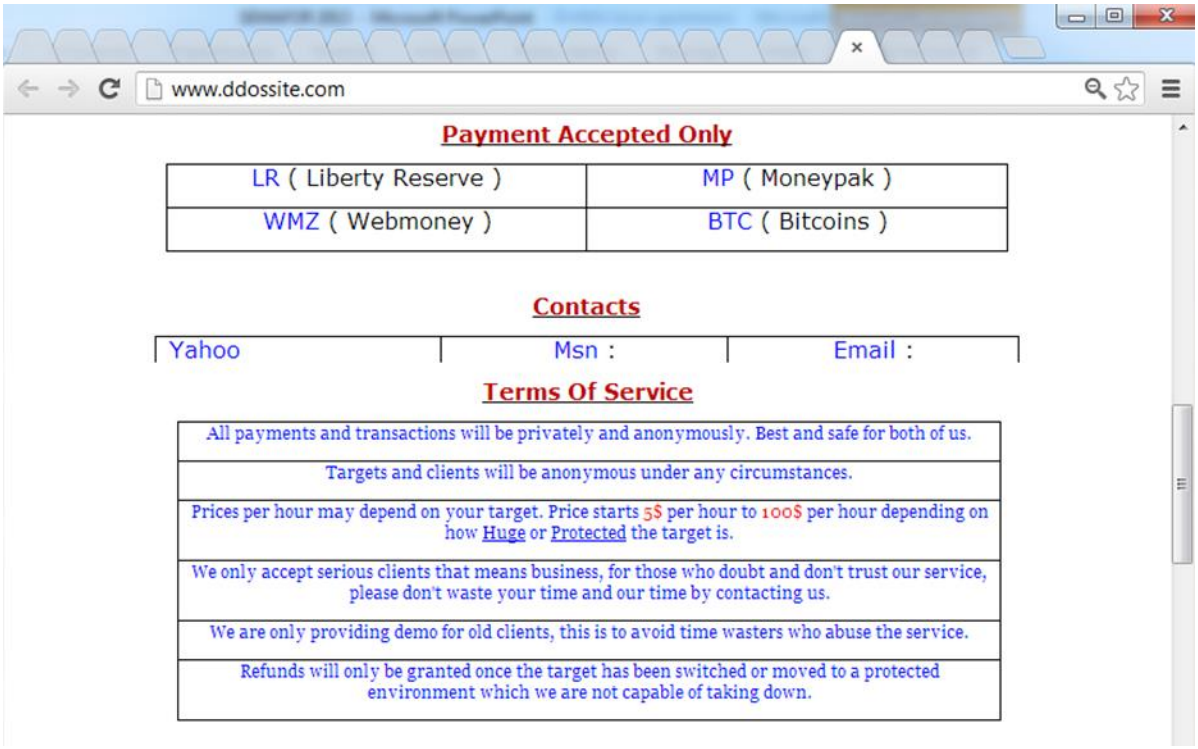
Zaczęło się od osiemnastolatka

Jest rok 1999, USA. Pewnego dnia „pada" popularny wśród użytkowników IRC serwer na Uniwersytecie Minnesoty, ale to dopiero początek. Kilka miesięcy później, w lutym 2000, użytkownicy, wcale przecież nieraczkującego, Internetu przez kilka godzin mają problemy ze skorzystaniem z zasobów Yahoo, eBay, CNN, Amazonu, czy ZDNetu. Awaria prądu? Atak terrorystyczny? Nie – to tylko znudzony piętnastolatek o pseudonimie MafiaBoy, który chciał zyskać „szacun na dzielni", wyszukał w sieci podatne komputery, przejął nad nimi kontrolę i zaatakował...

Statystycznemu internaucie ataki teleinformatyczne zazwyczaj kojarzą się z hackerem, niczym z hollywoodzkich filmów, który w brudnym, przypominającym norę mieszkaniu, obłożony pudełkami z pizzą sprzed miesiąca, stuka w klawiaturę niczym zawodowa maszynistka. No, może jeszcze – na fali ostatnich medialnych doniesień – z wyspecjalizowanymi jednostkami w strukturach armii pewnych (niekoniecznie azjatyckich) krajów. Od 2000 roku, gdy miały miejsce wspomniane na wstępie ataki.

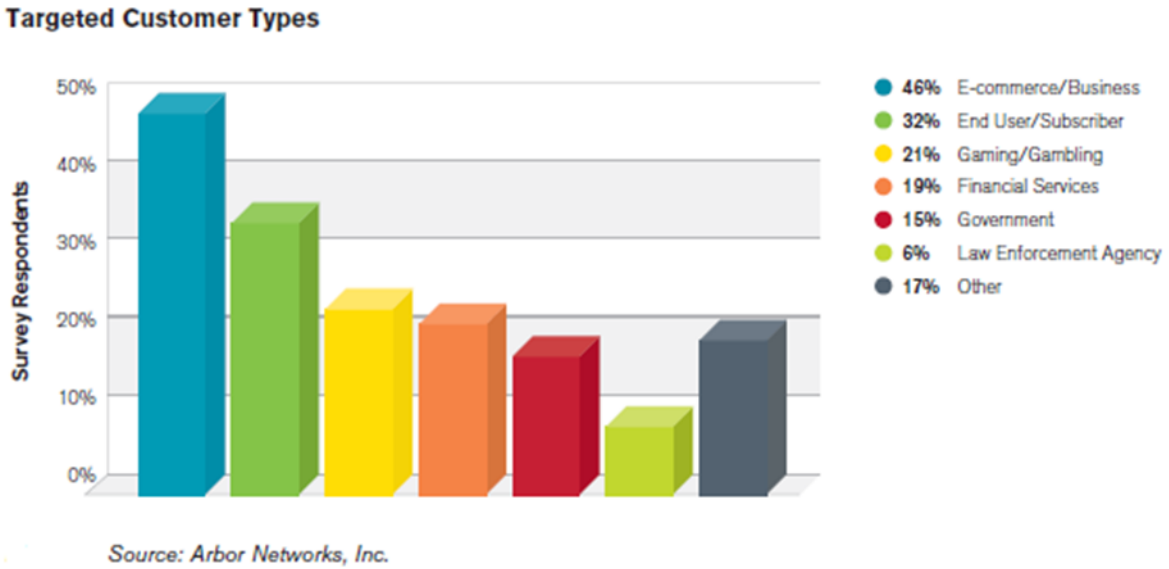
Rozproszona Odmowa Dostępu (Distributed Denial of Service, DDoS) urosła do miana najpopularniejszego cyberprzestępczego narzędzia. O co w tym wszystkim w ogóle chodzi?

W skrócie, DDoS polega na wysłaniu do zaatakowanego serwisu olbrzymiej liczby zapytań z wielu punktów sieci (stąd „rozproszony" w nazwie), mających w założeniu wysycić zasoby atakowanego systemu tak, by nie był w stanie przyjmować żadnych nowych połączeń. W efekcie na stronę-ofiarę nie dostanie się nikt. Można to porównać do wlewania wody w lejek – gdy strumień osiągnie poziom graniczny, wszystko zacznie się rozlewać na zewnątrz. Oczywiście od czasów MafiaBoy'a przepustowość lejków wzrosła, niestety podobnie stało się ze strumieniem wody. W dzisiejszych czasach „MafiaBoys" nie muszą sami tworzyć botnetu, mogą go po prostu kupić. Podaż znacznie przewyższa popyt – odcięcie od sieci biznesowej konkurencji kosztuje relatywnie niewiele. Niespadająca liczba podatności na złośliwe oprogramowanie i wzrastająca liczba komputerów z dostępem do Internetu to jedne z kilku czynników, wpływających na to, iż na chętnych czeka kilkadziesiąt milionów komputerów-zombie, połączonych w botnety, których moc obliczeniowa sprzedawana jest na czarnym rynku. Cenę rzędu 10 dolarów za godzinę, czy ok. 50 za dzień DDoS uniesie nawet kieszeń licealisty. Na dłuższe ataki już sobie nie pozwoli, ale 150 USD za tydzień „wypożyczenia" botnetu, czy ok. 1200 za miesiąc to niewiele dla firmy, która chce w nieuczciwy sposób osiągnąć przewagę nad konkurencją. Obawy przed wykryciem? Żadne – za takie usługi płaci się wyłącznie wirtualną gotówką. Jest ona oczywiście przeliczalna na prawdziwe pieniądze, nie da się jednak podążać śladem wykonywanych przy jej pomocy transakcji.



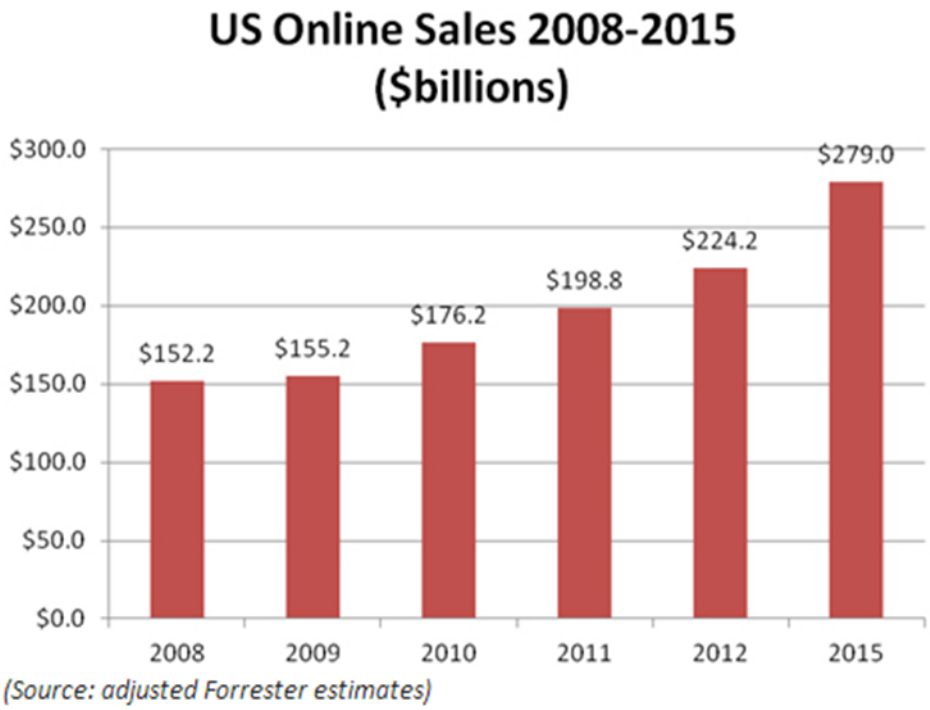
Nie tylko przestępcy

Dlatego też za atakami DDoS nie stoją tylko motywy kryminalne. Co więcej, według raportu Arbor Network główną motywacją do tego typu działań jest przenoszenie na grunt wirtualny dyskusji o podłożu politycznym, czy ideologicznym. Nie trzeba szukać daleko. Gdy opinia publiczna dowiedziała się o planach ratyfikowania przez Polskę umowy ACTA (Anti-Counterfeiting Trade Agreement - umowa dotycząca zwalczania obrotu towarami podrabianymi), w styczniu 2012 jedna po drugiej „padały" nasze witryny rządowe. Do tych ataków przyznawała się w czasie rzeczywistym grupa tzw. hacktywistów, funkcjonująca pod nazwą Anonymous (Anonimowi). Akurat tamte ataki nie zagroziły infrastrukturze krytycznej (ucierpiały jedynie strony informacyjne), sytuacja wyglądała znacznie gorzej trzy lata wcześniej, gdy ci sami Anonimowi w proteście przeciwko zatrzymaniu szefa WikiLeaks, Juliana Assange, zaatakowali – skutecznie – m.in. serwisy PayPala oraz organizacji płatniczych Visa i MasterCard. Dodatkowy „botnet" tworzyli wtedy haktywiści z całego świata, dołączając do ataku za pośrednictwem ogólnodostępnego w sieci narzędzia LOIC (Low Orbit Ion Cannon), gdzie wpisując atakowany adres przeprowadzamy DoS z własnego komputera (inna sprawa, że akurat w tym wypadku wykrycie sprawcy nie jest trudne, o czym część z nich przekonała się na własnej skórze.

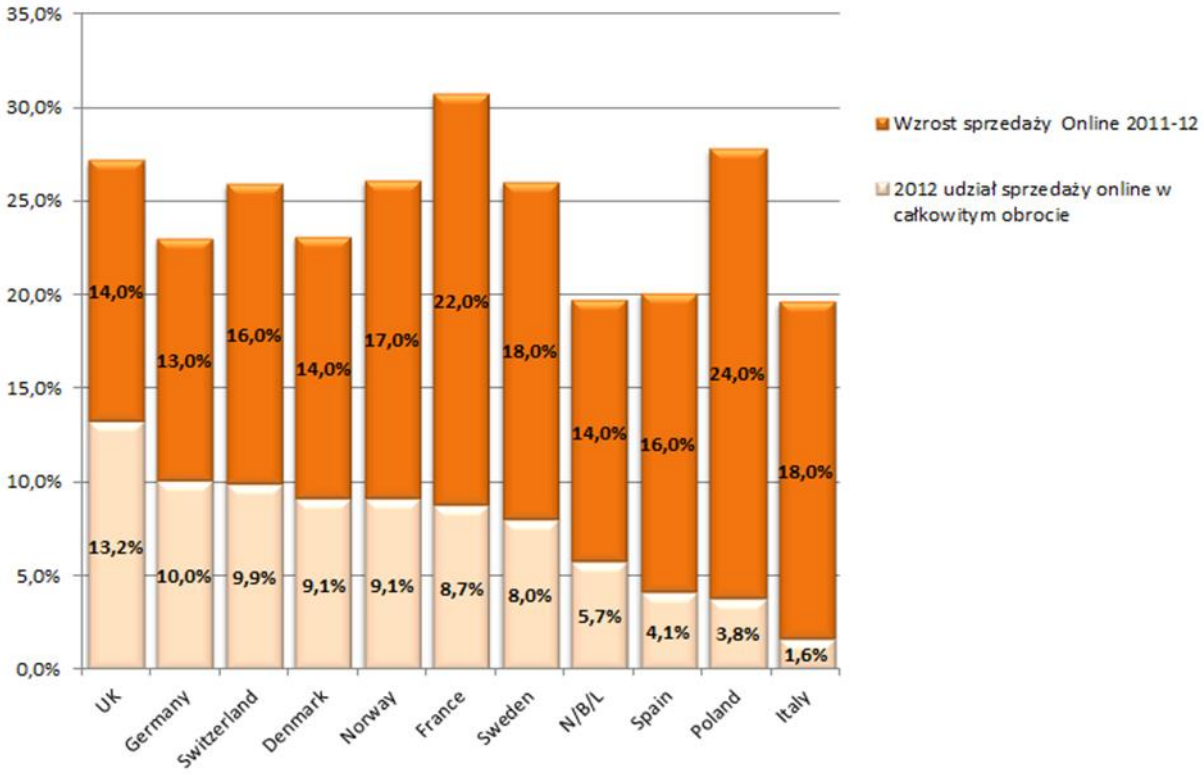


Source: Arbor Networks, Inc.

Nie ma ani cienia przesady w powiedzeniu, że: „Internet jest tak powszechny, że po prostu nie można w nim nie być. Inaczej skazujesz się na samowykluczenie". Obecny model biznesu niejako przestawił cykl, sprawiając, iż najpierw pojawiamy się w sieci, udostępniając użytkownikom ten kanał sprzedażowy, następnie zaś – jeśli w ogóle jest taka potrzeba – organizujemy klasyczny kanał dostaw. Do sieci trafimy niezależnie od naszej woli, a w świetle oczekiwań i potrzeb „cyber-społeczeństwa" jeśli firmy nie ma w Internecie, to znaczy, że nie istnieje. Dla użytkownika końcowego przy obecnym tempie życia kluczowa jest szybkość dostępu wiedzy i dóbr, a przed wszystkim wygoda, dostawcy zaś taki model oferuje znacznie większą efektywność kosztową i optymalizację procesu dostawy. A co się dzieje w przypadku ataku, gdy większość naszego biznesu oparte jest na sieci? Biznes staje, a koszty rosną z godziny na godzinę, nierzadko w postępie logarytmicznym. Co więcej, sytuacja wcale nie będzie się poprawiać, bowiem obrót handlowy w Internecie wzrasta w tempie wykładniczym (od 152,2 mld $ w 2008 r., poprzez 224,2 mld $ w ubiegłym roku do prognozowanych przez Forrestera 279 mld w 2015 roku). Polskę na tle Europy z jednej strony cechuje mały udział sprzedaży online, z drugiej jednak – największa tendencja wzrostowa na Starym Kontynencie.



(Source: adjusted Forrester estimates)



To tylko zasłona dymna

Największy odnotowany DDoS miał siłę 105 Gigabitów na sekundę (22 tysiące razy więcej, niż średni ruch z komputera jednego amerykańskiego internauty), jednak średnia dla tego typu ataków to 1,5 Gbps. Obrona własnymi siłami przed takimi zagrożeniami w większości przypadków nie jest po prostu możliwa. Co więcej, przez lata techniki DDoS też nie uniknęły rozwoju i obserwujemy spadek najprostszych ataków wolumetrycznych na rzecz najbardziej wyrafinowanych, aplikacyjnych. W tym ostatnim przypadku mamy do czynienia z wysyceniem zasobów infrastruktury dostarczającej konkretną funkcjonalność przy pominięciu pozostałych elementów. Tego typu atak może wykorzystywać mniejsze pasmo, przez co pozostaje znacznie trudniejszy do wykrycia. W efekcie w ostatnim czasie odsetek ataków aplikacyjnych wzrósł z 20 do 45 procent i nie wydaje się, by ten trend miał się odwrócić. Warto też pamiętać, że fakt, iż doświadczamy właśnie DDoS nie musi wcale świadczy o tym, że atakujący poprzestaje na tym. Ataki w warstwie aplikacyjnej bardzo często pełnią jedynie rolę „zasłony dymnej" odciągając dedykowane zasoby od faktycznego celu ataku, którym może być kradzież poufnych danych lub po prostu „wyczyszczenie" kont klientów e-bankowości.

Dlatego właśnie w strukturach Orange Polska uruchomiono całodobowe Security Operations Centre, wyspecjalizowane w ochronie przed opisanymi przeze mnie zagrożeniami. Działalność przez 24 godziny na dobę pozwala na niezwłoczne wykrycie zagrożenia na poziomie sieci i przekierowanie ruchu o charakterze anomalii do odpowiedniego urządzenia sieciowego, dzięki czemu osoba korzystająca z chronionych serwisów ma pełen dostęp do ich funkcjonalności, mimo trwającego ataku.

REAGOWANIE NA INCYDENTY W OBSZARZE

INFRASTRUKTURY KRYTYCZNEJ

Mirosław Maj
Fundacja
Bezpieczna
Cyberprzestrzeń

To, że domena teleinformatycznej infrastruktury krytycznej (dalej TIK) wymaga reagowania na incydenty, wiadomo od dawna. Zwłaszcza po tym, jak rozwiano wszelkie wątpliwości co do tego, że nadzorowanie i sterowanie urządzeniami odpowiedzialnymi za utrzymanie tej infrastruktury, narażone jest praktycznie na wszystkie bezpośrednio przychodzące z sieci internetowej zagrożenia. Inżynierowie odpowiedzialni za budowę i utrzymanie systemów TIK, przez długi czas bronili się przed poważnym rozważaniem takich scenariuszy, ale życie udowodniło, że to strategia. Seria poważnych naruszeń bezpieczeństwa w systemach SCADA na całym świecie udowodniła, że problem jest realny, a zamiatanie go pod dywan może być wyjątkowo niebezpieczne. Praktycznie wszyscy znają historię wirusa Stuxnet, głównie ze względu na jego polityczne konotacje, ale prawda jest taka, że ataki na systemy TIK trwają nieustannie, a ich konsekwencje od czasu do czasu bywają bardzo przykre. W kwestii ochrony TIK rozważa się przede wszystkim dwa problemy: stały problem zdefiniowania obszaru TIK oraz kwestię reagowania na incydenty w tym obszarze. W niniejszym artykule poruszony jest ten drugi temat, bo reagowanie na incydenty staje się coraz ważniejsze, a eksperci coraz częściej podkreślają przecenioną rolę profilaktyki w stosunku do dobrze zorganizowanej reakcji.

CERT rządowy czy CERT dla infrastruktury krytycznej?

Obserwacja trendów związanych z podejmowaniem tematu reagowania na incydenty (dalej IR – ang. Incident Response) dla TIK, wskazuje na istnienie dwóch ścieżek realizacji tego zadania oraz kształtowanie się trzeciej. Ale po kolei.

Po pierwsze, funkcję IR przypisuje się bardzo często jako zadanie dla CERT-ów rządowych lub CERT-ów wojskowych. Tak jest na przykład w Hiszpanii, na Litwie, w Luksemburgu, Finlandii, Danii, Słowenii, czy Gruzji. Jak widać – głównie w Europie. Tak jest też w Polsce, gdzie rządowy CERT.GOV.PL na swoich stronach pisze, że: „obszarem działania CERT.GOV.PL oraz podstawowymi „odbiorcami" usług (ang. constituency) oferowanych przez zespół, są użytkownicy systemów teleinformatycznych administracji państwowej (domena *.gov.pl), a także podmioty należące do tzw. krytycznej infrastruktury teleinformatycznej państwa". Wydaje się, że ten trend europejski związany jest z historyczną, ważną rolą europejskich CERT-ów, które przez swoje aktywne i skuteczne działanie sprawiły, że tematy najważniejsze dotyczące bezpieczeństwa IT przypisywane są właśnie tego typu komórkom.
W szczególności chodzi tu o zespoły wywodzące się z europejskiego środowiska akademickiego. Idea CERT-ów została więc przejęta również przez administrację państwową wielu krajów i to jest z pewnością zjawisko bardzo pozytywne. Mniej pozytywne jest to, że nie we wszystkich przypadkach przejęto również wypracowane przez te CERT-y zasady funkcjonowania, np.: dotyczące otwarcia się na współpracę międzynarodową i proaktywną wymianę informacji, co wydaje się krytyczne dla dobrego funkcjonowania każdego CERT-u. Gwoli ścisłości warto dodać, że mimo europejskich korzeni, trend ten nie jest ograniczony do Europy i podobny model funkcjonuje na przykład w Australii.

Drugi sposób podejścia do tematu reagowania w obszarze TIK, to sposób amerykański i typowe dla Amerykanów zadaniowe podejście do problemu, kończące się powstaniem kolejnego podmiotu, ściśle zajmującego się powierzonym zadaniem. W ten sposób doszło do powstania amerykańskiego ICS-CERT, czyli Industrial Control Systems-CERT. CERT ten, w odróżnieniu od CERT-ów rządowych, zajmuje się tylko i wyłącznie sprawami związanymi z ochroną TIK. A najlepszym dowodem na to jest fakt, że przecież w Stanach Zjednoczonych, które – przypomnijmy – są ojczyzną idei CERT-owej, istnieje też CERT rządowy – US-CERT.

Warto zauważyć jeszcze jeden trend, w którym rolę IR dla TIK przypisano nowopowstałym organizacjom, skupiającym w danym kraju wszelkie funkcje związane z ochroną cyberprzestrzeni. Tak jest na przykład w Holandii, gdzie tamtejszy CERT rządowy GOVCERT.NL wyewoluował w kierunku organizacji o nazwie National Cyber Security Centrum.
Nie wchodząc w ocenę poszczególnych modeli, bo byłoby to możliwe tylko w przypadku przeprowadzenia szczegółowych badań nad skutecznością poszczególnych rozwiązań, warto przyjrzeć się rozwiązaniu amerykańskiemu. Podstawowym powodem takiego wyboru jest fakt, że to właśnie dzięki zawężonemu i precyzyjnemu określeniu oczekiwań w stosunku do ICS-CERT zajmuje się on praktycznie tylko tym, czym CERT odpowiedzialny za IR w TIK zajmować się powinien. W rezultacie obserwacja poczynań takiego CERT-u daje szanse na rozpoznanie najważniejszych zadań.

Czym się zajmuje ISC-CERT?

ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

ICS-CERT jest częścią Departamentu Bezpieczeństwa Krajowego Stanów Zjednoczonych (Department of Homeland Security). Powstanie i funkcjonowanie tego CERTu jest realizacją zapisów Programu Ochrony Informatycznej Infrastruktury Krytycznej (PCII Program – Protected Critical Infrastructure Information Program) oraz Programu Bezpie-

czeństwa dla Systemów Kontroli (CSSP – Control System Security Program). Właśnie ten program jest częścią spinającą inne inicjatywy wokół tematu ochrony TIK. Na przykład, w programie uczestniczy też amerykański CERT rządowy – US-CERT. Główne cele tego programu to:

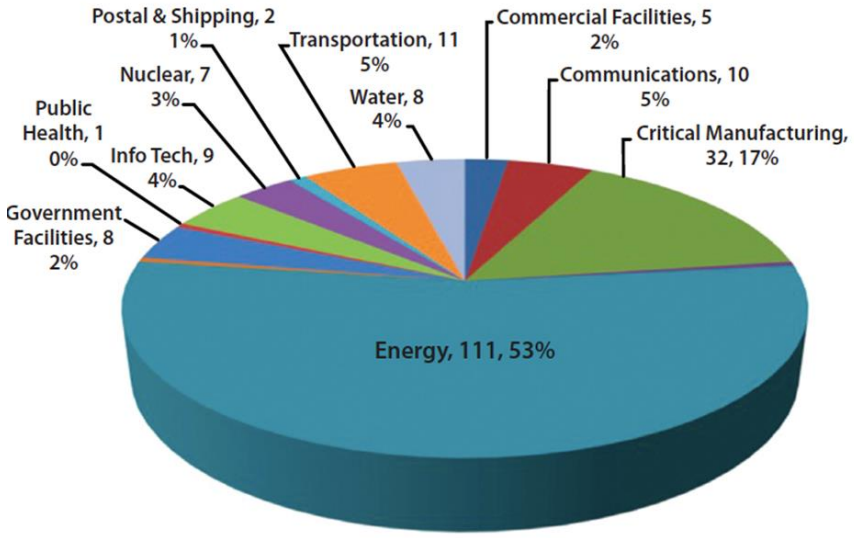
- analiza i zabezpieczanie infrastruktury krytycznej i chronionych systemów;
- identyfikacja słabości systemowych i ocena ryzyka;
- wypracowywanie wsparcia dla procedur ciągłości działania i odtwarzania atakowanych zasobów i serwisów.

Program ma również zapewniać przedstawicielom sektora prywatnego, do którego jak wiadomo należy zdecydowana większość infrastruktury krytycznej, dzielenie się poufną informacją dotyczącą bezpieczeństwa TIK w taki sposób, aby zachować bezpieczeństwo przekazywania tej informacji, w szczególności nieujawnianie jej, co mogłoby, zdaniem autorów programu, zwiększyć ryzyko zakłócenia funkcjonowania TIK w wyniku ataku. Oprócz samej wymiany informacji, chodzi również o wymianę doświadczeń i wspólne prace nad poprawą bezpieczeństwa i lepszą koordynację odpierania zagrożeń. To jest już konkretne zadanie dla ICS-CERT-u.

Zresztą dla realizacji wyżej wspomnianych celów stworzono dwie grupy robocze:

- Industrial Control Systems Joint Working Group (ICSJWG - http://ics-cert.us-cert.gov/Industrial-Control-Systems-Joint-Working-Group-ICSJWG) – właśnie dla współpracy z sektorem prywatnym oraz
- Control Systems Security Working Group (CSSWG) - dla przedstawicieli instytucji federalnych.

ICS-CERT jest aktywny również w obydwu najważniejszych obszarach działań CERT-ów – w obsłudze incydentów naruszających bezpieczeństwo, jak również w stałym prowadzeniu działań ostrzegawczych, uświadamiających i analitycznych. Co prawda niektóre z tych usług realizuje poprzez inne podmioty. Przede wszystkim zgłoszenia dotyczące słabości systemowych oraz złośliwego oprogramowania są zgłaszane do CERT Coordination Center, czyli pierwszego CERTu na świecie, dziś specjalizującego się między innymi dokładnie w tych dwóch dziedzinach. Natomiast incydenty związane z phishingiem są „odsyłane" do US-CERT. Sam ICS-CERT skupia się na incydentach związanych bezpośrednio z TIK. Swoją drogą, ten przykład pokazuje, że zadaniowe podejście i tworzenie nowych struktur jest możliwe między innymi dzięki bardzo precyzyjnemu przypisaniu zakresu odpowiedzialności.



Podział incydentów obsłużonych przez ICS-CERT w I poł. 2013, w odniesieniu do zgłaszających incydenty sektorów

Jeśli chodzi o działania ostrzegawcze, analityczne i uświadamiające, to ICS-CERT zapewnia cały wachlarz usług. Zespół publikuje:

- porady (advisories), które zawierają informacje o bieżących słabościach i występowaniu exploitów je atakujących,
- ostrzeżenia (alerty), które są alertami w sytuacjach wymagających szczególnej uwagi i reakcji,
- newslettery, które są wynikiem gromadzenia informacji poruszających wybrane tematy. Są one skierowane bezpośrednio do personelu zaangażowanego w ochronę TIK,
- raporty uświadamiające (Joint Security Awareness Reports), czyli wszelakie materiały i informacje (np.: o różnych przewidzianych inicjatywach czy konferencjach), będące cennym materiałem do stałego podnoszenia świadomości związanej z koniecznością zapewnienia bezpieczeństwa dla TIK,
- raporty, które w praktyce są albo technicznymi raportami z analiz zagrożeń albo raportami rocznymi ICS-CERT.

Uzupełnieniem tych działań proaktywnych są szkolenia organizowane przez zespół. Są to szkolenia online, np.: szkolenie OPSEC for Control Systems, które jest dostępne dla wszystkich (np. http://opsecics.inl.gov/dhsopsecr01/player.html) oraz szkolenia stacjonarne.

Czy CERT dla TIK ma co robić?

Wydaje się, że tak. W 2012 roku do zespołu zgłoszono 198 incydentów. Są to incydenty o szczególnym znaczeniu, raczej nie obsługiwane automatycznie, co oznacza, że z każdym z nich wiąże się konkretna, w niektórych przypadkach, niełatwa praca. Natomiast w 2013 roku, już w pierwszym półroczu fiskalnym (od października 2012 do maja 2013), zgłoszono 200 incydentów. Ponad połowa z nich (53%) dotyczy sektora energetycznego, a najczęściej spotykane ataki to SQL Injection, spear-phishing, czyli dedykowany phishing na konkretne osoby oraz „watering hole" atak, dla tych którzy są „odporni" na „spear-phishing".

Zakres działalności ICS-CERT pokazuje, że aby dobrze realizować usługi dla szczególnego sektora jakim jest IK, trzeba podjąć wyzwanie i świadczyć praktycznie wszystkie znane, kluczowe usługi CERT-owe. Natomiast najważniejsze jest, aby ci, którzy się tego podejmą, zwrócili uwagę na dwa bardzo ważne aspekty:

1. Zagrożenia dotyczą przede wszystkim systemów przemysłowych (SCADA) i bez wiedzy specjalistycznej z tej dziedziny oraz bez bliskiej współpracy z producentami tych systemów, nie da się realizować zadań.
2. Sektor TIK jako priorytet działania przyjmuje funkcję bezpieczeństwa określaną jako „dostępność", natomiast najgroźniejsze obecnie ataki na urządzenia sieciowe atakują ich poufność i integralność. Skuteczne zaatakowanie tych funkcji może doprowadzić w konsekwencji do utraty dostępności, a po drodze jeszcze do poważnej katastrofy. Dlatego bardzo ważne są działania uświadamiające wobec operatorów TIK i bliska współpraca z nimi, oparta o znajomość tego środowiska i jego potrzeb.

Specjalnie dla CIIP focus:

Damir Rajnovic o reagowaniu na incydenty w teleinformatycznej infrastrukturze krytycznej

Damir Rajnovic ma blisko 20 letnie doświadczenie w dziedzinie reagowania na incydenty. W 1995 roku stworzył i przez kilka lat kierował chorwackim zespołem CERT – CARNet CERT. Następnie był zaangażowany w projekt EuroCERT oraz współpracę ze światowymi producentami takimi jak CISCO czy Panasonic. Jest mocno zaangażowany w międzynarodową współpracę zespołów reagujących. W czasie ostatniej konferencji FIRST (Forum of Incident Response and Security Teams) został wybrany do władz FIRST. W trakcie tej samej konferencji był jednym z panelistów panelu „Global Disaster Recovery". Tematyki reagowania kryzysowego dotyczyła też nasza krótka rozmowa z Damirem Rajnovicem.

CIIP focus: Damir, reagowanie kryzysowe i zespoły reagujące CERT to światy bliskie sobie, ale nie tożsame. Każdy z nich zbiera przez lata swoje doświadczenia. Co Twoim zdaniem specjaliści z sektora teleinformatycznej infrastruktury krytycznej (TIK) mogliby się nauczyć od specjalistów z zespołów CERT-owych i na odwrót.

Damir Rajnovic: Jestem przekonany, że obydwie strony mogą się wiele od siebie nauczyć. Niektóre aspekty TIK i telefonii to pierwsze z brzegu dobre przykłady migracji usług do Internetu. CERT-y mogą mieć więcej doświadczenia ze sprawami odnoszącymi się do spraw internetowych i doświadczenia te mogą przekazywać do świata „telco". Z drugiej strony komunikacja bezprzewodowa (np.: radio, TV, łączność satelitarna) to tradycyjnie nie są mocne punkty CERT-ów, które koncentrują się na Internecie. CERT-y mogą się nauczyć o tych nowych technologiach, co może być z dużą korzyścią dla nich. W konsekwencji mogą przyczynić się do wykrycia nowych typów słabości tych rozwiązań.

CIIP focus: W Twojej opinii jak powinno być rozwiązane reagowanie na incydenty dla TIK. Czy to powinno być kolejne zadanie nowych CERT-ów, czy raczej to pole do popisu dla zupełnie nowych, dedykowanych organizacji?

DR: Moim zdaniem istniejące CERT-y w organizacjach, które już teraz zarządzają TIK powinny rozszerzyć swoje działania na obszar TIK. Na przykład tradycyjny dostawca usług telefonicznych prawdopodobnie również ma część internetową w swojej infrastrukturze i tam funkcjonuje CERT, dla pojawiających się incydentów. Taki CERT powinien rozszerzyć swoje usługi o część czysto telekomunikacyjną. To najprawdopodobniej doprowadziłoby do tworzenia wewnątrz organizacji nowego zespołu, aczkolwiek nie należy traktować takiego rozwiązania jako rozwiązanie domyślne.
Ogólnie rzecz biorąc, nie jestem zwolennikiem tworzenia nowych zespołów tylko dla takiego faktu, w szczególności jeśli miałoby to budować strukturę pionową i układ hierarchiczny. Moja pierwsza myśl dotycząca rozwiązania sytuacji to stworzenie nowego zespołu skupiającego kompetencje funkcjonujących obecnie specjalistów.

CIIP focus: A jaka jest Twoja opinia w sprawie partnerstwa publiczno-prywatnego (PPP) w dziedzinie radzenia sobie z sytuacjami kryzysowymi?

DR: PPP jest absolutnie kluczowe w takiej sytuacji, co wynika z faktu posiadania i zarządzani TIK przez sektor prywatny. Sektor prywatny może potrzebować pewnego wsparcia ze strony rządu, w szczególności do stworzenia systemów wykorzystywanych w sytuacjach kryzysowych. Takie systemy mogą posiadać dodatkowe funkcje i możliwości, które byłyby zamawiane i wykorzystywane tylko w sytuacji realnej potrzeby. Chodzi również o koszty związane z funkcjonowaniem takich systemów. Normalnie bowiem taki koszt jest przerzucany przez operatorów TIK na klientów końcowych.

CIIP focus: Bardzo dziękujemy za tą krótką ale bardzo dla nas intersującą rozmowę.

DR: Również dziękuję.

Baner konferencji FIRST (źródło: FIRST.org)

XXV Konferencja FIRST światowy zjazd CERT-ów

Mirosław Maj
Fundacja Bezpieczna Cyberprzestrzeń

W dniach 16 – 21 czerwca 2013 r. w Bangkoku odbyła się coroczna konferencja FIRST (Forum of Incident Response and Security Teams). To już 25-ta edycja tej konferencji. To najstarsza, cykliczna impreza zrzeszająca zespoły reagujące z całego świata. Pierwsza z nich miała miejsce w siedzibie pierwszego CERT-u na świecie, w Pittsburghu, w 1989 roku, niespełna rok po powstaniu tamtejszego zespołu - CERT Coordination Center. W tamtym czasie było to raczej kameralne wydarzenie. Dziś konferencja FIRST to światowa impreza, która z roku na rok bije rekordy frekwencji. W tym roku do stolicy Tajlandii zjechało ponad pięciuset uczestników z całego świata.

Konferencja FIRST to największy networking CERT-ów

O tym, że konferencja FIRST, a i sama organizacja, staje się coraz bardziej znaczącym wydarzeniem, niech świadczy fakt, że tegoroczna konferencja została otwarta na niespotykanym dotychczas szczeblu. Otwarcia dokonała bowiem premier Królestwa Tajlandii – Pani Yingluck Shinawatra.

Równie dużego prestiżu ceremonii otwarcia nadał przedstawiciel agencji Interpol, który opowiadał o wysiłkach agencji, szczególnie skierowanych na sprawy międzynarodowej współpracy, która ma poprawić zdolność do ścigania cyberprzestępstw.

Konferencja FIRST, tradycyjnie już, trwa cały roboczy tydzień, a nawet zaczyna się sesją networkingową w niedzielę wieczorem. Uczestnicy to przede wszystkim przedstawiciele zespołów CERT-owych, których jest zrzeszonych w FIRST ponad 200. Ale nie tylko. Warto podkreślić, że nie trzeba być członkiem FIRST, aby być uczestnikiem konferencji. Konferencja jest otwarta dla wszystkich zainteresowanych tematem bezpieczeństwa teleinformatycznego. Jeśli ktoś chce nasiąknąć tematyką bezpieczeństwa IT do reszty, to organizatorzy dostarczają mu w ciągu tygodniu doskonałej do tego okazji. Zainteresowani mogą brać udział w spotkaniach i wykładach już od wczesnych godziny porannych, a zakończyć swoją aktywność nawet po kilkunastu godzinach. Czasami staje się przed trudnym wyborem, ze względu na równoległe sesje. W tym roku odbywały się one w trzech obszarach tematycznych:

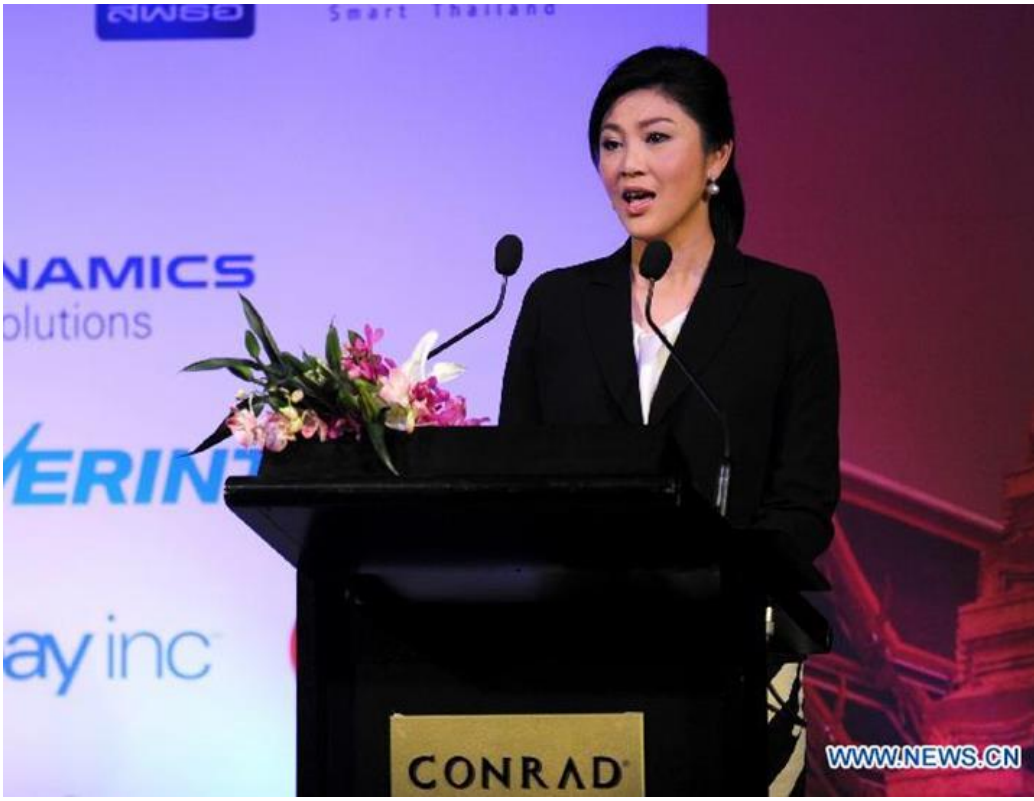
- Deep Technical Dives
- Technical Foundations
- Policy & Management

Obok głównych pozycji programu konferencji, w ciągu tygodnia konferencyjnego, organizowane są też spotkania dodatkowe. Szczególne znaczenia mają te, które są związane z działalnością FIRST-owych SIG-ów, czyli Special Interest Group. W tym roku spotykali się przedstawiciele trzech SIG-ów:

- CVSS-SIG (Common Vulnerability Scoring System) – grupa zajmująca się rozwojem i promocją standardu CVSS;
- Vendor SIG – grupa zrzeszająca przedstawicieli producentów, którzy wspólnie rozważają sprawy ich współpracy na rzecz bezpieczeństwa;
- VRDX-SIG: Vulnerability Reporting and Data eXchange SIG – grupa zajmująca się zagadnieniami identyfikacji i dzielenia się informacją o słabościach systemowych;
- CSIRT Metrics SIG – grupa która pracuje nad tworzeniem i promocją mierników opisujących działanie i skuteczność CERT-ów, np.: próba wypracowania wspólnej informacji o statystykach przestępstw komputerowych.

Na konferencji FIRST tradycyjnie można spotkać praktycznie wszystkich, których w czasie rozwiazywania incydentów poznaliśmy „wirtualnie" albo zaraz poznamy. Doświadczenie mówi, że nie ma lepszej metody na usprawnienie działań operacyjnych, w szczególności w nietypowych i niebanalnych sytuacjach, niż osobiste spotkania z osobami, z którymi za chwilę będziemy wymieniali istotne dane, prosili o pomoc w interwencji albo namawiali na nowy, ciekawy, wspólny projekt. Korytarze konferencyjne są wypełnione niemalże cały czas parami lub grupami osób, które dyskutują o spra-

wach z przeszłości lub omawiają przyszłą potencjalną współpracę. To niezwykle ważne wydarzenie dla środowiska.
Coroczny FIRST to również sprawy formalne dla organizacji, czyli przede wszystkim Walne Zgromadzenie Członków FIRST, w trakcie którego odbywają się wybory do dziesięcioosobowego Komitetu Sterującego FIRST. Komitet, dzień po wyborach spotyka się i wybiera swojego przewodniczącego (wtedy gdy kadencja poprzedniego upływa). Tak było w tym roku. Nowym szefem FIRST został Maarten Van Horenbeeck, reprezentujący Google Inc. Z rozmów z niektórymi nowowybranymi członkami FIRST wynika, że mają oni sporo pomysłów na zmiany w FIRST, głównie w kierunku uczynienia tej organizacji bardziej operacyjną i wspomagającą działanie poszczególnych członków. Czas pokaże czy ten kierunek zmian będzie odpowiednio silny.



Fot. Premier Królestwa Tajlandii – Pani Yingluck Shinawatra otwiera XXV konferencję FIRST. (fot. news.xinhua.net)

Ochrona IK w agendzie konferencji

Trzeba sobie zupełnie szczerze powiedzieć, że ochrona teleinformatycznej infrastruktury krytycznej to nie jest częsty punkt w agendzie konferencji FIRST. Chociaż, jeśli oderwiemy się od wyszukiwania tej tematyki wprost i przeanalizujemy pozycje programowe, to okazuje się, że ten temat nie jest pomijany. Na przykład referat Rolanda Dobbinsa za Arbor Networks o atakach DDoS na amerykańskie banki, to de facto temat jak najbardziej z zakresu ochrony IK. Podobnie jest zresztą z tematem, który miałem okazję osobiście przedstawiać, a który dotyczył podsumowania ćwiczenia Cyber-EXE Polska 2012 i zagadnieniu organizacji tego typu ćwiczeń na poziomie narodowym. Natomiast ściśle tematykę ochrony IK poruszali przedstawiciele krajów azjatyckich. Lauri Korts-Pärn i Masako Someya z japońskiego Cyber Defense Institute opowiadali o swoich doświadczeniach z prac nad poprawą bezpieczeństwa IK w Japonii. W prezentacji skoncentrowali się na praktycznych aspektach bezpieczeństwa systemów kontroli i sterowania procesami przemysłowymi (tzw. SCADA). Opowiadali także o swoich metodach pracy nad poprawą bezpieczeństwa tych systemów, czyli o technicznych audytach i organizowanych ćwiczeniach, podobnych do tych jakie mieliśmy w Polsce.
Przedstawiciel Indonezji Bisyron Wahyudi z ID-SIRTII przedstawił zaś doświadczenia indonezyjskiego CERT-u narodowego, związane z ich zaangażowaniem w sprawy ochrony IK. Głównie, doświadczenia te odnosiły się do zagadnień organizacyjnych. Można było usłyszeć o organizacji systemu obsługi incydentów, o tym czym de facto jest obsługa incydentów w ich przypadku, współpracy z producentami oraz pracach zawiązanych z konsolidacją całego środowiska podmiotów zainteresowanych ochroną IK.

Polska na konferencji FIRST

W tym roku przedstawiciele Polski byli widoczni w czasie konferencji, głównie za sprawą liczby pozycji w agendzie konferencji. Znalazły się w niej prezentacje zespołu CERT Polska oraz Fundacji Bezpieczna Cyberprzestrzeń. Polscy uczestnicy konferencji mieli chyba najlepszy współczynnik jeżeli chodzi o liczbę uczestników do liczby prezentacji. Zresztą nie tylko byliśmy widoczni na salach wykładowych. Równolegle do konferencji przeprowadzany był Dragon Research Group Security Challenge – konkurs polegający na rywalizacji czteroosobowych zespołów, które musiały rozwiązywać techniczne zadania związane z bezpieczeństwem. W konkursie liczyły się de facto tylko dwa zespoły, a na ośmiu członków tych zespołów aż trzech stanowili Polacy. W zwycięskim zespole znalazł się Adam Smutnicki z Wrocławskiego Centrum Sieciowo-Superkomputerowego.

Za rok w Bostonie

Przyszłoroczna konferencja FIRST odbędzie się tradycyjnie w czerwcu. Tym razem specjaliści bezpieczeństwa z całego świata wybiorą się do Bostonu. Po raz pierwszy w historii konferencja odbędzie się w jednym z poprzednich miejsc. Co ciekawe, dokładnie po dwudziestu latach konferencja FIRST trafi do dokładnie tego samego hotelu w jakim się odbyła w 1994 roku. Myślę, że wszyscy zajmujący się tematyką reagowania na incydenty powinni poważnie rozważyć swój udział w tym przedsięwzięciu. Być może język polski będzie częściej słyszalny na korytarzach konferencyjnych.

Całość programu konferencyjnego wraz ze streszczeniami wystąpień znajduje się pod adresem: http://conference.first.org/program/index.aspx

Teleinformatyczna infrastruktura krytyczna w pracach Europejskiej Agencji Bezpieczeństwa Sieci i Informacji

Krzysztof Silicki
Doradca Dyrektora NASK - Dyrektor ds. współpracy z ENISA,
Rada Zarządzająca ENISA

Europejska Agencja Bezpieczeństwa Sieci i Informacji (ENISA, www.enisa.eu) jest powstałą w roku 2004 z inicjatywy Komisji Europejskiej i Parlamentu – agencją zajmującą się problematyką bezpieczeństwa teleinformatycznego na poziomie europejskim (w czerwcu bieżącego roku ENISA uzyskała kolejny, siedmioletni mandat będący podstawą jej funkcjonowania jako agencji europejskiej w dziedzinie bezpieczeństwa sieci i informacji). Stanowi wsparcie dla krajów członkowskich Unii Europejskiej oraz samej Komisji w rozwijaniu wiedzy oraz wspieraniu inicjatyw na rzecz podnoszenia poziomu bezpieczeństwa w cyberprzestrzeni, w szczególności w takich obszarach jak ochrona infrastruktury krytycznej, strategie bezpieczeństwa cyberprzestrzeni, współpraca zespołów CERT/CSIRT i innych. ENISA dostarcza między innymi wielu niezależnych opracowań w postaci prac studialnych, raportów, poradników czy dobrych praktyk. W niniejszym artykule skupimy się na obszarze związanym z ochroną krytycznej infrastruktury w aspekcie teleinformatycznym.

Zbieranie i wymiana doświadczeń

Teleinformatyczna infrastruktura w krytycznych sektorach takich jak energetyka, transport, przemysł paliwowy, chemiczny czy w samym sektorze telekomunikacji szybko się rozwija, staje się coraz bardziej rozproszona i złożona. Szczególne znaczenie ma ta tendencja dla sektorów produkcyjnych, gdzie istnieje konieczność ciągłego, zdalnego monitorowania i sterowania procesami technologicznymi. Warto przyjrzeć się więc, w jaki sposób rozwijają się technologie teleinformatyczne oraz nowoczesne systemy sterowania – ICS (Industrial Control Systems). Największą podgrupę systemów ICS stanowi SCADA (Supervisory Control and Data Acquisition systems). Systemy ICS przechodzą znaczącą transformację – od firmowych, zamkniętych rozwiązań danych producentów o charakterze lokalnym – do systemów o otwartej architekturze, połączonych w ten czy inny sposób z sieciami korporacyjnymi i korzystającymi z Internetu. Nowoczesne rozwiązania używają też coraz częściej oprogramowania komercyjnego, znanego z sektora informatycznego. Ma to szereg zalet takich jak redukcja kosztów, interoperacyjność, łatwość zarządzania i możliwość dostępu zdalnego, ale z drugiej strony wprowadzają określoną klasę zagrożeń, znanych wcześniej z dziedziny teleinformatyki, w tym z sieci IP i Internetu.

ENISA traktuje swój dział zajmujący się pracą na rzecz wspierania bezpieczeństwa europejskiej, teleinformatycznej infrastruktury krytycznej (CIIP), jako jeden z najważniejszych i w ramach swych prac prowadzi szereg działań zarówno na poziomie technicznym i organizacyjnym, a także w obszarze europejskich regulacji. Celem głównym jest zgromadzenie doświadczeń i wiedzy pochodzącej z wielu obszarów takich jak: instytuty naukowe, dostawcy sprzętu i oprogramowania, operatorzy infrastruktury, administracja publiczna, CERTy, ciała standaryzacyjne, w celu wypracowania najlepszych praktyk, wskazówek czy poradników, które mogą posłużyć do wypracowania optymalnego podejścia przy rozwiązywaniu problemów bezpieczeństwa infrastruktury krytycznej.

ENISA, w dziedzinach którymi się zajmuje (w tym wypadku jest to CIIP), w celu głębszego zajęcia się określoną tematyką, powołuje grupy robocze ekspertów oraz organizuje warsztaty w celu wsparcia dyskusji i wymiany doświadczeń w Europie. Co więcej, przy wsparciu zewnętrznych ekspertów z różnych środowisk, w oparciu o badania oraz opinie zainteresowanych środowisk, publikuje raporty, zestawy dobrych praktyk lub poradniki.

Raport na temat bezpieczeństwa przemysłowych systemów sterowania (ICS)

W grudniu 2011 roku ENISA opublikowała raport o nazwie *Protecting Industrial Control Systems. Recommendations for Europe and Member States* zawierający rezultaty analiz dostępnych opracowań w dziedzinie bezpieczeństwa systemów sterowania, wyniki przeprowadzonych badań kwestionariuszowych w Europie, zestawienie istniejących standardów, poradników, dokumentów o charakterze regulacyjnym, a także opis istniejących inicjatyw na rzecz bezpieczeństwa systemów ICS. Podsumowano kluczowe spostrzeżenia po przeprowadzonej analizie oraz przeprowadzonym warsztacie.

Raport dotyczy wielu warstw: organizacyjnej, technicznej, prawnej, a także ekonomicznej czy świadomościowej. Podkreślono w nim aspekty związane z cyberbezpieczeństwem przemysłowych systemów sterowania, które w ogromnej większości nie były projektowane z myślą o bezpieczeństwie. Przykładowo – protokoły szeregowe nie zawierały mechanizmów uwierzytelniania, integralności czy szyfrowania transmisji. Obecnie są one integrowane ze stosem protokołu TCP/IP (transmisja pakietowa) lub zastępowane przez otwarte standardy, co naraża transmisję na znane zagrożenia/ataki, takie jak podsłuch, przechwytywanie sesji, zmiana zawartości pakietów itp. Także systemy operacyjne są zastępowane przez MS Windows czy Linux, a wiele aplikacji serwerowych pochodzi ze świata teleinformatyki – co równolegle wprowadza do świata systemów przemysłowych nowe zagrożenia. Środowisko sieciowe staje się coraz bardziej połączone i zależne od zdalnego zarządzania. Z drugiej strony, w odróżnieniu od zwykłych systemów przetwarzających i przesyłających informację, systemy ICS tradycyjnie muszą się charakteryzować dużo wyższymi parametrami niezawodnościowymi, mają inne priorytety działania, a ich nieprawidłowe działanie może spowodować dużo większe i bardziej dotkliwe skutki negatywne.

Mając na uwadze, że systemy komputerowego sterowania procesami podlegają już obecnie bardzo poważnym cyberzagrożeniom takim jak dedykowane ataki z wykorzystaniem specjalnie tworzonego szkodliwego oprogramowania (malware) np. Stuxnet, a także całej gamy znanych wirusów czy wszelkich podatności systemów operacyjnych, protokołów i wykorzystywanych aplikacji, istotnym jest, by w każdym przypadku oszacować ryzyko zagrożeń i wdrożyć odpowiednią architekturę i mechanizmy bezpieczeństwa.

W raporcie ENISA skorzystano z wielu znakomitych źródeł informacji, dobrych praktyk, raportów technicznych czy standardów takich instytucji jak brytyjski CPNI czy organizacji standaryzacyjnych (NIST, IEEE, ANSI/ISA, IES, ISO).

Opisano więc istniejące inicjatywy w zakresie bezpieczeństwa ICS, standardy, regulacje, a także braki czy pojawiające się wyzwania. Część dokumentu zawiera głębsze techniczne rozważania i jest skierowana do inżynierów systemowych, administratorów, specjalistów od bezpieczeństwa czy audytorów.

Istotną częścią raportu są oczywiście tzw. „key findings" oraz rekomendacje dla szeregu wspomnianych wyżej obszarów: technicznego, organizacyjnego, regulacyjnego, ekonomicznego.

Niestety, konkluzje dla Europy nie są imponujące w porównaniu z podejściem widocznym np. w Stanach Zjednoczonych, gdzie ustanowiono dedykowany program współpracy pomiędzy administracją a przemysłem pod nazwą CSSP (Control Systems Security Program). W Unii Europejskiej wprawdzie istnieje polityka w stosunku do CIIP, lecz brak jest skoordynowanych inicjatyw skierowanych na bezpieczeństwo systemów ICS. Nie istnieje także europejski standard lub odnośnik do standardów czy regulacji. Brak również organu odpowiadającego za tego typu regulacje. Przedsiębiorstwa działające w różnych krajach członkowskich mogą mieć do czynienia z różnymi regulacjami w tym zakresie.

Istnieje wiele wyzwań, które nie łatwo pokonać. W trakcie badań okazało się także, że operatorzy czy przedsiębiorstwa posiadające infrastrukturę ICS, najczęściej nie posiadają zintegrowanego systemu zarządzania wszystkimi aspektami cyberbezpieczeństwa. Wykorzystywana infrastruktura jest przestarzała, patrząc z punktu widzenia mechanizmów bezpieczeństwa, jednak z powodu długich okresów amortyzacji (15-20 lat), taki sprzęt będzie musiał być wykorzystywany jeszcze przez wiele, wiele lat.

W ten sposób sieci przemysłowe stają się coraz łatwiejszym obiektem ataków typu APT (Advanced Persistent Threat).

Nie jest możliwe, a nawet celowe, by przedstawić całą zawartość raportu w krótkim opracowaniu. Przytoczmy zatem chociaż skrótowo kilka rekomendacji w nim zawartych:

Rekomendacja 1: europejska strategia bezpieczeństwa ICS

- powinno powstać wspólne podejście UE do bezpieczeństwa ICS
- każdy kraj członkowski powinien zbudować swoje podejście, spójne z UE
- spójność z dyrektywami CIIP, inicjatywami np. EuroSCSIE, EP3R

Rekomendacja 2: tworzenie dobrych praktyk

- Unia Europejska powinna stworzyć dokumenty referencyjne określające zestaw najlepszych praktyk bezpieczeństwa sieci przemysłowych
- potrzebny jest konsensus w krajach członkowskich oraz wśród głównych interesariuszy
- całościowe podejście: bezpieczeństwo fizyczne i logiczne

Rekomendacja 3: tworzenie krajowych wzorców bezpieczeństwa ICS

- krajowe programy (lub strategie) w tym obszarze, powinny zawierać wzorce postępowania zarówno dla operatorów, jak i przedsiębiorstw, które mogłyby być łatwo adaptowalne przez ekspertów bezpieczeństwa w danej sytuacji
- wzorce te powinny obejmować aspekty bezpieczeństwa operacyjnego, wskazówki techniczne, zarządzanie bezpieczeństwa wraz z podziałem odpowiedzialności, kryteria biznesowe, czy aspekty zarządzania kryzysowego

Rekomendacja 4: wzrost świadomości i szkolenia

- częścią krajowych programów powinny być zaplanowane wydarzenia (konferencje, seminaria, szkolenia) w celu szerzenia wiedzy z dziedziny bezpieczeństwa ICS
- specjalną uwagą powinni być objete osoby z najwyższej kadry kierowniczej operatorów i przedsiębiorstw
- beneficjentami powinni być użytkownicy końcowi z różnych grup

Rekomendacja 5: wspólna platforma testowania lub system certyfikacji

- wspólna strategia europejska mogłaby prowadzić do ustanowienia platformy, (w modelu PPP), w ramach której możnaby testować współpracę różnych rozwiazań i ich wpływ na bezpieczeństwo
- alternatywnie, w Europie mógłby powstać standardowy model w zakresie bezpieczeństwa ICS (mógłby bazować np. na Common Criteria, bądź FIPS), który pozwalałby na prowadzenie procesu certyfikacyjnego, przez odpowiednie krajowe ośrodki

Rekomendacja 6: tworzenie ICS-CERTów

- krajowe programy bezpieczeństwa ICS powinny zakładać tworzenie zespołów typu CERT, reagujących na zagrożenia - dedykowanych do obszaru bezpieczeństwa teleinformatycznej infrastruktury przemysłowej (ICS-CERT)
- ICS-CERT powinien być ustanowiony we współpracy z istniejącymi strukturami CERT w danym kraju
- kraje członkowskie powinny współpracować, wymieniając informacje o zagrożeniach, podatnościach i atakach w ramach określonej platformy wymiany (np. EuroSCSiE)

Rekomendacja 7: rozwijanie badań naukowych

- rozwijanie badań naukowych i prac badawczo - rozwojowych w dziedzinie bezpieczeństwa sieci przemysłowych na poziomie krajowym i europejskim (programy ramowe)

Cały wachlarz prac

Powyższy raport jest tylko jednym z przykładów opracowań agencji ENISA z dziedziny bezpieczeństwa i odporności sieci przemysłowych, czy szerzej, z obszaru ochrony teleinformatycznej infrastruktury krytycznej.

W wielkim skrócie, w dalszej części artykułu zostały przywołane inne raporty, które dotyczą czy to bezpieczeństwa inteligentnych sieci energetycznych, modeli współpracy administracji i biznesu w ochronie infrastruktury krytycznej, dobrych praktyk i regulacji w zakresie zgłaszania i obsługi incydentów czy stosowanych metryk w celu badania rzeczywistej odporności infrastruktury.

Na pierwszy ogień przedstawiamy kilka raportów dotyczących bezpieczeństwa sieci przemysłowych.

"PROTECTING INDUSTRIAL CONTROL SYSTEMS" - Recommendation for Europe and Member States, grudzień 2011

- raport opisywany w niniejszym artykule

"APPROPRIATE SECURITY MEASURES FOR SMART GRIDS" - Guidelines to assess the sophistication of security measures implementation, grudzień 2012

- raport techniczny zawierający wytyczne określające tzw. minimalne środki bezpieczeństwa, jakie powinny być implementowane w środowisku smartgrid
- objęto nim 10 aspektów takich jak: zarządzanie ryzykiem, zarządzanie relacjami z dostawcami, procedury operacyjne, bezpieczeństwo personelu, obsługa incydentów, audyty, ciągłość działania, bezpieczeństwo fizyczne, bezpieczeństwo systemów informatycznych, bezpieczeństwo sieciowe

"SMART GRID SECURITY " - Recommendations for Europe and Member States, lipiec 2012

- raport zawiera rekomendacje dla sektora prywatnego i publicznego dotyczące bezpieczeństwa inteligentnych sieci energetycznych na podstawie badań studialnych i opinii ekspertów
- szereg rekomendacji jest współbieżnych z tymi z wcześniejszego raportu "Protecting Industrial Control Systems"
- opisano miedzy innymi obecny stan bezpieczeństwa sieci smartgrid w Europie, prace standaryzacyjne, znaczenie technologii ICT w smartgridach, przegląd realnych incydentów, podatności i zagrożeń dla sieci energetycznych, przegląd obowiązujących regulacji i dobrych praktyk

W sytuacji, kiedy większość infrastruktury krytycznej krajów członkowskich leży w rękach sektora prywatnego, naturalnym i koniecznym sposobem działania na rzecz podnoszenia odporności i bezpieczeństwa infrastruktury jest współpraca sektora rządowego z sektorem biznesowym. ENISA poświęca tematyce partnerstwa publiczno-prywatnego, szczególnie w dziedzinie CIIP, wiele miejsca. Poniżej kilka opracowań, które dotykają tego tematu.

"Cooperative models for effective public private partnership" - Desktop Research Report, 2011

- pierwszy raport gromadzący istniejącą wiedzę na temat istniejących, dobrych przykładów partnerstwa publiczno-prywatnego w dziedzinie CIIP
- dokonano przeglądu taksonomii, różnych modeli organizacyjnych, zestawu usług mogących funkcjonować w ramach PPP, przykładów definiowania zakresu działania i składu partnerów, modeli dobrowolnego partnertswa oraz partnerstwa obowiązkowego

"Cooperative models for effective public private partnership" - Good practice guide, 2011

- raport w postaci podręcznika dobrych praktyk w dziedzinie partnerstwa i współpracy PPP w dziedzinie bezpieczeństwa i odporności teleinformatycznej infrastruktury krytycznej
- stara się odpowiedzieć na kluczowe pytania dotyczące PPP w tym obszarze, takie jak: dlaczego partnerstwo publiczno prywatne jest ważne, kto powinien być aktywnie zaangażowany, jak najlepiej zbudować PPP w obszarze security and resilience, kiedy warto jest to robić oraz co stanowi kluczowe elementy PPP

"Network Security Information Exchanges " - Good practice guide

- raport poświęcony jest kwestii sposobów wymiany informacji pomiędzy podmiotami prywatnymi i publicznymi w ramach partnerstwa na rzecz podnoszenia bezpieczeństwa i odporności infrastruktury kryrtycznej
- przedstawiono modele oparte na koncepcji punktu (platformy) wymiany informacji (Network Security Information Exchange)
- dokonano agregacji wielu dobrych praktyk w tym zakresie , istniejących w krajach członkowskich

W ciągu ostatnich lat obserwujemy w Europie wzrost świadomości konieczności zgłaszania incydentów naruszania bezpieczeństwa do odpowiednich, wyspecjalizowanych jednostek, zwykle zwanych CERT lub CSIRT, ale także do organów regulacyjnych w danym sektorze gospodarki (np. telekomunikacja, energetyka) czy też organów odpowiedzialnych za bezpieczeństwo (np. danych osobowych, czy sieci administracji państwa). Zgłaszanie incydentów jest istotnym elementem procesu reagowania na zagrożenia w cyberprzestrzeni, tworzenia prawdziwego obrazu zagrożeń w postaci statystyk czy w końcu budowania właściwych strategii czy polityk bezpieczeństwa kraju czy poszczególnych, kluczowych sektorów takich jak telekomunikacja, energetyka, administracja, sektor finansowy i inne.

ENISA dokonała przeglądu istniejących oraz planowanych inicjatyw i regulacji w obszarze raportowania o zagrożeniach i incydentach. W ramach przyjętego w Unii Europejskiej tzw. pakietu telekomunikacyjnego funkcjonuje art.13a, regulujący kwestie zapewnienia bezpieczeństwa i zgłaszania do organu regulacyjnego istotnych incydentów naruszających bezpieczeństwo lub integralność sieci przez dostawców publicznych usług telekomunikacyjnych (W naszym kraju artykuł ten znajduje swoje odzwierciedlenie w znowelizowanym Prawie telekomunikacyjnym). Podobnie rzecz się ma z art. 4 dyrektywy o prywatności, wymagającej zgłaszania naruszeń danych osobowych do odpowiednich organów krajowych (w Polsce GIODO). W projektowanym rozporządzeniu UE dotyczącym elektronicznej identyfikacji i usług zaufania, także znajdują się zapisy dotyczące bezpieczeństwa i zgłaszania ich naruszeń (art. 15). Komisja Europejska planuje systematyczne rozszerzanie podobnych zapisów na inne sektory (sektor finansowy, zdrowia, administracja publiczna). Poniżej znajduje się lista opracowań agencji ENISA na ten temat:

"Cyber incident reporting in the EU" - an overview of security articles in EU legislation, sierpień 2012

- przegląd istniejących i planowanych regulacji w UE dotyczących obowiązku zapewniania minimalnego poziomu bezpieczeństwa przez dostawców usług wraz z obowiązkiem zgłaszania istotnych naruszeń do odpowiednich organów krajowych i europejskich

"Good practices on reporting security incidents" - 2009

- studium istniejących w UE schematów raportowania i obsługi incydentów naruszających bezpieczeństwo
- zestaw najlepszych praktyk w tej dziedzinie w każdym z etapów planowania, przygotowywania procedur, budowy, zarządzania - z uwzględnieniem wskazówek dotyczących procesu uzyskiwania coraz wyższego poziomu dojrzałości systemu raportowania i obsługi incydentów

"Technical guideline for minimum security measures" - Guidance on the security measures in Article 13a, grudzień 2011

- opracowanie mające charakter zestawu porad dla NRA (krajowych regulatorów) w zakresie implementacji artykułu13a pakietu telekomunikacyjnego, dotyczącego obowiązku zapewniania przez dostawców odpowiedniego poziomu bezpieczeństwa i integralności, zgłaszania do regulatora istotnych naruszeń, a także obowiązku krajowych regulatorów do przesyłania raportów do Komisji Europejskiej i agencji ENISA

W ramach programu agencji ENISA, zajmującego się odpornością sieci i usług na nieprzewidziane zdarzenia oraz ochroną teleinformatycznej infrastruktury krytycznej, powstały raporty na temat miar odporności infrastruktury oraz ramowych schematów mierzenia parametrów tejże odporności.

"Measurement frameworks and metrics for resilient networks and services" - Challenges and recommendations, 2010

- praca studialna na podstawie badań ankietowych wśród wielu interesariuszy w Europie na temat wyzwań i rekomendacji wartych przeanalizowania, w odniesieniu do odporności infrastruktury krytycznej
- zebrano informacje na temat istniejących praktyk oraz metryk, które posłużyły do stworzenia raportu technicznego (patrz niżej)

"Measurment frameworks and metrics for resilient networks and services" - Technical report, 2010

- raport stanowi próbę stworzenia zintegrowanego źródła wiedzy technicznej na temat metryk, taksonomii i wielu otwartych kwestii w dziedzinie mierzenia rzeczywistej odporności infrastruktury krytycznej
- znajdziemy w raporcie sekcje zawierające definicje kluczowych pojęć, przegląd istniejacych inicjatyw, prac i ram związanych z badaniem odporności sieci,
- zaproponowano dwuwymiarowe podejście do kategoryzacji miar oraz zaprezentowano szereg konkretnych metryk

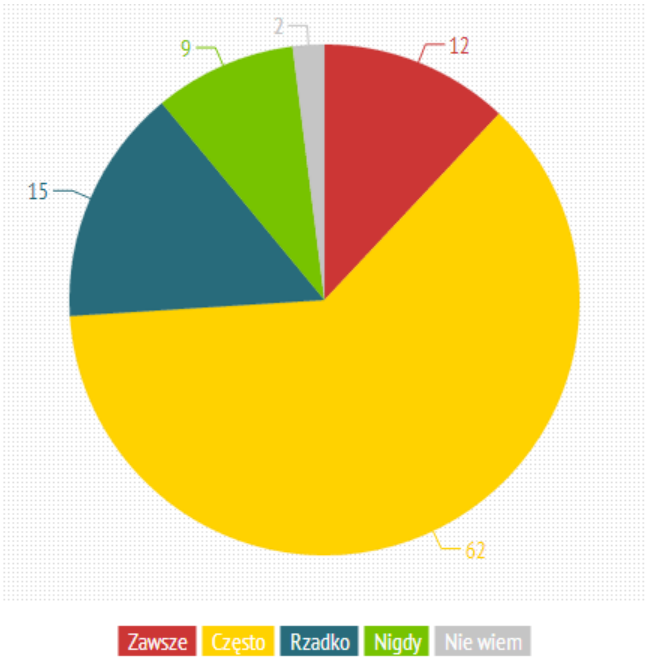
Wszystkie opracowania, które skrótowo zostały zaprezentowane w niniejszym artykule są publicznie dostępne na stronie Europejskiej Agencji Bezpieczeństwa Sieci i Informacji (ENISA) pod adresem: www.enisa.europa.eu, w sekcji „CIIP & Resillience".

BEZPIECZEŃSTWO DANYCH W SIECI INTERNET

Część II – bezpieczeństwo przechowywania haseł

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

Potwierdzanie tożsamości za pomocą loginu oraz hasła jest zdecydowanie najpopularniejszym sposobem uwierzytelniania w serwisach internetowych. Mechanizm ten jest prosty i zrozumiały dla użytkowników oraz łatwy w implementacji. Niestety, coraz częściej pojawiają się informacje o udanych atakach, które doprowadziły do wycieku danych z popularnych portali czy serwisów społecznościowych. W tym krótkim tekście postaram się przybliżyć zagadnienia związane z ochroną haseł przed ich ujawnieniem, po skutecznym pozyskaniu bazy danych użytkowników.



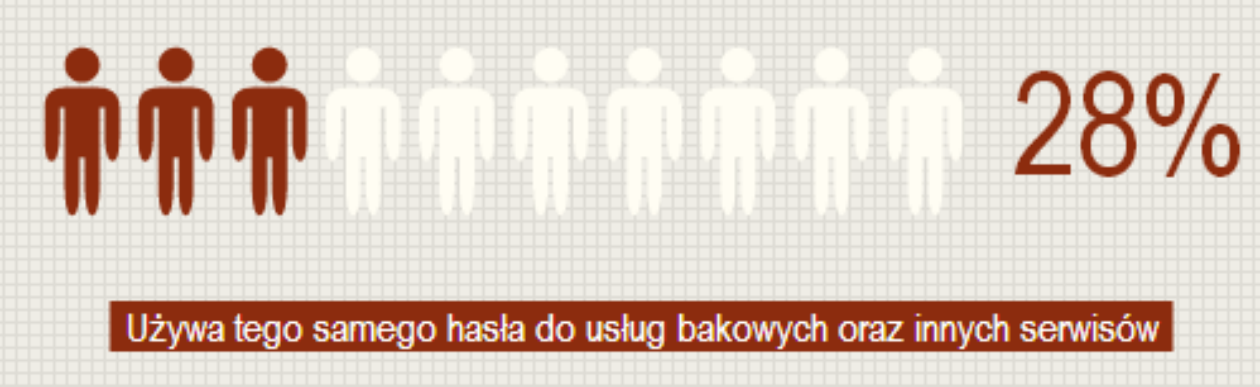
Użycie tego samego hasła w wielu miejscach – NorSIS Password Survey 2012

Dlaczego hasła są cenne?

Podstawowym zagrożeniem dla metody uwierzytelniania opartej na posiadanej wiedzy jest sam człowiek. Wymóg zapamiętania ciągu znaków chroniącego dostęp do określonych zasobów sprawia, że wybierane są te zawierające całe słowa lub kombinację słów oraz cyfr o średniej długości od kilku do kilkunastu znaków.

Zdobycie hasła jest istotne dla przestępców nie tylko dlatego, że daje dostęp do zasobów nim chronionych, ale często otwiera drzwi do innych serwisów lub usług. Jak podają statystyki NorSIS Password Survey 2012 – aż 12% użytkowników zawsze używa tego samego hasła w wielu miejscach za każdym razem, a 62% robi to często. Natomiast według informacji podanych przez APACS Online Banking Survey blisko 3 na 10 użytkowników stosuje to samo hasło do zabezpieczenia usług bankowych oraz innych serwisów.

Może więc dojść do sytuacji, w której atak na system posiadający słabsze zabezpieczenia, ale dużą bazę użytkowników, którzy posiadają takie same konta w innych serwisach (np. aukcyjnych, bankowych) okaże się bardziej opłacalny niż przełamanie zabezpieczeń tych dobrze chronionych zazwyczaj serwisów.

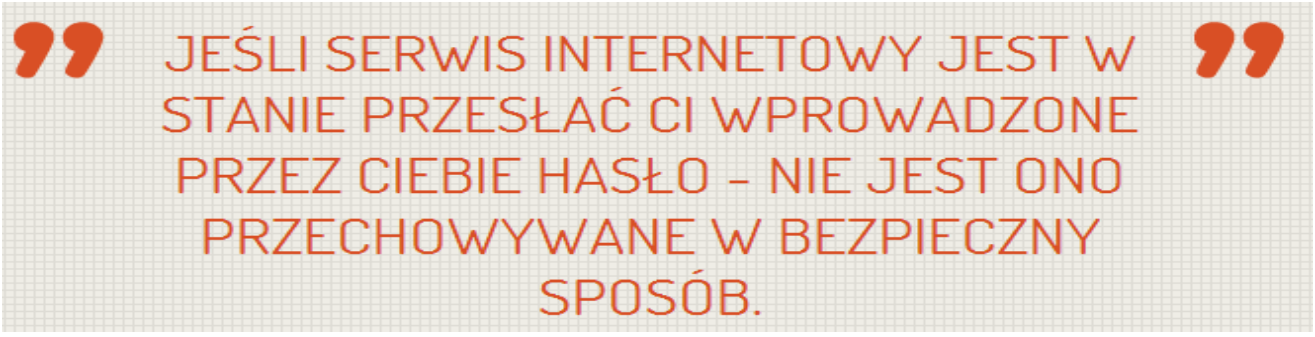


Sposoby przechowywania haseł

Wszystkie hasła muszą być zapisane w taki sposób, aby możliwe było sprawdzenie czy wprowadzona przez użytkownika wartość jest zgodna z tą ustaloną w procesie tworzenia konta. Można to osiągnąć przechowując je na wiele sposobów różniących się od siebie poziomem bezpieczeństwa oraz złożonością obliczeń potrzebną do dokonania takiego porównania, ale wszystkie można przyporządkować do kilku głównych grup.

Najprostszą i zarazem najmniej bezpieczną metodą jest przechowywanie haseł jako zwykły tekst [ang. plain text]. Metoda ta nie wymaga dodatkowych obliczeń przed dokonaniem porównania, jednak w przypadku wycieku bazy danych, wszystkie hasła dostępne są w sposób jawny.

Dużo lepszym sposobem jest przechowywanie ich w postaci zaszyfrowanej. Metoda ta jest bezpieczna, o ile razem z bazą haseł nie wycieknie klucz zastosowany do ich zabezpieczenia oraz został wybrany dobry algorytm szyfrujący, którego przełamanie nie jest opłacalne ze względu na czasochłonność tego procesu



.

Bezpieczeństwo przechowywania danych można osiągnąć za pomocą funkcji haszujących. Pozwalają one na jednokierunkowe przełożenie wprowadzonego tekstu na ciąg znaków, na podstawie którego nie jest możliwe odtworzenie oryginału. Dobra funkcja haszująca to taka, która ma małe prawdopodobieństwo wygenerowania takiego samego wyjścia dla różnych wejść oraz zapewnia, że wyniki dla podobnego testu będą się od siebie różniły w sposób, który nie pozwala na ustalenie wspólnego rdzenia.

Niestety, nawet tak zabezpieczone dane nie są nie-do-złamania. Możliwe jest wygenerowanie odpowiednio dużego zestawu par klucz – skrót, które następnie porównywane są ze zdobytymi zabezpieczonymi hasłami w celu odtworzenia ich pierwotnej formy. Jest to oczywiście zabieg czasochłonny, wymagający zastosowania komputerów o dużej mocy obliczeniowej i przestrzeni dyskowej. Wytworzone w ten sposób bazy nazywają się tęczowymi tablicami [ang. rainbow tables]. W Internecie bez problemu można znaleźć wygenerowane tą metodą zestawy dla popularnych funkcji haszujących (np. MD5, SHA-1), obejmujące swym zasięgiem wszystkie kombinacje znaków alfanumerycznych o długości nawet do 10 znaków.

W związku z tym, stosowane są dodatkowe techniki mające na celu maksymalne wydłużenie procesu przygotowania takich tablic. Podstawową z nich jest zastosowanie tzw. soli. Jest to dodatkowy ciąg znaków, który jest dodawany do hasła wprowadzonego przez użytkownika, w celu jego wydłużenia.

Inna popularną techniką jest key stretching – polega on wielokrotnym obliczaniu hasza za każdym razem używając wyniku poprzedniej operacji. W bezpiecznych algorytmach obie ww. techniki są łączone, co dodatkowo wydłuża proces obliczania wartości wynikowej oraz podnosi bezpieczeństwo.

Błędne koło

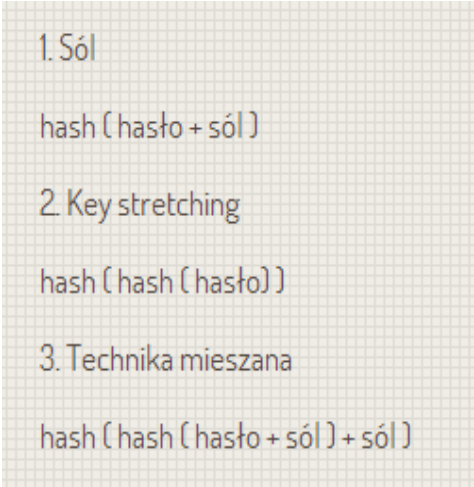
Ataków zakończonych skutecznym pozyskaniem haseł nawet z zabezpieczonej bazy jest obecnie znacznie więcej nie tylko z powodu wzrostu mocy obliczeniowej komputerów, ale również dzięki analizie statystycznej pozyskanych wcześniej danych i obserwacji zachowania użytkowników.

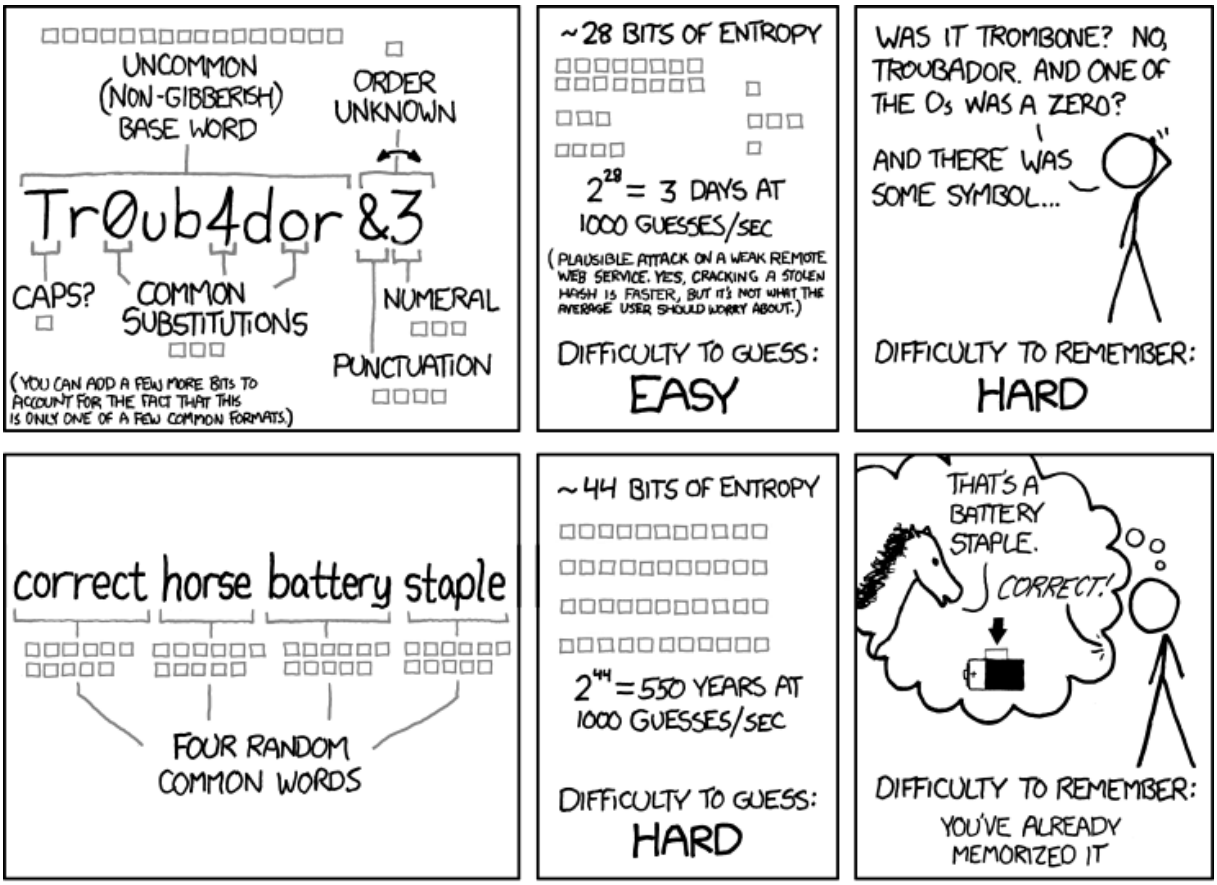
Zauważono, że nie ma sensu generowanie wszystkich kombinacji znaków, gdy dużo większą skuteczność można osiągnąć dobierając dane według określonego wzorca. W tym celu wykorzystywane są przede wszystkim metody słownikowe, które zakładają, że hasła należą do zestawu słów potocznego użycia lub nazw własnych (imiona, nazwiska, nazwy drużyn, firm itp.). Do zasad, które dodatkowo zwiększają prawdopodobieństwo trafienia należą na przykład.:

1. Jeśli w haśle występują cyfry to przeważnie są to 2-4 znaki występujące na jego początku lub końcu.
2. Jeśli w haśle występują znaki specjalne to są to najczęściej znaki „! @ # $" pojawiające się na początku, końcu lub oddzielające od siebie słowa.
3. Jeśli w haśle występują wielkie litery to na początku hasła lub na początku każdego słowa.
4. Często stosowane są hasła w których znaki układają się w ciąg sąsiadujących ze sobą klawiszy na klawiaturze
5. Popularną techniką zwiększania bezpieczeństwa hasła jest zastępowanie liter znakami specjalnymi przypominającymi je kształtem (np. P@ssw0rd)

Zachęcam każdego czytelnika do sprawdzenia, czy stosowane przez niego obecnie hasła pasują do wskazanych powyżej bardzo ogólnych wzorów. W rzeczywistości są one dużo bardziej precyzyjne i pozwalają zmniejszyć pulę generowanych tęczowych tablic o kilka rzędów wielkości przy dużym prawdopodobieństwie trafienia.

Czy jedynym wyjściem z tej sytuacji jest stosowanie skomplikowanych haseł będących przypadkowym zestawem wielkich i małych liter, cyfr oraz znaków specjalnych niezwykle trudnych do zapamiętania? Okazuje się, że nie. Kluczem jest tutaj nadal przede wszystkim długość posiadanego hasła oraz stosowanie nieszablonowych wzorców.





źródło: https://xkcd.com/936/

5 ZASAD BHP

1. *Stosuj różne hasła do wszystkich serwisów z których korzystasz – jeśli nie jesteś w stanie ich zapamiętać opracuj powtarzalną metodę ich tworzenia lub skorzystaj z oprogramowania do zarządzania hasłami.*
2. *Sprawdź czy w serwisach z których korzystasz lub którymi administrujesz hasła przechowywane są w sposób bezpieczny.*
3. *Okresowo zmieniaj swoje hasła, dzięki czemu unikniesz sytuacji, w której ktoś dostanie się do Twojego konta po udanym odszyfrowaniu wykradzionej wcześniej bazy.*
4. *Dbaj o to, żeby Twoje hasła były trudne do odgadnięcia – nie tylko, aby spełniały minima wymagane przy rejestracji.*
5. *Reaguj natychmiast na informacje o wycieku danych z serwisu z którego korzystasz.*