FUNDACJA
bezpieczna
cyberprzestrzeń

NAJWIĘKSZE ZAGROŻENIA DLA BEZPIECZEŃSTWA W INTERNECIE W 2015 ROKU

GŁOS POLSKICH EKSPERTÓW

RAPORT

Spis Treści

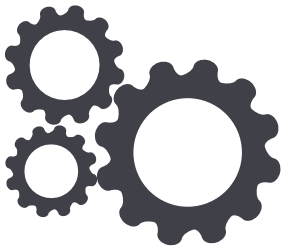
Wstęp

Fundacja Bezpieczna Cyberprzestrzeń już po raz trzeci przygotowała raport o zagrożeniach, jakie czyhają na nas w sieci Internet. Przygotowaliśmy raport, w którym chcemy przedstawić najbardziej prawdopodobne i najbardziej groźne zjawiska w cyberprzestrzeni. Tradycyjnie już, oprócz własnej opinii, uwzględniliśmy w nim opinie wielu specjalistów, z którymi współpracujemy z dziedziny bezpieczeństwa teleinformatycznego z naszego kraju. Niektórzy z nich na co dzień w ramach swoich obowiązków zajmują się również innymi tematami, co naszym zdaniem jeszcze bardziej uwiarygadnia raport dodając do niego spojrzenie z trochę innej, ale ważnej dla oceny zjawisk cyberbezpieczeństwa, perspektywy.

Dzięki odpowiedziom osób zaproszonych do wypełnienia ankiety powstała lista tego, co potencjalnie najgroźniejsze i najbardziej prawdopodobne w roku 2015. W naszych cyklicznych raportach zdecydowaliśmy się na prezentację głosu tylko polskich specjalistów, nadając raportom unikatową wartość.

Każdego roku firmy, żegnając stary rok, robią podsumowania i jednocześnie, wchodząc w nowy, planują budżety i działania strategiczne. Robią to najczęściej na podstawie opracowań i przewidywań własnych lub zewnętrznych. Podobnie jest, jeśli chodzi o branżę cyberbezpieczeństwa. Najważniejsze wydarzenia z tej dziedziny, w roku, który właśnie się skończył, to twarde dowody na to, że mówimy o rzeczach realnych. Natomiast przewidywania znajdujące się w tym raporcie mają nas uczulić na to, co potencjalnie najgroźniejsze. Liczymy na to, że nasz raport okaże się interesujący i pomocny w działaniach na rzecz minimalizacji ryzyka działań w cyberprzestrzeni.

MIROSŁAW MAJ
prezes zarządu
Fundacji Bezpieczna Cyberprzestrzeń

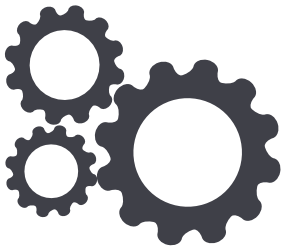


Metodyka

W celu zebrania opinii eksperckich przygotowana została ankieta. Ankieta zawierała zestawienie potencjalnych zagrożeń w 2015 roku. Lista tych zagrożeń powstała na podstawie innych podobnych ankiet oraz naszych własnych opinii co do jej kształtu. Dodatkowo lista mogła być uzupełniona przez propozycje eksperckie, w sytuacji kiedy zdaniem eksperta istotne zagrożenie nie pojawiło się w zestawieniu. Uczestnicy ankiety poproszeni zostali o wyrażenie swoich opinii na temat możliwości wystąpienia danego zagrożenia oraz poziomu niebezpieczeństwa w przypadku jego wystąpienia.

Zestawienie zawierało następujące 24 pozycje:

- Cyberkonflikty pomiędzy państwami powiązane z atakami dedykowanymi
- Zagrożenia zawiązane z BYOD (*Bring Your Own Device*)
- Phishing z wykorzystaniem poczty elektronicznej i serwisów WWW
- Haktywizm
- Powstawanie botnetów opartych o platformy mobilne
- Zagrożenia w serwisach społecznościowych
- Zagrożenia dla platformy Android
- Zagrożenia dla platformy iOS
- Zagrożenia dla platformy Windows Phone/Mobile
- Zagrożenia typu ransomware/scareware
- Wykorzystanie gier sieciowych w atakach
- Wycieki baz danych zawierających dane osobowe, hasła, numery kart kredytowych, itd.
- Ataki drive-by download
- Ataki na cloud-computing
- Zagrożenia związane z "Internet of Things"
- Ataki na platformy hostingowe
- Ataki na system DNS
- Kradzież wirtualnych walut
- Ataki na systemy sterowania przemysłowego (SCADA)
- Ataki DDoS na podmioty komercyjne
- Ataki DDoS na administrację publiczną
- Ataki na urządzenia medyczne
- APT – ataki ukierunkowane na organizacje
- Akcje cyberszpiegowskie na tle politycznym



W badaniu wzięło udział 40 ekspertów reprezentujących sektory:
administracji publicznej, organizacji pozarządowych, energetyczny, finansowy i dostawców.

Odpowiedzi można było nadać wagę poprzez przypisanie punktacji od 1 (waga najmniejsza) do 5 (waga największa)[1]. Ponadto każdy z ekspertów miał możliwość wyrażenia swojej opinii w postaci kilku zdań na temat tego, czego możemy się spodziewać i czego najbardziej obawiać w 2015 roku. Większość z ekspertów zdecydowała się na przedstawienie swojej opinii. Opinie te zawarliśmy w naszym raporcie.

[1] W związku z tak przyjętym wartościowaniem prawdopodobieństwo zdarzenia nie było określane w przedziale jednostkowym [0,1].

Przegląd najważniejszych wydarzeń 2014 roku

Przed przystąpieniem do omówienia zagrożeń, które mogą nas spotkać w roku 2015 roku, warto krótko przypomnieć te najważniejsze z zeszłego roku. Niewątpliwie w 2014 roku rzeczami, które w szczególny sposób wpłynęły na poziom bezpieczeństwa, to poważna luka w bibliotece OpenSSL – **Heartbleed** i luka **Shellshock** w popularnej UNIX-owej powłoce systemowej Bash. Oprócz nich często słyszeliśmy również o sieciowych konfliktach na poziomie międzynarodowym. Kolejny już rok z rzędu słyszeliśmy o poważnych włamaniach do firm i wyciekach danych, a nasze wszechobecne urządzenia mobilne atakowane są jeszcze częściej.

Spójrzmy na najważniejsze wydarzenia w ujęciu chronologicznym.

Pierwszy kwartał 2014 roku minął pod znakiem napięć i nasilenia się **konfliktów w cyberprzestrzeni** między Ukrainą i Rosją czego powodem był oczywiście konflikt między tymi krajami; według ekspertów bezpieczeństwa zarówno Kijów jak i Moskwa uruchamiają różne szkodliwe działania względem siebie.

W ostatnich dniach lutego usłyszeliśmy o **złośliwym programie na Android atakującym mobilne urządzenia w sieci TOR** (*The Onion Router*). To nowość i pierwszy przypadek tego typu – dotychczas sieć TOR nie była wykorzystywana w atakach na urządzenia mobilne. Mieliśmy już wcześniej do czynienia ze szkodliwymi programami pochodzące z tej sieci, jednakże do tej pory atakowały jedynie urządzenia stacjonarne.

Z początkiem kwietnia dowiedzieliśmy się o **Heartbleed.** Heartbleed to medialna nazwa luki bezpieczeństwa (CVE-2014-0160), która umożliwia wykradanie najróżniejszych danych. Podatne na ataki są wersje obecne w wielu dystrybucjach systemu GNU/Linux, co oznacza, że zagrożonych jest wiele usług działających w Internecie, włączając w to serwery WWW oferujące bezpieczne połączenie, sieci anonimizujące czy usługi VPN. Możliwe są również wycieki danych i kradzieże kluczy prywatnych!

Warto również odnotować bardzo ważne inne kwietniowe wydarzenie. W kwietniu 2014 roku miał miejsce **koniec wsparcia dla Windows XP** – jednego z najpowszechniejszych systemów operacyjnych w historii komputerów – uznawanego za jedną z najlepszych wersji systemu operacyjnego Microsoftu. System ten decyzją korporacji z Redmond przestał być aktualizowany.

W końcu maja usłyszeliśmy o bezprecedensowym przykładzie globalnej współpracy i **unieszkodliwieniu botnetu Zeus Gameover**. Akcję tę nazwano „Operacją Tovar". Mieliśmy okazję obserwować międzynarodowe działania podmiotów z 11 państw. Miejmy nadzieję, że taka forma międzynarodowej współpracy to przykład wytyczania nowego standardu w walce z cyberprzestępcami. „Operacja Tovar" pokazała, że do pełnego sukcesu potrzebna jest współpraca zarówno na poziomie państw, instytucji, operatorów telekomunikacyjnych, CERT-ów i innych podmiotów. Konieczne jest też uczestnictwo indywidualnych użytkowników komputerów. Każdy podmiot w sieci, w tym i jej zwykły użytkownik miał swoją rolę do odegrania. Takim przykładom warto się dokładnie przyjrzeć i próbować je przenosić na nasz grunt krajowy, gdzie nie zawsze współpraca wygląda najlepiej.

Na początku lipca firma Symantec opublikowała raport dotyczący **kampanii szpiegostwa komputerowego** wymierzonej w szereg firm, głównie z sektora energetycznego. Atakujący to grupa zwana **Dragonfly.** Agresorom udało się złamać zabezpieczenia wielu organizacji i przeprowadzić operacje szpiegowskie. To kolejny przykład ataku, w którym, gdyby zastosowano sabotaż, to mogłoby dojść do awarii energetycznych. Wśród celów Dragonfly znaleźli się operatorzy sieci energetycznych, duże elektrownie, operatorzy rurociągów naftowych oraz dostawcy sprzętu przemysłowego dla firm z branży energetycznej. Większość ofiar ma swoje siedziby w Stanach Zjednoczonych, Hiszpanii, Francji, Włoszech, Niemczech, Turcji i Polsce.

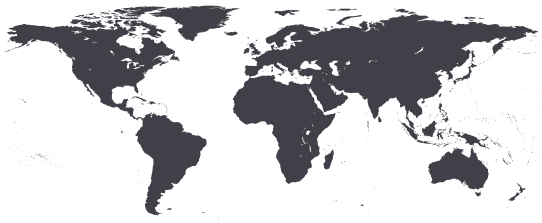
W drugiej połowie września 2014 roku dowiedzieliśmy **Shellshocku** – nowej luce, którą wykryto w popularnej komendzie UNIX-owej – Bash (Bourne Again Shell) – służącej do komunikacji użytkownika z systemem. Pozwala ona na zdalne wykonanie komand w systemie wykorzystującym powłokę Bash. Shellshock polega na błędnym sposobie interpretacji funkcji przypisanych do zmiennych. Zmienna może przybrać wartość, która w praktyce może okazać się komendą do wykonania. Bash zaś „zapomni" o tym, że przetwarza zmienną i, jeśli okaże się ona komendą wykonywalną, to po prostu ją wykona. Błąd jest szczególnie groźny, gdyż w Internecie i w sieciach wewnętrznych wykorzystywanych jest wiele usług używających Basha.

Na przełomie września i października 2014 roku usłyszeliśmy o operacjach cyberszpiegowskich **BlackEnergy i Sandworm (BackEnergy2)**. To kolejny dowód na to, że trwający konflikt na wschodzie Europy po części odbywa się również w cyberprzestrzeni. Tym razem chodziło o złośliwe oprogramowanie, trojana o nazwie BlackEnergy, które skutecznie zaatakowało wiele

organizacji na Ukrainie i w Polsce. Trojan znany jest co prawda co najmniej od 2007 roku, wówczas został przeanalizowany przez specjalistów z Arbor Networks jako złośliwe oprogramowanie wykorzystywane do prowadzenia ataków DdoS. Wykorzystywany był również w roku 2008 w czasie wojny rosyjsko-gruzińskiej do atakowania gruzińskiej infrastruktury teleinformatycznej, co było pierwszym wyraźnym sygnałem użycia BlackEnergy w konflikcie politycznym i skorzystania z niego przez stronę rosyjską. Wśród ofiar ataków były również cele w Polsce. Firma iSight opublikowała raport , w którym opisuje grupę cyberprzestępców, pracującą prawdopodobnie na zlecenie Rosji, która to grupa używa w swoich atakach błędu typu 0-day, na który podatne były wszystkie wspierane wersje Windows. Przypisanie grupie rosyjskiego pochodzenia wynika z dwóch powodów: użycia języka rosyjskiego w plikach konfiguracyjnych oraz doboru ofiar. Według iSight za atakami stoi kilka powiązanych grup szpiegowskich. Jedna z tych grup została nazwana „Sandworm" – po polsku czerw pustyni.

W październiku dowiedzieliśmy się o **APT28 – długoterminowej kampanii cyberszpiegowskiej**, o której raport przygotowała firma FireEye. Z raportu wynika, że prawdopodobnie stoi za nią grupa rosyjskich cyberprzestępców, nazwana przez FireEye – APT28. W kodzie ponownie znaleziono ślady wskazujące na Rosjan, m.in. szczątkowe rosyjskie komentarze. Działania APT28 skierowane były m.in. na organizacje w Gruzji, Europie Wschodniej, członków NATO i OBWE . Wśród celów znalazła się ponownie Polska. Musimy się przyzwyczaić, że nasz kraj pojawia się systematycznie na liście celów cyberataków.

Wydarzenia z grudnia 2014 roku mamy jeszcze wszyscy świeżo w pamięci. Związane były przede wszystkim z **cyberatakami na Sony Pictures Entertainment.** Nie wiadomo co było ich przyczyną. Medialnie króluje wskazywanie na produkcję filmową „The Interview", w której w negatywnym świetle jest przedstawiony przywódca północnokoreański. Dlatego powszechnie przyjmuje się, że to właśnie Korea Północna stoi za atakami na Sony, choć jednoznacznych i przekonywujących dowodów na to brak. Jak zresztą często w przypadku cyberataków. W trakcie ataków na firmę upublicznione zostały skradzione z Sony filmy, scenariusze do nowych projektów, poufne dane o opiece zdrowotnej pracowników firmy, a także wewnętrzna korespondencja. Na szczęście groźby ataków terrorystycznych podczas premiery filmu "The Interview" się nie sprawdziły.



Najwieksze zagrożenia w roku 2015 – prawdopodobieństwo wystąpienia

Zestaw, jaki zaproponowaliśmy do oceny, bazuje na pozycjach z lat ubiegłych. Został on jednak poszerzony o pozycje, które najczęściej pojawiają się w dyskusji na temat tegorocznych zagrożeń, oraz o wcześniejsze propozycje zgłaszane przez zaproszonych do badania ekspertów. Większość kategorii wydaje się dość oczywista. Spójrzmy najpierw na wyniki dotyczące odpowiedzi na pytanie o te zagrożenia, które będą w dopiero co rozpoczętym roku najbardziej prawdopodobne.

Prawdopodobieństwo zagrożenia w przypadku wystąpienia podanego poniżej zagrożenia. Skala 1-5 (1 - najmniej prawdopodobne, 5 - najbardziej prawdopodobne).

Na czoło klasyfikacji wybijają się trzy kategorie[2] :

- Phishing z wykorzystaniem poczty elektronicznej i serwisów WWW – **4,67**
- Ataki DDoS na podmioty komercyjne – **4,28**
- Zagrożenia dla platformy Android – **4,28**

Jak widać z tego zestawienia – zagrożenie, które jest wręcz klasyczne od wielu lat, czyli akcje phishingowe z wykorzystaniem poczty elektronicznej i serwisów WWW – wygrywa konkurencję. Podobnie zresztą było w roku ubiegłym, choć wartość tego prawdopodobieństwa była niższa (**4,39**). Ta opinia ekspertów to potwierdzenie kontynuacji tego trendu, który jest już bardzo długi. Jak widać, nie ma oczekiwania, że wiele się tutaj zmieni. Mamy do czynienia z zagrożeniem, które jest bardzo systematyczne i dodatkowo trudne do wyeliminowania. U jego podłoża stoją dwa elementy – ciągłe występowanie słabości systemowych najpopularniejszych systemów operacyjnych i aplikacji oraz niski poziom świadomości użytkownika, który oprócz łatwego ulegania socjotechnikom, dodatkowo nie aktualizuje swoich systemów co w konsekwencji prowadzi do infekcji kompuerowych.

Zagrożenia związane z systemem operacyjnym Android to ex-aequo druga pozycja wśród liderów najbardziej prawdopodobnych zagrożeń. I ta opinia nie dziwi. Według wielu statystyk liczba infekcji telefonów komórkowych przyrasta wręcz lawinowo. Infekcje Androida to w różnych statystykach minimum 90% wszystkich infekcji na platformy mobilne. Pozostałe platformy z naszego zestawienia – t.j. iOS i Windows Phone/Mobile nie są postrzegane jako aż tak niebezpieczne. Trend związany z niepokojem dotyczącym platformy Android utrzymuje się. W zeszłorocznym zestawieniu była to pozycja nr 3. Na razie nie widać przesłanek do zmiany tego stanu. Pozostaje mieć nadzieję, że uczestnicy zaczną bardziej dbać o swoje telefony, przede wszystkim aktualizując posiadaną wersję Androida. Być może również poprawi się wykrywalność zainfekowanych aplikacji dostępnych w Google Market i w ogóle w Internecie oraz skuteczne powiadamianie o nich.

[2] wszystkie wartości oceny odnoszą się do skali 1-5 (1 – najmniejsze prawdopodobieństwo, 5 – największe prawdopodobieństwo).

Tomasz Pietrzyk
Manager Systems Engineering Eastern Europe
FireEye

Tempo i trendy zmian cyberzagrożeń, z jakimi mają na co dzień do czynienia firmy i instytucje, wymusi wdrażanie dedykowanych zespołów i procesów reakcji na zagrożenia. Coraz większego znaczenia nabiorą centra SOC, w tym SOC prowadzone przez specjalizowane firmy. Widoczne będzie mniejsze zainteresowanie rozwiązaniami SIEM, które niestety nie spełniają pokładanych nadziei i nie zapewniają zwrotu z niemałych inwestycji na ich wdrożenie i utrzymanie w kontekście ochrony przed zaawansowanymi atakami.

Adam Haertle
Kierownik ds. Bezpieczeństwa
UPC Polska sp. z o.o.

Nie sądzę, by nadchodzący rok miał przynieść radykalne zmiany w zakresie występowania poszczególnych rodzajów zagrożeń oraz ich skutków. Spodziewam się raczej ciągłego rozwoju ataków skierowanych na pozyskanie wartościowych informacji zarówno w organizacjach komercyjnych jak i rządowych. Z punktu widzenia technologii ataków zapewne niewiele się zmieni, jednak wobec coraz większej powszechności mechanizmów obronnych atakujący będą rozwijać metody przekonywania ofiar do nieświadomej pomocy w procesie infekcji.

Przemysław Dęba
Dyrektor Bezpieczeństwa Systemów Teleinfomratycznych
Orange Polska

Już w tym roku widać było, jak wiele ciekawych danych - prywatnych, firmowych i instytucjonalnych znajduje się w zasobach serwisów chmurowych i jak łatwo wyciekają. Ten trend będzie rósł, chmury przyrastają do systemów operacyjnych w sposób nierozpoznawalny dla użytkowników, znacznie powiększaja się darmowe przestrzenie, a w ślad za tym nie idzie edukacja i środki ochrony. W 2015 roku niejednego się zatem dowiemy.

Taką samą ocenę jak ataki na Android uzyskała pozycja ataki DDoS na podmioty komercyjne. To nowa pozycja w naszym rankingu, która została do niego dodana na prośbe uczestników badania. Zapewne przyczyną tego postulatu są powszechne w tej chwili w naszym kraju ataki DDoS, które stały się chlebem powszednim wielu organizacji komercyjnych. Prawdopodobieństwo ataków na podmioty administracji państwowej zostało ocenione nieco niżej – **4,1**. Z punktu możliwości wyelimnowania ataki DDoS stanowią raczej trudną pozycję. Walka z nimi polega przede wszystkim na skutecznej reakcji a nie prewencji, gdyż na tę drugą wpływ zainteresowanych w ich ograniczeniu jest raczej niewielki.

Na drugim biegunie rankingu prawdopodobieństwa zagrożeń mamy dwie pozycje, które w punktacji nie przekroczyły wartości 3 punktów. Są to począwszy od najniżej notowanych:

- Ataki na urządzenia medyczne – **2,45**
- Wykorzystanie gier sieciowych w atakach – **2,98**

Ataki na urządzenia medyczne nadal dla zaproszonych do badania wydają się mało prawdopodobne. Rzeczywiście większość problemów związanych z cyberzagrożeniami w służbie zdrowia nadal przede wszystkim dotyczy wycieku danych pacjentów. Chociaż o skali tego zjawiska w przypadku Polski i w ogóle Europy możemy jedynie spekulować ze względu na brak prawodawstwa związanego z obowiązkiem informowania o takich zdarzeniach. Co różni nasz kontynent na przykład od Stanów Zjednoczonych. Niezależnie od tego nie oznacza to jednak, że problem cyberbezpieczeństwa w sektorze służby zdrowia nadal ograniczony będzie przede wszystkim do wycieku danych. Są przesłanki mówiące o tym, że może się to zmienić. Na przykład ostatnio sprawę możliwych cyberataków na urządzenia medyczne badał amerykański Departament Stanu i tamtejszy CERT dedykowany dla sektora infrastruktury krytycznej[3].

Druga z pozycji najmniej prawdopodobnych to wykorzystanie gier sieciowych w atakach. Jak widać, nadal gry sieciowe postrzegane są jako oaza względnego spokoju. Jednak częstsze informacje o kradzieży zasobów wirtualnych w GVE czy przejmowaniu w tych środowiskach komputerów grających mogą pojawić się w każdym momencie.

[3] http://www.reuters.com/article/2014/10/22/us-cybersecurity-medicaldevices-insight-idUSKCN0IB-0DQ20141022

Piotr Konieczny
Chief Information Security Officer
Niebezpiecznik

Nie wątpię, że w 2015 roku będziemy świadkami wielu widowiskowych ataków. Samochody, urządzenia medyczne, lodówki i inne do tej pory niepodpinane do internetu maszyny na pewno staną się celem ataków, zwłaszcza, że sporo z tych rozwiązań działa w środowisku utrudniającym aplikowanie regularnych aktualizacji i pracuje w oparciu o przestarzałe systemy operacyjne. Nie jestem tylko pewien, czy np. podmiana obrazka na wyświetlaczu multimedialnym w samolocie, jakkolwiek widowiskowa, rzeczywiście będzie niosła jakiekolwiek realne ryzyko dla pasażerów (w końcu to osobny system multimedialny) albo czy podniesienie temperatury w „zhackowanej" lodówce spowoduje znaczne straty finansowe... Dlatego moim zdaniem dalej bardziej powinniśmy się obawiać tego, że ktoś z naszych domowników złapie się na klasyczny phishing lub otworzy zainfekowany załącznik, w wyniku czego znikną mu środki z rachunku bankowego.

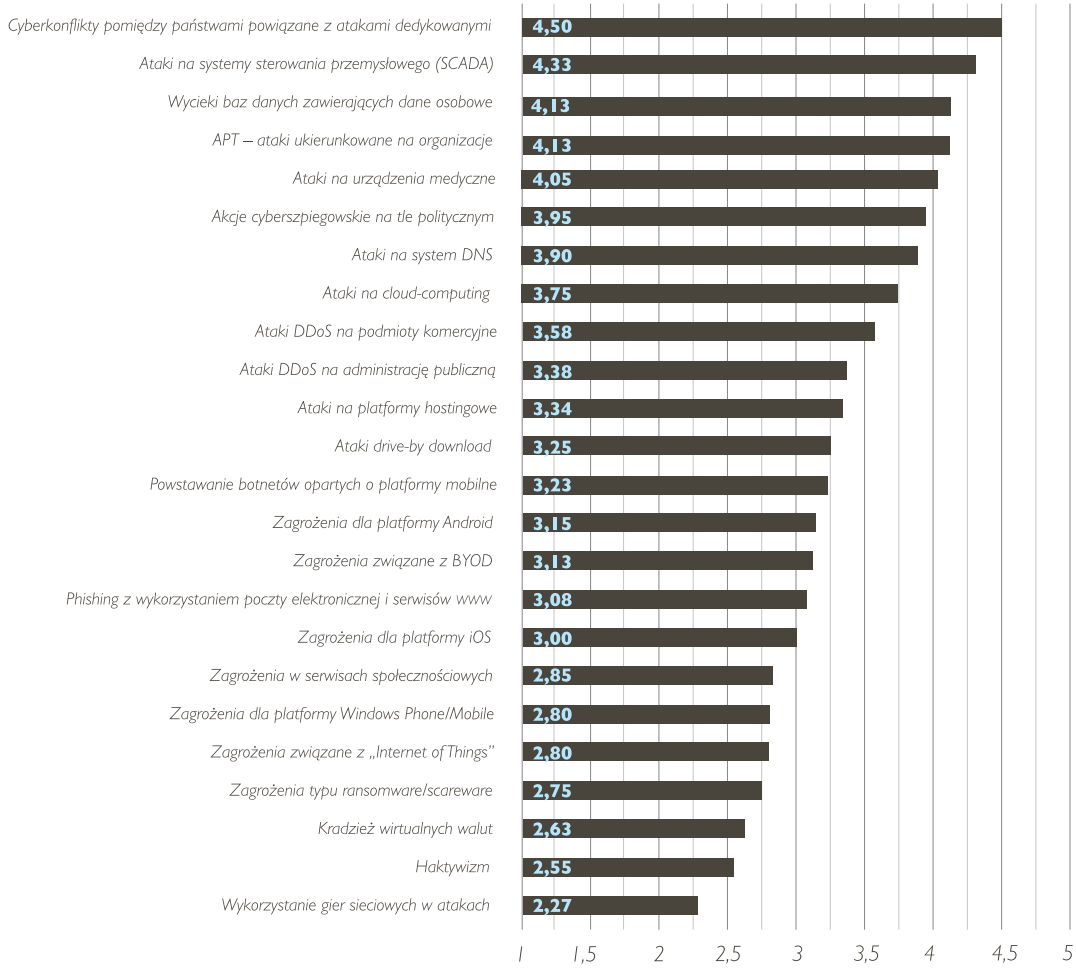
Mirosław Maj
CEO / CIO
Fundacja Bezpieczna Cyberprzestrzeń / ComCERT.PL

W mojej ocenie nadchodzący rok będzie czasem coraz większej liczby działań w cyberprzestrzeni, które będą towarzyszyły konfliktom i napięciom politycznym. Działania haktywistów, które miały głównie wydźwięk propagandowy, wypierane będą przez zorganizowane na poziomie rządów państw działania cyberszpiegowskie o poważnych konsekwencjach. Jeśli miałbym obstawiać jakikolwiek nowy trend to zwróciłbym uwagę na możliwość wystąpienia ataków na systemy wykorzystywane w służbie zdrowia. Być może pojawią się również ataki na „Internet of Things", które mogą być na tyle atrakcyjne w przekazie, że zwrócą większa uwagę na rosnące ryzyko przy rozwijaniu tej technologii.

Największe zagrożenia w roku 2015 roku – poziom zagrożenia

Prawdopodobieństwo wystąpienia to jedno, ale siła oddziaływania danego zagrożenia to drugie. Nie wszystkie zagrożenia wskazywane jako najbardziej prawdopodobne jednocześnie wskazywane były jako te, których konsekwencje wystąpienia byłyby najbardziej dokuczliwe i najgroźniejsze.

Poziom zagrożenia w przypadku wystąpienia podanego poniżej zagrożenia.
Skala 1-5 (1 - najmniej groźne, 5 - najbardziej groźne).



Wśród tych, które są najgroźniejsze pięć zagrożeń osiągnęło wartość co najmniej 4,0. Są to następujące zagrożenia:

- Cyberkonflikty pomiędzy państwami powiązane z atakami dedykowanymi – **4,50**
- Ataki na systemy sterowania przemysłowego (SCADA) – **4,33**
- Wycieki baz danych zawierające dane osobowe – **4,13**
- Ataki ukierunkowane na organizacje (APT) – **4,13**
- Ataki na urządzenia medyczne – **4,05**

Żadna z tych pozycji nie dziwi. Wszystkie odnoszą się albo do ataków na infrastrukturę krytyczną albo dotyczą tego co eksperci z dziedziny cyberbezpieczeństwa w większości przypadków bardzo cenią – czyli zachowanie prywatności.

Z rankingu wyraźnie widać, że wydarzenia ubiegłego roku, w szczególności jego drugiej połowy, czyli pojawienie się zagrożeń związanych z takimi terminami jak Dragonfly, BlackEnergy, Sandworm, APT28 czy atak na Sony, pobudziło wyobraźnie dotyczącą skutków takich ataków. W wielu przypadkach wymienione ataki powodowały realne i poważne straty. Nie ma wątpliwości, że wszystkie były bardzo groźne. Dodatkowo, o czym pisaliśmy we wstępie do raportu, nasz kraj systematycznie zaczął się pojawiać w informacjach dotyczących najgroźniejszych ataków. Konflikt za wschodnią granicą, w którym jesteśmy postrzegani jako wyraźny sprzymierzeniec strony ukraińskiej, że przeprowadzający cyberataki towarzyszące wojnie rosyjsko-ukraińskiej, na swoim celowniku mają również podmioty polskie – zarówno komercyjne jak i podmioty polskiej administracji państwowej. To również uzmysławia w większym stopniu poziom zagrożenia związany z tego typu atakami.

Na dole rankingu zagrożeń o największych konsekwencjach znajdują się:

- Wykorzystanie gier sieciowych – **2,27**
- Haktywizm – **2,55**
- Kradzież wirtualnych walut – **2,63**

Ta niska ocena to zapewne wynik braku bardzo negatywnych doświadczeń z konsekwencjami w przypadku zagrożeń związanych z grami sieciowymi czy haktywizmem. Zresztą obydwie pozycje zostały ocenione jako

Sławomir Górniak
Ekspert
ENISA

Adekwatne reagowanie na cyber zagrożenia w zmieniającym się środowisku nie jest celem, ale raczej podróżą, która być może nigdy się nie skończy. Wyścig w cyberprzestrzeni pomiędzy napastnikami a obrońcami się wciąż toczy i będzie toczył. Niestety, w tej chwili napastnicy są o krok do przodu. W tym wyścigu nie jest możliwe dorównanie przeciwnikom, nie rozumiejąc ich metod ataku. Dlatego zrozumienie zagrożeń jest istotnym elementem do ochrony cyberprzestrzeni. Nie przewiduję rewolucji w zagrożeniach w 2015 roku - raczej ich ewolucję. Po szczegóły, zachęcam do konsultacji opracowania agencji ENISA „Threat Landscape 2014".

Maciej Kołodziej
Konsultant, Administrator Bezpieczeństwa Informacji
FHU MatSoft, NK.pl

Mimo wzrastającego poziomu świadomości użytkowników i administratorów systemów informacyjnych w kwestiach ochrony i bezpieczeństwa informacji, moim zdaniem największym problemem wydaje się beztroska oraz nieprzestrzeganie elementarnych zasad ochrony i niestosowanie zabezpieczeń. Większość problemów i strat powodują drobne incydenty, zaniedbania użytkowników i braki inwestycyjne niż masowe ataki na systemy IT. Dlatego oprócz ochrony przed atakami rok 2015 powinien być rokiem edukacji w cyberprzestrzeni.

najmniej groźne również w roku ubiegłym. Pierwsze chyba nadal kojarzone są ze stratami wirtualnymi, natomiast drugie z prestiżem. Dodatkowo wśród ekspertów niska ocena zagrożeń związanych z haktywizmem może być reakcją na przypisywanie tym zagrożeniom zbyt wielkiej wagi poprzez media szukające sensacji, w sytuacjach, kiedy nie odróżnia się zagrożenia związanego ze zmianą witryny internetowej od sytuacji, kiedy z poważnych serwerów kradnie się poważne dane. W rzeczywistości straty związane z utratą wizerunku mogą być bardzo dotkliwe, w szczególności w budowaniu wizerunku państwa zdolnego do ochrony przed atakami z cyberprzestrzeni.

Nową pozycją w zestawieniu jest kradzież wirtualnych walut, która, jak widać, na razie nie wzbudza wielu emocji wśród kspertów. Oprócz poziomu zagrożenia związanego z obrotem wirutalnymi walutami również nisko zostało wycenione samo prawdopodobieństwo występowania takiego zjawiska (**3,38**). Trochę dziwi ten fakt, gdyż w internetowych mediach dość często wspominane są takie przypadki. Być może odpowiadający na pytania ocenili to zagrożenie nadal jako marginalne i przeprowadzane na niewielką skalę, a doniesienia medialne – jako przejaw zainteresowania atrakcyjnym tmatem.

Borys Łącki
Pentester **LogicalTrust**

W 2015 roku firmy będą kontynuowały nowe podejście do kwestii bezpieczeństwa, w którym nie tylko należy nastawić się na obronę przed atakiem ale należy nauczyć się całościowo obsługiwać, szybko zwiększającą się liczbę incydentów. Szerokie spojrzenie na problem z wielu stron, zarówno formalnej, jak i technicznej pozwoli na szybsze zdiagnozowanie źródła ataku, oszacowanie strat i przygotowanie środków zaradczych ograniczających straty finansowe i wizerunkowe. Atakujący będą natomiast coraz częściej publikowali nie tylko dane Klientów okradanych firm ale także dokumenty związane bezpośrednio z działalnością firmy jak wszelkie zestawienia finansowe, informacje o patentach i inne wrażliwe dane firmowe. Klienci indywidualni będą jeszcze częściej atakowani przez cyberprzestępców, celem wymuszenia okupu po kradzieży lub zaszyfrowaniu wrażliwych danych (dokumenty, zdjęcia, itp.), ze szczególnym uwzględnieniem platform mobilnych.

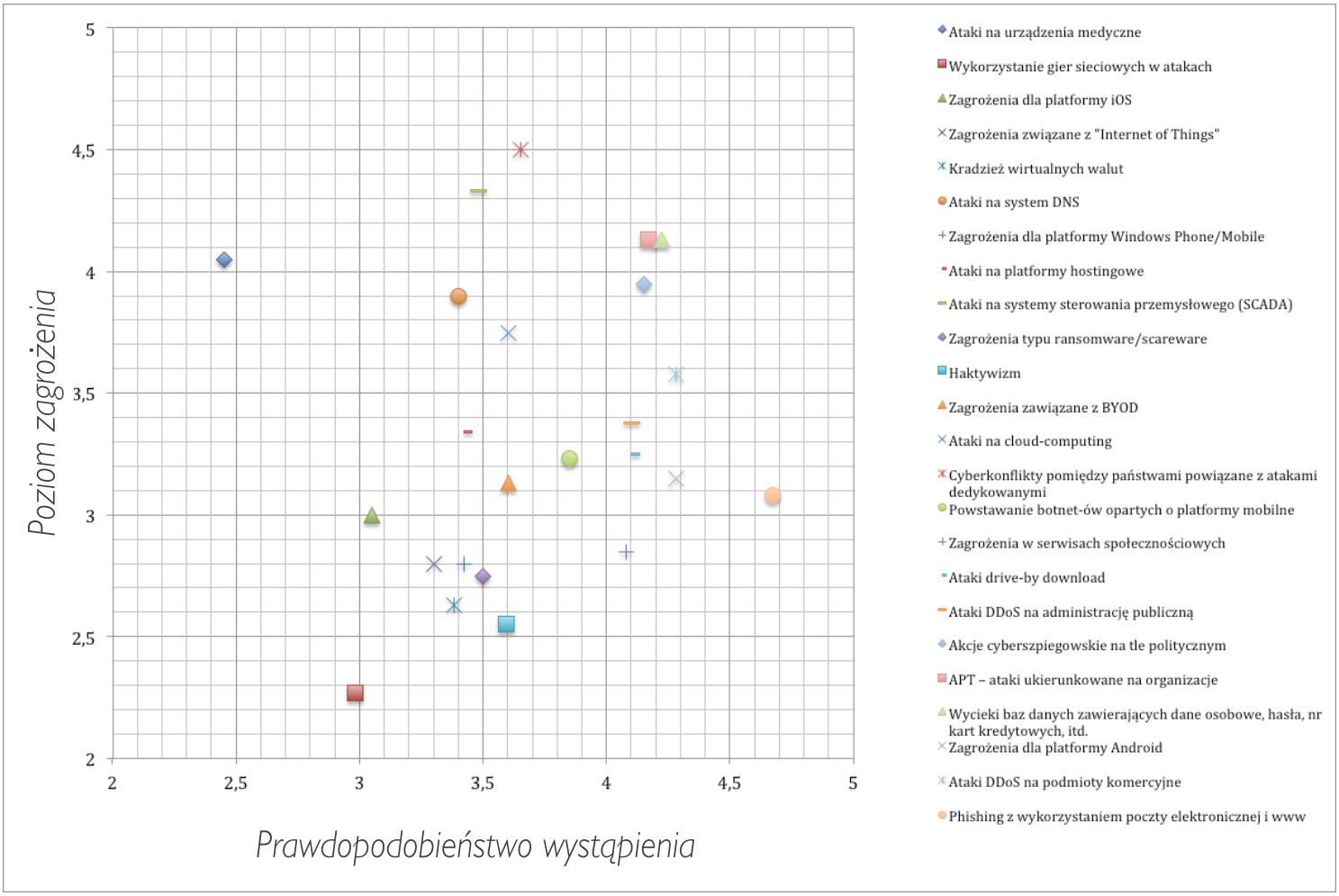
Maciej Łopaciński
Wiceprezes **Agora TC**

W 2014 roku nasiliły się tendencje do bałkanizacji internetu. Zagrożeniem dla dostępu do usług i treści w internecie w coraz większym stopniu są prawnicy i politycy. W marcu obywatele Turcji stracili dostęp do serwisów społecznościowych. W maju ETS nakazał firmie Google modyfikowanie wyników wyszukiwania informacji o osobach i prezentowanie obywatelom UE ocenzurowanych wyników wyszukiwania. Działania europejskich urzędów antymonopolowych, są za oceanem oceniane jako naruszenie pierwszej poprawki do konstytucji gwarantującej swobodę wypowiedzi. Roskomnadzor grozi portalom blokadą dostępu do nich, jeśli nie usuną treści niezgodnych z linią polityczną rządu FR. Internet utracił jedną ze swoich fundamentalnych cech - zapewnienia równego dostępu do wiarygodnej informacji.

Na co więc zwrócić najbardziej uwagę?

Podejście które zaproponowaliśmy w naszym badaniu, tj. ocena zarówno prawdopodobieństwa powszechnego wystąpienia zagrożeń jak i ocena ewentualnych skutków jego zajścia, pozwoliło nam na stworzenie prostej analizy ryzyka zagrożeń w 2015 roku. Zgodnie z prostą metodyką analizy ryzyka, najgroźniejsze są te zagrożenia których prawdopodobieństwo wystąpienia jest duże a spowodowane straty poważne.

Zagrożenia teleinformatyczne 2015 roku.



Warto więc najuważniej się przyjrzeć właśnie tym zagrożeniom, które na wykresie znalazły się w prawym, górnym rogu[4].

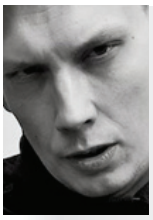
Wśród nich znajdują się takie jak:

- Wycieki baz danych zawierających dane osobowe, hasła, numery kart kredytowych, itd. (**4,22**; **4,13**)
- APT – ataki ukierunkowane na organizacje (**4,17**; **4,13**)
- Akcje cyberszpiegowskie na tle politycznym (**4,15**; **3,95**)
- Cyberkonflikty pomiędzy państwami powiązane z atakami dedykowanymi (np: Stuxnet) (**3,65**; **4,5**)
- Ataki DDoS na podmioty komercyjne (**4,28**; **3,58**)

To tylko bardzo uproszczona analiza ryzka. Każdy sam w zależności od charakteru podmiotu, jaki reprezentuje, i środowiska teleinformatycznego, w jakim działa, powinien takową analizę przeprowadzić na swój użytek. Mamy nadzieję, że dane z naszego raportu mogą być w jakimś stopniu przydatne przy tego typu analizach.

Maciej Miłostan
Analityk Bezpieczeństwa
PCSS

Krajobraz zagrożeń będzie oczywiście w dużej mierze zależny od tego jakie nowe podatności zostaną zidentyfikowane i w jaki sposób upublicznione. W roku 2015 będziemy prawdopodobnie świadkami prób wykorzystywania podatności w protokołach i bibliotekach kryptograficznych, co może prowadzić do nielegalnego pozyskiwania wrażliwych danych. Poważnym zagrożeniem dla właścicieli stron internetowych będzie, podobnie jak w minionym roku, aktywność botów skanujących sieć i poszukujących hostów z podatnymi systemami zarządzania treścią (CMS).



Paweł Wilk
Szef Think Tanku
BAD[SECTOR].PL

Rok 2015 będzie czasem kolejnych żniw szkodników mobilnych, których bezpieczeństwo użytkownicy zaniedbują. W mainstreamowych mediach usłyszymy być może o zagrożeniach związanych z Internet of Things i o tym, że BitCoin nie jest w istocie walutą anonimową. W środowiskach haktywistów przewiduję wzrost zainteresowania sieciami typu mesh i inteligentnymi kryptowalutami, a także poszukiwanie alternatyw dla kluczy RSA.

Adam Danieluk
ISSA Polska

Ostanie problemy z SSL/TLS pokazują jak bardzo obecny biznes jest uzależniony od szyfrowania i Internetu. W konsekwencji skuteczny atak na systemy szyfrowania będzie skutkował zmianą obecnego świata i sposobu w jaki działa biznes. Jeszcze w zeszłym roku nikt się nad takim ryzykiem poważnie nie zastanawiał. Obecnie po wykryciu szeregu podatności na SSL i ostatnio na TLS należy poważnie ocenić ryzyko kompromitacji wszystkich systemów kryptograficznych. W konsekwencji również działań jakie możemy podjąć aby chronić się przed tym zagrożeniem.

[3] dla przejrzystości wykresu skala osi X i osi Y została zawężona tak, aby obejmowała tylko rzeczywiście występujące wartości.

Inne możliwe zagrożenia w 2015 roku.

Eksperci, którzy wzięli udział w naszym badaniu, oprócz wskazanych zagrożeń w zestawieniu, zaproponowali również własne. Wśród nich najczęściej pojawiają się trzy: ataki na systemy bankowości internetowej, różnego rodzaju ataki na końcowych użytkowników oraz ataki na kryptografię.

Poniżej zamieszczamy wszystkie propozycje i opinie uczestników badania w ich oryginalnej formie. Niektóre z propozycji można by zakwalifikować do już istniejących kategorii. Niektóre rzeczywiście są zupełną nowością. Warto prześledzić tę listę, może ona być inspirująca we własnych rozważaniach na temat trendów związanych z cyberzagrożeniami w roku 2015.

Propozycje zagrożeń przedstawione przez uczestników badania:

- Dedykowane ataki na bankowość internetową
- Personalizowane ataki na klientów bankowości elektronicznej (w szczególności klientów zamożnych lub korporacyjnych)
- Ataki na kluczowe elementy systemu finansowego
- Ataki socjotechniczne na organizacje
- Ataki socjotechniczne (bardziej wysublimowane niż tylko phishing)
- Ataki z wykorzystaniem starych, klasycznych, ale niezałatanych podatności
- Nieprzestrzeganie aktualnego prawa jako zagrożenie dla biznesu
- Dług technologiczny narzędzi security
- Spear phishing
- Nowe podatności w bibliotekach i protokołach kryptograficznych
- Bezpieczeństwo protokołów kryptograficznych
- Ataki na kryptosystemy
- Ataki na stacje robocze
- Bezpieczeństwo systemów korzystających z implementacji open source, która nie jest dostatecznie testowana (open ssl ->

Cezary Piekarski
Senior Manager
Deloitte

W 2014 roku wiele teoretycznych zdarzeń, których obawiali się eksperci stało się rzeczywistością. Włamania o dużej skali, skuteczne ataki na instytucje finansowe w Polsce, udane „lokalne" kampanie phishing/malware dotykające instytucje, które do tej pory nie cieszyły się zainteresowaniem przestępców. Przedsiębiorstwa ze szczególnym uwzględnieniem firm z sektora bankowego zaczynają odczuwać realne koszty finansowe związane z incydentami bezpieczeństwa teleinformatycznego, a zagadnienia cyber-security stały się tematem intensywnych rozmów (i działań) wyższej kadry kierowniczej. 2015 rok zintensyfikuje te trendy – zobaczymy coraz więcej coraz bardziej spektakularnych ataków w tym ataków na polskie banki i ich klientów. Możemy spodziewać się również ataków motywowanych politycznie – w tym ataków na polską infrastrukturę krytyczną.

Marek Kołodziejski
Dyrektor Biura Bezpieczeństwa
TK Telekom spółka z o.o.

Względy ekonomiczne powodują, że firmy zaczęły akceptować rozwiązania BYOD. W odróżnieniu od kontrolowanego dostępu via VLAN przy użyciu sprzętu pracodawcy, stwarza to coraz większą lukę w zabezpieczeniach teleinformatycznych i fizycznych. Ponadto uniemożliwia to praktycznie działania prawne w tym zakresie w relacji przedsiebiorca - pracownik. Drugie duże zagrożenie wynikające z przyczyn ekonomicznych to usługa clud-computing. Poza „chmurami" typowo korporacyjnymi, tworzonymi na ich własne potrzeby, nie sposób zweryfikować rzeczywitego poziomu zabezpieczeń.

- Zwiększająca się ilość podatności tzw. serwerowych, tzn. dająca możliwość zdalnego wykonania kodu bez ingerencji użytkowników
- Brak jednolitego systemu powiadamiania o podatnościach. Pomimo pozornego przestrzegania reguł responsible disclosure w przypadku heartbleed i shellshock, wiele systemów było ciągle podatnych.
- Wycieki danych związanych z administracją publiczną
- Anonimowe płatności (nie tylko kryptowaluty)
- Ataki na płatności mobilne
- Niekompetencja administratorów
- Zaawansowane ataki na platformę Apple Mac OS
- Ataki na systemy POS (oparte na Windows i Linux)
- Wzrost ilości podatności ogłaszanych w systemach Unix/Linux
- Ataki ransomware (w stylu cryptolocker) na urządzenia mobilne
- Koordynowane ataki na PC i mobile obniżające wartość popularnej dwuskładnikowej autentykacji
- Ataki wymierzone w modele zaufania (np. X.509)
- Ataki sybilla wymierzone w sieć Tor
- Ataki badusb i inne wymierzone w firmware
- Ataki legislacyjne wymierzone w prywatność internautów
- Nadużycia wewnętrzne (nielegalny dostęp do danych)
- Kradzież danych przez użytkowników uprzywilejowanych
- Przejęcie witryn web do dystrybucji malware (tworzenie watering-hole)
- Bezprzewodowe połączenia sieci
- Płatności mobilne
- Ataki na zabezpieczenia kodów źródłowych
- Wewnętrzne ataki DoS (przez pracowników)
- Akcje cyberszpiegwskie na tle gospodarczym (np. ukryty kod w urządzeniach)

Propozycje przekazane przez ekspertów to naszym zdaniem bardzo ciekawe przewidywania. Być może wśród nich warto szukać tego, co w 2015 roku zaskoczy najbardziej. Jak wiadomo te największe zagrożenia w przeszłości były zazwyczaj niespodziankami dla Internautów i większości specjalistów.

Zbigniew Świerczyński
Adiunkt n-d
Wydział Cybernetyki WAT

Patrząc na zagrożenia płynące z cyberprzestrzeni można zauważyć coraz większą świadomość nie tylko samych zagrożeń, ale również konieczności pozyskiwania wiedzy i umiejętności praktycznych w zakresie reagowania na tego typu zdarzenia. Efektem osiągnięcia tego poziomu świadomości jest coraz większe zainteresowanie, również w Polsce, uczestniczeniem i organizowaniem praktycznych, wielowątkowych ćwiczeń z współdziałania i obrony w cyberprzestrzeni oraz tworzeniem symulatorów wspomagających tę formę edukacji. Gorąco (i również aktywnie) popieram ten kierunek uważając, że w przypadku odpierania zmasowanych, różnorodnych ataków cybernetycznych konieczna jest sprawna/skuteczna współpraca ekspertów z różnych obszarów bezpieczeństwa IT i nie tylko.

Tomasz Przybylski
Fundacja Bezpieczna Cyberprzestrzeń

W niedalekiej przyszłości przyjdzie nam zmierzyć się z wieloma niebezpieczeństwami związanymi z cyberprzestrzenią. Te, które zawiera raport, należą do grupy zagrożeń opisanych w literaturze, forach tematycznych, a wynikających ze stosowanych obecnie oraz planowanych do wdrożenia w niedługim czasie technologii. Uważam, że w przyszłym roku aktywność cyberprzestępców skoncentruje się na osłabieniu zaufania do usług uruchamianych w chmurze, jak również zwiększy się ilość zagrożeń wynikających z użytkowania urządzeń mobilnych, przy użyciu których wielu z nas łączy się z Internetem.

Podsumowanie

Przygotowany raport na temat prognoz dotyczących zagrożeń teleinformatycznych w 2015 roku jest trzecią edycją tego raportu po edycjach dotyczących roku 2013 i 2014. Jednocześnie jest najprawdopodobniej pierwszym tego typu raportem, na wyniki którego składają się z głosy polskich specjalistów ds. bezpieczeństwa teleinformatycznego. Dotychczas przy analizie tego co może być groźne w nadchodzącym okresie korzystaliśmy z opinii innych podmiotów i specjalistów z zagranicy.

Wyniki ankiety wskazują na to, że w dopiero co rozpoczętym roku powinniśmy w szczególny sposób obawiać się zagrożeń związanych z dedykowanymi, zaawansowanymi atakami o poważnych konsekwencjach. Chodzi głównie o ataki na duże przedsiębiorstwa i podmioty administracji państwowej. Najpoważniejsze zagrożenia niosą ze sobą przewidywania związane z atakami typu APT i DDoS. Z dużym prawdopodobieństwem będzie kontynuowany trend związany z cyberatakami o motywacjach politycznych, głównie w postaci akcji cyberszpiegowskich.

Szczególnej uwadze powinny podlegać również wszelkie zagrożenia związane z naruszaniem prywatności, np.: poprzez wyciek baz danych zawierających dane osobowe. Przy tych ostatnich niezwykle ważna jest dobrze rozwijana współpraca pomiędzy dostawcami usług i ich klientami.

Mariusz Szczęsny
Product Manager
Asseco Poland

Moim zdaniem na polu bitwy toczonej pomiędzy cyberprzestępcami i specjalistami ds. bezpieczeństwa jest coraz gorzej. Tak naprawdę, chyba wszyscy się tylko zastanawiamy kiedy ataki o dużej skali sparaliżują na dłuższy okres działanie jakiegoś Banku, instytucji publicznej, operatora ISP a co gorsza może nawet Rządu. Mam nadzieję że prędko do tego nie dojdzie, ale na najgorsze musimy być przygotowani i cały czas konieczne jest doskonalenie naszych systemów bezpieczeństwa. Co więcej, musimy się do tego przyzwyczaić że na bezpieczeństwie nie możemy i nie powinniśmy oszczędzać.

Dariusz Łydziński
Ekspert ds. Bezpieczeństwa
Energa SA

Celem ataków hakerskich będą przede wszystkim urządzenia mobilne. Wzrośnie częstotliwość ataków na prywatne i firmowe telefony oraz na komputery przenośne. Słabości i luki w oprogramowaniu mobilnym odgrywają coraz większą role w procesie infekowania tych urządzeń. Pojawi się coraz więcej problemów z urządzeniami mobilnymi, gdyż pracownicy podłączają się do firmowych sieci korzystając z prywatnych urządzeń, co może być przyczyną wprowadzania złośliwego oprogramowania wymierzonego w systemy firmowe sterujące procesami zarządzania. Coraz bardziej powszechne stają się ataki ukierunkowane na konkretne organizacje, firmy, osoby czy urządzenie przemysłowe podłączone do sieci. Ataki te będą przybierać na intensywności, tym bardziej że są trudniejsze do wykrycia, gdyż wykorzystywane w takim ataku oprogramowanie są skomplikowane i trudniej jest określić zleceniodawcę czy też przeprowadzającego taki atak. Rosnąca liczba zagrożeń ze strony cyberprzestępców wciąż wskazuje na przeprowadzanie licznych ataków na różne instytucje rządowe oraz firmy komercyjne jako główny cel tego typu działań. Cyberataki mogą doprowadzić do sparaliżowania działalności firmy oraz skutkować utratą wrażliwych informacji. Najpoważniejszymi konsekwencjami włamań są zakłócenia działalności firmy oraz utrata wrażliwych danych, które mogą wystawić firmę na niebezpieczeństwo strat i utratę reputacji.

Uczestnicy ankiety

Marek Antczak – *Doradca ds. Bezpieczeństwa IT / mBank SA*
Arkadiusz Buczek – *Specjalista ds. Cyberbezpieczeństwa / T-Mobile Polska SA*
Janusz Cendrowski – *Kierownik Produktu / Asseco Poland*
Anna Chendoska – *Kierownik Zespołu Kadr i Administracji / Bank Spółdzielczy w Wysokiem Mazowieckiem*
Adam Danieluk – *ISSA Polska*
Dariusz Dąbek – *Zastępca Dyrektora Departamentu / Ministerstwo Administracji i Cyfryzacji*
Przemysław Dęba – *Dyrektor Bezpieczeństwa Systemów Teleinfomratycznych / Orange Polska*
Przemysław Frasunek – *Dyrektor Działu Rozwiązań Multimedialnych, Dyrektor Działu Systemów Bezpieczeństwa / Atende Software sp. z o.o.*
Sławomir Górniak – *Ekspert / ENISA*
Adam Haertle – *Kierownik ds. Bezpieczeństwa / UPC Polska sp. z o.o.*
Marek Jurkiewicz – *Zastępca Dyrektora Departamentu / UKE*
Rafał Kasprzyk – *Adiunkt / Wojskowa Akademia Techniczna*
Marek Kołodziejski – *Dyrektor Biura Bezpieczeństwa / TK Telekom spółka z o.o.*
Maciej Kołodziej – *Konsultant, Administrator Bezpieczeństwa Informacji / FHU MatSoft, NK.pl*
Piotr Konieczny – *Chief Information Security Officer / Niebezpiecznik*
Jerzy Kosiński – *Adiunkt / Wyższa Szkoła Policji w Szczytnie*
Jarosław Kowalewski – *Z-ca Dyrektora Pionu Współpracy z Bankami / Zakład Usług Informatycznych NOVUM Sp. z o.o.*
Borys Łącki – *Pentester / LogicalTrust*
Maciej Łopaciński – *Wiceprezes / Agora TC*
Dariusz Łydziński – *Ekspert ds. Bezpieczeństwa / Energa SA*
Mirosław Maj – *CEO / CIO / Fundacja Bezpieczna Cyberprzestrzeń / ComCERT.PL*
Błażej Miga – *CERT Allegro Group / Grupa Allegro*
Maciej Miłostan – *Analityk bezpieczeństwa / PCSS*
Paweł Olszar – *Ekspert / ING Bank Śląski*
Cezary Piekarski – *Senior Manager / Deloitte*
Tomasz Pietrzyk – *Manager Systems Engineering Eastern Europe / FireEye*
Tomasz Przybylski – *Fundacja Bezpieczna Cyberprzestrzeń*

Elżbieta Rzeszutko – *Nauczyciel Akademicki / Politechnika Warszawska*
Marcin Siedlarz – *Threat Intelligence Analyst / Symantec*
Piotr Skibiński – *Dyrektor Biura Bezpieczeństwa Teleinformatycznego / Polkomtel Sp. z o.o.*
Tomasz Soczyński – *Z-ca Dyrektora Departamentu Informatyki / Biuro GIODO*
Jarosław Stasiak – *Manager Wydziału Bezpieczeństwa IT / mBank SA*
Mariusz Stawowski – *Dyrektor Działu Usług Profesjonalnych / CLICO*
Mariusz Szczęsny – *Product Manager / Asseco Poland*
Krzysztof Szczypiorski – *Profesor Nadzwyczajny / Politechnika Warszawska*
Zbigniew Świerczyński – *Adiunkt n-d / Wydział Cybernetyki Wojskowej Akademii Technicznej*
Artur Wach – *CISO / Bank Handlowy w Warszawie SA*
Paweł Weżgowiec – *Dyrektor Techniczny / ComCERT.PL*
Paweł Wilk – *Szef think tanku / BAD[SECTOR].PL*
Tadeusz Włodarczyk – *Główny specjalista / PSE SA*

Załączniki

Zagrożenie	Prawdopodobieństwo wystąpienia	Poziom zagrożenia
Cyberkonflikty pomiędzy państwami powiązane z atakami dedykowanymi	3,65	4,50
Zagrożenia zawiązane z BYOD (*Bring Your Own Device*)	3,60	3,13
Phishing z wykorzystaniem poczty elektronicznej i serwisów WWW	4,67	3,08
Haktywizm	3,59	2,55
Powstawanie botnetów opartych o platformy mobilne	3,85	3,23
Zagrożenia w serwisach społecznościowych	4,08	2,85
Zagrożenia dla platformy Android	4,28	3,15
Zagrożenia dla platformy iOS	3,05	3,00
Zagrożenia dla platformy Windows Phone/Mobile	3,42	2,80
Zagrożenia typu ransomware/scareware	3,50	2,75
Wykorzystanie gier sieciowych w atakach	2,98	2,27
Wycieki baz danych zawierających dane osobowe, hasła, nr kart kredytowych, itd.	4,22	4,13
Ataki drive-by download	4,10	3,25
Ataki na cloud-computing	3,60	3,75
Zagrożenia związane z „Internet of Things"	3,30	2,80
Ataki na platformy hostingowe	3,42	3,34
Ataki na system DNS	3,40	3,90
Kradzież wirtualnych walut	3,38	2,63
Ataki na systemy sterowania przemysłowego (SCADA)	3,48	4,33
Ataki DDoS na podmioty komercyjne	4,28	3,58
Ataki DDoS na administrację publiczną	4,10	3,38
Ataki na urządzenia medyczne	2,45	4,05
APT – ataki ukierunkowane na organizacje	4,17	4,13
Akcje cyberszpiegowskie na tle politycznym	4,15	3,95

Tabela 1 – Wyniki ankiety dotyczącej prawdopodobieństwa powszechnego wystąpienia oraz poziomu zagrożenia.

FUNDACJA
bezpieczna
cyberprzestrzeń

NAJWIĘKSZE ZAGROŻENIA
DLA BEZPIECZEŃSTWA W INTERNECIE W 2015 ROKU
GŁOS POLSKICH EKSPERTÓW

FUNDACJA BEZPIECZNA CYBERPRZESTRZEŃ
ul. Tytoniowa 20, 04-228 Warszawa, tel: +48 22 112 0 800
e-mail: kontakt@cybsecurity.org

www.cybsecurity.org