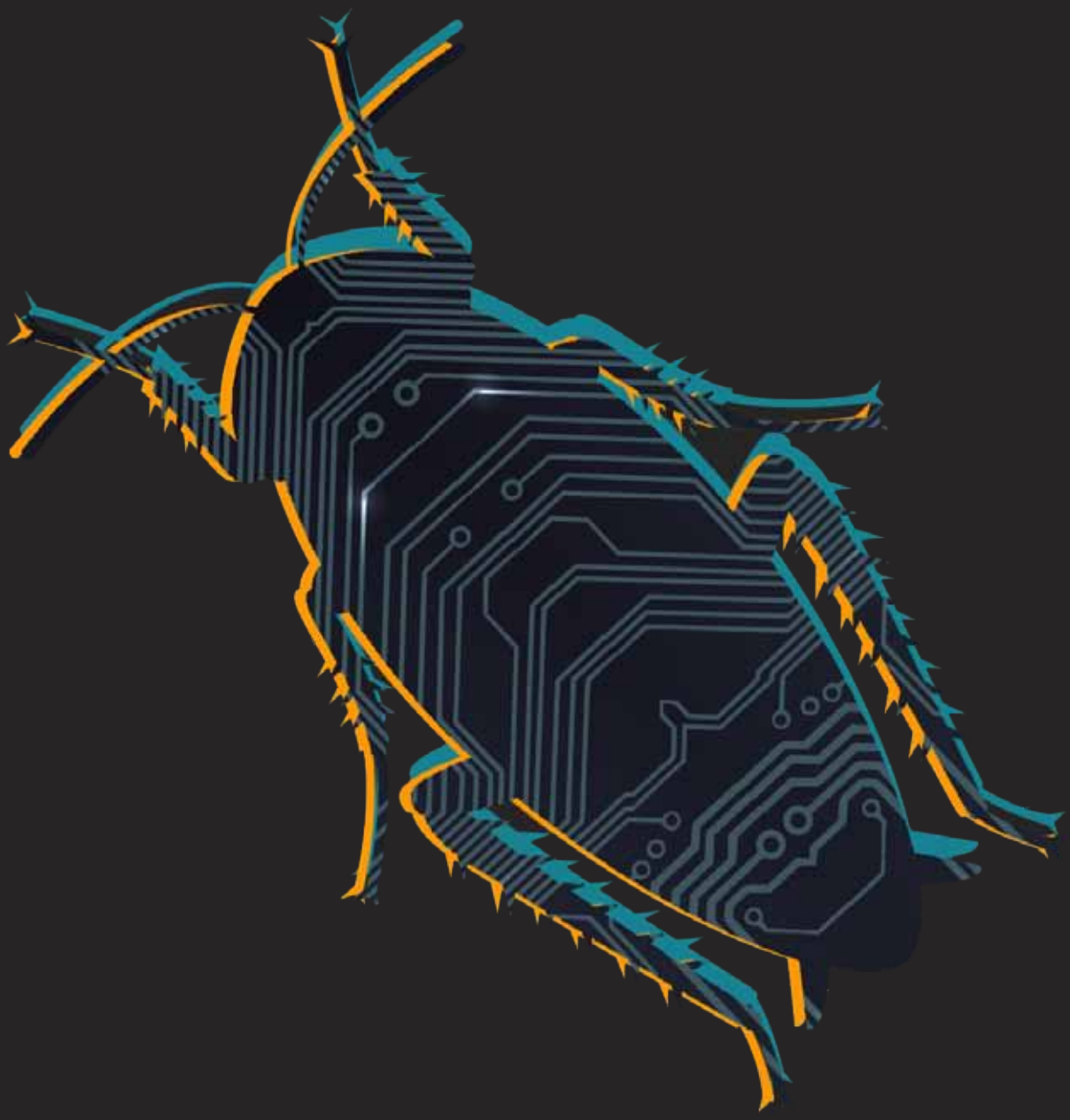
FUNDACJA
bezpieczna
cyberprzestrzeń

NAJWIĘKSZE ZAGROŻENIA DLA BEZPIECZEŃSTWA W INTERNECIE W 2016 ROKU

GŁOS POLSKICH EKSPERTÓW



RAPORT

Spis Treści

Wstęp

Fundacja Bezpieczna Cyberprzestrzeń już po raz czwarty przygotowała raport o zagrożeniach czyhających w sieci Internet. Początek roku to zwykle podsumowanie tego co było i pierwsza próba przygotowania się na to co może nastąpić. Wiele firm na podstawie opracowań i przewidywań własnych lub zewnętrznych przeprowadza w tym czasie analizy tego co działo się w minionym roku i jednocześnie, planuje budżety i działania strategiczne dotyczące wejścia w nadchodzący rok. Podobnie jest, jeśli chodzi o branżę cyberbezpieczeństwa. Tradycyjnie więc przygotowaliśmy dla Państwa raport, w którym chcemy przedstawić najbardziej prawdopodobne i najbardziej groźne zjawiska w cyberprzestrzeni jakie mogą się pojawić w nadchodzącym roku.

Na wstępie zamieszczamy podsumowanie tego co zdarzyło się w roku 2015. Przedstawimy również przewidywania w dalszej części tego raportu, chcemy uczulić na to, co potencjalnie najgroźniejsze. Naszym celem jest aby raport ten był pomocny w działaniach na rzecz minimalizacji ryzyka działań w cyberprzestrzeni. Specjaliści od zarządzania ryzykiem szczególnie mogą z niego skorzystać, chociażby dzięki wartościowaniu poszczególnych zagrożeń.

Chciałbym podkreślić unikatową wartość raportu, ze względu na fakt, że uwzględniliśmy w nim oprócz naszej własnej opinii, również opinie wielu polskich specjalistów z dziedziny bezpieczeństwa teleinformatycznego, z którymi współpracujemy. Zdecydowaliśmy się na prezentację głosu tylko polskich specjalistów, głosu ważnego dla oceny zjawisk cyberbezpieczeństwa z perspektywy rynku krajowego. Takiego ujęcia nie sposób znaleźć w żadnym z wielu raportów dotyczących przewidywań. Dzięki odpowiedziom osób zaproszonych do wypełnienia ankiety powstała lista tego, co potencjalnie najgroźniejsze i najbardziej prawdopodobne w roku 2016.

W tegorocznym raporcie zamieściliśmy również propozycję wykorzystania zawartych w nim danych do przeprowadzenia analizy ryzyka na własne potrzeby. Dzięki temu możliwe jest stworzenie unikalnego zestawu danych, który będzie wykorzystany w Państwa organizacji.

Serdecznie zapraszam do lektury i aktywnego wykorzystywania danych i informacji z naszego raportu. Jeśli ktoś chciałby podzielić się swoimi odczuciami z lektury lub doświadczeniami z korzystania z raportu, prosimy o kontakt mailowy na adres: kontakt@cybsecurity.org

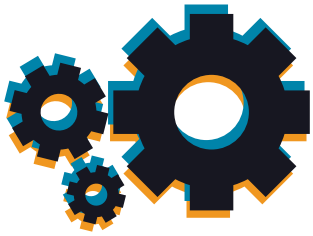
MIROSŁAW MAJ
prezes zarządu
Fundacji Bezpieczna Cyberprzestrzeń

Metodyka

W celu zebrania opinii eksperckich przygotowana została ankieta. Ankieta zawierała zestawienie potencjalnych zagrożeń w 2016 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:

- Akcje cyberszpiegowskie na tle politycznym
- APT – ataki ukierunkowane na organizacje, połączone ze spear phishingiem
- Ataki DDoS na administrację publiczną
- Ataki DDoS na podmioty komercyjne
- Ataki Drive-by Download/Watering Hole
- Ataki na cloud computing
- Ataki na platformy hostingowe
- Ataki na system DNS
- Ataki na systemy sterowania przemysłowego ICS/SCADA
- Ataki na urządzenia medyczne
- Cyberkonflikty pomiędzy państwami powiązane z atakami dedykowanymi
- Haktywizm
- Kradzież wirtualnych walut
- Phishing email and www
- Powstawanie botnetów opartych o platformy mobilne
- Wycieki baz danych zawierających dane osobowe, hasła, nr kart kredytowych, itd.
- Wykorzystanie gier sieciowych w atakach
- Zagrożenia dla platformy Android
- Zagrożenia dla platformy iOS
- Zagrożenia dla platformy Windows Phone/Mobile
- Zagrożenia typu ransomware/scareware
- Zagrożenia w serwisach społecznościowych
- Zagrożenia zawiązane z BYOD
- Zagrożenia związane z "Internet of Things"



W badaniu wzięło udział 42 ekspertów reprezentujących sektory:

Administracji publicznej, organizacji pozarządowych, energetyczny, finansowy i dostawców usług bezpieczeństa.

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 2016 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 2015 roku

Omawiając zagrożenia, które mogą nas spotkać w roku 2016 roku, warto przyjrzeć się temu co działo się w roku, który właśnie minął. W podsumowaniu najważniejszych wydarzeń 2015 r. korzystaliśmy z serwisów: Dziennik Internautów, Fundacja Bezpieczna Cyberprzestrzeń Kaspersky Lab, Niebezpiecznik, Zaufana Trzecia Strona. Niewątpliwie w 2015 roku rzeczami, które w szczególny sposób zapadły w pamięć to działalność grupy **Equation,** operacja cyberprzestępcza **Carbanak**, oprogramowanie **Superfish.**

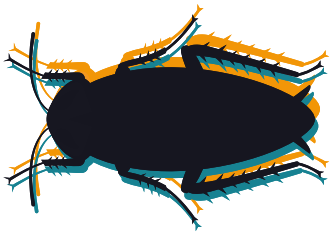
Krótka charakterystyka roku 2015 to:

– Wycieki firmowych danych,
– Współpraca międzynarodowa przeciwko cyberprzestępcom
– Poważne ataki na polskie organizacje (np.: Plus Bank, LOT, MON)
– Liczne kampanie złośliwego oprogramowania na polskich internautów
– Wzrost zainteresowania kwestiami cyberbezpieczeństwa mediów

Spójrzmy na najważniejsze wydarzenia w ujęciu chronologicznym uwzględniając zdarzenia dotyczące Polski.

PL Styczeń 2015 to zdarzenie na naszym krajowym rynku. Dowiadujemy się o **błędach w domenie GOV.pl.** W sieci pojawia się raport pod tytułem ALERT(666) E-ZINE #1, którego autor informował, że stworzył ów raport by zwrócić uwagę na problem bezpieczeństwa tej części sieci.

W lutym dowiedzieliśmy się o dużym napadzie na bank. Cybergang – **Carbanak** ukradł 1 mld dolarów ze 100 instytucji finansowych na całym świecie. **Carbanak** to międzynarodowy gang cyberprzestępców głównie z Rosji, Ukrainy i Chin. W ciągu około dwóch lat skradli oni blisko miliard dolarów amerykańskich instytucjom finansowym na całym świecie, w tym w Polsce. Ponadto oszuści po wniknięciu do sieci dość skutecznie zacierali ślady swojej działalności pod przykrywką legalnych działań.



Luty to także **Grupa Equation**, atakująca cele rządowe, wojskowe, placówki dyplomatyczne, firmy telekomunikacyjne, sektor finansowy, uczelnie wyższe oraz sektor energetyczny. Grupa Equation to przodek kampanii cyberprzestępczych Stuxnet oraz Flame. Cyberprzestępcy używali bardzo zaawansowanych i złożonych technik. Grupa aktywna jest od kilkunastu lat i w swoich atakach wykorzystuje bardzo profesjonalne narzędzia. Grupa stosuje ponadto metody szpiegowskie do dostarczania szkodliwych programów, do atakowanych organizacji, infekowania swoich ofiar a także potężny zestaw „implantów" (trojanów).

W lutym dowiadujemy się o oprogramowaniu **SUPERFISH**, które firma Lenovo instaluje na fabrycznie nowych laptopach. Oprogramowanie to wyświetla reklamy a dodatkowo potrafi podszywać się pod wszystkie szyfrowane witryny www. Dzięki oprogramowaniu posiadacz klucza prywatnego może przeprowadzać ataki MiMT na innych właścicieli.

W drugiej połowie lutego dochodzą do nas kolejne rewelacje z archiwum Snowdena dotyczące ataków na użytkowników sieci komórkowych. Według opublikowanych dokumentów **amerykańskie NSA i brytyjskie GCHQ wykradają klucze szyfrujące zapisane na kartach SIM.** Służby wywiadowcze wykradły ogromne ilości kluczy zapisywanych na kartach SIM bezpośrednio od ich producentów, by móc podsłuchiwać rozmowy poszczególnych użytkowników.

Drugiej połowie lutego Europol w ramach wspólnego działania organów ścigania z producentami oprogramowania i innymi przeprowadził operację **unieszkodliwienia działania botnetu Ramnit**. Zainfekowanych było 3 mln komputerów na świecie. Malware wyłączał ochronę antywirusową i umożliwiał cyberprzestępcom kradzież danych, w tym zdjęć i haseł do kont bankowych. Oprogramowanie rozprzestrzeniane za pośrednictwem wiarygodnie wyglądających linków zawartych w mailach lub poprzez sieci społecznościowe. Zaatakowane komputery były wykorzystywane do dalszego rozsyłania maili phishingowych, a także infekowania witryn internetowych.

PL W marcu usłyszeliśmy, że na początku roku miał miejsce „**poważny atak hakerski** na prywatną pocztę elektroniczną osób pracujących **w Ministerstwie Obrony Narodowej (MON) i Sztabie Generalnym Wojska Polskiego**". Informacje w marcu 2015 opublikował tygodnik „Wprost", a w listopadzie potwierdził ten atak były doradca Ministra Obrony Narodowej - Krzysztof Bondaryk.

Europol we współpracy z FBI i producentami oprogramowania antywirusowego w kwietniu **zamknął botnet Beebone**, polimorficzny malware 0-day zawierający typowe moduły używane do tworzenia sygnatur czy uaktualniania czarnych list (np. file hash, control server IP address, itd.) zmieniają się z każdym atakiem, utrudniają obronę i skutecznie rozprzestrzeniają się w sieci.

W kwietniu mieliśmy też informację o **unieszkodliwieniu botnetu – Simbda**. Interpol we współpracy z producentami oprogramowania antywirusowego zamknął serwery kontroli, wykorzystywane do komunikacji z zainfekowanymi maszynami. Część z nich działała w Polsce. Botnet Simbda składał się z ponad 700 tysięcy zainfekowanych komputerów na całym świecie, w ponad 190 krajach.

Na początku drugiego kwartału, miał miejsce **atak na francuską telewizję TV5**. Włamywacze podpisujący się jako Cyberkalifat, przejęli strony WWW i konta w serwisach społecznościowych, ale także wyłączyli nadawanie kanałów telewizyjnych i poważnie uszkodzili serwery firmy.

Kwiecień to też **krytyczny błąd w usłudze Microsoft (MS15-34)**. Odpowiednio skonstruowane żądanie HTTP może doprowadzić do wykonania dowolnego kodu z uprawnieniami administratora w każdej usłudze Microsoftu działającej w oparciu o HTTP.

Również w kwietniu dowiadujemy się o nowej, **zaawansowanej kampanii cyberszpiegowskiej Cozy Duke**. Wykorzystuje ona szkodliwe oprogramowanie do atakowania szczegółowo wybranych strategicznych celów. Ofiary znajdują się głównie na terenie USA – prawdopodobnie Biały Dom oraz Departament Stanu, a na liście celów atakujących znalazły się także organizacje rządowe i firmy z Niemiec, Korei Południowej i Uzbekistanu. Poza faktem atakowania celów najwyższego szczebla nowa operacja cyberprzestępcza wyróżnia się także innymi alarmującymi cechami - zastosowaniem zaawansowanych możliwości szyfrowania i zapobiegania wykryciu poprzez „walkę" z oprogramowaniem antywirusowym. Cozy Duke to operacja o rozbudowanym zakresie szkodliwej funkcjonalności z podobieństwami do wcześniejszych kampanii cyberszpiegowskich: MiniDuke, CosmicDuke i OnionDuke.

PL Na naszym rodzimym podwórku w kwietniu zaobserwowaliśmy **masową kampanię** rozsyłania na skrzynki e-mail **fałszywych wiadomości,** pochodzących **rzekomo od Allegro**, informujących o „włamaniu" na konto z prośbą o kliknięcie w zawarty w wiadomości link w celu odblokowania konta. W rzeczywistości, strona wyłudzała opłatę. Wiadomość przychodziła z podrobionego adresu security@allegro.pl.

PL Drugi kwartał zaczęliśmy więc z **phishingiem** i to będzie już zjawisko towarzyszące polskim internautom do końca roku. Z początkiem maja w skrzynkach polskich internautów, a w szczególności kont przypisanych do kont firmowych, pojawiły się informacje, **rzekomo od Poczty Polskiej.** Maile z załącznikami ze złośliwym oprogramowaniem typu ransomware, czyli szyfrującym pliki na dysku i wymuszającym wpłaty za ich odszyfrowanie. Jego najbardziej znanym przypadkiem jest CryptoLocker.

PL W maju polscy internauci dostają **masowe wysyłki e-maili z zainfekowanymi załącznikami,** w których rzekomo była wystawiona faktura.

Maj to również **VENOM** (ang. Virtualized Environment Neglected Operations Manipulation). Firma CrowdStrike poinformowała o odkryciu bardzo poważnego błędu w środowiskach wirtualizacyjnych Xen, KVM i QEMU, który umożliwia „opuszczenie" maszyny wirtualnej i przejęcie kontroli nad sąsiadującymi środowiskami wirtualnymi.

W czerwcu usłyszeliśmy o **włamaniu do sieci federalnego urzędu w USA** ds. zarządzania personelem (Office of Personnel Management) samo wydarzenie miało miejsce w kwietniu. Wykradziono dane około 4 milionów rekordów. O dokonanie ataku oskarżane zostały, jak to najczęściej bywa w takich przypadkach, Chiny.

PL W czerwcu przestępca ukrywający się za pseudonimem „Polsilver" **włamał się do systemu informatycznego Plus Banku** i szantażował go domagając się pieniędzy. Został zatrzymany na początku września. Ten przypadek był tematem wielu dyskusji i w jasny sposób wskazała na realne zagrożenie związane z bezpośrednim atakiem na infrastrukturę banku, a nie jak bywa w większości przypadków – na komputery klientów bankowości elektronicznej.

PL W czerwcu **Polskie Linie Lotnicze LOT poinformowały o awarii systemu teleinformatycznego**, w wyniku której uziemiono kilkadziesiąt lotów. Początkowo mówiono o ataku teleinformatycznym. Śledztwo w tej sprawie zostało umorzone a sąd w styczniu 2016 orzekł, że nie było ataku na system informatyczny LOT, ale cyberprzestępcy posłużyli się serwerami polskiej firmy, by zaatakować inny system. Ten przypadek od początku wzbudzał dużo kontrowersji. Szczególnie interesujące były rozbieżności pomiędzy opinią władz LOT-u i opinią specjalistów z ABW, którzy badali sprawę.

W lipcu dowiadujemy się o włamaniu do włoskiej **firmy Hacking Team**, producenta złośliwego oprogramowania używanego przez rządy całego świata. Dane z jej serwerów (ok. 400GB) zostały opublikowane w sieci, również znalazł się folder dotyczący Polski. Ten przypadek rzucił nowe światło na to na jaką skalę złośliwe oprogramowanie wykorzystują służby wielu państw.

W połowie lipca miał miejsce wielki **wyciek danych z serwisu Ashley Madison**. Wykradziono pełną bazę danych klientów serwisu, a także klucze domenowe i prywatne dokumenty pracowników serwisu.

Koniec lipca to **StageFright – największa do tej pory dziura jaką odkryto w Androidzie**. Jeden MMS, może umożliwić przejęcie kontroli nad większością smartfonów działających pod kontrolą systemu Android. Ofiara nie musi wykonywać żadnej akcji, nawet nie zorientuje się, że została zaatakowana, dlatego, że udany atak spowoduje skasowanie śladów włamywacza z telefonu ofiary. Są tacy, którzy nazywają StageFright Heartbleedem w świecie mobilnym.

W sierpniu ponownie słyszymy o problemach dotyczących Androidów. Poważna dziura w Androidach, podmienia zainstalowane aplikacje na fałszywe. Eksperci szacują, że dotyczy on około 55% telefonów z Androidem a za błąd odpowiedzialna jest klasa **OpenSSLX509Certificate**. Dziura pozwala podnieść uprawnienia aplikacji do poziomu uprawnień systemowych.

Wrzesień. **SYNfulKnock dziurawy firmware Cisco**, pozwala na zdalne przejęcie kontroli i dostęp do routerów. Wykryto modyfikacje oprogramowania niektórych modeli ruterów Cisco. Zmodyfikowane

rutery reagują na bardzo specyficzną kombinację modyfikacji pakietów TCP i umożliwiają zdalny, nieautoryzowany dostęp do swoich funkcji.

PL Dane dłużników Getin i Noble Banku były na sprzedaż. Na Torepublic sprzedawca, korzystający z nicka „alialbania" zamieszcza ofertę sprzedaży listy zawierającej dane 18 000 dłużników, aby uwiarygodnić ofertę ujawnił dane pierwszych 100 osób z listy. Do włamania doszło poprzez przejęcie kontroli nad komputerem pracownika banku.

We wrześniu również **firma Apple padła ofiarą ataku hakerskiego**. Do Apple App Store, oficjalnego sklepu z aplikacjami dostały się prawdziwe wersje programów zainfekowanych złośliwym kodem. Niebezpieczne aplikacje, stworzone były za pomocą **narzędzia XcodeGhost.** Narzędzie to posiada w kodzie zaimplementowane funkcjonalności, których celem jest wykradanie danych ze schowka oraz pozyskiwanie dane dostępowe do iClouda. Hasła kradzione są nie wprost z telefonu, ale przez wyświetlenie w obrębie aplikacji okna, które prosi o podanie loginu i hasła – phishing.

PL We wrześniu odnotowaliśmy **trzy nowe kampanie złośliwego oprogramowania na polskich internautów**. Wszystkie dotyczyły informacji rzekomo wysyłanych przez polskie firmy. Kampanie zawierały wezwanie do zapłaty, internauci otrzymywali faktury i dodatkowo np wezwanie do zapłaty, pojawiła się również kampania mówiąca o protokole odbioru robót.

Pod koniec września usłyszeliśmy o **wycieku danych z firmy Talk Talk.** Cyberprzestępcy mogli dotrzeć do danych osobowych i bankowych ok. 4 mln klientów TalkTalk. Brytyjski dostawca Internetu przyznał się, że mogło dojść do naruszenia danych.

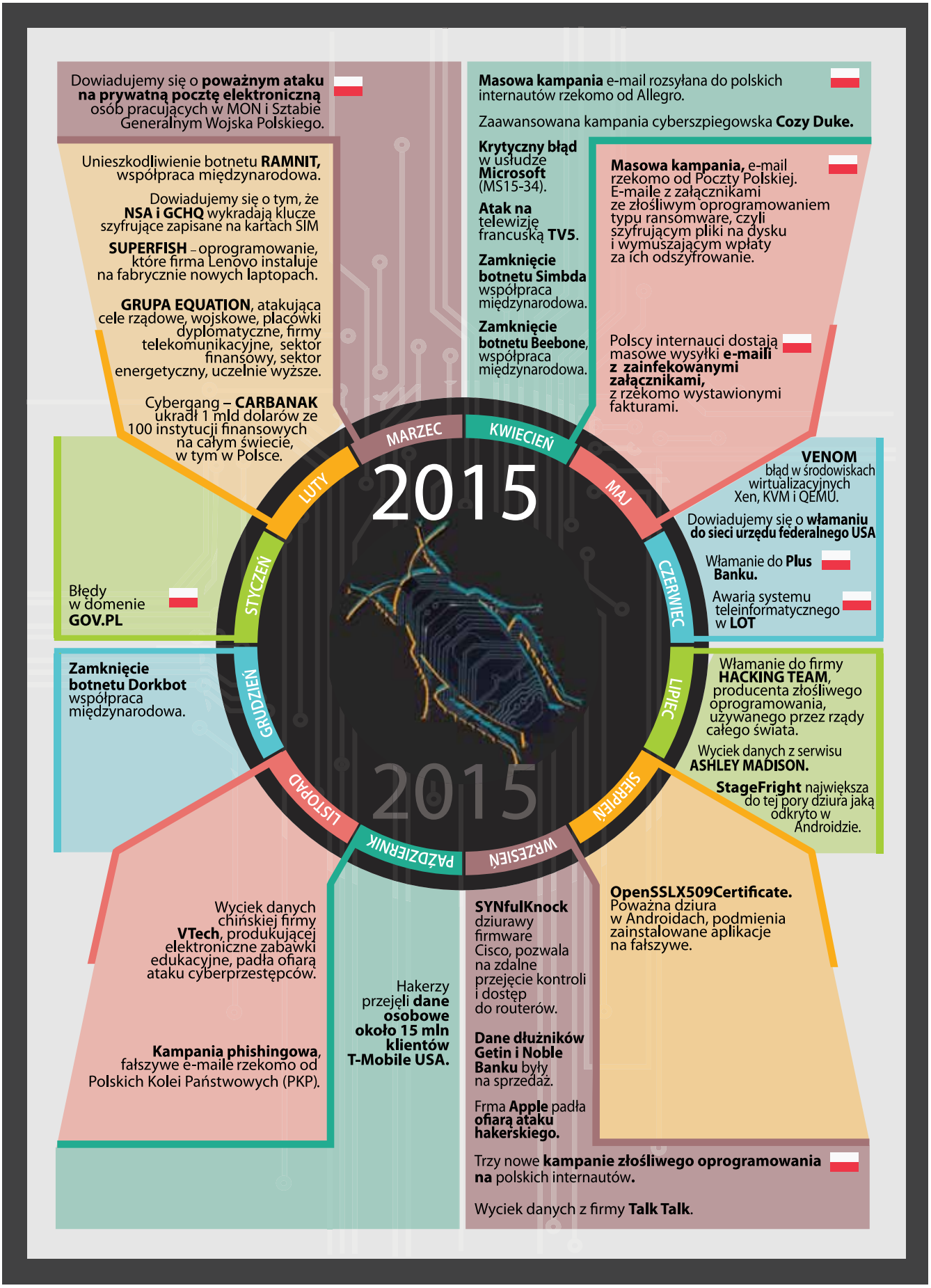
Październik. **Hakerzy przejęli dane osobowe około 15 mln klientów T-Mobile USA**. Słabym ogniwem okazała się firma sprawdzająca zdolność kredytową. Zasoby wykradzionej bazy zawierają dane osób, których zdolność kredytowa była sprawdzana w okresie ostatnich dwóch lat.

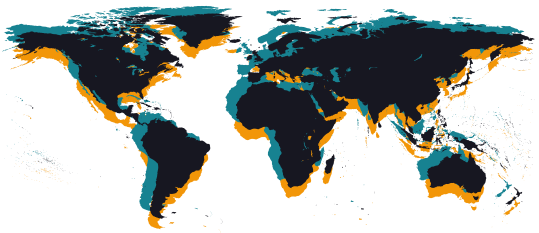
W listopadzie **kolejny wyciek**. Baza danych **chińskiej firmy VTech**, produkującej elektroniczne zabawki edukacyjne, padła ofiarą ataku cyberprzestępców. Wykradziono dane ponad 6 mln kont (nazwy użytkowników, hasła, adresy IP i informacje o pobranych plikach, również daty urodzenia, płeć i imiona dzieci oraz 190 gigabajtów zdjęć dziesiątek tysięcy twarzy dzieci.

PL Listopad to kolejna **kampania phishingowa**, fałszywe e-maile tym razem podszywające się pod Polskie Koleje Państwowe (PKP), próba wyłudzania opłaty za SMS Premium.

W grudniu. FBI, Interpol i Europol wraz z producentami oprogramowania i CERT Polska **unieszkodliwili grupę botnetów Dorkbot.** Złośliwe oprogramowane, które kradnie dane (również uwierzytelniające), wyłącza aplikacje bezpieczeństwa (np. programów antywirusowych) a także dystrybuuje inne złośliwe oprogramowanie. Szacunkowo w 2015 roku zainfekowanych było co najmniej milion komputerów z systemem Windows na całym świecie, również w Polsce.

Najważniejsze wydarzenia IT security 2015 w ujęciu chronologicznym.

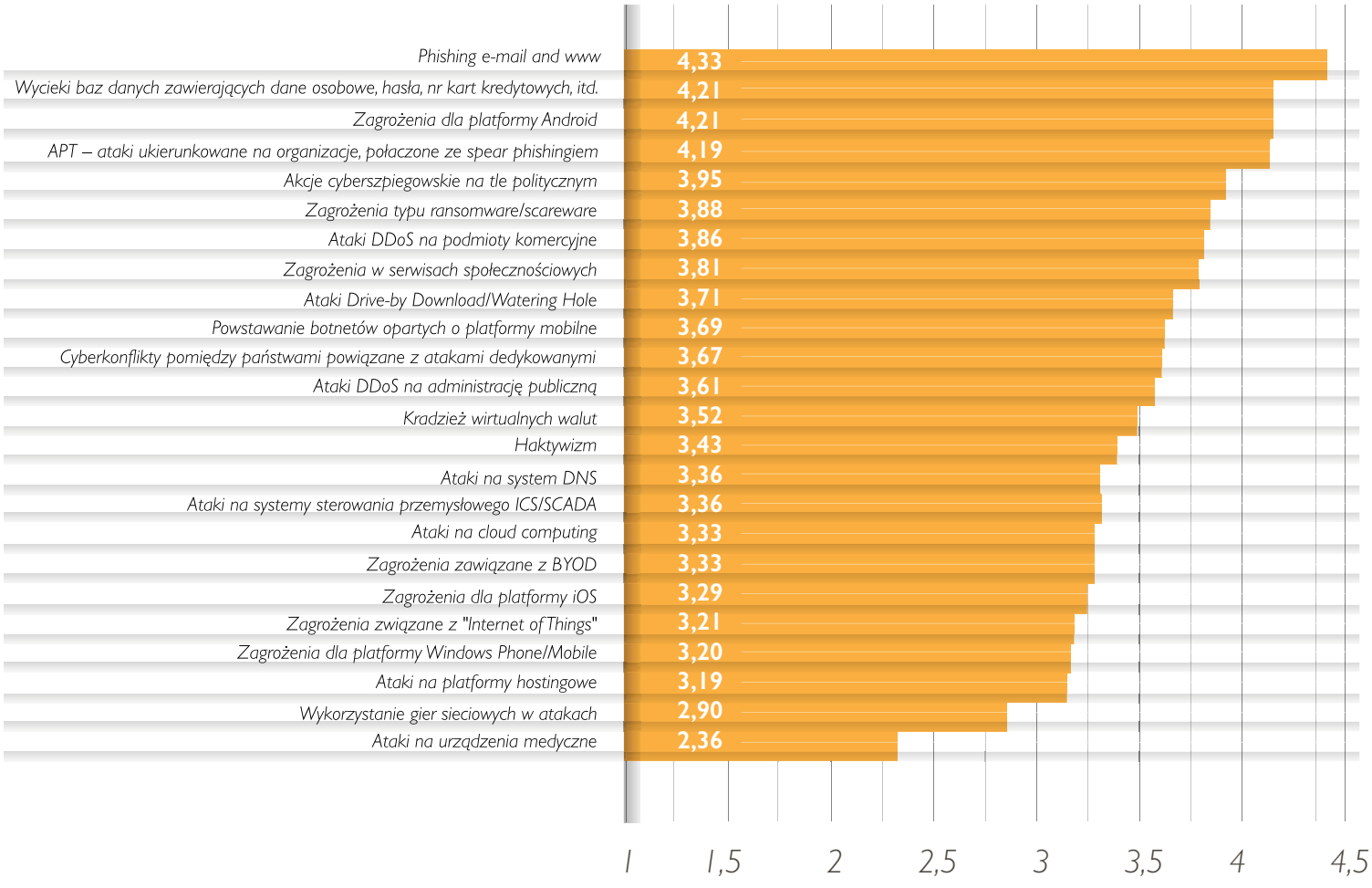


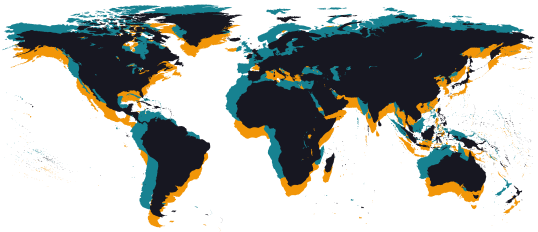


Najwieksze zagrożenia w roku 2016 – prawdopodobieństwo wystąpienia

Zestaw, jaki zaproponowaliśmy do oceny, bazuje na pozycjach z lat ubiegłych. 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 powszechnego wystąpienia wskazanego poniżej zagrożenia. Skala 1-5 (1 - najmniej prawdopodobne, 5 - najbardziej prawdopodobne).





Na czoło klasyfikacji wybijają się trzy kategorie[2] :

- Phishing e-mail and WWW – **4,33**
- Wycieki baz danych zawierających dane osobowe, hasła, nr kart kredytowych, itd. – **4,21**
- Zagrożenia dla platformy Android – **4,21**

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.
Można tylko odnotować przesunięcie się balansu z phishingu www na pocztę elektroniczną.
Podobnie zresztą było w dwóch poprzednich latach.
Jak widać nie ma zbyt dużego oczekiwania wśród ekspertów, że coś tutaj się zmieni, choć co ciekawe wartość tego prawdopodobieństwa była wyższa w poprzednich przewidywaniach (odpowiednio **4,39**; **4,67** dla lat 2014 i 2015). Ta opinia ekspertów ma odzwierciedlenie w rzeczywistości. W 2015 roku, począwszy od drugiego kwartału, polskich internautów nękały masowe kampanie e-mail (m.in. Poczta Polska, Allegro, PKP, Kruk SA) to potwierdzenie kontynuacji tego trendu, który jest już bardzo długi i jak widzimy w roku 2015 miał natężenie.

Zagrożenia związane z systemem operacyjnym Android to ponownie druga pozycja wśród liderów najbardziej prawdopodobnych zagrożeń. Trendowi migracji usług z komputerów stacjonarnych do urządzeń przenośnych niestety towarzyszy również migracja zagrożeń. Szczególnie dotyczy to właśnie systemu Android. Powód jest znany – otwarta architektura dystrybucji aplikacji i niewielka skłonność użytkowników do aktualizacji swoich systemów.
Taką samą ocenę wśród ekspertów zebrało zagrożenie związane z wyciekami danych. To reakcja na fakt, że takie przypadki na stałe zagościły w dossier działań cyberprzestępców wymuszających okup lub chcących skompromitować zaatakowaną organizację.

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

Jakub Bojanowski
Partner
Deloitte Polska

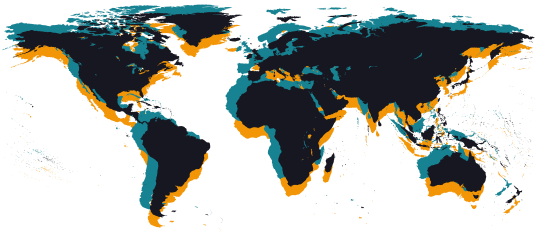
Myślę, że nowy typ zagrożeń, który będzie dominował za 3-5 lat nie został jeszcze objęty ankietą. Przyszłe zagrożenia będą ściśle powiązane z wdrażaniem nowych technologii, które dotychczas są wykorzystywane w wąskim zakresie i dlatego uważa się je za bezpieczne. Przykładem może być biometryka. Obecnie, jako rozwiązanie niszowe jest stosunkowo bezpieczna. Jej masowe wdrożenie zwiększy zainteresowanie ze strony cyberprzestępców, którzy na bieżąco będą odkrywali luki w nowych technologiach.

Arkadiusz Buczek
Specjalista ds. Cyberbezpieczeństwa
T-MOBILE POLSKA S. A.

W roku 2016 zagrożenia dotyczące systemów mobilnych znajdą się już w głównym nurcie problemów bezpieczeństwa. We wszystkich obszarach potrzebny będzie większy nacisk na monitorowanie i szybką reakcję.

Piotr Konieczny
Chief Information Security Officer
Niebezpiecznik

Rok 2015 pokazał, że nie musimy sami infekować się złośliwym oprogramowaniem, bo robią to za nas producenci naszego sprzętu, m.in. firmy Lenovo (SuperFish) czy Dell (eDellRoot), a z ataków na tzw. „Internet of Things" dalej nie wynika żadne realne zagrożenie dla przeciętnego Kowalskiego. Skłaniam się więc do tezy, że i w 2016 roku znów przede wszystkim borykać będziemy się z podstawowymi problemami
a) socjotechniką i użytkownikami bezmyślnie klikającymi na linki i załączniki w podrobionych e-mailach,
b) kontami przejmowanymi ze względu na słabe lub domyślne hasło oraz
c) brakiem wyobraźni producentów oprogramowania, prowadzącym do pojawiania się w ich rozwiązaniach znanych od lat błędów.



Borys Łącki
Pentester
LogicalTrust

Olbrzymie zyski cyberprzestępców z szantażowania firm oraz zwykłych użytkowników za pomocą złośliwego oprogramowania typu ransomware, sprawiły, że nadchodzący rok 2016 będzie obfitował w kolejne, jeszcze bardziej wyrafinowane sposoby szantażu. Może to być np. ransomware w środowisku serwerowym lub mobilnym albo szantaż związany z blokowaniem dostępu do popularnych usług. Coraz częściej będziemy mieli do czynienia z sytuacją, w której cyberprzestępcy będą szantażowali firmy, iż opublikują ich wrażliwe dokumenty, jeśli nie zostaną spełnione finansowe oczekiwania. Z uwagi na olbrzymią skuteczność i braki w edukacji związanej ze świadomością zagrożeń, możemy spodziewać się jeszcze większej liczby kampanii wykorzystujących najsłabsze ogniowo czyli użytkownika.

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

To co przewidywałem rok temu, czyli wzrost cyberzagrożeń na tle politycznym, niestety się sprawdziło. Nie widzę przyczyny, dla której ten trend miałby się odwrócić. Myślę, że może wręcz narastać, o czym świadczą chociażby ostatnie masowe ataki na sieci i serwisy w Turcji. Ten problem będzie dotyczyć zarówno rozgrywek na poziomie państw jak i haktywizmu. Dodatkowo sądzę, że jeszcze bardziej może dać się we znaki powszechne atakowanie Internetu Rzeczy. Po serii ataków raczej będących ciekawostkami, możliwe jest wystąpienie ataków o poważnych, niebezpiecznych konsekwencjach.

Na drugim biegunie rankingu prawdopodobieństwa zagrożeń mamy dwie pozycje, które w punktacji nie przekroczyły wartości 3 punktów. Jest to utrzymujący się trend bowiem w roku ubiegłym dokładnie te same dwie pozycje, również nie przekroczyły progu 3 punktów.

Są to począwszy od najniżej notowanych:

- Ataki na urządzenia medyczne – **2,36**
- Wykorzystanie gier sieciowych w atakach – **2,90**

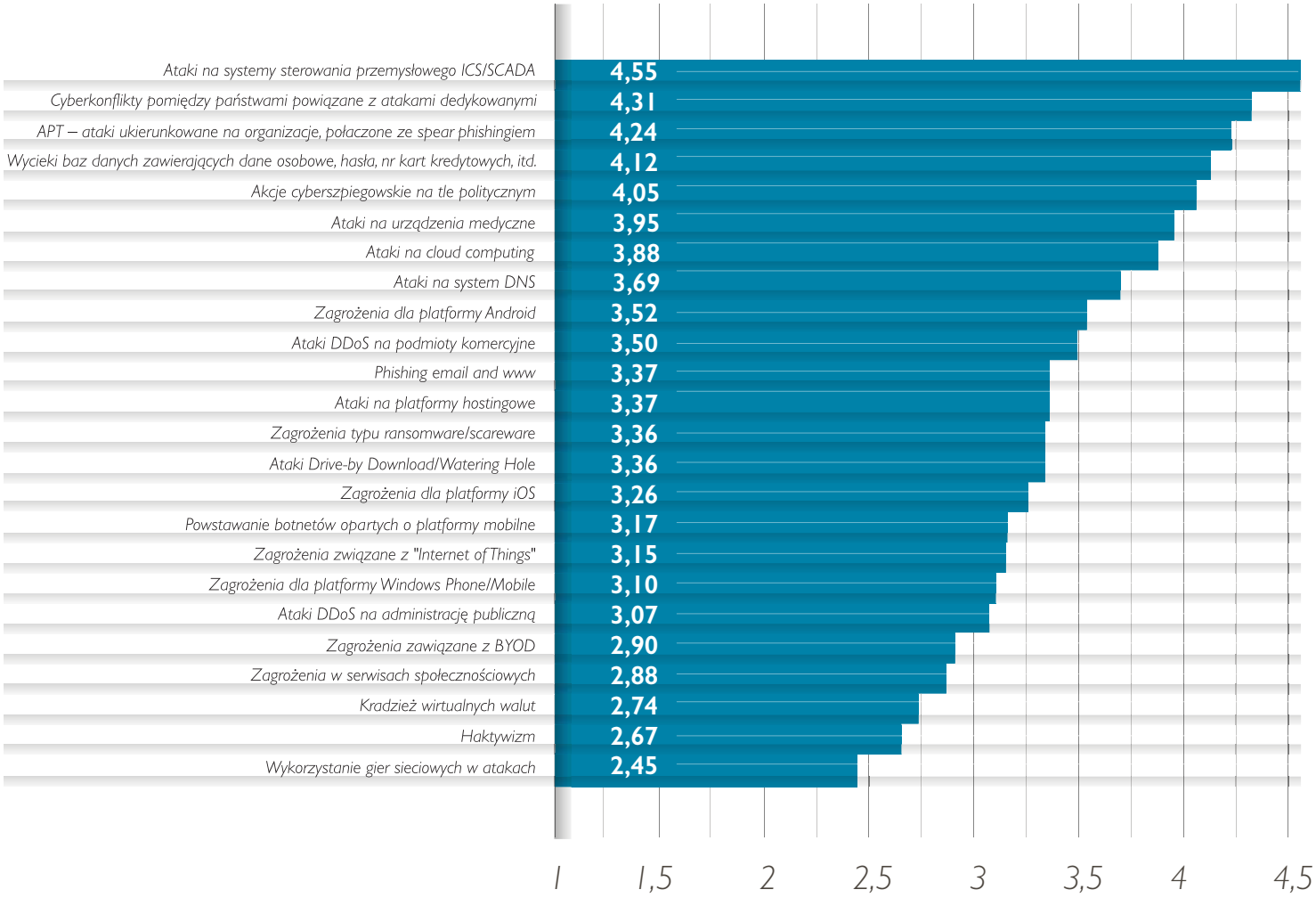
Jak widać pojawiające się coraz częściej informacje na temat słabości systemów używanych w służbie zdrowia nadal nie jest przekonywującym argumentem dla większości ekspertów i nisko oceniają oni prawdopodobieństwo jakiegoś wyraźnego przełomu w tej sprawie. Być może sytuację zmieni nadchodząca dyrektywa NIS (ang. Network Information Security), która wymagać będzie od sektora służby zdrowia bardzo poważnego zajęcia się sprawami cyberbezpieczeństwa. Może to zmusić do większej uwagi poświęconej nie tylko bazom danych pacjentów, ale i takim urządzeniom. Podobny efekt może być wchodzące rozporządzenie dotyczące ochrony danych osobowych. Być może jednak te zmiany nie będą jeszcze mocno widoczne w roku 2016 i na zmianę postrzegania przyjdzie nam jeszcze poczekać.
Środowisko gier sieciowych nadal ma pozostać oazą względnego spokoju. Tu nic się nie zmienia od lat.

Ciekawe jest natomiast inne zjawisko. Mimo tego, że trudno jest nazwać rok 2015 spokojnym, co widać dość dobrze z zamieszczonego przez nas podsumowania, to średnia ocena prawdopodobieństwa zagrożeń dla roku 2016 jest wyraźnie niższa niż była dla roku 2015. W zeszłym roku była ona na poziomie **3,7**, natomiast w tegorocznym raporcie wynosi ona **3,57**. Jeszcze lepiej to widać, jeśli spojrzymy na różnicę w liczbie zagrożeń, które przekroczyły wartość **4**. Dla roku 2015 było ich **9** dla roku 2016 tylko **4**. Pozostaje mieć nadzieję, że to udane przewidywanie.

Największe zagrożenia w 2016 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 niebezpieczeństwa 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:

- Ataki na systemy sterowania przemysłowego ICS/SCADA – **4,55**
- Cyberkonflikty pomiędzy państwami powiązane z atakami dedykowanymi – **4,31**
- APT – ataki ukierunkowane na organizacje, połaczone ze spear phishingiem – **4,24**
- Wycieki baz danych zawierających dane osobowe, hasła, nr kart kredytowych, itd. – **4,12**
- Akcje cyberszpiegowskie na tle politycznym – **4,05**

Od lat eksperci identyfikują te same obszary najbardziej groźnych cyberataków. Trudno się dziwić – analiza sytuacji nie pozostawia złudzeń, a nawet utrwala taki obraz. Najlepszym dowodem na to są chociażby groźne doniesienia zza naszej wschodniej granicy. Konflikt rosyjsko-ukraiński na dobre zagościł w cyberprzestrzeni, a nawet przekraczane są kolejne jego granice, jak na przykład cyberatak powiązany z dużą awarią energetyczną we wschodniej Ukrainie.
Również systematycznie pojawiające się raporty największych światowych graczy w dziedzinie „threat intelligance", w których informują o coraz to nowych operacjach cyberszpiegowskich wymierzonych w instytucje państwowe i organizacje międzynarodowe, nie pozostawiają złudzeń jeśli chodzi o duże zagrożenie wywodzące się z tej aktywności.

Na dole rankingu zagrożeń o największych konsekwencjach znajdują się:

- Zagrożenia zawiązane z BYOD – **2.90**
- Zagrożenia w serwisach społecznościowych – **2.88**
- Kradzież wirtualnych walut – **2.74**
- Haktywizm – **2.67**
- Wykorzystanie gier sieciowych w atakach – **2.45**

Krzysztof Surgut
CEO
Data Space Sp. z o.o.

Rośnie liczba poważnych incydentów w polskich firmach i instytucjach. Ujawnione przez gminy starty, wynikłe z działania malware, osiągają astronomiczne kwoty - liczone w milionach złotych. „Polski półświatek" już dostrzegł, że Internet to „żyła złota". A statystyki policyjne potwierdzają szybko rosnący trend przestępstw w polskiej cyberprzestrzeni. W 2015roku aresztowano 18 Polaków, należących do międzynarodowej grupy cyberprzestępców - wszystko za sprawą akcji prowadzonej przez Europol i Eurojust. To już nie są „zabawy nastolatków".

Przemysław Dęba
Dyrektor Bezpieczeństwa Systemów Teleinfomratycznych
Orange Polska

W 2015 roku mieliśmy do czynienia ze wzrostem prostych ataków na klientów detalicznych banków jak i targetowanych na konkretne instytucje dysponujące ciekawymi danymi. Co więcej najwyraźniej rośnie atrakcyjności rodzimych celów. Królował spear phishing, ale kolejne kampanie przysłużyły się wzrostowi świadomości statystycznego internauty. Będziemy mieli więc do czynienia z rozszerzeniem stosowanego arsenału. Podatności w mobilnych systemach operacyjnych i przeglądarkach czekają, a elementy socjotechniki znacznie zwiększają skuteczność ataku.

Tomasz Soczyński
Zastępca Dyrektora Departamentu Informatyki
Biuro GIODO

Działania legislacyjne i organizacyjne w celu wdrożenia nowych przepisów ogólnego rozporządzenia o ochronie danych oraz dyrektywy w sprawie policji i wymiaru sprawiedliwości. Po przyjęciu tego pakietu, dwuletni okres przewidziany na wdrożenie przepisów unijnego rozporządzenia, będzie wymagał od wszystkich zainteresowanych stron opracowania wytycznych, narzędzi i procedur organizowania w zakresie stosowania nowych przepisów, w tym zwłaszcza przyszłej współpracy między organami ochrony danych oraz zapewnienia spójności działań. Istotne też będzie określenie wzajemnych relacji pomiędzy nowym rozporządzeniem o ochronie danych a dyrektywą e-Privacy.

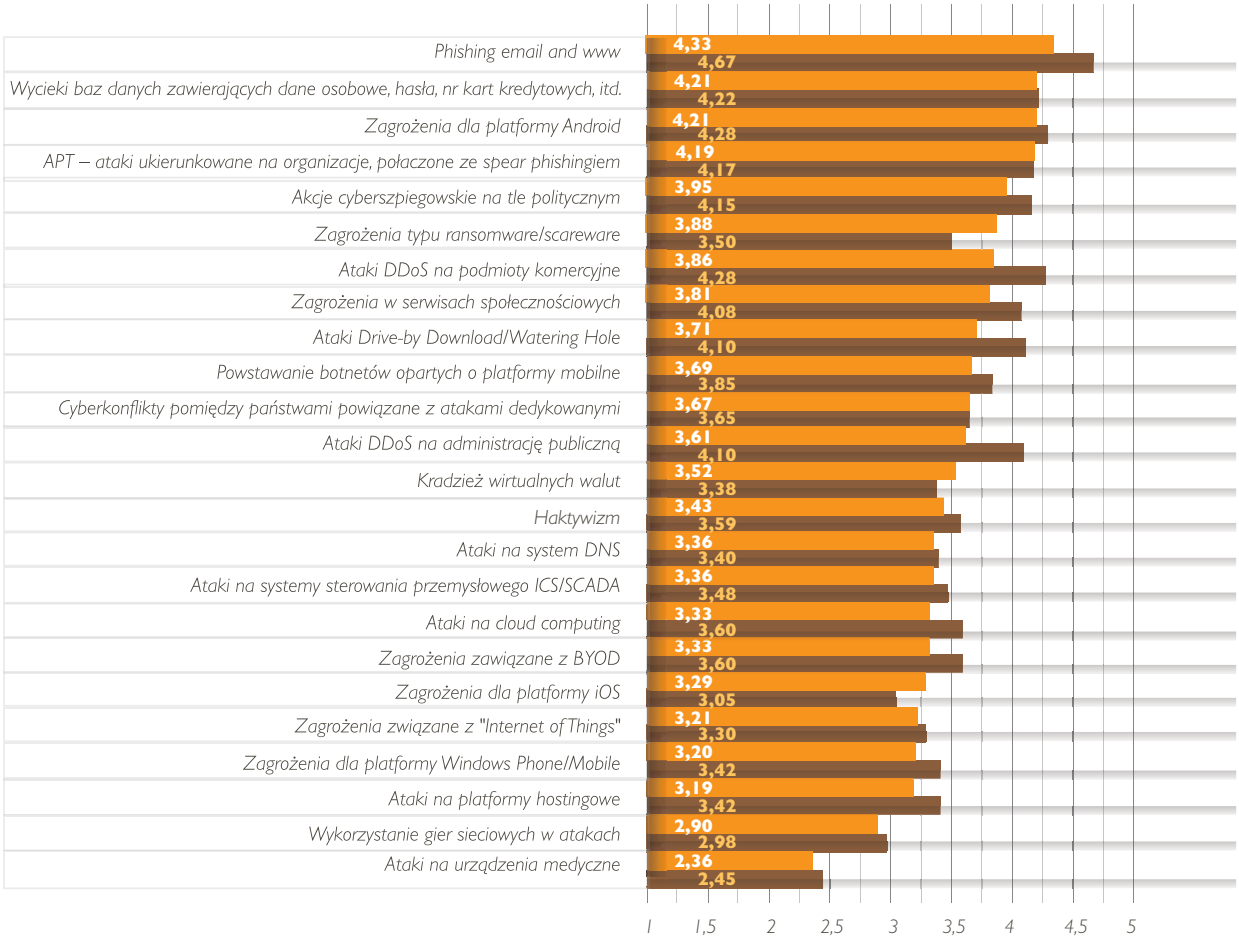
Maciej Kołodziej
Konsultant, Administrator Bezpieczeństwa Informacji
FHU MatSoft, E-detektywi.pl

Rok 2016 może okazać się dość interesujący dla bezpieczeństwa informacji, ze względu na sytuację geopolityczną, zagrożenia dotyczące e-terroryzmu oraz coraz większe uzależnienie wielu gałęzi przemysłu i usług od e-komunikacji i przesyłania dużych ilości newralgicznych danych za pośrednictwem sieci publicznych. Informacje powinny być odpowiednio chronione, ale lawinowy wzrost wolumenu ruchu, pogoń za lepszym wynikiem biznesowym, konkurencyjność oraz beztroska użytkowników sprzyjają popełnianiu błędów.

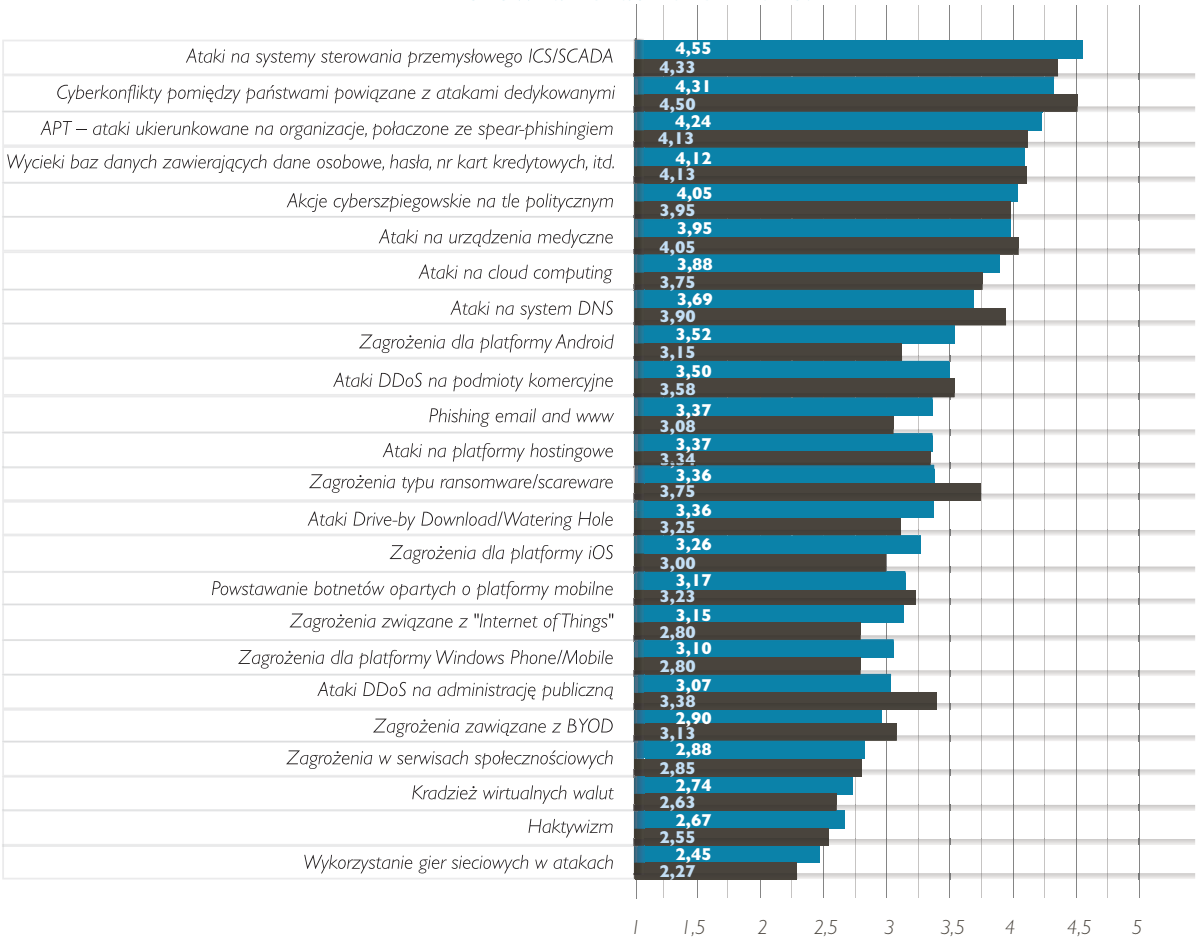
Dół rankingu jest praktycznie bez większych zmian. Warto może zauważyć, że wyskoczyło z tego zestawu, czyli ocenione jest na bardziej niebezpieczne, zagrożenie związane z „Internet of Things" Z bardziej szczegółowych obserwacji warto zauważyć kilka innych istotnych zmian w stosunku do 2015 r.
- wspomniany „awans" zagrożenia związanego z IoT (z **2,80** do **3,15**)
- wzrosła ocena zagrożenia związana z atakami na platformy mobilne – w szczególności to dotyczy systemu Android (wzrost z **3,15** na **3,52**), ale i iOS (z **3,00** na **3,26**) oraz Windows Phone/Mobile (z **2,80** na **3,10**)
- ataki na systemy sterowania przemysłowego uznane zostały za jeszcze bardziej niebezpieczne (wzrost z **4,33** na **4,55**)
- spadła ocena zagrożenia związana z atakami typu DDoS, zarówno na organizacje komercyjne (choć tu niewielka z **3,58** na **3,50**) jak i na administrację publiczną (z **3,38** na **3,07**)

Te szczegółowe zmiany są na pewno związane ze wzrostem zaniepokojenia, pojawiającym się w sytuacji skutecznych ataków na systemy sterowania, jeszcze bardziej na platformy mobilne i brakiem spektakularnych ataków typu DDoS, z jakimi mieliśmy do czynienia w latach ubiegłych, czy niepokojących „case study" dotyczących BYOD. Niewątpliwie w tych dwóch ostatnich obszarach w ostatnim okresie nastąpił dość istotny progres dotyczący skutecznej obrony, poprzez masowe wprowadzanie rozwiązań klasy anty-DDoS czy systemów chroniących platformy mobilne (np.: klasy MDM – Mobile Device Management).

Prawdopodobieństwo powszechnego wystąpienia zagrożenia. Porównanie lat 2015 i 2016.



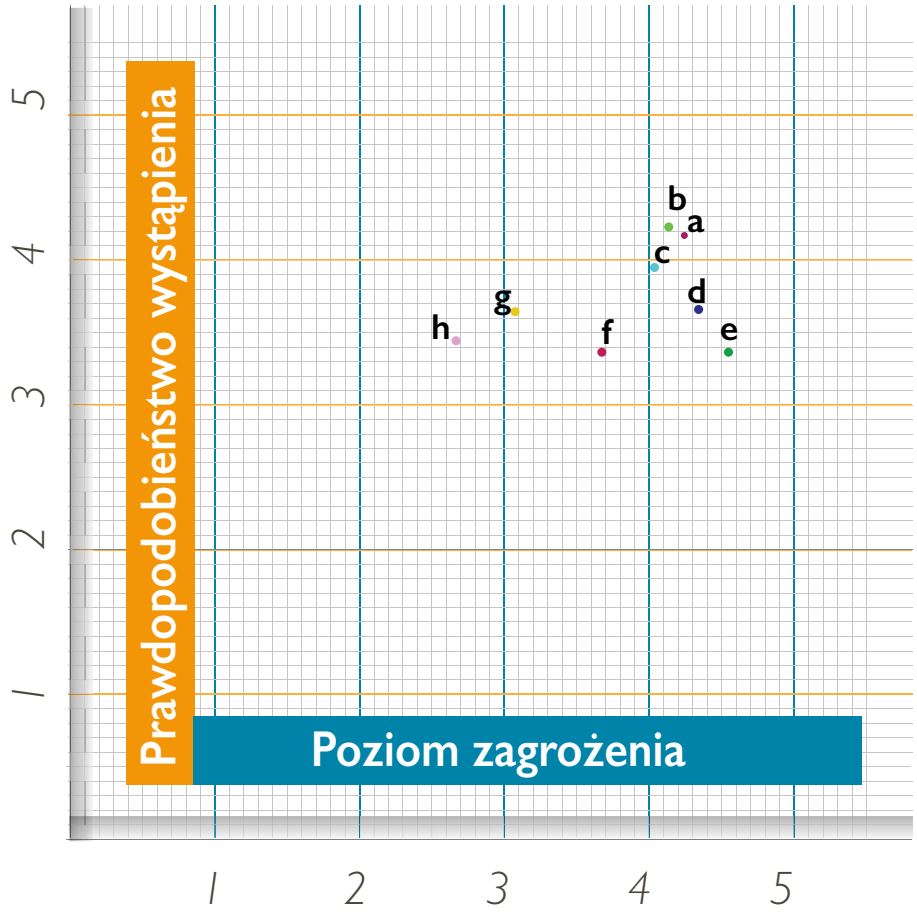
Poziom zagrożenia w przypadku wystąpienia zagrożenia. Porównanie lat 2015 i 2016.



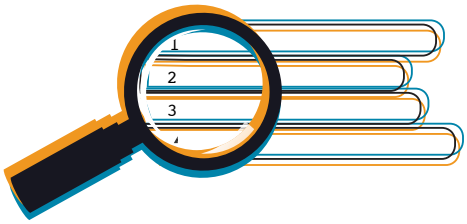
Profilowanie analizy ryzyka dla swojej organizacji

To tylko bardzo uproszczona analiza ryzyka. Każdy sam w zależności od charakteru podmiotu, jaki reprezentuje, i środowiska teleinformatycznego, w jakim działa, powinien takową analizę przeprowadzić na swój użytek. Na przykład profil reprezentacyjny dla instytucji finansowej może wyglądać następująco (tzn. podane poniżej pozycje mogą być wykorzystane do całościowej analizy ryzyka):

Mapa ryzyka na poziomie państwowym



- **a** APT – ataki ukierunkowane na organizacje, połączone ze spear phishingiem
- **b** Wycieki baz danych zawierających dane osobowe, hasła, nr kart kredytowych, itd.
- **c** Akcje cyberszpiegowskie na tle politycznym
- **d** Cyberkonflikty pomiędzy państwami powiązane z atakami dedykowanymi
- **e** Ataki na systemy sterowania przemysłowego ICS/SCADA
- **f** Ataki na system DNS
- **g** Ataki DDoS na administrację publiczną
- **h** Haktywizm



Dariusz Łydziński
Dyrektor ds. audytu i certyfikacji systemów bezpieczeństw
ComCERT.PL

W roku 2015 mieliśmy premierę systemu Windows 10, który udostępniany jest za darmo, co jest powodem rosnącej liczby jego instalacji, co też zapewne przyciągnie uwagę cyberprzestępców, którzy będą się starać wykorzystać szybko słabości nowych systemów operacyjnych. Wzrośnie także zagrożenie w zakresie kluczowych elementów infrastruktury krytycznej powodowane coraz większym zainteresowaniem przemysłowymi systemami sterowania.
Zwiększać się będzie również częstotliwość ataków na urządzenia mobilne, które są coraz powszechniej używane zarówno w życiu prywatnym, jak i służbowym.

Paweł Chwiecko
Vice President
Citi

Sytuacja polityczna na Bliskim Wschodzie oraz zaangażowanie mocarstw w próbę ustabilizowania tej sytuacji wraz z chęcią dominacji w tym procesie w celu osiągnięcia własnych korzyści będzie prowadziło do napięć na tle międzynarodowym (przykład Turcja-Rosja). Cyberkonflikty jak też zaawansowane APT na instytucje rządowe jak też gospodarcze będą się nasilały. Równolegle szpiegostwo gospodarcze (w szczególności prowadzone przez Chiny i Rosję) będzie zagrożeniem, z którym będą musiały liczyć się nawet mniejszego typu organizacje. Niewątpliwie też coraz większym problemem będą stawały się zagrożenia w sieciach społecznościowych połączone z zaawansowanych coraz bardziej dopracowanym phishing i malware prowadzące do kradzieży środków z bankowości elektronicznej.

- Zagrożenia zawiązane z BYOD
- Phishing e-mail and www
- Zagrożenia dla platformy Android
- Zagrożenia dla platformy iOS
- Zagrożenia dla platformy Windows Phone/Mobile
- Zagrożenia typu ransomware/scareware
- Wycieki baz danych zawierających dane osobowe, hasła, nr kart kredytowych, itd.
- Ataki Drive-by Download/Watering Hole
- Ataki na cloud computing
- Ataki na system DNS
- Ataki DDoS na podmioty komercyjne
- APT – ataki ukierunkowane na organizacje, połączone ze spear phishingiem

Taki profil można zastosować również dla większości organizacji o charakterze korporacyjnym, a nawet dla małych i średnich przedsiębiorstw.

Dla odróżnienia, analiza ryzyka dla państwa może uwzględniać następujące pozycje:

- Cyberkonflikty pomiędzy państwami powiązane z atakami dedykowanymi
- Haktywizm
- Wycieki baz danych zawierających dane osobowe, hasła, nr kart kredytowych, itd.
- Ataki na system DNS
- Ataki na systemy sterowania przemysłowego ICS/SCADA
- Ataki DDoS na administrację publiczną
- APT – ataki ukierunkowane na organizacje, połączone ze spear phishingiem
- Akcje cyberszpiegowskie na tle politycznym

To oczywiście tylko próby ujęcia profilowego dla poszczególnych odbiorców. Inne podejście może na przykład zakładać przypisanie wag dla poszczególnych pozycji. Mamy nadzieję, że dane z naszego raportu mogą być w jakimś stopniu przydatne przy tego typu analizach.

Inne możliwe zagrożenia w 2016 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 2016

Propozycje zagrożeń przedstawione przez uczestników badania:

- Ataki na systemy płatności internetowych
- Ataki na sieci bezprzewodowe (WiFi, GSM)
- Zatruwanie informacji w ogólnodostępnych systemach bezpieczeństwa (np.: w serwisach virustotal.com, malwr.com)
- Shadow IT / Insider (nieautoryzowane rozwiązania IT wewnątrz organizacji)
- Inwigilacja realizowana np. poprzez miejski monitoring
- Kompromitacja urządzeń biometrycznych
- Systemy komputerowe instalowane w środkach komunikacyjnych oraz gospodarstwa domowego
- Ataki terrorystyczne wspomagane atakami na infrastrukturę
- Ransomware na platformy serwerowe
- Wykorzystanie podatności w aplikacjach webowych

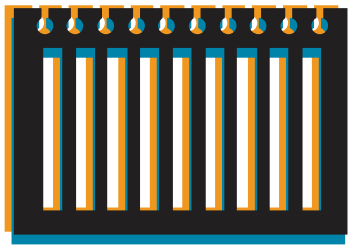
Jarosław Stasiak
Manager Wydziału Bezpieczeństwa IT
mBank SA

W najbliższym czasie uwaga przestępców będzie się prawdopodobnie w dalszym ciągu skupiać na urządzeniach mobilnych. Wpływ na to ma przede wszystkim stale rosnąca popularność tych urządzeń oraz zakres usług świadczonych przez różnych dostawców z wykorzystaniem kanału mobilnego. Nie bez znaczenia jest również fakt niskiej świadomości użytkowników w zakresie skutecznego zabezpieczenia telefonu przed ingerencją złośliwego oprogramowania lub nieuprawnionego, zdalnego dostępu. Już ten rok pokazał, że ilość malware, głównie na system Android, rośnie w zatrważającym tempie, a co raz to nowsze, ujawniane podatności dla tego systemu dodatkowo tylko ułatwiają kolejne ataki. Drugi obszar, który zapewne będzie celem przestępców to poufne, firmowe dane. Tutaj należy spodziewać się kolejnych spektakularnych ataków APT z wykorzystaniem spear phishingu i infiltracją kluczowych osób w danej organizacji, które zapewne ujrzą światło dzienne dopiero po jakimś czasie od jego zaistnienia. Wiele organizacji obecnie „zbroi" się w różnorodne, techniczne systemy, które mają je wspierać w skutecznej walce z tego typu atakami. Możliwości przestępców są niestety jednak ogromne. Dedykowane, złośliwe oprogramowanie wykorzystujące ujawniane 0-day'e , połączone dodatkowo z zaawansowaną socjotechniką sprawiają, że grono potencjalnych odbiorców, których da się skutecznie zaatakować jest duże. Działania osób odpowiedzialnych za bezpieczeństwo powinny się więc w dużej mierze skupiać na niesieniu „kaganka oświaty" i budowaniu świadomości wśród wewnętrznych użytkowników na temat aktualnych zagrożeń w cyberprzestrzeni.

Cezary Piekarski
Head of Security
Bank Millennium

Rok 2015 przyniósł nam dynamiczny rozwój, a także pierwsze znaczne sukcesy i porażki lokalnej cyberprzestępczości. Przynajmniej w warstwie informacji dostępnych publicznie nie ziściły się istotne ryzyka związane z sytuacją geopolityczną oraz potencjalnymi atakami motywowanymi politycznie. W mojej ocenie rok 2016 będzie rokiem dynamicznego, dalszego rozwoju polskiej cyberprzestępczości i będzie to jedno z głównych ryzyk dla sektora finansowego oraz jego Klientów. Oznacza to, że będziemy obserwować zupełnie nowe rodziny złośliwego oprogramowania oraz dobrze przygotowane kampanie ataków celowanych ukierunkowane głównie na małe i średnie przedsiębiorstwa oraz sektor publiczny. Zjawiska te zwiększą

Propozycje przekazane przez ekspertów, choć częściowo znajdujące się w ramach innych zagrożeń, to naszym zdaniem bardzo ciekawe przewidywania. Być może wśród nich warto szukać tego, co w 2016 roku zaskoczy najbardziej. Jak wiadomo te największe zagrożenia w przeszłości były zazwyczaj niespodziankami dla Internautów i większości specjalistów.



Podsumowanie

Przygotowany raport na temat prognoz dotyczących zagrożeń teleinformatycznych w 2016 roku jest czwartą edycją tego raportu po edycjach dotyczących roku 2013, 2014 i 2015. Jednocześnie jest 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.

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 2016 roku. Zgodnie z prostą metodyką analizy ryzyka, najgroźniejsze są te zagrożenia których prawdopodobieństwo wystąpienia jest duże a spowodowane straty poważne.

Wśród nich znajdują się takie jak:

- APT – ataki ukierunkowane na organizacje, połączone ze spear phishingiem (prawdopodobieństwo wystąpienia **4,19** / poziom zagrożenia w przypadku wystąpienia **4,24**)
- Wycieki baz danych zawierających dane osobowe, hasła, nr kart kredytowych, itd. (**4,21** ; **4,12**)
- Akcje cyberszpiegowskie na tle politycznym (**3,95** ; **4,05**)
- Cyberkonflikty pomiędzy państwami powiązane z atakami dedykowanymi (**3,67** ; **4,31**)
- Ataki na systemy sterowania przemysłowego ICS/SCADA (**3,36** ; **4,55**)
- Zagrożenia dla platformy Android (**4,21** ; **3,52**)

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. Skala przewidywań dotyczących tych drugich jest na tyle duża, że można wysnuć wniosek, że zagrożenia dla całości infrastruktury teleinformatycznej państwa to największe wyzwanie. Z pewnością ostatnie lata nie przyniosły tu dobrych informacji, co podsumowali autorzy raportu Najwyższej Izby Kontroli z czerwca 2015 roku. Pozostaje mieć nadzieje, że pojawiające się głosy ze strony administracji państwowej, wskazującej na priorytetowe działania w obszarze cyberbezpieczeństwa, zostaną poparte doświadczeniami roku 2016.

Niewątpliwie wyniki przewidywań ekspertów w dużej mierze pokrywają się z ich obserwacjami zdarzeń z roku poprzedzającego przewidywania. W ten sposób tworzony jest statystyczny obraz, na podstawie którego mało prawdopodobne jest wykrycie pojedynczego zjawiska, które może okazać się dominującym w nowym roku. Dlatego oprócz zapoznania się z danymi statystycznymi, zachęcamy do wczytania się w poszczególne wypowiedzi ekspertów. Być może właśnie w nich się kryje ta najbardziej dojrzała i trafna analiza przyszłych zagrożeń.

Dodatkową wartością, która może być wykorzystana jest zaproponowane przez nas podejście do profilowania ryzyka dla swojej organizacji. Każdy może sam wybrać zestaw, który jego zdaniem najbardziej odpowiada profilowi organizacji, dla której chciałby stworzyć analizę ryzyka.
Takie dane mogą być bardzo przydatne i być punktem wyjścia dla jeszcze bardziej zaawansowanych analiz. Serdecznie zachęcamy do aktywnego wykorzystania danych i informacji z naszego raportu.

Uczestnicy ankiety

Białek Krzysztof – *SOC & CERT Orange Polska Manager / Orange Polska SA*
Boetzel Piotr – *Territory Account Manager / Intel Security*
Bojanowski Jakub – *Partner / Deloitte*
Buczek Arkadiusz – *Specjalista ds. Cyberbezpieczeństwa / T-Mobile Polska SA*
Chendoska Anna – *Kierownik Zespołu Kadr i Administracji, Pełnomocnik ds bezpieczeństwa informacji / Bank Spółdzielczy w Wysokiem Mazowieckiem*
Chmielewski Bartosz – *Inżynier presales / Intel Security*
Chwiećko Pawel – *Vice President / Citi*
Cuch Konrad – *Wiceprezes / Główny Urząd Statystyczny*
Dąbek Dariusz – *Zastępca Dyrektora Departamentu Telekomunikacji / Ministerstwo Cyfryzacji*
Danieluk Adam – *Dyrektor Departamentu Bezpieczeństwa IT w First Data Polska SA*
Dęba Przemysław – *Dyrektor Bezpieczeństwa Systemów Teleinfomratycznych / Orange Polska*
Dworakowski Wojciech – *Partner Zarządzający / SecuRing*
Golak Dawid – *IT Systems Security Lead / Allegro Group*
Jurkiewicz Marek – *Naczelnik wydziału / DepartamenT Bezpieczenstwa Telekomunikacyjnego UKE*
Kasprzyk Rafał – *Adiunkt / Wojskowa Akademia Techniczna*
Kołodziej Maciej – *Konsultant, Administrator Bezpieczeństwa Informacji / FHU MatSoft, E-detektywi.pl*
Konieczny Piotr – *Chief Information Security Officer / Niebezpiecznik*
Kosiński Jerzy – *Profesor / Wyższa Szkoła Policji w Szczytnie*
Kowalewski Jarosław – *Z-ca Dyrektora Pionu Współpracy z Bankami / Zakład Usług Informatycznych NOVUM Sp. z o.o.*
Łącki Borys – *Pentester / LogicalTrust*
Łopaciński Maciej – *Wiceprezes / Agora TC*
Łydziński Dariusz – *Dyrektor ds. audytu i certyfikacji systemów bezpieczeństwa / ComCERT SA*
Maciąg Artur M. – *IT Security Analyst / Sektor Finansowy*
Maj Mirosław – *CEO / CIO / Fundacja Bezpieczna Cyberprzestrzeń / ComCERT.PL*
Miga Błażej – *CERT Allegro / Grupa Allegro Sp. z o.o.*
Miłostan Maciej – *Analityk bezpieczeństwa / Poznańskie Centrum Superkomputerowo-Sieciowe*
Olszar Paweł – *Ekspert zarządzania ryzykiem niefinansowym / ING Bank Śląski*

Pepłoński Jakub – *Kierownik ds. Współpracy z Organami Ścigania / Grupa Allegro sp. z o.o.*
Piekarski Cezary – *Head of Security / Bank Millennium*
Przygoda Michał *Sales Engineer / Intel Security*
Pyznar Maciej – *Szef Wydziału Ochrony Infrastruktury Krytycznej / Rządowe Centrum Bezpieczeństwa*
Sajdak Michał – *Konsultant d/s Bezpieczeństwa IT / Securitum*
Siedlarz Marcin – *Senior Threat Intelligence Analyst / FireEye*
Soczyński Tomasz – *Zastępca Dyrektora Departamentu Informatyki / Biuro GIODO*
Stasiak Jarosław – *Manager Wydziału Bezpieczeństwa IT / mBank S.A.*
Stawowski Mariusz – *Dyrektor ds. usług profesjonalnych / Clico*
Strzyżewski Piotr – *Kierownik zespołu / Centrum Komputerowe Politechniki Śląskiej*
Surgut Krzysztof – *CEO / Data Space Sp. z o.o.*
Świerczyński Zbigniew – *Adiunkt naukowo-dydaktyczny / Wydział Cybernetyki Wojskowej Akademii Technicznej*
Szczypiorski Krzysztof – *Profesor nadzwyczajny / Politechnika Warszawska*
Szydłowski Marcin – *Dyrektor Biura IT / Exatel*
Wach Artur – *CISO, Bank Handlowy w Warszawie SA*

Załączniki

Zagrożenie	Prawdopodobieństwo wystąpienia	Poziom zagrożenia
Cyberkonflikty pomiędzy państwami powiązane z atakami dedykowanymi	3,67	4,31
Zagrożenia zawiązane z BYOD (*Bring Your Own Device*)	3,33	2,90
Phishing e-mail i WWW	4,67	3,37
Haktywizm	3,43	2,67
Powstawanie botnetów opartych o platformy mobilne	3,69	3,17
Zagrożenia w serwisach społecznościowych	3,81	2,88
Zagrożenia dla platformy Android	4,21	3,52
Zagrożenia dla platformy iOS	3,29	3,26
Zagrożenia dla platformy Windows Phone/Mobile	3,20	3,10
Zagrożenia typu ransomware/scareware	3,88	3,36
Wykorzystanie gier sieciowych w atakach	2,90	2,45
Wycieki baz danych zawierających dane osobowe, hasła, nr kart kredytowych, itd.	4,21	4,12
Ataki Drive-by Download Watering Hole	3,71	3,36
Ataki na cloud computing	3,33	3,88
Zagrożenia związane z „Internet of Things"	3,21	3,15
Ataki na platformy hostingowe	3,19	3,37
Ataki na system DNS	3,36	3,69
Kradzież wirtualnych walut	3,52	2,74
Ataki na systemy sterowania przemysłowego ICS/SCADA	3,36	4,55
Ataki DDoS na podmioty komercyjne	3,86	3,50
Ataki DDoS na administrację publiczną	3,61	3,07
Ataki na urządzenia medyczne	2,36	3,95
APT – ataki ukierunkowane na organizacje połączone ze spear phishingiem	4,19	4,24
Akcje cyberszpiegowskie na tle politycznym	3,95	4,05

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

FUNDACJA
bezpieczna
cyberprzestrzeń

NAJWIĘKSZE ZAGROŻENIA DLA BEZPIECZEŃSTWA W INTERNECIE W 2016 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