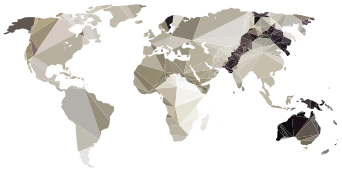
FUNDACJA
bezpieczna
cyberprzestrzeń

# NAJWIĘKSZE ZAGROŻENIA DLA BEZPIECZEŃSTWA W INTERNECIE W ROKU 2014

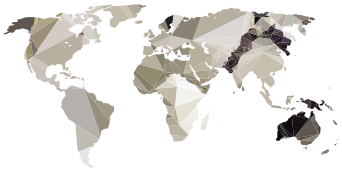
## GŁOS POLSKICH EKSPERTÓW

# RAPORT





# Spis Treści



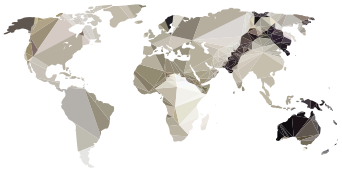


# Wstęp

Co roku, na jego przełomie, oprócz podsumowań pojawiają się prognozy. Nie inaczej jest jeśli chodzi o temat bezpieczeństwa w cyberprzestrzeni. Najważniejsze wydarzenia z dziedziny cyberbezpieczeństwa, w roku który właśnie się skończył to twarde dowody na to, że mówimy o rzeczach poważnych. Natomiast przewidywania, które znajdują się w tym raporcie mają nas uczulić na to co potencjalnie najgroźniejsze. Dla wielu zresztą tego typu opracowania są elementem poważnego planowania budżetów czy działań strategicznych, do czego zachęcamy.

Coroczna lektura raportów przygotowanych przez różne ośrodki zajmujące się bezpieczeństwem teleinformatycznym zainspirowała nas do stworzenia własnego raportu. Tegoroczny raport jest drugim z kolei. Aby był on jak najbardziej solidny, oprócz własnej opinii, ponownie uwzględniliśmy w nim opinie wielu innych specjalistów z dziedziny bezpieczeństwa teleinformatycznego z naszego kraju, których uważamy za autorytety w tej dziedzinie. Tak powstała lista tego co potencjalnie najgroźniejsze w roku 2014. Pojawiające się na przełomie roku tego typu raporty praktycznie niemalże w całości pochodzą z zagranicy. My zdecydowaliśmy się na prezentację głosu polskich specjalistów. Mamy nadzieję, że nasz raport jest ciekawą lekturą, a dla wielu stanie się pożytecznym materiałem, pomocnym w rozważaniach na temat tego co nas czeka w najbliższych miesiącach.

**MIROSŁAW MAJ**
prezes zarządu
Fundacji Bezpieczna Cyberprzestrzeń



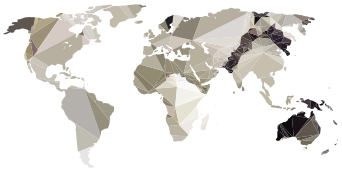


# Metodyka

W celu zebrania opinii eksperckich przygotowana została ankieta. Ankieta zawierała zestawienie potencjalnych zagrożeń w 2014 r. 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 prawdopodobieństwa powszechnego wystąpienia danego zagrożenia oraz poziomu niebezpieczeństwa w przypadku jego wystąpienia. Zestawienie zawierało 16 pozycji:

- Cyberkonflikty pomiędzy państwami powiązane z atakami dedykowanymi (np: Stuxnet)
- Zagrożenia zawiązane z BYOD
- Phishing email and 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 ransome/scareware
- Wykorzystanie gier sieciowych w atakach
- Wycieki baz danych zawierających dane osobowe
- Ataki drive-by download
- Ataki na cloud-computing
- Zagrożenia zawiązane z „Internet of Things"
- Masowe naruszenia prywatności.

W badaniu wzięło udział 23 ekspertów reprezentujących sektory administracji publicznej, organizacji pozarządowych, infrastruktury krytycznej, finansowy i komercyjny, w tym przedstawicieli firm świadczących usługi z zakresu bezpieczeństwa teleinformatycznego.
Odpowiedzi można było nadać wagę poprzez przypisanie punktacji od 1 (waga najmniejsza) do 5 (waga największa). Na koniec każdy z ekspertów poproszony został o wyrażenie swojej opinii w postaci kilku zdań, na temat tego czego możemy się spodziewać i czego najbardziej obawiać w 2014 roku. Większość z ekspertów zdecydowało się na przedstawienie swojej opinii. Opinie te zawarliśmy w naszym raporcie.



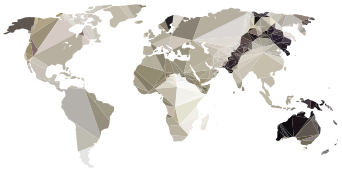


# Przegląd najważniejszych wydarzeń 2013 roku

Przed przystąpieniem do omówienia zagrożeń, które mogą nas spotkać w roku 2014 warto krótko przypomnieć te najważniejsze z zeszłego roku. Niewątpliwie w 2013 r. rzeczą, która przyćmiła wszystkie inne w temacie IT security to sprawa Edwarda Snowdena i wycieków NSA (National Security Agency). Rok 2013 to także między innymi sieciowe konflikty na poziomie międzynarodowym, ataki ukierunkowane, haktywizm. Kolejny już rok z rzędu słyszeliśmy o poważnych włamaniach do firm i wyciekach danych a nasze wszechobecne urządzenia mobilne atakowane są jeszcze częściej.

Edward Snowden były pracownik CIA (Central Intelligence Agency) i NSA, w czerwcu 2013 ujawnił na łamach prasy informacje o PRISM, programie inwigilacji prowadzonym przez NSA. Nie wnikając w wątki polityczne w tej sprawie jedno jest pewne, sensacyjne informacje Edwarda Snowdena sprawiły, że kwestie bezpieczeństwa w sieci Internet stały się dostrzegane już nie tylko przez specjalistów. Od tej pory na temat prywatności i poufności naszych danych prowadzone są niekończące się dyskusje a usługi i serwisy internetowe ułatwiające ochronę prywatnych danych rozkwitają – na przykład obserwujemy to przy okazji wzrostu popularności sieci Tor czy kryptowalut.

Pozostając w temacie kryptowalut. BitCoin to popularna waluta w świecie cyberprzestępczym, jest trudniejsza do monitorowania przez organy ścigania, przez co stanowi bezpieczniejszą, anonimową metodę płatności. Tam, gdzie można zarobić pieniądze kwitnie przestępczość. Tak jest również w przypadku Bitcoinów i z uwagi właśnie na to w 2013 kryptowaluty były w kręgu zainteresowań branży bezpieczeństwa.



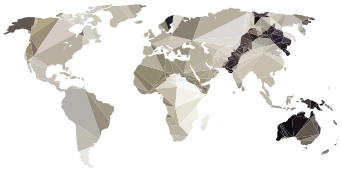


W kwietniu Kaspersky Lab wykrył kampanię, w której cyberprzestępcy wykorzystywali Skype'a do dystrybucji szkodliwego oprogramowania w celu wydobywania Bitcoinów. Cyberprzestępcy stosowali socjotechnikę jako początkowy wektor ataku i pobierali kolejne szkodliwe oprogramowanie do zainstalowania na maszynie ofiary. Współczynnik kliknięć w kampanii wynosił 2 000 na godzinę!

Na początku roku 2013, w lutym, dla wszystkich sensacją była publikacja raportu Mandianta na temat chińskich ataków APT (Advanced Persistent Threats). Amerykańska firma Mandiant zajmująca się analizą ruchu internetowego i cyber – bezpieczeństwem w swoim raporcie opisała włamania przedstawicieli Chińskiej Republiki Ludowej do baz danych organizacji działających głównie w USA, Kanadzie i Wielkiej Brytanii i wykradzenie z nich setek terabajtów danych. W raporcie opisano systematyczne kradzieże danych z co najmniej 141 firm skupionych w branżach uważanych przez chińczyków jako strategiczne: zbrojeniowej, energetycznej i medialnej. Ujawnione dane z raportu Mandianta dają do myślenia, czy możemy już użyć stwierdzenia, że pojęcie ,,wojen cybernetycznych'' to już fakt a nie termin używany w literaturze?

Również przykładem ataku ukierunkowanego APT jest ujawniony w czerwcu nowy wektor ataków o nazwie NetTraveler, który zainfekował setki ofiar stanowiących znane osoby wysokiego szczebla mieszkające w ponad 40 krajach.

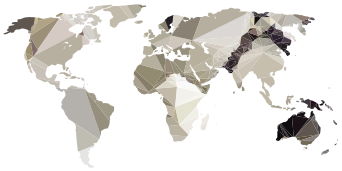
Rok 2013 to ponownie włamanie do firm i wycieki danych: włamanie do Adobe, włamanie do Opery, niemieckiego Vodafone czy do serwisu Evernote. Największe z nich to włamanie do Adobe - ponad 150 milionów wierszy z danymi. Niewątpliwie mamy tu do czynienia z największym do tej pory, opublikowanym i pochodzącym z jednego serwisu wyciekiem listy kont, adresów e-mail i zabezpieczonych haseł.





Omawiając najważniejsze wydarzenia roku 2013 nie można pominąć sprawy dynamicznego wzrostu zagrożeń dla platform mobilnych, a głównie popularnego systemu Android. Według Kaspersky Lab, trzeci kwartał minionego roku upłynął pod znakiem mobilnych botnetów, w połowie lipca 2013 r. zidentyfikowano pierwsze botnety osób trzecich, tj. mobilne urządzenia zainfekowane innymi szkodliwymi programami i wykorzystywane przez innych cyberprzestępców do rozprzestrzeniania mobilnego szkodliwego oprogramowania i tak rozprzestrzeniany był najbardziej wyrafinowany trojan dla Androida, znany jako Obad. Mobilne szkodliwe oprogramowanie jest zwykle wykorzystywane do kradzieży pieniędzy właścicieli telefonów. W III kwartale pojawił się nowy szkodliwy program, który pozwala cyberprzestępcom kraść pieniądze z kont bankowych ofiar, jak również z ich kont na telefonach komórkowych.

Przeprowadzone przez analityków Trend Micro badania wskazują, że w ciągu ostatnich miesięcy liczba złośliwego oprogramowania i aplikacji, które są niebezpieczne dla użytkowników systemu Android, przekroczyła 1 milion. W trzecim kwartale analitycy Trend Micro zidentyfikowali ponad 200 tys. przypadków infekcji złośliwym oprogramowaniem wymierzonych w systemy bankowości internetowej. Poza liczebnością ataków wzrosła także liczba wyszukanych technik kamuflażu wykorzystywanych przez przestępców. Ta tendencja obserwowana jest także w krajach Europy Środkowo-Wschodniej. Rosnąca popularność smartfonów w tym regionie spowodowała dynamiczny rozwój zagrożeń skierowanych w użytkowników mobilnych usług bankowych.

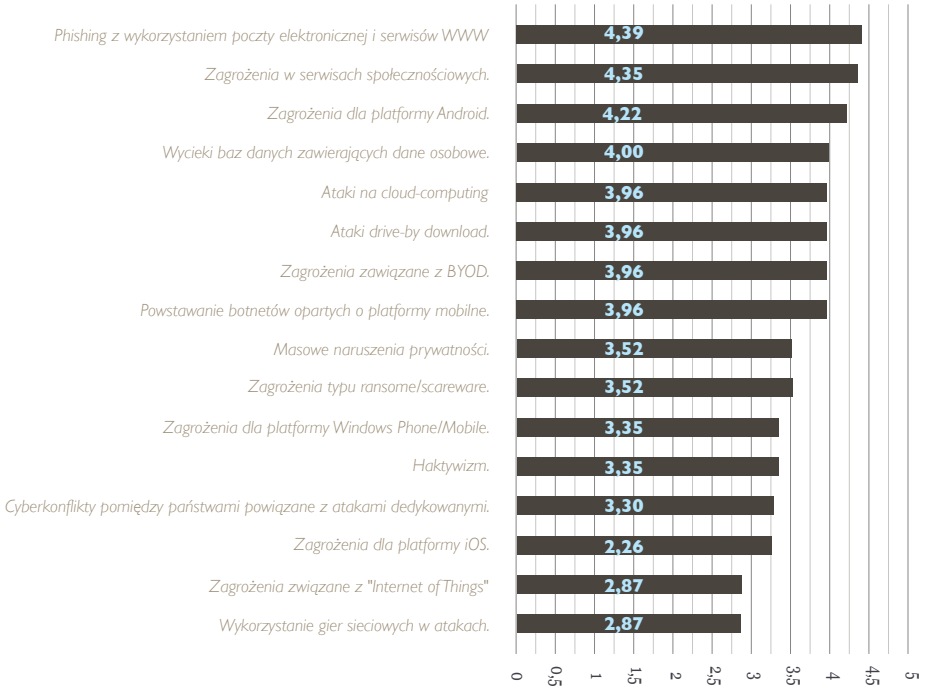


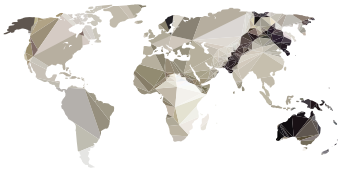


# Najwieksze zagrożenia w roku 2014 – prawdopodobieństwo wystąpienia

Po tym szybkim podsumowaniu roku 2013 przejdźmy do prognoz dotyczących roku 2014. Zaproponowaliśmy do oceny zestawienie tego co najczęściej pojawia się w dyskusjach o tegorocznych zagrożeniach, zestawienie poparte jest naszą opinią na ten temat. Każdy z ekspertów miał możliwość zgłoszenia dodatkowych zagrożeń jeśli uznał, że ominęliśmy jego „faworyta". Większość kategorii wydaje się dość oczywista. Zobaczmy jednak wyniki podsumowujące odpowiedzi na pytanie o zagrożenia, które będą w dopiero co rozpoczętym roku najbardziej powszechne.

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







## Na czoło klasyfikacji wybijają się trzy kategorie[1] :

- Phishing z wykorzystaniem poczty elektronicznej i serwisów WWW – **4.39**
- Zagrożenia w serwisach społecznościowych – **4.35**
- Zagrożenia dla platformy Android – **4.22**

Jak widać z tego zestawienia – zagrożenie które jest wręcz klasycznym od wielu lat, czyli akcje phishingowe z wykorzystaniem poczty elektronicznej i serwisów WWW – wygrywa konkurencję. Ta opinia ekspertów to potwierdzenie kontynuacji tego trendu, który jest już bardzo długi. Jak widać nie ma oczekiwania, że wiele się tutaj zmieni. Obserwacje zdają się potwierdzać taką możliwość. Mamy do czynienia z zagrożeniem, które jest bardzo systematyczne i dodatkowo trudno je wyeliminować. 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 komputerowych.

Właściwie te same negatywne czynniki decydują o sukcesie propagacji zagrożeń w serwisach społecznościowych. Warto sobie jasno powiedzieć, że mamy na myśli głównie wszechpanującego Facebooka. W tym przypadku jest chyba jeszcze z większym znaczeniem czynnika socjotechnicznego. Prawie każdy z posiadaczy konta w serwisie społeczościowym widział zachowanie swojego „znajomego", który prowadzony ciekawością związaną z zapoznaniem się z jakimś „interesującym filmikiem" doprowadzał do infekcji swojego komputera. W tle tego zagrożenia warto wspomnieć o całej masie danych na temat użytkowników pobieranych przez "ciekawskie" aplikacje z serwisów społecznościowych.

Zagrożenia związane z systemem operacyjnym Android to trzecia pozycja wśród liderów zagrożeń. Ta opinia nie dziwi. Według wielu statystyk liczba infekcji telefonów komórkowych przyrasta wręcz lawinowo osiągając kilkusetprocentowy wzrost w roku ubiegłym.

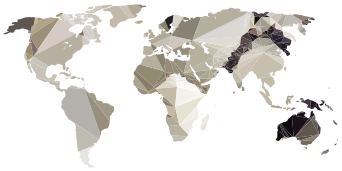
[1] wszystkie wartości oceny odnoszą się do skali **1-5** (**1** – najmniejsze prawdopodobieństwo, **5** – największe prawdopodobieństwo).

*Śmiałe kroki w kierunku przenoszenia różnych form biznesu do kanałów elektronicznych i obsługiwania ich przez coraz to bardziej innowacyjne urządzenia końcowe, będą z pewnością jednymi z wyzwań w 2014 roku. Standardowo nie należy zapominać o złośliwym oprogramowaniu, które pomimo stałej ewolucji, ciągle korzysta ze sprawdzonych w przeszłości elementów socjotechnicznych, bazujących na słabości – nie systemów informatycznych a konkretnie człowieka. Dodatkowo propagowany obecnie trend związany z „BYOD" w miejscach pracy, zestawiony z tzw. „higieną informatyczną" takich urządzeń prywatnych oraz brakiem odpowiednich środków proceduralnych, wskazuje na szereg możliwych zagrożeń czy nadużyć, w stosunku do urządzeń firmowych znajdujących się pod znacznie „większą" ochroną i kontrolą. Jak pokazuje przykład ostatnich lat, powinniśmy jednak zostawić pewną przestrzeń na branżowe „niespodzianki", dlatego też wszelkie elementy pro-aktywne muszą obowiązkowo towarzyszyć w naszych codziennych działaniach.*

*Marek Antczak / mBank SA*

*W roku 2014 należy się spodziewać gwałtownego rozwoju zagrożeń dotyczących platform mobilnych. Coraz więcej cennych informacji przechowujemy na swoich smartfonach lub tabletach i są to często urządzenia służące do dostępu do sieci firmowych. Cyberprzestępcy będą chcieli to wykorzystać a zabezpieczenie tych urządzeń stanie się w roku 2014 świadomym celem użytkowników.*

*Arkadiusz Buczek / T-Mobile Polska SA*





Infekcje Androida to minimum 90% wszystkich infekcji. Pozostałe platformy z naszego zestawienia – t.j. iOS i Windows Phone/Mobile nie postrzegane są jako aż tak niebezpieczne. Oczywiście tak dalej być nie musi, ale trudno na razie znaleźć przesłanki tego, że ten trend się zmieni. W tej sprawie warto apelować o powszechne wyrobienie odruchu aktualizacji systemu, a być może nawet aktualizacji automatycznej. Dane pokazują, że posiadanie najnowszej wersji systemu znacznie zredukowałoby liczbę infekcji.

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

- Wykorzystanie gier sieciowych w atakach – **2.87**
- Zagrożenia związane z „Internet of Things" – **2.87**

Jak widać nadal gry sieciowe postrzegane są jako oaza względnego spokoju. Choć niekoniecznie tak musi być dalej. Na razie słyszymy, o tym że GVE-y (Games and Virtual Environments) powszechnie wykorzystywane są przez agencje wywiadowcze do prowadzenia działalności operacyjnej[2]. Częstsze informacje o kradzieży zasobów wirtualnych w GVE czy przejmowaniu w nich komputerów grających mogą pojawić się w każdym momencie.
„Internet of Things" tak naprawdę dopiero zaczyna wkraczać do naszego życia. Stąd pewnie nie za bardzo oczekujemy zagrożeń z tej strony. To się też może zmienić jeśli urządzenia staną się bardziej powszechne. Właśnie pojawiła się informacja o pierwszej lodówce, dołączonej do botnetu i rozsyłającej spam[3].

*Rok 2014 może przynieść duże zagrożenie na poziomie globalnym związane z potencjalnymi konfliktami na Bliskim Wschodzie. Mam tu na myśli głównie Iran i Izrael. Cyber-konflikt będzie nieodzownym elementem scenariusza takiego konfliktu. Pośród innych zagrożeń widzę masowe ataki typu DDoS na instytucje zaufania publicznego, jak urzędy i banki. Będą do tego wykorzystywane głównie przejęte systemy hostowane w centrach danych dysponujące dużą przepustowością do sieci Internet. Spowoduje to kontynuację trendu wzrostowego przepustowości ataków i będzie to bardzo widoczne w Polsce. Dotychczasowe ataki DDoS w kraju na poziomie do 6Gbps przerodzą się w ataki na poziomie 10Gbps+. Do listy zagrożeń o których będzie głośno dodałbym także te związane z portalami skocznościowymi oraz masowe wycieki danych.*
*Paweł Chwiećko / Citi*

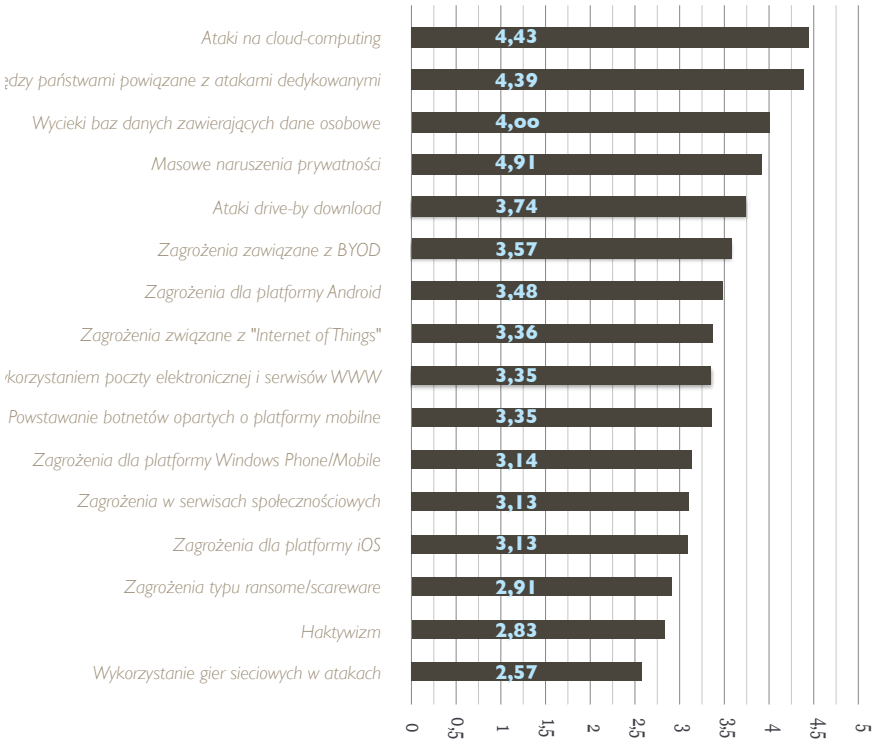
*Zagrożenie atakami wymagającymi wiedzy i doświadczenia z całą pewnością istnieje, niemniej do momentu do kiedy podstawowe zabezpieczenia nie staną się normą dla firm i pozostałych organizacji, więcej szkody przyniesie niefrasobliwość administratora systemu, który nie aktualizuje systemu, aplikacji, i nie zmienia domyślnych ustawień systemu, niż złożone ukierunkowane ataki.*
*Adam Danieluk / ISSA Polska*

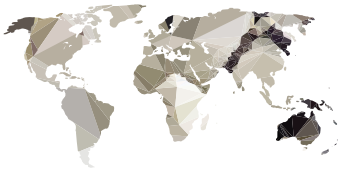
[2] http://www.propublica.org/article/world-of-spycraft-intelligence-agencies-spied-in-online-games
[3] http://www.businessinsider.com/hackers-use-a-refridgerator-to-attack-businesses-2014-1

# Najwieksze zagrożenia w roku 2014 – poziom zagrożenia

Prawdopodobieństwo wystąpienia to jedno, ale siła oddziaływania danego zagrożenia to drugie. Nie wszystkie zagrożenia wskazywane jako najbardziej prawdopodobne były jednocześnie wskazywane 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 trzy pozycje osiągnęły wartość co najmniej 4 w skali 1-5. Były nimi:

- Ataki na claud computing - **4.43**
- Cyberkonflikty pomiędzy państwami powiązane z atakami dedykowanymi – **4.39**
- Wycieki baz danych zawierające dane osobowe – **4.00**

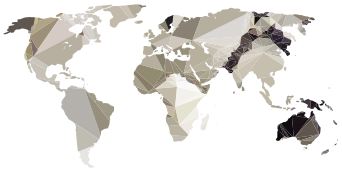
Zdaje się, że żadna z tych pozycji nie dziwi. Ciekawym spostrzeżeniem jest to, że każdą z nich można by przypisać innej kategorii użytkownika. Cloud computing to biznes, Cyberkonflikty – struktury państwowe a wycieki baz danych osobowych w konsekwencji najbardziej mogą dotyczyć użytkowników indywidualnych. Przy niewielkiej dozie wyobraźni można by też pokazać jak wszystkie te ataki mogą się łączyć. Na przykład: wiadomo, że od pewnego czasu cyberprzestępcy zaczęli masowo wykorzystywać centra danych do swojej działalności, np.: uruchamianiu ataków DDoS. Te ataki często skierowane są na serwery rządowe, a przy okazji włamań do centrów danych mogą następować również ataki na instalowane w nich rozwiązania „chmurowe" i kradzież przetwarzanych w nich danych osobowych. Taki scenariusz to jeden z licznych dowodów na to, że systemy informatyczne, ataki na nie, metody obrony to olbrzymi system naczyń połączonych często następuje synergia pewnych działań jak również wzajemne oddziaływanie ich na siebie.

*W 2014 spodziewam się spektakularnych przykładów ataków na urządzenia stanowiące "internet rzeczy". Obecna sytuacja kojarzy mi się z tą sprzed 20 lat, kiedy lawinowo zaczęła rosnąć liczba komputerów podłączonych do Internetu, a prawie nikt nie miał pojęcia, jakie czyhają na nie zagrożenia. Wiele lat musiało minąć, zanim opracowano i wdrożono przynajmniej częściowo skuteczne mechanizmy bezpieczeństwa. Niestety nie uczymy się na własnych błędach i nie myśląc o bezpieczeństwie, a kierując się własną wygodą, najchętniej podłączylibyśmy do sieci nie tylko telefon, telewizor i kamerę, ale także pralkę, lodówkę i samochód. Któregoś dnia możemy tego pożałować.*

*Adam Haertle / UPC Polska sp. z o.o.*

*Podobnie jak w roku ubiegłym, również w 2014 spodziewane jest zamieszanie formalno-prawne w Polsce i Europie, ponieważ wiele ważnych przepisów jest w toku nowelizacji, a użytkownicy cyberprzestrzeni są zmęczeni sprzecznymi komunikatami, niejasna przyszłością dla biznesu i nie są gotowi na zmiany, szczególnie że są one nieprecyzyjnie definiowane już na etapie tworzenia prawa. Przykładem jest planowana nowelizacja polskiego prawa świadczenia usług droga elektroniczna, prawa autorskiego, regulacji dla nadawców multimediów oraz przepisów technicznych i organizacyjnych dotyczących ochrony danych osobowych.*

*Maciej Kołodziej / FHU MatSoft, ComCERT SA*





Na dole rankingu zagrożeń o największych konsekwencjach znajdują się:

- Wykorzystanie gier sieciowych – **2.57**
- Haktywizm – **2.83**
- Zagrożenia typu ransome/scareware – **2.91**

Ta niska ocena to zapewne wynik brak bardzo negatywnych doświadczeń z konsekwencjami w przypadku zagrożeń związanych z grami sieciowymi czy haktywizmem. 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.

*Urządzenia mobilne są coraz aktywniej wykorzystywane nie tylko do zabawy, ale i do wspomagania procesów biznesowych w firmach. Obawiam się, że trudności związane z aktualizowaniem Androida na smartphonach boleśnie odczują w tym roku na własnej skórze firmy, które dopuszczają pracę w modelu BYOD. Mobilny malware staje się coraz bardziej powszechny. Rzeczą której jednak obawiam się najbardziej jest popularyzacja podłączania do Internetu wszystkiego, od "elektronicznych niań" poprzez drony aż do domowych lodówek. Te produkty, z racji swojej "innowacyjności" i dynamicznego rozwoju, często działają pod kontrolą niedostatecznie przetestowanego oprogramowania, które zawiera błędy umożliwiające atakującemu na przejęcie całkowitej kontroli nad urządzeniem, co w konsekwencji powoduje otwarcie wrót do naszej domowej sieci.*

*Piotr Konieczny / Niebezpiecznik.pl*

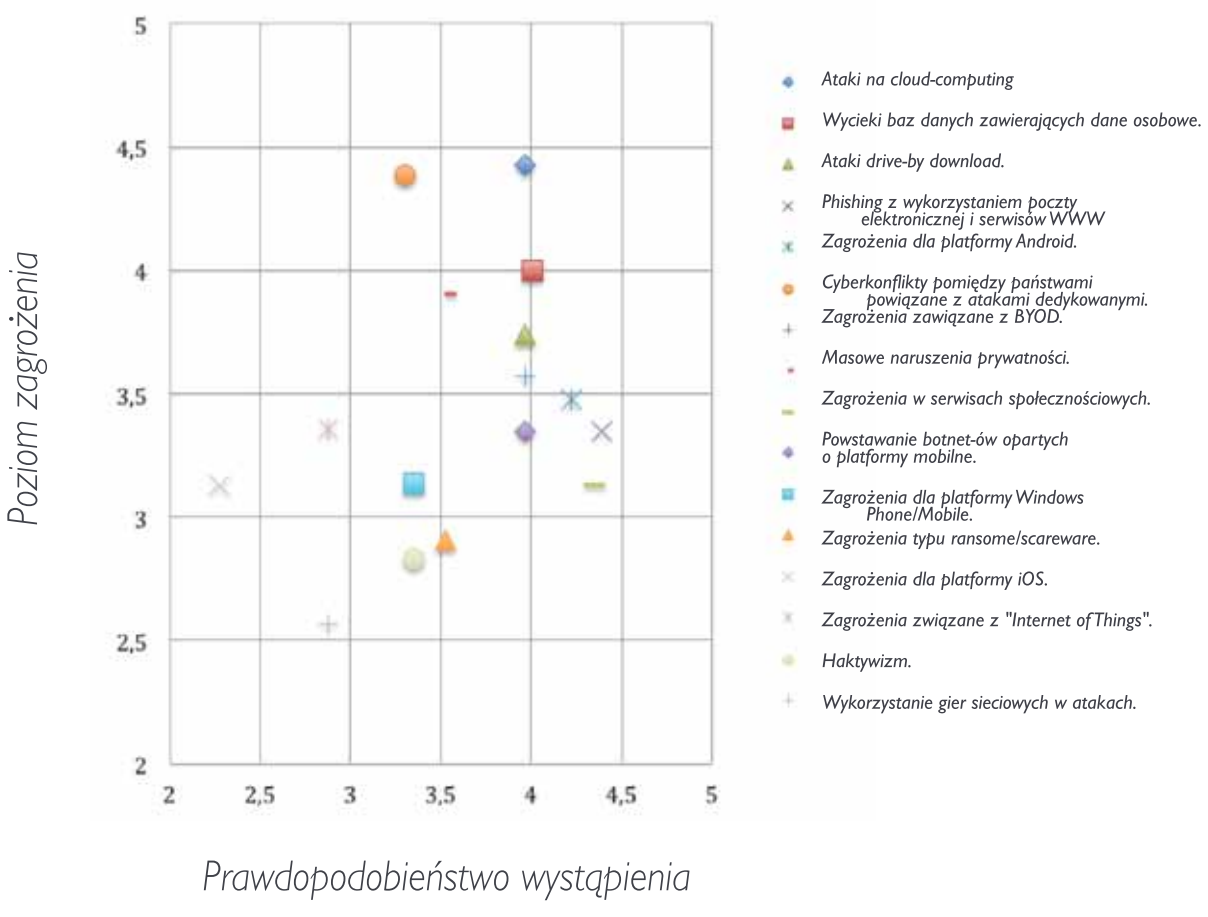
*Myślę, że obawiać należy się rzeczywistych albo wymyślonych zagrożeń powiązanych z żądaniami "okupu, odszkodowania, zapłaty za usługę" w kryptowalutach. To nie jest chyba zagrożenie, a raczej motywacja. Wykorzystania narzędzi i usług anonimizujących do tego co określa się mową nienawiści.*

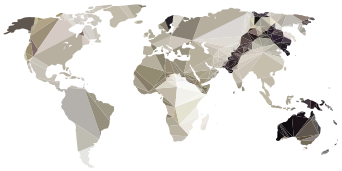
*Jerzy Kosiński / Wyższa Szkoła Policji w Szczytnie*

# Na co więc zwrócić uwagę najbardziej?

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 2014. Zgodnie z prostą metodyką analizy ryzyka, najgroźniejsze są te zagrożenia których prawdopodobieństwo wystąpienia jest duże a spowodowane straty poważne.

## Zagrożenia teleinformatyczne 2014 roku.







Warto więc najbardziej się przyjrzeć właśnie tym zagrożeniom. Wśród nich znajdują się takie jak:

- ataki na cloud-computing (prawdopodobieństwo – **3.96,** poziom zagrożenia – **4.43**)
- wycieki baz danych zawierające dane osobowe (**4.00, 4.00**)
- ataki drive-by download (**3.96, 3.74**)
- Phishing z wykorzystaniem poczty elektronicznej i serwisów WWW (**4.22, 3.48**)
- Zagrożenia dla platformy Android (**4.22, 3.48**)

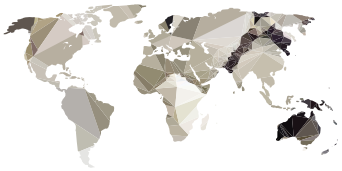
Taka uproszona analiza ryzyka to oczywiście tylko proste kalkulacje. Każdy sam w zależności od charakteru podmiotu jaki reprezentuje i środowiska teleinformatycznego w jakim działa powinien takową przeprowadzić na swój użytek. Mamy nadzieję, że dane z naszego raportu mogą być w jakimś stopniu przydatne przy tego typu analizach.

*Cyberprzestępcy zrozumieli, że kradzież wirtualnych dóbr wiąże się niewielką inwestycją, niskim ryzykiem wykrycia i skazania sprawcy oraz szansą na olbrzymie dochody. W roku 2014 spodziewam się wzrostu cyberprzestępczości, szczególnie w obszarach, które umożliwią finansowe wzbogacanie się złodziei. Urządzenia mobilne, phishing oraz ransomware, waluty typu BitCoin, ataki wymierzone w graczy oraz kierowane ataki w małe i duże firmy, to obszary, w których zaobserwujemy wzmożoną aktywność w 2014 roku.*

*Borys Łącki / Logicaltrust*

*W świetle informatyzacji instytucji administracji publicznej warto zwrócić uwagę na wzrastające ryzyko wycieków danych osobowych i danych wrażliwych np. związanych z pobieranymi świadczeniami leczniczymi. Zasadnicze znaczenie ma tu czynnik ludzki, czyli ewentualna nienależyta ochrona danych dostępowych przez użytkowników portali. Natomiast patrząc przez pryzmat dynamicznego rozwoju sektora mediów społecznościowych i technologii mobilnych, można się w najbliższym roku spodziewać dwóch rzeczy. Po pierwsze, wzrostu nadużyć związanych z danymi udostępnianymi na portalach społecznościowych przez beztroskich użytkowników. Po drugie, ekspansji kolejnych wersji złośliwego oprogramowania, na wszystkie popularne na rynku platformy mobilne.*

*Maciej Miłostan / PIONIER-CERT/PCSS*





# Inne możliwe zagrożenia w roku 2014.

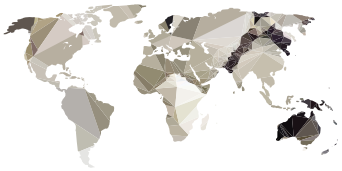
Eksperci, którzy wzięli udział w naszym badaniu, oprócz wskazanych zagrożeń w zestawieniu, zaproponowali również własne. Wśród nich najczęściej pojawiają się dwa: ataki typu DDoS oraz ataki na systemy sterowania przemysłowego typu SCADA. Nie sposób się z tym nie zgodzić. W szczególności z pozycją pierwszą, która pojawia się często zapewne również ze względu na wiele szkód jakie te ataki poczyniły w Polsce w 2013 r. Ataki na dobre zagościły w „polskim Internecie" i stały się zmorą dla wielu bardzo dużych ale także i małych podmiotów. Biorąc pod uwagę ich „komercyjny" aspekt związany z żądaniem okupu przez atakujących, rzeczywiście trzeba bardzo poważnie rozpatrywać to ryzyko. Jeden z ekspertów wymienił nawet pojawienie się zagrożenia „DDoS As a Service".
Oprócz tych dwóch najczęściej pojawiających się – eksperci wskazali kilka innych ciekawych. Na przykład:

- Ingerencje służb w Internet powodujące utratę zaufania ludzi do sieci i usług sieciowych
- Ataki na urządzenia medyczne I instalacje podtrzymujące życie
- Kradzież walut typu BitCoin
- Backdoory w powszechnie wykorzystywanych algorytmach
- Nowe mechanizmy w rozwoju złośliwego oprogramowania (wykorzystanie sieci anonimowych, destrukcja komputera przy próbie zablokowania botnetu, etc.)
- Sniffing w punktach wymianu ruchu
- DNS hijacking

To bardzo ciekawe przewidywania. Być może wśród nich warto szukać tego co w 2014 roku zaskoczy najbardziej. Jak wiadomo te największe zagrożenia w przeszłości były zazwyczaj niespodziankami dla Internautów i większości specjalistów.

*Rok 2014 będzie obfitował w wydarzenia związane z bezpieczeństwem w Internecie. Moim zdaniem dzięki coraz większej dostępności i prostocie narzędzi służących przełamywaniu zabezpieczeń czy przeprowadzaniu ataków typu DDoS (np. w modelu botnet-as-a-service) zagrożenia te staną się powszechniejsze. Zaobserwujemy nowe rodzaje ataków phishingowych wykorzystujących rosnący strach przed inwigilacją w Internecie, a prace nad nowymi metodami ochrony przed nadzorem ze strony "służb" będą przykuwały uwagę sektora oraz mediów głównego nurtu. Polski sektor usług finansowych zmierzy się z bardziej zaawansowanymi atakami niebędącymi jedynie lokalną wariacją globalnych zagrożeń, a dedykowanymi atakami na wybraną usługę w kanale elektronicznym. Być może atak ten dotknie coraz popularniejszych a jednocześnie będących wciąż mało zbadanymi systemów płatności mobilnych. Z podobnymi zagrożeniami będą musieli zmierzyć się użytkownicy i operatorzy walut wirtualnych. Istnieje ryzyko, że łatwość kradzieży walut wirtualnych oraz kruche zaufanie użytkowników spowoduje upadek jednego z największych operatorów lub nawet jednej z głównych wirtualnych walut. Jako odpowiedź na ewoluujące zagrożenia zaobserwujemy rosnącą presję regulacyjną (szczególnie w sektorze finansowym) oraz inicjatywy ponad sektorowe zmierzające do zapewnienia wspólnej platformy przeciwdziałania atakom w sieci. Nie wierzę, żeby którakolwiek z tych inicjatyw zakończyła się w 2014 r., ale podwaliny oraz grupy inicjatywne zbudowane w tym roku będą pracowały na dalszy sukces rozpoczętych przedsięwzięć.* *Cezary Piekarski / Deloitte Polska*

*Obecnie szybko zmieniający się świat i technologię, z których korzystamy dają nowe możliwości na wykazanie się nie tylko atakującym ale przede wszystkim osobom od bezpieczeństwa. Tendencja związana z pojawianiem się nowych form i sposobów ataków nie zmieni się, a wręcz przyspieszy. Miejmy nadzieje, że nadąży za tym poziom świadomości użytkowników także w obszarze ochrony prywatności.*
*Artur Ślubowski / RWE Polska*





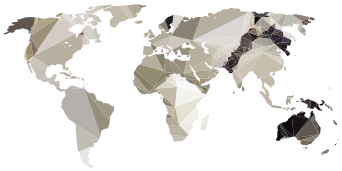
# Podsumowanie

Przygotowany raport na temat prognoz dotyczących zagrożeń teleinformatycznych w 2014 r. jest drugą edycją tego typu raportu po edycji dotyczącej roku 2013. Jednocześnie jest najprawdopodobniej pierwszym tego typu raportem, na wyniki którego składają się 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 nadchodzącym roku powinniśmy w szczególny sposób obawiać się **zagrożeń związanych z atakami na centra przetwarzania danych, w których świadczone są usługi „chmurowe".** Szczególnej uwadze powinny podlegać również wszelkie **zagrożenia związane z naruszaniem prywatności,** np.: poprzez wyciek baz danych zawierających dane osobowe. Kontynuowane mogą być zagrożenia dotyczące **phishingu i techniki infekcji określanej jako „drive-by download".** Natomiast **zagrożenia dla systemu Android** mogą kontynuować dość przerażającą dynamikę wzrostu.

*Znacząco rośnie liczba złośliwego oprogramowania na platformy mobilne, co w powiązaniu z coraz szerszym wdrażaniem ich w przedsiębiorstwach oraz z promocją BYOD zrodzi poważne zagrożenia dla poufności danych. Będzie przybywać incydentów kradzieży danych osobowych, coraz prościej przerobić je na pieniądze.*
*Tadeusz Włodarczyk / PSE SA*

*Myślę, że kontynuowany będzie wzrost zagrożeń związany z urządzeniami mobilnymi, które praktycznie stały się urządzeniami powszechnymi. Kolejnym obszarem mocnego zainteresowania cyberprzestępców mogą być zasoby przetrzymywane w tzw. "chmurze". Atak na "chmurę" podobnie jak na urządzenia mobilne może być niezwykle efektywny i dlatego przestępcy dołożą dużo wysiłków aby go realizować. W dziedzinie zagrożeń makro uważam, że możemy mieć pewne znaczące objawy powszechnego przyśpieszenia cyber-zbrojeń. Niewykluczone, że państwa, które przeznaczyły na to olbrzymie budżety zaczną testować swoje rozwiązania. Uważam też, że małe i średnie firmy czeka problem ataków typu DDoS. W ostatnim okresie wielcy zaczęli sobie z tym powoli radzić inwestując miliony w infrastrukturę. Mniejszych podmiotów nie stać na takie inwestycje. Natomiast duzi będą mieli coraz większy problem z atakami typu APT (Advanced Persistant Threat), czyli atakami dedykowanymi. Mirosław Maj / Fundacja Bezpieczna Cyberprzestrzeń / ComCERT SA*





# Uczestnicy ankiety

**Marek Antczak** - *Główny specjalista ds. bezpieczeństwa IT* - mBank S.A.

**Arkadiusz Buczek** - *Specjalista ds. Cyberbezpieczeństwa* - T-Mobile Polska S.A.

**Anna Chendoska** - *Kierownik Zespołku Kadr i Organoizacji, Pełnomocnik ZSZ: 9001;2008, 27001;2005* - Bank Spółdzielczy w Wysokiem Mazowieckiem

**Paweł Chwiećko** - *Vice President, Senior Security Engineer* - Citi

**Adam Danieluk** - *Prezes ISSA Polska*

**Przemysław Frasunek** - *Dyrektor Działu Rozwiązań Multimedialnych* - Atende Software sp. z o.o.

**Slawomir Górniak** - *Expert in Security Tools and Architecture* - ENISA

**Adam Haertle** - *Kierownik ds. Bezpieczeństwa Informacji* - UPC Polska sp. z o.o.

**Maciej Kołodziej** - *Konsultant, ABI* - FHU MatSoft, ComCERT

**Piotr Konieczny** - *CISO* - Niebezpiecznik.pl

**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** - *Audytor/Pentester* - Logicaltrust

**Maciej Łopaciński** - *Wiceprezes* - Agora TC

**Mirosław Maj** - *Prezes* Fundacji Bezpieczna Cyberprzestrzeń, *CIO* ComCERT SA

**Maciej Miłostan** - *Analityk bezpieczeństwa* - PIONIER-CERT/PCSS

**Paweł Olszar** - *Ekspert zarządzania ryzykiem niefinansowym w pionie bezpieczeństwa* - ING Bank Śląski

**Cezary Piekarski** - *Senior Manager* - Deloitte

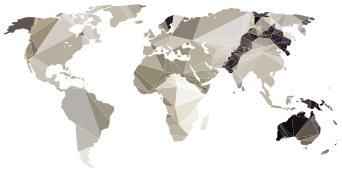
**Jarosław Stasiak** - *Manager, Wydział Bezpieczeństwa IT* - mBank S.A.

**Artur Ślubowski** - *Information Security Officer* - RWE Polska

**Zbigniew Świerczyński** - *Adiunkt* - Wydział Cybernetyki Wojskowej Akademii Technicznej

**Artur Wach** - *Dyrektor Departamentu Bezpieczeństwa Systemów Informatycznych i Zarządzania Dostawcami* - Bank Handlowy w Warszawie SA

**Tadeusz Włodarczyk** - *Główny specjalista* - PSE S.A.





# Załączniki

| Zagrożenie | Prawdopodobieństwo wystąpienia | Poziom zagrożenia |
|---|---|---|
| Ataki na cloud-computing | 3,96 | 4,43 |
| Wycieki baz danych zawierających dane osobowe. | 4,00 | 4,00 |
| Ataki drive-by download. | 3,96 | 3,74 |
| Phishing z wykorzystaniem poczty elektronicznej i serwisów WWW | 4,39 | 3,35 |
| Zagrożenia dla platformy Android. | 4,22 | 3,48 |
| Cyberkonflikty pomiędzy państwami powiązane z atakami dedykowanymi. | 3,30 | 4,39 |
| Zagrożenia zawiązane z BYOD. | 3,96 | 3,57 |
| Masowe naruszenia prywatności. | 3,52 | 3,91 |
| Zagrożenia w serwisach społecznościowych. | 4,35 | 3,13 |
| Powstawanie botnet-ów opartych o platformy mobilne. | 3,96 | 3,35 |
| Zagrożenia dla platformy Windows Phone/Mobile. | 3,35 | 3,14 |
| Zagrożenia typu ransome/scareware. | 3,52 | 2,91 |
| Zagrożenia dla platformy iOS. | 2,26 | 3,13 |
| Zagrożenia związane z "Internet of Things". | 2,87 | 3,36 |
| Haktywizm. | 3,35 | 2,83 |

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

FUNDACJA
bezpieczna
cyberprzestrzeń

# NAJWIĘKSZE ZAGROŻENIA DLA BEZPIECZEŃSTWA W INTERNECIE W ROKU 2014

## GŁOS POLSKICH EKSPERTÓW

© Copyright 2014 Fundacja Bezpieczna Cyberprzestrzeń. Wszystkie prawa zastrzeżone.
FUNDACJA BEZPIECZNA CYBERPRZESTRZEŃ
ul. Tytoniowa 20, 04-228 Warszawa, tel: +48 22 112 0 800
e-mail: kontakt@cybsecurity.org

www.cybsecurity.org