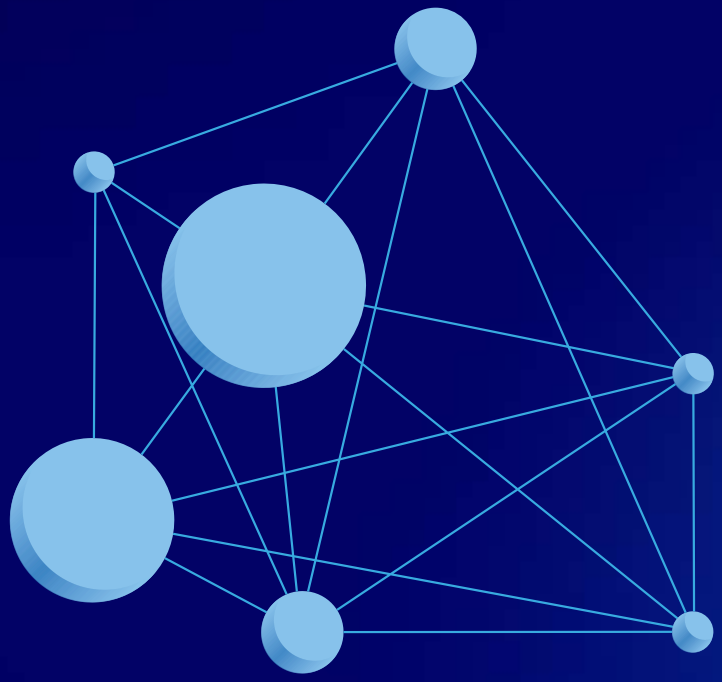


BEZPIECZNIEJ W SIECI .org

Raport BADAWCZY 2014

Spis treści

SŁOWO WSTĘPNE WICEPREMIERA, MINISTRA GOSPODARKI JANUSZA PIECHOCIŃSKIEGO DO RAPORTU BEZPIECZNIEJWSIECI.ORG

MINISTERSTWO GOSPODARKI

Szanowni Państwo,

Z przyjemnością objąłem patronatem honorowym Ministra Gospodarki inicjatywę Fundacji Bezpieczniejwsieci.org, jaką jest Raport o bezpieczeństwie w sieci 2014. Raport ten dotyczy bieżących problemów i zagrożeń związanych z korzystaniem z Internetu.

Wyniki badania wskazują, że Internet odgrywa w naszym życiu coraz większą rolę, staje się także coraz ważniejszym elementem gospodarki. Służy nam przede wszystkim do pracy i codziennych czynności. Tym bardziej powinniśmy pamiętać i zwracać uwagę na potencjalne zagrożenia i możliwości ich wykluczenia.

Dziś większość firm i instytucji umieszcza dane użytkowników w chmurze, a użytkownicy coraz więcej danych (prywatnych i służbowych) przechowują na komputerach i w Internecie. Ponadto wzrasta zainteresowanie obywateli zakupami on-line, co ilustrują rosnące kwoty transakcji, a także ich ilość. Z jednej strony pokazuje to zwiększone zaufanie do zdalnych zakupów, z drugiej dowodzi, jak ważna jest świadomość praw konsumenckich. Przepisy w tym obszarze są dość precyzyjne i regulują zarówno obowiązki usługodawców, jak i prawa konsumentów również na poziomie unijnych dyrektyw.

Dużym zainteresowaniem cieszy się także bankowość online oraz bankowość mobilna. Takie rozwiązania ułatwiają przedsiębiorcom i obywatelom działania w wielu obszarach. W przypadku firm trudno jest bowiem wyobrazić sobie funkcjonowanie bez szybkiego i zdalnego dostępu do konta, w szczególności w sytuacji, gdy przepisy nakładają obowiązki rozliczeń bezgotówkowych.

Według szacunków Komisji Europejskiej gospodarka internetowa stanowi prawie 6 proc. polskiego PKB. Handel elektroniczny jest także barometrem dla całej gospodarki. Istnieje bowiem duża korelacja pomiędzy e-commerce a inwestycjami, inflacją, konsumpcją i bezrobociem. Dlatego zagrożeniem może być zarówno nieupoważniony dostęp do danych jak i ich utrata.

Chciałbym podkreślić, że edukacja w zakresie bezpieczeństwa w sieci powinna stać się częścią systemu nauczania tak, jak ma to miejsce w przypadku innych dziedzin życia. Podejmowane przez Fundację działania informacyjne i edukacyjne w zakresie bezpiecznego korzystania z Internetu są bardzo ważne.

Mam nadzieję, że Raport o bezpieczeństwie w sieci 2014 będzie cieszył się szerokim zainteresowaniem wśród społeczeństwa.

Wicepremier, minister Gospodarki
Janusz Piechociński

INFORMACJA PRASOWA

Polacy wciąż łatwym celem dla cyberprzestępców

Najczęstszym cyberzagrożeniem, które dotknęło 2/3 internautów była utrata danych z komputera, dodatkowo 4 na 10 badanych otrzymało w roku 2013 oszukańcze maile z próbą wyłudzenia informacji do logowania. Mimo tego prawie co czwarty internauta (23%) nie jest w stanie wymienić spontanicznie żadnej metody zabezpieczeń komputera.

BezpieczniejwSieci.org już po raz czwarty prezentuje raport o stanie świadomości zagrożeń występujących w Internecie. Wynika z niego m.in. że niemal 1/3 respondentów (32%) nie posiada dużej wiedzy w zakresie ochrony komputera i danych, jednocześnie wykazując zainteresowanie poszerzeniem zasobu informacji w tym zakresie. To o 12% więcej w porównaniu z rokiem 2012, co wskazuje, że edukacja użytkowników na temat zagrożeń powstających w sieci powinna stanowić priorytet w budowaniu świadomego cyfrowego społeczeństwa XXI wieku. Co ciekawe dla respondentów oceniających dotkliwość zagrożeń napad na ulicy byłby tak samo odczuwalny jak wzięcie kredytu przez osobę trzecią posługującą się skradzionymi danymi, zaś kradzież portfela tak samo dolegliwa jak włamanie do konta internetowego. Wynika z tego, że zagrożenia świata wirtualnego są równie groźne jak te dotyczące integralności cielesnej.

Utrata danych osobowych w sieci

– Według szacunków Komisji Europejskiej gospodarka internetowa stanowi prawie 6 proc. polskiego PKB. Handel elektroniczny jest także barometrem dla całej gospodarki. Istnieje bowiem duża korelacja pomiędzy e-commerce, a inwestycjami, inflacją, konsumpcją i bezrobociem. Dlatego zagrożeniem może być zarówno nieupoważniony dostęp do danych jak i ich utrata – komentuje **wicepremier, minister gospodarki Janusz Piechociński** we wstępnym słowie do raportu Bezpieczniejwsieci.org.

– Wyniki badania ukazują, że użytkownicy internetu prezentują niski poziom znajomości podstawowych zagrożeń wpływających na utratę danych. Co prawda stan wiedzy dotyczący rozpoznawania określeń takich jak wirus, robak czy trojan jest zadawalający (2/3 badanych posiada wiedzę na temat podstawowych zagrożeń), jednak alarmującym wnioskiem wynikającym z raportu jest fakt, że tylko 1/5 respondentów (20%) kojarzy utratę danych z atakiem hakerskim – komentuje **Mariusz Rzepka – FORTINET Territory Manager na Polskę, Białoruś i Ukrainę.**

Coraz więcej Polaków kupuje w sieci

Polski internet zaczyna dojrzewać, ponad połowa respondentów kupuje towary i usługi w internecie za pośrednictwem portali aukcyjnych lub przez sklepy internetowe. Konsumenci chcą przede wszystkim jak najszybciej otrzymać towar za który zapłacili, ważne jest jednak, aby zwracali uwagę na kwestie bezpieczeństwa, a także otrzymywali wsparcie od instytucji państwowych, które działają w obszarze e-commerce.

Interesującym wnioskiem płynącym z badania jest fakt, że 47 proc. respondentów przegląda strony sklepów online, aby potem dokonać zakupu w tradycyjnym sklepie. Może to wiązać się z nieufnością do bezpieczeństwa e-zakupów.

– Nasz Urząd zdaje sobie sprawę jak ważne jest bezpieczeństwo w cyberprzestrzeni i jak ważna jest profilaktyka użytkowników usług na temat zagrożeń, dlatego też aktywnie współpracujemy z różnymi instytucjami działającymi w obszarze ochrony i bezpieczeństwa w sieci – komentuje **Renata Piwowarska, Dyrektor Departamentu Detalicznego Rynku Telekomunikacyjnego Urzędu Komunikacji Elektronicznej**.

– Prezes Urzędu Komunikacji Elektronicznej wprowadził certyfikowanie usług telekomunikacyjnych m.in. w kategorii Bezpieczny Internet, którego celem jest dopingowanie działań podejmowanych przez przedsiębiorców telekomunikacyjnych związanych z podnoszeniem bezpieczeństwa użytkowników – dodaje.

Oswajanie transakcji on-line

1/3 badanych płaci przelewami online przynajmniej raz w tygodniu, zaś 27 proc. płaci rachunki bieżące przy wykorzystaniu bankowego konta elektronicznego. Z badania przeprowadzonego przez Bezpieczniejwsieci.org wynika, że w 2013 roku płatność online przynajmniej raz w miesiącu wykonało 87 proc. badanych, dla porównania w roku 2011 transakcję online przynajmniej raz w miesiącu zadeklarowało 73 proc. zaś w 2012 roku 82 proc. Popularność bankowości online oraz płatności mobilnych wiąże się z ułatwieniami dla przedsiębiorców i użytkowników internetu. Nowoczesne rozwiązania w e-płatnościach gwarantują szybki dostęp do zdalnego konta w szczególności gdy niektóre przepisy nakładają obowiązki rozliczeń bezgotówkowych.

– *Jednym z najciekawszych wniosków części raportu bezpieczniejwsieci.org, dotyczącej zakupów online jest rosnąca liczba deklarowanych wydatków na dobra wirtualne (wzrost o 19%) i utrzymujące się na wysokim poziomie deklarowane wydatki w portalach aukcyjnych.*

– *Wzrost transakcji online o niskiej wartości (np. pliki muzyczne, dobra wirtualne) świadczą o dojrzałości rynku i o tym, że oswoiliśmy internet jako miejsce codziennych, mniej istotnych zakupów* – komentuje **Damien Perillat Dyrektor Zarządzający PayPal w Europie Środkowo-Wschodniej**.

Kolejnym ważnym wnioskiem są zmiany dotyczące metod używanych do finalizowania transakcji online. Widzimy wyraźnie, że rośnie zainteresowanie alternatywnymi formami płatności wobec najpopularniejszych obecnie przelewów bankowych online oraz płatności w internecie z użyciem karty. Według badań BWS w latach 2011 – 2013 wartość zakupów w sieci dokonywanych przy użyciu systemu PayPal wzrosła o 66 zł czyli o blisko 63%. Wzrost ten jest spójny z trendem jaki obserwujemy na całym świecie. Tylko w 2013 roku zyskaliśmy 20 mln nowych użytkowników na całym świecie i przeprocesowaliśmy transakcje o wartości 52 mld. dol. (wzrost 25% rok do roku). – dodaje Perillat.

Trend BYOD - zdjęcia cenniejsze niż pracownicze pliki tekstowe

W badaniu określono również jaki rodzaj plików jest najcenniejszy dla użytkowników. Interesującym wnioskiem jest fakt, że najbardziej wartościowymi dokumentami na urządzeniu są zdjęcia (37 proc. – bezcenne, 41 proc. bardzo wartościowe), pliki tekstowe związane z pracą są dopiero na trzecim miejscu (16 proc. bezcenne, 54 proc. bardzo wartościowe). Wyniki te są zbieżne z badaniami merytorycznego partnera Bezpieczniejwsieci.org, firmy FORTINET, która w raporcie Fortinet Security Census 2013 wskazała, że w roku 2013 aż o 150% wzrosła w Polsce liczba osób gotowych złamać korporacyjne zasady korzystania z własnych urządzeń w miejscu pracy. Już co druga osoba nie dostosowałaby się do zakazu łączenia się z siecią firmową przy użyciu smartfona. Z badania wynika również, że 16% respondentów nie poinformo-wałoby swojego pracodawcy, gdyby ich urządzenie osobiste użyte do celów służbowych padło ofiarą ataku hakerów.

Główne wnioski z raportu:

- ¾ badanych chce wiedzieć więcej o zagrożeniach w sieci
- 80 proc. badanych korzysta przynajmniej raz w miesiącu z usług finansowych online
- 50 proc. badanych korzysta przynajmniej raz w miesiącu z PayPal lub podobnych
- 55 proc. respondentów robi zakupy w serwisach aukcyjnych przynajmniej raz w miesiącu, zaś 50 proc. w sklepach internetowych.
- 20 proc. polskich internautów w przypadku ważniejszych haseł nie sprawdza ich siły
- Kredyt za pomocą skradzionych dokumentów jest oceniany jako tak samo dotkliwe zdarzenie jak napad na ulicy
- Najczęstszym zagrożeniem, które dotknęło 2/3 internautów osobiście, była utrata danych z komputera na skutek różnych przyczyn.
- Do otrzymywania oszukańczych e-maili wyłudzających dane przyznało się 41 proc. respondentów.

O BezpieczniejwSieci.org

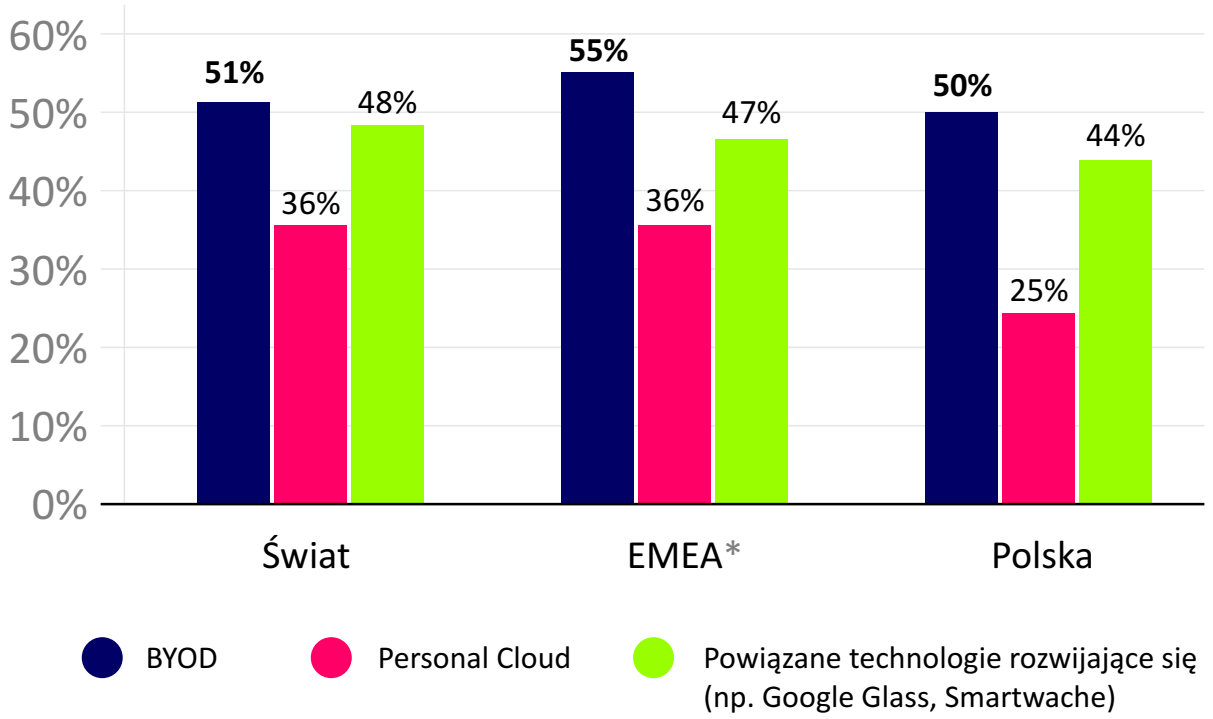
Bezpieczniej w Sieci jest wspólną inicjatywą instytucji publicznych oraz firm prywatnych, których celem jest propagowanie wiedzy o zagrożeniach w Internecie i sposobach radzenia sobie z nimi.
Wzoruje się na udanych kampaniach prowadzonych w ostatnich latach w Wielkiej Brytanii oraz Stanach Zjednoczonych, takich jak *getsafeonline.org* czy *staysafe.com*.
Wpierają ją Ministerstwo Gospodarki, Urząd Komunikacji Elektronicznej oraz PayPal i FORTINET.

Sekcja BYOD FORTINET

Bezpieczeństwo danych firmowych – BYOD, chmura, nowe technologie

W porównaniu do wyników badania Fortinet Security Census 2012, w roku 2013 aż o 150% wzrosła w Polsce liczba osób gotowych złamać korporacyjne zasady korzystania z własnych urządzeń w miejscu pracy. Już co druga osoba nie dostosowałaby się do zakazu łączenia się z siecią firmową przy użyciu smartfona. Z badania wynika również, że 16% respondentów nie poinformowałoby swojego pracodawcy, gdyby ich urządzenie osobiste użyte do celów służbowych padło ofiarą ataku hakerów.

Wykres 1
Jeżeli Twój pracodawca ma lub miał politykę zakazującą stosowania własnych urządzeń w pracy lub w celach zawodowych, czy kiedykolwiek skorzystałeś lub skorzystałbyś z własnych urządzeń, naruszając tę zasadę?



*EMEA - Region Europy, Bliskiego Wschodu i Afryki

Bezpieczeństwo danych firmowych – BYOD, chmura, nowe technologie

Średnio 89% respondentów na świecie stwierdziło, że korzysta z co najmniej jednej usługi przechowywania danych w chmurze, z których najpopularniejszą jest DropBox (38%). 70% osób korzystających z takich usług przyznało, że korzysta z nich również do celów służbowych. 12% osób tej grupy przechowuje w chmurze firmowe hasła, 16% informacje finansowe, 22% poufne dokumenty, takie jak kontrakty czy biznesplany, a aż 33% dane klientów!

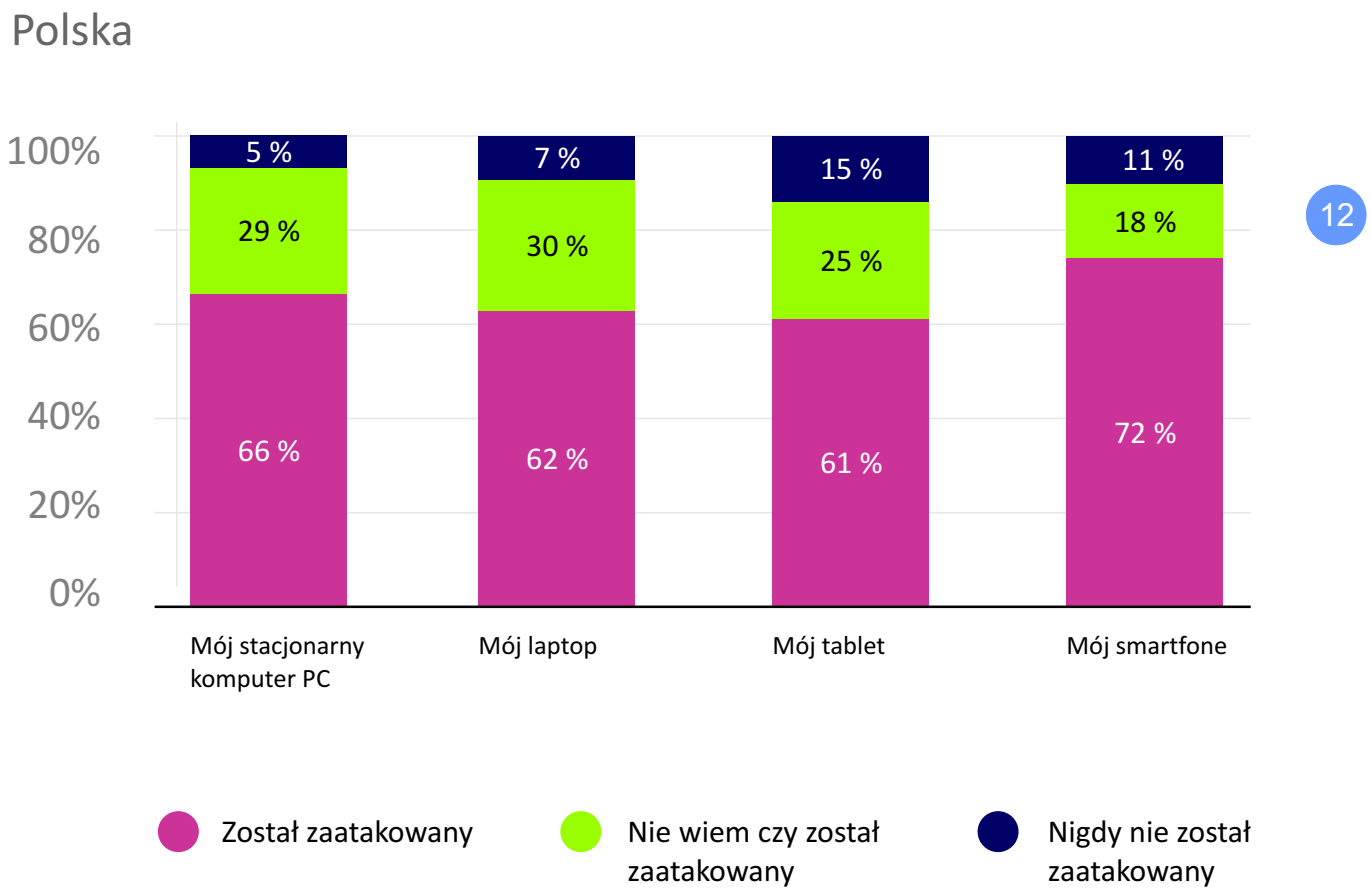
W tej kwestii Polacy są na szczęście bardziej sceptyczni. Aż 34% z nich w ogóle nie korzysta z prywatnych kont cloud w celach służbowych. O wiele mniej z nich trzyma w chmurze najbardziej poufne dane.

Wykres 2
Jakiego rodzaju dane korporacyjne trzymasz w serwisach opartych na chmurze?

Bezpieczeństwo danych firmowych – BYOD, chmura, nowe technologie

Wykres 3
Które z Twoich mobilnych urządzeń padło ofiarą działań cyberprzestępców?
Na którym z nich zauważyłeś atak w postaci wirusa, malware etc?

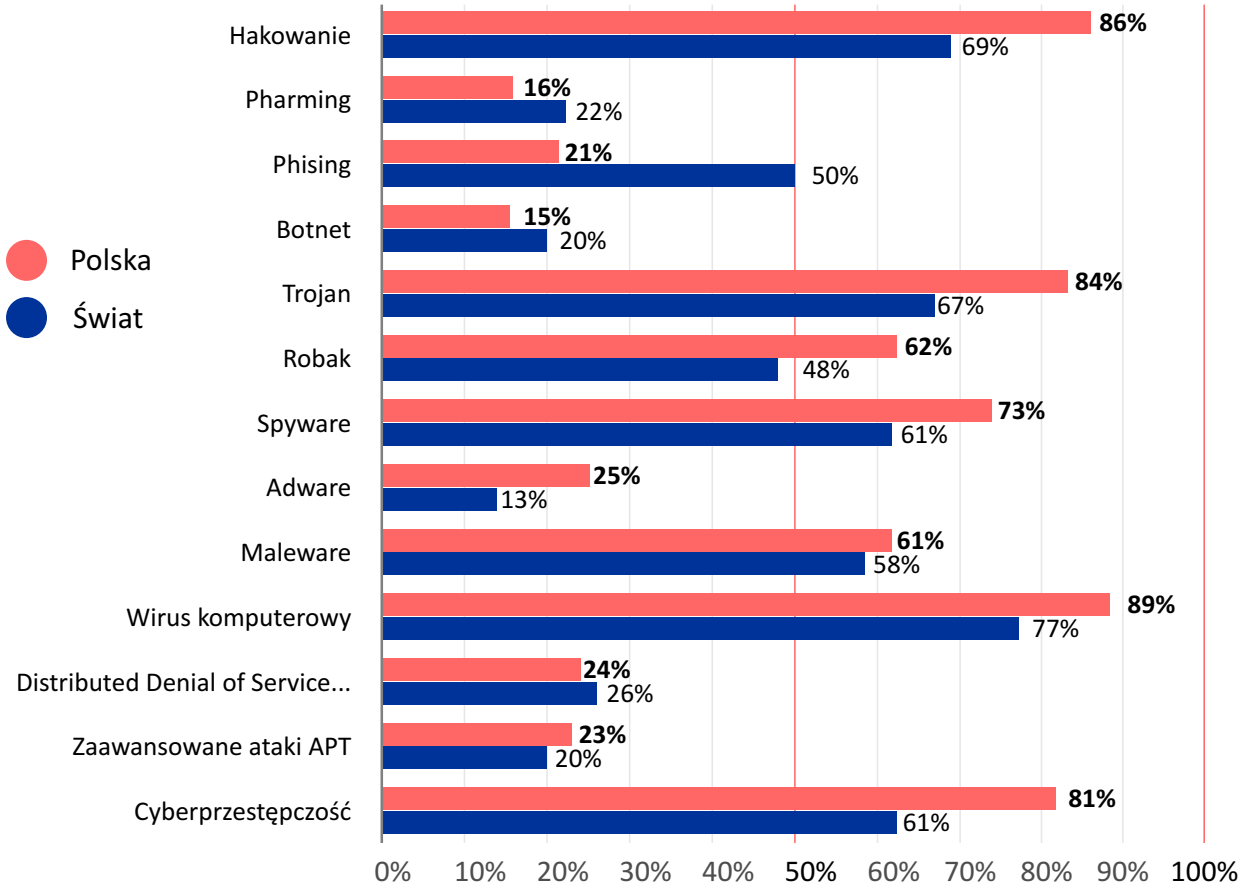
Na pytanie, czy twoje urządzenie wykorzystywanie w firmie kiedykolwiek zostało zaatakowane i jeśli tak, to jakie były tego konsekwencje, 64% respondentów z Polski wskazało na atak na komputer PC lub laptop, z czego połowa skutkowała obniżeniem wydajności i/lub utratą prywatnych i/lub firmowych danych. Znacznie rzadziej atakowane były smartfony (11%), przy czym nieco częściej skutkowały one utratą danych i/lub wydajności niż w przypadku ataków na komputery PC/laptopy, mimo że wśród badanej grupy było więcej posiadaczy smartfonów niż laptopów i komputerów PC. Niewiele większy odsetek ataków zanotowano w przypadku tabletów (15%).



Bezpieczeństwo danych firmowych – BYOD, chmura, nowe technologie

Badanie światowe obejmowało również ćwiczenie mające na celu ocenę świadomości różnych typów zagrożeń. Wyniki pokazały, że młodzi pracownicy są albo wcale nieświadomi zagrożeń albo posiadają dużą wiedzę w tym zakresie. Między tymi dwoma biegunami jest grupa 27% osób o minimalnej świadomości. Spytani o pojęcia, takie jak „APT" (zaawansowane kierunkowe ataki o długotrwałym działaniu), „DDoS" (rozproszony atak typu odmowa usługi), „botnet" i „pharming", nawet do 52% respondentów w ogóle nie orientuje się w tym temacie.

Wykres 4
Rozumiem poniżej wymienione zwroty i hasła:

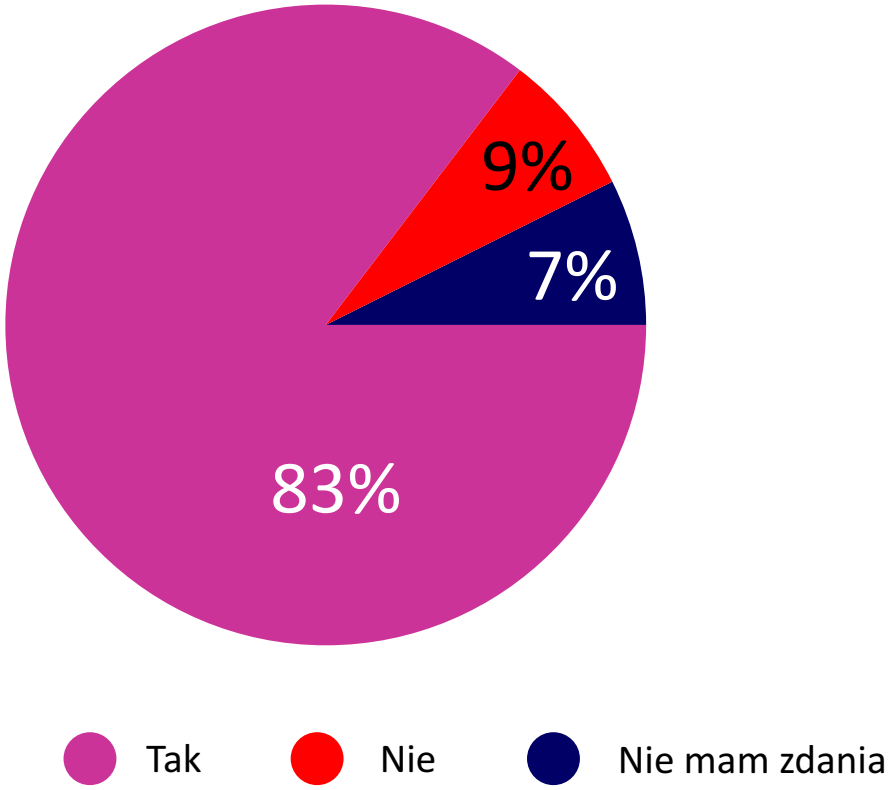


Bezpieczeństwo danych firmowych – BYOD, chmura, nowe technologie

Wykres 5
Czy czujesz, że powinieneś mieć obowiązek rozumienia ryzyka wystąpienia niebezpieczeństwa związanego z wykorzystaniem własnych urządzeń w pracy, jak i do pracy?

83% badanych w Polsce uważa, że powinno posiadać wiedzę na temat niebezpieczeństw związanych z BYOD. Niepokojące jest jednak to, że niemal 1/10 respondentów (9%), zupełnie lekceważy możliwość edukacji w tym zakresie. Gdy dołożymy do tego 7% osób nie mających zdania w tym temacie, okazuje się, że aż 16% wszystkich osób jest w bardzo dużym stopniu narażonych na zostanie ofiarą hakerskiego ataku w pracy.

Polska



Autorem komentarza jest **Mariusz Rzepka**
FORTINET Territory Manager na Polskę, Białoruś i Ukrainę.

Komentarz

Rok 2013 był niewątpliwie rokiem eskalacji trendu BYOD, czyli używania prywatnych urządzeń w pracy. Młoda generacja jest coraz bardziej otwarta na łączenie się z siecią firmową za pośrednictwem własnych smartfonów i tabletów. Dane z raportu Fortinet Security Census 2013 pokazują, że może to nieść ze sobą niebezpieczeństwo dla danych każdego przedsiębiorstwa. Prywatne urządzenie pracownika może się bowiem stać „bramą" do hakerskiego ataku na firmę.

Badanie pokazuje, jakie wyzwania stoją przed firmami i instytucjami chcącymi egzekwować zasady korzystania z własnych urządzeń do celów służbowych, usług przechowywania danych w chmurze oraz, co nieuniknione, inteligentnych urządzeń mających połączenie z internetem.

Zwraca również uwagę na fakt, że dla dyrektorów działów informatycznych śledzenie tego, gdzie są przechowywane dane firmowe i w jaki sposób jest uzyskiwany dostęp do nich, stanowi poważny problem. Rozwiązania z zakresu analizy bezpieczeństwa są dziś potrzebne firmom i instytucjom bardziej niż kiedykolwiek wcześniej.

Należy je wdrażać na poziomie sieci, tak aby umożliwić monitorowanie aktywności użytkowników w oparciu o ich lokalizację oraz używane aplikacje i urządzenia. Z badania wynika również, że edukowanie pracowników w kwestii zagrożeń oraz konsekwencji z nich wynikających to kluczowy aspekt zapewnienia bezpieczeństwa informatycznego firm i instytucji.

Komentarze

PayPal wyznacza standardy bezpieczeństwa i wspiera inicjatywę Bezpieczniej w Sieci.org w walce z zagrożeniami internetowymi

Damien Perillat
Dyrektor Zarządzający PayPal
w Europie Środkowo-Wschodniej

PayPal, globalny lider płatności mobilnych, wykracza poza tradycyjne metody uwierzytelniania. W ostatnim czasie firma stworzyła sojusz Szybkiej Identyfikacji Tożsamości Online FIDO (z ang. Fast Identity Online), organizację której celem jest tworzenie prostszych i bezpieczniejszych systemów autoryzacji. Wnioski z raportu pozwolą lepiej zrozumieć zagrożenia czyhające na Polaków w sieci i w konsekwencji zminimalizować skalę tych zagrożeń.

Wsparcie dla inicjatyw takich jak Bezpieczniej w Sieci.org wpisuje się w globalną politykę firmy polegającą na zwiększaniu wygody transakcji pieniężnych między ludźmi przy jednoczesnej poprawie ochrony przed cyberprzestępstwami, np. phishingiem.

Kluczowe wnioski

Badanie przeprowadzone przez fundację bezpieczniejwsieci.org skupia się na kluczowych z punktu widzenia firmy PayPal kwestiach związanych z bezpieczeństwem płatności online. Warto zauważyć, że przeważająca większość respondentów ufa zakupom w sieci. Przykładowo, w 2013 roku tylko 13% osób wskazywało na oszustwo (np. ze strony sklepów internetowych) jako najbardziej prawdopodobne zagrożenie w sieci. Dodatkowo liczba osób obawiających się przechwycenia ich poufnych danych przez hakerów nie zwiększyła się zauważalnie w latach 2011-2013. Jednocześnie płatności internetowe i mobilne kwitną na świecie i odnotowują gwałtowny wzrost również w Polsce, głównie za sprawą większej ilości transakcji dokonywanych w kraju jak i za granicą, m.in. przy użyciu bezpiecznych portfeli cyfrowych. Według danych IPSOS, PayPal jest drugą co do popularności, po transakcjach dokonywanych kartą, metodą płatności za zakupy dokonywane przez Polaków za granicą (34% Polaków dokonujących zakupów za granicą). Globalnie, suma transakcji dokonywanych za pomocą systemu PayPal wyniosła 180 mld $, co daje 24% wzrost w stosunku do roku poprzedzającego. Ponieważ coraz więcej osób dokonuje zakupów za pośrednictwem urządzeń przenośnych, kluczowe jest zapewnienie im zabezpieczeń na najwyższym światowym poziomie.

Jakie inicjatywy podjęto w skali globalnej w celu zapewnienia bezpieczeństwa?

PayPal™

Trzy filary sukcesu

Polityka bezpieczeństwa PayPal stanowi punkt odniesienia dla branży finansowej od ponad dekady. Opiera się ona na trzech podstawowych filarach.

Jednym z nich jest **Program Ochrony Kupującego**. Jak to działa? Na przykład, PayPal zrekompensuje straty w przypadku gdy zamówiony towar nie dotrze do odbiorcy lub nie będzie on zgodny z opisem sprzedającego.

Drugi filar to **wygoda**. PayPal nie wymaga wpisywania długich ciągów liczbowych czy skomplikowanych kombinacji by bezpiecznie dokonywać zakupów czy potwierdzać swoją tożsamość. Wszystkie dane osobowe przechowywane są w chmurze i nigdy nie są udostępniane osobom trzecim. Możesz wylogować się podając jedynie adres e-mail i hasło.

Ostatni filar to **innowacja**. To oznacza, że PayPal stale poszukuje szybszych i bezpieczniejszych metod płatności.

Sojusz FIDO dla bezpieczniejszej przyszłości bez haseł

Jednym z większych wyzwań stojących przed transakcjami internetowymi jest potrzeba *zapamiętywania wielu haseł*. Wierzymy w to, że w najbliższej przyszłości taka metoda uwierzytelniania zostanie uproszczona lub całkowicie wyeliminowana. Właśnie dlatego PayPal uruchomił sojusz FIDO. Organizacja ta ma na celu tworzenie prostszych i bezpieczniejszych systemów potwierdzania tożsamości w Internecie.

Klienci będą mogli logować się do dowolnego sklepu korzystającego z systemu PayPal przy użyciu czytnika linii papilarnych i to bez potrzeby podawania nazwy użytkownika czy hasła. **Jak to działa?** PayPal udostępnia bezpieczny portfel w chmurze i nie przechowuje informacji osobistych na urządzeniu. Na przykład, użytkownicy będą mogli użyć odcisku swojego palca do dokonywania płatności przy użyciu najnowszego smartfona Samsung Galaxy S5, ponieważ oprogramowanie **FIDO Ready™** na urządzeniu dokonuje bezpiecznej komunikacji pomiędzy czytnikiem linii papilarnych w urządzeniu a usługą PayPal w chmurze. Jedyną informacją udostępnianą systemowi PayPal jest unikalny klucz umożliwiający weryfikację tożsamości klienta, co eliminuje potrzebę przechowywania informacji biometrycznych na serwerach PayPal.

Dzięki sojuszowi FIDO, PayPal wniósł wygodę płatności na wyższy poziom bez poświęcania bezpieczeństwa na najwyższym światowym poziomie.

Walka z cyberprzestępczością jest łatwiejsza dzięki systemowi PayPal.

Badanie BWS pokazuje, że obecnie większa ilość polskich internautów miała styczność z fenomenem phishingu - próbą wyłudzenia danych osobowych lub zmylenia użytkownika poprzez wysyłanie fałszywych e-maili (np. udając instytucję finansową) - niż jeszcze 2-3 lata temu. Ponieważ zjawisko to jest stosunkowo nowe dla Polaków, bardzo ważna jest odpowiednia edukacja i tym samym zwalczanie problemu. Historie o cyberprzestępstwach działają na wyobraźnię, jednak w rzeczywistości zwykły użytkownik nie zdaje sobie sprawy z ilości zabezpieczeń czuwających nad jego bezpieczeństwem. Przykładowo, PayPal współpracuje z dostawcami usług e-mailowych i przechwytuje wiadomości śmieci oraz inne potencjalnie niebezpieczne e-maile wysyłane przez cyberprzestępców zanim te nawet pojawią się w naszych skrzynkach odbiorczych.
Dział bezpieczeństwa firmy zatrudnia m.in. byłych funkcjonariuszy organów ścigania, którzy współpracują z instytucjami na całym świecie celem ochrony użytkowników przed oszustwami i kradzieżą tożsamości.

PayPal zapoczątkował innowacyjne podejście do uwierzytelniania poczty elektronicznej. Wiosną 2011 roku, razem z grupą wiodących organizacji takich jak Yahoo Mail, Bank of America, Facebook, LinkedIn czy Gmail, rozpoczął współpracę mającą na celu walkę z phishingiem w skali internetu. Wspólnie stworzyli system DMARC, który chroni przed zjawiskiem phishingu ponad 2 miliardy ludzi na całym świecie.

Od czasu jego powstania, dołączyli do niego kolejni wielcy gracze, pomagając milionom ludzi unikać zagrożeń związanych z phishingiem. System DMARC ujednolica sposób uwierzytelniania e-maili pomiędzy nadawcami i odbiorcami przy użyciu dobrze znanych mechanizmów SPF (Sender Policy Framework) oraz DKIM (DomainKeys Identified Mail). W skrócie oznacza to, że nadawcy i odbiorcy e-maili dzielą się ze sobą informacjami. Odbiorcy dostarczają nadawcom informacje dotyczące ich infrastruktury uwierzytelniania, podczas gdy nadawcy mówią im co zrobić gdy odebrana wiadomość jest podejrzana. Efekty pracy systemu są znakomite. Twitter poinformował, że przed wdrożeniem systemu DMARC ponad 110 milionów wiadomości dziennie podszywało się pod ich domeny. Po wdrożeniu systemu, liczba ta spadła do 1000. Istnieje również wiele innych rozwiązań antyphishingowych. Na przykład, PayPal współpracuje z firmą Iconix, która posiada unikalne narzędzia weryfikujące podejrzane e-maile, które to pozwalają uniknąć otwierania szkodliwych treści.

Jak działa phishing i jak go uniknąć - 7 wskazówek firmy PayPal

Walka z cyberprzestępczością nie musi być skomplikowana. Czasami wymaga to tylko włączenia filtrów antyspamowych - jeśli nie będziesz otrzymywał fałszywych wiadomości ryzyko oszustwa znacznie spada. Oto kilka dodatkowych porad firmy PayPal pozwalających uchronić się przed phishingiem:

Jak działa phishing?

- Przestępca wysyła **dużą ilość maili** korzystając z listy e-maili zidentyfikowanych jako aktywne lub na adresy zupełnie losowe. **Wiadomości te sprawiają wrażenie wysłanych przez szeroko rozpoznawalne firmy.** Typowy przykład to fikcyjna historia zaprojektowana tak aby zwabić do kliknięcia w link lub wykonania połączenia telefonicznego na podany numer.
- Wiadomość phishingowa **poprosi cię o wypełnienie formularza lub kliknięcie** w przycisk który przekieruje cię na fałszywą stronę.
- Fałszywa strona **imituje stronę firmy na którą przestępcy powołują się w e-mailu**, celem wyłudzenia od nas wrażliwych danych.

W skrócie, osoba dotknięta phishingiem myśli, że podaje swoje dane zaufanej firmie, podczas gdy w rzeczywistości jest to przestępca. Wiadomości phishingowe mogą również zwabić nas do otwarcia podejrzanego załącznika lub przejścia na stronę internetową, która w konsekwencji zarazi nasz komputer złośliwym oprogramowaniem. **Jak wyłapać fałszywego e-maila?**

Jak wyłapać fałszywego e-maila?

Istnieje wiele wskaźników nieuczciwych e-maili:

- **Fałszywe poczucie pilności** - w wielu przypadkach fałszywe wiadomości poinformują cię o zagrożeniu twojego konta/komputera w przypadku braku nagłej reakcji.
- **Fałszywe linki** - mogą wyglądać na prawdziwe ale prowadzić na manowce. Sprawdź czy adres odnośnika pokrywa się z adresem w przeglądarce poprzez najechanie nad URL w wiadomości e-mail. Jeśli coś wzbudzi twoje podejrzenie, nie klikaj w link.
- **Załączniki** - prawdziwa wiadomość email wysłana przez PayPal lub inną firmę zapewniającą zabezpieczenia na najwyższym światowym poziomie nigdy nie będzie zawierać załączników lub oprogramowania. Załączniki mogą zawierać złośliwe oprogramowanie, więc nigdy nie powinieneś otwierać załączników bez stuprocentowej pewności, że są autentyczne.

· **Jeśli nie jesteś pewien czy e-mail jest autentyczny czy nie, powinieneś poczynić następujące kroki**: Nie klikaj w żaden link w wiadomości. Zamiast tego otwórz przeglądarkę, wejdź na stronę PayPal lub banku i zaloguj się. Jeśli czeka na ciebie jakaś pilna wiadomość, na pewno dowiesz się o tym po zalogowaniu.

Niebezpieczeństwo czai się wszędzie - nawet w portalach społecznościowych. Bądźmy świadomi!

Autorem wszystkich komentarzy jest **Mariusz Rzepka**
FORTINET Territory Manager
na Polskę, Białoruś i Ukrainę.

Edukacja w zakresie bezpieczeństwa to podstawa

Najnowsze badanie Fundacji Bezpieczniej w Sieci pokazuje, że niemal 1/3 respondentów (32%) nie posiada dużej wiedzy w zakresie ochrony komputera i danych, jednocześnie wykazując zainteresowanie poszerzeniem zasobu informacji w tym zakresie. To o 12% więcej w porównaniu z rokiem 2012, co wskazuje, że edukacja użytkowników na temat zagrożeń powstających w sieci powinna stanowić priorytet w budowaniu świadomego cyfrowego społeczeństwa XXI wieku. Komputery i inne urządzenia elektroniczne są nieodłącznymi towarzyszami naszego życia. Oprócz ułatwiania nam pracy i codziennych czynności, stanowią one jednak źródło różnych niebezpieczeństw. Hakerzy mogą skutecznie ograniczyć możliwości naszych urządzeń i utrudnić nam ich sprawne wykorzystanie, to jednak najmniej dotkliwe konsekwencje nieodpowiedniego obchodzenia się ze sprzętem IT. Ofiary cyberprzestępców mogą bowiem w skrajnych przypadkach zostać zmuszone do ponoszenia wysokich kosztów odzyskania swoich utraconych danych (tak działa oprogramowanie ransomware) lub nawet okradzione ze środków pieniężnych, zgromadzonych na ich bankowych kontach.

Co bardzo istotne, aż 74% wszystkich badanych przez Fundację użytkowników internetu korzysta z serwisów społecznościowych typu Facebook czy Twitter. W związku z tym należy podkreślić, że od pewnego czasu złą sławę zyskują infekcje STI (ang. Socially Transmitted Infections). Naturalnie najbardziej podatną na te techniki grupą są osoby ufne, między innymi młodzież, która często bezkrytycznie używa mediów społecznościowych i – nieświadoma zagrożeń – podaje wiele poufnych informacji. Powinniśmy wiedzieć jak się bronić przed STI.

OTO 3 PROSTE RADY:

***1**. Zawsze ustawiać **unikalne hasła**;*
***2.** Używać **skutecznego programu antywirusowego**;*
***3. Myśleć przed kliknięciem**. Jeśli widzimy, że nasz znajomy zamieścił na portalu nietypowy link, nie klikajmy go! **Należy unikać klikania** w linki o zbyt ogólnej treści, np. „hej, musisz to zobaczyć!". Powinniśmy także **zwracać uwagę na adresy URL** i upewniać się, że prowadzą do miejsc, które chcemy odwiedzić. Uważajmy na niebezpieczne strony internetowe, które mają w adresie URL nazwę znanego serwisu WWW w celu wywołania wrażenia, że strona ta jest powiązana z takim serwisem.*

Wyłudzanie pieniędzy w sieci popularne jak nigdy

Wyniki przeprowadzonego przez Fundację Bezpieczniej w Sieci badania pokazują, że użytkownicy końcowi prezentują przeciętną znajomość podstawowych zagrożeń mogących powodować utratę danych. Co prawda niemal 2/3 badanych rozpoznaje określenia takie jak wirus, trojan czy robak, jednak jedynie 5% spotkało się z kradzieżą danych czy phishingiem. **Najbardziej alarmujące jest jednak to, że tylko 1/5 respondentów (20%) kojarzy utratę danych z atakiem hakerskim. Świadomość tych zagrożeń powinna być znacznie większa. Hakerzy używają dziś bowiem wielu różnych sztuczek mających na celu zainfekowanie komputera złośliwym oprogramowaniem**, mającym na celu kradzież informacji. Ich działania obejmują m.in. maskowanie źródeł, z których są pobierane pliki (np. *aktualizacje Flash*) tak, aby wyglądały na zaufane, dezaktywowanie oprogramowania antywirusowego komputera, przekierowywanie użytkownika do zainfekowanych stron internetowych czy dodawanie złośliwych rozszerzeń do przeglądarek w celu przejęcia kontroli nad kontem użytkownika w portalu społecznościowym.

Oprócz utraty danych, każdy z nas może utracić również spore sumy pieniędzy. Najbardziej popularnym trojanem w 2013 roku był ZeuS. Urządzenia FortiGate na całym świecie zarejestrowały ponad **20 mln prób** zainfekowania sieci z jego użyciem. Od samego początku ZeuSa wykorzystywano głównie do przestępstw o charakterze finansowym, ale pod koniec 2013 roku znalazł on zastosowanie również w Cryptolockerze, oprogramowaniu typu *ransomware*. Cryptolocker wprowadził oprogramowanie typu *ransomware* w nowy wymiar. Generuje on bowiem pary unikalnych kluczy kryptograficznych w celu pełnego zaszyfrowania danych na zainfekowanym komputerze wraz ze wszelkimi podłączanymi dyskami, na których użytkownik mógł te dane zapisać. Następnie Cryptolocker informuje ofiarę, że ma w krótkim czasie zapłacić dość wysoki okup, sięgający nawet kilkuset dolarów. W przeciwnym razie klucz, którym zaszyfrowano dane ofiary, zostanie skasowany, co w praktyce całkowicie uniemożliwi odzyskanie danych.

Jak się chronić? Firewall to podstawa

Niewiele ponad **1/3 (36%)** badanych przez Fundację Bezpieczniej w Sieci użytkowników internetu przyznaje, że wykorzystuje zapory ogniowe (ang. *firewalls*) podczas codziennego surfowania. Nie jest to jednak dla nich najważniejsze narzędzie zabezpieczające komputer przed atakami czy utratą danych. Zapytani wprost, jakie rozwiązania bezpieczeństwa IT znają, **zaledwie 18% wszystkich badanych wymienia nazwę *firewall*.** To bardzo alarmujące zjawisko, gdyż to właśnie *firewall* jest jednym z najbardziej kluczowych zabezpieczeń naszych komputerów przed atakami cyberprzestępców. **Antywirusy, choć wykrywają dużo infekcji, nie są w stanie samodzielnie zabezpieczyć nas przed wpadnięciem w sidła złośliwego oprogramowania. Nowoczesne trojany i robaki potrafią skutecznie oszukiwać antywirus i często firewall jest ostatnim bastionem ochrony urządzenia przed zainfekowaniem.** Cyberprzestępcy wkładają mnóstwo wysiłku w tworzenie setek tysięcy nowych wariantów złośliwego oprogramowania, które każdego dnia są rozsyłane w nadziei, że któryś z nich uda się zainstalować na jakimś urządzeniu. **Niezależnie od sposobu wykorzystywania naszych urządzeń w sieci radzimy każdemu użytkownikowi zainstalowanie choćby najbardziej podstawowego, darmowego firewalla.**

Komentarz pani Renaty Piwowarskiej, Dyrektor Departamentu Detalicznego Rynku Telekomunikacyjnego UKE

Wg raportu GUS-u w 2013 r. blisko 72 % gospodarstw domowych posiadało dostęp do sieci Internet. Odsetek ten wyższy niż w latach ubiegłych potwierdza tak stałe zapotrzebowanie na usługę po stronie odbiorców jak i ciągły rozwój tego segmentu rynku.

Z Raportu „Bezpieczeństwo w Sieci w 2013 r." przygotowanego przez Agencję Badań Rynku i Opinii SW Reserch wynika, że 91 % osób mających dostęp do sieci aktywnie korzysta codziennie z poczty mailowej, serwisów społecznościowych (74 %), a 32 % wykorzystuje Internet do realizowania płatności za pomocą internetowych przelewów bankowych. Ponadto wynika też z niego, że stajemy się nie tylko coraz bardziej aktywni „w sieci", ale również, że jesteśmy coraz bardziej świadomymi użytkownikami. Świadomi możliwości jakie daje nam Internet, ale również i zagrożeń, jakie są z tym związane.

Ponad połowa respondentów przynajmniej raz w miesiącu dokonuje zakupów przez Internet za pośrednictwem portali aukcyjnych ebay, allegro.pl lub przez sklepy internetowe, a 42 % kilka razy w miesiącu dokonuje płatności poprzez www. 69 % internautów natomiast zna i stosuje narzędzia ochrony komputera i danych i stosuje programy antywirusowe. 18 % internautów stosuje ponadto firewall-e, trudne hasła, w mniejszym stopniu natomiast osoby „surfujące" po sieci zwracają uwagę przy przeglądaniu stron na mechanizmy potwierdzające bezpieczne logowanie (ssl) czy zaufane strony.
Tu pojawia się pole do działania m.in. dla naszego Urzędu jak również innych organizacji.
Nasz Urząd zdaje sobie sprawę jak ważne jest bezpieczeństwo w cyberprzestrzeni i jak ważna jest profilaktyka (edukacja i uświadamianie) użytkowników usług na temat zagrożeń, dlatego też aktywnie współpracujemy z różnymi instytucjami działającymi w obszarze ochrony i bezpieczeństwa w sieci.
Ponadto, w celu zapewnienia użytkownikom jak najlepszej ochrony przez nadużyciami, w tym przestępczością w sieci, Prezes Urzędu Komunikacji Elektronicznej wprowadził certyfikowanie usług telekomunikacyjnych m.in. w kategorii Bezpieczny Internet, którego celem jest dopingowanie działań podejmowanych przez przedsiębiorców telekomunikacyjnych związanych z podnoszeniem bezpieczeństwa użytkowników, w tym promowanie rozwiązań wykorzystujących dostępne na rynku narzędzia, mogące zapewnić najwyższy poziom zabezpieczenia przed przestępczością w sieci.

Metodologia

Metodologia

Do celów badawczych należało zbadanie:

1. Subiektywnego postrzegania zagrożeń w sieci:
- Określenie poziomu świadomości na temat zagrożeń w sieci
- Ocena znajomości narzędzi zapobiegających zagrożeniom w sieci
- Oszacowanie wysokości możliwych strat finansowych
- Wyszczególnienie sposobów wykorzystywania Internetu
- Przybliżenie prawdopodobieństwa zdarzeń zagrażających bezpieczeństwu w sieci

2. Zachowań związanych z ochroną danych na komputerze i telefonie komórkowym
- Wiedza i stosowane sposoby ochrony danych
- Doświadczenie związane z utratą danych
- Określenie sposobów ochrony komputera i danych

Badania odbywały się w trzech falach.
Pierwsza została zrealizowana w październiku 2011 roku (pytania odnosiły się do zachowań w Internecie w 2011 roku), druga odbyła się w styczniu 2013 (dotyczyła zachowań w Internecie w 2012 roku), trzecia z kolei została przeprowadzona w styczniu 2014 (a dotyczyła zachowań w Internecie w 2013).
Wszystkie badania zostały przeprowadzone metodą CAWI, czyli internetowych, zestandaryzowanych wywiadów kwestionariuszowych, przez agencję SW Research.

Próba badawcza miała charakter losowy. Operatem losowania był panel internetowy Swpanel.pl, do udziału w badaniu zaproszono osoby, które ukończyły 16 lat. Warunkiem koniecznym uczestnictwa w badaniu było korzystanie z Internetu przynajmniej raz w tygodniu. Badanie przeprowadzono na autorskim oprogramowaniu „3S" zintegrowanym z panelem internetowym Swpanel.pl.

W pierwszej fali badania, w 2011 roku, zebrano łącznie 1000 w pełni wypełnionych kwestionariuszy, a dopuszczalny błąd statystyczny w badaniu nie przekraczał 3,2 p. proc. dla całej próby. W drugiej fali, w 2012 roku, zebrano 1477 w pełni wypełnionych kwestionariusz, a dopuszczalny błąd statystyczny w badaniu nie przekraczał 2,6 p. proc. dla całej próby. W trzeciej fali zebrano 1002 w pełni wypełnionych kwestionariusz, a dopuszczalny błąd statystyczny w badaniu nie przekraczał 3,2p. proc. dla całej próby.

Kwestionariusz został opracowany przez **SW Research** przy ścisłej współpracy z Fundacją Bezpieczniej w Sieci.