Uniwersytet Ekonomiczny w Katowicach

Wydział Informatyki i Komunikacji

Kierunek: *Informatyka i ekonometria*

Michał Paniczek

Świadomość bezpieczeństwa w chmurze obliczeniowej

Awareness of security in cloud computing

Praca magisterska
napisana w Katedrze *Informatyki*
pod kierunkiem *dr Artura Strzeleckiego*

Pracę przyjmuję i wnioskuję o jej dopuszczenie
do dalszych etapów postępowania egzaminacyjnego

…… ……..
(data) *(podpis promotora pracy magisterskiej)*

KATOWICE *2016*

Katowice, dnia .....

.....Michał Paniczek.....
Imię i nazwisko

.....Informatyki i komunikacji.....
Wydział

.....Informatyka i ekonometria.....
Kierunek

OŚWIADCZENIE

Świadom odpowiedzialności prawnej oświadczam, że złożona praca magisterska pt.: Świadomość bezpieczeństwa w chmurze obliczeniowej
została napisana przeze mnie samodzielnie.

Równocześnie oświadczam, że praca ta nie narusza praw autorskich w rozumieniu ustawy z dnia 4 lutego 1994 roku o prawie autorskim i prawach pokrewnych (Dz. U. 1994, nr 24, poz. 83) oraz dóbr osobistych chronionych prawem.

Ponadto praca nie zawiera informacji i danych uzyskanych w sposób nielegalny i nie była wcześniej przedmiotem innych procedur związanych z uzyskaniem dyplomów lub tytułów zawodowych uczelni wyższej.

Wyrażam zgodę na przetwarzanie moich danych osobowych oraz nieodpłatne udostępnienie mojej pracy w celu oceny samodzielności jej przygotowania przez system elektronicznego porównywania tekstów oraz przechowywania jej w bazie danych tego systemu.

Oświadczam także, że wersja pracy znajdująca się na przedłożonej przeze mnie płycie CD jest zgodna z wydrukiem komputerowym pracy.

.....
(podpis składającego oświadczenie)

Spis treści

Wstęp

Ludzkość od zawsze borykała się z problemem dostępności zasobów. To ich brak, był głównym hamulcem i przeszkodą w rozwoju techniczno-technologicznym. Innowacyjne narzędzia, wytworzone przez jednego rzemieślnika, w danej lokalizacji, nie trafiały do innej. Ich twórca nie miał świadomości, że sąsiednia społeczność zgłaszała zapotrzebowanie na nią. Hamowało to obie. Jedna musiała poświecić czas, pomysł i zasoby na opracowanie rzeczy odkryte w drugiej. Ona zaś, nie mogła bogacić się swoim wynalazkiem, poprzez wymianę wiedzy, czy pozyskując nowe zasoby na odkrycie kolejnych technologii. W dobie informacji problem dostępności narzędzi przyjął inną formę. Związane jest to, ze zmianą ich postaci, które przyjęły współcześnie kształt informacji, programów użytkowych i zasobów obliczeniowych. Dostęp do tych narzędzi, zwanych obecnie zasobami, umożliwił rozwój globalnej sieci komputerowej – Internet. Technologia ta początkowo była wykorzystywana tylko w celach militarnych, obecnie znacząco przekroczyła obszar swojego zastosowania. Umożliwia ona dzielenie się zasobami w cyberprzestrzeni. Powstały wyspecjalizowane centra mocy obliczeniowych, zwanych chmurą obliczeniową. Tym samym, rozwiązany został problem przepływu narzędzi. Jednoczesny dostęp wielu użytkowników do zasobów zgromadzonych w chmurze skutkował powstaniem nowego problemu – bezpieczeństwa. Klienci centrów obliczeniowych, magazynują tam dane, o dużym poziomie istotności, których utrata, bądź wyciek, skutkować może znaczonymi konsekwencjami personalnymi, finansowymi i prawnymi. W kwestii zapewnienia bezpieczeństwa, społeczność użytkowników chmury obliczeniowej pokłada zaufanie w dostawcach usługi. Obowiązek ten spoczywa tak po stronie administratorów chmury obliczeniowej, jak i ich klientów.

Przedmiotem pracy jest przedstawienie stanu świadomości użytkowników oraz administratorów chmury obliczeniowej dotyczących potrzeby zapewniania bezpieczeństwa danych i zasobów zgromadzonych w chmurze obliczeniowej.

Celem poznawczym pracy jest przedstawienie, w oparciu o literaturę, zasad działania chmury obliczeniowej, znaczenia oraz istności bezpieczeństwa zasobów w niej zgromadzonych, a także form i celów ataków na nie. Dodatkowo, przedstawiono poziom świadomości przeciętnego użytkownika chmury obliczeniowej, dotyczącej wykorzystywanych przez niego centrów obliczeniowych oraz praktyk, w zakresie zapewnienia bezpieczeństwa przechowywanych zasobów.

Celem metodologicznym pracy jest przedstawienie możliwych do zastosowania przez użytkowników, administratorów i projektantów chmury obliczeniowej, praktyk oraz rozwiązań w celu zapewnienia bezpieczeństwa jej zasobów.

W pierwszym rozdziale przedstawiono istotę chmury obliczeniowej, jej podział ze względu na rodzaj świadczonej usługi oraz sposób wdrożenia. Zdefiniowano w nim podstawowe pojęcia wykorzystywane w dalszej części pracy.

Rozdział drugi poświęcony jest tematyce bezpieczeństwa. Przedstawiono jej istotność w życiu każdego człowieka. Przytoczono w nim również najczęściej występujące formy ataków na zasoby zgromadzone w chmurze obliczeniowej.

W rozdziale trzecim wykorzystano przeprowadzone badania. Przeanalizowano wyniki ankiety w celu przedstawienia stanu wiedzy użytkowników sieci komputerowych, dotyczącego wykorzystania zasobów chmury obliczeniowej oraz ich praktyk i zachowań związanych z bezpieczeństwem.

Rozdział czwarty został poświęcony sposobom ochrony zasobów zgromadzonych w chmurze obliczeniowej. Przytoczono regulacje prawne dotyczące zapewnienia bezpieczeństwa danych osobowych, jak również danych instytucji finansowych, jako przykład kompleksowego systemu ochrony. Zbudowano również wzorcowy model ochrony zasobów zgromadzonych w chmurze obliczeniowej, oparty o formy ataków oraz praktyki użytkowników, przedstawione we wcześniejszych rozdziałach.

Wnioski końcowe zostały zawarte w zakończeniu pracy.

Praca została napisana w oparciu o pozycje książkowe, wydane w językach polskim i angielskim, materiały konferencyjne o charakterze krajowym i międzynarodowym, ustawy oraz materiały powszechnie dostępne poprzez sieć Internet. W procesie pisania pracy, wykorzystano narzędzia Google Form do tworzenia internetowych ankiet, dostarczone przez firmę Google.

Rozdział I

Chmura komputerowa

Podłączając sprzęt do gniazdka elektrycznego, oczekujemy, że będzie w nim napięcie, które umożliwi działanie i poprawne funkcjonowanie odbiornika. Użytkownika z reguły nie interesuje, skąd tam się ono bierze i w jaki sposób zostało dostarczone. Nie dostrzegają istniejącej instalacji w domu, infrastruktury przesyłowej oraz pracy olbrzymich elektrowni, które wytwarzają energię elektryczną, dzięki której działają jego urządzenia. Z perspektywy informatycznej, gniazdko dostarcza pewną usługę, dzięki której można korzystać z dobrodziejstw zdobyczy technologicznych oraz wydajniej pracować. Szczegóły działania usługi są niejawne, ale jednocześnie istnieje możliwość poznania teoretycznego sposobu jej funkcjonowania.

Podobnie rzecz ma się z chmurą obliczeniową. Użytkownik nie jest zainteresowany zasadami funkcjonowania dostarczanej mu usługi, którą może być zarówno przestrzeń dyskowa jak również i moc obliczeniowa. Ważne są dla niego dostępność usługi oraz przydzielone zasoby, niezbędne do wykonania zadania. Pojęcie chmury obliczeniowej jest więc dla niego pojęciem abstrakcyjnym. Dostawcy usługi, tacy jak Amazon.com, Google czy Microsoft, niechętnie zdradzają szczegółowe zasady działania swojej usługi. Jest to najczęściej ich autorskie rozwiązanie, zapewniające im przewagę rynkową, a same prawa są objęte tajemnicą w formie patentu.

W tym rozdziale omówiona została tematyka chmury obliczeniowej. Została podana jej definicja oraz podstawowy podział, według którego można ja sklasyfikować. Przedstawiono również podstawowe koszty takich usług.

1.1. Definicja chmury obliczeniowej

W literaturze i zasobach internetowych istnieje wiele definicji chmury obliczeniowej. Najpopularniejszą i najczęściej podawaną jest ta, zaproponowana przez National Institute of Standards and Technology (NIST). „Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, applications and services) that can be rapidly provisioned and releasd with minimal management effort or services provider interaction” [WWW2]. Można to rozpatrzyć w następujący sposób. Chmura obliczeniowa to model przetwarzania danych, osiągalny w wygodny sposób z dowolnego miejsca, udzielany przez sieć na żądanie dostęp do wspólnych zasobów obliczeniowych (usługi, aplikacje, pamięć, serwerów, sieci). Mogą one

być błyskawicznie dostarczane i zwalniane, przy minimalnym zaangażowaniu zarządcy i dostawcy usługi. [WWW1]

Model musi spełniać 5 głównych cech, na które zawiera się [WWW2], [MaRo11]:

- Dostęp samoobsługowy na żądanie (ang. On-demand self-service) – bez ingerencji dostawcy usługi. Klient może sam określić poziom zasobów chmury obliczeniowej oraz skorzystać z tak zdefiniowanych możliwości obliczeniowych. Zasoby mogą być dostarczone z zewnątrz organizacji lub być częścią wewnętrznej niededykowanej infrastruktury.

- Swobodny dostęp przez sieć (ang. Broad Network Access) – dostęp do chmury obliczeniowej nie jest ograniczony do wykorzystywanej platformy sprzętowej (komputer, telefon, tablet, itd.) oraz miejsca dostępu. Podłączenie do usługi przebiega poprzez Internet z dowolnego miejsca.

- Łączenie zasobów (ang. Resource pooling) – dostawca zasobów usługi łączy wielu klientów używając technologii wirtualizacji, dzięki fizycznemu i wirtualnemu przydziałowi potrzebnych zasobów. Umożliwia to dynamiczny przydział i późniejsze uwalnianie wykorzystywanej mocy obliczeniowej. Takie działanie umożliwia dostawcy swobodne rozbudowywanie infrastruktury, dzięki czemu centra danych mogą być dowolnych rozmiarów. Przez takie postepowanie klient jest fizycznie oddzielony od serwerów i nie ma konkretniej wiedzy, gdzie w danym momencie znajdują się jego dane. Wiedza znajduje się na wyższym poziomie abstrakcji, np. w którym kraju znajdują się serwery lub które centrum danych aktualnie wykonuje prace dla klienta.

- Natychmiastowa elastyczność (ang. Rapid elasticty) – usługa powinna być elastycznie dostarczana i zwalniana według zapotrzebowania. W odpowiedzi na żądanie, usługa powinna być szybko skalowana. Może to nastąpić poprzez zwiększenie mocy obliczeniowej lub dodanie maszyny wirtualnej do pracy. Klient powinien mieć wrażenie, że dysponuje nieograniczonymi zasobami informatycznymi, w każdym momencie pracy.

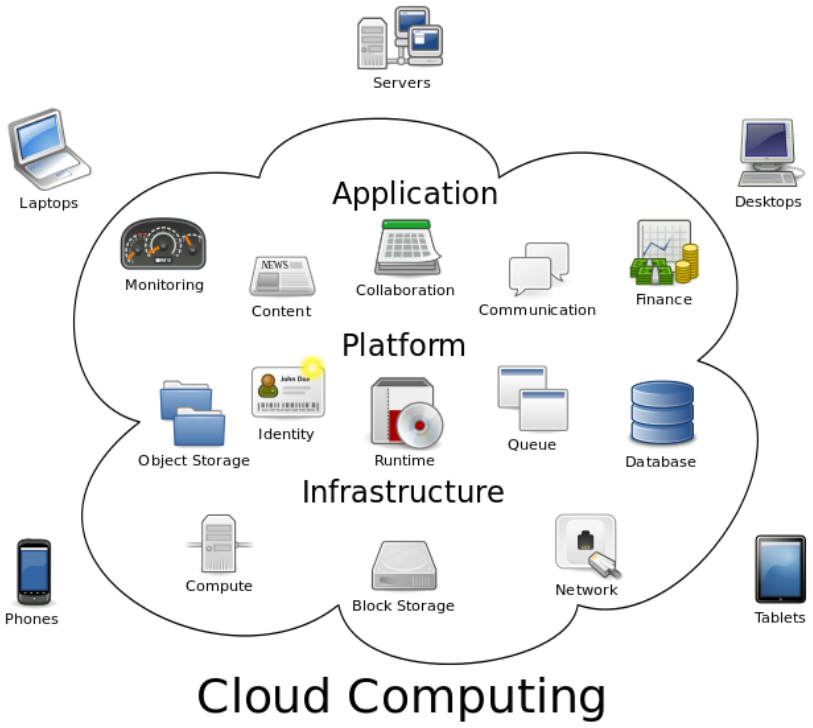
- Mierzalność usługi (ang. Measured service) – automatyczny system kontroli chmury umożliwia monitorowanie stopnia wykorzystania usługi. Mierzone są wykorzystana pamięć, moc obliczeniowa, obciążenie łącza, itd. Uzyskane

raporty zapewniają przejrzystość działań oraz stanową podstawę rozliczenia dostawcy z klientem.

A. Mateos w książce [MaRo11] definiuje chmurę obliczeniową w następujący sposób. „Na najwyższym poziomie chmurę obliczeniową można zdefiniować jako usługi (serwisy) obliczeniowe, oferowane przez zewnętrzne podmioty i dostępne na żądanie w dowolnym momencie, skalujące się dynamicznie w odpowiedzi na zmieniające się zapotrzebowanie.” Mateos wskazuje chmurę obliczeniową jako model ekonomiczny firmy, w mniejszym stopniu jako architekturę typu klient serwer. Jest ona alternatywą do posiadania własnego centrum danych, które wymaga zainwestowania sporych kosztów podczas budowy i dalszego utrzymania.

1.2. Podział chmury obliczeniowej ze względu na rodzaj usługi

Sklasyfikowanie chmury obliczeniowej do konkretnej dziedziny tego rozwiązania, nie przebiega w jednoznaczny sposób. Jednym z najpopularniejszych sposób podzielenia chmury to określenie jej jako zorientowanej na usługi. W języku angielskim występuje akronim EaaS (ang. Everything as a services), gdzie E zamienia się na pożądaną usługę. Wymienia się trzy główne gałęzie podziału: Infrastruktura jako usługa (IaaS), Platforma jako usługa (PaaS) oraz Oprogramowanie jako usługa (SaaS). Na rysunku nr 1 zaprezentowano przykładowy przydział komponentów dla każdej usługi. Został on dokonany w płaszczyźnie horyzontalnej. W dalszej części pracy, zostały omówione poszczególne dziedziny. Do napisania tego podrozdziału wykorzystano [MaRo11], [SaWo12], [Noga12], [Wart14], [Rosz13], [Zior12] oraz [WWW3], [WWW4], [WWW5].



Rysunek nr 1 Diagram chmury obliczeniowej prezentujący przykładowe komponenty
Źródło: http://foter.com/photo/cloud-computing-10/ - repozytorium wolnych zasobów

1.2.1. Infrastruktura jako usługa

Infrastruktura jako usługa to model chmury obliczeniowej, który polega na dostarczeniu klientowi serwerów lub maszyn wirtualnych, a infrastruktury informatycznej. Jest to najbardziej podstawowy typ chmury. Dostawca zapewnia użytkownikowi moc obliczeniową potrzebną do obsłużenia jego potrzeb, przestrzeń dyskową, prąd elektryczny, łącza internetowe oraz odpowiednią klimatyzację. Jest zobowiązany zapewnić jakość i nieprzerwany dostęp usług. Ponadto, udostępniony jest również interfejs umożliwiający m.in. nadzorowanie pracy, tworzenie backup-ów (kopii zapasowych) systemów operacyjnych, zarzadzanie dostępną przestrzenią i rozliczenie opłat. Wykupienie usługi nie wiąże się z fizycznym dostępem do urządzeń. W niektórych przypadkach dostawca może włączyć sprzęt klienta do dostępnych zasobów poprzez wirtualizację jego maszyn. Ten proces umożliwia zaoferowanie klientowi zwiększoną skalowalność oraz mniej przestojów w pracy.

Klient wybiera parametry udostępnionej infrastruktury oraz jej rozmiary. We własnym zakresie zaopatruje się w systemy operacyjne, na których będzie pracował. Dostarczenie systemu operacyjnego przez usługodawcę wiąże się z dodatkowymi opłatami. Użytkownicy instalują obraz systemu oraz ich oprogramowania w chmurze, a nie na fizycznej instancji serwera. Dostęp do maszyn wirtualnych może odbywać się przez łącze internetowe np. przez

przeglądarkę internetową lub przez dedykowany „cienki” program taki jak Citrix Xen, Microsoft hiper-V, Vmware vSphere, Oracle VM, Oracle VirtualBox.

Model finansowy chmury obliczeniowej jako infrastruktury jest bardzo uproszczony i opiera się na naliczeniu opłat za zarezerwowane maszyny oraz ich rzeczywiste wykorzystanie. Przykładowy wycinek cennika usług zaprezentowano na rysunku nr 2 Wielkość opłat opiera się: na parametrach maszyn wirtualnych (ich moc obliczeniowa, dostępną przestrzeń dyskową, pamięć RAM itd.), umiejscowienie serwerowni, wykorzystanie mocy obliczeniowej, dostępność serwerów oraz zainstalowane dodatkowe oprogramowanie. Dodatkowym czynnikiem jest okres kontraktu, na jaki zostanie podpisany z dostawcą. Opłaty są zazwyczaj naliczane w taryfie godzinowej.

Region: US East (N. Virginia)

	vCPU	ECU	Memory (GiB)	Instance Storage (GB)	mswinSQLEnterprise
Memory Optimized - Current Generation					
r3.2xlarge	8	26	61	1 x 160 SSD	$5.495 per Hour
r3.4xlarge	16	52	122	1 x 320 SSD	$10.774 per Hour
r3.8xlarge	32	104	244	2 x 320 SSD	$18.011 per Hour

Rysunek nr 2 Wycinek cennika wynajmu serwerów oferowanych przez Amazon EC2 z różnymi parametrami świadczonych usług
Źródło: http://aws.amazon.com/ec2/pricing/ (dostęp 04.05.2016r.)

1.2.2. Platforma jako usługa

Platforma jako usługa (ang. Platform as a Services, PaaS) udostępnia gotową platformę do pracy. Zawierają się w niej między innymi aplikacje bazodanowe, środowiska programistyczne, połączenia między nimi oraz niezbędną moc obliczeniową potrzebną do wykonywania zamierzonych zadań. PaaS jest przeznaczona szczególnie dla programistów. Klient nie potrzebuje kupować całego sprzętu potrzebnego do działania i instalowania na nim oprogramowania. Ten obowiązek spoczywa na dostawcy usługi. To dostawca zapewnia nieprzerwane działanie platformy oraz przeprowadza podniesienie (upgrade) działających programów do nowych wersji. Po stronie klienta leży rozwój jego programów i dostosowywanie wersji do zadanego środowiska. W tym rozwiązaniu, za możliwość szybkiego przystąpienia do pracy, po otrzymaniu gotowego środowiska, ograniczana jest

swoboda działania użytkownika. Aplikacje muszą powstać w języku wspieranym przez chmurę oraz nie jest dozwolone swobodne łączenie źródeł, jak to ma miejsce w tradycyjnym procesie deweloperskim.

Na rysunku nr 3 przedstawiono wycinek spisu dostępnych chmur obliczeniowych działających na modelu PaaS. Działają one z wykorzystaniem różnych języków i platform. Niektóre oferują więcej możliwych środowisk od innych.

Name	Status	Runtimes	Scaling	Hosting	Infrastructures	
MoPaaS	Production	erlang java node php python ruby			AS	Details
OrangeScape	Production	java				Details
AppHarbor	Production	dotnet			EU NA	Details
Microsoft Azure	Production	dotnet java node php python ruby extensible			AS EU NA OC SA	Details
Cloud Foundry	Production	go groovy java node php python ruby scala extensible				Details
Jelastic	Production	java node php python ruby extensible			AS EU NA SA	Details
Anynines	Production	groovy java node ruby scala extensible			EU	Details
Heirloom PaaS	Production	cobol java			NA	Details
OpenShift Enterprise	Production	java node perl php python ruby extensible				Details

Rysunek nr 3 Wycinek listy możliwych platform jako usługa z podstawowymi informacjami
Źródło: http://www.paasify.it/vendors

Następną cechą, na która warto zwrócić uwagę, jest oferowana możliwość ręcznego skalowania: wertykalnie (więcej procesorów, pamięci RAM, itd.), horyzontalnie (więcej instancji) lub działanie automatyczne.

Model finansowy platformy jako usługi nieznacznie odbiega od płatności w IaaS. Pierwsza platforma oferowana w chmurze, która nazywała się Zimki, pobierała tylko opłaty za użycie. Wliczało się w to użytą moc obliczeniową, wygenerowany ruch w sieci oraz liczbę wykorzystanych operacji jacascript). Spowodowało to powstanie całych aplikacji opartych wyłącznie na javascrypt-ach i działających w chmurze z całym interfejsem do monitorowania i kontrolowania życia aplikacji. Współcześnie do opłat za wykorzystanie wliczony jest również miesięczny abonament, płacony w zależności od zarezerwowanych usług.

Nazwa usługi	Region	Opis	Przybliżony koszt
Usługa aplikacji	West US	Wystąpienia: 3, godziny: 744, rozmiar: b3, warstwa: podstawowa, połączenia SNI: 0, połączenia IP: 0	$669,60
Baza danych SQL	East US	Bazy danych podstawowa: 2, rozmiar: b	$9,97
Maszyny wirtualne	West US	Maszyny wirtualne standard: 2, typ: windows, rozmiar: a3	$535,68
VPN Gateway	East US	Wysoki poziom wydajności, 20 punktów dostępu na godzinę(s), 2000 GB transferu	$79,80
Wsparcie		Wsparcie programistyczne	$29,00
Visual Studio Team Services	West Europe	Liczba użytkowników: 10, 9000 min kompilacji miesięcznie, 112000 min użytkowników wirtualnych, 9 hostowanych agentów + 0 agentów prywatnych	$560,00
		Miesięcznie	$1884,05

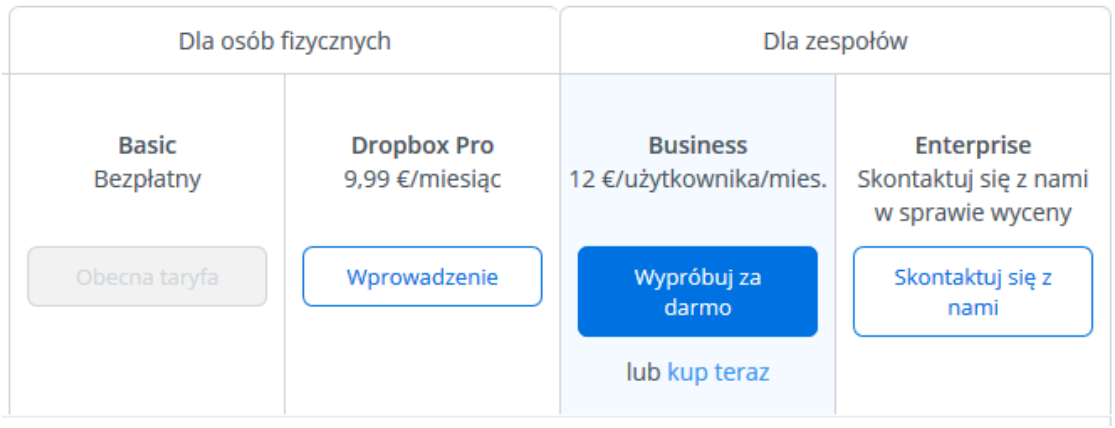
Tabela nr 1 Tabela kosztów miesięcznego wynajmu usług w chmurze Microsoft Azure
Źródło: opracowanie własne na podstawie https://azure.microsoft.com/pl-pl/pricing/calculator/

W tabeli nr 1 zaprezentowano przykładowy koszt miesięcznego wynajmu trzech usług, wspieranych przez 2 bazy, działających na 2 wirtualnych maszynach. Dodatkowo wykupiono 2000GB transferu oraz wsparcie od firmy Microsoft. Najważniejszym elementem zamówienia jest Visula Studio Team Services, które stanowi środowisko programowania, jednocześnie z możliwością testowania obciążania bazującego na chmurze. Zaproponowane ustawienia obejmują najczęściej kupowane usługi, zgodnie z propozycjami kalkulatora udostępnionego przez Microsoft.

1.2.3. Oprogramowanie jako usługa

Trzecią najczęściej wyróżnianą chmurą obliczeniową jest Oprogramowanie jako usługa. Aplikacja jest zainstalowana i wykorzystywana na serwerze usługodawcy, a klient może się do niej połączyć przez Internet. Eliminuje to potrzebę zakupu infrastruktury, nośnika oraz oprogramowania. Przechowywane są również dane należące do klienta, a więc również dostęp do nich odbywa się z dowolnego miejsca. Utrzymanie aplikacji jak i zapewnienie jej odpowiedniego upgradu (podniesienia do nowszej wersji) spoczywa na dostawcy. Usługę SaaS (ang. Software as a Service), można przyrównać do internetowej wypożyczalni programów. Użytkownik płaci każdorazowo za użycie danego oprogramowania, jednocześnie nie jest zobowiązany do ciągłego korzystania ze świadczonych mu usług. Stanowi to główną

korzyść w wykorzystaniu tego modelu. Klient nie ponosi opłat licencyjnych, ponieważ opłaty pobierane są za subskrypcję. Najczęściej wybierane są aplikacje do zarządzania kadrami (HR), zewnętrzna poczta elektroniczna, wirtualne dyski, programy rachunkowo - księgowe oraz zarządzanie relacjami z klientami CRM (ang. Customer relationship management).



Rysunek nr 4 Cennik przykładowej usługi typu SaaS - dropbox.com
źródło: https://www.dropbox.com/plans?trigger=wahexp (dostęp 17.05.2016r.)

Przykładowymi rozwiązaniami typu SaaS są: Microsoft Office 365, Onedrive.com, Salesforce (system CRM), mHR (system HR) lub dropbox.com. Na rysunku nr 4 przedstawiono przykładowy cennik usługi Dropbox. Podstawowa funkcjonalność jest zazwyczaj darmowa, ale zakres świadczonych usług jest drastycznie ograniczony. Dla płatnych wersji dostępna jest pełna funkcjonalność dla klienta, a opłaty naliczane są w formie abonamentu miesięcznego lub rocznego. Przy dużych kontraktach, cena jest ustalana oddzielnie.

1.3. Podział chmury obliczeniowej ze względu na sposób wdrożenia

Przetwarzanie w chmurze powstawało jako ogólnodostępne medium. Istnieje inna typologia chmury obliczeniowej. Jest ona rozróżniana poprzez fizyczną lokalizację serwerów i tych, którzy odpowiadają za jej utrzymanie, a nazwaną ze względu na sposób wdrożenia w organizacji. Zakłada ona istnienie trzech rodzajów chmur: publiczną, prywatną i hybrydową. Na rysunku nr 5 przedstawiono cechy charakterystyczne każdego elementu z tego podziału. W tym podrozdziale zostały one szczegółowo opisane. Zostało to oparte o [WWW2], [WWW6], [WWW7], [WWW8], [Hend13], [LLS14], [MaRo11], [PaZa13] i [Rosz13].

Rysunek nr 5 Porównanie chmur: publicznej, prywatnej i hybrydowej według natężenia ich cech charakterystycznych. Gdzie: 3 - silne natężenie, 2 – średnie, 1 – słabe, 0 – brak
Źródło: opracowanie własne na podstawie [Rosz13]

1.3.1. Chmura publiczna

Chmura publiczna (ang. Public cloud) jest najczęściej kojarzonym modelem dostępu do chmur obliczeniowych, ponieważ najlepiej oddaje idee współdzielenia przez Internet zasobów, dostarczanych przez zewnętrznego dostawcę [Rosz13].

Usługodawca może świadczyć wyspecjalizowany rodzaj usługi, ale posiadać w ofercie również modele (infrastrukturę informatyczną, platformy programistyczne oraz całe aplikacje), które można łączyć ze sobą, tworząc złożone systemy. Dostęp do chmury jest powszechny. Usługobiorca płaci za wykorzystaną infrastrukturę, czas pracy oraz przesłane dane, lecz może zrezygnować z usługi w dowolnym momencie. W razie wystąpienia zwiększonego zapotrzebowania, niż pierwotnie zostało zadeklarowane, istnieje możliwość dokupienia brakujących zasobów. W zależności od rodzaju platformy chmura może rozszerzać się w locie, bez potrzeby ingerencji klienta i ponownego uruchomienia wirtualnej maszyny oraz serwerów usługi. Opłaty są naliczane automatycznie, a informacje o nich dostępne są na portalu zarządzającym chmura obliczeniową.

Na rynku dostawców usług panuje duża konkurencja. Dostarczenie chmury publicznej dla firm ma w swojej ofercie m.n. Amazon, Google, Microsofr, Salesforce. Dzięki temu, klienci mają zapewnione atrakcyjne parametry oferowanego sprzętu przy konkurencyjnych cenach. Rywalizacja wymusza ciągłe udoskonalanie. Dostęp do chmury posiada również nabywca prywaty, zazwyczaj jednak w ograniczonej formie w postaci bezpłatnej poczty elektronicznej (Gmail, Hotmail), dyski wirtualne (Dropbox.com, Onedrive.com).

Cechy chmury publicznej zostały przedstawione na rysunku nr 5. Wyróżniającymi cechami jest słaba elastyczność dla działających infrastruktur, niskie koszty posiadania i utrzymania chmury publicznej, dużą wydajność infrastruktury oraz niskie bezpieczeństwo.

- Słaba elastyczność - Usługodawca oferuje jasno zdefiniowaną usługę oraz infrastrukturę. Nie ma możliwości dostosowania jej dla każdego potencjalnego klienta. Takowy jest zmuszony korzystać z istniejących zasobów. Generuje to możliwe problemy, podczas dostosowywania się do wszystkich potrzeb usługobiorcy.

- Niskie koszty posiadania – Korzystne dla klienta z powodu braku kosztów posiadania własnego sprzętu oraz potrzeb jego serwisowania. Dostawca usługi może wykorzystać efekt skali ograniczając koszty stałe dla stworzonej infrastruktury. Podejście masowe umożliwia rozważenie lokalizacji serwerowni w oparciu o najkorzystniejsze parametry terenu (temperatura, dostępność taniej energii, wykształcona kadra).

- Wysoka wydajność – Moc obliczeniowa nie jest marnowana, gdyż serwery mogą działać w sposób ciągły, bez generowania przestojów. Koszt uzyskania zadanej mocy obliczeniowej jest wtedy bardzo niski. Dodatkowo klient może dodać swoje własne zasoby. Dostarczana moc jest zależna od wysokości budżetu klienta.

- Słabe bezpieczeństwo – Transfer danych wrażliwych na serwery zewnętrzne nie jest postrzegany korzystnie przez kadrę zarządzającą. Dane firmy stanowią o jej przewadze na rynku. Wyciek danych może kosztować utratę przewagi lub całego przedsiębiorstwa. Bezpieczeństwo chmury publicznej sprowadza się do szybkości wykrycia i reagowania na luki w bezpieczeństwie. Istotna jest również redundancja czyli nadmiarowość zabezpieczeń dostawcy. Dostawca chmury publicznej zobowiązuje się do zapewnienia bezpieczeństwa danych

klienta. Świadczą o tym uzyskane certyfikaty, regularne audyty bezpieczeństwa oraz standardy bezpieczeństwa.

1.3.2. Chmura prywatna

Chmura prywatna (ang. Private cloud) to model chmury obliczeniowej, której zasoby znajdują się w siedzibie przedsiębiorstwa i są udostępnione poprzez zabezpieczone kanały komunikacji dla pracowników firmy, partnerów biznesowych oraz szeroko pojętym spółkom zależnym. Ma to na celu zapobieżenie nieautoryzowanemu dostępowi do sieci, gdzie cała moc obliczeniowa jest wykorzystywana na własne potrzeby. Aby rozpocząć pracę w chmurze prywatnej, wystarczy połączyć istniejący sprzęt wydajnym medium transmisji, a następnie zwirtualizować zadane zasoby. Można to zrobić za pomocą narzędzi hipernadzorcy, takich jak Vmware lub Xen. Zalecane jest wykorzystanie wyspecjalizowanych narzędzi do tworzenia chmur, które znajdują się na rynku w wersji komercyjnej lub na zasadzie open-sources. Zapewnia to płynniejsze działanie chmury oraz większy komfort klientów. Istnieją przypadki, gdy identyczna architektura znajduje się dodatkowo poza siedzibą firmy, aby zapewnić bezpieczne, zapasowe środowisko pracy.

Chmura prywatna nie jest zalecana dla małych przedsiębiorstw, które nie mogą sobie pozwolić na taką skalę przedsięwzięcia, jaka występuje podczas tworzenia chmury. Najczęstszymi użytkownikami są duże przedsiębiorstwa, które mają wysokie wymagania względem bezpieczeństwa, prawa lub specyfikę pracy, wymagającą podwyższonej elastyczności, bez możliwych kompromisów. Przy pełnej automatyzacji procesu, użytkownik może szybko postawić potrzebną platformę według wymaganych parametrów z istniejącej kopii lub stworzyć całkowicie nowy system.

Na rysunku nr 5 kolorem pomarańczowym przedstawiono cechy charakterystyczne dla chmury prywatnej. Należą do nich wysokie koszty utrzymania, duże bezpieczeństwo, średnia elastyczność i średnia wydajność.

- Duże koszty utrzymania – Podczas uruchamiania chmury należy uwzględnić projekt architektury tworzonej struktury, zakup nowego sprzętu wraz z możliwością przyszłej rozbudowy infrastruktury, zakup odpowiedniej platformy programowania wraz z wymaganą liczbą licencji dla eksploatowanych programów. Dodatkowo należy wliczyć koszty wdrożenia nowego rozwiązania w firme, stworzenie odpowiedniego działu odpowiedzialnego za utrzymanie oraz bezpieczeństwo chmury wraz

z wykwalifikowaną kadrą. Dodatkowo należy uwzględnić koszty stałe, t.j. opłaty za wykorzystany prąd i chłodzenie.

- Duże bezpieczeństwo – wynika bezpośrednio z umiejętności kadry odpowiedzialnej za bezpieczeństwo oraz z lokalizacji serwerów chmury. Już podczas tworzenia przyszłej infrastruktury, zostają wdrożone procedury bezpieczeństwa, które obowiązują w firmie. Zazwyczaj chmura nie znajduje się bezpośrednio w sieci Internet, przez co ogranicza się duże spektrum możliwych wektorów ataku. Pracownicy powinni stale zwiększać swoją świadomość i umiejętności z dziedziny bezpieczeństwa.

- Średnia elastyczność – W czasie tworzenia chmury, może ona spełniać swoje wymagania i dowolnie się dopasowywać. Z czasem jedna, ujawnią się jej ograniczenia względem własnej infrastruktury. To co początkowo spełniało założenia, z czasem będzie odbiegać od standardów. W przedsiębiorstwach, które korzystają z tego rozwiązania, może zaniknąć nacisk na modernizację sprzętu.

- Średnia wydajność – W podobny sposób jak kryterium elastyczności, w czasie tworzenia struktury, będzie zadowalająco spełniać swoje zadania. W tym modelu może zaniknąć potrzeba ciągłej modernizacji sprzętu, co jest nieodłączną cechą chmury publicznej. Prowadzi to do spadku wydajności posiadanej infrastruktury.

Naturalnym krokiem rozwoju przedsiębiorstwa jest przejście z chmury prywatnej do chmury hybrydowej, która może przynieść korzyści dla przedsiębiorstwa.

1.3.3. Chmura hybrydowa

Chmura hybrydowa (ang. hybrid cloud) to według NIST [WWW2] infrastruktura złożona z dwóch lub więcej chmur (publicznych, wspólnotowych lub prywatnych), gdzie każda działa we własnym zakresie, a w razie potrzeby przekazuje i współdzieli wymagane dane do pracy. W tym modelu przedsiębiorstwo zazwyczaj korzysta z chmury prywatnej i w razie potrzeby rozszerza swoje zasoby o te, dostarczone z chmury publicznej. Pozwala to minimalizować koszty wynikające z pracy chmury publicznej. W monecie połączenia oprogramowanie stara się zrównoważyć obciążenie chmur poprzez optymalizację zadań. Takie działanie jest określane mianem rozsadzania chmury (ang. cloud bursting). Polega ono na przenoszeniu aplikacji i wymaganych danych między chmurami. Jest wymagane

zastosowanie tej samej technologii we wszystkich wykorzystywanych chmurach. Przykładem oprogramowania umożlwiającego współdzielenie informacji między chmurami jest vSphere vMotion, umieszony w oprogramowaniu Vmware.

Na rysunku nr 5 kolorem czerwonym przedstawiono cechy charakterystyczne dla chmury hybrydowej. Należą do nich wysokie koszty utrzymania, duże bezpieczeństwo, duża elastyczność i wysoka wydajność.

- Wysoka wydajność – Użytkownik może korzystać z dostępnych zasobów w siedzibie firmy i w razie potrzeby może skorzystać z mocy obliczeniowej, zaczerpniętej z chmury publicznej. Tworzy to pozorną nieograniczoną moc obliczeniowa przy dużej wydajności.

- Wysoka elastyczność – Dzięki wykorzystaniu architektury chmury prywatnej, użytkownik może szybko zaspokoić zapotrzebowanie firmy i dowolnie rozszerzyć o nowe możliwości z kolejnej chmury. Dzieje się to poprzez oprogramowanie tego samego producenta, które jest stworzone do wspólnej pracy, a dodatkowo zwiększa elastyczność oraz bezpieczeństwo.

- Wysokie bezpieczeństwo – Połączenie chmur jest możliwe dzięki zastosowaniu tego samego oprogramowania. Ułatwia to nadzorowanie sprzętu, poprzez ograniczenie możliwych wektorów ataku. Dodatkowo, przy stworzonej chmurze prywatnej, są wdrożone wysokie standardy bezpieczeństwa. Podczas włączenia chmury publicznej, są one stosowane również w niej.

- Wysokie koszty utrzymania – Koszty wdrożenia i utrzymania są najwyższe z opisywanych w tej pracy. Generuje je kompleksowe wykorzystanie modeli chmur obliczeniowych.

Rozdział II Bezpieczeństwo w cyberprzestrzeni oraz sposoby przełamywania zabezpieczeń

Chmura obliczeniowa zapewnia wiele korzyści dla przedsiębiorstwa, które je zastosuje, jak i dla zwykłego użytkownika indywidualnego. Wraz z rozwojem chmury i zwiększaniem jej możliwości, będzie ona wkraczała w coraz bardziej żywotne elementy życia organizacji i jednostki. Zwiększy się zapotrzebowanie na ochronę zgromadzonych zasobów (obronność) i działających mechanizmów. Zgodnie z rozwojem cyfryzacji, zwiększa się liczba możliwych wektorów ataku na obiekt. Istnieje wiele zagrożeń. Są one fizyczne oraz wirtualne. W tym rozdziale zostanie przeprowadzona analiza sensu bezpieczeństwa oraz próba jego zdefiniowania na przykładzie jednostki, obszaru jako państwa oraz bezpieczeństwa w sieci. Zostanie również określona definicja zagrożenia oraz przedstawienie jego wpływu na bezpieczeństwo.

W dalszej części zostały omówione przykładowe zagrożenia i sposoby ataku na sieć, zasoby, oraz systemy działające w sieci Internet.

2.1. Bezpieczeństwo i jego znaczenie

Bezpieczeństwo stanowi podstawową potrzebę każdej istoty. Jest to fakt powszechnie akceptowany. Podstawowe potrzeby zostały scharakteryzowane i opisane na piramidzie potrzeb A. Maslowa. Według jego teorii potrzeby są zaspokajane stopniowo, a przejście do wyższych potrzeb nie odbywa się bez uzyskania wcześniejszych. Schemat został przedstawiony na rysunku nr 6.

Rysunek nr 6 Piramida potrzeb ludzkich według A. Maslowa
Źródło: http://www.graniczne.amu.edu.pl/PPGWiki/wiki/Mas%C5%82ow (dostęp 15.08.2016r.)

Składają się na nią podgrupy potrzeb:

- Fizjologiczne (zaspokojenie głodu, pragnienia, snu czy innych funkcji biologicznych).
- Bezpieczeństwa (zapewnienie życia bez trosk, poczucie psychicznego i fizycznego nie zagrożenia, stabilności, ochrony i porządku).
- Afiliacji (przynależności, kontaktu, miłości, przyjaźni).
- Szacunku (zdobycie osiągnięć, uznania, prestiżu, szacunku dla samego siebie oraz od innych osób).
- Samorealizacji (realizacji swoich zainteresowań, rozwoju, wykorzystania posiadach zdolności i wiedzy).

Bezpieczeństwo jest zbiorem potrzeb, które wymagają spełnienia zaraz po filologicznych. Powinno być podstawowym zadaniem każdego państwa i organizacji. Należy stworzyć system zabezpieczeń, a następnie ciągle do ulepszać. Zapewni to efektywniejsze działanie oraz pozwoli skupić się na bardziej zaawansowanych potrzebach i celach. Zagłębiając się w pojęcie bezpieczeństwa należy określić czym ono jest, w jakim środowisku się odbywa oraz na jakich płaszczyznach.

Pojęcie bezpieczeństwa nie posiada jednej, powszechnie uznanej definicji. Jest ona zależna od dziedziny, w ramach której podlega ona interpretacji. Pojawia się ona w różnych naukach: prawie, historii ekonomii, socjologii, politologii, stosunkach międzynarodowych i innych. Świadczy o tym między innymi Słownik Języka Polskiego [WWW12] w którym pod pojęciem bezpieczeństwo, ograniczono się do stwierdzenia „Stanu niezagrożenia". Stanowi to pochodną tłumaczenia pojęcia z łacińskiego sine cura (securitas), co można przetłumaczyć jako stan bez troski, bez zmartwień, zmian, niepokojów [KaSk98]. Dokładniejsza definicja została przedstawiona w pracy [PaSz12], według której, „bezpieczeństwo jest stanem, który daje poczucie pewności i gwarantuje tak jego zachowanie jak i szansę na doskonalenie. (…) odznacza się brakiem ryzyka utraty czegoś, co człowiek szczególnie ceni." Zgodnie z tym twierdzeniem możemy wyróżnić przestrzenie bezpieczeństwa, taki jak: narodowe, regionalne, globalne. Występują tez inne przestrzenie, przykładowo bezpieczeństwo socjalne, psychiczne, fizyczne lub personalne i strukturalne oraz militarne i niemilitarne, zewnętrzne i wewnętrzne. Inny aspekt przedstawił J .S. Nye w [Łęża14]. Określił on dwa sposoby przedstawienia bezpieczeństwa. W sposób pozytywny –

jako możliwość przetrwania danego podmiotu, oraz w sposób negatywny – jako stan braku zagrożenia.

W pracy [PaSz12] umieszczono stwierdzenie, że warto wyodrębnić trzy wymiary, które dzielą pojęcie bezpieczeństwa:

- Podmiotowe – rozważa się tu zapewnienie istnienie i przetrwania badanego podmiotu jako uczestnika życia społecznego.
- Przedmiotowe – zapewnienie przetrwania stanu posiadania jednostki, w tym również zachowania tożsamości oraz możliwego swobodnego rozwoju.
- Proceduralne – odnosi się do niestałych, zmieniających w czasie realiów, zapewniających subiektywne i obiektywne zaspokojenie dwóch wcześniejszych wymiarów.

Niektóre opracowania, takie jak [Łęża14], zawierają się stwierdzenia, że bezpieczeństwo stanowi jedną z cech porządku międzynarodowego, zarówno w aspektach praktycznych, jak i teoretycznych. Stwierdzenie jego braku powoduje niepokój oraz poczucie zagrożenia, co może skutkować niebezpiecznymi sytuacjami na arenie międzynarodowej jak i narodowej.

Bezpieczeństwo rozpatrywane w sensie narodowym przybiera inne znaczenie. Określa zdolność państwa do zabezpieczenia wartości wewnętrznych przed zagrożeniami czyhającymi na zewnątrz państwa jak i wewnątrz. Odnosi się to do zapewnienia istnienia państwa i narodu, obrony granic oraz zapewniania suwerenności wobec innych narodów [Zięb99]. Należy zaznaczyć, że bezpieczeństwo państwa stawiane jest ponad bezpieczeństwem międzynarodowym. Bierze się to z zależności rządzących wobec narodu oraz odpowiedzialności jaką biorą na siebie podejmując władzę. Z drugiej strony, ta teorii zwraca uwagę, że bezpieczeństwo państwowe tworzy ład międzynarodowy i zapewnia działania zewnętrzne i wewnętrzne. Stanowi to aspekt postępującej globalizacji, również w aspekcie bezpieczeństwa.

Państwo można uznać za bezpieczne tylko wtedy, gdy spełnione są następujące warunki składowe [KwLi00]:

- Nie jest zagrożone terytorium państwa

- Obywatele oraz mieszkańcy terytorium zajmowanego przez państwo, będą czuli się bezpiecznie. Muszą być zapewnione ich prawa i wolności oraz ich byt.
- Ustanowione władze będą działały w interesie obywateli, ich suwerenności, zgodnie z obowiązującą konstytucją.

Zadane składowe znajdują się w konstytucji RP w artykule 5: „Rzeczpospolita Polska strzeże niepodległości i nienaruszalności swojego terytorium, zapewnia wolności i prawa człowieka i obywatela oraz bezpieczeństwo obywateli, strzeże dziedzictwa narodowego(…)”. Stanowią one potwierdzenie badanych składowych.

Inną definicję bezpieczeństwa przedstawiło Biuro Bezpieczeństwa Narodowego dotyczącego cyberprzestrzeni. Stanowi ona składową ze źródeł [WWW9], [WWW10], [WWW11]. Według niej bezpieczeństwo cyberprzestrzeni obejmuje zespół przedsięwzięć technicznych, fizycznych, organizacyjno-prawnych i edukacyjnych, dzięki którym zostanie zapewnione funkcjonowanie cyberprzestrzeni bez zakłóceń. Państwowe cyberbezpieczeństwo stawia sobie za cel utrzymanie bezpiecznego funkcjonowania krytycznej infrastruktury teleinformacyjnej państwa oraz jej wykorzystanie jej strategicznych zasobów informacyjnych. W tym wypadku, bezpieczeństwo zostało sprowadzone do ochrony integralności sieci oraz zasobów. Możliwość działania i rozwoju wymaga zapewnienia ochrony przed możliwymi atakami szkodliwego oprogramowania oraz hakerów.

Rozpatrując istotę bezpieczeństwa, należy rozważyć jego związek ze zjawiskiem zagrożenia. Wcześniej, zostało już wskazane, ze brak zagrożenia jest czasami wyznacznikiem bezpieczeństwa. R. Zięba w [Zięb99] przedstawia w swojej pracy zagrożenie, jako stan psychiki lub świadomości zaistnienia czynników, które odbierane są jako niekorzystne lub niebezpieczne dla istnienia danej jednostki. W aspekcie państwowym leżą one u podstaw decyzji podejmowanych przez rządzących w celu ich zwalczania i umacniania bezpieczeństwa krajowego. W aspekcie cyberprzestrzeni odnoszą się one do możliwych ataków na istnienie i działanie systemów lub sieci.

Dokładniejszą definicję zagrożeń pod względem cyberprzestrzeni podaje Krzysztof Jakubowski w [Doro01]. Określa on zagrożenie jako „zjawisko kryminologiczne, obejmujące wszelkie zachowania przestępcze związane z funkcjonowaniem systemu elektronicznego przetwarzania danych, godząc bezpośrednio w przetworzoną informację, jej nośnik i obieg w komputerze oraz cały system połączeń komputerowych”. Zgodnie z tą definicja, zagrożenie

nie tylko może godzić w istnienie informacji, ale również w sposób jej przetwarzania, przekazywania oraz magazynowania.

2.2. Rodzaje ataków

W zmieniającym się świecie, w którym prężnie rozwija się cyberprzestrzeń, rozwijane są również zabezpieczenia w sieci. Wraz z nimi, opracowywane są coraz bardziej przemyślane sposoby przełamywania tych zabezpieczeń. Istnieje wiele rodzajów zagrożeń i możliwych ataków na istniejącą infrastrukturę w cyberprzestrzeni. W tym podrozdziale zostały przedstawione przykładowe ataki, stanowiące wyzwanie dla pojęcia bezpieczeństwa. Podrozdział został opracowany na podstawie następujących źródeł: [Batk11], [LiTi04], [Doro01], [WWW21], [WWW22], [WWW23], [WWW24], [WWW25], [WWW26], [WWW27], [WWW28], [WWW29]. Przykłady ataków cybernetycznych

a) Network snooping (namierzanie sieci) – jest to rodzaj ataku powszechnie uważany w środowisku za jeden z najbardziej wysublimowanych metod. W celu jej wykorzystania, atakujący używa przeróżnych analizatorów sieci. Na podstawie otrzymanych wyników agresor może określić, który atak będzie najkorzystniejszy dla jego celów. Maja one odnaleźć i zdefiniować słabe punkty sieci i jej zabezpieczeń. Jest to określane poprzez dogłębną analizę protokołów sieci oraz śledzenia odbywającego się w niej ruchu. Jedną z technik tego ataku jest próbkowanie, w czasie którego odbywa się próba połączenia z obiektami w danej sieci oraz określenie ich charakterystyki. Wykrycie tych metod jest niezwykle trudne, ponieważ odbywają się na podstawie poprawnych i legalnych sposobach dostępu do sieci. Najczęściej takie działania pozostają niewykryte. Obeznany z tematyką intruz, zazwyczaj tylko raz przeprowadza rozpoznanie sieci i na jego podstawie jest gotowy przeprowadzić kolejny, właściwy atak.

b) Skanowanie – stanowi rozszerzenie network snoopingu poprzez przeglądanie adresów sieciowych oraz portów sieciowych atakowanego obiektu. Przeglądanie adresów polega na przeszukiwaniu kolejnych adresów z zadanego zakresu by odnaleźć cel oraz jak najlepszego określenia budowy badanej sieci. W wypadku niezabezpieczonej sieci, można rozpoznać jej topologię oraz na jakich systemach operacyjnych działają serwery. Atak polega na wysyłaniu zapytania do pod każdy adres oraz oczekiwanie na odpowiedź. Nadejdzie ona w wypadku stwierdzenia istnienia adresata lub gdy z powodu niedostatecznych zabezpieczeń nie jest wyłączona odpowiedz na takie zapytania. Jest to atak stosunkowo łatwy do

wykrycia.

Inną metoda skanowania jest nasłuchiwanie portów sieciowych. Atak sprowadza się do odpytywania kolejnych portów, w celu stwierdzenia czy dany port jest otwarty oraz jakie usługi się przez niego odbywają w danym systemie. Dzięki tej metodzie można uzyskać informację na temat urządzeń wykorzystywanych w systemie zabezpieczeń. Dzieje się to poprzez ustalenie systemu operacyjnego ofiary, aktywnych aplikacji i wykorzystywanych protokołów transmisji. Atakujący zazwyczaj stara się ukryć odpytania pośród innych połączeń i odpytuje losowe porty. Większość standardowych zabezpieczeń potrafi wykryć powtarzające się odpytania do kolejnych portów i zablokować takie działania. Inną metoda ukrycia działań jest wydłużenie czasu działań i zmiana adresu z którego następuje atak. W takim wypadku, kolejne działania mogą dziać się kilka razy na dzień, a nie wszystkie naraz. Dodatkowo istnieje możliwość rozbicie pakietów, które tworzą odpytanie, na mniejsze, w celu łatwiejszego przeniknięcia przez filtry zabezpieczeń. Od skanowania zaczyna się większość ataków.

c) Fingerprinting – jest to atak wykorzystujący lukę w zabezpieczeniach, informujący o wersji systemu operacyjnego zainstalowanego na urządzeniu. Dzieje się tak dzięki odciskowi palca (ang. fingerprint) stosu TCP/IP. Badana jest kolejność występowania protokołów i w jaki sposób są interpretowane próbki pakietów. Każdy system interpretuje je na swój własny sposób i w odpowiedniej kolejności. Atak jest wykorzystywany jako przygotowanie do dalszych akcji, ponieważ poszczególne luki w oprogramowaniu są ściśle określony z platformą i systemem, w którym się znajdują. Istnieje możliwość pozyskanie danych o systemie z innych źródeł, jak banery zawierające nagłówki storn internetowych, czy mapowane aplikacje. Odnosi się ona do sprawdzania, jaka usługa korzysta z portu, oraz jakie pakiety mogą przez niego przejść.

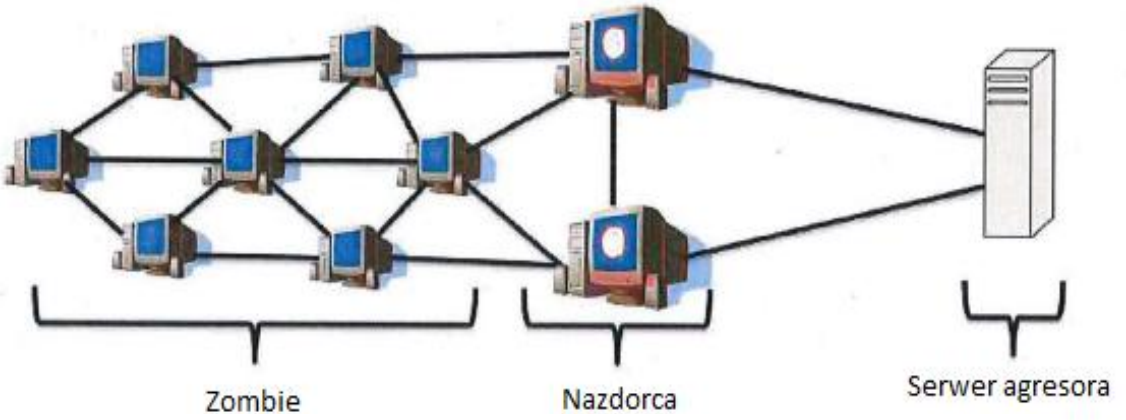
d) Podsłuch (ang. Sniffing) – jest to atak polegający na podsłuchiwaniu transmisji sieci. Za pomocą tej metody nie przeprowadza się bezpośredniego ataku na sieć, ale rejestruje odebrane identyfikatory wraz z hasłami, które są przesyłane przez autoryzowanych użytkowników w trakcie logowania do zabezpieczonych sieci. Podstawowe narzędzia do wykorzystywania tej metody zapisują tylko nazwy i hasła użytkowników. Zaawansowane narzędzia są w stanie zarejestrować cały ruch w sieci. Z tych narzędzie korzysta się również do diagnostyki sieci. Za

pomocą tej metody mogą być przechwycone również transmisje elektromagnetyczne wytwarzane przez podzespoły komputera. Do tych transmisji należy m.in. sygnał z karty graficznej do monitora lub wciskane przyciski na klawiaturze. Tak wysoko specjalistyczne wykorzystanie metody nie jest powszechnie stosowane, ponieważ dostrojenie się do emisji urządzeń jest trudne techniczne i kosztowne. Na taki wydatek mogą sobie pozwolić tylko duże organizacje i wywiad państwowy.

e) Flooding attack – jest to rodzaj ataku polegający na „zalaniu" (wysłaniu) ofiary ogromną liczbą pakietów i zapytań. Skutkuje to unieruchomieniem serwera, sieci lub klienta ofiary. Jest to bardzo niebezpieczne dla użytkownika sieci Internet, a w szczególności, korzystających z cloud computing. Można wyróżnić dwa podstawowe rodzaje ataku, gdzie jeden wynika z drugiego. Są nimi DoS oraz DDoS.

   - DoS – ang. Denial of Services (blokada usługi). Jest to atak łatwy do przeprowadzenia, nawet przez poczatkujących hakerów, a jego efekty widać natychmiastowo. Celem ataku jest unieruchomienie świadczonych przez serwer usług, przeciążenie danych obsługujących klientów lub wyłączenie sprzętu z użytku. Dzieje się to poprzez najczęściej poprzez zalanie sieć danymi, aż do wyczerpania dostępnego pasma transmisji. Dodatkowo, atakujący może korzystać z błędów w protokołach transmisji, ich złej implementacji na serwerze lub w oparciu o fizyczne i logiczne ograniczenia protokołów. W razie wykorzystana takiej luki w protokole, podatnym na atak staje się każdy host, który wykorzystuje dany protokół w swojej pracy. Wymagana jest wtedy korekta programu przez programistę. Efektem ataku może być: wstrzymanie usługi poprzez mechanizm starający się zachować niezawodność systemu, tymczasowo odłączając połączenia z konkretnych źródeł. Następnym efektem może być zniszczenie zasobów, poprzez doprowadzenie ich do niestabilnego stanu, który nie funkcjonuje prawidłowo. Powstaje wtedy błąd obiektu, który jest usuwany przez system. Może to skutkować zamknięciem całego systemu operacyjnego. Ostatnim efektem jest wyczerpanie zasobów. W takim wypadku, wysyłane obiekty docierają z opóźnieniem, czasem tak wielkim, ze zostają uszkodzone lub nieprzyjęte przez system.

- DDoS – rozproszona odmowa usługi (ang. distributed denial od service) to atak bazujący na DoS. Również ma na celu zajecie wszystkich dostępnych zasobów. Różnica polega na skali ataku, czyli przeprowadzaniu go z wielu komputerów. Przygotowując się do ataku, zarażane są różne komputery i serwery przez robaki i trojany, z których tworzone są sieci bot net. Jednostki w sieci są nazywane zombie, czyli takie które bez wiedzy



Rysunek nr 7 Schemat botnetu wykorzystywanego przy atakach DDoS
źródło: http://krebsonsecurity.com/2014/06/backstage-with-the-gameover-botnet-hijackers/ (dostęp 30.08.2016r)

właściciela są sterowane przez zewnętrzną osobę. Przykładowy Botnet został przedstawiony na rysunku nr 7.

Są one zorganizowane w hierarchię, gdzie dużą liczną hostów steruje tylko kilka nadzorców (masterów). To jednostki nadrzędne posiadają zakodowany adres ofiary, który przesyłają w dół hierarchii. Na sygnał agresora, zombie podejmuje próbę połączenia się z daną siecią lub hostem starając się skorzystać z jego usług. Ofiara próbując odpowiedzieć na zapytania, musi przydzielać zasoby do każdej prośby, docelowo przeciążając swoje zdolności do odpowiadania i unieruchamia usługi. Zaletą ataku jest trudność w wykryciu sprawcy, pomimo natychmiastowego rozpoznaniu agresji. Ponadto narzędzia użyte do ataku można wykorzystać do innych działań kryminalnych. Obrona przed tym atakiem jest niezwykle trudna, ponieważ może wystąpić naturalnie, podczas dużego zainteresowania użytkowników daną usługą. Próby ograniczenia możliwości połączeń, mogą skutkować zrażeniem

potencjalnych klientów. Bardzo często groźba ataku jest stosowany jako szantaż lub próba wpłynięcia na daną jednostkę lub podmiot.

f) Spoofing – istotą tego ataku jest podszycie się pod inny element sieci, który posiada autoryzowany dostęp. Ma to na celu oszukanie zastosowanego mechanizmu zabezpieczeń. Atakujący może pozyskać dostęp do sieci, danych lub zakłócić poprawne funkcjonowanie sieci. Atak odbywa się poprzez wysłanie odpowiednio spreparowane pakiety danych do sieci lub poprzez błędne wykorzystanie protokołów. Tą metodę ataku można podzielić na kilka rodzajów:

   - IP spoofing – nazywany maskaradą, opiera się na podmianie źródłowego adresu IP, który wskazuje na autoryzowaną maszynę. Może on pochodzić z wcześniej zdobytego źródła lub z publicznej puli adresów IP. Atak jest wykorzystywany w celu utrudnienia dostępu do usługi (DoS) poprzez komplikowanie wymiany pakietów w sieci.

   - DNS spoofing – Atak polega na sfałszowaniu serwera nazw (DNS) lub podmiany adresów IP przyporządkowanych do wpisywanych domen. Dzięki podmianie wzorca adresu, ofiara wpisując poprawną domenę, zostaje przekierowana na komputer agresora.

   - ARP spoofing – atak odbywa się wewnątrz sieci. W sieci każdy posiada swój adres składający się z IP i MAC urządzenia, zgodnie z protokołem ARP. Za pomocą niego odbywa się komunikacja wewnątrz sieci. Atakujący podszywa się pod znany host w sieci w czasie rozsyłania zapytania ARP w celu aktualizacji tablic. Poprawny adres wysyłany jest do agresora, który podmienia go na swoje dane, po czym przesyła go do ofiary. Za pomocą tego ataku, można ominąć zaporę ogniową oraz mechanizm dynamicznego przydzielania adresów. Efektem jest uzyskanie dostępu do danych.

   - Web spoofing – atak zazwyczaj polega na skopiowaniu lub odtworzeniu istniejącej strony. Jest to możliwe dzięki mechanizmom umożliwiającym oglądanie stron offline. Następnie strona jest modyfikowana, zgodnie z potrzebami agresora i wysyłana do ofiary za pomocą emaila lub przekierowania bezpośrednio z oryginalnej strony. Podczas ataku ofiara wysyła swoje dane, np. logowania, hasło lub dane karty kredytowej na

serwer atakującego, przekonana o prawdziwości portalu. Nie można się w pełni zabezpieczyć przed takim atakiem, bo podatne są na niego nawet zabezpieczone połączenia SSL. Celem ataku nie jest przełamanie zabezpieczeń sprzętowych, ale tych znajdujących się w głowie ofiary. Jest to jedna z metod stosowanych przy atakach socjotechnicznych.

g) SQL injection – jest to bardzo niebezpieczna metoda ataku, atakująca bazę danych SQL. Polega ona na wstrzyknięciu (dodaniu) przez atakującego do już istniejącego zapytania SQL swojego fragmenty. Możliwość ataku pojawia się zazwyczaj w razie wystąpienia braku sprawdzania wprowadzanego parametru przez użytkownika do zapytania. Wstrzyknięcie odbywa się prze okno do wprowadzania danych np. nazwiska na formularzu osobowym lub podczas wpisywania adresu WWW. Szerzej, atak może wystąpić w każdym miejscu, gdzie baza danych bezpośrednio łączy się z działającym programem. Dodając kod, atakujący może wprowadzić warunek zawsze spełniony, typu 1=1 lub inną instrukcję, która istotnie wpływaje na logikę działania programu. Na zakończenie należy zneutralizować stare zapytanie, np. komentując (wyłączając) je. Dodanie dodatkowego kodu może skutkować: ominięciem zabezpieczeń uwierzytelniających dostęp (logowanie się), odczyt i modyfikacje danych w bazie, możliwość wprowadzania komend do systemu operacyjnego, zmuszając go do wykonania niepożądanych zadań, przeglądania i edycji plików znajdujących się na komputerze, na którym znajduje się baza danych. Obrona przed tym atakiem polega na sprawdzaniu wprowadzanych danych, czy zgadza się typ zmiennych (czy jest to liczba, gdy jest taka wymagana) lub uniemożliwianie wprowadzanie znaków specjalnych.

h) Przełamywanie hasła (Brute Force) – jest to najbardziej prymitywny rodzaj ataku, ale za jego pomocą można przełamać prawie każdy szyfr symetryczny i asymetryczny. Polega na odgadnięciu, zmienieniu, odszyfrowaniu lub usunięciu hasła dostępowego lub całych mechanizmów zabezpieczeń. Początkujący agresorzy uczą się tej metody, ponieważ nie wymaga wiedzy specjalistycznej i szczególnych umiejętności. Atak Brute Force (metoda siłowa) polega na wprowadzaniu kolejnych haseł z zakresu możliwych haseł do czasu odgadnięcia właściwego. Jest to bardzo czasochłonna metoda. Odgadnięcie 3 znakowego hasła stanowi kwestie sekund, ale dla haseł dłuższych od 8 znaków, czas potrzebny na

sprawdzenie wszystkich kombinacji jest mierzona w setkach lat. Istnieją metody i narzędzia przyśpieszające odgadywania haseł. Można mierzyć częstotliwość występowania konkretnych liter, określenie długości zaszyfrowanych treści oraz porównywanie do podobnych zaszyfrowanych haseł. Do celów automatyzacji stworzono całe słowniki potencjalnych haseł, zgodnie z przyzwyczajeniami większości użytkowników, którzy stosują hasła ze słów używanych w znanym im językach. Są one rozwijane o potencjalne slogany, ksywki, nazwy własne. Istotna jest wiedza na temat atakowanego celu. Ludzie często stosują ważne dla nich daty lub imiona członków rodziny i bliskich. Dodatkowym ułatwieniem może być znajomość części zabezpieczonego tekstu. Inną metodą jest stworzenie tablic z zahaszowanymi hasłami, czyli takimi, jakie są przechowywane przez system. Ich rozmiary stanowią ich główną wadę, czyniąc przechowywanie ich niepraktycznym. Przechowuje się wycinek gotowych haszy, z których można, znając zastosowany algorytm, odtworzyć pozostałe w przeciągu kilku minut. Są to swoiste półprodukty haseł. Wykorzystuje się na zasadzie przyrównywani i sprawdzaniu podobieństw. Jest to duże szybsze, gdyż nie czeka się na odpowiedz systemu zabezpieczeń. Należy zauważyć, że wiele potencjalnych systemów stosuje bardzo proste metody zabezpieczeń, lub już w trakcie ich implementacji popełniono błędy. W takich wypadkach metody kryptograficzne nie spełniają swoich zadań. Wtedy łamanie haseł przebiega dużo szybciej, niż wynikałoby z poziomu zaawansowania zabezpieczeń. Nie ma skutecznej metody obrony przed takim atakiem głównie ze względu na jego prostotę. Aby się zabezpieczyć, należy stosować zaawansowane metody kryptograficzne oraz trudne, długie hasła, zawierające znaki specjalne.

i) Przejęcie (ang. Hijacking) – jest to atak polegający na przejęciu połączeń miedzy dwoma maszynami użytkowników. Następuje on zazwyczaj w jednej sieci, w której znajduje się agresor. Atak polega na nasłuchiwaniu przesyłanych pakietów w sieci, przechwytywaniu ich, modyfikacji i przesyłaniu ich dalej. Stanowi to połączenie Spoofingu i Sniffingu. Jest to trudny do przeprowadzenia atak, ale skutkujący pozyskaniem dużej ilości danych, cennych dla agresora. Są dwa najpopularniejsze odmiany ataku. Pierwszą z nich jest przejęcie i podszycie się pod jedną z maszyn. W takim wypadku, w momencie przejęcia połączenia, z ofiary na agresora, oryginalne łącze zostaje zsynchronizowane, a docelowo

zerwane. Ofiary wysyłają do agresora pakiety z danymi, zgodnie z kodami potwierdzającymi swoja tożsamość. Drugim najpopularniejszym sposobem ataku jest „Man in the middle" czyli atak z pośrednikiem. Podczas trwania tej odmiany ataku, atakujący odczytuje i modyfikuje komunikację pomiędzy stronami tak, by nie były świadome pośrednika. Dzięki temu, istnieje możliwość podsłuchania zaszyfrowanych transmisji, podsuwając swój kod zabezpieczeń swoim ofiarom. W monecie jej przejęcia, następuje degeneracja istniejącego połączenia, ale dalej świadczona jest usługa. Strony wymieniają się danymi, a agresor przechwytuje i wykrada poufne dane. Dzięki takiemu postepowaniu, otrzymuje się dostęp do danych, bez konieczności łamania zaszyfrowanych transmisji i zabezpieczonych plików.

j) Insider attack – atak wewnętrzny jest niezwykle niebezpieczny, ponieważ jest podatna na niego cała infrastruktura i systemy przedsiębiorstwa. W przeważającej liczbie przypadków, systemy są bardziej podatne na atak wewnętrzny niż zewnętrzny. W razie agresji, może nastąpić kradzież lub zniszczenie danych poufnych, wymazanie kopii zapasowych. Sieć może zostać zainfekowana lub nawet zniszczona. Atakującym może być były lub aktualny pracownik organizacji lub firmy outsorsingowej. Agresor zazwyczaj posiada autoryzowany dostęp do jednostki z wysokim poziomem bezpieczeństwa i może znać wewnętrzną strukturę sieci. Jedyną skuteczną obroną przed tym zagrożeniem jest poprawna polityka organizacji, zakładająca blokowanie dostępu dla byłych pracowników.

k) User to Root attack – Jest to atak z wykorzystaniem hasła administratora. Podobnie jak w ataku Insider attack, atakujący posiada pełen dostęp do systemu. Dane logowania admiratora może być pozyskane metodą socjotechniczną lub ukradzione. Dane mogą zostać pozyskane również bez wiedzy administratora, na przykład atakując systemy zabezpieczające, przepełniając bufor danych w systemie konsolowym, który może zwrócić odpowiednie dane. Dzieje się tak, gdy programista statycznie zablokuje wielkość bufora, uniemożliwiając jego rozszerzenie lub obsługę wyjątku.

l) Atak fizyczny – może zostać przeprowadzony bezpośrednio na infrastrukturę przedsiębiorstwa lub sieci. Zakłada zniszczenie i unieruchomienie hostów i serwerów w sieci, kradzież danych lub skompromitowanie dostawcy usługi. Atak

może być przeprowadzony również na jednostkę dostarczającą zasilanie oraz linie przesyłowe energii. Wszystkie czynności zakładają fizyczną ingerencję w infrastrukturę, która może nastąpić w razie niewystarczających zabezpieczeń i środków ochrony mienia. Istotne dla dużych serwerowni jest posiadanie własnego źródła zasilania, chroniącego przed skutkami odcięcia od sieci elektrycznej. Do ataku fizycznego należy zaliczyć wkroczenie do serwerowni oddziałów prewencyjnych i porządkowych danego państwa. Niezależnie od tego, czy służby te działają legalnie w danym kraju, może to być niezgodne z prawami kraju właściciela danych. Taki wypadek z punktu widzenia ofiary, zaliczany jest do kradzieży, a dane bezpowrotnie utracone.

m) Atak socjotechniczny – jest to atak wymierzony nie w system czy infrastrukturę, ale w człowieka. Jest to odpowiedź na tezę zawartą w książkach, których przedstawicielem jest [Podg68] Podgórecki A. Według niego, człowiek jest najsłabszym ogniwem każdego systemu zabezpieczeń. Dzieje się tak, dzięki wrodzonym i nabytym zwyczajom i schematom działania. Jest to całe spektrum ataków, skupiające się na wykorzystaniu i przekonaniu człowieka do działania, poprzez sugestie i manipulację. Atak taki jest znany w historii i był wykorzystywany od dawna. Wraz z rozwojem technologii, został po prostu przystosowany do działania w sieci. Celem ataku jest szeroko rozumiany umysł ofiary, dzięki któremu można pozyskać interesujące dane, potrzebne do działania agresora. Przygotowując się do ataku, agresor czerpie z różnych dziedzin naukowych, takich jak: ekonomia polityczna, psychologia społeczna i kulturowa oraz wszelkie nauki polityczne. W celu przeprowadzenia udanego ataku, agresor musi zebrać informacje o ofierze. Może je pozyskać z oficjalnych stron, profili społecznych firmy gdzie pracuje ofiara, notek prasowych czy z telewizji. Istotne są równie dane z prywatnych blogów, stron i profili. Sprawdza się w tym wypadku powiedzenie, "Co trafi do Internetu, już zawsze tam zostanie". Im więcej pozyskanych informacji, tym większa szansa na pozytywne przeprowadzenie ataku. Istotny jest fakt, że osoba zaznajomiona z metodami manipulacji i w socjotechnice, potrafi odtworzyć informację o ofierze ze strzępków danych i pozornie niepowiązanych ze sobą cechami i faktami. Bierze się to ze skłonności ludzi do podążania po utartych schematach działania, niewymagających twórczego myślenia. W ten sposób, dzięki prostej sugestii, można więcej osiągnąć, niż

przekonując ofiarę do konkretnego działania. Następnym etapem ataku jest stworzenie tożsamości odpowiadającej profilowi ataku oraz nawiązanie kontaktu z ofiarą. W terminie tożsamość zawiera się stworzenie profilu i charakterystyki osoby, z którą będzie rozmawiała ofiara. Równie dobrze, może to być konkretna wiadomość, komunikat, storna lub wszelkie inne medium komunikacji. Celem jest zdobycie zaufania ofiary, sprawdzenie i zweryfikowanie posiadanych danych oraz poszerzenie wiedzy o celu. Stworzona baza wiedzy, zostanie wykorzystana w następnym etapie. Jest nim tzw. wywołanie. Jest to „subtelne pozyskanie informacji", które odbywa się w czasie normalnej rozmowy, bez świadomości ofiary, o byciu sprawdzanym. Osoby rozmawiające z nieznajomym mają skłonność do bycia uprzejmym i wewnętrzną chęć do bycia pomocnym. Co więcej, Batko A. w [Batk11] twierdzi, że ludzie starają się nie kłamać nieznajomym w rozmowie, nawet kiedy mówią o rzeczach prywatnych i objętych tajemnica służbową. Nie zdaja sobie sprawy, że dla agresora nie ma terminu „nieistotne dane". Nawet informacja o zainteresowaniach czy rodzinie, może posłużyć do sprofilowania i ułatwienia odgadnięcia hasła. Ofiara zazwyczaj podaje agresorowi istotne dane, nie będąc świadomym błędnego postępowania. Istnieje kilka wariantów ataku socjotechnicznego w cyberprzestrzeni. Można do nich zaliczyć następujące ataki:

i. Pfishing – jest to atak socjotechniczny, polegający na tworzeniu fałszywych stron lub mail, używanych w celu pozyskania danych logowania ofiary. Jest to odmiana spoofing, ale z ograniczonym zastosowaniem technologicznych, a nacechowanych psychologicznym podejściem. Formularze mogą być rozszerzone o dokładniejsze dane do podania. Atakujący rozsyła masowo spreparowane wiadomości, umożliwiające przekierowanie ofiar na swoje fałszywe strony. Wiadomości są zwykle opatrzone wiarygodnym komunikatem o prośbę weryfikacji danych, odblokowanie konta lub wręcz udziałem w konkursie. Innym sposobem na oszukanie ofiar jest stworzenie stron o podobnych adresach do oryginalnych, ale zawierający literówkę lub inna domenę. Najczęściej wykorzystuje się te metodę do wyłudzenia danych logowania do banku lub kart kredytowych. Można ją wykorzystać również w celu pozyskania dostępu do chmury obliczeniowej. Na stronach lub w emailach zawarte są drobne błędy stylistyczne lub lingwistyczne. Maja one na celu szybkie odfiltrowanie osób spostrzegawczych

i inteligentnych. Oszukanie tych jednostek jest trudniejsze i mniej opłacalne, od ludzi roztargnionych i nieuważnych.

ii. NLP – to neurolingwistyczne programowanie, nie ma nic wspólnego z techniką i atakami na infrastrukturę. Korzysta on z dziedziny Socjotechnicznej, ale w przeciwieństwie do standardowego, krótkoterminowego ataku, ten może być długoterminowy i wielofalowy. W czasie ataku wykorzystuje się emocje, poglądy, przekonania i nastawienie ofiary do świata. Agresor sugeruje, przekonuje i manipuluje ofiarą, w celu zdobycia jego zaufania, protekcji lub sztucznej przyjaźni. Przybiera postawę nadrzędna nad swoja ofiarą, dążąc do z góry określonych celów. Ta metoda jest bardzo brutalna i wysoce nieetyczna. Bazuje ona na szeroko rozumianym kłamstwie. Przy braku ingerencji w sam system, atakujący może pozyskać nawet całe bazy danych. Wszystko zależy od nakładów pracy i czasu przeznczonego na atak.

iii. Spam i maile z odsyłaczem – Spam to niechciane wiadomości rozsyłane w Internecie poprzez pocztę elektroniczną. Cechuje się brakiem skonkretyzowanego odbiorcy wiadomości, masowym wysyłaniem wiadomości do użytkowników sieci. Otrzymują je osoby, które nie wyraziły wcześniej zgody na otrzymywanie wiadomości oraz nie są w stanie wypisać się z listy mailingowej. Cały sens ataku z wykorzystaniem spamu i maili z odsyłaczem, jest wykorzystanie ofiar, do prezentacji im danych i zarabiania na tym.

Agresor może pozyskać dane ofiar poprzez atak o nazwie Hoax czyli fałszywej plotce. Opiera się on na wysyłaniu prośby o udostepnienie danej wiadomości wszystkim swoim znajomym i kontaktom w książce adresowej. Specjalny skrypt zbiera wtedy adresy i wysyła je do agresora. Może on wtedy wysyłać reklamy do pozyskanej listy mailingowej i na tym zarabiać. Dodatkową opcją jest wysyłanie maili z oszustwami typu „Nigeryjski szwindel”. Polega on na podsyłaniu ofiarom wiadomości o wygranej lub spadku, a agresor jest prawnikiem lub urzędnikiem który bada dana sprawę. Prosi wtedy o mała opłatę na za koszty pracy lub jakieś potrzebne badanie do postępowania. Ofiara często wysyła datek, myśląc o szybkim rozwiązaniu sprawy i zyskaniu głównej nagrody - wabika. Następnie występuje prośba o kolejną wpłatę i cykl jest powtarzany aż do zniechęcenia się ofiary. Pomimo poręczanych małych datków, dzięki efektowi skali, agresor zyskuje finansowanie na przeprowadzenie innych ataków, bezpośrednio wymierzone w cenne dane.

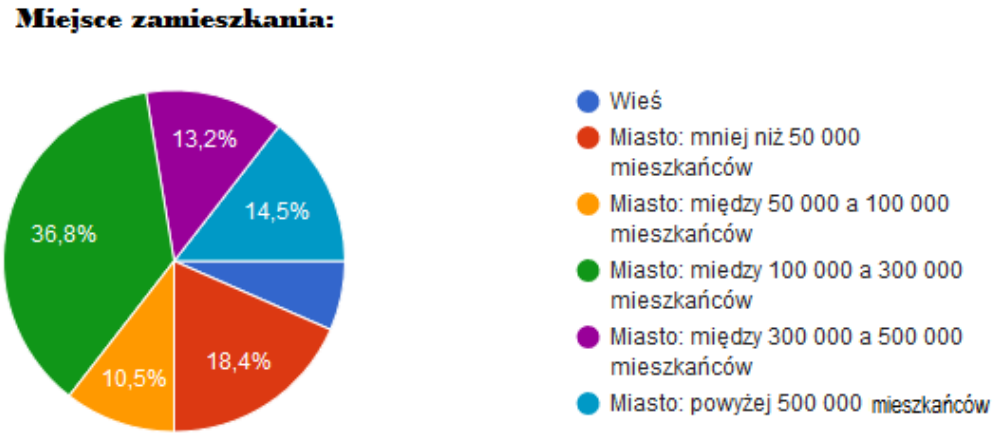
Rozdział III Analiza wyników ankiety dotyczącej bezpieczeństwa w chmurze obliczeniowej i ogólnorozumianej cyberprzestrzeni

3.1. Cel ankiety

Ankieta została przeprowadzona w celu sprawdzenia wiedzy przeciętnego użytkownika komputera na temat chmury obliczeniowej oraz sposobów ochrony własnej własności w cyberprzestrzeni. Dodatkowym jej aspektem było sprawdzenie wśród ankietowanych świadomości występowania zagrożeń.

3.2. Adresaci ankiety

Ankieta została przeprowadzona wśród osób stale korzystających z Internetu, mogącym mieć styczność z rozwiązaniami opartymi o chmurę komputerową. Do ankiety zostały zaproszone również osoby rzadziej korzystające z Internetu, ale korzystające z usług w chmurze obliczeniowej. W ankiecie wzięło udział 152 respondentów, wśród których znalazło się 57,9% kobiet (88 osób), a pozostałą część stanowili mężczyźni, czyli 42,1% (64 osoby). W ankiecie najliczniejszą grupą wiekową stanowiły osoby młode w przedziale wiekowym 20-29 lat i stanowili 71,1% całej puli respondentów. Drugą grupą z największą liczbą reprezentantów były osoby w wieku 30-39 lat i stanowiły 18,4% ankietowanych. Był to celowy zabieg, gdyż skierowano ankietę do ludzi uznawanych za zaznajomionych z cyberprzestrzenią. Umożliwiło to zobrazowanie ich przyzwyczajeń oraz zachowań. Udało się dzięki temu uzyskać obszerniejsze dane, przedstawiające nieraz zaskakujące wyniki przeprowadzonego sondażu. Pozostałe grupy wiekowe posiadają miedzy 2-4% respondentów każda. Ankietowani są w przeważającej większość osobami wykształconymi, co najmniej z średnim i wyższym wykształceniem – 97,3% w tym 77,6% (97 osoby) posiada wyższe wykształcenie. Badani zamieszkują równomiernie wszystkie przedziały według ludności w miastach, z czego najwięcej uplasowało się w miastach z ludnością między 100 000, a 300 000 mieszkańców – 36,8%. Najmniej respondentów pochodzi ze wsi – 6,6%. Podział respondentów według miejsca zamieszkania został przestawiony na rysunku nr 8.



Rysunek nr 8 Rozkład miejsca zamieszkania respondentów
Źródło: Opracowanie własne na podstawie ankiety pt. „świadomość bezpieczeństwa w chmurze obliczeniowej"

Pytania zostały pogrupowane w kwestionariusze w sekcje o wspólnej tematyce w celu uzyskania bardziej dogłębniej analizy zjawiska i pozyskania dokładniejszych danych.

3.3. Opis ankiety

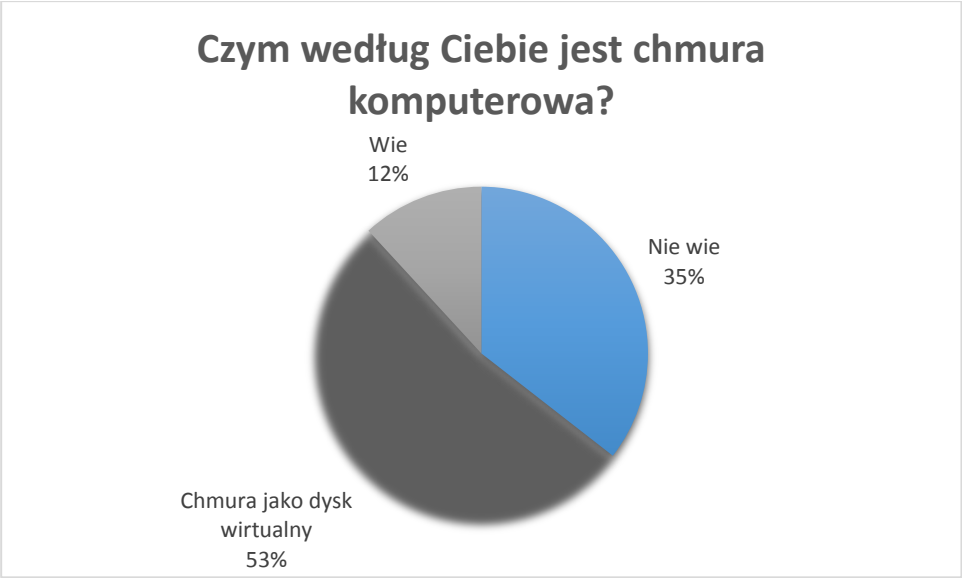
Badanie zostało rozpoczęte 23 sierpnia 2016 roku i trwało do 1 września 2016r. Zostało one przeprowadzone wyłącznie w formie elektronicznej przy zastosowaniu narzędzia Google Forms do tworzenia ankiet, udostępnione swoim użytkownikom. Dzięki niemu, według potrzeb ankietera, można dowolnie tworzyć formularze, poprzez dodawanie i edycję pytań według potrzeb ankietera. Uzyskane odpowiedzi są automatycznie gromadzone w formularzu odpowiedzi oraz eksportowane do zewnętrznego pliku Excel w którym można łatwo zagregować otrzymane dane. Badanie trwało nie więcej niż 5 minut i natychmiast po jego zakończeniu możliwe było podejrzenie wyników ankiety. Całość zapewniała anonimowość ankietowanego, a z danych o użytkowniku, zapisywany był tylko data wypełnienia ankiety. Pytania występowały w formie pytań otwartych i zamkniętych, przy czym większość pytań było w formacie prawda/fałsz. Wymuszono odpowiedzenie na wszystkie pytania, a dodatkowo, przejście do następnej sekcji było możliwe tylko po uzupełnieniu wszystkich odpowiedzi bez możliwości powrotu do wypełnionych sekcji. Pytania zawarte w sekcji otwartej oraz wielokrotnego wyboru, zostały po zakończeniu badania ocenione i usystematyzowane według wspólnych cech, które objawiły się w kwestionariuszu. Na podstawie pytań i odpowiedzi powstała analiza. Pytania z ankiety często odbiegały od analizowanych zagadnień. Było to działanie celowe.

3.4. Prezentacja i analiza uzyskanych wyników ankiety

W pierwszym pytaniu, ankietowani zostali zapytani, czy w ogóle korzystają z chmury obliczeniowej. Jest to stosunkowo nowe rozwiązanie technologiczne, które posiada rozwinięty marketing z wielkimi akcjami promującymi. Na tym pytaniu wiele osób zrezygnowało z wypełniania ankiety, twierdząc, że tematyka ich nie dotyczy.

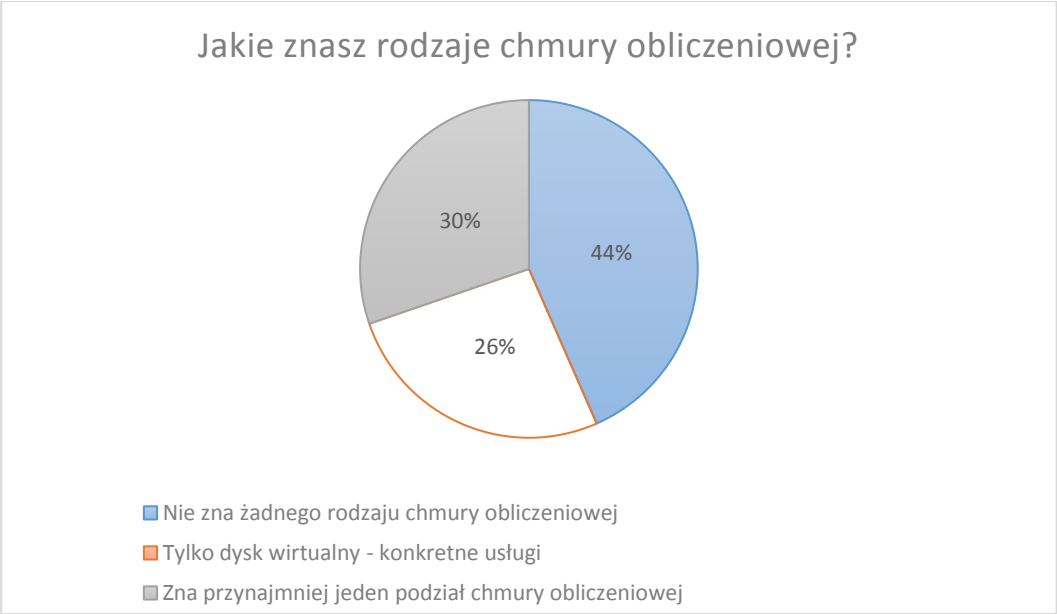
Rysunek nr 9 Czy korzystasz z chmury komputerowej?
Źródło: Opracowanie własne na podstawie ankiety pt. „świadomość bezpieczeństwa w chmurze obliczeniowej"

Okazało się, że aż 71,1% osób, które wypełniły ankietę, twierdzi, że korzysta z chmury obliczeniowej w ten czy inny sposób. Dominantę w badaniu stanowiła grupa wiekowa 20-29 lat, co odpowiada za wysoki wskaźnik wykorzystania chmury komputerowej. Grupa ta jest szczególnie podatna na akcje przeprowadzone na portalach społecznościowych [WWW14]. Należy zauważyć, że chmura obliczeniowa jest współcześnie bardzo rozwinięta, co również powiększa współczynnik korzystających z niej. Zaskakujące jest, że blisko 30% (28,9%) twierdzi, że nie korzysta z tego rozwiązania technologicznego. Rozpatrując definicję chmury obliczeniowej w szerszym spektrum, to większość rozwiązań współczesnego Internetu z niej korzysta. Istnienie przestrzeni, która może się elastycznie rozszerzać, udostępniając moc obliczeniową dla użytkownika oraz jest dostępna z każdego miejsca na ziemi. Nawet zwykła poczta elektroniczna potrafi zawrzeć się w tej definicji, co sugeruje niewiedzę ankietowanych na temat chmury. Większość ankietyzowanych uważa chmurę obliczeniową jako swoisty dysk, a nie usługę.



Rysunek nr 10 Czym według Ciebie jest chmura komputerowa?
Źródło: Opracowanie własne na podstawie ankiety pt. „świadomość bezpieczeństwa w chmurze obliczeniowej"

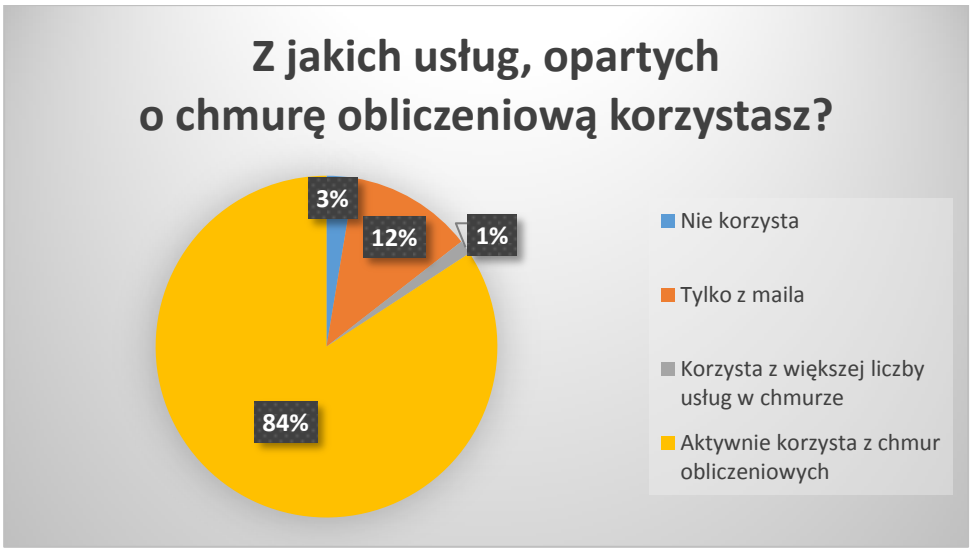
Większość ankietowanych, bo 53% (80 osób) określiło chmurę obliczeniową jako dysk wirtualny. Jest to niezwykle medialna i przydatna usługa. Dla większość użytkowników spełnia wszystkie podstawowe założenia, jakie stawiają wobec chmury, czyli miejsce do trzymania swoich kopi zapasowych i plików, którymi mogą chcieć się podzielić z innymi ludźmi. Znacząca jest możliwość przesyłania plików między własnymi komputerami bez bezpośredniego nadzoru oraz pracy dodatkowym nakładem. Synchronizacja przebiega automatycznie. Wynik ankiety pokrywa się ze statystykami opublikowanymi w [WWW14]. Zgodnie z nimi, Dropbox.com – bardzo popularny dysk wirtualny – posiada ponad 500 milionów zarejestrowanych użytkowników. Według [WWW16] stanowi to 1/7 wszystkich użytkowników Internetu. Należy nadmienić, że jest to tylko jedna z trzech najpopularniejszych usług oferujących przestrzeń dyskową dla zwykłych użytkowników. Należą również do nich OneDrive firmy Microsoft oraz Google Drive. W opozycji do tej grupy, znalazło się 35% ankietowanych, którzy nie potrafili odpowiedzieć poprawnie, czym jest chmur obliczeniowa. Wśród nadesłanych odpowiedzi, wyróżniały się odpowiedzi o chmurach atmosferycznych. W stosunku do liczby użytkowników, którzy twierdzili, że korzystają z chmury obliczeniowej wyróżnia się znacząca różnica. Jedynie 12% ankietowanych potrafiło dokładnie wskazać, czym jest chmura obliczeniowa. Bierze się to, ze specyfiki środowiska, w którym została przeprowadzona ankieta. Kilku z ankietowanych może interesować się tematyką chmury obliczeniowej na co dzień. Wielu z nich potrafiło również podać podział, który można zastosować w odniesieniu do chmury komputerowej.



Rysunek nr 11 Jakie znasz rodzaje chmury obliczeniowej?
Źródło: Opracowanie własne na podstawie ankiety pt. „świadomość bezpieczeństwa w chmurze obliczeniowej"

Wśród ankietowanych, 44% nie zna żadnego podziału chmury obliczeniowej. Stanowi to wzrost niepewności ankietowanych w stosunku do poprzedniego pytania. Do ludzi nieznających definicji dołączyli ankietowani, którzy nie znają więcej rozwiązań niż dysk wirtualny. 26% ankietowanych podkreśliło ten fakt, zamieszczając odpowiedzi, których wspólnym mianownikiem jest sprowadzenie chmury obliczeniowej do podziału dysków wirtualnych. Większość przedstawiła podział na dostawców usługi. Pomiędzy tymi odpowiedziami uplasowała się grupa 30% ankietowanych, którzy poprawnie potrafili wskazać podział chmury. Niektórzy podawali definicje zgodna z NISC, ale większość ankietowanych wskazywała na podział XaaS. Stanowi to ciekawy aspekt ankiety, w odniesieniu do 12% ankietowanych, którzy poprawnie określili chmurę. Jest to skutek analitycznego podejścia ankietowanych do zagadnienia i wymienienia cech, które posiada dysk wirtualny oraz inne usługi.

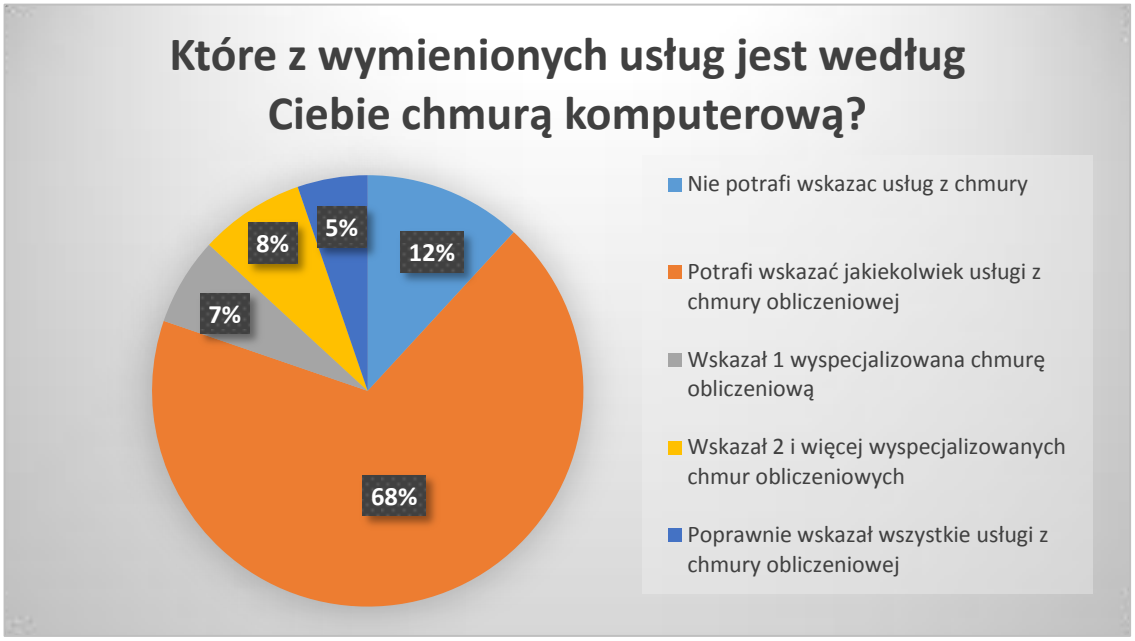
W celu uszczegółowia odpowiedzi, użytkownicy otrzymali listę możliwych usług w chmurze obliczeniowej. Wszystkie opcje, które znalazły się na liście, należą do usług komputerowych. Otrzymane wyniki zostały uszeregowane i określone według wspólnych mianowników.



Rysunek nr 12 Z jakich usług, opartych o chmurę obliczeniową korzystasz?
Źródło: Opracowanie własne na podstawie ankiety pt. „świadomość bezpieczeństwa w chmurze obliczeniowej" i pytania „Czy korzystasz z którejś z wymienionych usług?"

Omawiana sekcja ankiety została stworzona, w oparciu o tezą, według której użytkownicy nie wiedzą, iż korzystają z chmury obliczeniowej na co dzień. Po zadaniu szczegółowego pytania, sugerując użytkownikom dokładne propozycje, otrzymano wynik, w którym 97% ankietowanych korzysta z rozwiązań opartych o chmurę obliczeniową. Wszyscy (97%) wybrali pocztę elektroniczną jako rozwiązanie, z którego korzystają na co dzień. Następnymi najczęściej wybieraną opcją były dysk wirtualny posiadający 77,6% (118 osób) oraz ogranizer w stylu kalendarza Google z 40,8%. Wielu ankietowanych łączyło wybrane opcje, z czego wywnioskowano, że 84% ankietowanych aktywnie korzysta z chmur obliczeniowych w różnych formach. Zostały do nich wytypowane osoby, które wskazały przynajmniej 3 zaproponowane usługi. Wśród ankietowanych znalazły się osoby, które wykorzystują platformy programowania w chmurze, w przypadku badania była nią Google App Engine. Wśród całej próby ankietowanych znalazło się jedynie 1,3% profesjonalnych użytkowników chmury. Wśród ankietowanych, liczba użytkowników niekorzystających z chmury zmalała do 3% z wyłączeniem osób, które ograniczają się do korzystania za emaila.

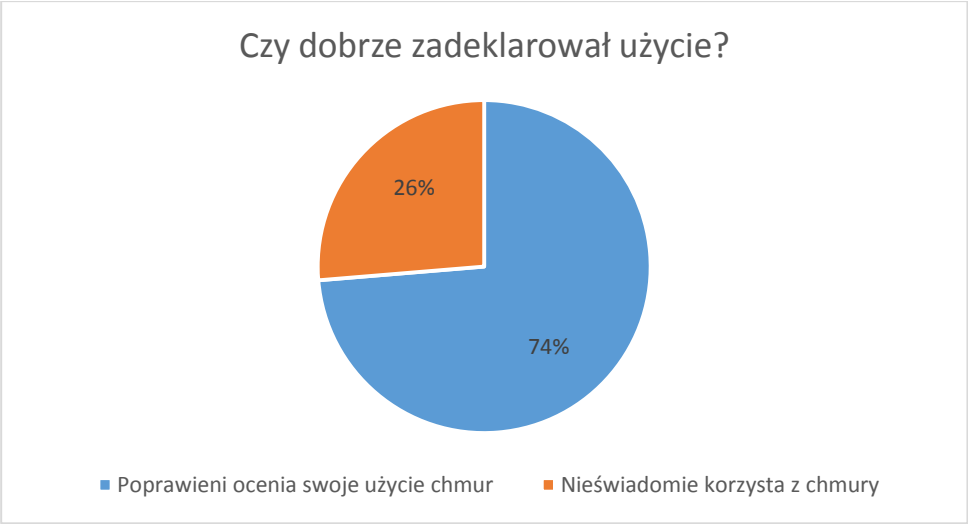
Ostatnim zadaniem w tej sekcji było wskazanie usług, które działają w obrębie chmury obliczeniowej. Lista zawierała te same pozycje co wcześniejsze pytanie, lecz została poszerzona o dwie błędne odpowiedzi oraz jedną poprawną. Otrzymane wyniki zostały ocenione i przedstawione na rysunku nr 13.



Rysunek nr 13 Które z wymienionych usług jest według Ciebie chmurą komputerową?
Źródło: Opracowanie własne na podstawie ankiety pt. „świadomość bezpieczeństwa w chmurze obliczeniowej"

Większość ankietowanych potrafiła wskazać tylko jedną usługę, świadczoną w chmurze obliczeniowej. Stanowiło to 68% osób z próby. Większość z nich ograniczała się tylko do wskazania jednej prawidłowej odpowiedzi lub zaznaczało również błędne odpowiedzi. Najliczniej ankietowani wskazywali na dysk wirtualny jako chmurę – 88,2% ankietowanych. Znaczące jest, że opcję systemu ERP płatnego za usługę wskazało tylko 17,1% ankietowanych. Wywodzi się to z braku świadomości ludzi, w jakich warunkach usługa uważana jest za chmurę. 20% ankietowanych wskazało poprawnie chociaż jedną wyspecjalizowaną chmurę obliczeniową oferującą zróżnicowane platformy i rozwiązania. W nich zawarło się tylko 5% wszystkich ankietowanych, którzy poprawnie wskazali wszystkie odpowiedzi.

Na zakończeniu pierwszego zestawu pytań, przenalizowano deklarowane wykorzystanie chmury, w stosunku do rzeczywistego korzystania z usług oraz wiedzy na jej temat.



Rysunek nr 14 Czy dobrze zadeklarował użycie chmury
Źródło: Opracowanie własne na podstawie ankiety pt. „świadomość bezpieczeństwa w chmurze obliczeniowej"

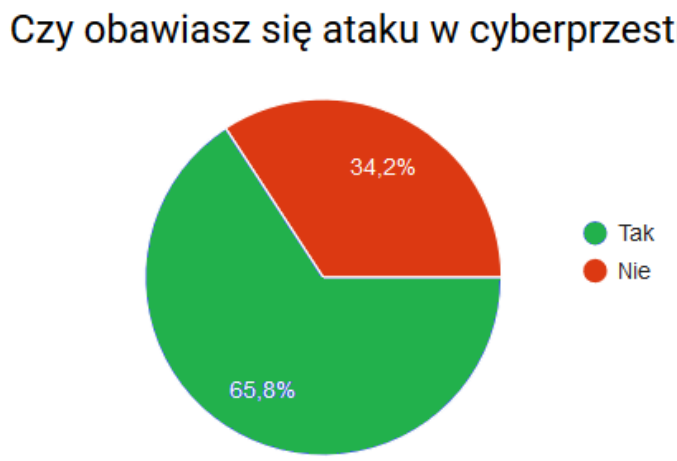
Niespodziewanie, swoje wykorzystanie chmury obliczeniowej poprawnie zadeklarowało 74% ankietowanych. Jest to zaskakujący wynik, zestawiając je z wiedzą użytkowników na temat samego technologicznego rozwiązania. Błędnie swój wybór wskazało 26% użytkowników, przy czym wszyscy zadeklarowali, że nie korzystają z tego typu rozwiązań. Można założyć, ze nieświadomie dążą w stronę korzystania z nowinek technologicznych.

Wśród użytkowników, świadomie korzystających z chmury obliczeniowej, prawie wszyscy posiadają różnej formy dysków wirtualnych. Wiąże się to z udostępnianiem rożnego rodzaju danych w Internecie. Podczas zamieszczania danych, użytkownicy pomijają kwestie bezpieczeństwa i prywatności, zapominając, że wszystko co zostało wgrane do chmury, może zostać w jakiś sposób wykorzystane lub użyte. Kilka lat temu, w prasie branżowej znalazła się seria artykułów, opisujący wyciek zdjęć celebrytek. Opis ataku znajduje się w [WWW17]. Agresor odgadł hasła do wirtualnych dysków i zgrał znajdujące się tam zdjęcia, a następnie wystawił je na sprzedaż. Przez światowe media przetoczyła się fala krytyki względem agresora, a nie poruszono kwestii bezpieczeństwa zgromadzonych danych, które nie zostały specjalnie zabezpieczone.

W następnej sekcji ankiety przygotowano pytania dotyczące zgromadzonych danych w chmurze obliczeniowej, obaw użytkowników względem ataku na ich dane oraz różnego rodzaju pytania dotyczące bezpieczeństwa. Zapytano również o nawyki ankietowanych.

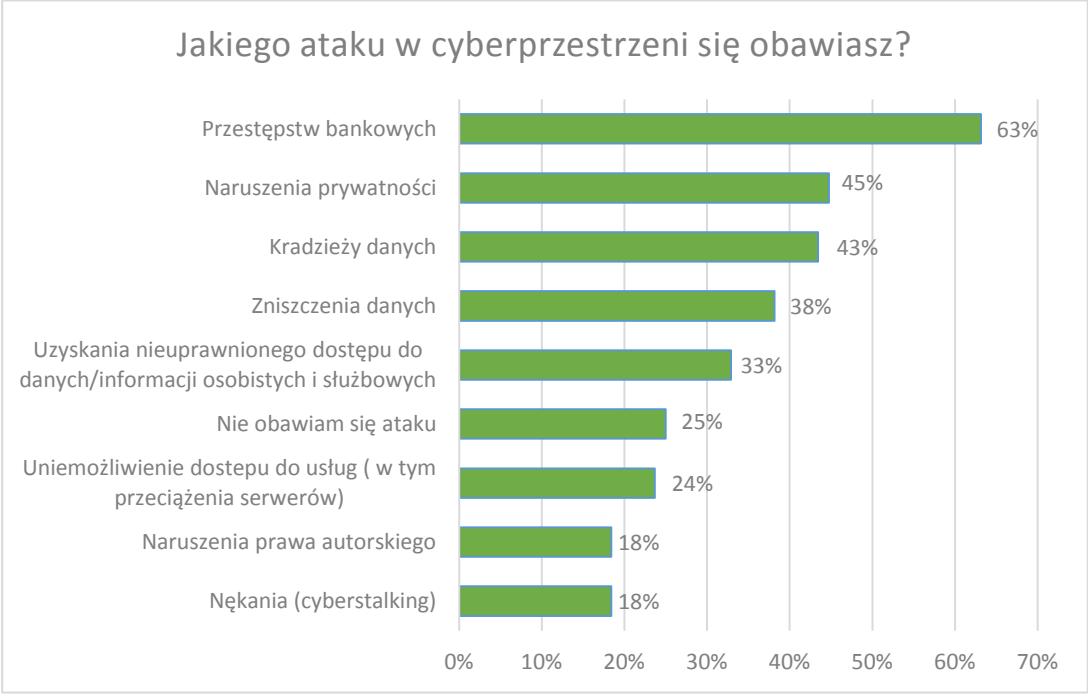
Rysunek nr 15 Jakie dane zostały przez Ciebie umieszczone w chmurze?
Źródło: Opracowanie własne na podstawie ankiety pt. „Świadomość bezpieczeństwa w chmurze obliczeniowej"

Najczęściej umieszczanymi danymi w chmurze okazały się zdjęcia, które wgrało do chmury 69,5% ankietowanych. Dodatkowo wśród najczęściej upublicznianych danych znalazło się imię (65,5% osób) oraz adres email (60,5%), przy czym większość dysków wirtualnych opiera się o adres email jako login. Jest to dowód, że ankietowani zdecydowali się zataić niektóre udostępniane dane. Zgodnie z zamieszczonymi danymi, 62% ankietowanych umieściło dane, które mogą zostać pozyskane z innych źródeł w sieci. Stanowi to swoisty kompromis pomiędzy prywatnością a bezpieczeństwem. W razie wystąpienia wycieku danych, szkody zostaną zminimalizowane. W opozycji do nich znalazły się osoby, które udostępniły wszystkie dane, dzięki którym można ukraść ich tożsamość. Wśród ankietowanych 6% wskazało na taki zestaw wgranych danych. Również 12% ankietowanych zlekceważyło względy bezpieczeństwa i zamieściło dane służbowe. W razie wystąpienia przecieku, może im grozić odpowiedzialność finansowa, karna oraz zwolnienie dyscyplinarne. Należy wymienić dane, które były najrzadziej umieszczane w sieci. Należą do nich: dane przedsiębiorstwa – 15,5%, adres zamieszkania – 13,5% oraz numer pesel – 10% ankietowanych. Duża liczba zamieszczanych danych, nasuwa pytanie o obawy ataku w cyberprzestrzeni.



Rysunek nr 16 Czy obawiasz się ataku w cyberprzestrzeni?
Źródło: Opracowanie własne na podstawie ankiety pt. „Świadomość bezpieczeństwa w chmurze obliczeniowej"

W nawiązaniu do wcześniejszych pytań, zaskakująco, bo aż 65,8% ankietowanych, obawia się ataku w cyberprzestrzeni. Za to jedyne 34,2% spośród osób z próby twierdzi, że takiego ataku się nie obawia. Naturalnym jest obawa przed atakiem, tym bardziej, że wykazują go osoby o różnej świadomości zagrożeń.



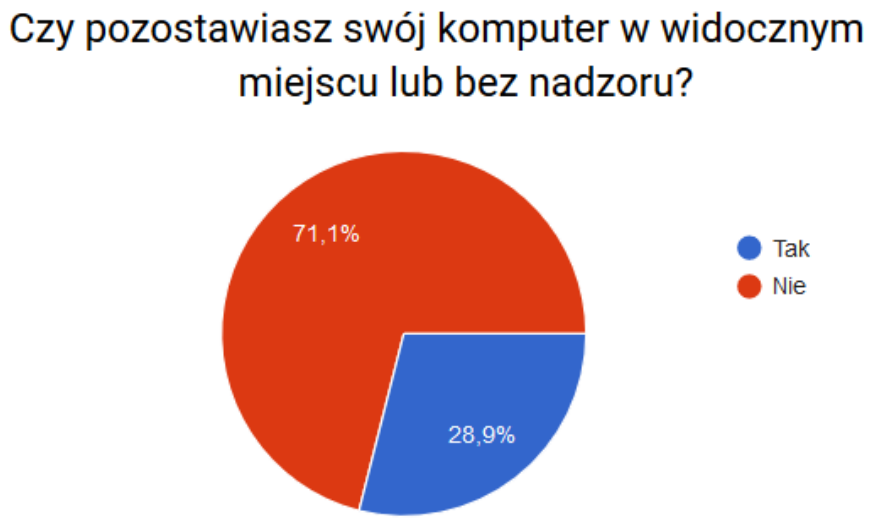
Rysunek nr 17 Jakiego ataku w cyberprzestrzeni się obawiasz?
Źródło: Opracowanie własne na podstawie ankiety pt. „Świadomość bezpieczeństwa w chmurze obliczeniowej"

Analizując odpowiedzi respondentów, największe obawy wzbudzają przestępstwa bankowe, naruszające prywatność, kradzieży danych oraz zniszczenia danych. Uzyskane odpowiedzi pokrywają się z kolejnymi raportami CERT Polska – [WWW18], [WWW19]

o stanie bezpieczeństwa sieci Internet. Właśnie do tych 4 przypadków w latach 2014 i 2015 zanotowano najwięcej ataków i oszustw. Przy tworzeniu całkowitej puli ataków w cyberprzestrzeni, oszustwa komputerowe stanowią 47,82%. Rozszerzając spektrum, kradzież tożsamości wraz z podszywaniem się pod kogoś, stanowi 29,88% wyszkach ataków. Spośród ankietowanych, najmniej kwestionariuszy zawierało odpowiedzi dotyczące nękania w cyberprzestrzeni, naruszenia praw autorskich oraz uniemożliwienie dostępu do usług – ataku typu DoS.

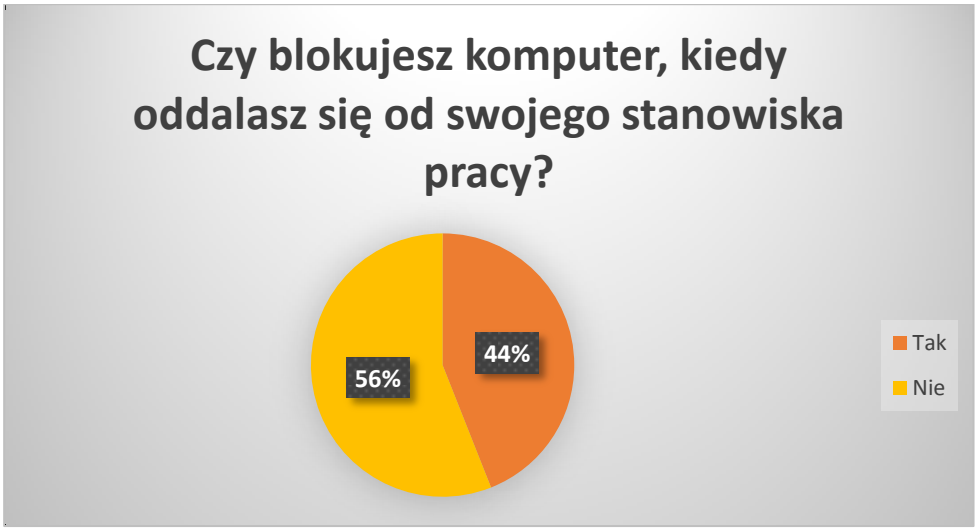
Obawa o swoje bezpieczeństwo jest rzeczą naturalną, co wywodzi się z natury człowieka i troski o swój byt. Ludzie bardziej troszczą się o sprzęt, który fizycznie posiadają niż o zasoby cyfrowe. Ma to swoje korzenie w niedocenianiu informacji, którymi dysponują. Dla konkretnej jednostki dane mogą być bezwartościowe, za to dla agresora mogą posiadać znaczną wartość. Dodatkowo, właściciel może nie być świadomy faktu wykradzenia danych, ponieważ nie znikają one z jego dysku, jeżeli nie zapragnie tego haker. Najczęściej zostają one powielone z zamiarem późniejszego wykorzystania. Także w wypadku kradzieży danych w prawdziwym świecie, ofiara ma trudności określenia czasu i okoliczności wykradzenia danych. Różnica w czasie może być liczona miesiącach lub latach. Przykładem takiej sytuacji może być wyciek haseł dostępowych do chmury obliczeniowej Dropbox.com, który został opisany na portalu niebezpeicznik.pl [WWW32]. Firma po czterech latach przyznała się do rzeczonego wycieku, gdzie dane klientów były wielokrotnie wykorzystywane przez hakerów. Faktem jest, że użytkownicy portalu wielokrotnie zgłaszali prawdopodobne wykorzystanie ich danych umieszonych w chmurze przez osoby trzecie. Brak jest dokładnych statystyk dotyczących tego, ile danych wyciekło i zostało wykorzystanych, kiedy były używane oraz czy dane innych użytkowników nie zostały naruszone i czy są bezpieczne.

Inne zachowanie użytkowników obserwuje się podczas dbania o fizyczne nośniki. Ludzie potrafią docenić wartość sprzętu, a zarazem bardziej o niego dbają i się troszczą. Rzadziej obserwuje się zjawisko pozostawiania bez opieki cennych rzeczy. Jedną z podstawowych metod zabezpieczenia danych jest troska o sam nośnik. Spośród ankietowanych, ponad dwie trzecie respondentów (71,1%) zadeklarowała, że zwraca uwagę na to, gdzie pozostawia swój komputer lub pod czyją opieką. Zjawisko to należy oceniać pozytywnie, gdyż świadczy to o większej świadomości z zakresu bezpieczeństwa i ochrony danych.



Rysunek nr 18 Czy pozostawiasz swój komputer w widocznym miejscu lub bez nadzoru??
Źródło: Opracowanie własne na podstawie ankiety pt. „Świadomość bezpieczeństwa w chmurze obliczeniowej"

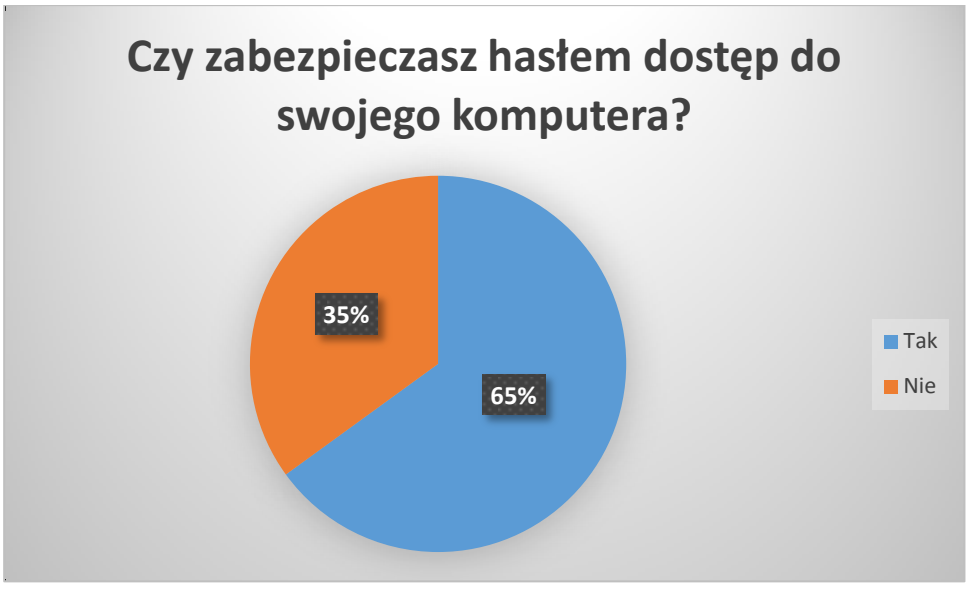
Z drugiej strony, 28,9% respondentów pozostawia swój sprzęt elektroniczny bez nadzoru lub w widocznym miejscu. Przyczyną takiego postepowania może być wyobrażenie złodzieja danych w świadomości współczesnych ludzi. Przybiera on postać młodego Azjaty, który próbuje wykraść dane z komputera przez wyrafinowane sposoby ataku. Nie doceniają staromodnej kradzieży nośnika lub sprzętu. Istotny jest również możliwy dostęp do komputera w celu kradzieży danych lub modyfikacji i uszkodzenia zasobów. Wśród osób pozostawiających swój komputer bez nadzoru, znajdują się głównie osoby młode z wyższym wykształceniem. Stanowią one 90% respondentów, które przyznały się do takiego postepowania. Młodzi ludzie przystępują z większą ufnością do osób, w przeciwieństwie do osób starszych, nauczonych fizycznego chronienia dostępu do danych.



Rysunek nr 19 Czy blokujesz komputer, kiedy oddalasz się od swojego stanowiska pracy?
Źródło: Opracowanie własne na podstawie ankiety pt. „Świadomość bezpieczeństwa w chmurze obliczeniowej"

Odmienne zachowanie respondentów odnotowuje się w znanym sobie środowisku i wśród ludzi, z którymi obcują na co dzień. Ludzie nie wierzą, że znane im jednostki mogą wykorzystać ich dane w swoim celu, nierzadko na szkodę ofiary. Przyczynia się do tego, że nie zabezpieczają w sposób właściwy dostępu do swojego urządzenia. Postępowanie takie jest często niezgodne z polityką bezpieczeństwa miejsca pracy oraz zasad postepowania z danymi wrażliwymi. Potwierdzeniem tej tezy są odpowiedzi na zadane pytanie, gdzie 56% ankietowanych przyznało, że nie zabezpiecza dostępu do komputera, gdy opuszcza stanowisko pracy. Biorąc pod uwagę specyfikacje portu USB 3.0, w czasie 5 minutowego pobytu pracownika w toalecie, przy niezabezpieczonym komputerze, mogło by wyciec, według [WWW33], blisko 23GB danych wrażliwych., Przy najczęściej przyjmowanych zasadach polityki bezpieczeństwa, każde oddalenie się od stanowiska pracy, powinno być poprzedzone przez wylogowanie się z sytemu oraz zabezpieczenie komputera hasłem.

Posiadanie hasła jest najbardziej podstawową formą zabezpieczenia usługi i danych. Jest ono przechowywane jako tajny parametr, ukryte lub zamaskowane również na serwerach, z którym jest porównywane w razie żądania dostępu. Dostęp jest wtedy przyznawany na zasadzie: wejdziesz, jeśli wiesz gdzie. Do większość kont, we współczesnej cyberprzestrzeni, wystarczy posiadanie hasła, bez zróżnicowanych urządzeń ani sterowników, które mogą potwierdzić tożsamość uwierzytelnianej osoby. Najważniejszą cechą takiego rozwiązania jest prostota w jego zapamiętaniu, w przeciwieństwie do skomplikowanego klucza kryptograficznego, którego standardowe rozmiary liczone są w setkach znaków.



Rysunek nr 20 Czy zabezpieczasz hasłem dostęp do swojego komputera
Źródło: Opracowanie własne na podstawie ankiety pt. „Świadomość bezpieczeństwa w chmurze obliczeniowej"

Według wyników ankiety 35% respondentów nie stosuje hasła do zabezpieczenia swoich danych na komputerze. Jest to równoznaczne z brakiem jakichkolwiek zabezpieczeń urządzeń. Każda osoba trzecia, może w dowolnym monecie skopiować dane z komputera. W opozycji do tej grupy respondentów znalazła się 65% grupa respondentów, która zabezpiecza hasłem swój komputer. Należy nadmienić, ze ankietowani uwzględnili również komputery służbowe, na których posiadanie hasła zostało wymuszone przez administratora.

Negatywnym skutkiem wymuszenia posiadania hasła jest zastosowanie banalnych haseł zabezpieczających, co przedstawia poniższy wykres.

Rysunek nr 21 Czy stosujesz trudne do odgadnięcia hasła?
Źródło: Opracowanie własne na podstawie ankiety pt. „Świadomość bezpieczeństwa w chmurze obliczeniowej"

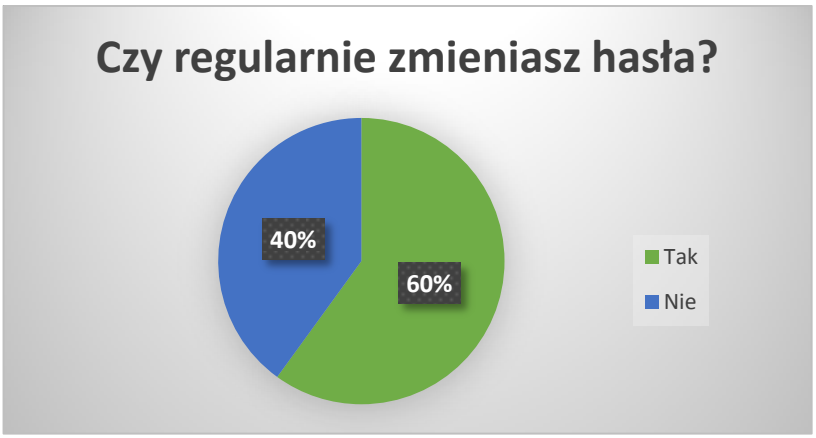
Hasło uważane za trudne do odgadnięcia powinno posiadać kilka podstawowych elementów: duża liczba znaków, znaki specjalne, litery, liczby, różna wielkość liter. Każdy z tych punktów zwiększa nakład pracy hakera, który musi włożyć, aby odgadnąć prawidłową sekwencję dostępową. Złamanie zbyt długiego i trudnego hasła może okazać się zbyt kosztowne. Niestety, użytkownicy stosują hasła proste do odgadnięcia, które są proste w zapamiętaniu. Składają się one z elementów ściśle powiązanych z ich osobą. Najczęściej hasła te zawierają imiona bliskich, daty urodzin, miejsce zamieszkania i itp. Złamanie takich zabezpieczeń wymaga przeprowadzenia podstawowego wywiadu społecznego, na temat ofiary. Do posiadania takich haseł przyznało się 81,6% ankietowanych. Należy mieć na uwadze, ze użytkownicy nie posiadają świadomości, czym jest trudne do odgadnięcia hasło, stad wyniki mogły ulec zniekształceniu. Pozytywnie o poziomie zaawansowania swoich haseł

wypowiedziało się 18,4% ankietowanych. Graficzna interpretacja została przedstawiona na rysunku nr 21.

Według badaczy [WWW34], użytkownicy, którzy już posiadają skomplikowane hasło, maja tendencje do stosowania go w wielu miejscach, co automatycznie krytycznie obniża jego walory obronne. W razie wykradzenia hasła z jednego źródła, agresor uzyskuje dostęp do większej liczby kont. Zwiększa to opłacalność przeprowadzonego ataku.

Rysunek nr 22 Czy stosujesz to samo hasło do różnych logowań?
Źródło: Opracowanie własne na podstawie ankiety pt. „Świadomość bezpieczeństwa w chmurze obliczeniowej"

Zaskakująco, wśród ankietowanych, aż 68% przyznało się, ze używa tego samego hasła do wielu portali i kont. Świadczy to o lekkomyślności ankietowanych, ale zarazem udowadnia ludzką wygodę oraz trudność do zapamiętywania dużej liczby skomplikowanych haseł. Pojawiły się głosy, że hasła głównie utrudniają dostęp autoryzowanym użytkownikom, niż potencjalnym agresorom. Pozostali ankietowani, czyli 32% (49 osób), stosuje unikalne hasła do różnych kont. Istotną kwestią jest częstotliwość zmiany haseł.



Rysunek nr 23 Czy regularnie zmieniasz hasła?
Źródło: Opracowanie własne na podstawie ankiety pt. „Świadomość bezpieczeństwa w chmurze obliczeniowej"

Wśród ankietowanych, 60% odpowiedziało, że zmienia regularnie hasła. Pozostali ankietowani, czyli 40% twierdzi, że nie zmienia haseł. Taka duża liczba respondentów, którzy zmieniają hasła, bierze się z polityki bezpieczeństwa firm i certyfikatów ISO, w których pracują. Według nich, hasła powinny być średnio zmieniane co miesiąc i nie powinno się powtarzać w przeciągu kilku następnych zmian. Skutkuje to powstaniem haseł z danego ciągu, gdzie kolejne hasła różnią się do siebie kolejnym numerem lub znakiem specjalnym. Jest to praktyka patologiczna, z racji prostoty odgadnięcia kolejnego hasła, gdy zna się jakiekolwiek wcześniej użyte. Google w swojej rekomendacji [WWW34], już nie zaleca takich praktyk.

Inną metoda obrony swoich danych przed włamywaczem jest posiadanie włączonego i poprawnie skonfigurowanego firewall-a, czyli zapory ogniowej. Stanowi on mur przed nieautoryzowanym dostępem do sieci lokalnej. Organiczna ona również wypływ danych z wnętrza sieci, poprzez przekierowywanie ruchu i pakietów przez jej mechanizmy obronne.

Rysunek nr 24 Czy posiadasz włączoną zaporę ogniową (firewall)?
Źródło: Opracowanie własne na podstawie ankiety pt. „Świadomość bezpieczeństwa w chmurze obliczeniowej"

Większość ankietowanych, bo aż 71% posiada włączoną zaporę ogniową. Jest ona standardowo włączona wraz z nowa instalacją systemu Windows. Również w polityce bezpieczeństwa przedsiębiorstw wymogiem jest posiadanie włączonej zapory. Zatrważające jest, że 29% ankietowanych wyłączyło firewall-a. Dobrowolnie i świadomie pozbawili się podstawowej ochrony przed potencjalnymi agresorami z sieci.

Według przytoczonych już w tej pracy badań [WWW18], najwięcej ataków przypada, nie poprzez złamania zabezpieczeń lub wycieku danych, ale za pomocą wyciągniecie ich od

samych użytkowników, poprzez atak phishing. Ankietowani zostali poproszeni o ustosunkowanie się do zachowań dotyczących maili od nieznanych adresatów.

Rysunek nr 25 Czy otwierasz maile/linki od nieznanych nadawców?
Źródło: Opracowanie własne na podstawie ankiety pt. „Świadomość bezpieczeństwa w chmurze obliczeniowej"

Adres e-mail nie jest daną prywatną, a wręcz stanowi identyfikator użytkownika. Rejestrując się na nowych portalach, podaje się go w celu identyfikacji. Często, wymagana jest zgoda na przetwarzanie danych, a zarazem pozwolenie na przesyłanie ich danych innym podmiotom, które mogą już wykorzystać adresy w nielegalnych celach. Przy dużej liczbie otrzymywanych wiadomości, która dziennie wyrażona w dziesiątkach, a nawet setkach sztuk, weryfikacja tożsamości nadawcy staje się niemożliwa. Zjawisko potęguje brak spójnej książki adresatów. Skutkuje to zaprzestaniem weryfikacji nadawców przez niektórych odbiorców. Potwierdzeniem tej tezy stanowią odpowiedzi respondentów, gdzie blisko 21% nie sprawdza, czy otrzymana wiadomość lub link jest od nieznanych nadawców. Skutkuje to częstym podawaniem danych na fałszywych stronach, na które zostaną przekierowanie oraz zainfekowaniem swoich komputerów. Z drugiej strony, 79% respondentów, stara się zwracać uwagę na nadawców wiadomości.

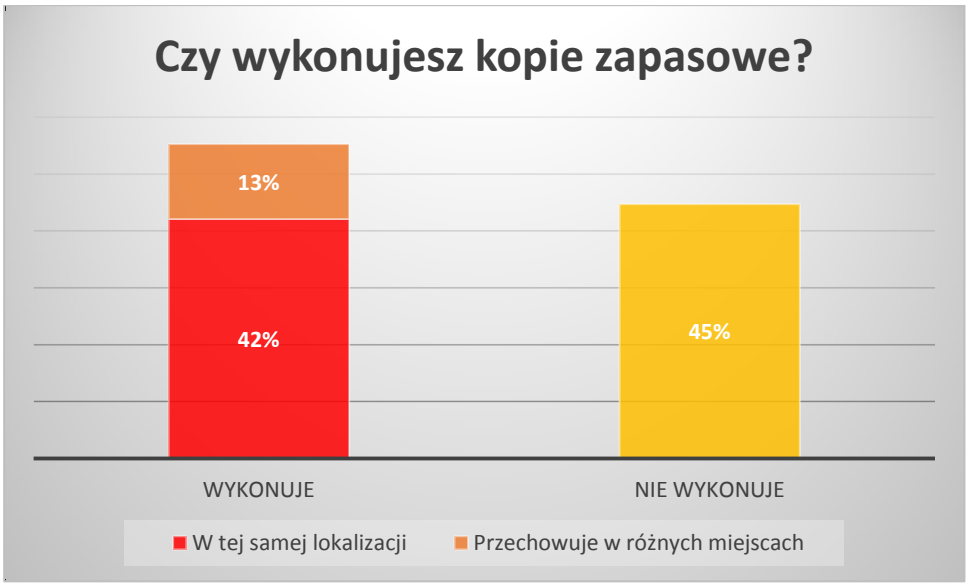
Rozszerzeniem prezentowanym wcześniej zagadnienia jest pytanie dotyczące otwierania plików o nieznanym rozszerzeniu. Użytkownicy błędnie zakładają, że przesłanie danych przez rozpoznanego nadawcę, może wpłynąć szkodliwie na pracę ich komputera. Nie biorą pod uwagę możliwości podszycia się pod nadawcę lub przesłanie dalej zainfekowanego wcześniej pliku. Dawniej zagrożenie stanowiły tylko pliki o rozszerzeniu .exe albo .bat, które uruchomiały szkodliwe aplikacje. Obecnie szkodliwe oprogramowanie może być podpięte

pod dowolny format plików, w tym .pdf i .doc (tekstowy), które są swobodnie przesyłane miedzy użytkownikami.

Rysunek nr 26 Czy weryfikujesz rozszerzenia załączników, zanim je otworzysz?
Źródło: Opracowanie własne na podstawie ankiety pt. „Świadomość bezpieczeństwa w chmurze obliczeniowej"

Praca w dużym przedsiębiorstwie, ze względu na minimalizację kosztów, odbywają się na stacji roboczej. Otwarcie zainfekowanego pliku na takowej, może skutkować zainfekowaniem całego serwera, a zarazem wyciekiem danych z serwerów. Zgodnie z wynikami danych, 32% respondentów naraziło firmę, w której są zatrudnieni, na wyciek danych poprzez brak weryfikacji otrzymanych plików. Poprawnie zachowuje się 68% respondentów, czyli 103 osoby, które zwracają uwagę na format plików, jakie otrzymują. Należy zauważyć, że osoby świadome weryfikacji rozszerzeń, biorą pod uwagę tylko dane wyświetlane przez przeglądarkę. Zdarzają się przypadki, gdy pomimo uważania, otworzyć się zły plik, ponieważ próbują się one podszyć pod właściwy. Na poziomie współczesnej technologii, sztuczna zmiana rozszerzenia jest możliwa i wykonywana na podstawie ogólnie dostępnego menadżera plików.

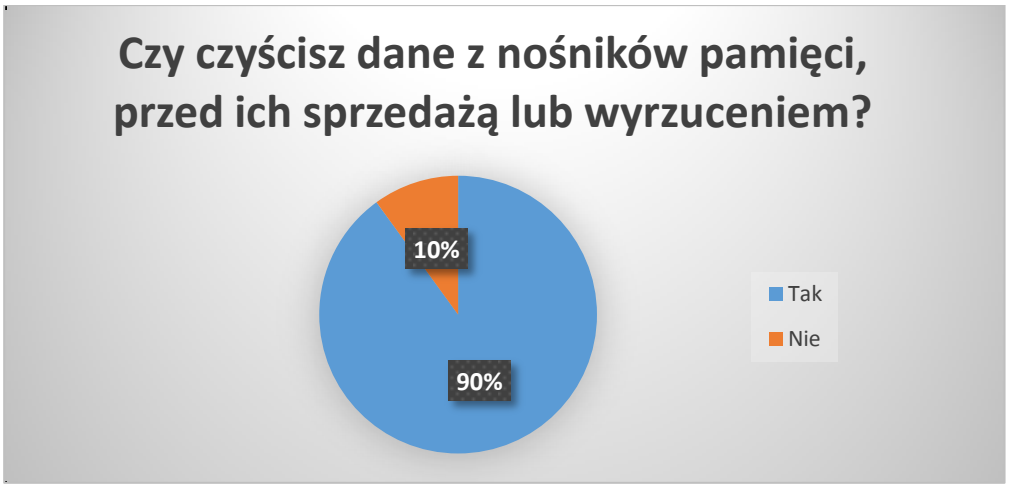
Administratorzy sieci mawiają: „Użytkownicy komputerów dzielą się na dwie grupy. Ci którzy robią kopie zapasowe oraz Ci, którzy będą robić kopie zapasowe." Wypadek utraty danych nie występuje na co dzień, ale jest bardzo dotkliwy w razie wystąpienia. Występuje on najczęściej w wyniku skoku napięcia, przez który dysk ulega uszkodzeniu. Przechowywane na nim dane zostają utracone, co we współczesnym modelu działalności gospoda4rczej, może skutkować całkowitym paraliżem funkcjonowania przedsiębiorstwa. W ramach przeprowadzonej ankiety, respondentom zadano pytanie dotyczące wykonywania kopi zapasowych posiadanych danych.



Rysunek nr 27 Czy wykonujesz kopie zapasowe?
Źródło: Opracowanie własne na podstawie ankiety pt. „Świadomość bezpieczeństwa w chmurze obliczeniowej"

Zgodnie z przedstawionymi danymi na rysunku nr 27, 45% ankietowanych nie robi kopii zapasowej posiadanych danych. Świadczy to o braku świadomości ryzyka wystąpienia awarii bądź też utraty danych w wyniku celowego działania osoby trzeciej. W opozycji do nich znajduje się grupa respondentów, którzy będąc świadomi możliwego ryzyka, tworzą kopie zapasowe. Należy jednak zauważyć, że tylko 13% przechowuje kopie na nośnikach innych niż podstawowe dane, co chroni ich przed wystąpieniem zjawisk podatnych na uszkodzenie danych. Dzięki rozproszeniu repozytorium, jest ono również odporne na atak, którym padła serwerownia 2be.pl, o której pisał portal niebezpeicznik.pl w artykule [WWW37]. Klienci serwerowni utracili wszystkie dane, które zgromadzili. Wszystkie kopie zapasowe z tego okresu były przechowywane w jednym miejscu, oraz posiadały wspólne hasło dostępowe. Podczas ataku, agresor posiadał to hasło, przy czym wykasował wszystkie napotkane dane wraz z kopiami zapasowymi. Najnowsza kopia, która ocalała, znajdowała się w innej lokalizacji, fizycznie niepołączonej z innymi serwerami i pochodziła sprzed 2 lat.

Częstym grzechem użytkownika jest udostepnienie danych, które zawarte są na sprzedawanych przez niego urządzeniach. W ankiecie zadano pytanie dotyczące konieczności skasowanych danych w sprzedawanym urządzeniu. Wyniki odpowiedzi świadczą o dobrych praktykach i dużej świadomości respondentów, ale niestety nie potwierdzają posiadanych przez nich umiejętności do odpowiedniego obchodzenia się z danymi.



Rysunek nr 28 Czy czyścisz dane z nośników pamięci, przed ich sprzedażą lub wyrzuceniem?
Źródło: Opracowanie własne na podstawie ankiety pt. „Świadomość bezpieczeństwa w chmurze obliczeniowej"

Według ankiety, 90% respondentów czyści dane ze sprzedawanego urządzenia. Większość użytkowników korzysta z podstawowych narzędzi udostępnianych przez system operacyjny. Dane te nie są usuwane permanentne, ponieważ zasady działania usuwania plików, opiera się na odcięciu dostępu do pliku, a nie fizycznym ich wymazaniu. Ankietowani nie są świadomi możliwości odzyskania danych przez specjalistyczne narzędzia. Faktem jest, że na rynku działają firmy, które świadczą usługi odzyskiwania usuniętych danych lub z uszkodzonych nośników. 10 % ankietowanych w ogóle nie czyści nośników ze sprzedanych urządzeń, co świadczy o braku świadomości użytkowników. Dobrym przykładem jest wyciek numery telefonu prezydenta Polski, który został udostępniony, ponieważ urzędnik państwowy sprzedał telefon komórkowy, bez uprzedniego wyczyszczenia jego pamięci masowej. [WWW36].

3.5. Podsumowanie

Przygotowana ankieta składała się z 3 sekcji, w której pytania były pogrupowane w 6 kategorii. Na podstawie tak skonstruowane ankiety, istniała możliwość dogłębnego zbadania zachowań respondentów oraz ich wiedzy. Dodatkowo, niektóre pytania były ze sobą skorelowane, których zależność wpływała na całkowity ogląd wiedzy respondentów. Na ich podstawie powstała powyższa analiza odpowiedzi ankietowanych. Dzięki szczegółowym odpowiedziom, powstała możliwość stworzenia ogólnego profilu ankietowanych.

Przeprowadzone badania wykazały, że użytkownikom brak podstawowej wiedzy na temat mechanizmów działania chmury obliczeniowej oraz ich praktycznego zastosowania

w oferowanych im usługach internetowych. Większość respondentów utożsamia chmurę obliczeniową z dyskiem wirtualnym, czyli miejscem przechowywania ich prywatnych danych. Dominująca grupa nie zna innej funkcjonalności chmury, pomimo ciągłego korzystania z usług zaliczanych do kategorii chmury obliczeniowej. Blisko jedna czwarta użytkowników, nie mała świadomości korzystania z chmury obliczeniowej. Ankietowani głównie zamieszczali w chmurze obliczeniowej dane powszechnie dostępne, ale blisko jedna czwarta opublikowała dane wrażliwe, których upublicznienie mogło by pociągnąć poważne konsekwencje dla nich samych oraz firm, w których pracują.

Większość użytkowników obawia się ataku w cyberprzestrzeni, a w szczególności utraty środków pieniężanach, zgromadzonych na rachunku bankowym, w wyniku ataku hakera. W następnej kolejności użytkownicy obawiają się naruszenia prywatności oraz kradzieży danych osobowych. Pomimo obaw na temat zgromadzonych danych na swoich urządzeniach, znacząca grypa ankietowanych nie podejmuje podstawowych działań zmierzających do ich ochrony. Przeprowadzone badania dowodzą, że to użytkownicy głównie ponoszą winę za udostępnienie osobom trzecim ich danych, a tym samym za negatywne skutki takich działań. Przyczyną takiej sytuacji jest brak świadomości podstawowych działań, które w praktyce zapewniają bezpieczeństwo. Ankietowani głównie doceniają wartość fizyczną nośników i sprzętu, a pomijają poziom istotności informacji. Respondenci dbają o swój sprzęt. Większość zabezpiecza go hasłem, jednakże wygoda przeważa nad bezpiecznym korzystaniem z danych. Dominująca cześć ankietowanych posiada łatwe do odgadnięcia hasło oraz używa go wielokrotnie nie różnych portalach. Dodatkowo regularnie zmieniają hasła, co nie zawsze jest pożądaną praktyką we współczesnej cyberprzestrzeni.

Na korzyść ankietowanych należy zaliczyć posiadanie przez nich włączonej zapory ogniowej oraz godna pochwały jest praktyka czyszczenia urządzeń z danych przed ich wyrzuceniem lub sprzedaniem. Większość respondentów sprawdza nadawców wiadomości oraz rozszerzenia otrzymanych załączników. Niekorzystnie wypada spora liczba ankietowanych, która ignoruje te praktyki. Niewiele ponad połowę respondentów robi kopie zapasowe danych. Niestety, tylko niewielka część przechowuje je w innej lokalizacji niż macierzyste pliki, sprawiając, że stworzone kopie stają się bezwartościowe.

Głównymi problemami ankietowanych to niewiedza, wygoda oraz brak świadomości odpowiedniego postepowania w sieci.

Rozdział IV Sposoby zabezpieczania danych na co dzień i w chmurze obliczeniowej

Zabezpieczanie danych w cyberprzestrzeni nie należy do rzeczy prostych. Wcześniej w tej pracy przedstawiono wiele możliwych ataków. Każdy z nich przebiega wieloetapowo. Wybierając konkretny rodzaj ataku, agresor może przełamać tylko część zabezpieczeń. W takim wypadku atak sprowadza się do wybierania odpowiedniej ścieżki poprzez zabezpieczenia ofiary, torując sobie drogę do cennych danych. Stanowi to strategiczną i taktyczną przewagę agresora nad obrońcą. Podczas obrony, wymagane jest zabezpieczenie wszystkich potencjalnych punków dostępu oraz ustanowienie dodatkowych perymetrów ochronnych, aby uniemożliwić wykradzenie większej ilości danych, w sytuacji przełamania zabezpieczeń. To na tej podstawie tworzy się różnica między kosztami zabezpieczenia systemu, a przeprowadzonego ataku. Jedynym rzeczywistym sposobem ochrony jest zmuszenie agresora do poniesienia tak wielkich kosztów ataku, że proceder pozyskania danych stanie się dla niego niekorzystny. Wtedy można uznać system za bezpieczny. Inna sytuacja zachodzi, gdy agresorowi nie zależy na zdobyciu informacji, tylko na wyrządzeniu jak najbardziej dotkliwych szkód. W takim wypadku system nigdy nie może być uznany w pełni za bezpieczny. Koszty na obronność powinny stanowić priorytetową pozycję w budżecie właściciela. Aby uzyskać jak największe bezpieczeństwo, należy zastosować wiele praktyk już podczas tworzenia zabezpieczeń systemu oraz zwiększyć świadomość użytkowników. Jedynie ta kombinacja czynników może przynieść relatywnie dobre wyniki.

W tym rozdziale przedstawiono możliwe sposoby zabezpieczenia chmury obliczeniowej przed niepożądanym dostępem. Następnie zaprezentowano stosowane techniki obrony i zabezpieczenia sieci, które mogą zwiększyć świadomość użytkowników cyberprzestrzeni, a dotyczą zabezpieczenia zgromadzonych zasobów i danych.

4.1. Bezpieczeństwo w chmurze obliczeniowej

Obowiązująca w Polsce ustawa o ochronie danych osobowych, (Dz. U. z 2015r. poz. 2135 t.j. ze zm.) nakłada na każdy podmiot i administratora witryn Internetowych obowiązek ich ochrony przed nieupoważnionym dostępem czy przejęciem. Do danych objętych ochroną zalicza się wszelkiego rodzaju dane pozwalające na identyfikację konkretnej osoby. Należą do nich miedzy innymi: imię, nazwisko, adres, e-mail, numer telefonu, numer IP czy

prywatne pliki użytkowników. Autorzy i administratorzy baz danych powinni również dostosować do innych przepisów, ustaw i rozporządzeń, które odnoszą się do dziedziny ochrony danych osobowych. Jednym z ważniejszych jest Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. (Dz. U. z 2004 r. Nr 100, poz. 1024) wraz z załącznikami do niego. Twórcy centrów danych, którzy świadczą usługi w ramach chmury obliczeniowej, na terenie Polski, muszą dostosować się do tych przepisów. Załączniki do (Dz. U. z 2004 r. Nr 100, poz. 1024) jasno definiują, w jaki sposób powinna być zbudowana infrastruktura, która będzie przechowywać dane. Załącznik A w akapitach I-VII mówi o sposobach zachowania użytkownika względem dostawcy usługi oraz o podstawowych standardach bezpieczeństwa i środkach, jakie należy podjąć. Załącznik B odnosi się do środków bezpieczeństwa, podejmowanych w razie przechowywania danych o podwyższonym poziomie tajności. Załącznik C, analogicznie jak pozostałe, cechuje środki bezpieczeństwa występujące na wysokim poziomie. Dzięki temu dokumentowi powstało zagadnienia logicznej i fizycznej ochrony danych w chmurze, przed możliwym ich wyciekiem i nieupoważnionym do nich dostępem. Takie zabezpieczenia są budowane przed zagrożeniami, które pochodzą z publicznej sieci Internet. Logiczne zabezpieczenie danych powinno obejmować wiele aspektów działalności centrów danych. Do najważniejszych dziedzin zalicza się monitorowanie i kontrola przepływu danych miedzy systemami administratora, a siecią otwartą oraz zapytaniami pochodzącymi z sieci publicznej, w głąb centra danych. W oparciu o wyżej wymienione ustawy i rozporządzenia, przygotowano podstawowe czynności, które należy podjąć, aby zapewnić bezpieczeństwo danych w chmurze obliczeniowej oraz by polepszyć już istniejące. Zostały one rozszerzone, posiłkując się źródłami: [MaRo11], [WWW30], [WWW40], [WWW41], [WWW42].

4.1.1. Umowne zabezpieczenia usługi świadczonej w chmurze obliczeniowej

Standardowa chmura publiczna zapewnia elastyczność pracy w przestrzeni świadczonej usługi i jest dostępna z każdego miejsca na ziemi. Oferowana moc obliczeniowa pochodzi z zwirtualizowanych jednostek zlokalizowanych w jednym wielkim centrum danych. Według starych standardów, takie informacje powinny wystarczyć większości klientom do pracy na serwerach oferowanych przez dostawców usługi w chmurze obliczeniowej. Współcześnie, globalni liderzy informują klientów, w jakim regionie znajdują się serwery, z których aktualnie korzystają, ale dokładniejsze dane nieraz bywają utajniane. Dzieje się tak ze względu na sposób zabezpieczania takich centrów danych. Z perspektywy banków, takie podejście do tematu jest niedopuszczalne, ponieważ muszą one wiedzieć gdzie

przechowywane są ich dane. Postepowanie takiej jest wymuszone przez Komisję Nadzoru Finansowego, która między innymi sprawuje nadzór nad bankami w Polsce oraz nad rynkiem kapitałowym, emerytalnym, ubezpieczeniowym oraz instytucjami pieniądza elektronicznego. Podstawowe standardy wobec współpracy z zewnętrznymi dostawcami usług znalazły się w Rekomendacji D [WWW30]. Według niego, „bank powinien posiadać sformalizowane zasady współpracy z zewnętrznymi dostawcami usług informatycznych, zapewniające bezpieczeństwo danych i poprawność działania środowiska teleinformatycznego, uwzględniając również usługi świadczone przez podmioty należące do grupy kapitałowej banku." W razie przekazania części uprawnień do zewnętrznego podmiotu, który zapewnia usługi, dzięki którym przetwarzane są dane posiadające wysoki stopień poufności, dostawca powinien spełnić szereg specjalistycznych powinności. Występuje taka okoliczność w razie przekazania ich do infrastruktury opartej na chmurze obliczeniowej. Należą do nich:

- Dane, które są wysyłane poza infrastrukturę banku, powinny być odpowiednio zabezpieczone przed ewentualnym dostępem osób trzecich. Powinne być jasno sprecyzowane mechanizmy kontroli takich danych. Przykładowo: wszystkie przesyłane dane musza być szyfrowane.

- Bank powinien mieć gwarancję oraz narzędzie, dzięki któremu otrzyma wszelkie informacje na temat wystąpienia jakiegokolwiek incydentu, który może zagrażać bezpieczeństwu danych. Dostawca usługi powinien automatycznie raportować o takich zdarzeniach. Dodatkowo powinny zostać ustalone zasady i tryb współpracy miedzy podmiotami w razie wystąpienia jakiegokolwiek zdarzenia.

- Banki powinny posiadać pełne informacje na temat lokalizacji przechowywanych danych. Bardzo ważne są jasno zdefiniowane przepisy prawa, według których będą zależne dane banku i serwery dostawcy. Świadczone usługi powinny być zgodne z prawem lokalnym oraz zapewniać czytelne powiazania z Polskim prawodawstwem, dzięki którym nie zostanie ono złamane. Bankom zaleca się przechowywanie danych w europejskiej przestrzeni. Krytycznie wyrażana jest opinia o lokowaniu danych na serwerach znajdujących się w USA. Ustawa PATRIOT Act zapewnia tamtejszym sądom możliwość sprawdzenia danych w serwerowniach zlokalizowanych na terenie tego kraju. Zgodnie z tą ustawą, w razie wystąpienia podejrzenia dzianina na

szkodę rządu USA oraz zagrażającego jego istnieniu [WWW39] , mogą one zażądać dostępu do danych. Stanowi to rażące naruszenie polskiego ustawodawstwa względem poufności danych.

- Przed rozpoczęciem współpracy, powinny być zapewnione skuteczne i sprawdzone mechanizmy, które pozwolą bezpiecznie i w zorganizowany sposób zakończyć dalszą współpracę. Dzięki tym mechanizmom, powinny zostać zwrócone dane właścicielowi. Przechowywane kopie zapasowe wraz z niepotrzebnymi już danymi powinny zostać trwale i całkowicie usunięte.
- Bank powinien przeanalizować wcześniejsze wypadki naruszenia bezpieczeństwa. Na ich podstawie musi być przeprowadzona analiza zasadności wymuszenia, jak również przedstawienie przez dostawcę odpowiednich certyfikatów. Powinny one być zgodne z uznanymi na arenie międzynarodowej normami, które dotyczą bezpieczeństwa informacji. Najistotniejsze jest przeanalizowanie tych procedur w razie przetwarzania danych w lokalizacjach znajdujących się poza granicami Europejskiego Obszaru Gospodarczego.
- Strony umowy świadczenia usług powinny mieć jasno określone obowiązki oraz zakres odpowiedzialności, jaką ponosi każda ze stron. Powinny się również znaleźć zapisy dotyczące kar umownych w razie nieprzestrzegania warunków umowy. Najważniejszą jest kwestia bezpieczeństwa przechowywanych danych przez usługodawcę.

4.1.2. Fizyczna ochrona centrów danych

Operatorzy największych na świecie centów danych, czyli Amozaon, Google czy Microsoft, mają opracowane projekty budowy i zarządzania ogromnymi fermami serwerów, ponieważ tą tematyką zajmują się od dziesięcioleci. Naturalnym więc było, przeszczepienie zdobytych doświadczeń na grunt chmury obliczeniowej.

Ze względów bezpieczeństwa, najnowocześniejsze centra danych znajdują się w nierzucających się w oczy budynkach, które są zlokalizowane tak, by jak najlepiej wtapić się w otoczenie. Takie budynki powinny być budowane w cetnarach biznesowych lub wręcz w okolicach zamieszkania ludności. Ważna jest też bliskość węzłów telekomunikacyjnych,

gdyż to gwarantuje osiągnięcie najlepszych parametrów łącz teleinformatycznych. Bardzo często stosuje się mocno zaawansowane zabezpieczenia w budynkach wraz z ochroną o przeszkoleniu wojskowym. W celu zapewnienia lepszej ochrony, można skorzystać z różnych rozwiązań. Należą do nich:

- Telewizja przemysłowa, obejmująca swoim zasięgiem zarówno zewnętrzne otoczenie budynku jak i wnętrze.
- Strefy bezpieczeństwa z kontrolowanym dostępem. Może się opierać o system kart magnetycznych lub inny marker biometryczny
- Standardowa lista osób z uprawnieniami, które mogą wejść do obiektu
- Ochrona monitorująca ośrodek
- Centrum operacyjne i zwalczania zagrożeń
- Pracownicy obsługi technicznej
- Wielostopniowe systemy alarmowe pracujące w trybie ciągłym

A. Mateos w [MaRo11], twierdzi, że budynki powinny być chronione lepiej od baz wojskowych, a dostęp ściśle ograniczony. Osoba, która próbuje dostać się na teren ośrodka, powinna przechodzić wieloetapowy sprawdzenie tożsamości, oparte o więcej niż jedna cecha charakterystyczna. W razie pozytywnego przejścia przez weryfikację tożsamości, odwiedzający musi poruszać się w towarzystwie autoryzowanego personelu. Wszystkie wizyty są rejestrowane i rutynowo sprawdzana jest ich zasadność.

Dane w chmurze są przechowywane na serwerach w danej lokalizacji w sposób rozproszony. Jednostka nadzorcza przydziela sumaryczną moc obliczeniową i przestrzeń dyskową, ale nie występuje ona fizycznym na jednym urządzeniu, a powiązane są w charakterystyczne węzły. W nim są aktywnie zamieszczone dane klienta oraz kopia zapasowa innego węzła. W razie awarii któregoś serwera, można w ten sposób w locie przywrócić jego funkcjonalność na innej jednostce. Poprzez takie podejście do zbierania danych, stworzono system, który można wykorzystać jako jeden z elementów bezpieczeństwa. Bez dokładnych map z rozmieszczeniem danych, kradzież jednego nośnika uniemożliwi odzyskanie pełnych danych konkretnego klienta, ponieważ nigdy nie znajdują się całościowo w jednej lokalizacji [WWW38]. W razie kryptograficznego zabezpieczenia danych, staje się niemożliwe uzyskanie jakichkolwiek informacji z tego wolumenu. Z drugiej

strony, zarządca serwerowni potrafi wskazać fizyczną lokalizacje danych w obrębie danego obiektu, w razie wystąpienia takiego zapotrzebowania. Sam dostęp do danych możliwy jest przez klienta działającego przez Internet. Użytkownik nie ma dostępu do innej przestrzeni, niż ta, do której ma autoryzowany dostęp. Praca na danych odbywa się przez interfejs i bramę komunikacyjną, która komunikuje się z jednostką zarządczą. Posiada ona zmapowaną budowę sieci, która należy do osoby zgłaszającej żądanie. To przez nadzorcę komunikują się serwery, pozbawione możliwości komunikowania się miedzy sobą. Takie podejście umożliwia separację danych między każdym serwerem oraz użytkownikiem. Zastosowanie bramy dostępowej uniemożliwia zastosowanie szerokiej gamy ataków, takich jak: sniffing czy spoofing.

4.1.3. Logiczna ochrona centrów danych

Ochrona logiczna stanowi rozszerzenie zabezpieczeń fizycznych. Odbywa się to całkowicie w cyberprzestrzeni.. Dostęp do danych i samych usług odbywa się przez dedykowanego klienta, który obsługuje takie funkcje. Może on oddzielać dane, do których się łączy tak, by działały tylko w kontekście zalogowanego klienta. Można osiągnąć ten efekt poprzez wydzierżawienie uprawnień tylko dla danej sesji. Z definicji, muszą one posiadać certyfikaty bezpieczeństwa, które są powszechnie cenione na świecie. Są one wymagane podczas świadczenia usług dla instytucji finansowych oraz rządowych.

Uprawnienia do działania w chmurze obliczeniowej są dziedziczone wraz z systemami operacyjnymi, które zostały uruchomione w przestrzeni wirtualnej. Zarządca może przydzielić kilka wolumenów z systemami do każdego użytkownika, ale musi on mieć możliwość i uprawnienia do pracy z nimi. Stanowi to analogiczne rozwiązanie, jakie można spotkać w tradycyjnej serwerowni. Różni się stopniem kręgów uprawnień, które musi rozpatrzyć użytkownik. W razie wystąpienia szczególnie wrażliwych danych, można dodatków zaszyfrować dane, poprzez oprogramowanie kryptograficzne, które znajduje się na jednostce nadzorczej. W przypadku połączenia się przez innego nadzorcę, niemożliwe jest odzyskanie danych przez jednostkę niepożądaną. Podobna sytuacja zachodzi podczas wybrania subregionu, w którym przechowywane są dane. Nie ma możliwości sięgnięcia do zasobów znajdujących się w innym subregionie, ponieważ nie pozwalają na to uprawnienia. Każdy subregion znajduje się w innej lokalizacji, a przenoszone są zazwyczaj kopie zapasowe miedzy nimi. W razie wystąpienia krytycznej awarii, można błyskawicznie się przełączyć na nowy region, nie tracąc danych i płynności działania.

Do logicznego zabezpieczenia danych należy zaliczyć sposoby usuwania danych z centrów danych. Usunąć dane można poprzez interfejs klienta, który komunikuje się z jednostka nadzorcza. Inną opcją jest skasowanie całego dysku wirtualnego z przydzielonej przestrzeni. Kasowanie danych w chmurze obliczeniowej przebiega poprzez nadpisanie bajtów danych przez losowy ciąg zero-jedynkowych wartości. Proces odbywa się kilkukrotnie, w celu uniemożliwienia odczytania, a nawet odzyskania danych przez wyspecjalizowane oprogramowanie. W razie skasowania całego dysku wirtualnego, bez wcześniejszego jego nadpisania, kasowane są mapy dostępowe do danych. Dzieje się to w sposób podobny do standardowych systemów operacyjnych. Dane są dopiero zerowane podczas nowego przydzielenia danej przestrzeni do następnego klienta.

4.1.4. Certyfikaty bezpieczeństwa

Każde zabezpieczenie jest uważane za dobre i spełniające swoje funkcje, do momentu przetestowania ich z realnym zagrożeniem. Z drugiej strony, nie wystawia się cennych zasobów na możliwe ataki. W celu wypracowania kompromisu, powstały certyfikaty, zaświadczające o przejściu audytu bezpieczeństwa danych w cyberprzestrzeni oraz fizycznych nośników. Otrzymanie certyfikatu bezpieczeństwa to długotrwały i kosztowny proces ciągłych kontroli zabezpieczeń, sposobów obchodzenia się z incydentami oraz ogólnie rozumianej polityki firmy. Przed rozpoczęciem audytu, przez wiele miesięcy są gromadzone dane ewidencji. Sam audyt trwa około 6 miesięcy i jest przeprowadzany raz w roku. Opisane w tym rozdziale możliwe praktyki zabezpieczenia chmury obliczeniowej, stanowią częściowo zalecenia, potrzebne do uzyskania certyfikatu bezpieczeństwa SAS70 typu II [WWW41]. Był on wydawany przez Amerykański Instytut Biegłych Rewidentów. Organizacja posiadająca ten certyfikat, wykazywała się wystarczającą wewnętrzną kontrolą jednostki i dbałością o jego poprawienie. Posiadanie tego certyfikatu było wymagane, by można było pracować ze sprawozdaniami finansowymi klientów. Stanowił on zabezpieczenie dla przejrzystości sprawozdań. Ten certyfikat został rozwinięty i zastąpiony przez SAE16. Od swojego poprzednika różni się głównie pisemnym zaświadczeniem dostawcy usługi, który podlega audytowi, o strukturze w jakiej działa organizacja. Dodatkowo wskazywani są klienci oraz rodzaj świadczonych im usług. Zaświadczane dane musza być rzeczywiste, a przedsiębiorstwo musi działać w zadeklarowanej strukturze. W Europie istnieje lustrzany certyfikat o nazwie ISAE 3402 [WWW42]. Do tych standardów odnosi się rekomendacja KNF [WWW30]. Wśród popularnych certyfikatów znajduje się jeszcze ISO 27001 – przyznawany systemom zarządzania informacjami.

Posiadanie certyfikatów przez dostawcę chmury obliczeniowej zaświadcza o zabezpieczeniu dostępu do danych, przed możliwymi atakami hakerów. W tej przestrzeni ciężko uzyskać lepsze efekty bez znaczącego skoku technologicznego. Należy się skupić nad możliwymi użytkownikami chmury obliczeniowej i sieci, gdyż to w nich znajduje się potencjalne medium ataku agresorów, którzy chcą pozyskać wartościowe dane.

4.2. Zapobieganie nieupoważnionemu dostępowi do zasobów komputera

Świadomość użytkowników chmury obliczeniowej, w stosunku do zagrożeń współczesnej cyberprzestrzeni i sposobów zabezpieczania się, plasuje się na niskim poziomie. Udowodniła to przeprowadzona ankieta. Podjęto próbę wskazania podstawowych technik ochrony danych w cyberprzestrzeni oraz zaproponowano postępowanie mogące zwiększyć świadomość użytkowników. Wcześniej w tej pracy, w rozdziale 2 zostały omówione najczęstsze ataki na sieć i korzystających z nich ludzi. Należą do nich:

- Skanowanie
- Ataki DoS i DDoS
- Insider attack w tym ARP spoofing
- Podsłuch
- DNS spoofing
- Brute force
- Ataki fizyczne na platformę
- Atak socjotechniczny

Na ich podstawie stworzono modelowe środki bezpieczeństwa dla standardowego użytkownika.

Osoba rozpoczynająca korzystanie z cyberprzestrzeni powinna poprawnie skonfigurować zaporę ogniową oraz połącznie internetowe. Takie działanie ograniczy znacząco większość potencjalnych zagrożeń, a niektóre nawet wykluczy. Dobry firewall ogranicza możliwość poznania wewnętrznej topologii sieci wraz z zainstalowanymi

systemami operacyjnymi na stacjach roboczych. Stanowi to organicznie danych pozyskany podczas skanowania. Docelowo, utrudni to planowanie następnych kroków podczas w popełnianiu czynów kryminalnych.

Następnym krokiem w zabezpieczaniu sieci lokalnej, powinno być pozamykanie wszystkich nieużywanych portów w routerze oraz na platformie, z której użytkownik łączy się z Internetem. Pozostawienie nieblokowanych zbyt dużej liczby portów, utrudnia nadzorowanie ich oraz sprawia, że staje się niemożliwe pełne kontrolowanie sieci. Przeciętny użytkownik pozostawia otwarte porty, które nie są domyślenie blokowane. Jest to skutek braku wiedzy o istnieniu takiego pojęcia jak port w sieci oraz umiejętności, pozwalających zablokować nieużywane porty.

Użytkownik Internetu, który posiada jakąś instancję świadczącą usługi dla klientów, już ma możliwość obrony przed potencjalnym atakiem typu DoS lub DDoS. Opiera się ona na minimalizowaniu wyrządzonych szkód. Współcześnie istnieją narzędzia, które zablokują możliwość połącznie do danego serwera, a jednocześnie zabezpieczą istniejącą infrastrukturę oraz oferowany produkt. W takim wypadku, zawsze wystąpi odmowa dostępu, ale nie wygeneruje to dodatkowych kosztów, które należało by pokryć na odzyskanie danych oraz na opłacenie pracowników. Inną metodą obrony jest zakupienie większego łącza internetowego, który zapewni dłuższy czas działania serwera, przed wyczerpaniem puli adresów i jego zablokowaniem. Skutkiem takiego postepowania, będzie umożliwienie wykrycia potencjalnego ataku, a następnie odcięcia adresów, z których on następuje. W wypadku ataku DoS, atak przebiega z wąskiego źródła, a wiec szybkość reakcji powinna być zwiększona, a wyrządzone szkody ograniczone. Przed atakami typu DoS i DDoS przeciętny użytkownik nie może się obronić. W razie otrzymania bardzo dużej liczby odpytań, większość standardowych urządzeń sieciowych się zawiesi lub przestanie odpowiadać. Najważniejszym zadaniem powinno być dla niego, niedopuszczenie do zarażenia komputera złośliwym oprogramowaniem, który spowoduje, że platforma dołączy do bot netu, wykorzystywanego w atakach DoS. Zarażony komputer. będący zombii, działa dużo wolniej niż powinien według specyfikacji technicznej, co utrudnia korzystanie z niego. Aby zabezpieczyć się przed przejęciem komputera, należy posiadać odpowiedni antywirus, który zapobiegnie instalacji na nim szkodliwego oprogramowania. Jest to jedyna rzecz, którą może zrobić przeciętny użytkownik w starciu z DoS. Następnym krokiem jest profilaktyka działań, poprzez nie odwiedzenie niepożądanych stron internetowych, na których mogą znajdować się złośliwe podprogramy.

W zabezpieczaniu się przed potencjalnymi atakami i złośliwym oprogramowaniem, należy zadbać o osoby i jednostki mogące znaleźć się w sieci, a znające jej rozłożenie wraz z zabezpieczeniem. Współczesne wirusy mogą przedostawać się przez sieć lokalną omijając zewnętrzny firewall. Wykorzystują one protokół ARP do rozsiewania niepożądanych treści na inne komputery. W ten sposób komputer może stać się zombii i dołączyć do bot netu, ale również może nastąpić przekierowanie sesji do agresora. W takim momencie zyska on nieograniczony dostęp do ofiary. Zdarzają się przypadki podłączenia zainfekowanego komputera do podsieci. W takim wypadku jedyną obroną jest posiadanie dobrego antywirusa z aktualną bazą sygnatur złośliwego oprogramowania, która będzie w stanie zablokować niepożądane działania agresora. Wirusy lub agresor wewnątrz sieci, może próbować podmienić przechowywane DNS, które tłumaczą wpisane adresy znakowe na odpowiednie adresy IP. Najlepszą obroną jest zastosowanie podstawowych adresów, dostarczanych przez Googla. Są one powszechnie uważane za bezpieczne. Ograniczenie serwerów dostarczających prywatne DNS, może uchronić przed niepożądanymi działaniami. Dzięki takiemu podejściu, szybko można zidentyfikować podmienienie DNS.

Rozpatrując sposoby zabezpieczenia zasobów cyfrowych przed osobą z wnętrza sieci, należy zastanowić się, czy nie należy zabezpieczyć platformy przed różnego rodzaju atakami fizycznymi. Najprostszym sposobem zabezpieczania danych jest zamykanie na klucz drzwi do pomieszczenia, w którym znajduje się komputer. Wielu użytkowników skupia się na potencjalnym ataku z sieci, a bagatelizuje znane z kart historii przypadki włamania do mieszkań i gabinetów. W ich następstwie mogą zostać skradzione dokumenty z cennymi informacjami oraz nośniki danych, które je zawierają. Należy zastosować zdroworozsądkowe podejście do tej dziedziny zabezpieczeń. Zagłębiając się w tematyce fizycznego ograniczenia dostępu, nie należy pozostawiać komputera bez nadzoru w widocznym miejscu. Pomijając możliwość fizycznej kradzieży, w razie dostępu do komputera, agresor może zrobić dowolną rzecz z zastaną platformą. W książce [LiTi04], w odniesieniu do sytuacji uzyskania fizycznego dostępu, pada konkluzja, według której ofiara jest przegrana, gdy dopuściła do takiej sytuacji. Metodą na utrudnienie dzianina agresora jest zabezpieczenie dostępu do komputera za pomocą hasła.

Metoda blokowania hasłem jest powszechnie znana, jednak wiele osób bagatelizuje jego znaczenie dla bezpieczeństwa, na korzyść łatwego dostępu i wygodnego użytkowania. Hasła powinny być zbudowane z losowych znaków, nie znajdujących się w słowniku. Nie powinno być krótkie, a jego długość powinna być ponad 10 znaków. Dodatkowo hasło

powinno być wzbogacone o dodatkowe znaki specjalne. Nie należy ograniczać się do jednego znaku specjalnego oraz nie powinny występować obok siebie. Ograniczenie te należy zastosować wobec umiejscowienia znaków na klawiaturze oraz również jako kolejne znaki w haśle. Dopełnieniem dobrego hasła stanowi kilka cyfr wplecionych hasło. Niektóre firmy posiadają politykę bezpieczeństwa, która wymusza częste zmiany haseł dla swoich pracowników. Z założenia, miało to ograniczyć potencjalny wyciek danych, w razie zdobycia dostępu przez osoby niepożądane. Wtedy posiadałyby one ograniczony czas, kiedy dysponowałyby dostępem. W razie wystąpienia takiego wymogu, należy stosować hasła niepasujące do wcześniej stosowanego. Nie należy stosować hasła seryjnego, gdzie zmianą stanowiłyby przyrost liczby numerycznej lub kolejny znak specjalny według zadanego klucza. Przekreśla to sens posiadania zaawansowanego zabezpieczenia. Pracownicy powinni być informowani o takim wymogu. Zastosowanie hasła seryjnego skutecznie potrafi oszukać mechanizmy sprawdzajcie hasła i ich bezpieczeństwo. Podczas tworzenia hasła należy unikać słów ze słownika, szczególnie takich uchodzących za popularne w użytku oraz takie które można łatwo powiązać z osoba wymyślającą hasło. Do takich słów można zaliczyć imię członka rodziny, miejscowość urodzenia, zamieszkania, imię zwierząt domowych, ulubiony sport czy serial. W razie przeprowadzenia jakiegokolwiek wywiadu na temat ofiary, takie słowa klucze zostaną wykorzystane w pierwszej kolejności. W razie stworzenia bardzo trudnego hasła, należy je zapamiętać, a nie zapisywać go na żadnej kartce lub innym nośniku, który mogłaby zdobyć osoba postronna. Do rożnych profili, kont i storn należy stosować zróżnicowane hasła. Wtedy agresor będzie zmuszony łamać hasła do każdej instancji osobno, co znacząco zwiększy czas wymagany na zdobycie danych oraz sprawi, że koszty przeprowadzenia akcji, przekroczą potencjalną wartość zdobytych danych.

Stworzone hasło dostępowe, powinno być przechowywane na serwerach w sposób nie jawy, wręcz zaszyfrowany lub zahaszowany. Za haszowane dane posiadają stało-liczbową reprezentację pseudolosowej liczby. Takie zaprezentowanie hasła umożliwia stworzenie sumy kontrolnej, na podstawie której można określić, czy dane były zmodyfikowane. Zabezpieczać przez szyfrowanie należy nie tylko hasła, ale również wszelkiego rodzaju połączenia oraz same dane. Zaszyfrowane połączenia posiadają tę zaletę, że w razie jej przechwycenia przez osoby trzecie, nie będą one w stanie pozyskać jakichkolwiek danych bez specjalistycznych narzędzi. Połączenia te są trudnodostępne oraz kosztowne, co organiczna ich potencjalne masowe zastosowanie. Szyfrowanie danych powinno być zwyczajem każdego użytkownika cyberprzestrzeni, który posiada w niej jakiekolwiek wartościowe informacje. Standard

przechowywania danych w takiej postaci, znacząco ograniczyłby proceder kradzieży danych wrażliwych, a ponadto wpłynąłby pozytywnie na poprawę bezpieczeństwa. Dla osób korzystających z publicznych chmur obliczeniowych należących do potentatów na rynku, takie zachowanie stanowi normalną praktykę. Należy ją rozszerzyć na inne dziedziny życia. Jednocześnie szyfrowane dane zabezpieczą przed możliwym podsłuchaniem komunikacji użytkowania z chmurą obliczeniową.

Po zaszyfrowaniu danych, bardzo ciężko pozyskać je w inny sposób, niż bezpośrednio od samego właściciela lub osoby, która je zabezpieczyła. Ludzie niechętnie dzielą się swoimi danymi, chyba, że zostaną do tego przekonani lub przez przypadek. Wtedy ludzie podają je świadomie, przekonani że nie robią nic złego, co później może nieść za sobą nieraz bardzo poważne konsekwencje. Jest wiele metod ataku socjotechnicznego, dlatego nie sposób wskazać uniwersalną metodę obrony przed tym typem ataku. Sama koncepcja wykorzystania czyiś nawyków, uczuć i zachowań, a nawet wiedzy na temat zabezpieczeń sprawia, ze obrona jest niezwykle trudna. Przekonali się o tym czytelnicy portalu niebezpeicznik.pl, których przypadek został opisany w [WWW43]. Ofiary znały podstawowe sposoby zabezpieczenia się przed oszustwem, ale ich koncentracja i czujność została uśpiona, czego konsekwencją była strata dużej ilości pieniędzy. Na tym przykładzie można wyróżnić kilka podstawowych czynności, które należy wykonać za każdym razem, kiedy użytkownik kontaktuje się z kimkolwiek w cyberprzestrzeni. Należą do nich:

- W razie otrzymania jakieś wiadomości w cyberprzestrzeni, należy dokładnie sprawdzić nadawcę tej wiadomości, aby upewnić się, czy ktoś nie podszywa się pod autoryzowane serwery. W takich wypadkach, nazwa może wiązać się z jakimś znanym portalem lub profilem, ale domen nie jest zgodna ze wykorzystywanym standardowo.

- Należy przeanalizować wiadomość, która się otrzymało. Większość oszustw jest bardzo prymitywna. Często zagraniczny agresor wykorzystuje podstawowego tłumacza do przekonwertowania wiadomości na język odbiorcy. Inne wiadomości mogą zostać wysłane z kont znanych użytkownikowi osób, tak jak na rysunku nr 29. Użytkownik otrzymuje wiadomość z prośbą o pomoc od osoby którą zna, ale również taka wiadomość może pochodzić od osoby nieznanej. Zazwyczaj taka wiadomość zawiera prośbę o pomoc finansową, udział w konkursie lub w celu weryfikacji jakiś

danych. Takie zapytania należy weryfikować przez inny kanał komunikacji niż cyberprzestrzeń. Podejrzenia powinny wzbudzić zmiana stylu pisania nadawcy oraz nietypowe prośby. Takie zdarzenia należy zgłaszać samej osobie, od której otrzymało się wiadomość, o ile jest to znajomy oraz na policję w celu ukrócenia procederu kryminogennego.

Rysunek nr 29 Przykład ataku socjotechnicznego
Źródło: Facebook, rozmowa prywatna

- Następnym krokiem w celu zabezpieczenia się jest weryfikacja linków, które użytkownik otrzymał. Należy wyróżnić, czy zawierają protokół zabezpieczający transmisję, wyrażony przedrostkiem HTTPS. W razie jego zastosowania, trudniej jest podszyć się pod znane domeny. Dodatkowo po kliknięciu w link wyświetla się właściciel protokołu, który umieścił w nim swój podpis. Należy zwracać uwagę, czy adres nie posiada jakiś dodatkowych dopisków, które mogą zawierać konkretne zapytanie w postaci skryptu, ale będą ukryte przed ofiarą. Na końcu, powinno się weryfikować domenę, do której odsyła link. W artykule [WWW43], budowa linku opierała się o allegro.showtime.pl/(…), przy czym słowo showtime było zacieniowane, czego niektórzy użytkownicy mogli nie zauważyć.
- Wiadomość powinno sprawdzać się, pod kątem obecności złośliwego oprogramowania lub ukrytych skryptów. Można w tym celu używać programów antywirusowych, które powinny informować o nieodpowiedniej

zawartości. Innym sposobem jest wyświetlanie źródła maila, który jest reprezentacją wiadomości przed przetworzeniem jej przez przeglądarkę.

- Nie należy ulegać uprzejmościom rozmówcy i bezgranicznie mu wierzyć. Agresor może próbować uśpić czujność rozmówcy. Taka sytuacja miała miejsce w zdarzeniu z relacji w [WWW43]. Oszust sam sugerował odpowiednie rozwiązania, rzekomo w celu zwiększenia bezpieczeństwa. Dodatkowo okazywała troskę o pomyślność transakcji, która właśnie się odbywała.

- Po odczytaniu treści wiadomości, należy przeanalizować zasadność jej samej. W przypadku prośby o autoryzację, należy rozważyć, czy w ten sposób komunikacji przynależy do polityki bezpieczeństwa organizacji, która je wysłała. Najważniejsze jest określenie, czy użytkownik sam zgłosił takie zapotrzebowanie, czy jest ono wygenerowane przez osobę trzecią.

- Należy zwiększać świadomość osób mniej obytych z technikami zabezpieczenia zasobów. Próby wyłudzenia danych występują, ponieważ istnieją jednostki, które im ulegają. Wraz ze wzrostem świadomości zagrożeń i bezpieczeństwa, spadnie współczynnik przestępstw w cyberprzestrzeni.

Zakończenie

Celem poznawczym pracy było przedstawienie w oparciu o literaturę, zasad działania chmury obliczeniowej, znaczenia oraz istności bezpieczeństwa zasobów w niej zgromadzonych, a także form i celów ataków na nie. W rozdziale pierwszym przedstawiono sposoby działania chmury obliczeniowej oraz zasadność jej zastosowania w przedsiębiorstwach i dla użytkowników indywidualnych. W rozdziale drugim omówiono zagadnienia i istotność zabezpieczeń przed zróżnicowanymi formami ataków. W rozdziale trzecim przedstawiono wyniki przeprowadzonego badania dotyczącego świadomości użytkowników na temat bezpieczeństwa w chmurze obliczeniowej. Cel poznawczy osiągnięto dzięki analizie publikacji naukowych oraz źródeł internetowych, a także przeprowadzonemu badaniu grupy użytkowników chmury obliczeniowej.

W czwartym rozdziale przedstawiono wzorcowy model stosowanych rozwiązań zabezpieczeń oraz istniejące normy prawne mające na celu zapewnienie bezpieczeństwa danych zgromadzonych w chmurze obliczeniowej. Osiągnięto tym samym cel metodologiczny pracy, którym było przedstawienie możliwych do zastosowania praktyk oraz rozwiązań użytkowników, administratorów i projektantów chmury obliczeniowej, w celu zapewnienia bezpieczeństwa jej zasobów.

Przeprowadzona analiza publikacji naukowych oraz dostępnych źródeł internetowych, a także analiza przeprowadzonego badania, umożliwiły wyciagnięcie dodatkowych wniosków.

Na podstawie analizy przeprowadzonego badania, stwierdzono niski poziom wiedzy użytkowników, na temat wykorzystywanych usług z chmury. Większość z nich wie, że korzysta z chmury obliczeniowej, ale rozpatruje ją jedynie w kategorii dysku wirtualnego gdzie przesyła swoje dane, bez odpowiedniego ich zabezpieczania. Wielu z nich, nieświadomie korzysta z innych usług świadczonych w ramach chmury obliczeniowej. Użytkownicy zazwyczaj nie umieszczają danych wrażliwych w cyberprzestrzeni, ale osobiście ich dodatkowo nie zabezpieczają. Użytkownicy obawiają się ataków w cyberprzestrzeni, ale jak wynika z analizy wyników ankiety, nie znają podstawowych praktyk zabezpieczania się w sieci. Lęki nie wpływają na próby poprawy zabezpieczeń. Wielu z nich utożsamia bezpieczeństwo danych z bezpieczeństwem fizycznym, zaniedbując inne formy bezpieczeństwa. Wartość danych oceniają na podstawie nośników, na których się znajdują. Sprawia to, ze staja się łatwymi celami dla potencjalnych agresorów.

Przedstawione w pracy metody zabezpieczania się w sieci powinny być powszechnie nauczana. Obowiązkowo należałoby dodać je do programu nauczania w szkołach oraz na szkoleniach pracowniczych. Przełożyłoby się to na poprawę bezpieczeństwa w sieci. Podwyższanie świadomości społeczeństwa, na temat bezpieczeństwa, może zapewnić pasywną ochronę, nawet dla tych użytkowników, którzy się do niej świadomie lub nieświadomie nie stosują. Napastnicy natrafiając na zwiększony opór ofiar, będą musieli docelowo zrezygnować lub ograniczyć szkodliwe działanie, z powodu na trudności w dostępie do danych oraz wysokiego kosztu ich pozyskania.

Załączniki

Załącznik 1. Kwestionariusz ankiety pt.: "Świadomość bezpieczeństwa w chmurze obliczeniowej"

Czy korzystasz z chmury komputerowej?

- Tak
- Nie

Czym według Ciebie jest chmura komputerowa?

……

Jakie znasz rodzaje chmury obliczeniowej

…….

Czy korzystasz z którejś z wymienionych usług?

- Poczta elektroniczna (Gmail, Hotmail, itd.)
- Dysk wirtualny (Dropbox, OneDrive, Google Drivie)
- Amazon EC2
- Google App Engine
- Amazon SimpleDB
- Cloudkick
- Kalendarz Googl lub pokrewne
- Program do rozliczania podatków, dostępny przez stronę internetowa
- Wordpress
- Nie korzystam

Które z wymienionych usług jest według Ciebie chmurą komputerową?

- Poczta elektroniczna (Gmail, Hotmail, itd.)
- Dysk wirtualny (Dropbox, OneDrive, Google Drivie)
- Amazon EC2
- Google App Engine
- Amazon SimpleDB
- Cloudkick
- Kalendarz Googl lub pokrewne
- Program do rozliczania podatków, dostępny przez stronę internetowa
- Wordpress
- Skype
- Systemy ERP (płatny za wykorzystanie)
- Salesforce

Jakie dane zostały przez Ciebie umieszczone w chmurze?

- Płeć
- Wiek
- Imię
- Nazwisko
- Aders email
- Zdjęcia
- Pesel
- Dane przedsiębiorstwa/ pracodawcy
- Adres zamieszkania

- Nie umieszcza prywatnych danych w chmurze

Czy zabezpieczasz hasłem dostęp do swojego komputera?

- Tak
- Nie

Czy blokujesz komputer, kiedy oddalasz się od swojego stanowiska pracy?

- Tak
- Nie

Czy pozostawiasz swój komputer w widocznym miejscu lub bez nadzoru?

- Tak
- Nie

Czy stosujesz trudne do odgadnięcia hasła?

- Tak
- Nie

Czy regularnie zmieniasz hasła?

- Tak
- Nie

Czy stosujesz to samo hasło do różnych logowań?

- Tak
- Nie

Czy posiadasz włączoną zaporę ogniową (firewall)?

- Tak
- Nie

Czy czyścisz dane z nośników pamięci, przed ich sprzedażą lub wyrzuceniem?

- Tak
- Nie

Czy otwierasz maile/ linki od nieznanych nadawców?

- Tak
- Nie

Czy weryfikujesz rozszerzenia załączników, zanim je otworzysz?

- Tak
- Nie

Czy wylogowujesz się z odwiedzanych kont?

- Tak
- Nie

Czy wykonujesz kopie zapasowe?

- Tak

- Nie

Czy kopie zapasowe przechowujesz w różnych miejscach?

- Tak
- Nie
- Nie dotyczy

Czy zabezpieczasz kopie zapasowe rożnymi hasłami?

- Tak
- Nie
- Nie dotyczy

Czy obawiasz się ataku w cyberprzestrzeni?

- Tak
- Nie

Jakiego ataku w cyberprzestrzeni się obawiasz?

- Przestępstw bankowych
- Kradzieży danych
- Naruszenia prywatności
- Uzyskania nieuprawnionego dostępu do danych/informacji osobistych/informacji służbowych
- Uniemożliwienie dostępu do usług (w tym przeciążenia serwerów)
- Zniszczenia danych
- Nękania (cyberstalking)
- Naruszenia prawa autorskiego
- Nie obawiam się ataku

Jesteś

- Kobietą
- Mężczyzną

Twój przedział wiekowy

- poniżej 20 lat
- 20-29 lat
- 30-39 lat
- 40-50 lat
- Powyżej 50 lat

Miejsce zamieszkania

- Wieś
- Miasto: mniej niż 50 000 mieszkańców
- Miasto: między 50 000 a 100 000 mieszkańców
- Miasto: miedzy 100 000 a 300 000 mieszkańców
- Miasto: między 300 000 a 500 000 mieszkańców
- Miasto: powyżej 500 000 mieszkańców

Jakie jest Twoje wykształcenie

- Podstawowe
- Średnie
- Zawodowe
- Wyższe

Bibliografia

Literatura

[Batk11] Batko A.: *Haker umysłów,* wyd. Helion, Gliwice 2011

[ChuC11] Chu-Carrol M..: *Google App Engine. Kod w chmurze,* wyd. Helion, Gliwice 2011

[Doro01] Doroziński D.: *Hakerzy. Technoanarchiści cyberprzestrzeni,* wyd. Helion, Gliwice 2001, s. 287-288

[Hend13] Handzel Z.: *Cloud computing – czyli chmura obliczeniowa i możliwości jej wykorzystania w mediach,* [w:] Glinka B., Hensel P. (red.), *Problemy zarządzania vol. 11 nr 4 (44) Zarządzanie humanistyczne*, wyd. Wydział zarządzania uniwersytetu Warszawskiego, Warszawa 2013

[KaSk98] Kaczmarek J., Skowroński A.: *Bezpieczeństwo: Świat –Europa – Polska,* wyd. Atlas, Wrocław 1998, s 5

[Kuba13] Kubalińska M.: *Wpływ cloud computing na budowę społeczeństwa informacyjnego i rozwój gospodarczy,* źródło: http://www.ur.edu.pl/file/50167/10.pdf dostęp 10.01.2016r.

[KuNi13] Kuc M., Niemczyk W.: *Rynek usług cloud computing – współczesne wyzwania, zagrożenia, perspektywy,* źródło: http://zif.wzr.pl/pim/2013_1_1_27.pdf dostęp 10.01.2016r.

[KwLi00] Kwiatkowka-Basałaj B., Lisiecki M.: *Pojęcie bezpieczeństwa oraz prognostyczny model jego zapewnienia,* [w:] Tyrał P. (red.), *Zarządzanie bezpieczeństwem – Międzynarodowa konferencja naukowa Kraków 11-13 maja 2000*, wyd. Profesjonalnej Szkoły Biznesu, Kraków 2000

[Łęża14] Łężak D.: *Bezpieczeństwo wewnętrzne państwa a organizacja Mistrzostw Europy w Piłce Nożnej Euro 2012,* [w:] Osiński J.. (red.), *bezpieczeństwo – współczesne wymiary*, wyd. Oficyna wydawnicza Szkoła główna handlowa w Warszawie, Warszawa 2014

[LiTi04] Littlejohn Sinder D., Tittel E.: *Cyberprzestępczość – Jak walczyć z łamaniem prawa w Sieci,* wyd. Helion, Gliwice 2004

[LLS14] Li K., Li Q., Shin T.: *Cloud Computing and Digital Media: Fundamentals, Techniques, and Applications* wyd. CRC Press, Boco Raton 2014

[MaRo11] Mateos A., Rosenberg J.: *Chmura obliczeniowa. Rozwiązania dla biznesu,* wyd. Helion, Gliwice 2011

[Noga12] Nogal P.: *Biznes w chmurach,* źródło: Zarządzanie i Finanse = Journal of Management and Finance. - 2012, R. 10, nr 1, cz. 1, s. [447]-457., wyd. Wydział Zarządzania Uniwersytety Gdańskiego, Gdańsk 2012

[Pańk09] Pańkowska M.: *Model biznesowy przetwarzania rozproszonego cloud computing,* [w:] Gołuchowski J., Frączkiewicz-Wronki A. (red.), *Technologie wiedzy w zarządzaniu publicznym '10*, wyd. Akademii Ekonomicznej im Karola Adamieckiego w Katowicach, Katowice 2009

[PaSz12] Paździor M., Szmulik B.: *Instytucje bezpieczeństwa narodowego,* wyd. C.H. Beck, Warszawa 2012, rozdział I

[PaZa13] Pałka D., Zaskórski P.: *Bezpieczeństwo danych w chmurze obliczeniowej,* [w:] Grzywny Z.(red.). *Bezpieczeństwo w procesach globalizacji – dziś i jutro*, wyd. Wyższa Szkoła Zarządzania Marketingiem i Języków Obcych w Katowicach, Katowice 2013

[Podg68] Podgórecki A.: *Logika praktycznego działanmia*, wyd. Książka i Wiedza, Warszawa 1968, t2. S. 47

[Rosz13] Roszkowski M.: *Model chmury obliczeniowej jako narzędzie społeczeństwa informacyjnego*, [w:] Zeszyty naukowe nr 763. Ekonomiczne problemy usług nr 105. *Europejska przestrzeń komunikacji elektronicznej. Tom II*, wyd. Wydawnictwo naukowe Uniwersytetu Szczecińskiego, Szczecin 2013

[SaWo12] Sadecki B., Wolny W.: *Idea chmury obliczeniowej z zastosowaniem w biznesie*, [w:] Porębska-Miąc T., Sroka H.: Systemy wspomagania organizacji. SWO 2012, wyd. Wydawnictw Uniwersytetu Ekonomicznego w Katowicach, Katowice 2012

[Wart14] Wartych R.: *Cloud computing jako jeden z dominujących trendów w rozwoju usług IT*, źródło: Zeszyty Naukowe Uniwersytetu Gdańskiego. Studia i Materiały Instytutu Transportu i Handlu Morskiego. - 2014, nr 11, s. 89-104, Wydawnictwo Uniwersytety Rzeszowskiego, Rzeszów 2013

[Zięb99] Zięba R.: *Instytucjonalizacja bezpieczeństwa europejskiego: koncepcje – struktury – funkcjonowanie*, wyd. Scholar, Warszawa 1999

[Zior12] Ziora L.: *Rola technologii cloud computing w zarządzaniu przedsiębiorstwem,* [w:] Zeszyty naukowe nr 702. Ekonomiczne problemy usług nr 87. *Gospodarka elektroniczna, Wyzwania rozwojowe. Tom I*, wyd. Wydawnictwo naukowe Uniwersytetu Szczecińskiego, Szczecin 2012

Netografia

[WWW1] Chmura obliczeniowa – ekspertyza. Dla Dyrekcja generalna ds. Polityki Wewnętrznej Uni Europejskiej 2012 http://www.europarl.europa.eu/RegData/etudes/etudes/join/2012/475104/IPOL-IMCO_ET%282012%29475104_PL.pdf (dostęp 14.03.2016r.)

[WWW2] Rekomendacja dla National Institute of Standards and Technology http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf (dostęp 03.05.2016r.)

[WWW3] Angielska strona Wikipedia, wpis o Cloud computing https://en.wikipedia.org/wiki/Cloud_computing (dostęp 04.05.2016r.)

[WWW4] Dokumentacja Amazon elastic Compute Cloud (amazon EC2) http://aws.amazon.com/documentation/ (dostęp 04.05.2016r.)

[WWW5] Strona Microsofru Azure z informacjami o produktach i cennikach usług https://azure.microsoft.com/pl-pl/ (dostęp 09.05.2016r.)

[WWW6] Artykuł z portalu Gartner na temat chmury hybrydowaej http://blogs.gartner.com/thomas_bittman/2012/09/24/mind-the-gap-here-comes-hybrid-cloud/ (dostęp 7.06.2016r.)

[WWW7] Opis chmury publicznej z portalu techtarget.com http://searchcloudcomputing.techtarget.com/definition/public-cloud (dostęp 7.06.2016r.)

[WWW8] Artykuł o chmurze prywatnej zawierający jego szczegółowy opis http://www.informationweek.com/private-clouds-take-shape/d/d-id/1070793? (dostęp 7.06.2016r.)

[WWW9] Doktryna cyberbezpieczeństwa Rzeczpospolitej Polski wydana przez Biuro Bezpieczeństwa Narodowego dnia 20.01.2015, http://en.bbn.gov.pl/ftp/dok/01/DCB.pdf (dostęp 15.08.2016r.)

[WWW10] Opracowanie Doktryny cyberbezpieczeństwa Rzeczpospolitej Polski w 2015 roku, odnośnie [WWW9] https://wszystkoconajwazniejsze.pl/tomasz-aleksandrowicz-doktryna-cyberbezpieczenstwa-rzeczypospolitej-polskiej (dostęp 15.08.2016r.)

[WWW11] Słownik pojęć stosowany przez Biuro Bezpieczeństwa Narodowego https://www.bbn.gov.pl/pl/bezpieczenstwo-narodowe/minislownik-bbn-propozy/6035,MINISLOWNIK-BBN-Propozycje-nowych-terminow-z-dziedziny-bezpieczenstwa.html (dostęp 15.08.2016r.)

[WWW12] Pojęcie bezpieczeństwo według słownika PWN http://sjp.pwn.pl/slowniki/bezpiecze%C5%84stwo.html (dostęp 15.08.2016r.)

[WWW13] Pojęcie bezpieczeństwo według encyklopedii PWN http://encyklopedia.pwn.pl/encyklopedia/bezpiecze%C5%84stwo.html (dostęp 15.08.2016r.)

[WWW14] Artykuł o wykorzystaniu chmury obliczeniowej w marketingu http://interaktywnie.com/biznes/artykuly/biznes/chmura-w-marketingu-dlaczego-marketerzy-wybieraja-rozwiazania-typu-cloud-computing-251149 (dostęp 7.09.2016r.)

[WWW15] Statystyki użytkowników, korzystających z dysku wirtualnego dropbox.com http://expandedramblings.com/index.php/dropbox-statistics/ (dostęp 07.09.2016r.)

[WWW16] Statystyki liczby użytkowników Internetu http://www.internetlivestats.com/internet-users/ (dostęp 07.09.2016r.)

[WWW17] Przykładowy wyciek danych z chmury obliczeniowej, zawierający zdjęcia celebrytek https://niebezpiecznik.pl/post/namierzono-wlamywacza-ktory-opublikowal-nagie-zdjecia-modelek-i-aktorek-a-powazna-dziura-w-find-my-iphone-zalatana/ (dostęp 08.09.2016r.)

[WWW18] Raport CERT o stanie polskiego Internetu i odnotowanych zagrożeniach na rok 2014 https://www.cert.pl/wp-content/uploads/2015/11/Raport_CP_2014.pdf (dostęp 08.09.2016r.)

[WWW19] Raport CERT o stanie polskiego Internetu i odnotowanych zagrożeniach na rok 2015 https://www.cert.pl/PDF/Raport_CP_2015.pdf (dostęp 08.09.2016r.)

[WWW20] Artykuł o podstawowych zasadach w zabezpieczaniu komputerów i nośników danych http://www.computerworld.pl/news/397526/10.zasad.bezpieczenstwa.ktorych.nie.powinny.ignorowac.male.i.srednie.firmy.html (dostęp 10.09.2016r.)

[WWW21] Artykuł o fingerprint – odciskach palców systemów operacyjnych https://nmap.org/man/pl/man-os-detection.html (dostęp 1.09.2016r.)

[WWW22] Definicja ataku wewnętrznego https://www.techopedia.com/definition/26217/insider-attack (dostęp 30.08.2016r.)

[WWW23] Opis ataku spoofing oraz jego odmian http://www.computerworld.pl/news/315264_1/Spoofing.sztuka.ataku.i.obrony.html (dostęp 28.08.2016r.)

[WWW24] Opis ataku SQL injection http://www.securitum.pl/baza-wiedzy/publikacje/sql-injection (dostęp 24.08.2016r.)

[WWW25] Artykuł o klasyfikacji włamań internetowych http://hackme.pl/articles.html?article_id=247 (dostęp 23.08.2016r.)

[WWW26] Wykład o włamaniach do sieci http://edu.pjwstk.edu.pl/wyklady/bdk/scb/main06.html (dostęp 23.08.2016r.)

[WWW27] Artykuł o prawie i bezpieczeństwie w chmurze obliczeniowej http://sylwesterjezierski.pl/prawo-i-bezpieczenstwo-w-chmurze-obliczeniowej-mini-przewodnik-dla-biznesmena/ (dostęp 22.08.2016r.)

[WWW28] Artykuł cechujący zagrożenia w chmurze komputerowej http://websecurity.pl/tag/chmura-zagrozenia/ (dostęp 22.08.2016r.)

[WWW29] Bezpieczeństwo w chmurze komputerowej http://www.benchmark.pl/testy_i_recenzje/bezpieczenstwo-danych-w-chmurze.html (dostęp 15.08.2016r.)

[WWW30] Bezpieczeństwo centra danych w chmurze obliczeniowej http://www.spidersweb.pl/2014/07/zabezpieczenia-danych-w-chmurze.html (dostęp 14.09.2016r.)

[WWW31] Rekomendacja KNF dotycząca przetwarzania danych w chmurach obliczeniowych m.n 10.6 -10. 12 https://www.knf.gov.pl/Images/Rekomendacja_D_8_01_13_uchwala_7_tcm75-33016.pdf (dostęp 24.08.2016r.)

[WWW32] Artykuł o wycieku danych z chmury obliczeniowej Dropbox.com https://niebezpiecznik.pl/post/dropbox-po-4-latach-przyznaje-ze-doszlo-do-kradziezy-hasel/ (dostęp 10.09.2016r.)

[WWW33] Specyfikacja USB 3.0 http://www.usb.org/developers/docs/documents_archive/usb_30_spec_070113.zip (dostęp 10.09.2016r.)

[WWW34] Zalecenia dotyczące posiadania haseł http://pomoc.onet.pl/46,4374,faq_serwis.html (dostęp 11.09.2016r.)

[WWW35] Zalecenia Google dotyczące ochrony haseł https://www.google.com/intl/pl_pl/safetycenter/everyone/start/password/ (dostęp 11.09.2016r.)

[WWW36] Artykuł o udostepnieniu numeru prezydenta w otwartej specyfikacji https://niebezpiecznik.pl/post/numer-telefonu-prezedenta/ (dostęp 11.09.2016r.)

[WWW37] Opis utraty kopi zapasowych z serwerowni 2be.pl https://niebezpiecznik.pl/post/wlamanie-do-serwerowni-2be-pl-od-5-dni-klienci-sa-pozbawieni-wszystkich-uslug-i-traca-dziesiatki-tysiecy-zlotych-kazdego-dnia/ (dostęp 11.09.2016r.)

[WWW38] Opis aspektów związanych z bezpieczeństwem platformy oktawave – chmury obliczeniowej https://kb.oktawave.com/Knowledgebase/Article/View/264/94/rozszerzony-opis-aspektow-zwizanych-z-bezpieczestwem-platformy-oktawave#Zabezpieczenie (dostęp 13.09.2016r.)

[WWW39] Objaśnienie ustawy Patriot Act https://www.justice.gov/archive/ll/highlights.htm (dostęp 13.09.2016r.)

[WWW40] Opis certyfikatu bezpieczeństwa SSAE16 http://ssae16.com/SSAE16_overview.html (dostęp 15.09.2016r.)

[WWW41] Opis certyfikatu bezpieczeństwa SAS70 http://sas70.com/ (dostęp 15.09.2016r.)

[WWW42] Opis certyfikatu bezpieczeństwa ISAE3402 http://isae3402.com/ (dostęp 15.09.2016r.)

[WWW43] Atak phishing na użytkownikach portalu OLX.PL https://niebezpiecznik.pl/post/kupujesz-na-olx-uwazaj-na-scam-na-allegro/ (dostęp 21.09.2016r.)

Akty prawne

1. Ustawa z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz. U. z 2015r. poz. 2135 t.j. ze zm.)

2. Rozporządzenie Ministra Spraw Wewnętrznych i administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100, poz. 1024)
3. Załącznik do rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. (poz. 1024)

Spis rysunków

Spis tabel

Spis załączników