POLSKO-JAPOŃSKA WYŻSZA SZKOŁA TECHNIK KOMPUTEROWYCH

Wydział Informatyki

Katedra Sieci Komputerowych

Programowanie systemowe i sieciowe

Imię Nazwisko

Nr albumu SXXXXXX

NOWE WYZWANIA W BEZPIECZEŃSTWIE

Praca Magisterska

Promotor

Dr inż. Bardzo Mądry

Warszawa, grudzień 2014

SPIS TREŚCI

1. WSTĘP

Niniejsza praca przedstawia wyzwania, zagrożenia i zabezpieczenia związane z nowymi technologiami informatycznymi rozwijającymi się w obecnych czasach w zawrotnym tempie. Rozwój technologii mobilnych i chmurowych spowodował rozmycie się granic funkcjonowania przedsiębiorstw, i czyni tradycyjne podejście do ochrony informacji - oparte na zabezpieczeniu granic - zupełnie nieadekwatnym do aktualnej sytuacji. Brak podjęcia odpowiednich działań to prosta droga do incydentu, który może spowodować poważne zagrożenie dla bezpieczeństwa i rozwoju organizacji. „Nieautoryzowane ujawnienie wrażliwych informacji może spowodować narażenie firmy na odpowiedzialność prawną czy straty finansowe. Aby zminimalizować takie ryzyko, niezbędne są: dobry plan ochrony, właściwe narzędzia oraz zaangażowanie pracowników.” (Gazprom, 2169)

2. KOLOKACJA, SERWEROWNIA CZY CHMURA ?

Jakie usługi powinniśmy trzymać w naszej firmowej twierdzy bronionej przed światem zewnętrznym wysokimi murami naszych centrów danych? Jakie powinniśmy wyprowadzić do odległych kolokacji i pozwolić na samodzielne życie?

Administratorzy muszą być także gotowi na gorzką rozłąkę z usługami, które odlecą w chmurę.

Ze strony czysto ekonomicznej opłacalność utrzymywania własnej serwerowni jest wątpliwa. Jednak cały czas się to robi.

Głównymi przyczynami utrzymywania własnego data center są:

- bezpieczeństwo i wrodzona nieufność firm,
- skomplikowane kwestie finansowo/inwestycyjne,
- prawo — czasami ospale reagujące na zmiany rzeczywistości,
- chęć utrzymywania swoich rzeczy przy sobie.

Zmiana jest jednak nieunikniona i konieczna. Trzeba porzucić stary, sentymentalny schemat (mimo że daje wrażenie bezpieczeństwa) — własne data center z szafami rackowymi wypchanymi po „dach”, serwerami oraz macierzami — i wybrać inną drogę. Mniej romantyczną oraz bezkompromisową, ale za to perspektywiczną.

2.1. Kolokacja — czyli co warto wypchnąć poza…

Rysunek 1 - Typowe centrum kolokacyjne

Usługi, które na pewno możemy kolokować w odległej lokalizacji, to:

- serwer WWW,
- DNS-y,
- poczta (w niektórych przypadkach).

Możemy się zastanawiać, dlaczego? Po pierwsze — systemy najbardziej wrażliwe z punktu widzenia bezpieczeństwa są przeniesione poza lokalizacje i pule adresowe firmy. Po drugie — nie będzie oczywiste, że zaraz za korporacyjnymi serwerami WWW lub MX znajdują się nasze dane.

Dzięki temu, że centra kolokacyjne mają o wiele bardziej zaawansowaną infrastrukturę niż standardowa serwerownia małej firmy, możemy zapomnieć o zdezelowanych UPS-ach, cieknącej klimatyzacji, ciągłych zanikach transmisji ISP, czy walce z SLA.

Należy, a wręcz wymagane jest, aby zobaczyć lokalizację, do której migrujemy. Lista klientów danego centrum kolokacyjnego także może powiedzieć wiele o jakości usług przez nie oferowanych. Pamiętajmy o tym, że Internet jest jak papier - zniesie wszystko, a nie trafimy wtedy do „centrum kolokacyjnego” w „ziemiance”.

Poziom ciągłości biznesowej naszych usług może wzrosnąć znacząco, jeżeli wybrana przez nas firma zapewnia standardy, które spełniają nasze oczekiwania. Przykładowo, dla nas dużym osiągnięciem będzie doprowadzenie do tego, że mamy dwóch naprawdę niezależnych dostawców Internetu. Natomiast centrum kolokacyjne ma zazwyczaj takich kilku. Tak samo z zasilaniem — my mamy pana Gucia na jedną czwartą etatu i z problemem choroby „filipińskiej", a oni Tier 3 — wypełniony agregatami, UPS-ami i czym tam sobie jeszcze zamarzymy.

Podsumowując, dzięki kolokacji nasze serwery znajdą się w monitorowanej 24 godziny na dobę serwerowni, wyposażonej w systemy chłodzenia i filtrowania powietrza oraz zasilanie awaryjne. Na dodatek najczęściej centra danych położone są w lokalizacjach jak najmniej narażonych na katastrofy naturalne (powodzie, trzęsienia ziemi, pożary itd.).

Kwestie backupu przy tej dostępności można rozwiązać w prosty sposób tworząc go do siebie - do firmy. Obsługa kolokacji także może zapewnić regularne wykonywanie pełnych kopii zapasowych danych i umożliwić ciągłe monitorowanie stanu backupu. Można też bardziej systemowo - z planem Disaster Recovery, opartym o odrębnie działające środowisko w autonomicznej kolokacji, oddalonej o kilkaset kilometrów.

Dochodzimy teraz do kwestii ekonomicznych. Gdy przeliczymy bardzo skrupulatnie, ze wszelkimi szczegółami, utworzenie własnego data center i jego utrzymanie (generujące bardzo duże koszty stałe obejmujące wydatki na infrastrukturę, energię, personel etc.) oraz porównamy to ze zdalną kolokacją, to może się okazać, że własne serwerownie nie mają najmniejszego sensu, a „wyrzucenie" naszych serwerów, wraz z usługami na nich działającymi, okaże się bardzo opłacalne.

2.2. Własna serwerownia — z czym rozstać się nie można…

Rysunek 2 - Typowa serwerownia

Nie wolno nam ruszyć urządzeń, które przechowują wrażliwe informacje:

- dane osobowe,
- dane laboratoryjno-projektowe,
- systemy mainframe.

Dane osobowe to sprawa oczywista. Wpływ GIODO (Generalnego Inspektora Ochrony Danych Osobowych) na działania specjalistów IT przypomina eksperymenty Iwana Pawłowa. Jeżeli podczas jakiejkolwiek dyskusji na temat infrastruktury serwerowej, jej bezpieczeństwa, architektury itd. pada magiczne słowo „dane osobowe" wszyscy uczestniczący w tej rozmowie zamierają ze strachu przed konsekwencjami, które te słowa implikują. Spory na temat tego, czy „nieszczęsne" dane osobowe można i powinno się przenosić poza swoją lokalizację, są zażarte i niekończące się.

Można oczywiście skierować nurtujące nas pytania do GIODO i otrzymać wyczerpującą odpowiedź. Na przykład - GIODO podczas kontroli może zażądać od nas dostępu do serwerowni. A co jeżeli dana serwerownia jest w Niemczech czy Holandii? Odpowiedź jest prosta - w każdym

państwie członkowskim Unii Europejskiej jest odpowiednik GIODO i nasza instytucja może poprosić tamtejsze służby do przeprowadzenia kontroli bądź wydania opinii.

Ale co jeśli taka serwerownia jest poza UE? Tu trzeba się zastanowić czy to będzie zgodne z ustawą i dyrektywą unijną, gdy będziemy posiadać stosowną umowę na piśmie o powierzeniu przetwarzania danych osobowych z firmą spoza UE. Na terenie UE jest to proste, gdyż należy się powołać na dyrektywę 95/46 WE w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych art. 17 pkt 3 – 4.

Na koniec trzeba pamiętać o tym, że odpowiedź od GIODO nie ma mocy stanowiska formalnego:

”…Generalny Inspektor Ochrony Danych Osobowych może dokonać wiążącej oceny okoliczności przetwarzania danych osobowych jedynie w decyzji administracyjnej, po przeprowadzeniu stosownego postępowania i zbadaniu wszystkich okoliczności faktycznych sprawy, jak również po dokonaniu analizy stosownych przepisów prawa.

Oznacza to, że na list ten nie można się powoływać, jak na kazus prawny. Można jednak na podstawie treści listu domniemywać stanowisko inspektora w ocenie sytuacji podczas toczącego się postępowania, które zakończone zostałoby wydaniem decyzji administracyjnej.”[1]

„Wydaje się więc, że najlepiej nie robić „nic”. Co prawda owo „nic” bywa bardzo kosztowne i problematyczne, ale zdecydowanie o wiele mniej ryzykowne niż igranie z „Wielkim Bratem” GIODO.” (Madry, 2022)

Dane projektowe i laboratoryjne warto utrzymać we własnej serwerowni ze względu na ich ogromną wartość. Są one aktywami naszego przedsiębiorstwa i są o wiele cenniejsze niż informacje, ile zarabia prezes

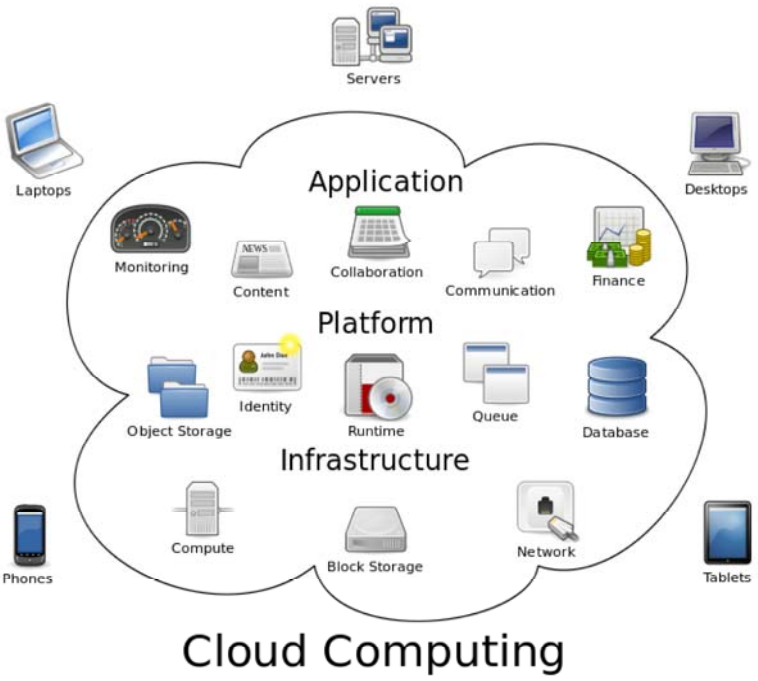
[1] http://ostium.pl/uodo/giodo-ochorna-danych-osobowych/opinia-giodo-o-hostingu-zagranicznym/

itp.. Bardzo ważnym czynnikiem w przypadku tego typu danych jest zapewnienie nadzwyczajnie szybkiego czasu dostępu. Poza tym zajmują one terabajty na naszych macierzach. Powyższe elementy sprawiają, że utrzymywanie tych usług w odległej lokalizacji mogłoby nas kosztować wiele niepotrzebnych problemów — ekonomicznych, technicznych, prawnych.

Przejdźmy teraz do wielkich czarnych pudełek utrzymujących w sobie bazy danych, czyli spotykanych w naszych serwerowniach systemów mainframe. Są duże, bardzo szybkie i potwornie głodne prądu. Poza tym wymagają krystalicznie czystego pomieszczenia i odpowiednio schłodzonego powietrza. Każde zanieczyszczenie pyłem lub zbyt duże wahanie temperatury w serwerowni powoduje możliwość wyłączenia i uszkodzenia maszyn. Przeniesienie czegoś takiego do kolokacji równe jest wyrokowi „śmierci” w firmie. Nikt nie wie, gdzie to się wyłącza, ludzie z serwisu chcą kosmicznych sum za obsługę, a prezes firmy dostaje zawału widząc wycenę całego przedsięwzięcia. Poza tym centra kolokacyjne odpowiednio policzą za specjalne pomieszczenia do tych wielkich czarnych pudełek (czystość i odpowiedni system chłodzenia) oraz za pożartą energię. Migracja plus koszty utrzymaniowe w większości przypadków okażą się spektakularną porażką finansową.

Rysunek 3 – Mainframe

2.3. Cloud Computing — czyli odlot w chmurę…

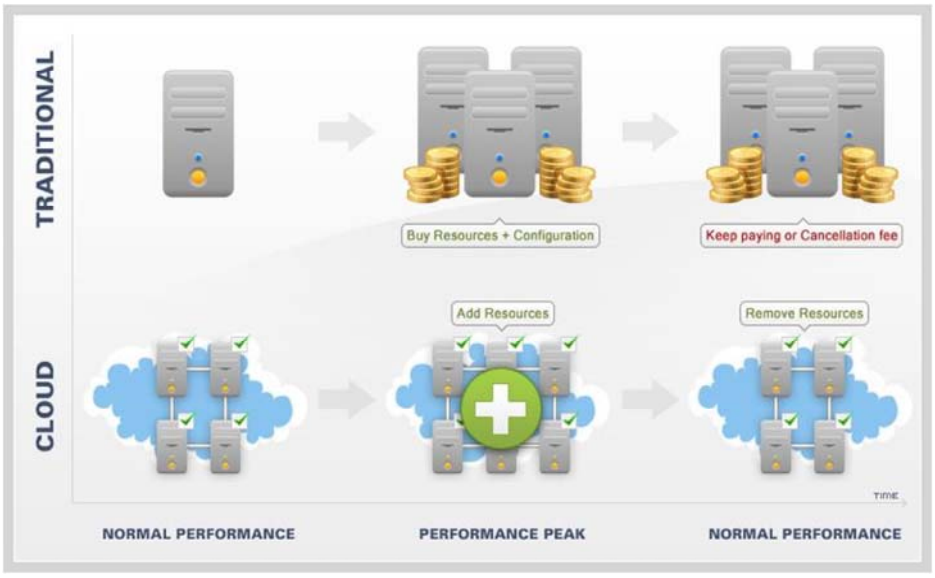


Rysunek 4 – Cloud Computing

Rozwiązaniem pośrednim wobec chmury jest kolokacja. Problemy organizacyjne i mentalne rozwiązane podczas przenosin do kolokacji nie będą już brane pod uwagę przy późniejszej migracji w chmurę, co niesłychanie ułatwi nam przekonanie do niej naszego kierownictwa. Oczywiście i tu nie obejdzie się bez nowych wyzwań, ale przynajmniej wiele będziemy mieli za sobą.

Cloud Computing ma już pewien poziom dojrzałości usług. Oprogramowanie w centrum kolokacyjnym prezentuje nam zasoby w sposób biznesowy. Nie mamy już do czynienia (tak jak w modelu kolokacyjnym) ze wstawianiem serwerów i liczeniem ich poboru mocy itp. Tu płacimy tylko za realne wykorzystanie mocy obliczeniowej przez nasze aplikacje. Ważne jest to, że chmura publiczna pozbawia nas sztywnych kosztów — takich jak m.in. sprzęt. Jest on dla nas nieistotny, ponieważ w pełni opieramy się na zasobach dostawcy. Zmieniają się więc sposób prezentacji kosztów oraz ich struktura.

Główne zalety chmury to łatwość skalowania zasobów, duża wydajność oraz brak problemów związanych z utrzymaniem sprzętu. Możemy w niej sami tworzyć „serwery” i dowolnie je skonfigurować. Pełna kontrola, możliwość zmian ustawień oraz rozliczanie godzinowe powodują, że jest to najbardziej elastyczne rozwiązanie. Sami określamy sposób zagospodarowania dostępnych zasobów, mamy przy tym możliwość powiększenia ilości dostępnej pamięci operacyjnej lub zwiększenia wydajności procesora praktycznie na zawołanie. Nie ma potrzeby przy tym dopełniać jakichkolwiek dodatkowych formalności w postaci umów czy aneksów i działa to w obydwie strony, tzn. bez problemu możemy zwiększyć i zmniejszyć dostępne zasoby. Kolejną zaletą tego rozwiązania jest to, że serwery w chmurze możemy uśpić na godziny nocne, by następnego dnia rano uruchomić je za pomocą jednego kliknięcia lub wcześniej zaplanowanego zadania. Serwer w chmurze to Maluch, który porusza się wolno i spala bardzo mało, ale w sekundę może stać się Ferrari pędzącym z niewyobrażalną prędkością i pożerającym hektolitry paliwa. Nie jest to możliwe w przypadku zakupu/wynajmu serwerów dedykowanych, które musza być „obliczone” na podołanie „szczytowi wydajnościowemu” - występującemu zazwyczaj niezbyt często, przez co przez większość czasu moc obliczeniowa tych maszyn się „marnuje”.



Rysunek 5 – Zalety rozwiązań w chmurze

Chmura daje nam możliwość uruchamiana różnych rodzajów usług. Trzeba tu wziąć pod uwagę charakterystykę naszej firmy, jej zasoby i wymagania — dokładnie tak samo jak w przypadku kolokacji. Głównymi systemami do przeniesienia są serwery WWW, DNS oraz poczty. Kolejnymi kandydatami do migracji do chmury są systemy zarządzania projektami czy pracy grupowej. Również repozytorium plików, dostępne z każdej lokalizacji na świecie i na każdym urządzeniu, jest doskonałym rozwiązaniem. Usługi projektowe, wymagające bardzo szczegółowego rozliczenia kosztów są zdecydowanie najlepszymi kandydatami do przenosin w chmurę. Łatwość w obliczeniu wykorzystanych zasobów, a co za tym idzie i nakładów finansowych to bardzo istotny element, który pozwala na ogromne uproszczenia w międzywydziałowych rozliczeniach.

Kolejne systemy, których migracje należy rozważyć, to systemy deweloperskie i testowe. Daje to dostęp do bardzo klarownego systemu informacji na temat działania projektu, jego bilansu finansowego i opłacalności oraz — co jest najistotniejsze z naszego punktu widzenia — możliwości pokazania zespołowi projektowemu, że każdy ruch w IT kosztuje.

Na koniec przedstawiony zostanie przykład pokazujący zalety chmury przy zakładaniu start up-u:

- nie trzeba wydawać pieniędzy na zakup serwerów, infrastruktury i obsługi do nich,
- w każdej chwili można zwiększyć lub zmniejszyć swoje zasoby w chmurze — łatwa regulacja kosztów i możliwość zwiększenia oraz zmniejszenia mocy obliczeniowych w chwilach rozrostu firmy lub zastoju na rynku,
- brak niespodzianek typu: uszkodzenie sprzętu, konserwacja

A my zajmujemy się „tylko” swoim biznesem…

Niezależnie od tego, czy wybierzemy kolokację, czy też chmurę obliczeniową, musimy być świadomi tego, co robimy, świadomi naszych wymagań, naszej renomy oraz jakości firmy, która dostarcza nam wyżej wymienione usługi. Nie możemy też zapominać o swoich słabościach i niedostatkach dostawcy. Wybór między własną serwerownią a zdalnym fizycznym data center czy też wirtualnym w chmurze wydaje się być – patrząc na pozostałe wyzwania – końcowym, najprzyjemniejszym krokiem.

3. BEZPIECZEŃSTWO SIECIOWE - PROGNOZY

Rozdział nawiązuje do artykułu z portalu branżowego www.computerworld.pl[2], w którym doskonale są przedstawione zagrożenia sieciowe na rok 2013. Dodatkową wartością tego raportu jest uwzględnienie w nim naszej krajowej specyfiki, co przemawia za uwzględnieniem tej publikacji w niniejszej pracy.

„W 2013 roku powinniśmy najbardziej obawiać się ataków na urządzenia mobilne, wyłudzania przez cyberprzestępców poufnych informacji oraz wycieków całych baz danych - prognozują polscy specjaliści od bezpieczeństwa sieciowego.

Zestawienie najpoważniejszych zagrożeń w roku 2013 powstało na podstawie ankiety przygotowanej i opracowanej przez Fundację Bezpieczna Cyberprzestrzeń. Ankieta została skierowana do krajowych ekspertów w dziedzinie bezpieczeństwa sieciowego, siedemnastu z nich udzieliło wyczerpujących odpowiedzi.

Ankieta zawierała zestawienie potencjalnych zagrożeń w 2013 r. Ich lista powstała na bazie międzynarodowych raportów i pomysły autorów. Dodatkowo lista była uzupełniona przez ekspertów, kiedy istotne zagrożenie nie pojawiło się w zestawieniu. Uczestnicy ankiety zostali poproszeni o wyrażenie opinii na temat prawdopodobieństwa powszechnego wystąpienia danego zagrożenia oraz poziomu niebezpieczeństwa w przypadku jego wystąpienia.

Siłą raportu jest jego zakotwiczenie w polskich realiach. Krajową specyfikę w niektórych przypadkach widać wyraźnie, chociażby w ocenie działań prawno-regulacyjnych czy występowania niektórych szczególnych zagrożeń technicznych, które już wystąpiły w polskiej cyberprzestrzeni.”

[2] http://www.computerworld.pl/artykuly/387784/Zagrozenia.sieciowe.2013.html

Prawdopodobne najczęstsze zagrożenia (skala od 0 min. do 5 maks.):

- zagrożenia dla platformy Android - 4,35;
- phishing – przez pocztę elektroniczną i serwisy WWW - 4,24;
- wycieki informacji z baz danych zawierających dane wrażliwe - 4,12.

Najpoważniejsze skutki w razie wystąpienia danego ataku (0-5):

- cyberkonflikty pomiędzy państwami - 4,18;
- wycieki informacji z baz danych zawierających dane wrażliwe - 4,00;
- ataki na Cloud Computing - 3,65.

Jak widać nasi specjaliści wysoko oceniają możliwość i konsekwencje potencjalnych wycieków danych wrażliwych. Wskazują także na niepokojąca prawidłowość używania tych samych loginów i haseł do wszystkich serwisów. Co w przypadku wycieku danych z jakiegoś serwisu społecznościowego może skutkować poważnymi problemami - np. dostęp do kont bankowych przez osoby niepowołane.

W raporcie zostały też wskazane typy zagrożeń spoza dostarczonej listy.

Finansowe:

- ataki na systemy giełdowe,
- ataki związane z płatnościami elektronicznymi (m.in. kradzieże danych kart kredytowych przy użyciu malware'u),
- ataki na karty debetowe paypass i płatności z wykorzystaniem technologii NFC.

Prawo, regulacje i dobre praktyki:

- zwiększenie kontroli nad Internetem przez instytucje międzynarodowe i rządowe,
- brak skutecznych metod współpracy sektora publicznego (zwłaszcza rządowego) z sektorem prywatnym, w kwestii szeroko rozumianego bezpieczeństwa IT,
- brak klarownych kryteriów oceny i porównania skuteczności środków ochrony przed atakami sieciowymi,
- zamieszanie w przepisach skutkujące zamykaniem serwisów internetowych.

Inną ważną informacja jest to że „w prestiżowym rankingu opublikowanym przez amerykański zespół bezpieczeństwa TeamCymru Polska od wielu tygodni zajmuje niechlubne pierwsze miejsce w rankingu największej aktywności botnetów i praktycznie nie wypada z listy TOP 10, krajów, z których pochodzi szkodliwa aktywność teleinformatyczna." (Kassenberg i Nieszczególny, 2014)

Następnym wskazanym problemem jest to „,że dla poziomu bezpieczeństwa w Internecie bardzo duże znaczenie ma prawidłowe podejście do spraw prawodawstwa, regulacji i popularyzowania dobrych praktyk. To sygnał, który powinien zachęcać do działań obie strony dialogu. Nasze doświadczenia w tej sprawie nie są najlepsze i warto odebrać ten głos jako obawę, że skutki podobnych zaniedbań mogą być groźne. Opinie warto zadedykować Ministerstwu Administracji i Cyfryzacji, które przy opracowaniu dokumentu >Polityka Ochrony Cyberprzestrzeni RP< całkowicie pominęło uwagi, jakie pojawiły się w trakcie konsultacji społecznych." (Gazprom, 2169)

Natomiast ze światowej perspektywy należy się przyjrzeć szczególnie tego typu zagrożeniom:

- ataki na Cloud Computing - coraz więcej korporacji trzyma tam dane, więc niewystarczająco chronione usługi chmury obliczeniowej mogą stanowić słaby punkt w bezpieczeństwie firmy,
- ataki Advanced Persistent Threat wymierzone w konkretne osoby publiczne (prezesów największych firm, polityków) za pośrednictwem urządzeń mobilnych,
- ataki wykorzystujące luki w komunikacji M2M (Machine-to-Machine) - skierowane zazwyczaj na platformy związane z bezpieczeństwem narodowym - placówki specjalizujące się w rozwijaniu uzbrojenia i produkcji technologii wojskowych,
- botnety będą atakować równocześnie urządzenia mobilne i stacjonarne - nowe formy ataków DDoS, które uderzą w oba typy urzadzeń równocześnie,
- wzrost ilości złośliwych programów atakujących urządzenia mobilne - użytkownicy odchodzą od tradycyjnych platform na rzecz nowszych, mniejszych urządzeń mobilnych - zabezpieczenie tych urządzeń jest obecnie trudniejsze niż zwykłych komputerów.

Można zauważyć że głównie wzrastają zagrożenia związane z platformami mobilnymi oraz wyciekami danych. Nadchodzą też ciężkie dni dla Cloud Computing, które rozwija się coraz bardziej i przez to pojawia się coraz częściej na celowniku. W niniejszej pracy przedstawiono sposoby ograniczenia ryzyka związanego z tymi zagrożeniami. Ale trzeba być cały czas czujnym i zachować zdrowy rozsadek - nawet najlepsze zabezpieczenia nie pomogą, jeśli atak skierowany jest na człowieka. A wiadomo, że jest on najsłabszym ogniwem i na większość z nas znajdzie się sposób.

4. PODSUMOWANIE

Podsumowując, dziedzina ogólnie rozumianego Bezpieczeństwa Informacji będzie się dalej dynamicznie rozwijała i będą się w tym zakresie pojawiać coraz to nowe zagrożenia - niektóre już istnieją, ale nie zdajemy sobie z nich sprawy. Nieustanny wyścig między nowymi sposobami zabezpieczeń, a nowatorskimi metodami ataku będzie napędzał rozwój pionierskich rozwiązań w tzw. Bezpieczeństwie Informacji tak aby spróbować nadążyć za tzw. Postępem. Ponieważ jest on bardzo szybki, szczególnie w zakresie mechanizmów hackerskich i ich wykrywania, to materiał zawarty w tej pracy szybko straci swoja aktualność.

5. BIBLIOGRAFIA

Gazprom. (2169). Jak napisać pracę inzynierską. W B. Madry, *Wszystko o....* (strony 69-666). Moskwa: PJATK.

Kassenberg, A. i Nieszczególny, W. (2014). *Bezpieczeństwo.* Warszawa: Dobry.

Madry, B. (2022). Pierwsza Zapora. *Zawsze w Sieci*, 444-999.

6. SPIS ILUSTRACJI