Zbigniew Pietras, Wioletta Rudnicka-Bykowska

Prognozy zagrożeń systemów IT

Przegląd Naukowo-Metodyczny. Edukacja dla Bezpieczeństwa nr 1, 53-63

2013

Zbigniew PIETRAS
Toruńska Wyższa Szkoła Przedsiębiorczości
Wioletta RUDNICKA-BYKOWSKA
Akademia Humanistyczno-Ekonomiczna w Łodzi

PROGNOZY ZAGROŻEŃ SYSTEMÓW IT

Każdego dnia i prawie na każdym kroku mamy do czynienia z komputerem. Te pracujące w systemach komputerowych wielkich sieci firmowych, jak również posiadane na użytek własny w domu są narażone na różnego rodzaju zagrożenia. Obecnie, w czasach, gdy te systemy mają tak wielkie znaczenie w zapewnieniu ciągłości pracy przemysłu, usług, a nawet dla istnienia całych skupisk ludzkich, słowo zagrożenie ma kluczowe znaczenie, a bezpieczeństwo tychże systemów powinno być traktowane priorytetowo. Codziennie spotykamy wiele przypadków nieodpowiedzialnego podejścia do kwestii bezpieczeństwa systemów czy też zaniedbywania zabezpieczania poufnych informacji. Od czasu do czasu można przeczytać lub zobaczyć, zazwyczaj w portalach internetowych zajmujących się bezpieczeństwem, rzadziej w prasie fachowej czy telewizji, zgubne rezultaty takich zaniedbań.

Firmy coraz poważniej traktują zadanie zabezpieczenia systemów informatycznych przed groźbami włamań, wykradzenia danych, infekcji ze strony złośliwego oprogramowania i związanych z tym strat finansowych. Rozmiary zagrożeń internetowych wzrosły w ciągu minionego roku aż o 240%, wynika z raportu firmy Panda Software. W poprzednich latach zagrożenia nigdy nie miały tak wielkiej skali. Wzrosła nie tylko ilość złośliwego oprogramowania, ale również jego jakość odmiany wirusów i zakres ich niszczycielskiego oddziaływania. Zarówno korporacyjni, jak i indywidualni użytkownicy powinni zwracać szczególną uwagę na wykonywanie kopii zapasowych swoich danych, zwłaszcza tych o kluczowym znaczeniu zaleca Aleksander Gostew, analityk Kaspersky Lab.[1] Nieustanny rozwój i zmiany zachodzące w systemach IT, ujawniane błędy bezpieczeństwa w stosowanych urządzeniach, oprogramowaniu lub ich konfiguracji oraz niedoskonałości technologii powodują, że wraz z upływem czasu niemal wszystkie systemy IT mogą stać się podatne na zagrożenia bezpieczeństwa.

Dokładna identyfikacja zasobów informacyjnych pozwoli na skuteczną ich ochronę Można je podzielić na kilka ogólnych grup: informacje właściwe, algorytmy, oprogramowanie i sprzęt. **Informacje właściwe** to przetworzone dane w ramach działalności organizacji, posiadające pewną wartość poznawczą. Zazwyczaj mają postać zagregowanych i strukturalizowanych zbiorów, którymi łatwo można zarządzać. Gromadzi się je na bieżąco. Odtworzenie utraconych informacji przy braku środków zabezpieczających jest bardzo kosztowne, a czasem wręcz niemożliwe. **Algorytmy** to metody i procedury postępowania z określonymi informacjami. Te metody mogą być unikalne w obrębie organizacji,

[1] Raport zabezpieczenia antywirusowe są niezbędne, *www.gazetaprawna.pl*

ale równie dobrze mogą stanowić tzw. dobro powszechne. Korzystając z algorytmów można tworzyć nowe informacje lub odtworzyć utracone. Stąd wartość algorytmów jest zwykle większa niż wartość informacji właściwych. **Oprogramowanie** pozwala na realizację oraz automatyzację wykonywania algorytmów. Oprogramowanie może mieć charakter uniwersalny, seryjny, masowy, „z pudełka", ale może również być dedykowane do konkretnych zadań lub nawet firm, indywidualizowane, „szyte na miarę". Utrata oprogramowania łączy się z kosztem zakupu nowego, ewentualnymi sankcjami finansowymi za złamanie umowy licencyjnej. Wszelkiego rodzaju błędy w oprogramowaniu mogą powodować różnorodne straty dla organizacji związane z m.in. morale pracowników, zasobami firmy (czas, pieniądze), realizacją działań wewnętrznych i zewnętrznych firmy, reputacją, wiarygodnością jako partnera. **Sprzęt**, stanowiący platformę działania oprogramowania, dostarcza odpowiednie zasoby wykorzystywane przez oprogramowanie, którego celem jest realizacja algorytmów przetwarzających informacje. Awarie sprzętu również powodują koszty, spadek morale i opóźnienia w wykonywaniu zadań, ale ich skala jest stosunkowo niewielka i tylko w wyjątkowych wypadkach ma wpływ na długoterminowy sukces firmy.[2]

Niniejsze opracowanie podejmuje próbę prognozy zagrożeń systemów IT pod względem liczby, procentowego rozkładu zagrożeń wirusami, piractwa komputerowego oraz nadużyć internetowych, w tym: kradzieży informacji oraz niszczenia i zniszczenia a także zmiany informacji (szczególnie tych istotnych).

1. Prognoza liczby zagrożeń

Dopasowanie liniowej i wielomianowej funkcji regresji[3] dla liczby oszustw komputerowych (wykres nr 1) kształtuje się na małym poziomie około 46%, wartości współczynnika determinacji liniowej R^2.

Średnio roczna liczba przestępstw za analizowany okres wynosi 365, czyli jedno oszustwo na dzień. Biorąc pod uwagę średni roczny przyrost na poziomie 18% można szacować, że liczba oszustw do końca bieżącego roku może wzrosnąć w przedziale od około 500 do około 570.

Dopasowanie liniowej funkcji regresji dla liczby bezprawnie uzyskanych informacji (wykres nr 2) kształtuje się na bardzo wysokim poziomie około 90%. Analogiczna sytuacja występuje dla funkcji wielomianowej, która również jest na wysokim poziomie, około 83% wartości współczynnika determinacji liniowej R^2.

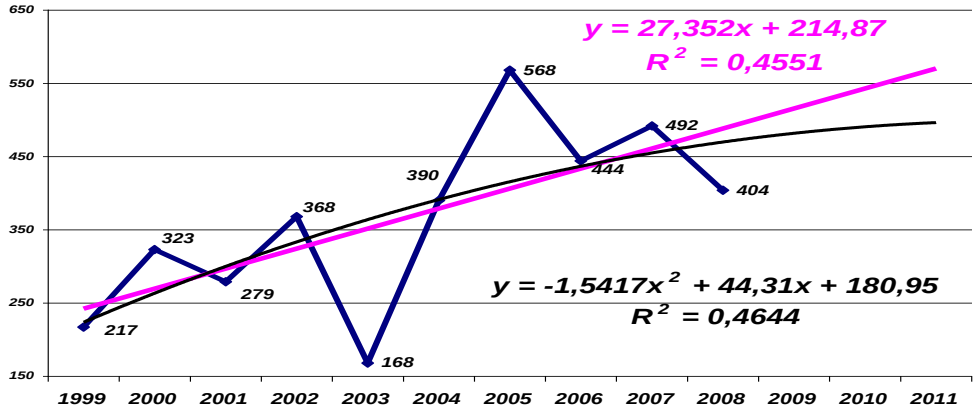
Dla liczby bezprawnie uzyskanych informacji średnio roczna za analizowany okres wynosi 274, biorąc pod uwagę średni roczny przyrost na poziomie 23% można szacować, że liczba oszustw do końca bieżącego roku może wzrosnąć w przedziale od około 531 do około 650.

---

[2] Bezpieczeństwo systemów informacyjnych – rodzaje zagrożeń, *www.egospodarka.pl*

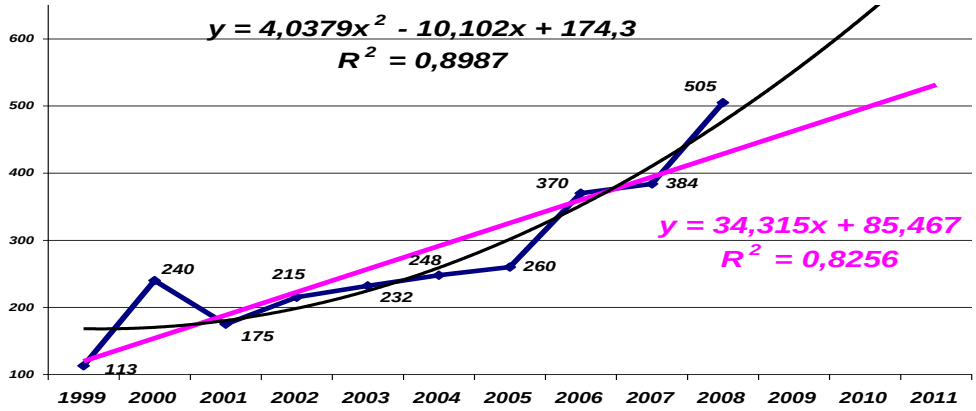
[3] Informacje na temat sposobu wyboru funkcji trendu można znaleźć m.in. w pracy M. Osińska, (red. nauk.), *Ekonometria współczesna*, Wyd. Dom Organizatora, TNOiK. Toruń 2007, rozdz. 9

Wykres nr 1: Liczba oszustw komputerowych wraz z prognozą[4]



Źródło: Z. Pietras oprac. na podst. danych KGP; *http://www.policja.pl/portal/pol/4/321/Przestepczosc_komputerowa.html*

Wykres nr 2: Liczba bezprawnie uzyskanych informacji[5]



Źródło: Z. Pietras oprac. na podst. danych KGP; *http://www.policja.pl/portal/pol/4/321/Przestepczosc_komputerowa.html*

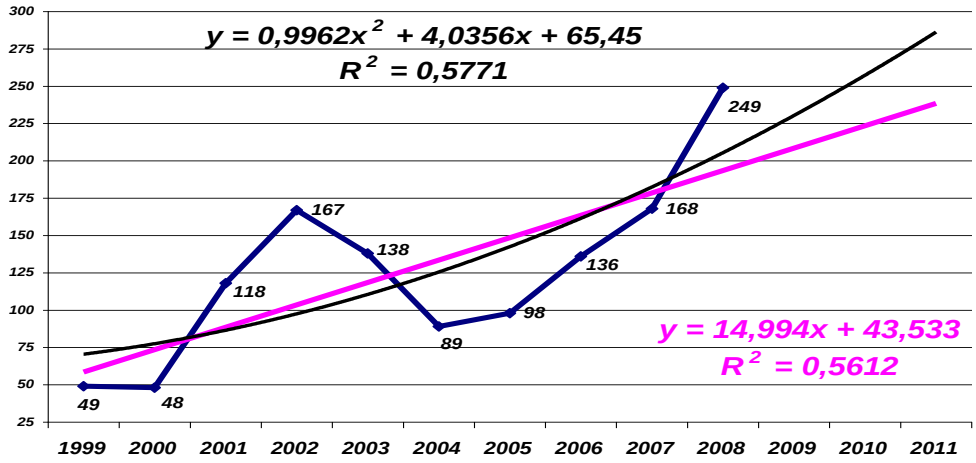
[4] Art. 287. § 1. Kto, w celu osiągnięcia korzyści majątkowej lub wyrządzenia innej osobie szkody, bez upoważnienia, wpływa na automatyczne przetwarzanie, gromadzenie lub przesyłanie informacji lub zmienia, usuwa albo wprowadza nowy zapis na komputerowym nośniku informacji, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.
§ 2. W wypadku mniejszej wagi, sprawca podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.

[5] Art. 267. § 1. Kto bez uprawnienia uzyskuje informację dla niego nie przeznaczoną, otwierając zamknięte pismo, podłączając się do przewodu służącego do przekazywania informacji lub przełamując elektroniczne, magnetyczne albo inne szczególne jej zabezpieczenie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.
§ 2. Tej samej karze podlega, kto w celu uzyskania informacji, do której nie jest uprawniony, zakłada lub posługuje się urządzeniem podsłuchowym, wizualnym albo innym urządzeniem specjalnym.
§ 3. Tej samej karze podlega, kto informację uzyskaną w sposób określony w § 1 lub 2 ujawnia innej osobie.

Dopasowanie liniowej funkcji regresji dla liczby zniszczeń lub zmiany istotnych informacji (wykres nr 3) kształtuje się na średnim poziomie około 56%. Analogiczna sytuacja występuje dla funkcji wielomianowej, która również jest na średnim poziomie około 58% wartości współczynnika determinacji liniowej R^2.

Dla liczby zniszczeń lub zmiany istotnych informacji średnio roczna za analizowany okres wynosi 126, (czyli średnio co drugi dzień roboczy niszczono lub dokonywano zafałszowania istotnych informacji) biorąc pod uwagę średni roczny przyrost na poziomie 28% można szacować, że liczba oszustw do końca bieżącego roku może wzrosnąć w przedziale od około 238 do około 280.

Wykres nr 3: Liczba zniszczeń lub zmiany istotnych informacji[6]



Źródło: Z. Pietras oprac. na podst. danych KGP*; http://www.policja.pl/portal/pol/4/321/Przestepczosc_komputerowa.html*

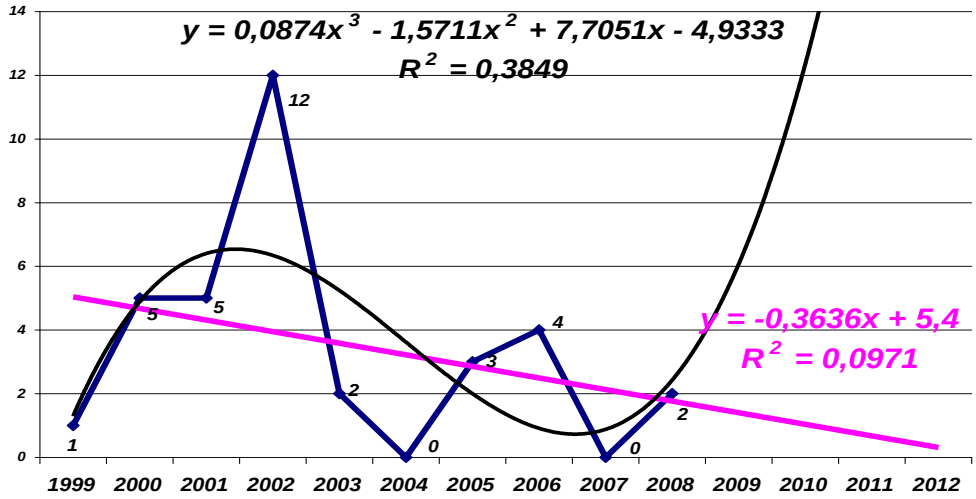
Dopasowanie liniowej funkcji regresji dla liczby niszczonych danych informatycznych (wykres nr 4) kształtuje się na bardzo niskim poziomie około 9%. Dla funkcji wielomianowej, która jest na niskim poziomie około 38% wartości współczynnika determinacji liniowej R^2.

Dla liczby niszczonych danych informatycznych trudno jednoznacznie prognozować sytuację przy zachowującym się ogólnie trendzie malejącym należy sądzić, że coraz lepsze zabezpieczenia oraz zbierane doświadczenia pozwolą na dalsze zmniejszenie liczby niszczonych danych. Biorąc pod uwagę znaczne wahnięcia, należy się również poważnie liczyć ze znaczącym wzrostem tego typu przestępstw.

---

[6] Art. 268. § 1. Kto, nie będąc do tego uprawnionym, niszczy, uszkadza, usuwa lub zmienia zapis istotnej informacji albo w inny sposób udaremnia lub znacznie utrudnia osobie uprawnionej zapoznanie się z nią, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.
§ 2. Jeżeli czyn określony w § 1 dotyczy zapisu na komputerowym nośniku informacji, sprawca podlega karze pozbawienia wolności do lat 3.
§ 3. Kto, dopuszczając się czynu określonego w § 1 lub 2, wyrządza znaczną szkodę majątkową, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.

Wykres nr 4: Liczba niszczonych danych informatycznych[7]



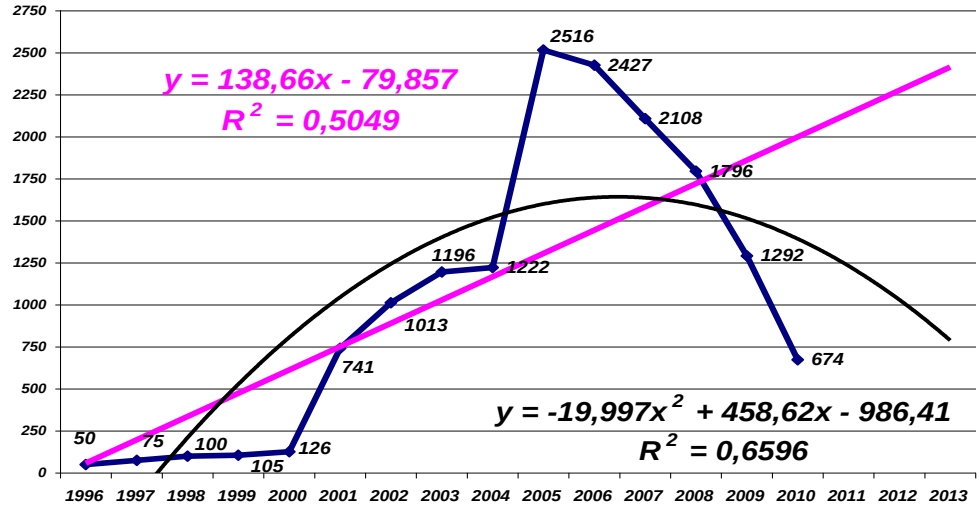
Źródło: Z. Pietras oprac. na podst. danych KGP; *http://www.policja.pl/portal/pol/4/321/Przestepczosc_komputerowa.html*

Dopasowanie liniowej funkcji regresji dla liczby przypadków naruszenia bezpieczeństwa teleinformatycznego w polskim Internecie (wykres nr 5) kształtuje się na średnim poziomie około 66%. Analogiczna sytuacja występuje dla funkcji wielomianowej, która oscyluje na poziomie około 50% wartości współczynnika determinacji liniowej R^2.

Dla liczby przypadków naruszenia bezpieczeństwa teleinformatycznego w polskim Internecie, średnio roczna za analizowany okres wynosi ponad 1 000 (czyli średnio ponad 4 przypadki na dzień roboczy). Chcąc prognozować na najbliższe lata, należałoby uwzględnić zarówno średni roczny przyrost na poziomie 47%, jak również tendencję spadkową od 2005 roku na średnim poziomie około 21%. Biorąc powyższe pod uwagę, można szacować, że liczba przypadków naruszenia bezpieczeństwa teleinformatycznego w polskim Internecie do końca 2013 roku może się wahać w dość znacznym przedziale od około 760 do 2400 przypadków.

[7] Art. 269. § 1. Kto, na komputerowym nośniku informacji, niszczy, uszkadza, usuwa lub zmienia zapis o szczególnym znaczeniu dla obronności kraju, bezpieczeństwa w komunikacji, funkcjonowania administracji rządowej, innego organu państwowego lub administracji samorządowej albo zakłóca lub uniemożliwia automatyczne gromadzenie lub przekazywanie takich informacji, podlega karze pozbawienia wolności od 6 miesięcy do lat 8.
§ 2. Tej samej karze podlega, kto dopuszcza się czynu określonego w § 1, niszcząc albo wymieniając nośnik informacji lub niszcząc albo uszkadzając urządzenie służące automatycznemu przetwarzaniu, gromadzeniu lub przesyłaniu informacji.

Wykres nr 5: Liczba przypadków naruszenia bezpieczeństwa teleinformatycznego w polskim Internecie



Źródło: Z. Pietras oprac. na podst. danych KGP; *http://www.policja.pl/portal/pol/4/321/Przestepczosc_komputerowa.html*

2. Prognoza rozkładu zagrożeń

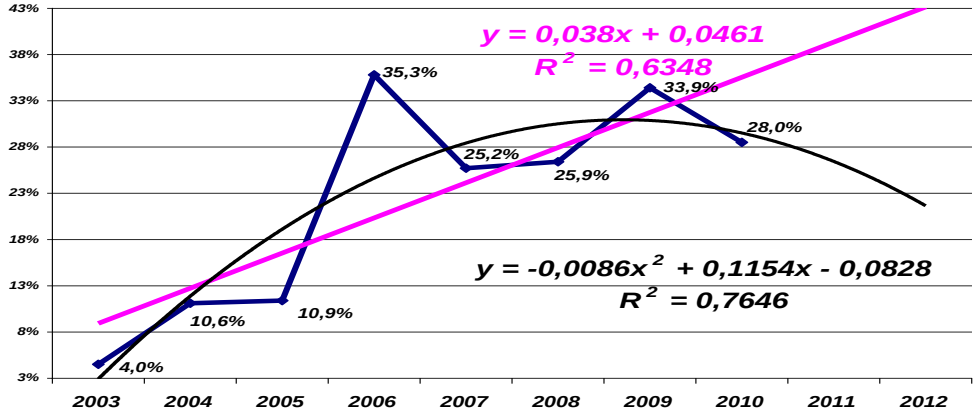
W 2010 roku wysłano 107 trylionów maili[8] (90 trylionów roku 2009), dziennie wysyłano około 294 miliardów maili (247 miliardów w roku 2009) – z tego 262 miliardów maili to spam, czyli 89,1% spośród wszystkich wysłanych maili to spam (w roku 2009 było to 81%) W czasie 1 roku liczba użytkowników kont pocztowych na świecie wzrosła do 1,88 miliarda (1,4 w roku 2009), 2,9 miliarda skrzynek e-mail na koniec roku 2010.

Dopasowanie liniowej funkcji regresji dla rozkładu procentowego SPAM-u (wykres nr 6) kształtuje się na średnim poziomie około 63%, natomiast dla funkcji wielomianowej oscyluje na wysokim poziomie około 76% wartości współczynnika determinacji liniowej R^2.

Dla rozkładu procentowego SPAM-u średnio roczny wzrost za analizowany okres kształtuje się na poziomie około 23%. Biorąc pod uwagę średni roczny przyrost na poziomie 22% można szacować, że % SPAM-u do końca przyszłego roku może się wahać w przedziale od około 23% nawet do około 45%.

[8] *http://ittechblog.pl/2011/01/13/rok-2010-w-liczbach* (pobrano 29.06.2011 r.)

Wykres nr 6: Rozkład procentowy SPAM-u wraz z prognozą



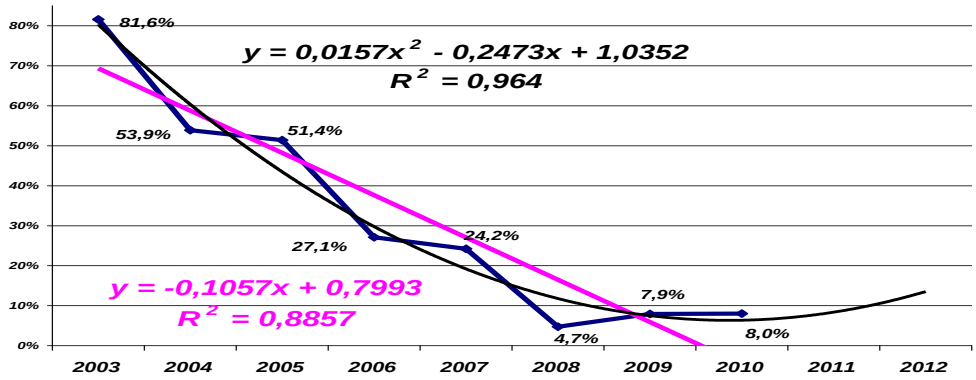
Źródło: Z. Pietras oprac. na podst. Raport CERT Polska 2010, Analiza incydentów naruszających bezpieczeństwo teleinformatyczne, http://www.cert.pl/PDF/Raport_CP_2010.pdf, s. 28

Dosyć pozytywne zjawisko można zaobserwować w przypadku rozkładu procentowego skanowania, gdzie mamy wybitnie tendencję malejącą.

Dopasowanie liniowej funkcji regresji dla rozkładu procentowego skanowania (wykres nr 7) kształtuje się na wysokim poziomie około 89%, natomiast dla funkcji wielomianowej oscyluje na bardzo wysokim poziomie 96% wartości współczynnika determinacji liniowej R^2.

Dla rozkładu procentowego skanowania średnio roczny spadek za analizowany okres kształtował się na poziomie około 32% (r/r). Biorąc to pod uwagę można prognozować, że % skanowania do końca przyszłego roku może się wahać w przedziale do około 10%, przyjmując w tej kategorii zjawisko marginalne.

Wykres nr 7: Rozkład procentowy skanowania wraz z prognozą



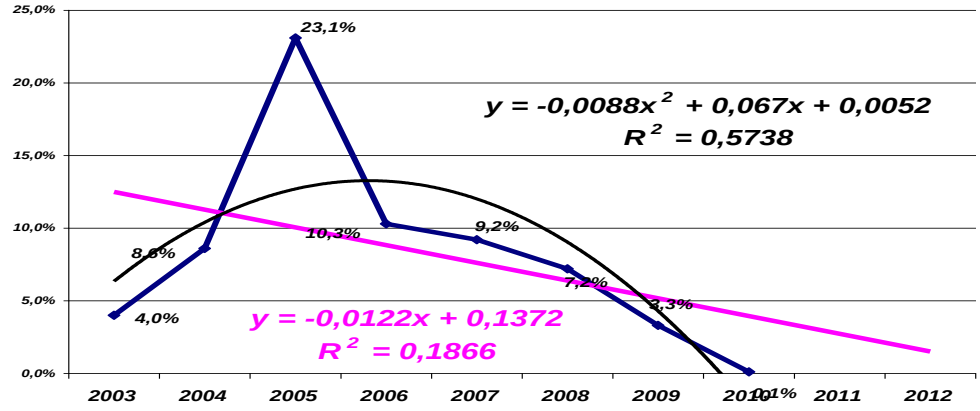
Źródło: Z. Pietras oprac. na podst. Raport CERT Polska 2010, Analiza incydentów naruszających bezpieczeństwo teleinformatyczne, http://www.cert.pl/PDF/Raport_CP_2010.pdf, s. 28

Pozytywne zjawisko zachodzi również w przypadku rozkładu procentowego sklasyfikowanego złośliwego oprogramowania, gdzie mamy również do czynienia z tendencję malejącą.

Dopasowanie liniowej funkcji regresji dla rozkładu procentowego sklasyfikowanego złośliwego oprogramowania (wykres nr 8) kształtuje się na bardzo niskim poziomie około 19%, natomiast dla funkcji wielomianowej oscyluje na średnim poziomie 57% wartości współczynnika determinacji liniowej R^2.

Dla rozkładu procentowego sklasyfikowanego złośliwego oprogramowania średnio roczny spadek za analizowany okres kształtował się na poziomie około 8-9% (r/r). Uwzględniając ten fakt można prognozować, że % sklasyfikowanego złośliwego oprogramowania do końca przyszłego roku może się obniżyć do około 1,5%, przyjmując i w tej kategorii raczej zjawisko marginalne.

Wykres nr 8: Rozkład procentowy sklasyfikowanego złośliwego oprogramowania wraz z prognozą



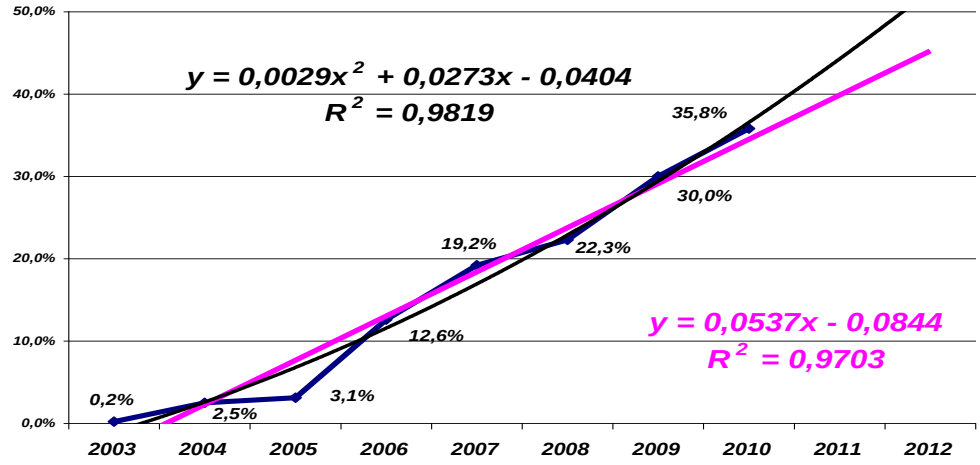
Źródło: Z. Pietras oprac. na podst. Raport CERT Polska 2010, Analiza incydentów naruszających bezpieczeństwo teleinformatyczne, *http://www.cert.pl/PDF/Raport_CP_2010.pdf,* s. 28

Niepokojącym zjawiskiem może się okazać kradzież tożsamości i podszywania się, gdzie od 2003 roku mamy do czynienia z tendencję wzrostową.

Dopasowanie liniowej funkcji regresji dla rozkładu procentowego kradzieży tożsamości i podszywania się (wykres nr 9) kształtuje się na bardzo wysokim poziomie około 97%, natomiast dla funkcji wielomianowej oscyluje również na bardzo wysokim poziomie 98% wartości współczynnika determinacji liniowej R^2.

Dla rozkładu procentowego kradzieży tożsamości i podszywania się, średnio roczny wzrost za analizowany okres kształtował się na poziomie około 16% (r/r), uwzględniając ten fakt można prognozować, że % kradzieży tożsamości i podszywania się do końca przyszłego roku może znacząco wzrosnąć do poziomu około 50%, przyjmując i w tej kategorii raczej zjawisko niebezpieczne.

Wykres nr 9: Rozkład procentowy dla kradzieży tożsamości i podszywania się wraz z prognozą



Źródło: Z. Pietras oprac. na podst. Raport CERT Polska 2010, Analiza incydentów naruszających bezpieczeństwo teleinformatyczne, *http://www.cert.pl/PDF/Raport_CP_2010.pdf*, s. 28

3. Zakończenie i wnioski

Największe niemieckie banki w tajemnicy wymieniły w zeszłym roku, ze względów bezpieczeństwa, co trzeci bankomat. To efekt plagi złodziei kradnących pieniądze z kart kredytowych. W 2010 roku okradli aż 200 tysięcy Niemców.

W świetle przeprowadzonych analiz i ocen można z dużym prawdopodobieństwem stwierdzić, że należy się liczyć z utrzymującą się tendencją:

a) wzrostową w liczbie:
   - oszustw komputerowych;
   - bezprawnie uzyskanych informacji;
   - zniszczeń lub zmiany istotnych informacji;
   - przypadków naruszenia bezpieczeństwa teleinformatycznego w polskim Internecie;

b) malejącą w liczbie:
   - niszczonych danych informatycznych.

Analizując i oceniając rozkład procentowy możemy się liczyć z trendem:

a) wzrostowym w rozkładzie procentowym dla:
   - SPAM- u;
   - dla kradzieży tożsamości i podszywania się;

b) malejącą w rozkładzie procentowym dla:
   a) skanowania;
   b) sklasyfikowanego złośliwego oprogramowania.

Takiego stanu rzeczy z punktu działalności logistycznej możemy upatrywać przede wszystkim:

a) w stawianych sobie celach przez przestępców (nowa kategoria – materializm);
b) w edukacji poznawania nowych technik, sposobów;
c) w starzeniu się sprzętu wykorzystywanego w organizacjach (przedsiębiorstwach, bankach, biurach projektowych laboratoriach, itp. ośrodkach);
d) w szkoleniach i ćwiczeniach w celu utrzymania właściwej wysokiej sprawności;
e) w zwiększającej się liczbie internautów:
   - pod koniec 2000 roku liczba korzystających z Internetu to około 361 mln osób, liczba ludności 6 124 mln osób – średnio co 17 obywatel ziemi miał dostęp do sieci;
   - w grudniu 2008 roku około 1,0 miliard użytkowników powyżej 15 roku życia, liczba ludności 6 707 mln osób – średnio co 6 obywatel ziemi (6,7) miał dostęp do sieci;
   - do końca 2010 roku liczba internautów przekroczyła 2,0 miliardy, liczba ziemian 7 000 mln – średnio co 4 obywatel ziemi (3,5) miał dostęp do sieci;
f) w ciągłych modernizacjach na sieciach (w organizacja produkcyjnych i usługowych dostęp do sieci bez ograniczeń);
g) w braku właściwych rozwiązań legislacyjnych.

Digitalizacja gospodarki, wraz ze wszystkimi możliwościami i korzyściami, niesie jednak ze sobą konieczność zmagania się z dotychczas nieznanymi zagrożeniami. Ich źródło tkwi w specyfice najistotniejszego zasobu, jakim stała się informacja. Z tego powodu organizacje kładą coraz większy nacisk na szeroko rozumiane bezpieczeństwo systemów informatycznych. Najsłabszym ogniwem w łańcuchu zabezpieczeń jest człowiek. Dlatego bardzo ważne dla bezpieczeństwa organizacji jest ustawiczne uświadamianie pracownikom o możliwych zagrożeniach. Przy projektowaniu zabezpieczeń specjaliści ds. bezpieczeństwa stosują trzy zasady zakładające, że o skuteczności zabezpieczeń decyduje najsłabsze ogniwo łańcucha zabezpieczeń, bezpieczeństwo nigdy nie jest pełne, komuś trzeba zaufać. Dlatego zamiast mówić o bezpieczeństwie organizacji, lepiej postawić sobie za cel zmniejszanie ryzyka do minimum. Dbałość o bezpieczeństwo jest procesem ciągłym, nie mającym końca. Nieustannie należy uaktualniać systemy za pomocą najnowszych programów korygujących luki w zabezpieczeniach, szukać słabości środowiska informatycznego oraz wdrażać najlepsze systemy zabezpieczeń. Potrzeba ochrony danych jest nie tylko potrzebą globalną ale wchodzi z zakres potrzeb rozumianych jako podstawowe potrzeby, w tym wypadku bezpieczeństwa, będące w piramidzie potrzeb A. Maslowa koniecznymi do prawidłowej egzystencji człowieka.

Streszczenie

Każdego dnia i prawie na każdym kroku napotykamy komputery. Te, wykorzystywane do pracy w dużych sieciach korporacyjnych, jak i te do użytku domowego. Wszystkie komputery są narażone na wiele różnych zagrożeń. Każdego dnia dowiadujemy się o nowych przypadkach nieodpowiedzialnego podejścia do systemów ochrony i zaniedbań w ochronie informacji poufnych.

Obecnie prawie każdego dnia możemy przeczytać lub obejrzeć wiadomości na temat katastrofalnych skutków takich zaniedbań. W dzisiejszych czasach, kiedy te systemy są tak ważne w zapewnianiu ciągłości przemysłu, usług, a nawet egzystencji całych grup ludzi, słowo "zagrożenie" jest kluczowe, a ochronie tych systemów powinien być przypisany najwyższy priorytet.

Summary

Every day and almost at every turn we encounter computers. Those, working in the large corporate networks as well as for personal use at home. All computers are exposed to many various threats. Every day we learn of new cases of irresponsible approach to systems security or neglect in protecting confidential information. Now almost every day we can read or watch news about the disastrous results of such negligence. Currently, in time when these systems are so important in ensuring continuity of industry, services, and even the existence of entire groups of people, the word threat is crucial, and the security of these systems should be given highest priority.

Bibliografia

1. Osińska M., (red. nauk.) *Ekonometria współczesna*, Wyd. Dom Organizatora, TNOiK. Toruń 2007
2. Raport CERT Polska 2010, Analiza incydentów naruszających bezpieczeństwo teleinformatyczne, *http://www.cert.pl/PDF/Raport_CP_2010.pdf*
3. Dane KGP