

---

# Czy jest bezpiecznie?

## Bezpieczeństwo systemów komputerowych i danych

Wykład ogólnouniwersytecki

Prof. dr hab. Ireneusz Grabowski

[www.fizyka.umk.pl/~ig](http://www.fizyka.umk.pl/~ig)

Google: Irek Grabowski

## Czym się zajmuję na co dzień?

Rozwojem (wymyślanie, testowanie, obliczenia dla układów rzeczywistych) metod opisujących układy wieloelektronowe – atomy, cząsteczki, białka, układy biologiczne, ciało stałe (układy krystaliczne), ...

- Opis materii na poziomie elektronowym – przewidujemy własności atomów, cząsteczek, ..., enzymów, białek, kryształów, ..., oddziaływanie np. światła z cząsteczkami, ....
- Mechanika kwantowa, Równanie Schrodingera, chemia kwantowa, - Kto wykorzystuje takie metody?: chemicy, biolodzy, fizycy, przemysł chemiczny, farmaceutyczny, nanotechnologia, ..., wojsko – ekologiczne paliwo dla rakiet balistycznych !!!

## Informatyka stosowana

- Bezpieczeństwo danych elektronicznych (także sieci LAN i Internet)
- Tworzenie i wdrażanie oprogramowania.
- Metody numeryczne
- Administracja systemami sieciowymi

$$V'_{Dco}(\mathbf{r}) = \sum_{pq} \left\{ \sum_{ijab} \frac{2(ia|jb) - (aj|bi)}{\varepsilon_i + \varepsilon_j - \varepsilon_a - \varepsilon_b} \left[ 2 \sum_c \frac{(ca|jb)}{\varepsilon_i - \varepsilon_c} (ic|q) \right. \right. \\ \left. \left. + 2 \sum_k \frac{(ik|jb)}{\varepsilon_a - \varepsilon_k} (ka|q) \right] \right\} (\mathbf{X}_{so}^{-1})_{pq} g_p(\mathbf{r}). \quad (22)$$

$$V''_{Dco}(\mathbf{r}) = \sum_{pq} \left\{ \sum_{ijab} \frac{2(ia|jb) - (aj|bi)}{\varepsilon_i + \varepsilon_j - \varepsilon_a - \varepsilon_b} \left[ 2 \sum_{l \neq i} \frac{(la|jb)}{\varepsilon_i - \varepsilon_l} (il|q) + 2 \sum_{d \neq a} \frac{(id|jb)}{\varepsilon_a - \varepsilon_d} (da|q) \right. \right. \\ \left. \left. - \frac{1}{2\varepsilon_i + \varepsilon_j - \varepsilon_a - \varepsilon_b} ((ii|q) + (jj|q) - (aa|q) - (bb|q)) \right] \right\} (\mathbf{X}_{so}^{-1})_{pq} g_p(\mathbf{r}) \quad (23)$$

$$V'_{Sc\sigma}(\mathbf{r}) = \sum_{pq} \left\{ \sum_{ia} \frac{f_{ia}}{\varepsilon_i - \varepsilon_a} \left[ 2 \sum_c \frac{(ci|q)}{\varepsilon_i - \varepsilon_c} f_{ca} + 2 \sum_k \frac{(ka|q)}{\varepsilon_a - \varepsilon_k} \right. \right. \\ \left. \left. + 2 \sum_{kc} \frac{(ck|q)}{\varepsilon_k - \varepsilon_c} (4(ia|ck) - (ic|ka) - (ik|ca)) \right] \right\} (\mathbf{X}_{so}^{-1})_{pq} g_p(\mathbf{r})$$

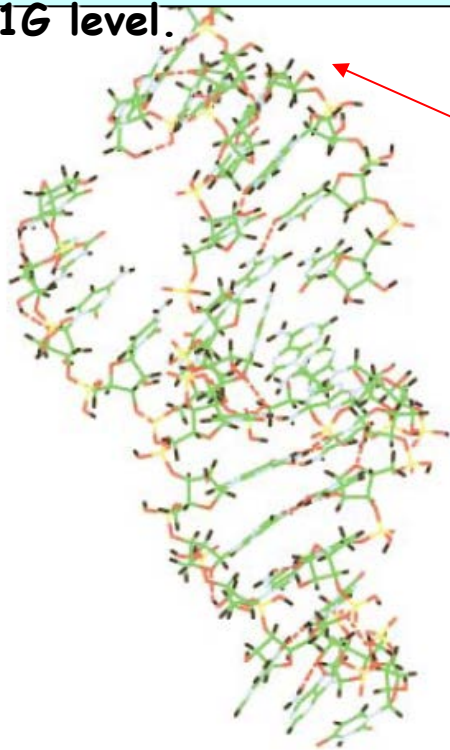
$$\langle 0 | \{ \hat{i}^{\dagger} \hat{j}^{\dagger} \hat{b} \hat{a} \} \{ \hat{p}^{\dagger} \hat{q} \} \{ \hat{c}^{\dagger} \hat{d}^{\dagger} \hat{l} \hat{k} \} | 0 \rangle = \quad (3.18)$$

$$= \langle 0 | \{ \hat{i}^{\dagger} \hat{j}^{\dagger} \hat{b} \hat{a} \} \{ \hat{p}^{\dagger} \hat{q} \} \{ \hat{c}^{\dagger} \hat{d}^{\dagger} \hat{l} \hat{k} \} + \{ \hat{i}^{\dagger} \hat{j}^{\dagger} \hat{b} \hat{a} \} \{ \hat{p}^{\dagger} \hat{q} \} \{ \hat{c}^{\dagger} \hat{d}^{\dagger} \hat{l} \hat{k} \} + \{ \hat{i}^{\dagger} \hat{j}^{\dagger} \hat{b} \hat{a} \} \{ \hat{p}^{\dagger} \hat{q} \} \{ \hat{c}^{\dagger} \hat{d}^{\dagger} \hat{l} \hat{k} \} + \\ + \{ \hat{i}^{\dagger} \hat{j}^{\dagger} \hat{b} \hat{a} \} \{ \hat{p}^{\dagger} \hat{q} \} \{ \hat{c}^{\dagger} \hat{d}^{\dagger} \hat{l} \hat{k} \} + \{ \hat{i}^{\dagger} \hat{j}^{\dagger} \hat{b} \hat{a} \} \{ \hat{p}^{\dagger} \hat{q} \} \{ \hat{c}^{\dagger} \hat{d}^{\dagger} \hat{l} \hat{k} \} + \{ \hat{i}^{\dagger} \hat{j}^{\dagger} \hat{b} \hat{a} \} \{ \hat{p}^{\dagger} \hat{q} \} \{ \hat{c}^{\dagger} \hat{d}^{\dagger} \hat{l} \hat{k} \} + \\ + \{ \hat{i}^{\dagger} \hat{j}^{\dagger} \hat{b} \hat{a} \} \{ \hat{p}^{\dagger} \hat{q} \} \{ \hat{c}^{\dagger} \hat{d}^{\dagger} \hat{l} \hat{k} \} + \{ \hat{i}^{\dagger} \hat{j}^{\dagger} \hat{b} \hat{a} \} \{ \hat{p}^{\dagger} \hat{q} \} \{ \hat{c}^{\dagger} \hat{d}^{\dagger} \hat{l} \hat{k} \} + \{ \hat{i}^{\dagger} \hat{j}^{\dagger} \hat{b} \hat{a} \} \{ \hat{p}^{\dagger} \hat{q} \} \{ \hat{c}^{\dagger} \hat{d}^{\dagger} \hat{l} \hat{k} \} + \\ + \{ \hat{i}^{\dagger} \hat{j}^{\dagger} \hat{b} \hat{a} \} \{ \hat{p}^{\dagger} \hat{q} \} \{ \hat{c}^{\dagger} \hat{d}^{\dagger} \hat{l} \hat{k} \} + \{ \hat{i}^{\dagger} \hat{j}^{\dagger} \hat{b} \hat{a} \} \{ \hat{p}^{\dagger} \hat{q} \} \{ \hat{c}^{\dagger} \hat{d}^{\dagger} \hat{l} \hat{k} \} + \{ \hat{i}^{\dagger} \hat{j}^{\dagger} \hat{b} \hat{a} \} \{ \hat{p}^{\dagger} \hat{q} \} \{ \hat{c}^{\dagger} \hat{d}^{\dagger} \hat{l} \hat{k} \} + \\ + \{ \hat{i}^{\dagger} \hat{j}^{\dagger} \hat{b} \hat{a} \} \{ \hat{p}^{\dagger} \hat{q} \} \{ \hat{c}^{\dagger} \hat{d}^{\dagger} \hat{l} \hat{k} \} | 0 \rangle =$$

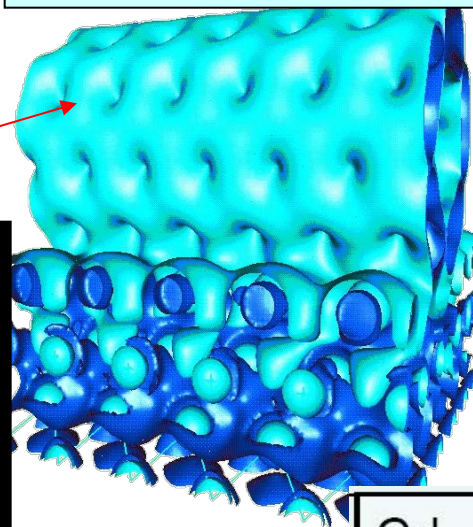
$$= \langle 0 | [ \delta_{iq} \delta_{jl} \delta_{bc} \delta_{ad} \delta_{pk} - \delta_{iq} \delta_{jl} \delta_{ac} \delta_{bd} \delta_{pk} - \delta_{iq} \delta_{jk} \delta_{bc} \delta_{ad} \delta_{pl} + \delta_{iq} \delta_{jk} \delta_{bd} \delta_{ac} \delta_{pl} + \\ + \delta_{il} \delta_{jq} \delta_{bd} \delta_{ac} \delta_{pk} - \delta_{il} \delta_{jq} \delta_{bc} \delta_{ad} \delta_{pk} - \delta_{ik} \delta_{jq} \delta_{bd} \delta_{ac} \delta_{pl} + \delta_{ik} \delta_{jq} \delta_{bc} \delta_{ad} \delta_{pl} - \\ - \delta_{ik} \delta_{jl} \delta_{bp} \delta_{ad} \delta_{qc} + \delta_{ik} \delta_{jl} \delta_{bd} \delta_{ap} \delta_{qc} - \delta_{il} \delta_{jk} \delta_{bd} \delta_{ap} \delta_{qc} + \delta_{il} \delta_{jk} \delta_{bp} \delta_{ad} \delta_{qc} - \\ - \delta_{ik} \delta_{jl} \delta_{bc} \delta_{ap} \delta_{qd} + \delta_{ik} \delta_{jl} \delta_{bc} \delta_{ap} \delta_{qd} + \delta_{ik} \delta_{jl} \delta_{bp} \delta_{ac} \delta_{qd} - \delta_{il} \delta_{jk} \delta_{bp} \delta_{ac} \delta_{qd} ] | 0 \rangle \quad (3.19)$$

$$H \cdot \psi = E \cdot \psi$$

•1026 atom fragment of RNA, calculated using linear scaling DFT at the LSDA/3-21G level.



•Total electron density  $n(r)$  for a carbon nanotube on an Aluminum slab from an LDA simulation



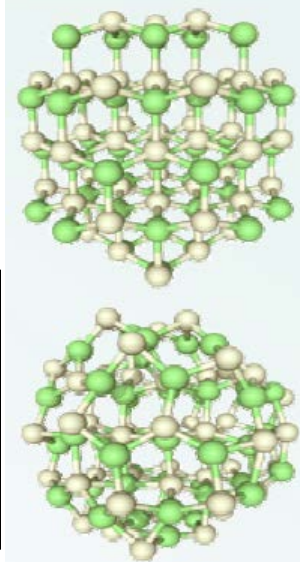
•Gaussian  
•NwChem  
•Gamess  
•Crystal  
•Wien2K  
•Amber  
•Q-Chem  
•VASP

BLYP  
LDA  
B3LYP

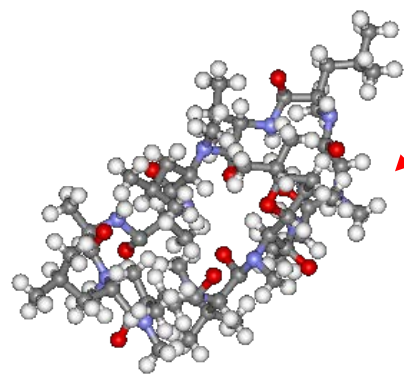
6-31G\*  
augcc-PVDZ

x1000 procesorów

Cd<sub>45</sub>Se<sub>45</sub>  
1.5 nm



•Cyclosporin (DFT B3LYP):  
•Basis: 6-31G\*



•Accurate DFT calculations are required to accurately predict the electronic structure of CdSe quantum dots. (LDA, PBE)



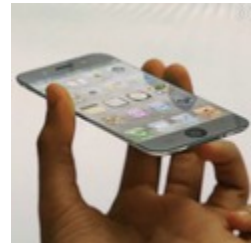
# Superkomputery w fizyce i życiu codziennym

[www.top500.org](http://www.top500.org)



## Porównanie mocy obliczeniowych komputerów

- Tianhe-2 (MilkyWay-2) 54,3 PFLOPS
- Titan - Cray XK7 – 27 PFLOPS
- Sequoia - 16,32 PFLOPS
- K computer -10,51 PFLOPS
- Zeus z ACK Cyfronet na AGH -185 TFLOPS
- IF UMK – 2 TFLOPS
- IPad 2 - 1,6 Gflops
- Core i7 965 XE to 70 Gflops



zajęcia dla każdego – bardziej popularne niż naukowe  
tematyka i problemy znane a wręcz oczywiste

Spróbujmy jak najszerzej spojrzeć na tematykę: teraz jesteś  
użytkownikiem, jutro pracownikiem a wkrótce „szefem”

Teraz jesteś dzieckiem a niedługo rodzicem

Wykład nieobowiązkowy (ok. 20 godzin spotkań)

Jeśli się uda, to wymiana zdań i konwersatorium

Prezentacja pełni funkcje pomocniczą





## Plan

1. Ogólne informacje dotyczące problematyki bezpieczeństwa danych elektronicznych i systemów komputerowych
2. Rola i znaczenie informacji oraz systemów komputerowych we współczesnym świecie w kontekście bezpieczeństwa.
3. Waga i wartość danych elektronicznych w różnych aspektach i wymiarach (życie prywatne, działalność instytucji, firm, administracji ...)
4. Klasyfikacja zagrożeń.
5. Najważniejsze zagrożenia danych elektronicznych i podstawowe metody ochrony przed tymi zagrożeniami
6. Organizacja zabezpieczeń, polityka bezpieczeństwa w domu, firmie, instytucji.
7. Backup i archiwizacja – porównanie efektywności i jakości różnych metod, usług, urządzeń oraz narzędzi.

## Plan cd

8. Bezpieczeństwo w Internecie i na poziomie usług sieciowych
9. Bezpieczeństwo systemów operacyjnych i aplikacji użytkowych (od smartfona i smartTV do serwera)
10. Rola użytkownika i administratora w zakresie bezpieczeństwa systemu
11. Analiza i audyt bezpieczeństwa danych elektronicznych.
12. Elementy kryptografii, zagadnienia dotyczące podpisu elektronicznego i infrastruktury klucza publicznego i ich zastosowania w praktyce.
13. Ochrona danych osobowych, prywatności i tożsamości w systemach komputerowych i Internecie.



- **Internet** i prasa
- W. Stallings, Network Security Essentials. Prentice Hall, 2003
- J. Stokłosa, T. Bliski, T. Pankowski, Bezpieczeństwo danych w systemach informatycznych. PWN, 2001
- N. Ferguson, B. Schneier, Kryptografia w praktyce., Helion, 2004
- S. Garfinkel, G. Spafford, Bezpieczeństwo w Unixie i Internecie. Wyd. RM, 1997
- W. R. Cheswick. Firewalle i bezpieczeństwo w sieci. Helion, 2003
- W. Stallings - Kryptografia i bezpieczeństwo sieci komputerowych. Koncepcje i metody bezpiecznej komunikacji , Helion, 2012.
- C. Easttom - Computer Security Fundamentals, 2nd ed, Pearson, 2012.
- J. Erickson – Hacking. Sztuka penetracji, wyd. II, Helion, 2008.
- W. Stallings - Kryptografia i bezpieczeństwo sieci komputerowych. Matematyka szyfrów i techniki kryptologii , Helion, 2011.
- W. Stallings, L. Brown – Computer Security. Principles and Practice, Pearson, 2009.

## Literatura (cz. 2)

- M. Rash – Bezpieczeństwo sieci w Linuksie, Helion, 2008.
- W. Stallings, L. Brown – Computer Security. Principles and Practice, 2nd ed., Pearson, 2012.
- E. Nemeth, G. Snyder, T. R. Hein, B. Whaley, T. Morreale, N. McClain, R. Jachim, D. Schweikert, T. Oetiker - Unix i Linux.
- Przewodnik administratora systemów , Helion, 2011.
- W. Stallings – Cryptography and Network Security. Principles and Practice, 5th ed., Pearson, 2011.
- M. T. Goodrich, R. Tamassia – Introduction to Computer Security, Pearson, 2011.
- W. Stallings – Computer Organization and Architecture. Designing for Performance, 8th ed., Pearson, 2010.
- R. Trost – Practical Intrusion Analysis. Prevention and Detection for the Twenty-First Century, Addison-Wesley, 2009.
- M. Grajek, L. Gralewski – Narodziny kryptografii matematycznej, WN Semper, Warszawa, 2009.
- D. Stinson, Kryptografia w teorii i praktyce, WNT 2005.

## Literatura (cz. 3)

- D. A. Wheeler - Secure Programming for Linux and Unix HOWTO, Linux Documentation Project, 2003.
- A. S. Tanenbaum – Systemy operacyjne, Helion, 2010.
- A. Silberschatz, P.B. Galvin, G. Gagne – Podstawy systemów operacyjnych, WNT, 2005, 2006 (tł. 6th ed.).
- W. Stallings – Systemy operacyjne, Robomatic, 2004; PWN, 2006 (tł. 5th ed.).
- W. Stallings – Network Security Essentials. Applications and Standards, 4th ed., Pearson, 2011.
- E. Çayırıcı, C. Rong – Security in Wireless Ad Hoc and Sensor Networks, Wiley, 2009.
- A. Belapurkar et al. – Distributed Systems Security. Issues, Processes and Solutions, Wiley, 2009.
- N. Dhanjani et al. – Hacking. The Next Generation, O'Reilly, 2009.

## Zaliczenie przedmiotu:

- Wykonane 2-3 praktyczne prace domowe
- Egzamin pisemny z zagadnień poruszanych na wykładzie

## Wkład do oceny:

- Prace domowe 40%
- Egzamin 60%

## Kryteria zaliczenia:

- 50%-59% ocena dostateczna
- 60%-69% dostateczny plus
- 70%-79% dobry
- 80%-85% dobry plus
- 86%-100% bardzo dobry



Zapewnienie bezpieczeństwa systemów komputerowych to ogół działań mających na celu zabezpieczać dane przechowywane w komputerze, tak by nie mogły zostać wykorzystane przez niepowołane osoby czy też narażone na trwałą lub nawet tymczasową utratę.

- Skala problemu.
- Możliwe sytuacje awaryjne.
- Zapobieganie.
- Akcja Ratunkowa.
- Organizacja zabezpieczeń.

Na wykładzie szeroko spojrzymy na różne aspekty bezpieczeństwa danych elektronicznych

## Problem? Czy warto tracić czas na taką tematykę?

Najczęściej problemami bezpieczeństwa danych w firmie (także w domu) zaczynamy się interesować dopiero wtedy, gdy odtworzenie owoców długotrwałej pracy ( 1 dzień, 1 miesiąc, 1 rok, ...) staje się kłopotliwe lub wręcz niemożliwe z powodu awarii systemu, lub dane dostały się w niepowołane ręce.

Uświadomienie sobie wagi problemu zanim „coś” się stanie jest podstawowym warunkiem ochrony danych w firmie, ale oczywiście nie jedynym.

Problem dotyczy każdego z nas – od szarego pracownika pracującego przy stanowisku (także w domu), poprzez administratora systemu, projektanta aplikacji, programistę, ..., do kierownictwa firmy.

Najczęściej niewielkim kosztem i nakładem pracy (organizacyjnej), można zminimalizować straty (lub prawdopodobieństwo ich wystąpienia).

Nie ma 100% zabezpieczenia, ale to nie oznacza, że nie ma sensu się zabezpieczać.

## Prasówka

- Według CERT Polska, zespołu reagującego na wszelkie zdarzenia naruszające bezpieczeństwo w sieci, **każdego dnia w Polsce zainfekowanych wirusami zostaje 280 tys. komputerów**. Coraz więcej jest też ataków na systemy rządowe. Zaledwie od 2012 r. do końca 2014 r. ich liczba wzrosła 16-krotnie. Cyberprzestępczość to dziś problem całego świata. Tylko w pierwszym kwartale tego roku firma Kaspersky, producent oprogramowania antywirusowego, zanotowała 2 mld 206 mln szkodliwych ataków na **komputery** i urządzenia mobilne. Z zeszłorocznego raportu "Globalne koszty cyberprzestępczości" przygotowanego przez Center for Strategic and International Studies z Waszyngtonu wynika, że **cyberprzestępczość kosztuje światową gospodarkę niemal 445 mld dol. rocznie**. Osoby prywatne na całym świecie tracą rocznie ok. 160 mld dol. To skutki przede wszystkim **kradzieży danych osobowych i własności intelektualnej**. Ile wynoszą takie straty w Polsce, nie wiadomo. Szacuje się je na kilka miliardów złotych.



## Prasówka

- W Polsce dwóch na trzech internautów pada w sieci ofiarą przestępców, którzy polubili ostatnio urządzenia mobilne - pisze "Puls Biznesu"
- Gazeta powołuje się na przygotowany na zlecenie firmy Symantec raport "Norton Cybercrime Report 2014", z którego wynika, że w ostatnich dwunastu miesiącach w globalnej sieci zostało zaatakowanych ponad pół miliarda osób.

W Polsce ofiarą cyberprzestępczości padło 7,2 miliona internautów. Łączne straty z powodu przestępstw w sieci szacowane są na 110 miliardów dolarów rocznie.

- "Puls Biznesu" dodaje, że przestępcy atakują szybko rozwijające się platformy mobilne i sieci społecznościowe, **których użytkownicy są mniej świadomi zagrożeń. Tymczasem dwóch na trzech użytkowników smartfonów czy tabletów nie stosuje żadnych zabezpieczeń.** Czułości brakuje też na Facebooku czy Twitterze - z danych Symanteca wynika, że w Polsce co dziesiąty użytkownik serwisów społecznościowych zgłasza włamanie do profilu i próbę podszywania się.
- Koń trojański Win32/PSW.Fareit, który w ostatnim tygodniu lutego był wyjątkowo aktywny na terenie Polski to kieszonkowiec - jego głównym zadaniem jest **kradzież loginów i haseł zapisanych w ponad 100 różnych programach, a następnie niezauważone "ulotnienie się" z zainfekowanej maszyny.**

## Prasówka

- Zagrożenie „inteligentnych domów”, smartTV, kamerki internetowe
- GUS szacuje, że około 50% Polaków ma smartphona. To oznacza około ponad 10 milionów telefonów. Czy warto dbać o ich bezpieczeństwo?
- Firma rozsyła po całej Polsce pisma z przedsądowym wezwaniem do zapłaty za rzekome udostępnienie filmu w sieci. Nazwy plików znajdujące się na wezwaniach sugerują, że sprawa dotyczy głównie polskiej pornografii, w tym serii "Podrywaczki", "Masturbowanie", "Polskie uczennice", "Blow-job" i "Autosex". Spółka powołuje się na wyniki "dochodzenia przeprowadzonego przez organy ścigania" i wzywa "do naprawienia szkody". [Pismo zawiera IP komputera, z którego miała zostać wyrządzona szkoda, czyli udostępniony w sieci film,](#)

- W 2015 okazało się, że auta BMW można otworzyć zdalnie. I to bardzo łatwo, **bowiem transmisja danych pomiędzy samochodem a serwerami firmy nie była szyfrowana**. Jeżeli ktoś ją przechwycił, to bardzo szybko mógł podsłuchać do czego służą poszczególne komendy i przejąć kontrolę nad samochodem. Usterka dotyczyła ponad 2 mln pojazdów.
- Włamywacz o pseudonimie "alialbania" pochwalił się swoim przestępstwem w tzw. ciemnej sieci (ang. darknet, czyli internet niewidoczny dla zwykłych użytkowników, który można znaleźć w sieci TOR powstałej, aby zapewnić internautom anonimowość). Stwierdził, że uzyskał dostęp do komputera jednego z pracowników **Getin Noble** Banku i wykradł dzięki temu dane osobowe klientów oraz informacje na temat ich zadłużenia.

Włamywacz twierdzi, że ma dane w sumie 18 tys. dłużników. Jako dowód opublikował listę z informacjami o stu klientach Getin Noble Banku. Złodziej napisał w darknecie, że **uzyskał dostęp do komputera pracownika banku przez zainfekowanie go złośliwym oprogramowaniem**.

Prawdopodobnie zrobił to, wysyłając pracownikowi e-maila z wirusem. To bardzo częsty sposób włamywania się na cudze **komputery** stosowany przez cyberprzestępców. Używają oni do **tego socjotechniki i wykorzystują naiwność oraz niewiedzę pracowników instytucji, do których chcą się włamać**.

- Awaria serwerów LOT, wg opinii badającego sprawę analityka, która właśnie trafiła do prokuratury, wynika, że niezabezpieczone odpowiednio serwery LOT posłużyły hakerowi do tzw. ataku DDoS (Distributed Denial of Service - atak, który wykorzystuje wielką liczbę komputerów, przeciążając i paraliżując atakowany serwer) - na podmiot trzeci. Jaki? To próbuje ustalić prokuratura.

Wg eksperta badającego przyczyny awarii, hakerzy wykorzystali błędną konfigurację zapory sieciowej LOT. Za to zaniedbanie w spółce zostały wyciągnięte konsekwencje personalne.

Jak powiedział "Rzeczpospolitej" ekspert ds. cyberprzestępczości Sebastian Małycha, "skoro cyberprzestępcy mogą rozkazać komputerom LOT wykonanie ataku DDoS, to oznacza, że zostały zainfekowane szkodliwym oprogramowaniem".

S. Małycha mówi też o zagrożeniach tym spowodowanych. - Daje to otwarte drzwi do innych działań, np. dostępu do danych, ich kradzieży, zmiany czy skasowania. Może też być punktem wyjścia do penetracji innych sieci LOT - powiedział ekspert, dodając, że "wówczas zagrożenie byłoby znacznie poważniejsze.

- Od kilku dni sprzedawcy z Allegro dostają maile o rzekomej pomyłce w zamówieniu. Kliknięcie w zawarty w niej link i pobranie pliku może służyć kosztować.

Mail o tytule "Pomyłka w otrzymanym zamówieniu" jest dość szczegółowy i bardzo wiarygodny. Przedsiębiorcy z [Allegro](#) dostają wiadomość, w której ich rzekomy klient skarży się na błąd przy transakcji - pieniądze wpłacił, ale otrzymał nie taki towar, jak chciał. I proponuje sprzedawcy, by ten zwrócił mu pieniądze lub wysłał w ciągu doby prawidłowy towar. I na dowód przesyła link do pliku z potwierdzeniem przelewu.

[Link prowadzi do strony stworzonej przez oszusta](#), na której sprzedawca widzi, że pliku (z dowodem wpłaty) w programie Word nie da się otworzyć ze względu na stare oprogramowanie. Nieświadomy niczego sprzedawca ma jednak wyjście - może ściągnąć aktualizację (przez kliknięcie na stronie opcji "Napraw teraz") na swój komputer i ją zainstalować. To właśnie w tym momencie pada ofiarą zastawionej przez przestępców pułapki. Aktualizacja jest w rzeczywistości wirusem.

- Jak tego uniknąć? Przede wszystkim pod żadnym pozorem nie wolno otwierać linków od nieznanymi maili

Konto e-mail użytkownika

Drogi, Niedawno wykryto nietypowe działania z konta e-mail, więc skrzynka pocztowa została tymczasowo zawieszona przez administratora systemu,

należy odzyskać swoje konto, klikając na poniższy link lub skopiuj do przeglądarki: <http://systemadminforpocztahelpdesk.ezweb123.com/>

W związku z tym, można otrzymać tę wiadomość w folderze spamu, prosimy przejść do skrzynki odbiorczej i kliknąć w link.

Przepraszamy za niedogodności. Systemu Administrator @ 2015. All Rights Reserved.

- Po wywiadzie Tomasza Lisa w "Gazecie Wyborczej", dziennikarz padł ofiarą zmasowanego hejtu internetowych trolli. Tym razem jednak zaatakowano w prawdziwie perfidny sposób nie tylko samego Tomasza Lisa (nazwano go "pedofilem"), ale też jego żonę i córki.

Pojawiły się insynuacje na temat ich rzekomych uzależnień. "Pan Lis niech uważa na swoje córki, bo ludzie plotkują coraz bardziej" - napisała Irena Szafrńska, prawicowa blogerka. Potem było już tylko gorzej. Do nagonki dołączyli kolejni.

- **Z kolei Szafrńska ogłosiła, że padła ofiarą hakerów. "Ktoś włamał się na moje konto zmieniając hasło" - napisała.**



- Hasło do konta mailowego kosztuje około 20 groszy, skan dowodu osobistego - 10 zł. Handel kradzionymi danymi w sieci trwa w najlepsze.

Oczywiście im więcej informacji o danej karcie płatniczej i jej posiadaczu, tym wyższa cena. Najdroższy, pełny pakiet zawiera m.in. numer rachunku bankowego, numer PIN, nazwę użytkownika i hasło oraz imię i nazwisko właściciela rachunku, jego datę urodzenia czy nazwisko panieńskie jego matki. - Przestępca posiadający cyfrowy odpowiednik fizycznej karty może dokonywać zakupów lub pobierać środki aż do momentu, gdy właściciel zorientuje się, że to nie on zlecił dane transakcje i skontaktuje się ze swoim bankiem.

## ILE FIRM W OSTATNICH DWÓCH LATACH PADŁO OFIARĄ CYBERATAKÓW

DANE W PROC.

POLSKA



EUROPA ŚRODKOWO-WSCHODNIA



ŚWIAT



## CYBERPRZESTĘPSTWA W POLSCE W 2015 R.

DANE W PROC.



**37,4**  
Obrażliwe i nielegalne treści



**24,7**  
Ataki DDoS (blokowanie stron)



**4,7**  
Infekcja wirusami



**5**  
Oszustwa (phishing, kradzież tożsamości, udane włamania)



**20,9**  
Próby włamań

### 325 tys. euro

- tyle za pomocą phishingu prawie udało się wyludzić cyberprzestępcy od jednej z pomorskich firm. Policja w ostatniej chwili zablokowała przelew w bank.

© GAZETA WYBORCZA

### 40 mln euro

- na tyle brytyjski teleoperator TalkTalk wycenił straty finansowe po włamaniu hakera, który wykradł dane 156 tys. klientów.

### 276 mln euro

- tyle międzynarodowa grupa cyberprzestępców wykradła rok temu ze stu banków na całym świecie, w tym w Polsce, dzięki atakowi phishingowemu.

ŹRÓDŁO: PwC, CERT ORANGE POLSKA

- Itd..
- Włączyłem komputer i dobre dziesięć sekund patrzyłem z niedowierzaniem, co się tam dzieje, zanim dotarło do mnie, że to hakerski atak - stwierdził [prezydent](#) Republiki Czeskiej Milosz Zeman. Okazuje się, że [hakerzy](#) włamali się do jego komputera i umieścili na twardym dysku zdjęcia z dziecięcą pornografią. "Pravo" pisze, że informatycy z urzędu prezydenckiego ustalili, iż cyberatak wyprowadzono z amerykańskiego stanu Alabama. Zeman uznał, że w tej sytuacji szanse na ściganie hakerów przez czeski wymiar sprawiedliwości są raczej niewielkie.

- Odkryto bardzo poważną dziurę w protokole komunikacji bezprzewodowej Bluetooth, która może dotknąć nawet kilka miliardów urządzeń na całym świecie. W ekstremalnych przypadkach możliwe jest zdalne przejęcie kontroli nad urządzeniem i to bez wiedzy użytkownika.
- Zagrożenie (a w zasadzie zestaw aż 8 podatności) wykryli specjaliści z firmy Armis, nadając im nazwę [BlueBorne](#). Niestety dotyczy ono dość szerokiego spektrum sprzętu - smartfonów z Androidem oraz iOS, notebooków z systemem Windows i Linux, urządzeń typu IoT (Internet of Things - internet rzeczy), telewizorów, a nawet samochodów. Dzięki nim możliwe jest zdalne przejęcie kontroli nad urządzeniem (również przechwycenie transmisji między dwoma urządzeniami komunikującymi się przez Bluetooth) i uruchomienie złośliwego kodu.
- Co więcej, potencjalny napastnik wcale nie musi mieć wcześniej sparowanego sprzętu z urządzeniem ofiary. Wystarczy, że znajduje się ona w zasięgu jego sygnału.

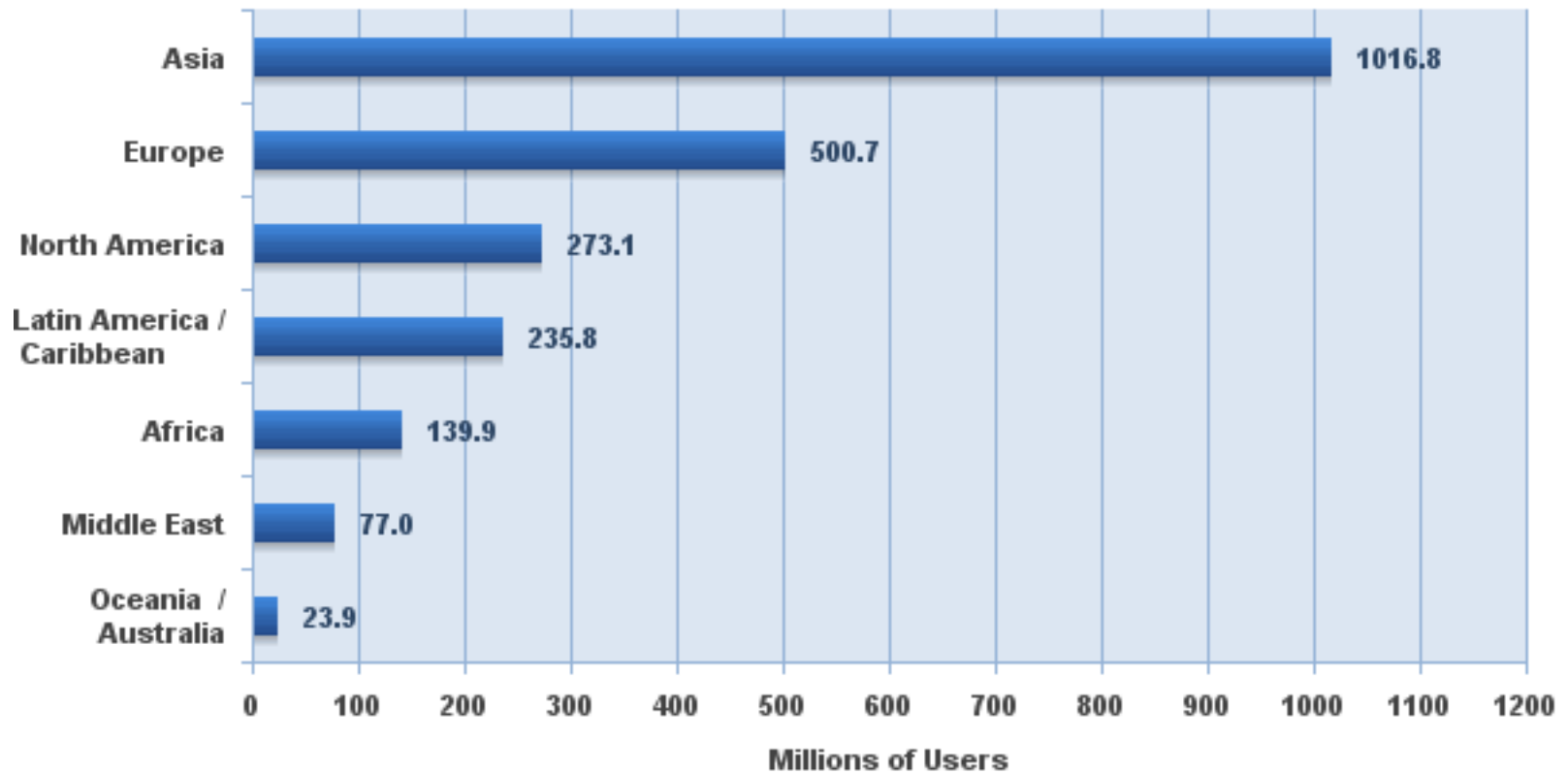
- Na domiar złego hakerzy mogą stworzyć złośliwe oprogramowanie, które samodzielnie będzie się rozprzestrzeniać między zainfekowanymi urządzeniami. [Jak pisze Niebezpiecznik.pl](#) możliwy jest zatem scenariusz, w którym zainfekowana bransoletka fitness zaatakuje inteligentną lodówkę podczas wizyty znajomego u sąsiada, co z kolei spowoduje zagrożenie dla znajdującego się w naszym garażu samochodu.

- Niestety przedstawiciele Armis nie mają dobrych wieści. Duża część z urządzeń, których dotyczy zagrożenie nie dostanie już odpowiedniej aktualizacji usuwającej znalezione luki, bowiem producenci zakończyli okres wsparcia dla nich. Rozesłano już niezbędne informacje do największych koncernów technologicznych (Apple, Google, Microsoft) oraz producentów sprzętu, jednak z szacunków Armis, bez koniecznych aktualizacji pozostanie nawet 40 proc. urządzeń z technologią Bluetooth na pokładzie.

- Co możecie zrobić? Na pewno ograniczyć korzystanie, a nawet wyłączyć Bluetooth na swoim urządzeniu do czasu otrzymania stosownej poprawki. I jak pisze Niebezpiecznik.pl, nie wystarczy jedynie wyłączyć trybu "discoverable". Konieczne będzie całkowite odcięcie transmisji.

- Jak dowiedzieć się, czy wasz sprzęt jest bezpieczny? Specjaliści sugerują pobranie i zainstalowanie stosownej aplikacji sprawdzającej podatność na BlueBorne ([tutaj wersja dla Androida](#)).

## Internet Users in the World by Geographic Regions - 2011



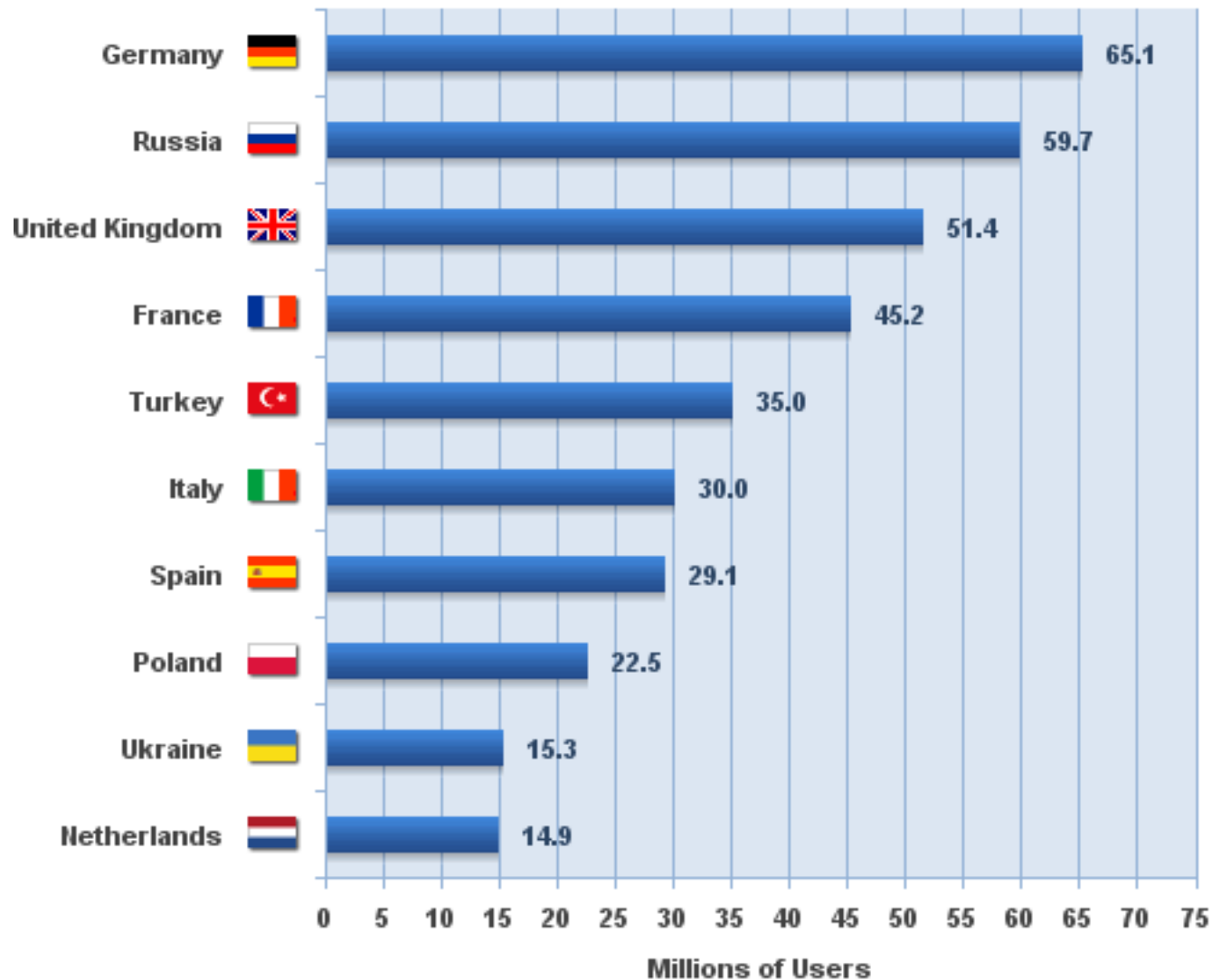
Source: Internet World Stats - [www.internetworldstats.com/stats.htm](http://www.internetworldstats.com/stats.htm)

Estimated Internet users are 2,267,233,742 on December 31, 2011

Copyright © 2012, Miniwatts Marketing Group

# Top 10 Internet Countries in Europe

## March 31, 2011



Source: Internet World Stats - [www.internetworldstats.com/stats4.htm](http://www.internetworldstats.com/stats4.htm)

Basis: 476,213,935 estimated Internet Users in Europe on 2010Q1

Copyright © 2011, Miniwatts Marketing Group



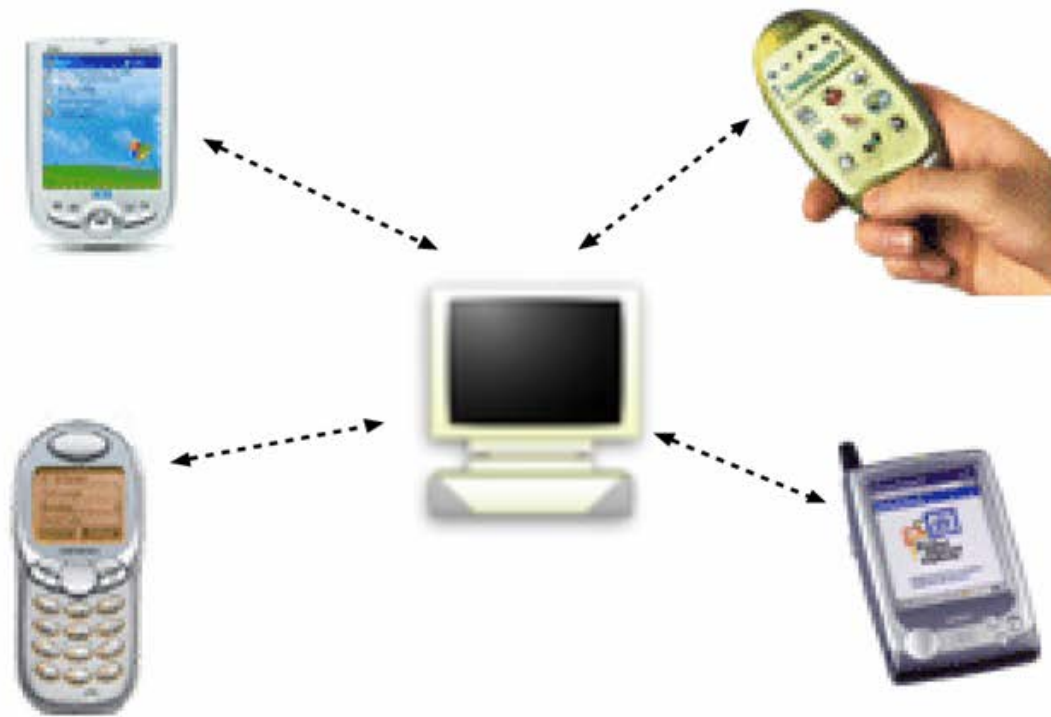
# My także jesteśmy częścią Internetu i sieci!

Sieci komputerowe



E-STUDIA INFORMATYCZNE

## PAN



## Problem? (spojrzenie indywidualne)

Proszę odpowiedzieć **szczerze** na następujące pytania

- Kiedy ostatnio wykonywałem kopię bezpieczeństwa swoich danych (laptop, tel. komórkowy, e-mail, zdjęcia, ...)?
- Kiedy ostatnio uruchamiałem skanowanie komputera (lub sprawdzałem tzw. logi programu antywirusowego)?
- Czy w mojej firmie opracowano i wdrożono politykę bezpieczeństwa danych elektronicznych? (czy np. archiwizowane są bieżące dane, pliki, poczta, ...?, czy monitorowany jest dostęp do Internetu?)
- Czy zwracam uwagę na wskaźniki bezpiecznego połączenia? ( czy wiem co to są te wskaźniki ;- ) ?
- Czy jako administratorowi/programiście zdarza mi się pracować na produkcyjnym systemie?
- Czy zabezpieczyłem „jakoś” swój telefon komórkowy/tablet, ...,
- Czy rozumiem znaczenie jakości , poufności i przechowywania hasła
- .....
- **ZADANIE DOMOWE**

# Bezpieczeństwo informacji

Zgodnie z U.S. National Information Systems Security Glossary:

Bezpieczeństwo systemów informacyjnych (INFOSEC) to ochrona przed nieuprawnionym dostępem do informacji lub jej modyfikacją.

Ochrona powinna obejmować:

- przechowywanie, przetwarzanie, transmisję;
- zabezpieczenie przed
  - odmową usługi (DoS – denial of services) wobec (1) użytkowników upoważnionych (authorized)
  - lub (2) dostarczeniem usługi użytkownikom nieupoważnionym;
- środki umożliwiające wykrycie, dokumentację oraz przeciwdziałanie zagrożeniom.

# Bezpieczeństwo informacji (nie tylko elektronicznej)

Systemy informacyjne to pojęcie daleko szersze niż systemy komputerowe – informacja nie musi być przechowywana w formie elektronicznej.

Ogólnie przyjmuje się, że na bezpieczeństwo informacji składają się 3 elementy – tzw. CIA triad (od angielskich odpowiedników tych pojęć):

- **poufność** (confidentiality) – informacja jest dostępna jedynie dla podmiotów do tego upoważnionych;
- **spójność/integralność** (integrity) – wszelkie nieuprawnione modyfikacje informacji są niedozwolone;
- **dostępność** (availability) – do informacji można uzyskać dostęp w każdych okolicznościach, które są dopuszczone przez politykę bezpieczeństwa informacji.
- Do tej trójki z czasem dołączono także: możliwość rozliczania/**rozliczalność** (accountability), czyli ustalenia odpowiedzialnych za wykonane operacje.

## Czynniki decydujące o znaczeniu bezpieczeństwa

O doniosłości problematyki bezpieczeństwa dla współczesnej cywilizacji decyduje przede wszystkim wszechobecność technik komputerowych.

- Rola systemów informatycznych (szczególnie sieci) dla funkcjonowania współczesnej cywilizacji jest nie do przecenienia; nie ma już praktycznie obszaru działalności człowieka, w którym żadne elementy techniki komputerowej (bądź szerzej mikroprocesorowej) nie byłyby obecne.

**Jesteśmy całkowicie uzależnieni od systemów informatycznych.**

- Globalizacja i wszechobecność oraz wszech-dostępność technologii informatycznych
- trudności związane ze skonstruowaniem i eksploatacją systemu spełniającego wysokie wymagania w zakresie bezpieczeństwa (niedoskonałości technologii, konfiguracji i polityki bezpieczeństwa)
- elementarny konflikt interesów występujący pomiędzy użytecznością systemu a ryzykiem związanym z jego wykorzystaniem i użytkowaniem systemów o podwyższonym bezpieczeństwie.

Systemy informatyczne (szczególnie ZISZ) są dziś niezbędne do prawidłowego funkcjonowania przedsiębiorstwa. Często zależy od nich realizacja zadań biznesowych. Dla banków, biur maklerskich, linii lotniczych i kolejowych oraz wielu innych podmiotów zakłócenia w pracy systemów IT oznaczają wymierną stratę.

Problematyka bezpieczeństwa w systemach informatycznych należy do priorytetowych zagadnień związanych z funkcjonowaniem przedsiębiorstwa.

Bezpieczeństwa nie można kupić jako produktu. Bezpieczeństwo to stan, który uzyskuje się dzięki zastosowaniu środków fizycznych (np. sejfy, kamery), technicznych (np. Firewall, IDS (intrusion detection system)), organizacyjnych (np. procedury i kontrola) oraz prawnych (np. ubezpieczenie).

## Szerokie spojrzenie

- Bezpieczeństwo danych firmowych
- Bezpieczeństwo danych osobowych
- **Nasza prywatność**, tożsamość, wizerunek
- Bezpieczeństwo naszych dzieci
- Bezpieczeństwo naszych pieniędzy (ciągle brak intuicji)
- Nasza kariera i przyszłość (kto „na prezydenta”?)
- Dostępność do danych, usług, ....
- Niezawodność
- ...

## Co tracimy?

### Co tracimy?

- Wprowadzone dane (często bez szansy odtworzenia □)
- Bezpośrednie straty finansowe.
- Czas swój i pracowników.
- Ujawnienie ważnych, strategicznych danych.
- Prywatność.
- wizerunek
- Dezorganizacja pracy.
- Zaufanie.
- CZAS
- ...



### Dane

Niemal 70 procent dokumentów, jakie powstają obecnie w firmach lub są tworzone przez użytkowników prywatnych w Polsce i na świecie, ma postać cyfrową.

Niemal 90 procent z nich nigdy nie zostanie jednak wydrukowanych i pozostaną one jedynie w pamięci naszych dysków komputerowych, kart pamięci i innych nośników, których nowsze wersje pojawiają się każdego roku na rynku.

# Ogólne problemy konstrukcji zabezpieczeń

## Nie istnieje absolutne bezpieczeństwo.

Szybki rozwój technologii informatycznych implikuje powstawanie coraz to nowych zagrożeń.

Czas reakcji na nie nigdy nie jest zerowy i w związku z tym nawet dla najlepiej opracowanego systemu zabezpieczeń istnieje ryzyko powstania okresu dezaktualizacji zastosowanych mechanizmów bezpieczeństwa.

Ludzka słabość, w szczególności omylność projektantów, programistów, użytkowników systemów informatycznych, skutkująca błędami w oprogramowaniu systemowym i aplikacyjnym oraz niewłaściwym lub **niefrasobliwym** jego wykorzystaniu.

## Ogólne problemy konstrukcji zabezpieczeń

Napastnik na ogół nie pokonuje zabezpieczeń, tylko je obchodzi.

Przeprowadzenie skutecznego ataku na jakikolwiek aktywny mechanizm zabezpieczeń jest czasochłonne i stosowane tylko w ostateczności.

Zwykle mniej kosztowne i szybsze jest znalezienie luki w środowisku systemu informatycznego, zabezpieczanego owym mechanizmem niż łamanie jego samego, która to luka pozwoli skutecznie wtargnąć do systemu niejako „z boku” zabezpieczeń.

większość ataków przeprowadzanych na systemy informatyczne realizowana jest „od środka”, czyli przez zaufanych, poniekąd, użytkowników systemu, którzy znając system jakim się posługują niewątpliwie łatwiej mogą znaleźć i wykorzystać luki bezpieczeństwa.

## Ogólne problemy konstrukcji zabezpieczeń

**Nie należy pokładać zaufania w jednej linii obrony.**

Obejście aktywnego mechanizmu zabezpieczeń często bywa możliwe i może istotnie narażać bezpieczeństwo całego systemu.

W związku z tym, naturalną konsekwencją tego jest konstruowanie wielopoziomowych zabezpieczeń poprzez budowanie kolejnych swoistych „linii obrony”, z których każda po przejściu poprzedniej stanowić będzie, przynajmniej potencjalnie, kolejną zaporę dla atakującego.

**Złożoność jest najgorszym wrogiem bezpieczeństwa.**

Skomplikowane systemy są trudne do opanowania, również pod względem bezpieczeństwa.

Istotnym usprawnieniem zarządzania systemem jest jego modułarna konstrukcja, dająca szansę na zwiększenie kontroli nad konfiguracją i funkcjonowaniem systemu.

## Ogólne problemy konstrukcji zabezpieczeń

**System dopóty nie jest bezpieczny, dopóki nie ma pewności że jest.**

Bardzo łatwo popełnić błąd zakładając zupełnie inaczej - dopóki brakuje odnotowanych symptomów, iż bezpieczeństwo systemu zostało naruszone, możemy spać spokojnie.

Zaobserwowanie ataku nie jest trywialne nawet w systemie poprawnie monitorowanym.

Ponadto symptomy ataku zwykle występują dopiero po jego zakończeniu, kiedy to może być zbyt późno by przeprowadzać akcję ratunkową, kiedy ucierpiały już newralgiczne składniki systemu, poufne dane lub reputacja firmy.

**Wzrost poziomu bezpieczeństwa odbywa się kosztem wygody.**

Użytkownicy systemu pragną przede wszystkim efektywności i wygody swojej pracy.

# Filary bezpieczeństwa systemów komputerowych

- **Poufność** - Zespół wszystkich działań mających na celu zapobieganiu by informacja zastrzeżona nie dostała się w niepowołane ręce
- **Integralność** - Mechanizm, gwarantujący, że kluczowe dane nie zostaną zmodyfikowane przez nieautoryzowanego użytkownika
- **Dostępność** - Nieprzerwany dostęp do zasobów lub informacji opartym na autoryzowanym dostępie do tychże danych
- **Niezawodność** - Pewność, że system będzie działał stabilnie w oczekiwany przez użytkowników sposób,
- **Autentyczność** - Weryfikacja tożsamości i autentyczności zasobów

Bezpieczeństwo jest elementem szerszego kontekstu, nazywanego wiarygodnością systemu komputerowego. W kontekście tym wyróżnia się w sumie cztery atrybuty wiarygodności:

System wiarygodny =

- dyspozycyjny (available) = dostępny na bieżąco
- niezawodny (reliable) = odporny na awarie
- bezpieczny (secure) = zapewniający ochronę danych
- bezpieczny (safe) = bezpieczny dla otoczenia, przyjazny dla środowiska

# Strategie ochrony

Istnieją dwie wiodące strategie ochrony systemów informatycznych. Pierwsza, tradycyjna strategia opiera się na analizie ryzyka.

**Analiza ryzyka** identyfikuje obszary systemu informatycznego, gdzie wymagane jest wprowadzenia zabezpieczeń. Przy czym zabezpieczenia powinny być zastosowane w pierwszej kolejności do ochrony zasobów stanowiących największą wartość (zwykle dane) oraz tych zasobów, dla których istnieje duże zagrożenie i które są na to zagrożenie podatne.

Druga strategia ma charakter bardziej praktyczny. Wychodzi ona z założenia, że **nadużycia bezpieczeństwa** w systemach informatycznych są **nieuniknione** (np. ataki wirusów, włamania) i należy odpowiednio przygotować się do ich obsługi.

Zarówno analiza ryzyka jak i nieunikniona utrata bezpieczeństwa, powinny być przedmiotem rozważań przy ustalaniu polityki bezpieczeństwa przedsiębiorstwa.



## Strategia bezpieczeństwa

Opracowanie skutecznych zabezpieczeń jest problemem bardzo złożonym. Wymaga uwagi i systematyczności na każdym etapie.

Decydujące znaczenia ma etap projektowy, na którym popełnione błędy mogą być nienaprawialne w kolejnych etapach.

Etap projektowy powinien rozpocząć się od wypracowania strategii firmy dotyczącej bezpieczeństwa (i to nie wyłącznie systemu informatycznego). Polega to w ogólnym schemacie na odpowiedzi na następujące pytania:

# Co chronić?" (określenie zasobów)

# „Przed czym chronić?" (identyfikacja zagrożeń)

# „Ile czasu, wysiłku i pieniędzy można poświęcić na należną ochronę"  
(oszacowanie ryzyka, analiza kosztów i zysku)

## Określenie zasobów = „Co chronić?”

- sprzęt komputerowy
- infrastruktura sieciowa
- wydruki
- strategiczne dane
- kopie zapasowe
- wersje instalacyjne oprogramowania
- dane osobowe
- dane audytu
- zdrowie pracowników
- prywatność pracowników
- zdolności produkcyjne
- wizerunek publiczny i reputacja

## Identyfikacja zagrożeń = „Przed czym chronić?”

- włamywacze komputerowi
- infekcje wirusami i innym złośliwym oprogramowaniem
- awarie sprzętu
- destruktywność pracowników / personelu zewnętrznego
- błędy w programach
- kradzież dysków / laptopów (również w podróży służbowej)
- .....
- utrata możliwości korzystania z łączy telekomunikacyjnych
- bankructwo firmy serwisowej / producenta sprzętu
- ....
- choroba administratora / kierownika (jednoczesna choroba wielu osób)
- klęski żywiołowe
- ....

## Polityka bezpieczeństwa

U podstaw działania każdej firmy powinna leżeć spójna i co ważniejsze przestrzegana przez wszystkich pracowników polityka bezpieczeństwa danych.

Polityka bezpieczeństwa powinna być respektowana bezwzględnie przez pracowników wszystkich szczebli, zarówno pracowników szeregowych jak i kierownictwo, bowiem od każdego pracownika bez wyjątku zależy bezpieczeństwo firmy.

Polityka bezpieczeństwa wiąże się przede wszystkim z określeniem obszarów zagrożenia i ustaleniem zasad działania w razie jego wystąpienia.

# Polityka bezpieczeństwa

Do podstawowych elementów polityki bezpieczeństwa zaliczamy:

- Zabezpieczenia lokalizacyjne,
- Zabezpieczenie sprzętowe (serwer i stacje robocze),
- Zabezpieczenia programowe,
- Analiza architektury sieci lokalnej,
- Archiwizacja danych,
- Kontrola dostępu do systemu (system haseł i praw),
- Szkolenia użytkowników systemu.
- ....

## Polityka bezpieczeństwa

Polityka bezpieczeństwa stanowi element polityki biznesowej firmy.

Jest to często (powinien być) formalny dokument opisujący strategię bezpieczeństwa. Jej realizacja podlega następującym etapom:

1. zaprojektowanie
2. zaimplementowanie
3. zarządzanie (w tym monitorowanie i okresowe audyty bezpieczeństwa)

Szczególnie godnym podkreślenia jest etap 3. odzwierciedlający ciągłą ewolucję jaką przechodzą działalność firmy, środowisko rynkowe jej funkcjonowania, zagrożenia i technologie obrony.

Wymaga to ciągłego "trzymania ręki na pulsie".

# Polityka bezpieczeństwa

Zakres tematyczny jaki powinna obejmować polityka bezpieczeństwa to:

- \* definicja celu i misji polityki bezpieczeństwa
- \* standardy i wytyczne których przestrzegania wymagamy
- \* kluczowe zadania do wykonania
- \* zakresy odpowiedzialności

## Specyfikacja środków

Polityka bezpieczeństwa winna definiować środki jej realizacji obejmujące takie elementy jak:

- \* ochrona fizyczna
- \* polityka proceduralno-kadrowa (odpowiedzialność personalna)
- \* mechanizmy techniczne

## Normy i zalecenia zarządzania bezpieczeństwem

Istnieje wiele dokumentacji poświęconej realizacji polityki bezpieczeństwa, w tym również norm i standardów międzynarodowych, którymi należy posłużyć się przy opracowywaniu **własnej (firmowej) polityki bezpieczeństwa**.

Kanonem jest norma ISO/IEC Technical Report 13335 (ratyfikowana w naszym kraju jako PN-I-13335). Norma ta jest dokumentem wieloczęściowym obejmującym następujące zagadnienia:

- TR 13335-1 terminologia i modele
- TR 13335-2 metodyka planowania i prowadzenia analizy ryzyka, specyfikacja wymagań stanowisk pracy związanych z bezpieczeństwem systemów informatycznych
- TR 13335-3 techniki zarządzania bezpieczeństwem
  - ✓ zarządzanie ochroną informacji
  - ✓ zarządzanie konfiguracją systemów IT
  - ✓ zarządzanie zmianami
- TR 13335-4 metodyka doboru zabezpieczeń
- WD 13335-5 zabezpieczanie połączeń z sieciami zewnętrznymi



Przed czym chronić?

Im większa świadomość grożących nam niebezpieczeństw, tym skuteczniej możemy się zabezpieczać.

## Różne rodzaje ataków komputerowych

- Obrażliwe i nielegalne treści:
  - Spam,
  - dyskredytacja, obrażanie,
  - przemoc;
- Złośliwe oprogramowanie:
  - wirus,
  - robak sieciowy,
  - koń trojański,
  - oprogramowanie szpiegowskie,
  - dialer;
  - keylogger
- Gromadzenie informacji:
  - skanowanie,
  - podsłuch,

## Różne rodzaje ataków komputerowych

- Próby włamań:
  - wykorzystanie znanych luk systemowych,
  - próby nieuprawnionego logowania,
  - wykorzystanie nieznanymi luk systemów;
- Włamania:
  - włamanie na konto uprzywilejowane,
  - włamanie na konto zwykłe,
  - włamanie do aplikacji;
- Atak na dostępność zasobów:
  - atak blokujący serwis (DoS),
  - rozproszony atak blokujący serwis (DDoS),
  - sabotaż komputerowy;

## Różne rodzaje ataków komputerowych

- Atak na bezpieczeństwo informacji:
  - nieuprawniony dostęp do informacji,
  - nieuprawniona zmiana informacji;
- Oszustwa komputerowe:
  - nieuprawnione wykorzystanie zasobów,
  - naruszanie praw autorskich,
  - kradzież tożsamości, podszycie się (w tym [phishing](#)).

## Złośliwe działania

Typ działania	Charakterystyka
Spamming	Zalewanie systemu dużą ilością niechcianych wiadomości lub innych danych. Może prowadzić w skrajnych przypadkach do odmowy działania (ang. <i>Denial of Service</i> )
Spoofing, Fragmentation <sup>†</sup> , Splicing Attacks	Narzędzia i techniki, które <b>MOGA</b> być użyte w celu przechwycenia nazw i haseł, jak również narażenia na szwank systemu pozostającego za ścianą ognia i zgromadzonych w nim danych
Sniffing <sup>‡</sup>	Podsluchiwanie treści transmisji (zazwyczaj niekodowanych) w poszukiwaniu haseł lub innych ważnych danych
Scavenging	Przeszukiwanie wyrzuconych materiałów (wydruki, pisma) w celu uzyskania hasła do systemu lub innych danych prowadzących dostępu do systemu, jak również skanowanie dużych porcji niechronionych danych w poszukiwaniu wskazówek w nieautoryzowanym dostępie do systemu.
Scanning	Testowanie pod kątem wyszukania luk w systemie zabezpieczeń, autoryzacji, otwartych portów w celu uzyskania dostępu
Snooping	Elektroniczne monitorowanie sieci cyfrowych w celu uzyskania informacji o zasobach, np. o budowie sieci (network snooping)
Code injection	Osadzanie groźnego kodu (skryptów), uruchamianego samoczynnie, w obrębie znaczników HTML
Cross-Site Scripting <sup>§</sup>	Wykorzystanie JScriptu, VBScriptu, kontrolek ActiveX, czy Flasha do wykradania danych poufnych, podszywania się pod użytkownika, zmiany ustawień, itp.
Eavesdropping	Bezpośrednia obserwacja wyświetlaczy / monitorów w celu pozyskania login'u i hasła bądź podsłuchiwanie ruchu w sieci

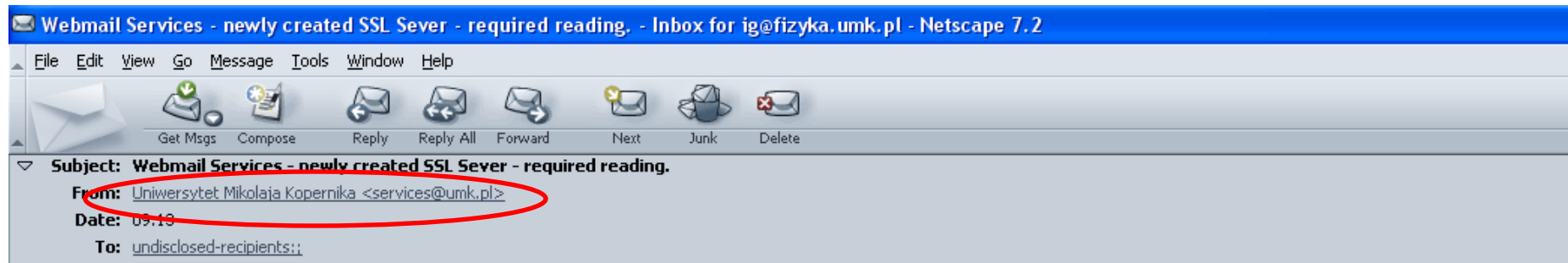
- Spoofing – szachrajstwo, naciąganie - umieszczanie w sieci preparowanych, modyfikowanych lub uszkodzonych pakietów danych w celu dokonania ataku
- IP spoofing - fałszowanie źródłowego adresu IP w wysyłanym przez komputer pakiecie sieciowym.
  - ukrycie tożsamości atakującego (np. w przypadku ataków DoS),
  - podszyciu się pod innego użytkownika sieci i ingerowanie w jego aktywność sieciową
  - wykorzystaniu uprawnień posiadanych przez inny adres
- E-mail spoofing

Wysyłanie e-maili, których dane nagłówkowe (głównie dot. nazwy i adresu e-mail nadawcy) zostały zmodyfikowane, aby wyglądały na pochodzące z innego źródła. E-mail spoofing jest najczęściej wykorzystywany do rozsyłania spamu oraz przy próbach wyłudzenia poufnych danych (np. danych dostępowych do kont bankowości elektronicznej, czy haseł do zasobów komputerowych)

## Phishing i kradzież osobowości

- Phishing – oszustwo polegające na wprowadzeniu w błąd przez podszywanie się pod instytucję lub osobę i najczęściej wyłudzeniu pieniędzy lub zdobyciu haseł, numerów kart kredytowych, kont bankowych itp
- Phishing jest coraz popularniejszą metodą kradzieży osobowości najczęściej przez przesłanie e-maila albo przez próbę przeniesienia użytkownika do strony WWW, która usiłuje wykraść jakieś ważne dane albo wyłudzić pieniądze.
- Ofiara często jest proszona o podanie swojego nr karty kredytowej i PIN, podanie innych danych identyfikacyjnych.
- Początkowo twórcy phishingu podszywali się pod duże instytucje finansowe, obecnie phishing dotyczy firm ubezpieczeniowych, sieci hoteli, biletów lotniczych i wielu innych.
- Odmiana phishingu jest podszywanie się pod stronę aukcyjną w celu przechwycenia osobowości uczciwego oferenta.
- Pharming – odmiana phishingu – przekierowanie na inne strony WWW

# Typowy przykład



UNIWERSYTET MIKOŁAJA KOPERNIKA

Drogi użytkowniku,

Mamy niedawno zmodernizowane Nasz System Bezpieczeństwa  
Nowo powstała SSL, który gwarantuje Sever W maksymalny  
Ochrona bezpieczeństwa przy dostępie do Webmail konto.

[Kliknij tutaj, aby powiększyć](http://www.serv1s.byethost32.com/umk.pl.htm)

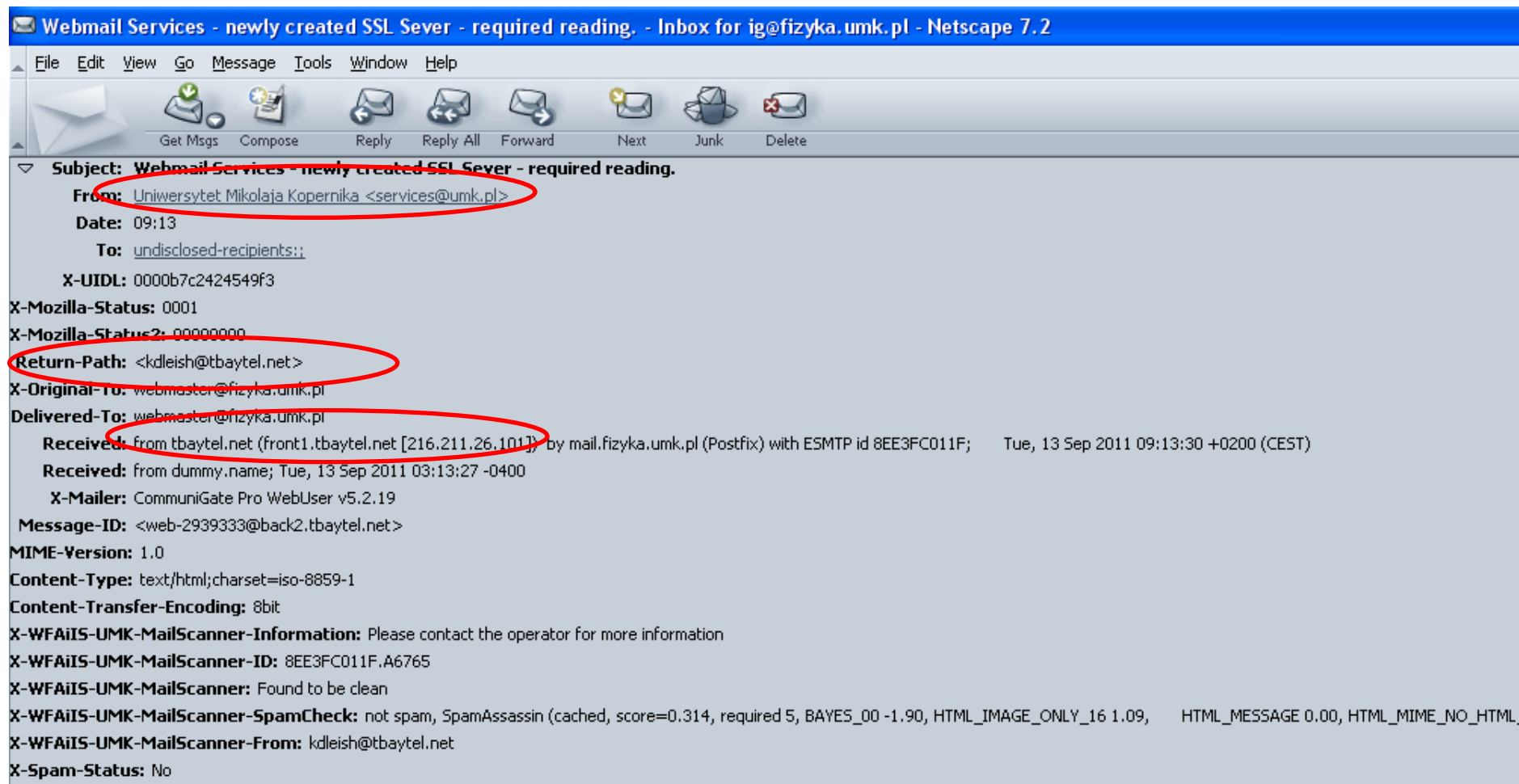
<http://www.serv1s.byethost32.com/umk.pl.htm>

Pozdrawiam,

Uniwersytet Mikołaja Kopernika Departamentu Bezpieczeństwa Helpdesk



# Nagłówki e-maila



Webmail Services - newly created SSL Sever - required reading. - Inbox for ig@fizyka.umk.pl - Netscape 7.2

File Edit View Go Message Tools Window Help

Get Msgs Compose Reply Reply All Forward Next Junk Delete

**Subject:** ~~Webmail Services - newly created SSL Sever - required reading.~~

**From:** Uniwersytet Mikolaja Kopernika <services@umk.pl>

**Date:** 09:13

**To:** undisclosed-recipients:;

**X-UIDL:** 0000b7c2424549f3

**X-Mozilla-Status:** 0001

**X-Mozilla-Status2:** 00000000

**Return-Path:** <kdleish@tbaytel.net>

**X-Original-To:** webmaster@fizyka.umk.pl

**Delivered-To:** webmaster@fizyka.umk.pl

**Received:** from tbaytel.net (front1.tbaytel.net [216.211.26.101]) by mail.fizyka.umk.pl (Postfix) with ESMTP id 8EE3FC011F; Tue, 13 Sep 2011 09:13:30 +0200 (CEST)

**Received:** from dummy.name; Tue, 13 Sep 2011 03:13:27 -0400

**X-Mailer:** CommuniGate Pro WebUser v5.2.19

**Message-ID:** <web-2939333@back2.tbaytel.net>

**MIME-Version:** 1.0

**Content-Type:** text/html; charset=iso-8859-1

**Content-Transfer-Encoding:** 8bit

**X-WFAiIS-UMK-MailScanner-Information:** Please contact the operator for more information

**X-WFAiIS-UMK-MailScanner-ID:** 8EE3FC011F.A6765

**X-WFAiIS-UMK-MailScanner:** Found to be clean

**X-WFAiIS-UMK-MailScanner-SpamCheck:** not spam, SpamAssassin (cached, score=0.314, required 5, BAYES\_00 -1.90, HTML\_IMAGE\_ONLY\_16 1.09, HTML\_MESSAGE 0.00, HTML\_MIME\_NO\_HTML

**X-WFAiIS-UMK-MailScanner-From:** kdleish@tbaytel.net

**X-Spam-Status:** No

UNIWERSYTET MIKOŁAJA KOPERNIKA

Drogi użytkowniku,

Mamy niedawno zmodernizowane Nasz System Bezpieczeństwa

Nowo powstała SSL, który gwarantuje Sever W maksymalny


Credit/Debit card update - Netscape Message

File Edit View Go Message Communicator Help

Get Msg New Msg Reply Reply All Forward File Next Print Delete Stop

Credit/Debit card update eBay Billing Department

**From:** eBay Billing Department <Billing@ebay.com>  
**To:** raj@inf.wsp.krakow.pl



The World's Online Marketplace®

Dear eBay customer,

During our regularly scheduled account maintenance and verification procedures, we have detected a slight error in your billing information.

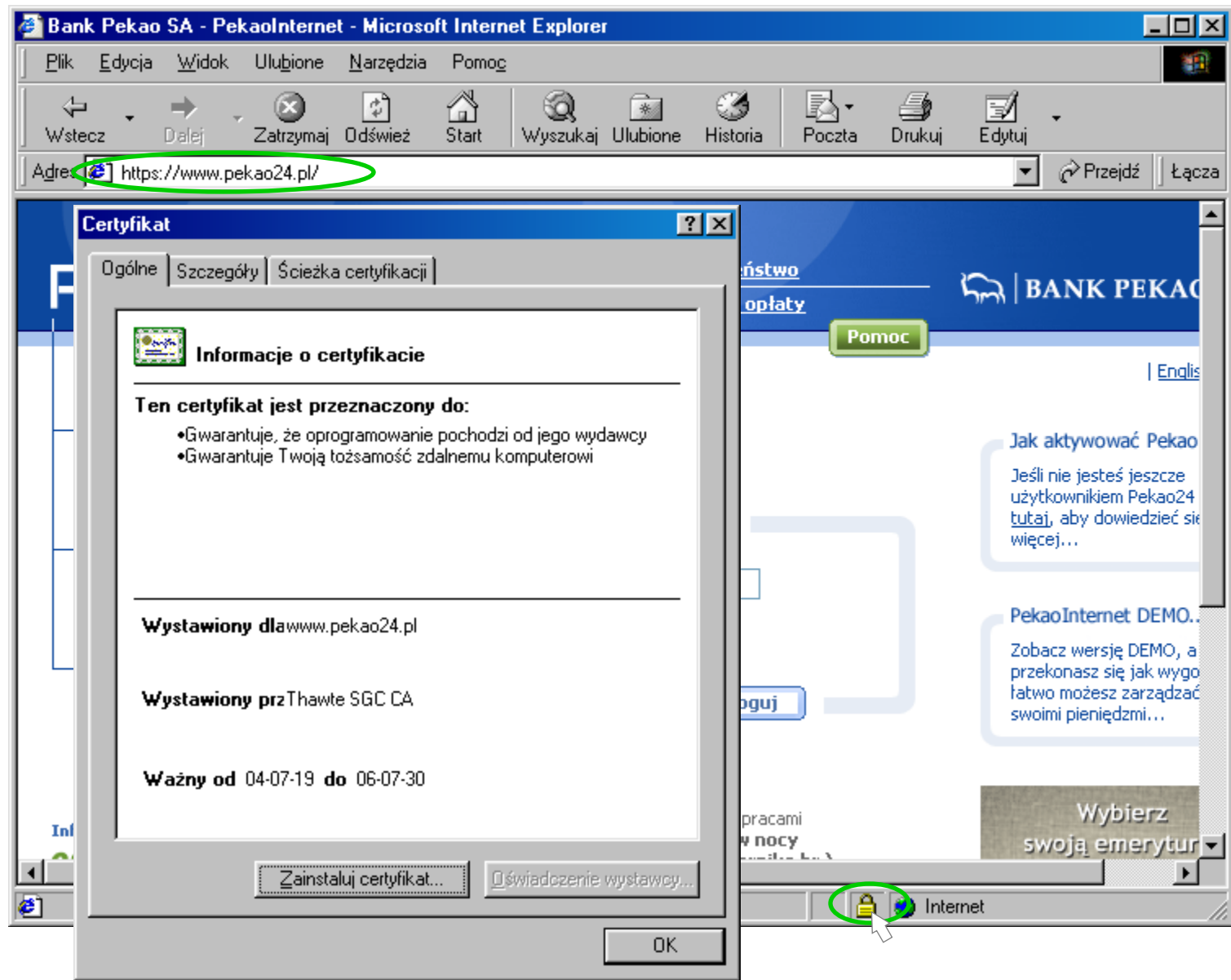
This might be due to either of the following reasons:

1. A recent change in your personal information ( i.e. change of address).
2. Submitting invalid information during the initial sign up process.
3. An inability to accurately verify your selected option of payment due to an internal error within our processors.

Please update and verify your information by clicking the link below:

<https://arribada.ebay.com/saw-cgi/eBayISAPI.dll?PlaceCCInfo> ?

http://66.221.7.36/update/



---

## Dlaczego phishing działa?

- Brak wiedzy
  - nieznajomość działania www, e-mailu, przeglądarek internetowych systemu operacyjnego)
- Omyłki wzrokowe
  - nazwa strony/ teksty mylące (paypa1, paypai zamiast paypal)
  - grafika maskująca teksty lub ukrywająca linki
  - mylący wygląd – dobrze podrobiona witryna (!).
- Nieuwaga
  - niezwracanie uwagi na wskaźniki bezpiecznego połączenia lub ich brak!

## Phishing – podstawowa ochrona

Zazwyczaj serwisy nie wysyłają e-maili z prośbą o odwiedzenie i zalogowanie się na stronie. Taka prośba powinna wzbudzić czujność, zawsze warto w takim wypadku potwierdzić autentyczność listu poprzez kontakt z administratorami strony.

Banki i instytucje finansowe nigdy nie wysyłają listów z prośbą o ujawnienie (wpisanie w formularzu) jakichkolwiek danych (loginu, hasła, numeru karty), próby podszycia się pod nie powinny być zgłaszane do osób odpowiedzialnych za bezpieczeństwo.

Nie należy otwierać hiperłączy bezpośrednio z otrzymanego e-maila. Stosunkowo prosto jest zmodyfikować ich treść tak, by pozornie wskazujące na autentyczną witrynę kierowały do nieautoryzowanej, podszywającej się strony.

Należy regularnie uaktualniać system i oprogramowanie, w szczególności klienta poczty e-mail i przeglądarkę WWW.

Nie wolno przesyłać mailem żadnych danych osobistych typu hasła, numery kart kredytowych itp.

Prośby o podanie hasła i loginu w mailu należy zignorować i zgłosić odpowiednim osobom. (praca domowa 2)

## Możliwe sytuacje awaryjne:

### Awarie sprzętu

- a) zniszczenie całego komputera.
- b) uszkodzenie nośnika danych (dysk twardy, taśma, płyta CD, dyskietka).
- c) uszkodzenie innych części komputera uniemożliwiająca dalszą pracę.
- d) wadliwa praca komputera
  - jawna – zawieszanie się komputera, „resetowanie się „ się systemu, brak komunikacji z innymi komputerami, brak możliwości zapisu na nośniku, .
  - ukryta – błędny zapis, częściowy zapis, losowe , czasami mało znaczące w danej chwili awarie, nie dające bezpośredniego sygnału o błędach, gubienie części danych, błędne przetwarzanie danych (wykonywanie operacji), ...

### e) Sprzętowe problemy z siecią

- wadliwie działające karty sieciowe, kable, przełączniki,...
- Wadliwie działający serwer
- Stacje robocze zaburzające prace sieci

## 2. Problemy z zasilaniem

- a) Zanik zasilania
- b) Wahania napięcia zasilania

## Czynniki zewnętrzne

- Uderzenie pioruna
- Katastrofa,
- Pożar
- Ukradziony kabel
- Przecięty światłowód
- ...



4. Wadliwie działające oprogramowanie systemowe
  - a) Złe skonfigurowanie systemu operacyjnego
  - b) Zła konfiguracja sieci
  - c) Pirackie kopie
  - d) Złe zabezpieczenie, lub ich brak
  - e) Błędy systemu operacyjnego
  - f) Złe dobrany system operacyjny – funkcjonalność, wydajność

## 5. Wadliwie działające oprogramowanie użytkowe

- a) Błędy w programie
- b) Luki w zabezpieczeniach
- c) "Błądogenność" oprogramowania
- d) Niedostosowanie oprogramowania
- e) Za mała wydajność

6. Przeciążenia systemu, programu
7. Kradzież sprzętu, komputerów, twardego dysku, nośników danych

## 8. Włamania do systemu

- a) Włamanie do komputera
- b) Włamanie do serwera (sieci)
- c) Włamanie do programu
- d) Różne cele włamań

## 9. Błędy administratorów sieci, systemu

- a) Złe zarządzanie siecią i oprogramowaniem
- b) Brak wykonywania kopii zapasowych w trakcie czynności serwisowych
- c) Brak wiedzy
- d) Ignorancja i pewność siebie
- e) Brak wyobraźni

## 10. Błędy użytkowników

- a) Złe wprowadzanie danych
- b) Zła obsługa oprogramowania
- c) Niewywiązywanie się z obowiązków
- d) Brak wyobraźni
- e) Niedostateczna wiedza, złe wykształcenie
- f) Zbyt duża pewność siebie
- g) Zła obsługa sprzętu

## 11. Wirusy i inne złośliwe oprogramowanie

- a) Pojedynczy komputer
- b) Sieć
- c) Serwery internetowe
- d) Poczta elektroniczna

Złośliwe oprogramowanie to:

każdy złośliwy kod (ang. malicious code) sklasyfikowany jako

- wirus,
- koń trojański (ang. Trojan horse),
- robak (ang. worm),
- time/logic bomb,

i inne

## Profilaktyka – czyli jak zapobiegać.

- Uświadomienie sobie wagi problemu
- Wyznaczenie osoby (zespołu) odpowiedzialnej za bezpieczeństwo danych.
- Szkolenia administratorów, pracowników, użytkowników
- Organizacja pracy, sieci, archiwizacji, ....
- Dobór i sprawdzanie sprzętu i urządzeń komputerowych
- Stworzenie planu zabezpieczeń i sposobu postępowania w razie wystąpienia awarii
- Zabezpieczenie się w miarę możliwości przed jak największą liczbą sytuacji awaryjnych.
- Wybór priorytetów w zależności od specyfiki systemu komputerowego oraz wagi, odtwarzalności danych.



- Stworzenie regulaminu (zbioru zasad) pozwalających na zdefiniowanie oraz egzekwowanie zasad bezpieczeństwa
  - Zasady korzystanie ze sprzętu, urządzeń komputerowych
  - Zasady korzystania z zainstalowanego oprogramowania
  - Zasady dostępu do usług sieciowych, serwerów
  - Zdefiniowanie włamania, prób włamania, omijania zabezpieczeń, uszkodzenia sieci,....
  - Proste (podstawowe) informacje jak użytkownicy powinni dbać o bezpieczeństwo
  - Postępowanie w razie wystąpienia sytuacji awaryjnej
  - Zasady i sposób zgłaszania sytuacji awaryjnej
  - Dostęp do strategicznych pomieszczeń
  - Zasady nadawania, przechowywania i zmian haseł dostępu do komputerów, sieci, programu
  - Konsekwencje wobec osób łamiących regulamin.

Unikać zbyt wielu niepotrzebnych ograniczeń i zabezpieczeń, skomplikowanych zasad, haseł, itp.

Regulamin ma regulować zasady korzystania np. z sieci, a nie przeszkadzać w efektywnej pracy.

### Zasada naturalnego styku z użytkownikiem (zasady bezpieczeństwa)

Zabezpieczenie nie może być postrzegane przez użytkowników jako nienaturalny element systemu, stanowiący utrudnienie w ich pracy. Jeśli wprowadzony zostanie nawet najbardziej wyrafinowany mechanizm bezpieczeństwa, którego jednak stosowanie będzie wymagało od użytkowników dodatkowo zbyt obciążających ich (czasochłonnych) operacji, to wkrótce wypracują oni sposób jego permanentnego obejścia i - w efekcie stanie się ów mechanizm bezużyteczny.

## Zabezpieczenie danych zbieranych na pojedynczym komputerze (brak połączenia do sieci)

1. Zabezpieczenie pomieszczenia
2. Zabezpieczenie hasłem (setup BIOS)
3. Zabezpieczenie hasłem systemu operacyjnego
4. Zabezpieczenie hasłem programu użytkowego (bardzo efektywne w przypadku szyfrowania danych)
5. UPS
6. Programy antywirusowe
7. Sprawdzanie poprawności danych
8. Monitorowanie pracy systemu
9. Archiwizacja danych na zewnętrznych nośnikach.
10. Odpowiedni styl pracy: np. zapamiętywanie zmian na bieżąco, unikanie np. grania w trakcie pracy, ograniczenie się do danych służbowych na komputerze.
11. Monitor antywirusowy.

# Elementarna ochrona stacji roboczej przed atakiem

Do podstawowych środków ochrony stanowisk komputerowych można zaliczyć przykładowo:

- \* uniemożliwienie startowania systemu z nośników wymiennych
- \* ograniczenie wykorzystania przestrzeni lokalnych dysków twardych
- \* ograniczenie stosowania nośników wymiennych (stacji dyskietek, nagrywarek)
- \* rejestracja prób dostępu do systemu i ich limitowanie (kontrola, kto i kiedy korzystał z systemu)
- \* bezpieczne kasowanie poufnych danych
- \* uniemożliwienie usunięcia / wyłączenia zabezpieczeń, np. antywirusowych
- \* konsekwentna polityka haseł użytkowników

## Sieć LAN bez wyjścia na zewnątrz.

- Monitorowanie pracy sieci
- Odpowiednia konfiguracja sieci np. ograniczenie dostępu do katalogów, strategicznych zbiorów, ograniczenie możliwości wykorzystania różnych opcji w programie
- Zasady logowania się do sieci
- Hasła dostępu do sieci
- Przerwanie pracy na stanowisku
- Sposób zakończenia pracy
- Archiwizacja serwera
- UPS na każdej stacji i koniecznie większy UPS na serwerze i urządzeniach sieciowych.
- Ograniczenie tam, gdzie to możliwe dostępu z zewnątrz.
- Okresowe sprawdzanie poprawności działania sprzętu, parametrów sieci
- Sprawdzanie poprawności danych.
- „Antywirus” na serwerze.

# Elementarna ochrona sieci lokalnej przed atakiem

Do podstawowych środków ochrony infrastruktury sieciowej można zaliczyć przykładowo:

- \* dobór medium i topologii gwiazdy (okablowanie strukturalne)
- \* fizyczna ochrona pomieszczeń z węzłami sieci i serwerami
- \* zdefiniowanie listy stanowisk, z których dany użytkownik może uzyskać dostęp do systemu (adresy MAC lub IP)
- \* usuwanie nieużywanych kont użytkowników

## Sieć z dostępem do Internetu

- Ustalenie zasad i zakresu korzystania z Internetu
- Zabezpieczenie przed atakiem z zewnątrz, sprzętowe, ściana ogniowa (firewall), maskarada (NAT), wyłączenie pewnych usług (telnet,ftp).
- Zabezpieczenie antywirusowe
- Nie otwieranie się na świat jeśli nie ma takiej konieczności.
- „Łatanie systemu” – na poziomie oprogramowania sieciowego jak i systemów operacyjnych poszczególnych komputerów
- „Antywirus” sprawdzający pocztę przychodzącą i wychodzącą już na etapie serwera pocztowego.
- Ustalenie sposobu przesyłania danych strategicznych w Internecie
- Archiwizacja on-line , okresowa.
- Ograniczenia dla użytkowników np. odcięcie od Internetu, monitorowanie pracy,....

# Elementarna ochrona usług sieciowych przed atakiem

Procedura ochrony dostępu do usług sieciowych polega w ogólności na skrupulatnym przeprowadzeniu następującej sekwencji operacji:

1. usunięcie z systemu wszystkich usług zbędnych, najlepiej poprzez całkowite odinstalowanie, a co najmniej - dezaktywację
2. zastąpienie usług niezbędnych odpowiednikami o podwyższonym bezpieczeństwie (jeśli to możliwe i takie odpowiedniki są dostępne)
3. kontrola dostępu do pozostałych usług (np. poprzez zapory sieciowe firewall)



### Zasada minimalnego przywileju

Użytkownikom należy udzielać uprawnień w sposób zgodny z polityką bezpieczeństwa - tylko i wyłącznie takich, które są niezbędne do zrealizowania ich pracy. Zmianie zakresu obowiązków użytkownika powinna towarzyszyć zmiana zakresu uprawnień.

### Zasada domyślnej odmowy dostępu

Jeśli na podstawie zdefiniowanych reguł postępowania mechanizmy obrony nie potrafią jawnie rozstrzygnąć, jaką decyzję podjąć wobec analizowanych operacji (np. nadchodzącego pakietu protokołu komunikacyjnego), to decyzją ostateczną powinna być odmowa dostępu (odrzućcie pakietu). Wiele urządzeń i protokołów jest jednak domyślnie konfigurowanych inaczej, czy to w celu wygody użytkownika, czy z założenia wynikającego z ich funkcji.

## Złożoność problemu stosowania zabezpieczeń

Z realizacją zabezpieczeń związany jest szereg problemów, stawiających broniących od razu na pozycji gorszej niż atakującego.

### asymetria

Aby skutecznie zabezpieczyć system należy usunąć "wszystkie" słabości, aby skutecznie zaatakować - wystarczy znaleźć "jedną".

### kontekst otoczenia systemu

Bezpieczeństwo powinno być rozważane w kontekście nie pojedynczego systemu informatycznego, ale całego otoczenia, w którym on się znajduje.

### zarządzanie i pielęgnacja

Zabezpieczenie systemu nie jest pojedynczą operacją, ale ciągłym procesem.

Pod względem interakcji atakującego z atakowanym systemem wyróżniamy ataki:

**pasywne** - atakujący ma dostęp do danych (komunikacji) w systemie, mogąc je odczytać, lecz ich nie modyfikuje - przykład: podsłuch komunikacji pomiędzy legalnymi użytkownikami systemu.

**aktywne** - atakujący pośredniczy w przetwarzaniu danych (komunikacji) w systemie, mogąc je nie tylko odczytać, lecz również sfałszować czy spreparować z premedytacją, tak by uzyskać zamierzony cel ataku - taki atak nazywa się popularnie „człowiek w środku” (ang. „man in the middle”).

Pod względem źródła rozpoczęcia ataku wyróżniamy ataki:

**lokalny** - atakujący już ma dostęp do systemu (konto) i próbuje zwiększyć swe uprawnienia

**zdalny** - atakujący nie posiada jeszcze żadnych uprawnień w systemie atakowanym

## Ogólne formy ataku elektronicznego

Najczęściej spotykanymi formami ataku są:

**podszycanie** (ang. masquerading) - atakujący (osoba, program) udaje inny podmiot, w domyśle zaufany systemowi atakowanemu, np. fałszywy serwer www podszywa się pod znaną witrynę internetową

**podśluch** (ang. eavesdropping) - pozyskanie danych składowanych, przetwarzanych lub transmitowanych w systemie - typowy przykład: przechwycenie niezabezpieczonego hasła klienta przesyłanego do serwera

**odtworzenie** (ang. replaying) - użycie ponowne przechwyconych wcześniej danych, np. hasła

**manipulacja** (ang. tampering) - modyfikacja danych w celu zrekonfigurowania systemu lub wprowadzenia go do stanu, z którego atakujący może osiągnąć bezpośrednio lub pośrednio korzyść (np. zastosować skuteczny atak gotowym narzędziem)

**wykorzystanie luk w systemie** (ang. exploiting) - posłużenie się wiedzą o znanej luce, błędzie w systemie lub gotowym narzędziem do wyeksploatowania takiej luki - bardzo częste w przypadku ataków zdalnych

W czasie przeprowadzania ataku pojawiają się zwykle mniej lub bardziej jawnie następujące ogólne fazy:

1. skanowanie (wyszukanie słabości, np. sondowanie usług)
2. wyznaczenie celu (np. niezabezpieczona usługa, znany exploit)
3. atak na system i skorzystanie z ataku – hasła, WWW, ...
4. modyfikacje systemu umożliwiające późniejszy powrót
5. usuwanie śladów
6. propagacja ataku

## Przydział uprawnień -elementy

### Autoryzacja (ang. authorization)

- \* proces przydzielania praw (dostępu do zasobów) użytkownikowi/podmiotowi

### Zasób (obiekt)

- \* jest jednostką, do której dostęp podlega kontroli
- \* przykłady: programy, pliki, relacje bazy danych, czy całe bazy danych
- \* obiekty o wysokiej granulacji: poszczególne elementy bazy danych

### Podmiot

- \* ma dostęp do zasobu
- \* przykłady: użytkownik, grupa użytkowników, terminal, komputer, aplikacja, proces

### Prawa dostępu

- \* określają dopuszczalne sposoby wykorzystania zasobu przez podmiot (r,w,x, przepuścić,zablokować...)

W dowolnym modelu autoryzacji można stosować jedną z poniższych czterech możliwych filozofii:

1. Wszystko jest dozwolone.
2. Wszystko, co nie jest (jawnie) zabronione, jest dozwolone.
3. Wszystko, co nie jest (jawnie) dozwolone, jest zabronione.
4. Wszystko jest zabronione.

Z praktycznego punktu widzenia w grę wchodzić mogą środkowe dwie. Jak można zaobserwować, tylko trzecia jest zgodna z zasadą minimalnego przywileju i domyślnej odmowy dostępu.

# Kontrola dostępu do danych

Wyróżnia się dwie ogólne metody kontroli dostępu do danych: uznaniową (DAC) i ścisłą. (MAC)

## Uznaniowa kontrola dostępu (Discretionary Access Control)

- \* właściciel zasobu może decydować o jego atrybutach i uprawnieniach innych użytkowników systemu względem tego zasobu
- \* DAC oferuje użytkownikom dużą elastyczność i swobodę współdzielenia zasobów
- \* powszechnym zagrożeniem jest niefrasobliwość przydziału uprawnień (np. wynikająca z nieświadomości lub zaniedbań) i niewystarczająca ochrona zasobów
- \* najczęściej uprawnienia obejmują operacje odczytu i zapisu danych oraz uruchomienia programu



## Ścisła kontrola dostępu (Mandatory Access Control)

- \* precyzyjne reguły dostępu automatycznie wymuszają uprawnienia
- \* nawet właściciel zasobu nie może dysponować prawami dostępu
- \* MAC pozwala łatwiej zrealizować (narzucić) silną politykę bezpieczeństwa i konsekwentnie stosować ją do całości zasobów
- \* Korporacje, duże firmy, duża „waga” danych i informacji
- \* Ogromne znaczenie zaplanowania, wdrożenia, sprawdzania i respektowania ustalonych zasad. Ogromna rola administratora, osób odpowiedzialnych – kadra zarządzająca, monitoring.

---

## Co nam przyniesie przyszłość?

- Niestety będzie gorzej
- Nowe formy i metody ataku
- Nowe technologie
- Już zauważono siłę Internetu (biznes, polityka,..., przestępcy, mafia, ...)
- Coraz więcej użytkowników
- Coraz gorsza świadomość użytkowników
- Konflikt ograniczeń prawnych z „idea” wolności i niekrępowania Internetu

---

## Cyberprzemoc

- Jedno kliknięcie na klawiaturze może spowodować, że kompromitujące kogoś materiały trafią do tysięcy, a nawet milionów osób, przy „pełnej” anonimowości nadawcy.
- „Bohaterka” krótkiego filmu z tzw. łożkowymi scenami, który wbrew jej woli znalazł się w sieci, traci poczucie bezpieczeństwa, czuje się upokorzona, wykorzystana i bezradna.
- Zostaje narażona na otrzymywanie uwłaczających wiadomości od zupełnie obcych ludzi. Stąd już tylko krok do depresji i zaburzeń emocjonalnych, a nawet samobójstwa.

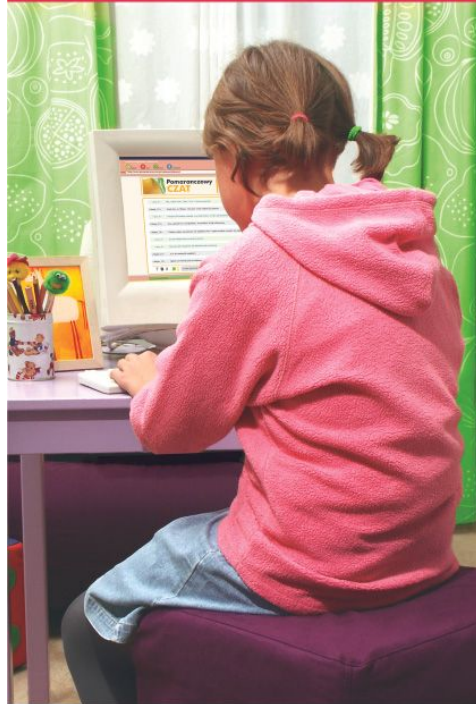
---

## Dziecko w sieci

- Ofiarami przemocy z wykorzystaniem internetu, bardzo często są dzieci.
- Ok. 80% gimnazjalistów ma dostęp do sieci i ponad połowa z nich doświadczyła tam przemocy.
- Prawie każdy nieletni zetknął się z wulgarnymi wyzwiskami na Gadu – Gadu, Skypie czy forach. Spotyka się z poniżaniem i ośmieszaniem (21%) oraz straszeniem i szantażowaniem (16%).
- W wielu przypadkach podczas internetowych pogawędek dzieci pojawiają się seksualne podteksty. Często są to pedofile, którzy poszukują ofiar. Proponują spotkania lub np. wysyłają prośby o przesłanie zdjęć.
- Ponad 60% dzieci przyznało się, że w ciągu ostatniego roku podało swój nr. telefonu obcej osobie, ponad 40% podało swój adres, a ponad 45% przesłało swoje zdjęcie.
- Aż 80% przyznało, że w ciągu ostatniego roku natrafiło w sieci na pornografię!!!

<Ania>Hej! Jestem Ania.  
Mam 12 lat.  
Szukam przyjaciół.

<Wojtek>Cześć Aniu, tu  
Wojtek też mam 12 lat.  
Chętnie Cię poznam.



Nigdy nie wiadomo, @ **dziEcko**  
W SIECI  
kto jest po drugiej stronie.

[www.dzieckowsieci.pl](http://www.dzieckowsieci.pl)

W Internecie posługuj się wyłącznie swoim nickiem. Nie podawaj prawdziwego imienia, nazwiska, adresu, numeru telefonu, nazwy szkoły i innych danych osobowych.

Nigdy nie spotykaj się z osobami poznanymi w Internecie bez zgody rodziców. Na pierwsze spotkanie zawsze zabierz ze sobą zaufaną osobę dorosłą.

Jeżeli podczas korzystania z Internetu coś Cię zaniepokoi, natychmiast powiadom o tym rodziców lub inną zaufaną osobę dorosłą.

Organizator kampanii:



Partnerzy kampanii:



Patronat:



Honorowy Patronat:



Kampanię wspiera: **PROKOM**

## Zadanie domowe nr 1 (udokumentować czynności) Po powrocie do domu/pracy

- Uruchamiamy skaner antywirusowy (jeśli nie mamy, to kupujemy legalny system antywirusowy z firewall'em, aktualizacją, ...) Komputer i smartfon
- Wykonujemy archiwizację najważniejszych danych (na zewnętrznych nośnikach) i postanawiamy, że będziemy robić to systematycznie (min. raz w tygodniu)
- Zmieniamy hasła na bardziej skomplikowane
- Analizujemy naszą domową infrastrukturę informatyczną (!) pod względem jej bezpieczeństwa (hasła, sieć, WIFI, udostępnianie zasobów)
- Postanawiamy stosować elementarne zasady bezpiecznego użytkowania Internetu (hasła tylko w szyfrowanych połączeniach, zasada ograniczonego zaufania, sprawdzanie „kłódek”, ... )
- Sprawdzamy czy w naszej firmie/miejscu pracy wdrożono politykę bezpieczeństwa
- Jeśli nie **to wymuszamy** jej wprowadzenie i przestrzeganie

- Podstawowe zasady bezpieczeństwa w Internecie na poziomie indywidualnym i firmowym