Bezpieczeństwo - wprowadzenie

- 1. Haking
- 2. Programy destrukcyjne
- 3. Bezpieczeństwo – definicja, normy prawne
- 4. Zagrożenia, Podatności, Ataki
- 5. Inicjatywy na rzecz bezpieczeństwa

1. Haking

XI 2010

1.1 Haking
1.2 Hakerzy
1.3 Haking dziś

- Pod koniec lat 50-tych klub modelarza kolejowego przy MIT otrzymał stare oprzyrządowanie telefoniczne
- Stworzyli system, który pozwalał operatorom na zdalne sterowanie różnymi elementami przez „wdzwanianie się"
- Narodziny **hakingu** – pomysłowego sposobu wykorzystania sprzętu do nowych zastosowań
- Cel hakera: zaspokojenie nieustannego głodu wiedzy

[Hacking sztuka penetracji]

Phreaking (*phone* + *freak*) – włamania do sieci telefonicznej

- Gwizdek dodawany do płatków śniadaniowych Cap'n Crunch generował dźwięk 2600Hz, sterujący elektromechaniczną centralą telefoniczną
- Nowe centrale elektroniczne – również były podatne na *„ataki"*
- Sterowanie obu typami central - **kolorowe pudełka** (emitują specjalne tony lub wprowadzają fizyczne zmiany w obwodach telefonicznych)

- red box – wybieracz tonowy cyfrowo generujący dźwięki – po przebudowie można było symulować dźwięk ćwierćdolarówek wrzucanych do automatu
- blue box – pozwalało na prowadzenie rozmów międzymiastowych (ton 2600Hz)
- dayglo box – pozwalało na korzystanie z linii telefonicznej sąsiada
- aqua box – uniemożliwiało ustalenie przez FBI trasy połączenia telefonicznego
- mauve box – pozwalało na podsłuchiwanie linii telefonicznej
- chrome box – kontrolowało sygnały w linii telefonicznej

- 1983: FBI aresztuje grupę nastolatków, *414*, oskarżonych o włamanie do około 60 komputerów
- 1984: Powstaje kwartalnik *2600: The Haker Quarterly*
- 1985: Powstaje czasopismo *Phrack*
- 1989: Pierwszy wyrok prawomocny dla hakera (Kevin Mitnick)
- 1990: Legion of Doom zaatakował połączenia z numerem 911
- 1992: Kevin Poulsen oskarżony o kradzież tajemnic państwowych
- 1995: Wladimir Lewin kradnie 4mln dolarów z Citibanku
- 2000: Atak na: Yahoo, Amazon, Buy, CNN
- 2010: **WikiLeaks**: wyciek poufnej korespondencji dyplomatycznej

Haking
Podział hakerów

T. Lukaszewski

W zależności od stwarzanego niebezpieczeństwa hakerów (crackerów, intruzów, włamywaczy, napastników, wandali, przestępców) można podzielić na następujące kategorie:

- eksperci do spraw bezpieczeństwa
- przypadkowi włamywacze
- osoby poszukujące wrażeń (np. studenci)
- hobbyści
- włamywacze-kryminaliści
- szpiedzy przemysłowi
- niezadowoleni pracownicy (tzw. **wróg wewnętrzny**)

Haking
Kevin Mitnick (Condor) 1963

T. Lukaszewski

- najbardziej znany haker świata
- Condor – „Trzy dni Condora"
- aresztowany przez FBI 15 lutego 1995r i oskarżony o włamania do systemów komputerowych
- uwolniony 21 stycznia 2000 roku z zakazem używania Internetu aż do 21.01.2003
- Obecnie pracownik firmy Defensive Thinking

[en.wikipedia.org]

U.S. Department of Justice
United States Marshals Service

WANTED
BY U.S. MARSHALS

NOTICE TO ARRESTING AGENCY: Before arrest, validate warrant through National Crime Information Center (NCIC).
United States Marshals Service NCIC entry number: (NIC/ W721440921).

NAME: .....MITNICK, KEVIN DAVID
AKS(S): .....MITNIK, KEVIN DAVID
MERRILL, BRIAN ALLEN

DESCRIPTION:
Sex: .....MALE
Race: .....WHITE
Place of Birth: .....VAN NUYS, CALIFORNIA
Date(s) of Birth: 08/06/63; 10/18/70
Height: .....5'11"
Weight: 190
Eyes: .....BLUE
Hair: .....BROWN
Skintone: .....LIGHT
Scars, Marks, Tattoos: .....NONE KNOWN
Social Security Number (s): 550-39-5695

Haking
Kevin Mitnick (Condor)

T. Lukaszewski

- Jako dziecko włamywał się do szkolnego systemu komputerowego.
- W 1981, mając 17 lat, wraz z kolegami włamał się do komputerów firmy **Pacific Bell**. Skazany na 3 miesiące w zakładzie poprawczym.
- 1983 – 6 miesięcy za włamanie do **ARPAnetu**
- 1987 – 36 miesięcy (w zawieszeniu) za włamanie do **SCO**
- 1988 włamanie do laboratorium **Palo Alto** – próba zdobycia kodu źródłowego systemu VMS. 12 miesięcy.
- Od 1989 uciekał przed FBI (bał się niesprawiedliwego wyroku). Aresztowany w 1995, skazany w 1999, zwolniony w styczniu 2000 roku, do stycznia 2003 roku zakaz używania sprzętu komputerowego i urządzeń elektronicznych

Haking
Kevin Mitnick (Condor)

T. Lukaszewski

Filmy bazujące na biografii Mitnicka:

- Gry Wojenne (Wargames) (1983) – opowieść o nastolatku, który włamuje się do systemu komputerowego armii amerykańskiej i zaczyna grać z komputerem
- Operation Takedown (2000) – film fabularny oparty o biografię Kevina
- Freedom Downtime (2001) – film dokumentalny, stworzony przez sympatyków Kevina - protest wobec fałszywego obrazu przedstawionego w „Takedown" oraz wobec traktowania hackerów (trzymani przez kilka lat w więzieniach bez wyroków sądowych)

Haking
Robert Tappan Morris 1965

T. Lukaszewski

- twórca pierwszego robaka (1988)
- Ph.D. na Harvardzie (1999)
- profesor MIT (od 1999)

[en.wikipedia.org]

Haking
Robert Morris

- Sprawca pierwszej i przez długie lata rekordowej afery, która kosztowała 100 mln USD.
- Będąc doktorantem na Uniwersytecie Cornell, w listopadzie 1988 stworzył program, który zablokował ponad 6000 komputerów.
- Program ten nazwano "**worm**". Wykorzystywał on lukę w mechanizmie przesyłania poczty między komputerami podłączonymi do internetu. Program wyszukiwał okoliczne komputery i przesyłał tam swoją kopię.
- Morris popełnił błąd – program uruchamiał się wielokrotnie na każdym z komputerów. Skutkowało to zablokowaniem systemów.
- Aresztowany z dużym opóźnieniem został skazany na 3 lata obserwacji, 400 godzin prac społecznych i 10 tys. USD.

Haking
Kevin Poulsen (Dark Dante) 1965

- znany z przejęcia linii telefonicznych stacji radiowej – w celu wygrania Porsche 944
- otrzymał najwyższy wyrok sądowy w historii hackingu
- obecnie „editorial director" SecurityFocus

[en.wikipedia.org]

Haking
Kevin Poulsen (Dark Dante)

- Pierwszy haker oskarżony o szpiegostwo (listopad 1989).
- Expert od zabezpieczeń, nocą włamywał się do systemów rządowych – zdobył m.in. dokumenty taktyczne US Air Force.
- Przez 17 miesięcy unikał aresztowania. W tym czasie szlifował umiejętności zdobywania nagród w konkursach radiowych.
- W 1990 roku przejął wszystkie linie telefoniczne stacji KIIS-FM w Los Angeles. Sto druga osoba dzwoniąca po zagraniu odpowiedniej sekwencji utworów miała otrzymać samochód Porsche. Był 102-gi.
- 11 kwietnia 1991 roku został ujęty na nocnych zakupach w supermarkecie. Został rozpoznany przez sprzedawcę.
- Skazany na 51 miesięcy pozbawienia wolności i 56.000 USD na rzecz oszukanych stacji radiowych

Haking
Jon Lech Johansen (DVD Jon) 1983

Hakin9 10/2007

- Norweski programista (matka **Polka**)
- Stworzył program deszyfrujący zakodowane DVD – DeCSS
- 2001 - Stworzył zestaw sterowników do odtwarzacza MP3 JazPiper
- 2003 - Stworzył program QTFairUse do odczytywania zakodowanych strumieni AAC
- 2004 – Opracował wtyczkę do odtwarzania mediów zabezpieczonych systemem FairPlay
- 2007 - Złamał część zabezpieczeń nowego iPhone'a – pokazał możliwość aktywacji telefonu bez wiązania się umową z autoryzowanym operatorem AT&T

Haking
Julian Paul Assange 1971

- Zaangażowany w WikiLeaks
- 30.11.2010 Interpol wystawił list gończy
- WikiLeaks to 11 września światowej dyplomacji (wg. Pentagonu)

Haking
Hakerzy w Polsce

„Gorion"
paweł jabłoński

Haking
Dzień dzisiejszy

- (1) Hakerów zatrudniają: wywiad, banki, sklepy internetowe
- (2) Haking (cyberprzestępstwo) to biznes:
  - Kilkaset euro – wykonanie ataku na sieć w konkretnej firmie
  - Kilkaset euro – rozesłanie 20 milionów e-maili (spamu)
  - Kilkaset euro – zakup bazy 5 milionów adresów
  - Kilkaset euro – informacje o lukach w zabezpieczeniu sieci

Komputer Świat 23/2007

Programy destrukcyjne

X 2010

Programy destrukcyjne
Wprowadzenie

- **Programy destrukcyjne** nazywane są też **złośliwym kodem** (ang.*malware, malicious software*)
- Cel programów:
  - nękanie użytkowników i/lub
  - niszczenie danych
- Podział:
  - Wirusy
  - Robaki
  - Konie trojańskie

Programy destrukcyjne
Wirusy

- Koncepcja samopowielających się programów – John von Neuman, Teoria i organizacja skomplikowanych automatów, 1949 rok
- W połowie lat 70. tych w systemie operacyjnym Tenex stworzony został program **The Creeper**, który sam się rozprzestrzeniał w sieci. Do zwalczania go administratorzy napisali program **The Reeper**, uważany za pierwszy w historii **program antywirusowy**
- Jednakże niemal do 1983 roku wirusy były sprawą czysto teoretyczną i poza środowiskami akademickimi fascynowały jedynie niektórych autorów powieści science fiction.

Programy destrukcyjne
Wirusy

- W 1983 roku Fred Cohen rozpoczął na Uniwersytecie w Cincinati praktyczne eksperymenty z napisanymi przez siebie wirusami. Jako pierwszy użył terminu **„wirus komputerowy"**
- W maju 1984 roku Prof K.A.Dewdney opisał w "Scientific American" skodyfikowane reguły gry zwanej **wojnami rdzeniowymi**
- W kwietniu 1985 roku w "Scientific American" w rubryce poświęconej wojnom rdzeniowym, opublikowany został list włoskich programistów Roberto Cerutti i Marco Morocutti. Opisali oni jak pod wpływem gry doszli do **koncepcji prawdziwego wirusa**

Programy destrukcyjne
Wirusy

Pierwsze prawdziwe wirusy – 1986:

- **VIRDEM** (Ralf Burger) – powstał w celach demonstracyjnych, pokazywał mechanizmy replikacyjne i sygnalizował potencjalne zagrożenia. Pomimo jawnego demonstrowania obecności zdołał się rozpowszechnić
- **Brain** – w Pakistanie powstał jeden z najsłynniejszych wirusów. Jego autorzy odkryli, że sektorze rozruchowym dyskietki mogą się znaleźć instrukcje inne niż te, które służą do ładowania systemu operacyjnego – pierwszy atak 19.01.1986 roku

Programy destrukcyjne
Wirusy – obrona

T. Łukaszewski

- W 1989 r. Powstaje program antywirusowy firmy IBM
- W 1991 Symantec prezentuje własny program antywirusowy
- W 1996 r. Powstaje MKS sp. z o.o.

Marek Sell
zajmował się walką
z wirusami komputerowymi
od 1988 r.
zmarł 13 czerwca 2004r.

Programy destrukcyjne
Wirusy – definicja

T. Łukaszewski

- Program lub fragmentem kodu, który reprodukuje się na różne sposoby i czasem wykonuje pewne działania.
- Nie może działać niezależnie – wymaga działania programu gospodarza

Wirus nie może spontanicznie pojawić się na dysku twardym – musi zostać przekopiowany i uruchomiony przez człowieka. Jeżeli wirus nie jest w stanie zainfekować pliku, dokumentu ani dyskietki, to nie może się rozprzestrzeniać

Programy destrukcyjne
Wirusy – podział

T. Łukaszewski

- bootsektorowe (atakujące sektory startowe)
- drążące (dopisujące się do innych programów bez zwiększenia ich długości)
- polimorficzne (potrafią zmieniać swoją formę)
- makrowirusy
- rezydentne (pozostające w pamięci operacyjnej komputera)
- fałszywe alarmy (hoax) (w postaci wiadomości e-mail)

Programy destrukcyjne
Wirusy – przykłady

T. Łukaszewski

wirus czernobylski (CIH) (1999)

- Zaatakował 26 kwietnia 1999 roku (dzień przed rozpoczęciem się konferencji InfoSecurity'99)
- Działał tylko w systemach Windows 95 i 98 oraz Me
- Zamazywał dysk losowymi danymi lub **uszkadzał Flash Bios**

Programy destrukcyjne
Wirusy – przykłady

T. Łukaszewski

Melissa (1999)

- Makrowirus
- Zarażenie – zawirusowany dokument Worda
- Otwarcie dokumentu - uruchomienie wirusa, który pobierał z książki adresowej Microsoft Outlook lub Outlook Express 50 początkowych adresów i wysyłał przez Internet swoją kopię
- Wirus ponadto infekował plik Normal.dot - wszystkie dokumenty utworzone po zarażeniu wirusem były również zakażone

Programy destrukcyjne
Robaki – definicja

T. Łukaszewski

- **Robak** (ang. worm) jest bardzo podobny do wirusa. Różnica: **może rozpowszechniać się samodzielnie**
- Ponadto jego celem jest przenoszenie się z **komputera** na **komputer**, nie zaś z pliku na plik
- Większość obecnych wirusów należy do klasy robaków
- Włamują się one do systemów wykorzystując **słabe punkty** w oprogramowaniu

Programy destrukcyjne
Robaki – definicja

- The term "worm" actually comes from a science fiction story called The Shockwave Rider written by John Brunner in 1975.
- In short, the story is about a totalitarian government that controls its citizens through a powerful computer network. A freedom fighter infests this network with a program called a "**tapeworm**" forcing the government to shut down the network, thereby destroy its base of power.

[http://www.snowplow.org/tom/worm/worm.html]

Programy destrukcyjne
Robaki – przykłady

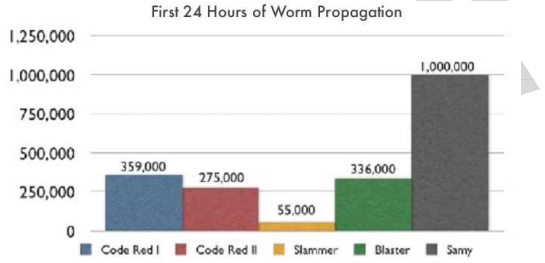
- (Listopad 1988) około 6000 komputerów zostało zainfekowanych programem napisanym przez R. Morrisa.
- (2000) **Love Bug (Love Letter, I Love You)** – w załączniku był skrypt VisualBasic – pobranie adresów i rozesłanie się
- (2001) **Code Red** (Chińczycy) miał przeprowadzić zmasowany atak typu DDOS na oficjalną stronę prezydenta USA (błędy IIS)
- (2001) **Blue Code** (USA) usuwał chiński produkt z zainfekowanych serwerów, sam się instalował i atakował stronę internetową jednej z firm chińskich
- (2001) **Nimda** - typowy robak rozsyłający się samoistnie pocztą elektroniczną – wystarczy podgląd załącznika (błędy IE, IIS)
- (2002) **KLEZ** - wykorzystywał lukę zabezpieczeń IFRAME IE

Programy destrukcyjne
Robaki – przykłady

- (2002) **BUGBEAR** rozprzestrzeniał się przez NETBIOSa
- (2003) **SQL SLAMMER**, **MS BLAST** (atakuje 135/tcp)
- (2004) **MY DOOM**, wykonywalny załącznik ze sfałszowanym nagłówkiem FROM, sieć P2P KazaA
  - wersja A atakowała SCO (atak DOS)
  - wersja B 4.02.2004 miała zaatakować serwery internetowe Microsoftu, ale Microsoft stosuje technologię firmy Akamai (rozproszenie serwerów)
  - wersja F atakowała witrynę RIAA
- (2004) **SASSER** – podatność LSASS (atakuje 445/tcp)
- (2005) UDF Worm (MySQL 3306/tcp), **SAMY** (XSS)
- (2006) Nyxem.E (Blackmal.E, Kama Sutra, MyWife.E)

Programy destrukcyjne
Robaki – przykłady

- Prędkość rozprzestrzeniania się robaków (pierwsze 24 godziny)



Programy destrukcyjne
Konie trojańskie

- **Koń trojański** (**trojan**) to: program, który wydaje się realizować pożądane i pożyteczne funkcje, lecz realizujący funkcje nieznane jego użytkownikowi.
- Działają bardzo podstępnie i bardzo trudno określić dokonaną przez nich skalę zniszczeń (penetracji systemu)
- Celem jest ujawnienie istotnych informacji o systemie, na którym został uruchomiony lub doprowadzenie do pokonania zabezpieczeń

Pr

- www.av-comparatives.org
- www.antivirus.about.com
- www.av-test.org
- www.antywirus.net.pl

*: those products got lower awards due false alarms

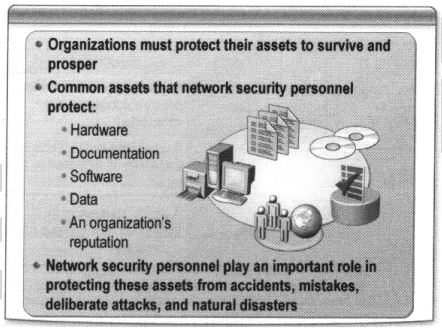
Bezpieczeństwo

III 2008

Shimorski R., Shinder D., Shinder T., Wielka Księga Firewalli, Helion, 2004

Microsoft Official Course 2810A: Fundamentals of Network Security

Mielnicki Tomasz, Audyt bezpieczeństwa informatycznego, praca dyplomowa magisterska, Poznań 2005 (normy)



Czym jest bezpieczeństwo?

- **Poziom, do jakiego program lub urządzenie jest zabezpieczone przed nieautoryzowanym wykorzystaniem** (w danej chwili – ponieważ ciągle pojawiają się nowe zagrożenia)
- **Poziom bezpieczeństwa** zależy od:
  - możliwych do poniesienia wydatków
  - kompromisu pomiędzy bezpieczeństwem a użytecznością

Nie istnieje **absolutne bezpieczeństwo**:

- Nie jesteśmy w stanie przewidzieć wszystkich zagrożeń
- Czas reakcji na zagrożenia nie jest zerowy
- Ludzka słabość, omylność projektantów
- Niewłaściwe i niefrasobliwe wykorzystanie aplikacji

Zatem co możemy zrobić? ...

Osiągać taki poziom bezpieczeństwa, by **atakującemu nie opłacało się nas zaatakować**

Utrudniając życie atakującemu należy pamiętać, że:

- Atakujący na ogół omija zabezpieczenia, często atakując od środka
- Obrona powinna składać się z kilku linii
- Złożoność (skomplikowanie) jest wrogiem bezpieczeństwa
- Brak zaobserwowania ataku nie oznacza że go nie było

Podstawowe **obszary bezpieczeństwa** informacji – **CIA + AAN**:

- **C**onfidentiality (poufność): dostęp tylko dla stron upoważnionych
- **I**ntegrity (integralność): możliwość wykrycia modyfikacji
- **A**vailability (dostępność): zapewnienie niezakłóconego dostępu
- **A**uthentication (uwierzytelnianie): weryfikacja tożsamości osoby
- **A**uthorization (autoryzacja): kontrola dostępu do zasobów
- **N**onrepudation (niezaprzeczalność): możliwość udowodnienia inicjatorowi transakcji, że to faktycznie ona była inicjatorem

[Wielka Księga Firewalli]

Bezpieczeństwo
Bezpieczeństwo elementem wiarygodności

T. Lukaszewski

System wiarygodny:

- **Dyspozycyjny** (available) – dostępny na bieżąco
- **Niezawodny** (reliable) – odporny na awarie
- **Bezpieczny** (secure) – zapewniający ochronę danych
- **Bezpieczny** (safe) – bezpieczny dla otoczenia

Bezpieczeństwo
Polskie akty prawne

T. Lukaszewski

- **U. z dnia 29 sierpnia 1997 r. o ochr. danych osobowych**
- **U. z dnia 22 stycznia 1999 r. o ochr. informacji niejawnych**
- **U. z dnia 27 lipca 2001 r. o ochr. baz danych**

- U. z dnia 18 września 2001 r. o podpisie elektronicznym
- U. z dnia 5 lipca 2002 r. o ochr. niektórych usług świadczonych drogą elektroniczną
- U. z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną
- U. z dnia 16 lipca 2004 r. Prawo telekomunikacyjne

- Rozporządzenie Prezesa Rady Ministrów z dnia 25 sierpnia 2005 r. definiujące podstawowe wymagania dot. bezp. teleinformatycznego

Bezpieczeństwo
Standardy UE

T. Lukaszewski

- Dyrektywy Parlamentu Europejskiego i Rady UE,
- Rezolucja Rady UE z 28.01.2002r w sprawie bezpieczeństwa informacji i sieci teleinformatycznych,
- Decyzje Komisji UE z 29.11.2001r w sprawie zasad i procedur bezpieczeństwa w ochronie informacji i sieci teleinformatycznych,
- Ramowa Propozycja Decyzji Komisji UE z 19.04.2002r w sprawie ataków na systemy informatyczne,
- standard ISO-15408 określający wymogi bezpieczeństwa systemów informatycznych,
- **standard ISO/IEC 17799**

Bezpieczeństwo
Standard x7799

T. Lukaszewski

- (UK)BS 7799 – brytyjska norma zarządzania bezpieczeństwem informacji
  - BS 7799-1: opis zalecanych zabezpieczeń (**wytyczne**)
  - BS 7799-2: podstawa nadawania certyfikatów „Systemom Zarządzania Bezpieczeństwem Informacji" (**wymagania**)

- (EU) ISO/IEC 17799:2000 (odpowiednik BS 7799-1)

- (PL) PN-I-13335-1: Technika informatyczna – Wytyczne do zarządzania bezpieczeństwem systemów informatycznych, PKN, styczeń 1999
- (PL) PN-ISO/IEC17799:2003 „Technika informatyczna. Praktyczne zasady zarządzania bezpieczeństwem informacji" (tłumaczenie ISO)
- (PL) PN-I-07799:2005 „Systemy zarządzania bezpieczeństwem informacji. Część 2: Specyfikacja i wytyczne do stosowania." (wg. BS 7799-2)

Zagrożenia, Podatności, Ataki

T. Lukaszewski

Zagrożenia Podatności Ataki

III 2010

Microsoft Official Course 2810A: Fundamentals of Network Security

Zagrożenia, Podatności, Ataki
Źródła zagrożeń

T. Lukaszewski

Źródła zagrożeń (**Network Security Threads**):

- **błędy w systemach, technologiach** (protokół TCP/IP, systemy operacyjne, ochrona haseł, brak uwierzytelniania)
- **zła konfiguracja** (ujawnianie informacji o kontach, proste hasła, niebezpieczne ustawienia domyślne)
- **niedostateczne przeszkolenie użytkowników, brak odpowiedniej polityki bezpieczeństwa** (brak polityki, brak lub błędna kontrola dostępu, nieprzestrzeganie zasad, brak planów na wypadek katastrof)

Zagrożenia, Podatności, Ataki
Rodzaje zagrożeń

T. Lukaszewski

- **przejęcie dokumentów i danych**
- **wprowadzenie nieprawdziwych danych do systemu**
- **niszczenie danych**

- **uzyskanie nieautoryzowanego dostępu** (ataki na hasła, social engineering, wykorzystanie błędów protokołów systemów konfiguracji)
- **podszywanie się pod użytkowników, przechwycenie sesji**
- **zmiany konfiguracji serwerów i urządzeń sieciowych**

- **blokowanie komputerów lub poszczególnych usług (DoS)**
- **zainfekowanie systemu szkodliwymi programami**

Zagrożenia, Podatności, Ataki
Konsekwencje zagrożeń

T. Lukaszewski

- ośmieszenie i utrata zaufania klientów i firm współpracujących
- utrata lub zniszczenie istotnych dla firmy danych
- kradzież poufnych dokumentów dotyczących działania firmy
- kradzież nowych technologii
- przerwa w działaniu istotnych systemów informatycznych firmy
- bankructwo firmy

Zagrożenia, Podatności, Ataki
Podatności

T. Lukaszewski

Source	Example vulnerabilities
Users	• Sharing passwords or using weak passwords • Not understanding or ignoring security policies • Opening e-mail, visiting Web sites, or downloading software that contains malicious code • Being manipulated into violating security policies
Network administrators	• Misconfiguring services and not patching preinstalled software • Not adequately securing network access accounts • Not adequately securing physical access to hardware • Ignoring security policies
Software	• Using operating systems and applications that have design flaws that make them accessible to manipulation by attackers

Zagrożenia, Podatności, Ataki
Klasy i rodzaje ataków

T. Lukaszewski

Klasy ataków:

- Ataki pasywne/aktywne
- Ataki lokalne/zdalne

Podstawowe rodzaje ataków:

- Ataki rozpoznawcze – zazwyczaj wstęp dla dwóch pozostałych
- Ataki w celu uzyskania (nieautoryzowanego) dostępu
- Ataki w celu zablokowania usługi (ataki DoS)

Zagrożenia, Podatności, Ataki
Formy ataków

T. Lukaszewski

Formy ataków:

- podszywanie się (masqueradi ng)
- podsłuch (eavesdropping)
- odtwarzanie (replaying)
- manipulacja (tampering)
- wykorzystywanie luk w systemie (exploiting)

Zagrożenia, Podatności, Ataki
www.symantec.com

T. Lukaszewski

Vulnerabilities View all Vulnerabilities

Severity	Name	Discovered
	Microsoft IIS Repeated Parameter Request Denial of Service Vulnerability	09/14/2010
	Adobe Flash Player CVE-2010-2884 Unspecified Remote Code Execution Vulnerability	09/13/2010
	Microsoft Windows and Office Uniscribe Font Parsing Engine Remote Code Execution...	09/14/2010
	Sun Java SE November 2009 Multiple Security Vulnerabilities	10/29/2009
	Microsoft Silverlight & .NET Framework CLR Virtual Method Delegate Code Executio...	08/10/2010
	Microsoft Silverlight ActiveX Control Pointer Memory Corruption Vulnerability	08/10/2010
	Microsoft Excel SxView Record Parsing Memory Corruption Remote Code Execution Vu...	06/08/2010
	Microsoft Windows Print Spooler Service Remote Code Execution Vulnerability	09/14/2010
	Microsoft Windows Cinepak Codec Media Decompression Remote Code Execution Vulner...	08/10/2010

Inicjatywy na rzecz bezpieczeństwa

III 2010

Inicjatywy na rzecz bezpieczeństwa 2004

Jesień 2004

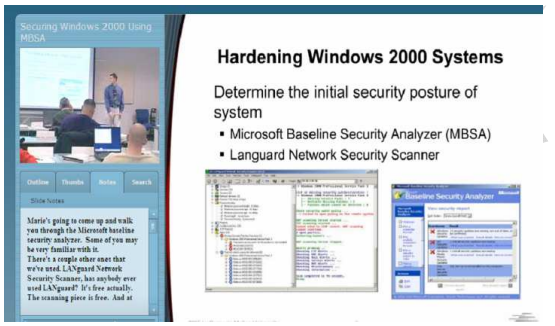
- Centrum bezpieczeństwa Microsoftu
  - Informowanie i edukacja
  - Infolinia 0 801 802 000
- Projekt Bezpieczny Komputer
  - Microsoft, Intel, Symantec, G DATA RSA
  - Cykl szkoleń
- Akademia Bezpieczeństwa
  - Cykl szkoleń
- Strażnik systemu (1 edycja)

Inicjatywy na rzecz bezpieczeństwa DBI: 2005 -2010

Dzień Bezpiecznego Internetu

- Inicjatywa Komisji Europejskiej
- Bezpieczny dostęp dzieci i młodzieży do Internetu

Inicjatywy na rzecz bezpieczeństwa vte.cert.org



Inicjatywy na rzecz bezpieczeństwa inne

- www.saferinternet.pl
- www.dzienbezpiecznegokomputera.pl
- bezpiecznykomputer.pl
- www.centrumxp.pl
- niebezpiecznik.pl
- scan.sygate.com
- www.symantec.com/securitycheck
- browsercheck.qualys.com
- www.startup-it.pl

- **Programy destrukcyjne są coraz bardziej wyrafinowane**, łączą cechy wirusów, robaków i trojanów
- **Bezpieczeństwo** to poziom zabezpieczenia przed nieautoryzowanym dostępem
- **Elementy bezpieczeństwa**: (CIA) poufność, integralność, dostępność (AAN) uwierzytelnianie, autoryzacja, niezaprzeczalność
- **Standardy bezpieczeństwa** bazują na BS 7799
- **Źródła zagrożeń**: błędy produktu, konfiguracji, brak szkoleń
- **Formy ataków**: podszywanie się, podsłuch, odtwarzanie, manipulacja, wykorzystanie luk