



Sieci komputerowe

Wykład 7
24.04.2019

dr inż. Łukasz Graczykowski
lukasz.graczykowski@pw.edu.pl

Semestr letni 2018/2019



Bezpieczeństwo

“Hacker” a “cracker”

- **Hacker** to osoba czasami znana z imienia i nazwiska, pasjonat, entuzjasta, zajmuje się badaniem działania oprogramowania i szukaniem błędów, nie tworzy szkód i informuje administratorów
- **Cracker** to z kolei osoba, której celem jest działanie destrukcyjne, w celu osiągnięcia korzyści



Black Hats
Individuals with extraordinary computing skills, resorting to malicious or destructive activities. Also known as **crackers**



White Hats
Individuals professing hacker skills and using them for defensive purposes. Also known as **security analysts**

Provided by : www.isoftdl.com



Gray Hats
Individuals who work both offensively and defensively at various times



Suicide Hackers
Individuals who will aim to bring down critical infrastructure for a "cause" and not worry about facing 30 years in jail for their actions

Ochrona danych

- Ochrona danych musi zapewniać:
 - **poufność** – nikt nieuprawniony nie ma swobodnego dostępu do danych
 - **uwierzytelnianie** – zagwarantowanie autentyczności pochodzenia informacji
 - **nienaruszalność** – zapewnienie integralności informacji
 - **niezaprzeczalność** – niepodważalność faktu przekazania danych
 - **kontrolę dostępu** – przykładowo na podstawie loginów i haseł
 - **dyspozycyjność** – zapewnienie ciągłej dyspozycyjności

Polityka bezpieczeństwa

- W każdej szanującej się firmie powinien istnieć dokument **“Polityka bezpieczeństwa”**
 - określa, co w firmie powinno być chronione i jakimi metodami
 - powinien definiować procedury postępowania w razie awarii czy włamania
 - powinien być zgodny z normami prawnymi, np. PN-EN ISO/IEC 27001:2017-06
- Równie ważne jest również przestrzeganie ww. dokumentu
 - trzeba wyznaczyć osobę lub osoby odpowiedzialne za wdrażanie dokumentu
 - jasne konsekwencje jego nieprzestrzegania
- Przykładowo – co się stanie w przypadku awarii klimatyzatora w serwerowni?

Poziom bezpieczeństwa



Politechnika Krakowska
ul. Warszawska 24
31-155 Kraków

Polityka bezpieczeństwa IT na Politechnice Krakowskiej

Załącznik do Zarządzenia nr 20 Rektora PK z dnia 17 kwietnia 2018 r.

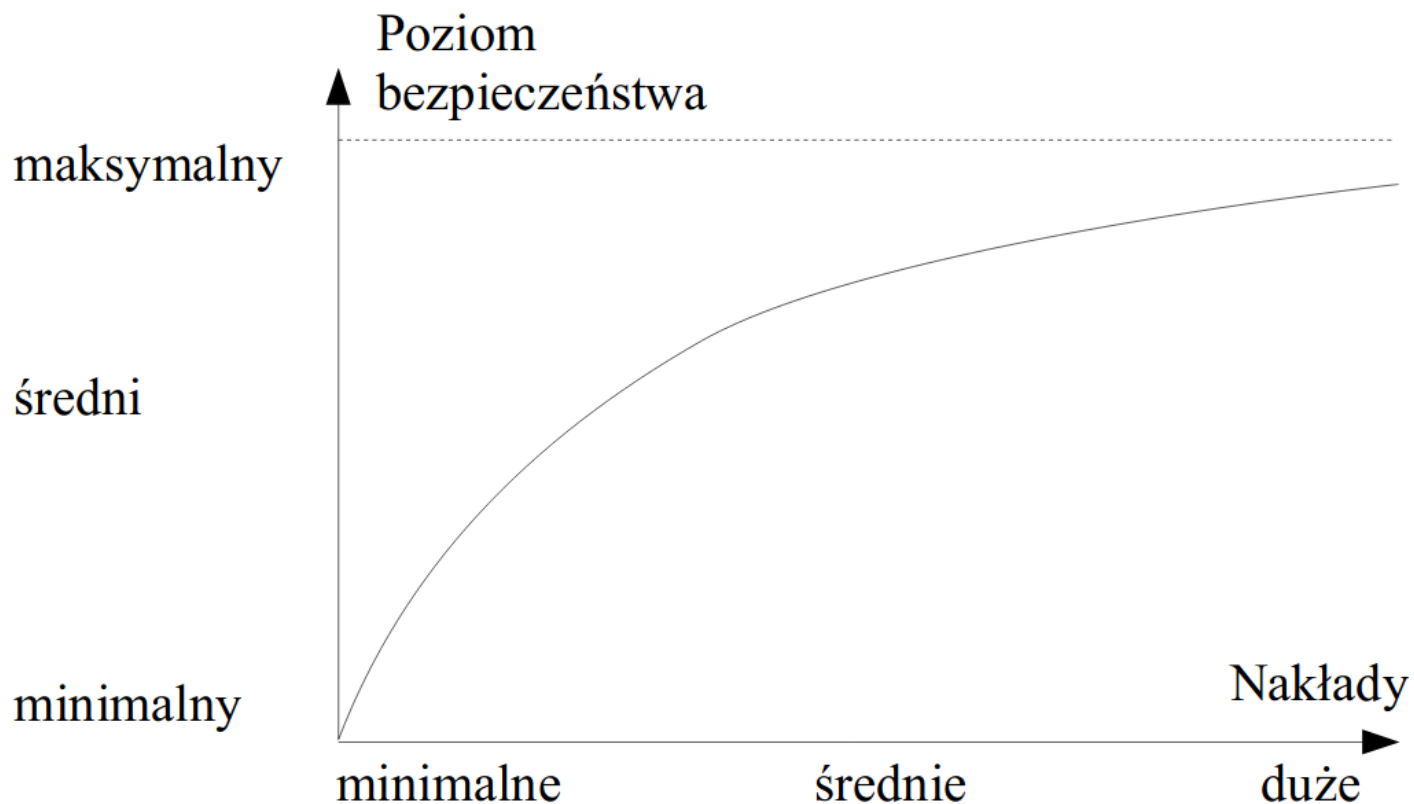
- Nie znalazłem na PW...
 - trzeba pewnie dokładniej przejrzeć Biuletyn Informacji Publicznej PW

Spis treści

1. Zakres Polityki	4
2. Słownik pojęć	6
3. Ogólne zasady zarządzania bezpieczeństwem informacji	9
4. Odpowiedzialność za bezpieczeństwo aktywów informacyjnych	11
5. Działania związane z oceną i doskonaleniem mechanizmów ochrony aktywów informacyjnych	15
6. Zarządzanie aktywami informacyjnymi i ich klasyfikacja	16
6.1. Zarządzanie sprzętem	16
6.2. Zarządzanie oprogramowaniem	17
6.3. Klasyfikacja systemów informatycznych	17
7. Określenie i realizacja zasad współpracy z podmiotami zewnętrznymi z uwzględnieniem ochrony aktywów informacyjnych	19
8. Bezpieczeństwo fizyczne i środowiskowe	20
9. Określenie i stosowanie standardów bezpieczeństwa systemów informatycznych	23
9.1. Standard bezpieczeństwa Microsoft Windows	23
9.2. Standard bezpieczeństwa Linux	24
9.3. Standard bezpieczeństwa OS X	26
9.4. Redundantność komponentów	27
9.5. Standard bezpieczeństwa aplikacji	27
10. Zarządzanie zmianami, w tym testowanie i akceptacja zmian	29
11. Zarządzanie cyklem życia systemów informacyjnych w aspekcie ich bezpieczeństwa	30
12. Zarządzanie pojemnością infrastruktury informatycznej	33
13. Zarządzanie kopiami zapasowymi	34
14. Ochrona przed niebezpiecznym oprogramowaniem, w tym niebezpiecznymi kodami mobilnymi	35
15. Bezpieczeństwo sieci informatycznych	37
16. Zarządzanie nośnikami informacji: wytwarzanie, inwentaryzacja, kontrola, przechowywanie, użytkowanie, niszczenie	39
16.1. Elektroniczne nośniki przenośne	39
16.2. Nośniki elektroniczne wbudowane w sprzęt informatyczny	39
16.3. Wydruk dokumentów papierowych	39
17. Bezpieczna wymiana informacji	40
18. Monitorowanie i rozliczalność operacji związanych z przetwarzaniem informacji	41
19. Zarządzanie dostępem do informacji	42
19.1. Nadawanie uprawnień	42
19.2. Odbieranie uprawnień	43
19.3. Przegląd uprawnień	43
20. Ochrona komputerów przenośnych	44
21. Bezpieczna realizacja zdalnego dostępu	45
22. Mechanizmy techniczne i organizacyjne zapewniające integralność danych	46
23. Zarządzanie incydentami naruszenia bezpieczeństwa informacji ...	47
24. Zarządzanie ciągłością działania	49
25. Działania kontrolne	50

Poziom bezpieczeństwa

- Poziom bezpieczeństwa jest nieproporcjonalny do poniesionych nakładów
- Minimalne nakłady początkowo powodują znaczące zwiększenie poziomu bezpieczeństwa
- **Nigdy nie da się osiągnąć 100% poziomu bezpieczeństwa**



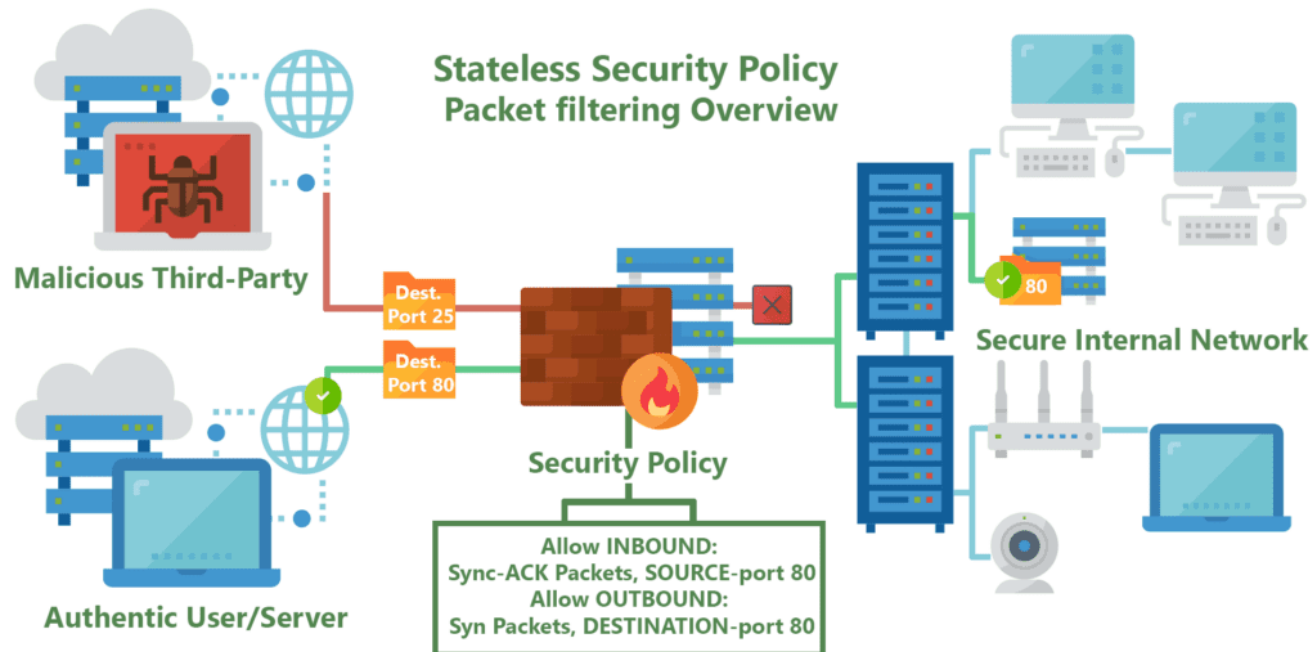
Warstwy TCP/IP a bezpieczeństwo

- W analizie bezpieczeństwa można się oprzeć na warstwach TCP/IP
- Możemy dodać dwie warstwy: zasoby fizyczne oraz człowiek
 - nawet komputer odłączony od sieci może paść ofiarą ataku lub awarii! (np. sprzątaczką z wodą i zalanie)

Warstwa	Przykłady zagrożeń/ataków
Zasoby fizyczne	Awaria zasilania, zalanie, pożar, przegrzanie, włamanie lub kradzież, uszkodzenia łączy, nieuprawniony dostęp fizyczny do sprzętu lub infrastruktury
Warstwa dostępu do sieci	Sniffing, arp-spoofing, mac-flooding
Warstwa Internetu	Spoofing, icmp-redirect, icmp-flood
Warstwa transportowa	Skanowanie, DoS, DDoS, DNS-spoofing
Warstwa aplikacji	Buffer overflow, string formatting, SQL injection, wirusy, konie trojańskie, robaki, błędy w skryptach, backdoor
Człowiek	Social engineering, „hasło pod klawiaturą”, nieuwaga

Firewall

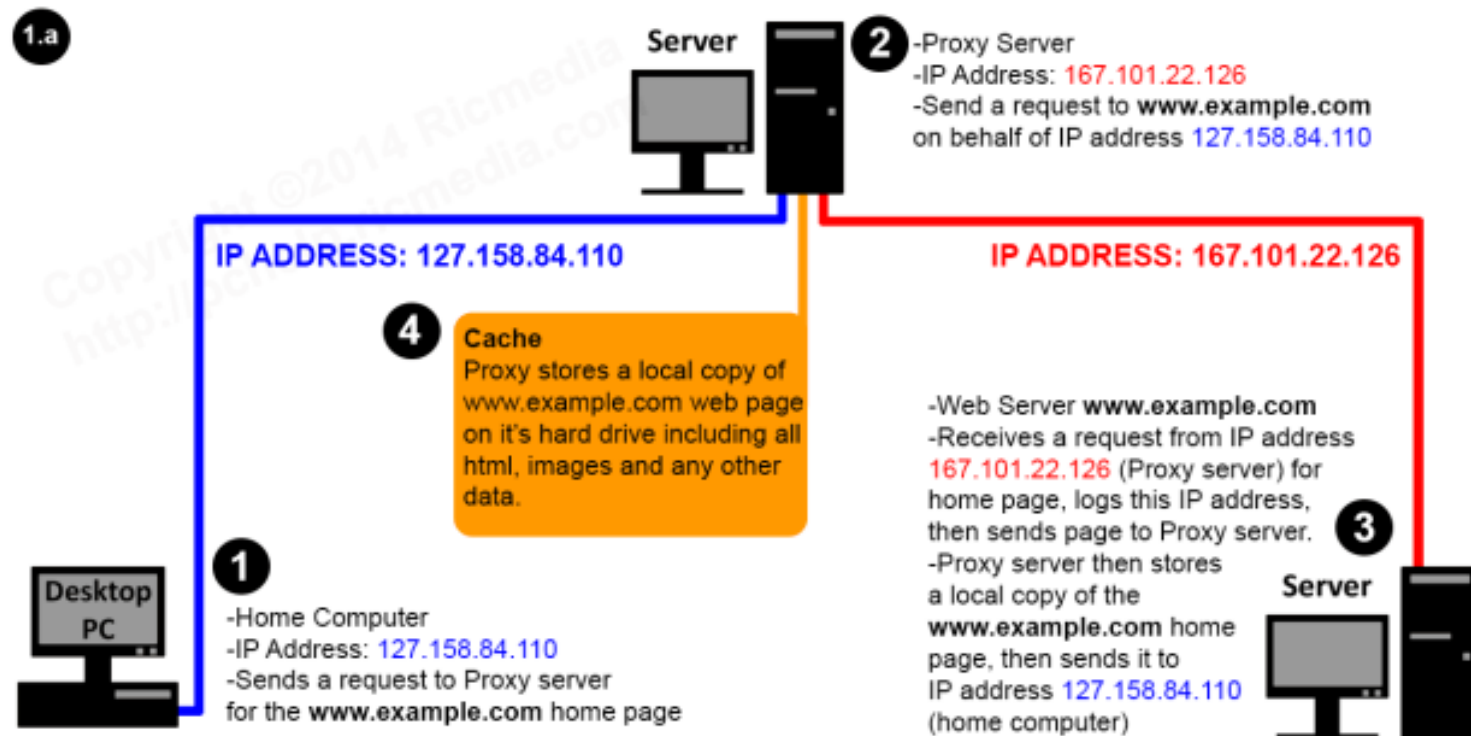
- **Firewall** (*zapora ogniowa*) – zabezpieczenie przed próbą podłączenia się do zasobów, które nie powinny być udostępnione:
 - **filtrujący** – działa w warstwie Internetu na poziomie IP; na podstawie numeru IP oraz numeru portu przepuszcza lub nie dany datagram; wadą jest brak kontroli użytkownika, ale bardziej zaawansowane **firewalle z inspekcją stanu** (*statefull inspection*) mogą kontrolować całą sesję i korzystają również z wyższych warstw



Firewall

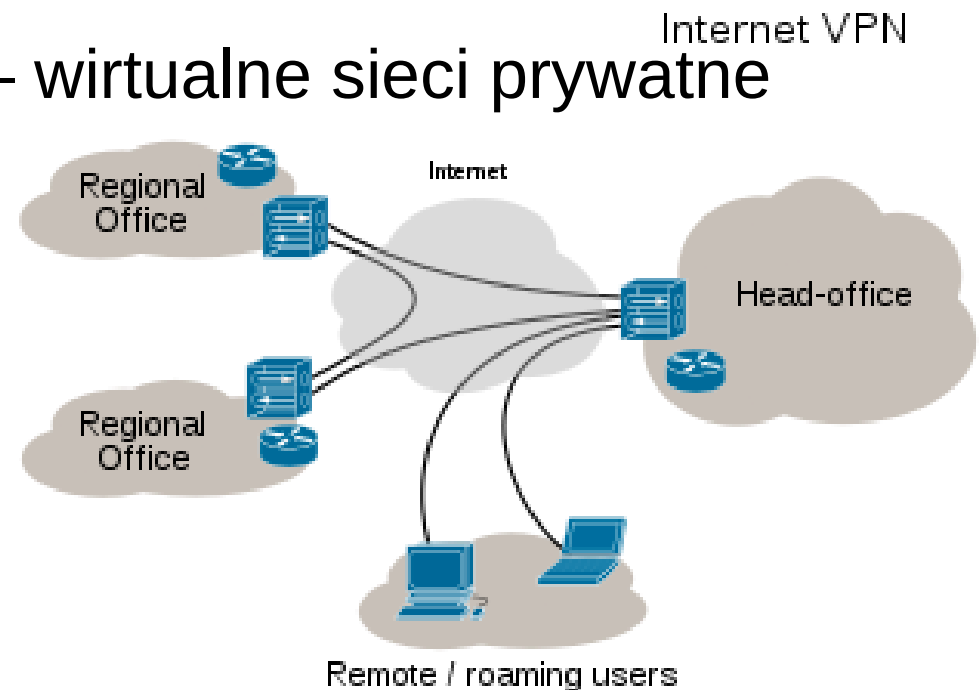
- **połączeniowy** – zestawiają połączenia pomiędzy siecią lokalną a Internetem wg określonych reguł, np. poprzez *serwery proxy*
- **Serwer połączeniowy (proxy)** – wykonują połączenia sieciowe zamiast komputera sieci lokalnej; najczęściej udostępnianie WWW, ale możliwe też inne usługi (uwaga na strony dynamiczne, np. PHP)

Web Proxy Server



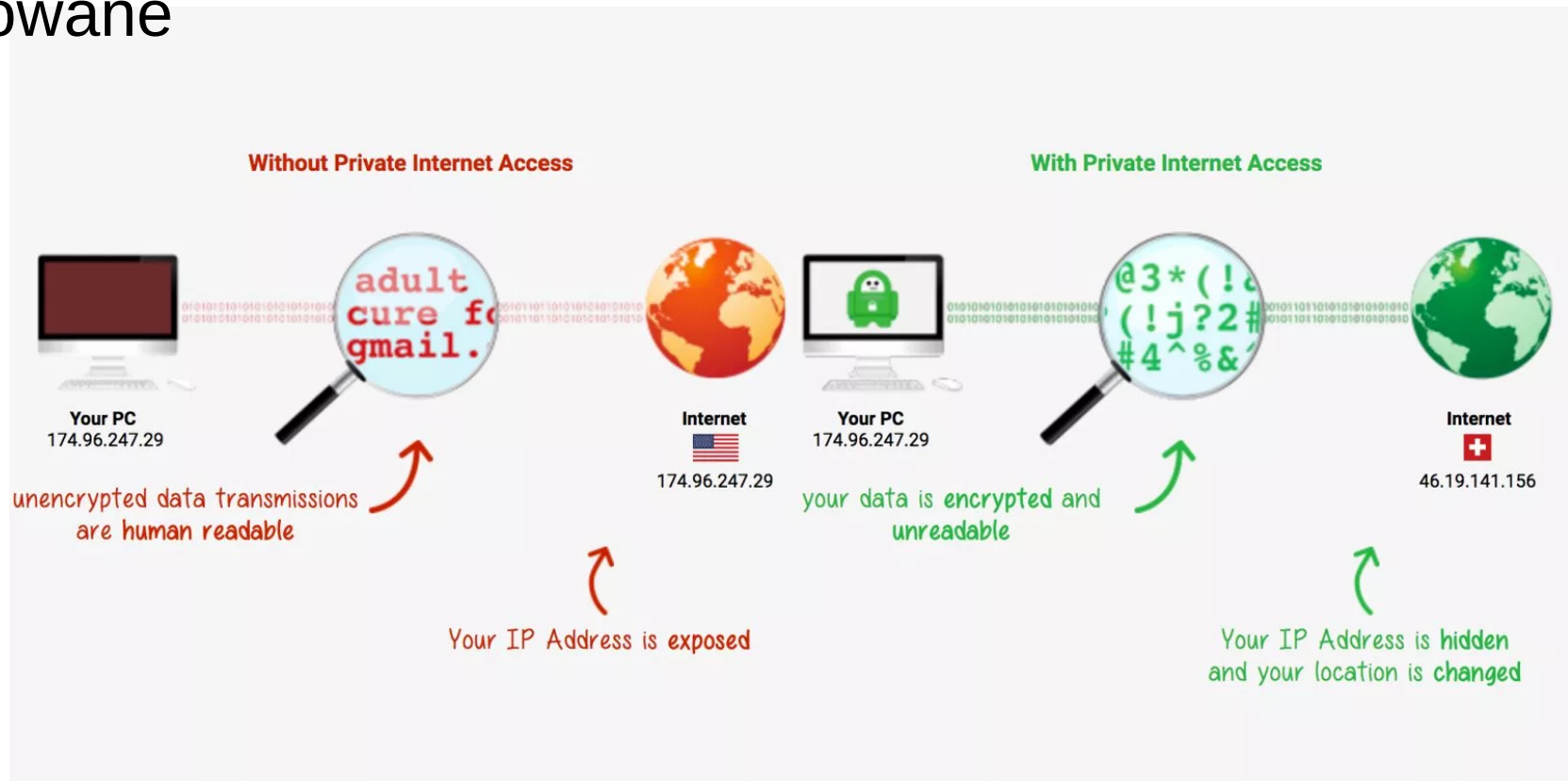
Inne technologie bezpieczeństwa

- **NAT** – to już znamy, translacja adresów IP sieci wewnętrznej i adresy nieroutowalne – sieć lokalna widoczna pod zupełnie innymi adresami
 - ataki na sieć lokalną zostaną “przejęte” przez serwer NAT, który powinien być lepiej zabezpieczony niż komputery klienckie
- **Kryptografia** – szyfrowanie połączeń oraz wiadomości (w tym klucze publiczne i prywatne, certyfikaty)
- **VPN** (*Virtual Private Network*) – wirtualne sieci prywatne



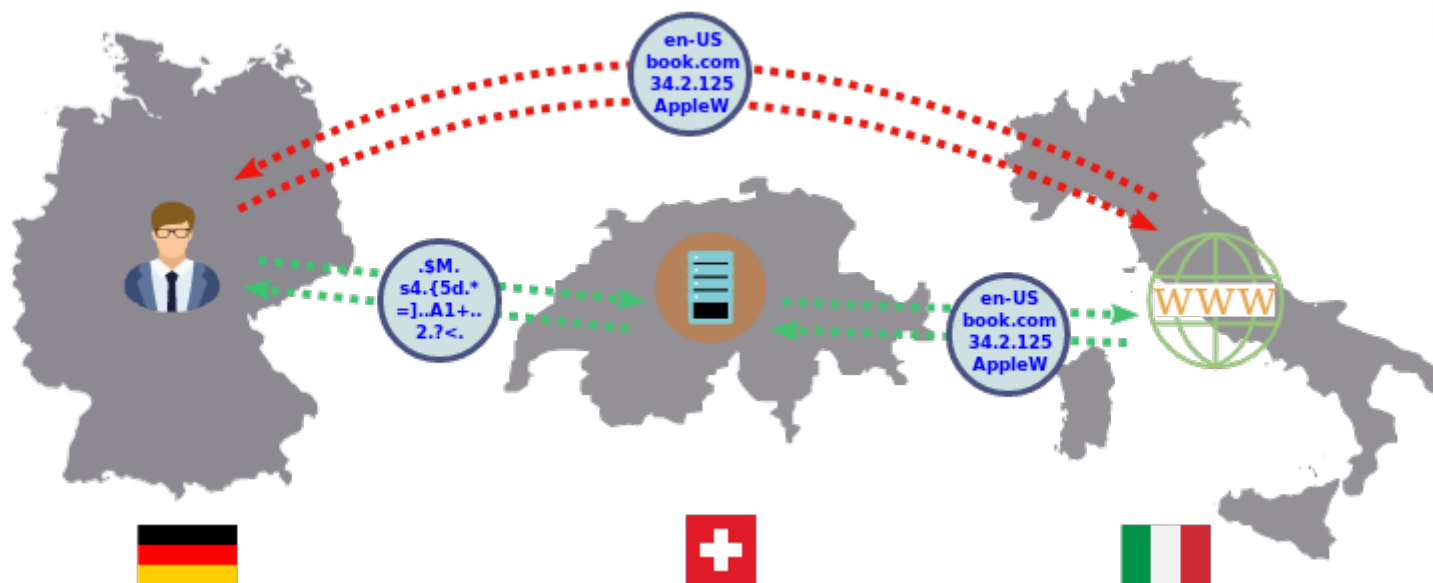
VPN

- **VPN** (*Virtual Private Network*) – wirtualne sieci prywatne, sieć transmitująca prywatne dane przez infrastrukturę telekomunikacyjną – z reguły taka usługa u operatora kosztuje; dostawca usług wydziela w swojej sieci połączenie (między naszymi routerami granicznymi), które będzie należało do nas i to od nas zależy co i jak prześlemy – połączenie z VPN szyfrowane



VPN

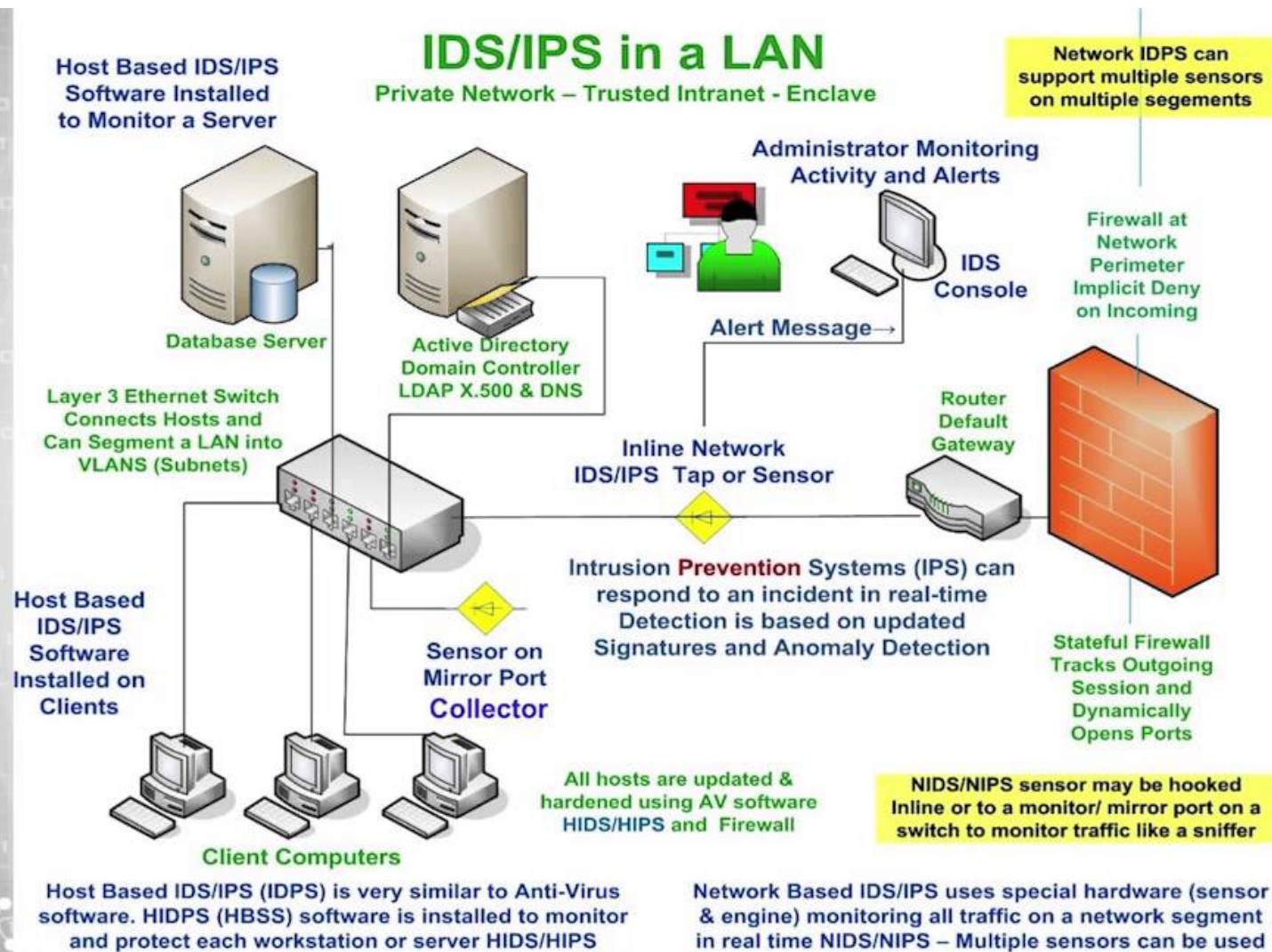
- Istnieje wiele firm, gdzie możemy wykupić usługę VPN, np. NordVPN ostatnio reklamowany



IDS i IPS

- **IDS** (*Intrusion Detection System*) – urządzenie lub program służący do wykrywania prób włamań do zasobów chronionych; np. złodzieje mogą wykorzystywać luki w oprogramowaniu (np. w naszym firewall). Dzielimy je na kilka rodzajów:
 - **Host IDS** (*systemowy IDS*) – analizuje pracę systemu operacyjnego
 - **Network IDS** (*sielowy IDS*) – analizuje ruch sieciowy i wykrywa odstępstwa
 - **Network Node IDS** (*IDS stacji sieciowej*) – system instalowany na poszczególnych stacjach sieciowych i analizuje jedynie ruch na tej stacji, najczęściej stosowany w VPN
- **IPS** (*Intrusion Prevention System*) – system aktywnej reakcji na ataki i następnie raportują co się stało (człowiek nie jest w stanie odpowiednio szybko zareagować)

IDS i IPS



Wirusy

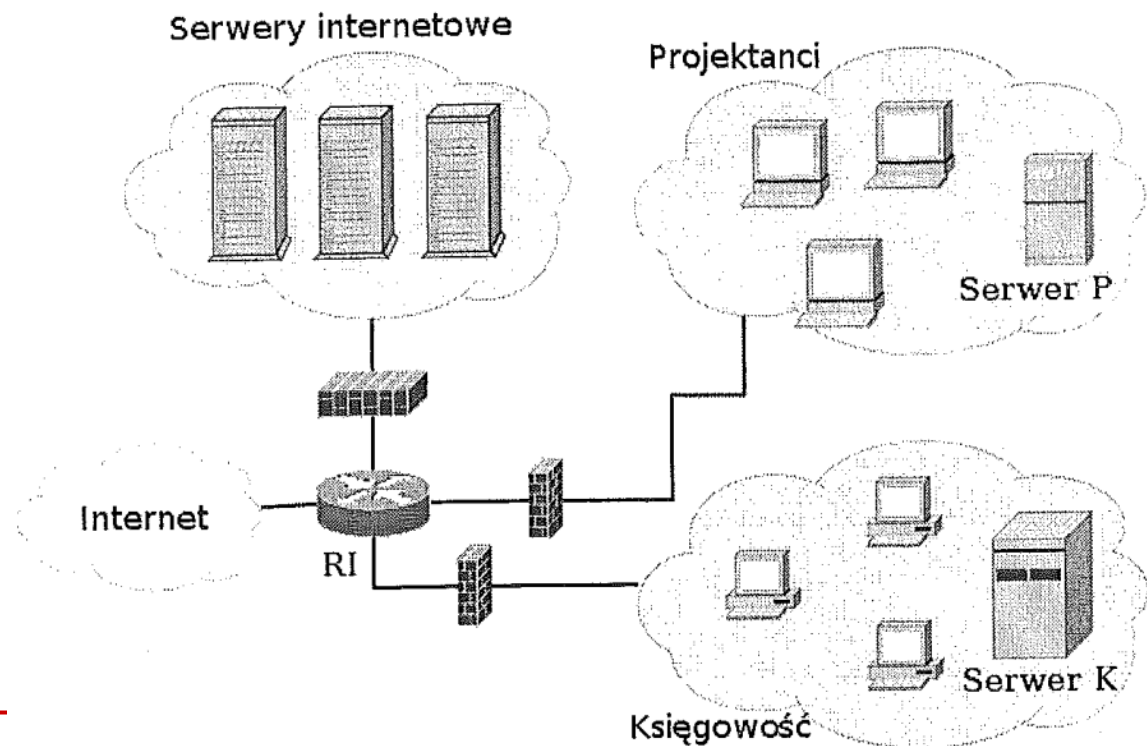
- Systemy zabezpieczeń stają się coraz bardziej doskonałe, coraz lepsi są administratorzy → trudno włamać się do sieci wewnętrznej
- Po co się trudzić, skoro można np. napisać e-mail do pracownika z nazwą typu (patrz Helion) *hot_girl.jpg.exe*
- W takim przypadku cracker opanowuje maszynę w sieci lokalnej **od wewnątrz** a słabym ogniwem jest czynnik ludzki
- W polityce bezpieczeństwa powinniśmy mieć zapisane i egzekwowane, że każdy pracownik na służbowej maszynie posiada aktualne oprogramowanie antywirusowe
- Oprogramowanie antywirusowe należy też instalować (i regularnie uaktualniać) na serwerach pocztowych

Zasady bezpiecznej konfiguracji

- System operacyjny z kontrolą dostępu, różnymi uprawnieniami dla użytkowników, grup użytkowników, kontrola dostępu do systemu plików
- Do zdalnych połączeń tylko szyfrowane protokoły (np. SSH)
- Minimalizacja programów niezbędnych do pracy na komputerze (tylko to co konieczne)
- Częste i regularne aktualizacje oprogramowania
- Serwer nigdy nie służy do pracy indywidualnej (np. przeglądania stron WWW)
 - nie odpalamy przeglądarki na serwerze
- Każda usługa sieciowa precyzyjnie konfigurowana – modyfikujemy domyślne ustawienia
- Przynajmniej na serwerze: firewall, IDS, backup, logi aktywności

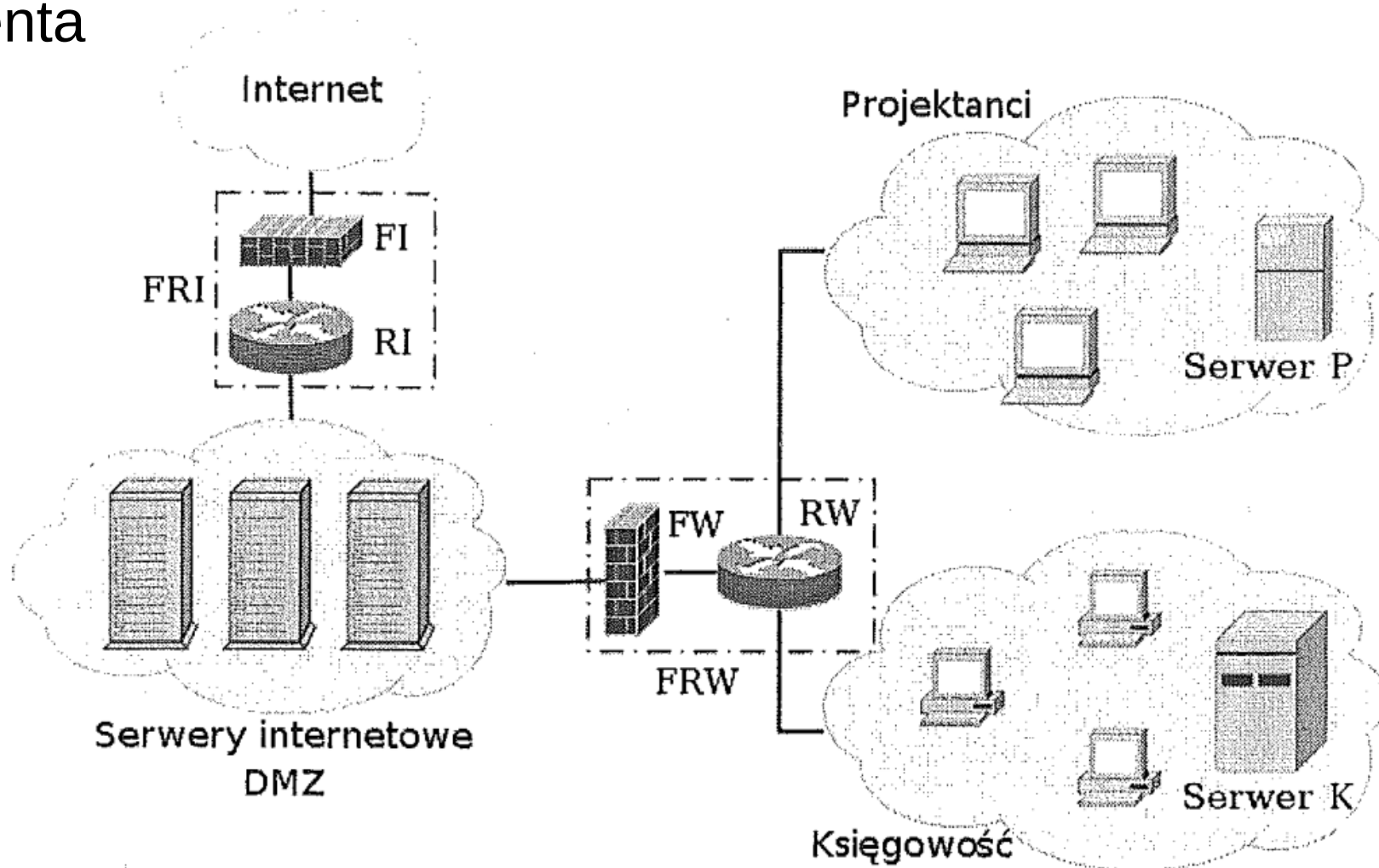
Projektowanie sieci

- Dzielimy sieć na wiele logicznych podukładów (np. Księgowość, dział IT, itp.)
- Poszczególne działy są w różny sposób narażone, inne są też konsekwencje incydentów
- Można wyodrębnić też strefy (jeden lub kilka działów) o różnym poziomie zabezpieczeń w zależności od ryzyka oraz wagi przechowywanych danych – można je oddzielić wewnętrznymi firewallami i IDS'ami



Projektowanie sieci

- Schemat, w zależności od potrzeb i dostępnych środków można modyfikować, np. wprowadzając dwie zapory po drodze do klienta



Ataki – rozpoznanie sieci

Założmy, że chcemy włamać się do sieci wewnętrznej firmy XYZ

- 1) Analiza zasobów Internetowych** (strony oficjalne, fora internetowe – może np. na forum ktoś szukał pomocy o systemie operacyjnym → wiemy czego używają) → obrona: **zdrowy rozsądek**
- 2) Inżynieria społeczna** – podszywanie się pod osoby upoważnione i uzyskiwanie dostępu do sieci (np. telefon do jakiegoś działu i prośba o hasło) → obrona: **zdrowy rozsądek i szkolenie pracowników**
- 3) Analiza DNS i użycie whois** – można dzięki temu znaleźć zakres IP przydzielonych firmie, dane administratora czy dostawcę Internetu
- 4) Mapowanie sieci** – uzyskiwanie listy aktywnych numerów IP i topologii połączeń poprzez ICMP (ping) oraz tracerout → obrona: blokowanie ICMP, IDS

Ataki – rozpoznanie sieci

Założmy, że chcemy włamać się do sieci wewnętrznej firmy XYZ

5) Skanowanie portów – próba ustalenia na których portach TCP/UDP nasłuchują procesy serwów → obrona: **konfiguracja serwerów, IDS**

- Szczegółowe metody – podręcznik

sieci komputerowe

Wydanie II



Kompendium

Kompletne omówienie zagadnień sieci komputerowych

▽ Topologie i nośniki

▽ Sieci bezprzewodowe

▽ Usługi sieciowe i protokoły

▽ Administrowanie siecią

▽ Bezpieczeństwo w sieciach

Karol Krysiak

Helion 

Ataki – identyfikacja systemu operacyjnego

- W wyniku rozpoznania sieci zwykle wybrany zostaje cel ataku (konkretna maszyna)
- Następnie następuje szczegółowa analiza danego urządzenia, w tym identyfikacja systemu operacyjnego (*fingerprinting*):
 - **Winiетки** (*banners*) – zwracane przez usługi sieciowe informacje, np.:

```
# telnet www.pewna.domena.pl 80
Trying 192.168.1.1...
Connected to pewna.domena.pl.
Escape character is '^]'.
dsdsbleble
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<HTML><HEAD>
<TITLE>501 Method Not Implemented</TITLE>
</HEAD><BODY>
<H1>Method Not Implemented</H1>
dsds to /index.html not supported.<P>
Invalid method in request dsds<P>
<HR>
<ADDRESS>Apache/1.3.20 Server at www.pewna.domena.pl Port 80</ADDRESS>
</BODY></HTML>
Connection closed by foreign host.
```

Drugim łatwym sposobem jest wykorzystanie polecenia netcat:

```
# nc 192.168.1.1 22
SSH-1.99-3.1.0 SSH Secure Shell (non-commercial)
```

Ataki – identyfikacja systemu operacyjnego

- Następnie następuje szczegółowa analiza danego urządzenia, w tym identyfikacja systemu operacyjnego (*fingerprinting*):
 - **Winiетки (banners)** – zwracane przez usługi sieciowe informacje → obrona: **usunięcie zbędnych informacji**
 - Analiza implementacji protokołu TCP/IP – czyli implementacji funkcjonalności, które nie zostały dostatecznie szczegółowo zdefiniowane, lub są zaimplementowane błędnie (np. niedokładności implementacji RFC, nieprzestrzeganie wytycznych przez programistów narzędzi)
 - przykładowo w nagłówku IP istnieje pole TTL (time to live) – odległość jaką może przebyć pakiet w sieci – każdy kolejny router zmniejsza to pole o 1 i gdy osiągnie 0 jest usuwany. Nigdzie nie zostało zdefiniowane jaka powinna być początkowa wartość, np. Linux używa 64 a Windows 128
- Mając wirusa, możemy też podsłuchać ruch z/do systemu

Ataki – włamanie do sieci lub systemu

- **Uzyskiwanie kombinacji login-hasło:**
 - Inżynieria społeczna – hasła oparte na powszechnie dostępnych danych personalnych, “hasło pod klawiaturą”, itp.
 - Metoda brute-force (sprawdzenie wszystkich możliwości) – tylko dla prostych haseł
 - Podśluchiwanie ruchu – hasła wysyłane w postaci otwartej
- **Wykorzystanie “backdoors”:**
 - umieszczenie w serwerze metody uzyskiwania hasła
 - specjalne programy zainstalowane w trakcie włamania
- **“Exploits” - błędy w oprogramowaniu:**
 - “buffer overflow”, “string formatting” - zmiana kodu programu przez wysyłane dane
 - “SQL injection” - skłonienie serwera bazy danych do wyświetlenia informacji z bazy danych

Ataki – “Spoofing”

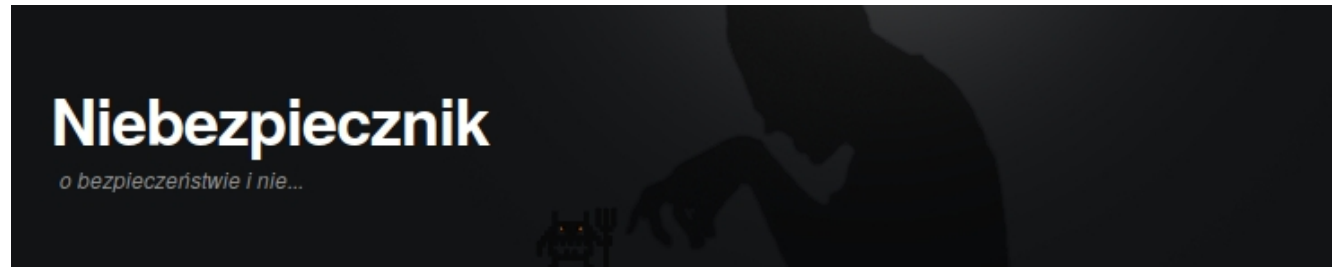
- **Spoofing** – podszywanie się pod inną osobę/system/proces w celu przejęcia informacji/sesji/komunikacji
 - ARP spoofing – komunikacja na dany numer IP jest wysyłana na inny adres
 - TCP spoofing – próba włączenia się lub nawiązania połączenia TCP, tak aby przejąć transmisję informacji
 - “man-in-the-middle” - próba przekierowania połączenia tak, aby przebiegało przez podsłuchujący system (to już omówiliśmy mówiąc o WiFi)
 - DNS spoofing – podanie fałszywej odpowiedzi serwera DNS i przejęcie połączenia do danego hosta

Ataki – destabilizacja pracy

- Czasami następuje nie tyle włamanie się do systemu czy sieci, a zakłócenie ich pracy:
 - pochłanianie pasma (zabieranie części docierających informacji)
 - pochłanianie zasobów – np. inicjowanie dużej ilości połączeń TCP
 - Ataki na DNS (wysyłanie ogromnej ilości pytań do DNS i przepełnienie buforów)
 - unieruchomianie serwerów przez wykorzystanie błędów w implementacji usług sieciowych
 - Denial of Service (DoS) i Distributed Denial of Service (DDoS) – skoordynowana akcja jednego (DoS) lub wielu komputerów (DDoS) zalewająca serwer/sieć ogromną ilością informacji/zapytań

Ataki – bezpieczeństwo

- Polecam również bieżącą lekturę strony niebezpiecznik.pl



- Najwięcej włamań wynika z błędu ludzkiego (np. Kliknięcia na zły link w e-mailu, czy błędach administratorów)

9:20
18/4/2019 Facebook wyłudził 1,5 mln haseł do e-maili po czym “niechący” wykraść użytkownikom książki kontaktowe

21:01
21.3.2019 Hasła 600 milionów użytkowników Facebooka były dostępne bez szyfrowania. Przez przypadek...

10:52
4.4.2019 Pocięły dane 540 mln użytkowników Facebooka, ale ich administrator nie spieszył się z reakcją

20:40
4.3.2019 [AKTUALIZACJA #2] Rządowy serwis loterii paragonowej serwuje porno w domenie gov.pl i ujawnia masowy, globalny atak na “porzucone” domeny

14:19
3.4.2019 To nie był “wyciek” tylko “błąd ludzki”? Dlaczego warto separować kod od danych

Autor: redakcja | Tagi: Hacked!, loteria paragonowa, pornografia

14:58
28.3.2019 Domyślny PIN umożliwił kradzież 120 tys. litrów paliwa
Autor: Marcin Maj | Tagi: dystrybutory paliwa, Francja, klucze, paliwo, PIN, stacje benzynowe, USA

11:33
25.3.2019 Chcesz oddać lub sprzedać dysk? Nie myśl, że sprzedawca go bezpiecznie wyczyści

Ataki – bezpieczeństwo

20:05
10/2/2019

Jak ukraść miliony z polskich firm jednym e-mailem lub listem?

Tuż przed weekendem **RMF** poinformowało o tym, że należąca do **Polskiej Grupy Zbrojeniowej** spółka **Cenzin** straciła **4 miliony złotych** bo — na podstawie “fałszywego” maila od kontrahenta — pieniądze przelała na złe konto. Ta metoda kradzieży w internecie jest stara jak świat. Na **niebezpiecznikowych szkoleniach dla firm przestrzegamy przed nią** od ponad 9 lat! Ale niestety, tego typu ataki regularnie powracają, a straty prawie zawsze idą w co najmniej **setki tysięcy złotych**. W tym artykule, chciałbym więc zwrócić Wam uwagę na to **jak wykryć tego typu przekręty** oraz co zrobić, żeby Twoja firma nie była kolejną, która pośle miliony złodziejom...

- **560 000** zapłaciło warszawskie metro za usługi sprzątania komuś, kto podszył się pod firmę Impel i “podmienił” numer rachunku sfalszowanym pismem.
- **3,7 miliona złotych** przelał złodziejom Podlaski Zarząd Dróg Wojewódzkich, bo podszyli się pod wykonawcę Unibep i na piśmie z prośbą o zmianę numeru rachunku umieścili pieczętkę, a urzędnicy w pieczętki wierzą...

Nie tylko Polacy mają problemy z takimi oszustwami. Za granicy nazywa się je mianem **Business Email Compromise**, a rekordzistą jest firma z branży ...bezpieczeństwa: **Ubiquiti**. Ten znany producent urządzeń sieciowych **złodziejom przelał aż 46,7 milionów dolarów**. Ciekawy był też **przypadek** firmy Ryanair, która za paliwo zapłaciła 5 milionów euro nie temu, komu powinna.



KONIEC