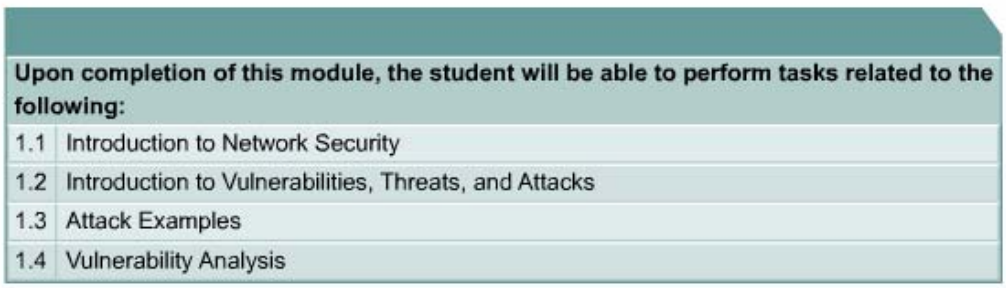
Module 1: Vulnerabilities, Threats, and Attacks

FIGURE 1



Upon completion of this module, the student will be able to perform tasks related to the following:	
1.1	Introduction to Network Security
1.2	Introduction to Vulnerabilities, Threats, and Attacks
1.3	Attack Examples
1.4	Vulnerability Analysis

Uvod

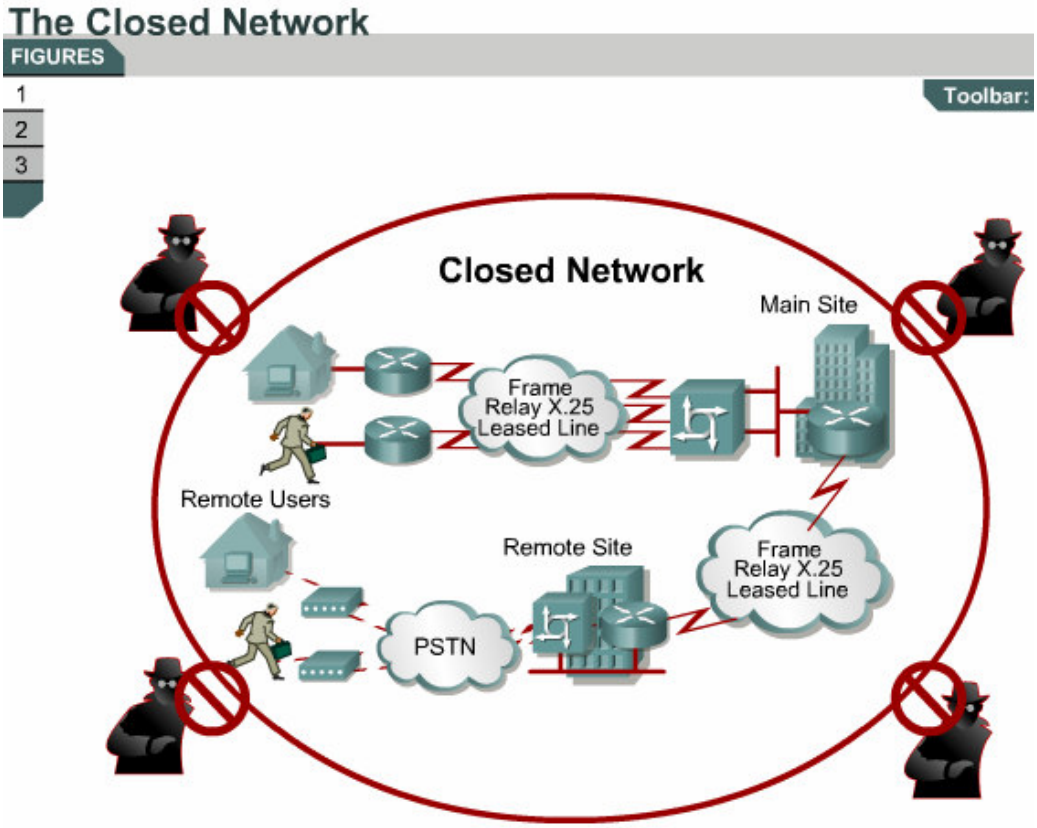
Internet nastavlja rasti eksponencijalno. Zbog toga što osobne, institucionalne i poslovno kritične aplikacije postaju prevladavajuće na internetu, možemo trenutno uočiti velike prednosti takvog pristupa. Ipak ove mrežno orijentirane / bazirane aplikacije i servisi mogu biti pozicije ozbiljnog sigurnosnog rizika za pojedinca kao i za informacijsku bazu poduzeća i vladinih institucija. U mnogim slučajevima, žurba da se konektira na mrežu / internet radi se na račun odgovarajuće mrežne sigurnosti. Informacija je vrijednost koja mora biti zaštićena. Bez odgovarajuće zaštite odnosno mrežne sigurnosti, mnogi pojedinci, poduzeća i institucije su u položaju da izgube tu vrijednost.

Mrežna sigurnost je proces putem kojega je digitalna informacijska vrijednost zaštićena. Cilj mrežne sigurnosti je da zaštiti povjerljivost, zadrži cjelovitost i osigura dostupnost. Imajući to na umu, postavlja se imperativ da sve mreže budu zaštićene od opasnosti i osobnih slabosti da bi poslovanje moglo dosegnuti svoje maksimalne potencijale. Tipično, ove opasnosti su prisutne zbog ranjivosti sustava, što može biti dodatno povećano neodgovarajućim konfiguriranjem sklopovske ili programske podrške, lošom konfiguracijom mreže, slabostima tehnologije koje se ne mogu izbjeći ili neopreznošću krajnjeg korisnika.

1.1. Uvod u mrežnu sigurnost

1.1.1 Potreba za mrežnom sigurnosti

Sigurnost ima jednu osnovnu svrhu, da zaštiti vrijednost. Tijekom povijesti, u većini slučajeva, to je značilo izgraditi snažne zidove koji bi zaustavili „loše dečke“ i ugraditi mala, dobro čuvana, vrata za pristup „dobrim dečkima“. Ta strategija dobro funkcionira za centralizirana mainframe računala u zatvorenim mrežama.



Zatvorena mreža se tipično sastoji od mreže dizajnirane i implementirane u okruženje poduzeća i omogućava spajanje samo poznatim korisnicima bez spajanja na javnu mrežu. Mreže su tako bile građene u prošlosti i imale relativno visok nivo sigurnosti zbog izostanka spoja na vanjske mreže.

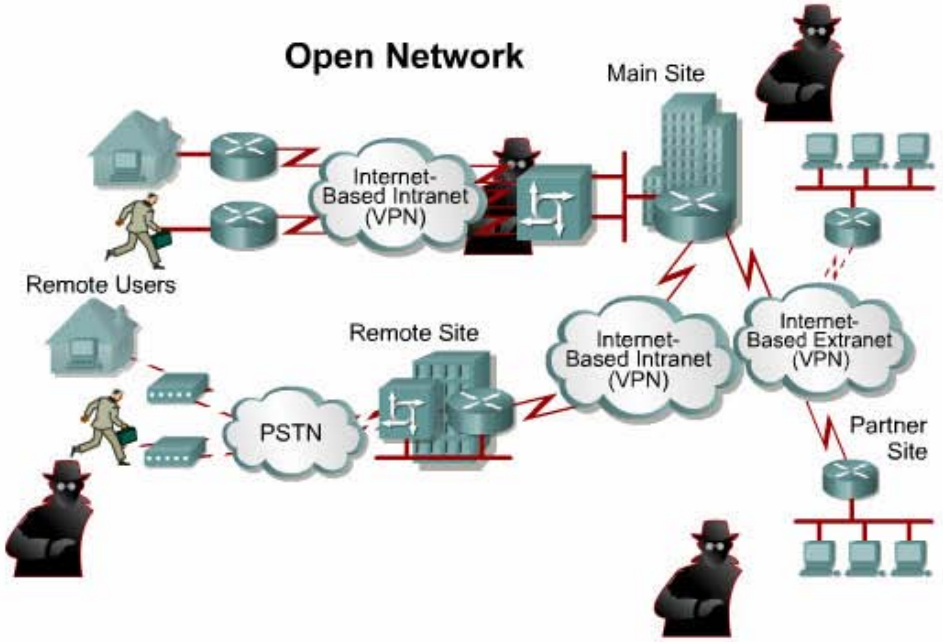
Pojavom i razvojem osobnih računala, LAN-ova (Local Area Network) i šioko otvorenim pristupom preko interneta, današnje mreže postaju sve otvorenije.

The Network Today

FIGURES

1
2
3

Toolbar: Maximize

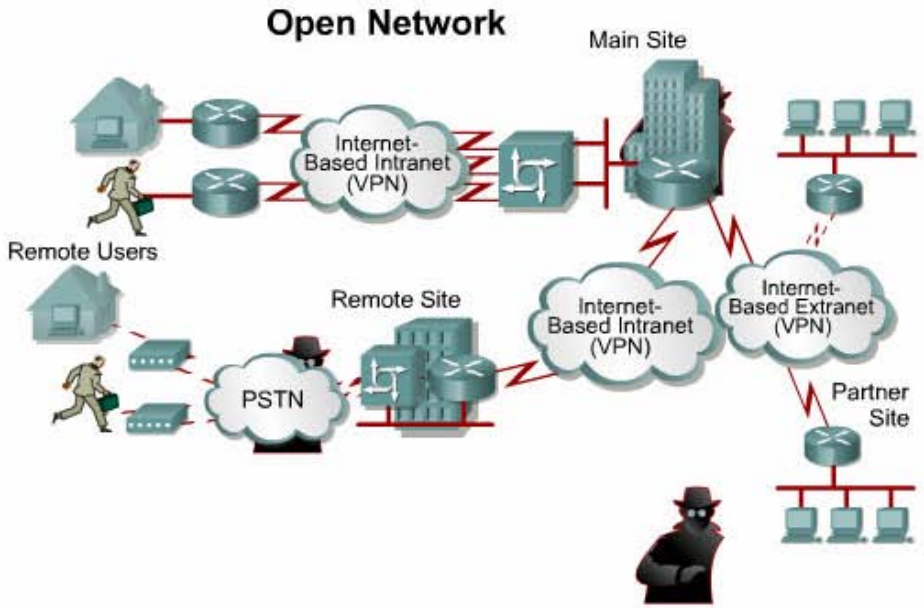


The Network Today

FIGURES

1
2
3

Toolbar: Maximi



Kako su e-business and internet nastavili rasti a time i otvorenost mreža prema vanjskom svijetu, traženje ravnoteže između izoliranosti i otvorenosti bit će od kritične važnosti, zajedno sa sposobnošću razlikovanja „dobrih i loših dečkih“.
Štoviše, rast mobilnog poslovanja i bežičnih mrežnih tehnologija imati će istu težinu kao i top na zidove starih dvoraca, uništavajući stari model zatvorenih mreža i zahtijevati da sigurnosna rješenja postanu u potpunosti integrirana, više transparentna i još više prilagodljiva.

Povećanjem broja LAN-ova i osobnih računala, internet kreira nebrojeno mnogo sigurnosnih rizika. Pojavila se potreba za uvođenjem firewall uređaja. Firewall uređaj je sklopovska ili programska podrška koja uvodi pravila kontrole pristupa između dviju ili više mreža. Ta tehnologija omogućava poslovanju ravnotežu između sigurnosti i jednostavnog pristupa internetu koji se, u većini slučajeva koristi za e-mail i Web pretraživanje.

Taj balans je bio kratkog vijeka, ali ipak, porastom extranet poslovanja firewall je ostao nezamijenjiv na mjestu spoja internih i vanjskih mreža i poslovnih procesa.

Poslovanje je brzo uočilo ogromne uštede prebacivanjem upravljanja lancem dostave robe i resursa na svoje poslovne partnere, spajanjem sustava prodaje i pretvaranjem klasičnih prodavača u mobilne zaposlenike kao i otvaranje komercijalnih priključnih točaka poslovnim partnerima i krajnji kupcima. Firewall je počeo sadržavati module za otkrivanje nedozvoljenog upada u mrežu, potvrdu vjerodostojnosti, autorizaciju i sistem za procjenu unutarnjih slabosti mreže. Danas, uspješna poduzeća vraćaju udarac držeći loše dečke van sustava s rastućim mogućnostima da dobrim dečkima omogući ulaz u sustav.

Većina ljudi očekuje od sigurnosnih mjera da osiguraju sljedeće:

- Korisnik može pristupiti samo područjima za koje ima ovlaštenje
- Korisnik može dohvatiti smao informacije za koje ima ovlaštenje
- Korisnik ne može prouzročiti štetu podacima, aplikacijama ili operativnom okruženju sistema

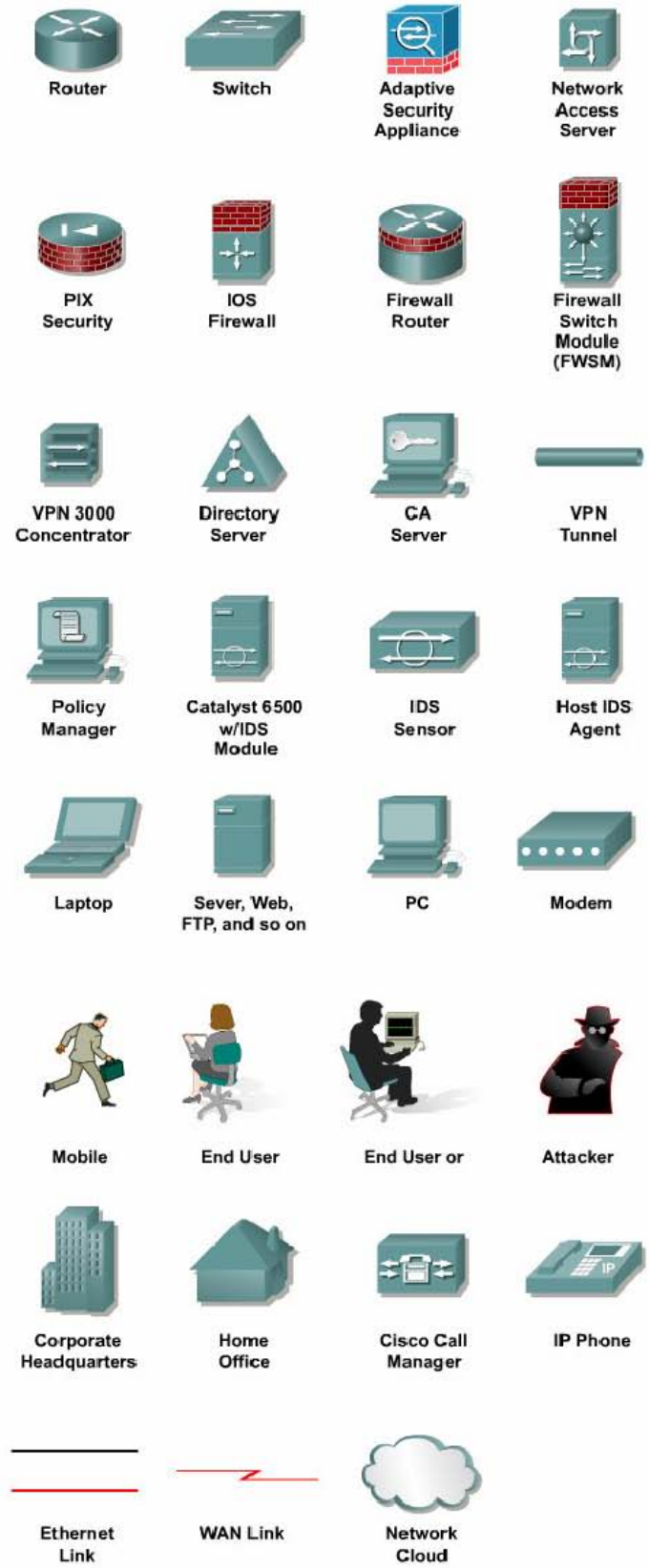
Riječ sigurnost znači zaštitu od zlonamjernog napada od strane vanjskog korisnika i uključuje kontrolu utjecaja greške na sustav.

Graphic Symbols

FIGURES

1
2
3

Graphic Symbols



1.1.2 Identificiranje potencijalnih rizika mrežne sigurnosti

Zadatak analize rizika je da identificira rizke koji prijete mreži, mrežnim resursima i podacima. Nakana analize rizika je da idntificira komponente mreže, utvrdi važnost svake komponente i na kraju uvede odgovarajući nivo sigurnosti. Ovo pomaže održavanju ravnoteže između zahtjeva za sigurnošću i zahtjeva za pristup mreži.

Identifikacija imovine – elemenata mreže
Prije nego što mreža može biti osigurana, pojedine komponente koje sačinjavaju mrežu moraju biti identificirane. Neophodno je da se napravi inventura sadržaja mreže. Svi uređaji i krajnje točke u mreži kao što su host-ovi i serveri također moraju biti uključeni u tu inventuru. Kada se kompletna inventura jednom napravi, komponentama mogu biti pridodani prioriteti i može biti procijenjena njihova ranjivost, odnosno osjetljivost na vanjske utjecaje.

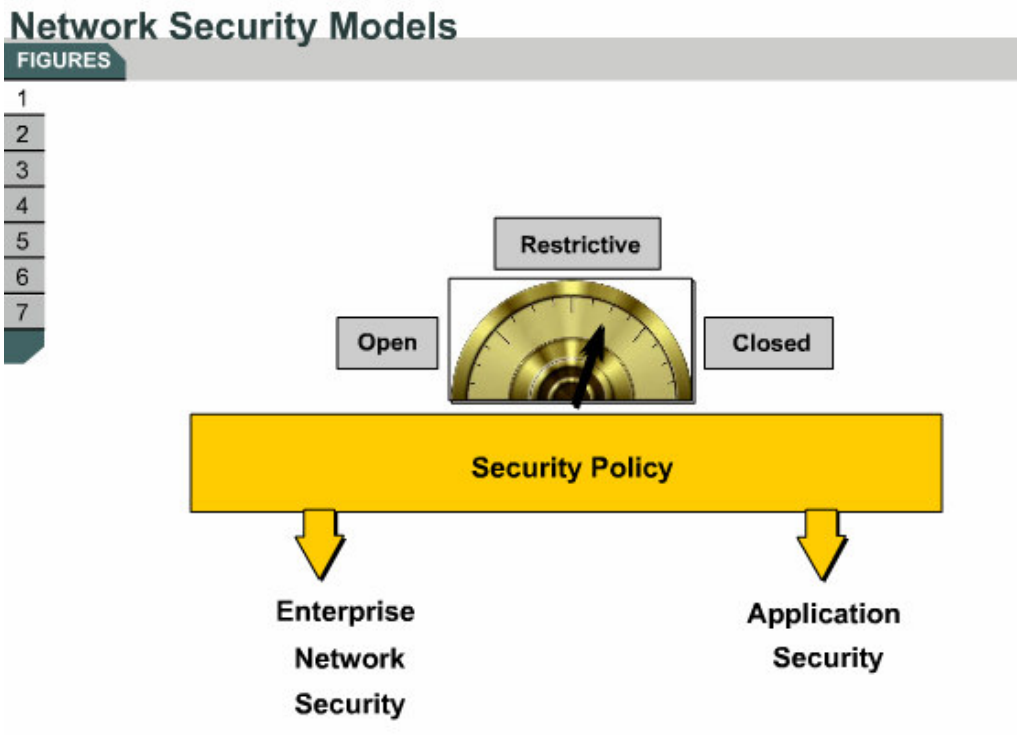
Procjena ranjivosti
Kada su mrežni elementi jednom identificirani može im biti procijenjena ranjivost. Razlozi za ranjivost mogu biti slabosti tehnologije, loša konfiguracija mreže ili sigurnosne procedure. Svaka otkrivena pozicija potencijalne ranjivosti mora se posebno razmatrati s ciljem smanjenja opasnosti, odnosno potencijalnog napada koji bi mogao iskoristiti tu ranjivost. Ranjivost se može rješavati na razne načine kao što su dodavanje software-skih zakrpa, rekonfiguriranjem uređaja u mreži ili instalacijom protumjera, kao što su firewall-ovi ili anti-virus software-i.

Identifikacija opasnosti
Opasnost je događaj koji može iskoristiti slabosti mreže i prouzročiti negativan utjecaj na nju. Potencijalne opasnosti po mrežu moraju biti identificirane te mora biti razmotrena odgovarajuća slabost koja ju je omogućila, s ciljem minimiziranja rizika koji prijete od te opasnosti.

1.1.3 Otvoreni protiv zatvorenog sigurnosnog modela

Unatoč svim sigurnosnim mjerama uvijek ima određenih nesuglasica između korisničke produktivnosti i sigurnosnih mjera. Cilj bilo kojeg dizajna sigurnosnog sustava ja da pruži maksimalnu sigurnost s minimalnim utjecajem na korisnika, njegov način priključivanja na mrežu i produktivnost. Neke sigurnosne mjere, kao sto je enkripcija mrežnih podataka, nisu restriktivne u smislu pristupanja mreži ili u smislu produktivnosti. S druge strane, nezgrapan ili sustav s nepotrebno puno zahtjeva za validaciju i autorizaciju može frustrirati korisnika i onemogućiti pristup kritičnim resursima mreže.

Poslovne potrebe i zahtjevi moraju diktirati sigurnosne procedure. Sigurnosne procedure ne smiju određivati kako će funcionirati poslovanje na mreži. Kako su interne organizacije korisnika predmet stalnih promjena, sigurnosne procedure moraju biti konstantno unaprijeđivane i ažurirane kako bi slijedile nove poslovne pravce razvoja, promjene tehnologija i rasporeda resursa.



Sigurnosne procedure mogu znatno varirati u svom dizajnu. Tri osnovna tipa sigurnosnih modela su:

- otvoreni
- restriktivni
- zatvoreni

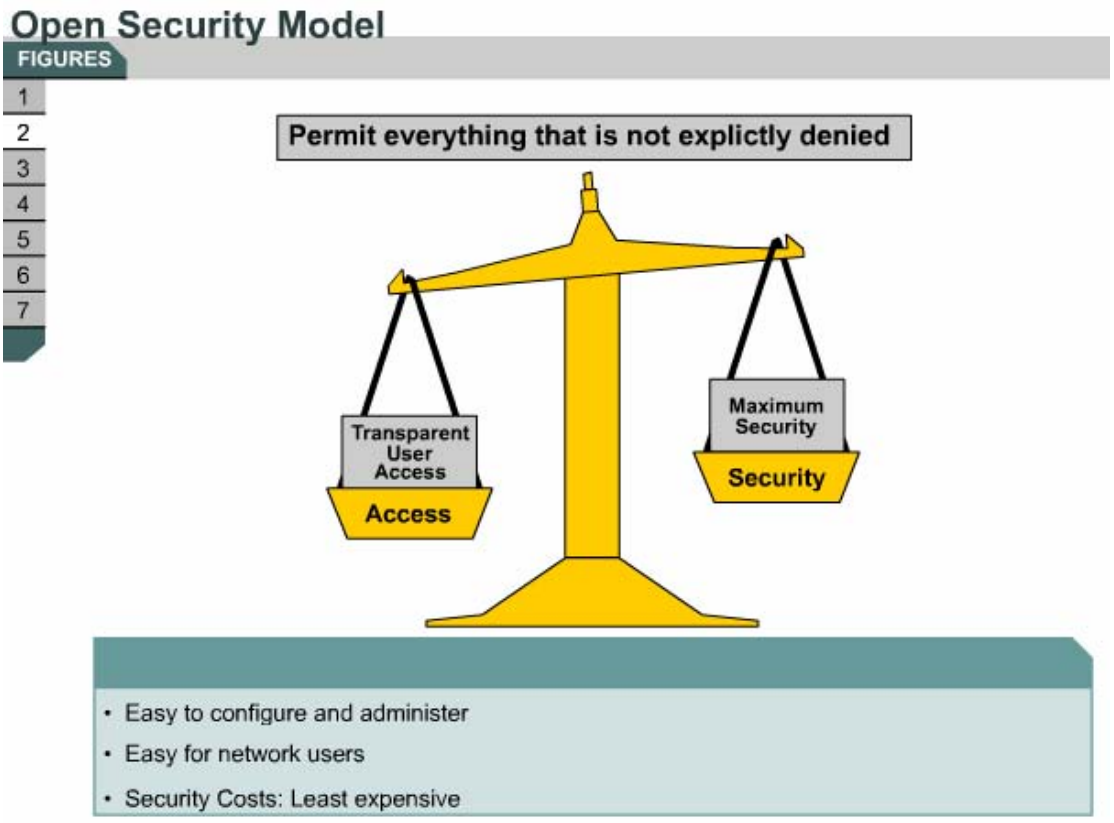
Važno je spomenuti:

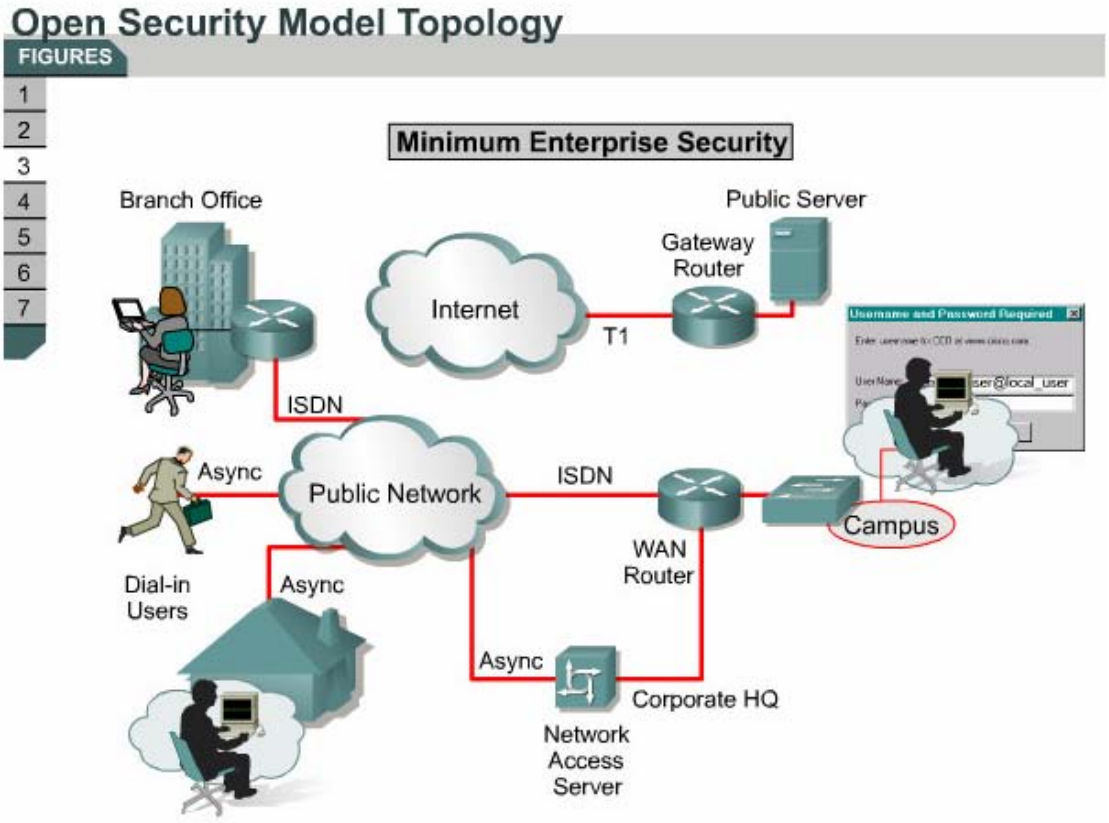
- Za početak sigurnosni model može biti otvoreni ili zatvoreni
- Potrebno je odabrati najbolju kombinaciju sigurnosnih proizvoda i tehnologija i implementirati ih u model
- Sigurnost na nivou aplikacije može sadržati Secure Socket Layer (SSL) tehnologiju

Kao i sigurnosni modeli, mnogi uređaji mogu biti klasificirani kao otvoreni, restriktivni ili zatvoreni. Na primjer router i switch su tipični primjeri otvorenih uređaja, inicijalnim postavkama dozvoljavajući visoki stupanj funkcionalnosti i servisa. S druge strane, firewall je tipičan zatvoreni sustav koji ne dozvoljava nikakve servise sve dok ih se ne „uključi“. Operacijski sistem servera može pripadati bilo kojoj od ove tri kategorije, ovisno o dobavljaču opreme. Važno je razumjeti te principe kada priključujemo bilo koji element opreme.

Otvoreni pristup

Otvoreni sigurnosni model je najjednostavniji za implementaciju





Vrlo malo sigurnosnih mjera ugrađeno je u ovaj model mreže. Administrator konfigurira postojeću programsku i sklopovsku opremu i njene bazične sigurnosne opcije. Firewall, Virtual Private Network (VPN), Detekcija upada (Intrusion Detection System) i ostale mjere koje zahtjevaju dodatne troškove uglavnom nisu implementirane. Jednostavni pristup lozinkom osnova je ovog modela. Ako se i koristi enkripcija, ona je implementirana na nivou individualnog korisnika ili servera.

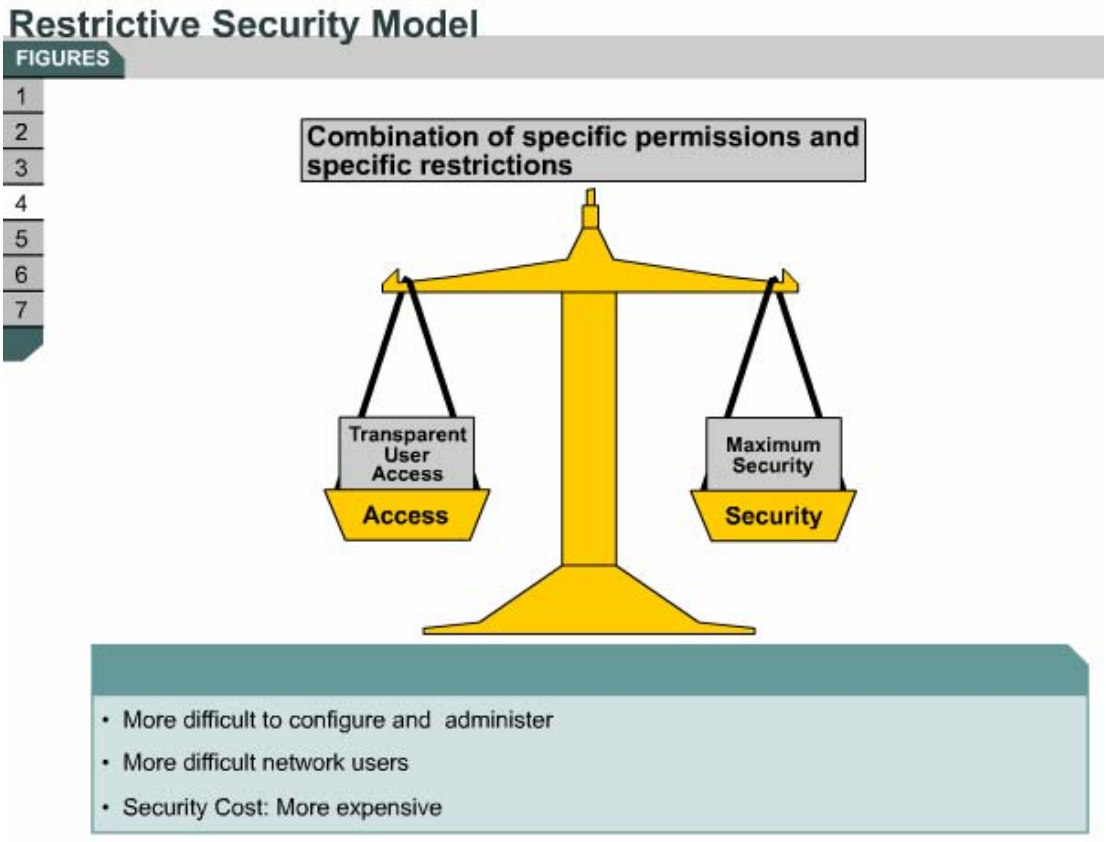
Ovaj model podrazumijeva da je zaštita podataka minimalna, korisnici su poznati i rizik je minimalan. Ipak, ovo ne isključuje potrebu arhiviranja podataka u većini scenarija otvorenog sigurnosnog modela. LAN mreže koje nisu spojene na Internet ili javnu WAN mrežu su najčešći korisnici ovog sigurnosnog modela.

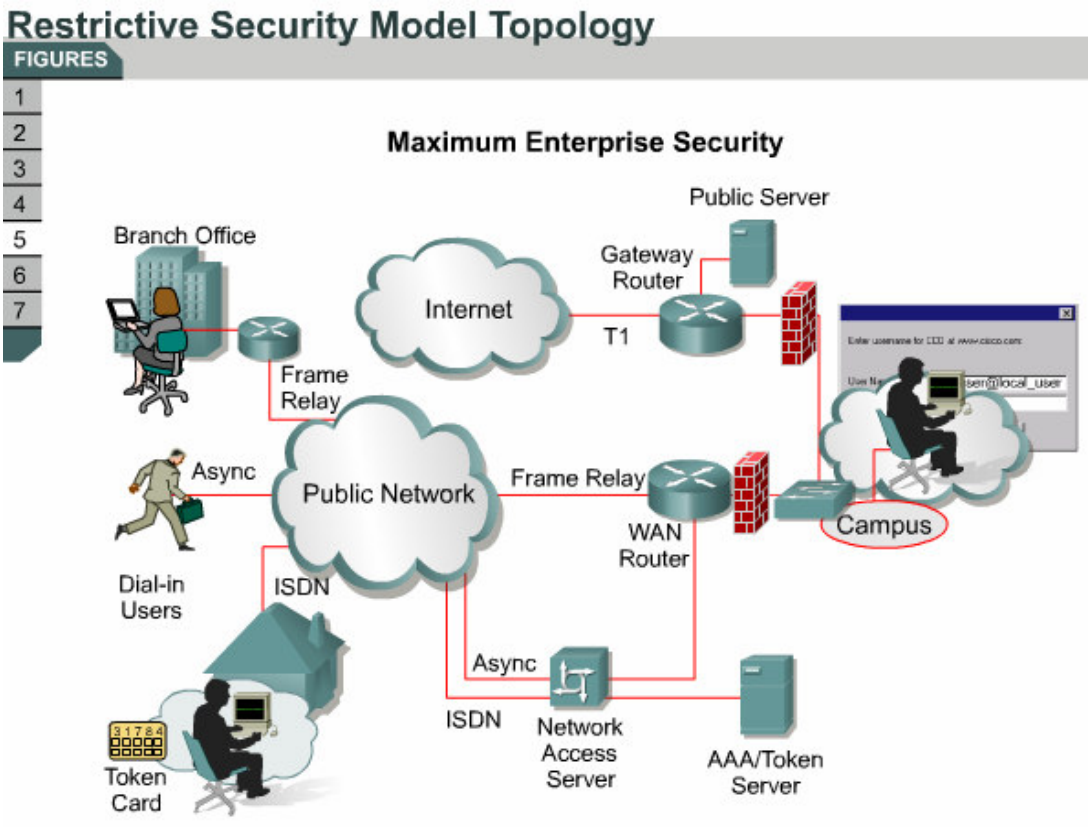
Ovaj model dizajna mreže daje korisniku slobodan pristup svim područjima. Ako se pojavi sigurnosni problem, on obično rezultira velikom štetom i gubitkom podataka. Mrežni operator najčešće nije odgovoran za tako nastalu štetu.

Restriktivni pristup

Restriktivni sigurnosni model puno je složeniji za implementaciju. Većina sigurnosnih mjera implementirana je u ovom dizajnu. Administrator konfigurira postojeću programsku i sklopovsku podršku za sigurnosne zadatke i dodatno implementira skuplju sklopovsku i programsku podršku kao što je Firewall, VPN, IDS i uvodi identitet servera. Firewall i identifikacija servera postaju osnova ovog modela.

Ovaj model podrazumijeva da je štićena vrijednost značajna i stvarna, da neki korisnici nisu korisnici od povjerenja i da je opasnost stvarna i vjerojatna. LAN, koji je spojen na Internet ili javnu WAN mrežu, najvjerojatnije će implementirati ovaj model. Jednostavnost korištenja od strane korisnika je smnjena, a sigurnosni sistem je pod stalnom napetošću.





Zatvoreni pristup

Zatvoreni sigurnosni model najsloženiji je za implementiranje. Sve dostupne sigurnosne mjere ugrađene su u ovaj model. Administrator konfigurira postojeću programsku i sklopovsku podršku na nivo maksimalne sigurnosti, uz dodatnu implementaciju skuplje sklopovske i programske podrške kao što je Firewall, VPN, IDS i uvodi identitet servera.

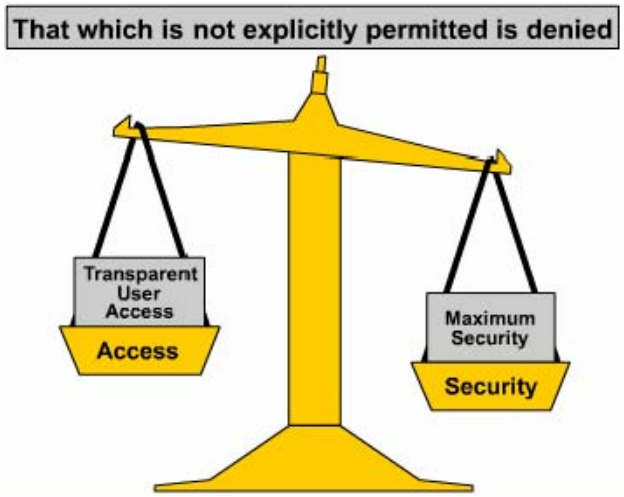
Ovaj model podrazumijeva da je štićena imovina od vrhunske važnosti, da se nema povjerenja ni u jednog korisnika i da je opasnost vrlo učestala. Korisnički pristup je vrlo problematičan i složen. Od mrežnog administratora zahtjevaju se posebne vještine i značajno više vremena za administriranje mreže. Štoviše, kompanije zapošljavaju veći broj administratora kako bi se mogao održavati ovaj visoki sigurnosni standard.

U mnogim poduzećima i organizacijama, ovakvi administratori najčešće su vrlo nepopularni dok implementiraju i održavaju sigurnosni model. Odjel mrežne sigurnosti mora objasniti da oni samo implementiraju sigurnosne mehanizme koji su dizajnirani i odobreni od strane poduzeća. Politika, koja je u pozadini zatvorenih sigurnosnih modela može biti vrlo velika. U slučaju proboja sigurnosnog sustava ili gubitka na mreži, mrežni operator nosi znatno više odgovornosti za nastale probleme.

Closed Security Model

FIGURES

1 2 3 4 5 6 7

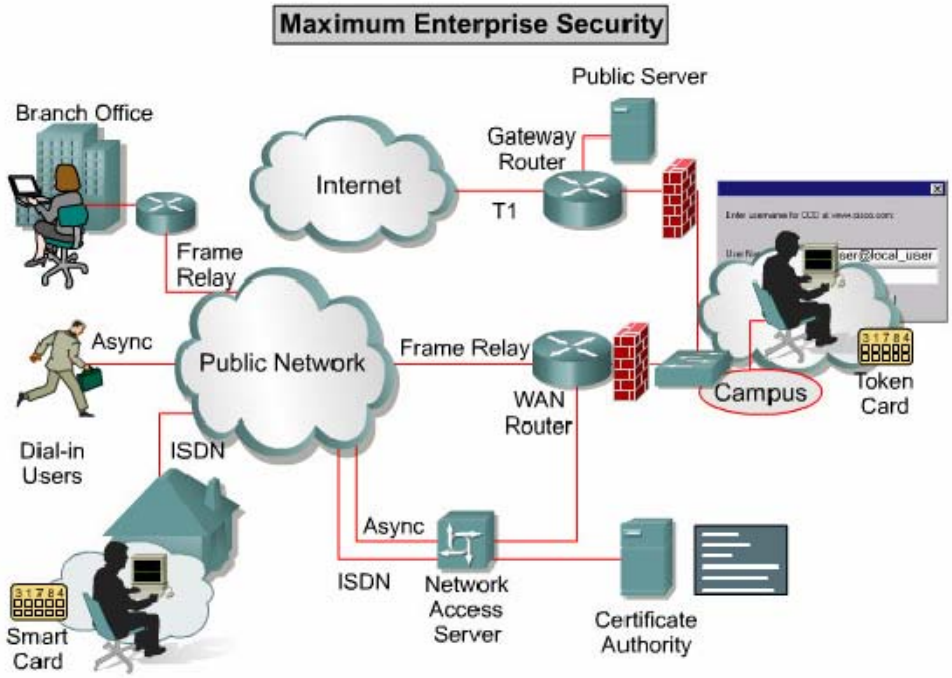


- Most difficult to configure and administer
- Most difficult network users
- Security Cost: Most expensive

Closed Security Model Topology

FIGURES

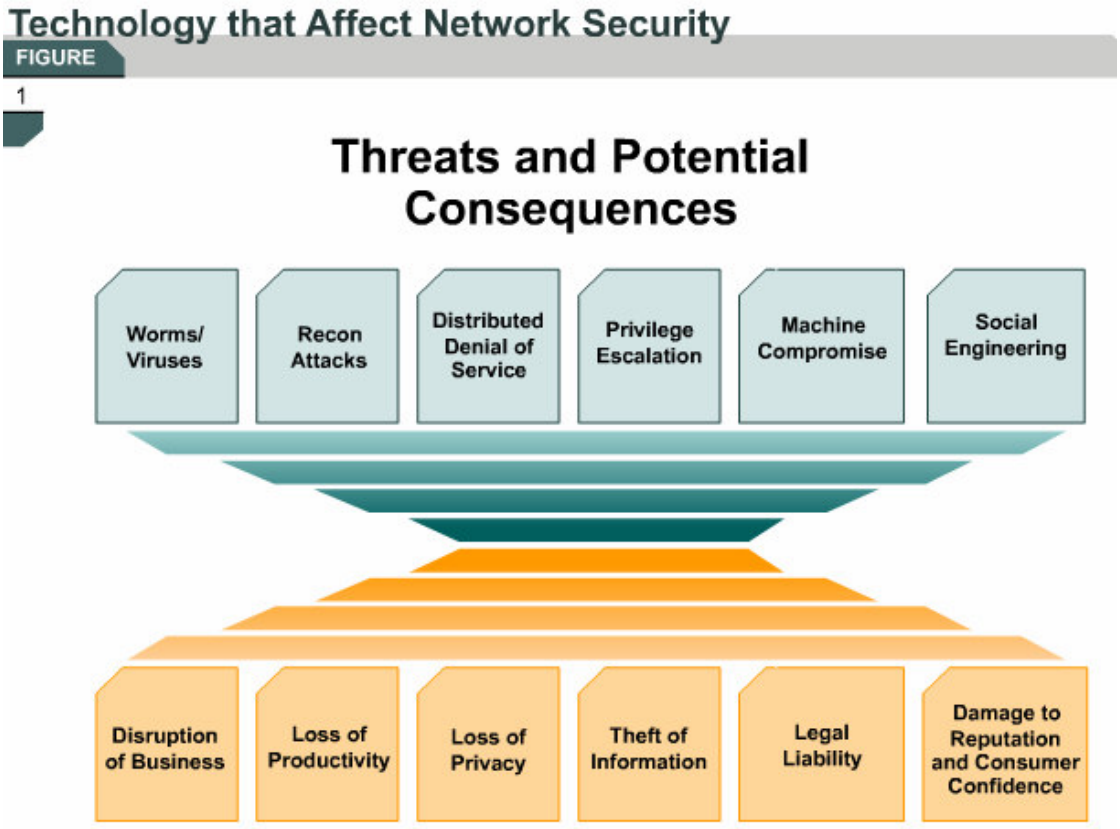
1 2 3 4 5 6 7



1.1 Uvod u mrežnu sigurnost

1.1.4 Trendovi u mrežnoj sigurnosti

Kao i u svakoj brzorastućoj industriji, promjene su očekivane. Nove vrste potencijalnih opasnosti za mrežnu sigurnost se stalno pojavljuju. Kompromis u mrežnoj sigurnosti može rezultirati ozbiljnim posljedicama kao što su gubitak privatnosti, krađa informacija i čak legalne odgovornosti.



Legalna pitanja i briga o privatnosti

Za mnoga poduzeća i institucije danas najznačajniji razlog za pokretanje i korištenje sigurnosnih procedura je usklađenost sa zakonom. Svako poduzeće je potencijalno odgovorno u slučaju da hacker ili virus našteti poslovnim operacijama. Slično tome, ako je poslovanje poduzeća preneseno na e-poslovanje i katastrofalni ili ozbiljni napad otežava to poslovanje, moguća je sudska tužba.

Legalna odgovornost u tim situacijama ovisi o tome koje preventivne sigurnosne tehnologije su korištene i dostupne i da li su te tehnologije na razuman, troškovno efikasan način implementirane. Kao rezultat, dosljednost u korištenju tih mjera u stvari znači implementaciju tehnologija kao što su Firewall, alati za otkrivanje neželjenih upada u mrežu, filteri sadržaja, analiza prometa, formiranje privatnih virtualnih mreža, konstantna procjena rizika i testiranje slabosti mreže. Naravno, sudski spor nije jedini pravni spor s kojim je e-poslovanje danas suočeno. Zakonodavci brinu oko nedostatka mrežne sigurnosti, posebno u područjima gdje raste ugroženost prava na privatnost.

1998. Europska Unija donijela je opsežne direktive o povjerljivosti osobnih podataka koje omogućavaju osobama strogu kontrolu vlastitih osobnih podataka. Mnoge zemlje izvan SAD-a usvojile su jednake ili slične mjere. U SAD-u preko 1000 mjera uvedeno je u državnu legislativu u 1999. i 2000., a brojne mjere su u fazi usvajanja.

U SAD-u se obrazovanje, financijski servisi, vlada i zdravstvo trenutno trude da zadovolje vladine smjernice za mrežnom sigurnošću i privatnošću. U financijskom sektoru postoji Gramm-Leach-Blilely (GLB) odrednica, objavljena 1999. GLB poništava dugogodišnji antitrust zakon koji zabranjuje bankama,

osiguravajućim zavodima i firmama koje se bave sigurnošću da razmjenjuju informacije jedna s drugom. Ideja je bila da manja poduzeća tada objave preuzimanje ili udruživanje što bi pomoglo razvoju konkurentnosti prema velikim financijskim institucijama. U taj zakon uključeno je više zaštita privatnosti klijenata. U praksi, poduzeća su obavezna objasniti korisniku koje podatke namjerava razmijeniti i s kim i dati mu mogućnost da on to ne dozvoli. Zakon je obvezao banke da pošalju takve obavijesti korisnicima do 1. lipnja 2001.

Vlada SAD-a je zadovoljna s Government Information Security Reform Act koji je objavljen u listopadu 2002. i usmjerava vladine agencije da povećaju planirana sredstva za sigurnost svojih kompjuterskih sistema. Predstavnici General Accounting Office (GAO) i ostalih federalnih agencija obavijestili su Kongres da, unatoč zakonu, federalne agencije su još uvijek nedovoljno opremljene u ključnim sigurnosnim pitanjima.

Na strani zdravstvene zaštite Health Insurance Portability and Accountability Act of 1996 (HIPAA) zahtjeva od Department of Health and Human Services da razvije grupu nacionalnih standarda za transakcije u području zdravstvene zaštite i osigura da elektronski transfer informacija o pacijentima bude povjerljiv barem na nivou povjerljivosti kod papirnatog oblika. Cijena usklađivanja procjenjuje se na 4 Milijarde USD.

Na kraju, mnoge obrazovne institucije u SAD-u se moraju uskladiti s Children Internet Protection Act (CIPA), ako žele primati ikakva budžetska sredstva od Američke administracije.

Bežični pristup
Rastuća upotreba spajanja na bežične lokalne mreže (WLAN) i rapidni rast pristupa internetu preko mobilnih telefona posebno u Europi i Aziji zahtjeva potpuno novi pristup sigurnosti. RF pristupi ne respektiraju Firewalls kako je to slučaj s klasičnim žičnim pristupom. Štoviše, spori procesori, mali ekrani i ograničene tastature na mobitelima i PDA (PersonalDigital Assistant) uređajima ruše mnoge standarde u pristupu sigurnosti, autentifikaciji i autorizaciji.

Potreba za brzinom
Broj širokopojasnih veza na internet iz privatnih kuća i stanova eksponencijalno raste. Mnoga poduzeća i institucije došli su do zaključka da višestruke T1 i E1 veze na internet nisu više suvišne. Trenutni software bazirani pristupi imaju dosta problema u kontroliranju OC-1 ili većih brzina.

Nedovoljan broj IT stručnjaka
Nedostatak IT stručnjaka posebno je uočljiv u području sigurnosti. Da bi riješili taj problem mnoga poduzeća i institucije posežu za izdvajanjem dnevnih obaveza iz poduzeće i prebacivanjem istih u specijalizirane tvrtke (outsourcing). Poslovni model izdvajanja određenih aktivnosti i prebacivanje istih u specijalizirane tvrtke postaje značajno rastući u svijetu sigurnosti. Zbog toga, sigurnosni modeli moraju biti više upravljivi u takvom modelu. Jasno, to ne smanjuje potrebu za stručnjacima u mrežnoj sigurnosti, nego ih samo grupira u specijalizirane tvrtke.

ISO/IEC 17799
ISO/IEC 17799, Informacijske tehnologije – pravila i praksa za upravljanje sigurnošću podataka, je standard sigurnosti podataka koji je objavljen u ISO (International Organization for Standardization) i IEC organizaciji (International Electrotechnical Commission). ISO/IEC 17799 nastoji biti zajedničko polazište i praktične smjernice za razvoj i organizaciju sigurnosnih standarda i efikasno upravljanje sigurnošću.

ISO/IEC 17799 je originalno objavljen 2000. godine i revidiran 2005. Revidirana verzija iz 2005. sadrži sljedeća poglavlja:

- Sigurnosna pravila
- Sigurnost mrežne organizacije i informacija
- Upravljanje imovinom i elementima mreže
- Sigurnost ljudskih resursa
- Fizička sigurnost i zaštita okoliša
- Upravljanje komunikacijama i operacijama
- Kontrola pristupa
- Preuzimanje, razvoj i održavanje informacijskog sistema
- Sigurnost informacija i upravljanje incidentima
- Usklađenost

1.1 Uvod u mrežnu sigurnost

1.1.5 Organizacije za pružanje usluga u području sigurnosti informacija

Postoje brojne tvrtke koje pružaju korisne informacije ljudima u sferi sigurnosti. Te organizacije pružaju informacije o otkrivanju i odgovoru na prijetnje bilo da su one već nastale ili su tek u razvoju. Informacije o slabostima same mreže, najbolja sigurnosna rješenja kao i trening i certifikacija su također mogući. Neovisna procjena sigurnosnih rizika pruža poduzećima i organizacijama objektivan uvid u kvalitetu sigurnosnih mjera i opreme u mreži. Na primjer, Common Criteria, FIPS 140, i ICSA su neki od neovisnih testova za certifikaciju i procjenu stanja mreže.

CERT/CC
CERT Coordination Center (CERT/CC) je međunarodni centar za zaprimanje sigurnosnih izvješća. CERT/CC igra glavnu ulogu u koordiniranju odgovora na Internetske sigurnosne prijetnje. CERT/CC je smješten na Software Engineering Institute (SEI) upravljen od strane Carnegie Mellon University.

US-CERT
United States Computer Emergency Readiness Team (US-CERT) je tim za suradnju između Department of Homeland Security i javnog i privatnog sektora. US-CERT je utemeljen 2003 s ciljem zaštite nacionalne Internet infrastrukture tako da koordinira odbranu i reagira na prijetnje internetskoj sigurnosti.

US-CERT je odgovoran za:

- analizu i smanjienje cyber prijetnji i slabosti mreža
- distribuciju informacija o prijetnjama i mrežnim slabostima
- koordiniranje odgovora na prijetnje

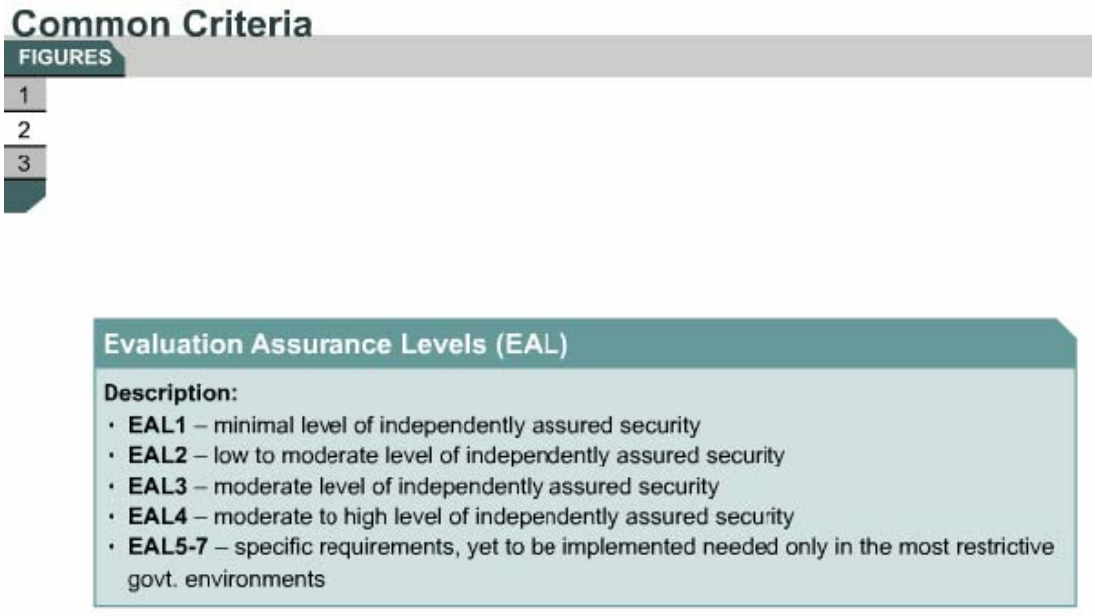
SANS Institut
SysAdmin, Audit, Network, Security (SANS) Institute ustanovljen je 1989. kao organizacije za korporativna istraživanja i edukaciju. SANS institut razvija i održava istraživanja o različitim aspektima mrežne sigurnosti. Ovi dokumenti dostupni su potpuno besplatno. SANS također vodi Internet Storm Center – sistem ranog upozorenja za internet prijetnje.

(ISC)^2

International Information Systems Security Certification Consortium, Inc. (ISC)2 je neprofitna organizacija koja sakuplja najbolja iskustva u području informacijske sigurnosti. (ISC)2 je kreirao dva certifikata koji su u skladu s tom najboljom praksom, Systems Security Certified Practitioner (SSCP) i Certified Information Systems Security Professional (CISSP).

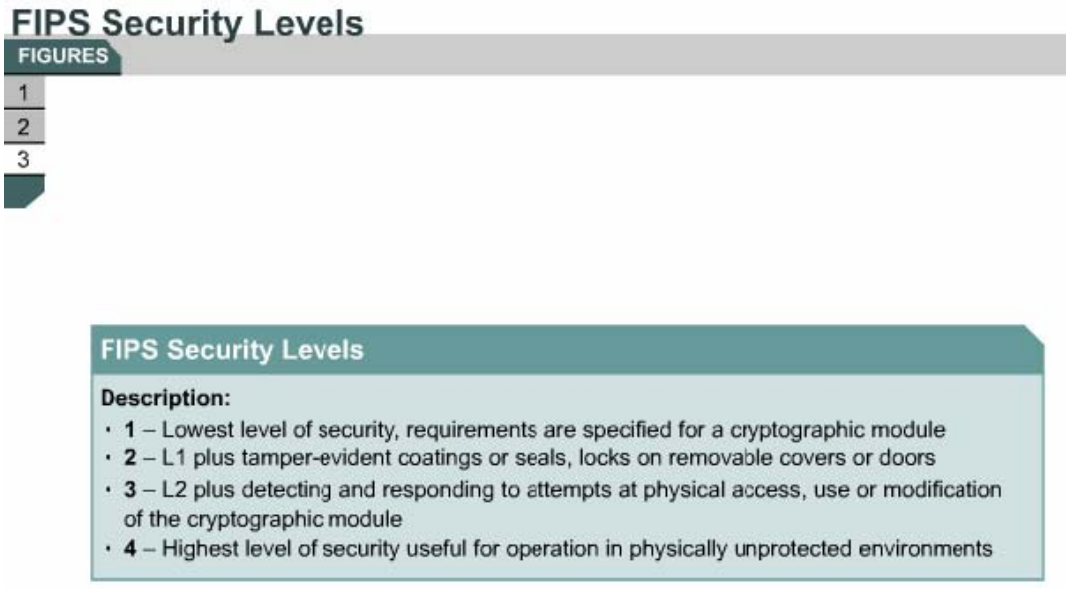
Common Criteria

Common Criteria je međunarodni standard za razvoj IT sigurnosti. Razvijen je od strane konzorcijuma 14 zemalja s ciljem zamjene velikog broja različitih standarda koje je svaka zemlja imala i postavljanja jednog kvalitetnog standarda za međunarodnu upotrebu. Iako je sedam sigurnosnih nivoa definirano u procesu procjene, nivo 4 (Evaluation Assurance Level 4 (EAL4)) se smatra za ciljni nivo.



FIPS

Federal Information Processing Standard (FIPS) 140 je SAD i Canadian Government standard koji specificira sigurnosne zahtjeve za kriptografske module. FIPS 140 ima četiri nivoa sigurnosti. Nivo 1 je najniži, a Nivo 4 najviši. Svaki nivo dodaje sigurnosne elemente na niži nivo, što znači da, npr., nivo dva sadrži sve elemente nivoa 1 uz dodanu razliku do nivoa 2.



ICSA

ICSA Labs testira firewalls prema standardnom setu funkcija i kriterijskih elemenata. ICSA Labs trenutno testira firewall-ove prema Modular Firewall Product Certification Criteria version 4.0. ICSA također testira VPN opremu za interoperabiliti. To testiranje potvrđuje da proizvod ili grupa proizvoda koji koriste kriptografiju pružaju efikasne sigurnosne servise. ICSA Certifikacija postoji da bi se osigurala grupa mjerljivih, javnih standarda za komercijalne sigurnosne protokole.