Network Security
Elements of Network Security Protocols

Principi e Criteri di Progettazione di Architettura Sicure di Rete

- Pianificazione della sicurezza
- Cenni al Risk Assessment
- Politiche di sicurezza

"If you believe that any problem in security can be solved by cryptography, then you have not understood the problem"

(Roger M. Needham)

Caso di studio: Dribbles Co.

- L'azienda Dribbles Corporation produce e vende dispositivi elettronici per l'intrattenimento.
- L'azienda vuole dotarsi di una infrastruttura di rete per attestare la propria presenza su Internet (Web ed email) rispetto ai propri clienti
- L'azienda vuole utilizzare la rete anche per le proprie attività quotidiane interne con l'obiettivo di diventare "paper-free"

"La sicurezza è un processo" –B. Schneier

- **Asset Identification –** che cosa si vuole proteggere
- **Threat Assessment –** da quali minacce ci si vuole proteggere
- **Risk Assessment –** qual è la possibilità che una minaccia si realizzi
- **Security Policy –** (cosa fare) insieme di regole tecniche e comportamentali che hanno l'obiettivo di allontanare il rischio
- **Security Plan –** (come farlo)realizzazione delle politiche per raggiungere il grado di sicurezza prefissato
- **Security Audits –** descrive il livello corrente di sicurezza

Roadmap

- **Asset Identification**
- **Threat Assessment**
- **Risk Assessment**
- **Security Policy**
- **Security Policy implementation**
- **Security Audits**

Asset identification

Si identificano le risorse da proteggere

- Hardware – Apparati di rete, server, end-host, laptop, periferiche, storage & communication media
- Software – database, sistemi operativi, sistemi informativi, compilatori, applicazioni, programmi acquistati, programmi sviluppati in casa
- Dati – dati usati durante l'esecuzione, dati memorizzati su vari media, dati stampati, dati archiviati; log & audit records
- Persone – competenze
- Documentazione – su hardware, software, procedure
- Supplies – carta, cartucce, toner,…

Roadmap

- **Asset Identification**
- **Threat Assessment**
- **Risk Assessment**
- **Security Policy**
- **Security policy implementation**
- **Security Audits**

Threat Assessment

Si identificano le minacce

- Minacce ai requisiti di sicurezza
  - Accessi non autorizzati alle risorse (privacy)
  - Modifiche non autorizzate alle risorse (integrity)
  - Denial of service (availability)
- Una minaccia può essere
  - intenzionale
  - accidentale

Assets and Security Properties (cont.)

Asset	Confidentiality	Integrity	Availability
Hardware			
Software			
Data			
People			
Documentation			
Supplies			

- Guida al ragionamento
- Formato non rigido

Assets and Security Properties (cont.)

- Nella compilazione della tabella bisogna considerare gli effetti di
- errori accidentali
- insider malizioso
- outsider
- disastri fisici e naturali
- …

Assets and Security Properties (ex.)

Asset	Conf.	Integrity	Availability
Hardware		overloaded, destroyed, tampered with	failed, stolen, destroyed, unavailable
Software	stolen copied, pirated	impaired by Trojan Horse, modified, tampered with	deleted, misplaced, usage expired
Data	disclosed, accessed by outsider, inferred	damaged • sw error • hw error • user error	deleted, misplaced, destroyed
People			quit, retired, terminated, on vacation
Document.			lost, stolen, destroyed
Supplies			lost, stolen, damaged

Roadmap

- **Asset Identification**
- **Threat Assessment**
- **Risk Assessment**
- **Security Policy**
- **Security policy implementation**
- **Security Audits**

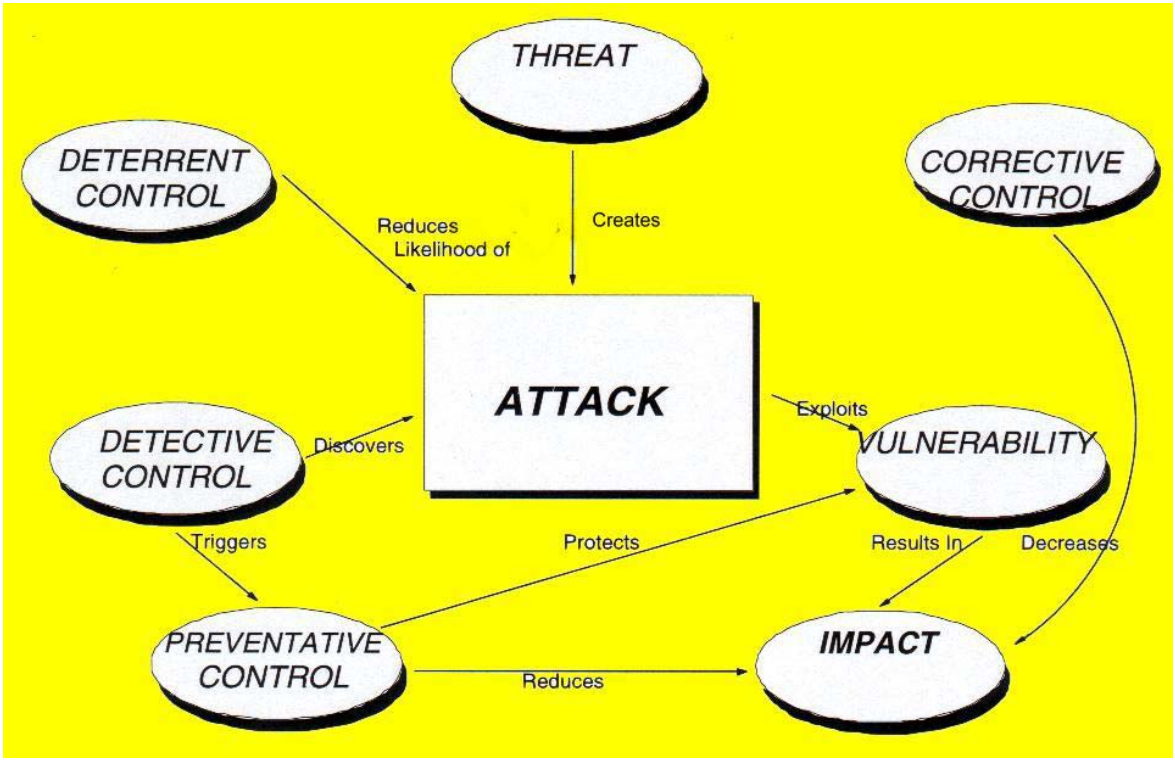
Risk Assessment

In questa attività

- si analizza un sistema ed il suo contesto operativo,
- si determinano le minacce, si valuta il potenziale danno che ciascuna minaccia può causare
- ciascuna minaccia, si determinano i controlli ed i relativi costi
- si esegue un'analisi costi-benefici

"Security does not come cheap" –Bruce Schneier

Minacce & controlli



Risk Assessment

Parametri fondamentali:

- **risk likelihood** misura la probabilità che una minaccia si concretizzi in un attacco. Quando tale probabilità vale 1 si dice cha abbiamo un problema
- **risk impact** misura il costo o la perdita associata a tale attacco
- **risk exposure** = risk likelihood $\times$ risk impact
- **risk control** indica il grado di controllo finalizzato ad eliminare o almeno ridurre l'impatto (i meccanismi di sicurezza sono esempi di metodi per il controllo del rischio)

Strategie di riduzione del rischio

Strategie di riduzione del rischio (risk reduction)

- evitare il rischio cambiando i requisiti di sicurezza o altre caratteristiche del sistema
- trasferire il rischio allocandolo ad altre organizzazioni o stipulando un'assicurazione che copra le eventuali perdite
- assumere il rischio, accettandolo, controllandolo con le risorse disponibili e preparandosi ad affrontare le eventuali perdite

Risk leverage

Risk leverage dà una misura dell'efficacia di una strategia di riduzione del rischio

- Risk exposure before reduction
- Risk exposure after reduction
- Cost of risk exposure

$$\text{risk leverage} = \frac{(\text{risk exp. before}) - (\text{risk exp. after})}{\text{cost}}$$

Risk leverage (example)

Acquisto di un antivirus

- **Risk: virus infection**
- Costo annuo per "ripulire" i sistemi infettati 10,000$ @ probabilità del 30% 3,000$
- Efficacia del controllo: -10% 1,000$
- Costo del controllo 100$
- Costi e perdite annuali attesi (3,000 – 1000 + 100) = 2100 $
- Risparmio (3,000 – 2,000) = 900$
- Risk Leverage 10

Risk leverage (example)

Acquisto di software per il controllo degli accessi

- **Rischio: rivelazione di dati riservati; elaborazioni basate su dati errati**
- Costo per la ricostruzione dei dati: $1,000,000 @ probabilità 10% per anno 100K$
- Efficacia del controllo: 60% -60K$
- Costo del controllo: 25K$$
- Costi e perdite attese (100 – 60 + 25) 65$
- Risparmio 35K$
- Risk leverage 2.4

Risk leverage (example)

Sostituzione dell'accesso di rete

- **Rischio: accesso ed uso non autorizzato della rete**
- Accessi non autorizzati ai dati: 100K$ @ 2% probabilità annua 2K$
- Uso non autorizzato dei programmi: 10K$ @ 40% probabilità annua 4K$
- Perdite annuali aspettate: 6K$
- Efficacia del controllo: 100% 6K$
- Costo del controllo: HW (50,000 ammortizzato su 5 anni) 10K$
- Costo del controllo: SW (20,000 ammortizzato su 5 anni) 4K$
- Costo del controllo: Personale (ogni anno) 40K$
- Costo annuo del controllo 54K$
- Costi e perdite annue: (6 – 6 + 54) +54K$
- Risparmio: (6 – 54) -48K$
- Risk leverage: (6/54) 0.11

Valutazione della Risk Likelihood

- **Calcolo delle probabilità classico**: approccio teorico che richiede però un modello del sistema. Non sempre ciò è possibile o semplice.
- **Frequenza relativa**: approccio che si basa su osservazioni e misure eseguite sul sistema stesso. I dati necessari alla valutazione della frequenza relativa di certi eventi possono essere già collezionati (dal SO, router, firewall, personale IT,…)
- **Probabilità soggettiva**: il metodo frequenza relativa presuppone l'esistenza del sistema; se il sistema non esiste ci si può basare sul giudizio di un analista esperto che indica delle probabilità (soggettive) sulla base delle sue conoscenze relative ad un sistema simile.

Esempio di Probabilità Soggettiva

Frequenza	Rating
più di una volta al giorno	10
una volta al giorno	9
una volta ogni tre giorni	8
una volta alla settimana	7
una volta ogni due settimane	6
una volta al mese	5
una volta ogni quattro mesi	4
una volta l'anno	3
una volta ogni tre anni	2
meno di una volta ogni tre anni	1

Valutazione del Risk Impact

- Costi dell'hardware, costi del software
- *Costi nascosti*
- Alcuni aspetti da considerare per valutare i costi nascosti
  - aspetti legali
  - aspetti economico-finanziari
  - immagine
  - danni ad organizzazioni, cose e persone

Risk Assessment: pro e contro

Pro

- Maggiore consapevolezza
- Collegamento degli obiettivi di sicurezza a quelli di gestione
- identificazione di asset, vulnerabilità e controlli
- Decisioni più consapevoli da parte dei manager
- Giustificazione delle spese fatte per la security

Contro

- Falso senso di precisione e sicurezza
- Difficile da fare
- Immutabilità
- Mancanza di accuratezza

Roadmap

- **Asset Identification**
- **Threat Assessment**
- **Risk Assessment**
- **Security Policy**
- **Security policy implementation**
- **Security Audits**

Definizione di una security policy (cont.)

- La politica di sicurezza è un documento di gestione di alto livello in cui si specificano obiettivi ed intenti
- Una politica di sicurezza specifica
  - le limitazioni all'accesso delle risorse (chi può accedere a quali risorse ed in che modo)
  - le regole per l'accesso alle risorse
- La politica di sicurezza costituisce la base per:
  - la progettazione ed implementazione della rete;
  - l'utilizzo della rete
  - l'auditing

Politica di sicurezza: contenuti (cont.)

- Identificare l'udienza cui si rivolge
  - utenti, clienti, possessori
- Scopo
  - promuovere l'efficienza del business
  - facilitare la condivisione delle informazioni all'interno dell'organizzazione
  - proteggere le informazioni personali e relative al business
  - assicurare la disponibilità delle informazioni di supporto al business
  - assicurare un luogo di lavoro produttivo e sicuro
  - rispettare leggi e regolamenti

Politica di sicurezza: contenuti

- Quali risorse devono essere protette
  - cosa viene protetto
- Natura della protezione
  - chi ha accesso alle risorse da proteggere
  - quale grado di protezione deve essere garantito alle risorse da proteggere
  - come tale accesso viene garantito
  - come viene negato l'accesso a soggetti non autorizzati
  - chi è responsabile della protezione delle varie risorse

Definizione di una security policy (cont.)

La politica di sicurezza deve

- essere generale e duratura
  - la politica cambia quando cambia la "missione" aziendale, quando cambiano leggi e regolamenti, …
  - la politica non deve contenere dettagli implementativi
- realistica
  - tecnologia, prestazioni, costi, usabilità, leggi e costumi,…
- utile

Definizione di una Security Policy

Elementi di una politica di sicurezza (**RFC 2196**)

- **Computer Technologies Purchase Guidelines**
- **Privacy Policy**
- **Access Policy**
- **Accountability Policy**
- **Authentication Policy**
- **Availability statement**
- **Information Technology System & Network Maintenace Policy**
- **Violation Reporting Policy**
- **Supporting Information**

Roadmap

- **Asset Identification**
- **Threat Assessment**
- **Risk Assessment**
- **Security Policy**
- **Security policy implementation**
- **Security Audits**

Security Policy Implementation

- In questa attività si implementa la politica di sicurezza definita
- Condizioni di successo
  - Informazione e consenso
    - perché è necessaria una SP
    - quali sono le ragioni alla base della SP
    - quali sono i rischi ed i costi analizzati per definire la SP
  - Responsabilità

Roadmap

- **Asset Identification**
- **Threat Assessment**
- **Risk Assessment**
- **Security Policy**
- **Security policy implementation**
- **Security Audits**

Security Audits

- In questa attività
  - **si analizza**, **si testa** e **si migliora** la SP;
  - **si identificano** certe abitudini degli utenti che possono portare ad attacchi;
  - **si rendono gli utenti consapevoli** delle implicazioni in termini di sicurezza delle loro azioni
- L'attività di auditing può concretizzarsi in misure tecnologiche e/o formative

Requisiti dell'Azienda (I)

Caso di Studio: Dribbles Co.

L'azienda vuole utilizzare la rete per le seguenti attività:

- Contatti ed acquisti da parte dei clienti e gestione delle relative informazioni
- Gestione delle informazioni relative alla ricerca ed allo sviluppo di prodotti
- Gestione delle informazioni aziendali
- Interazione tra i dipendenti

Requisiti dell'Azienda (II)

Caso di Studio: Dribbles Co.

L'azienda richiede che

I. i dati aziendali "sensibili" nonché i dati relativi allo sviluppo di prodotti futuri siano mantenuti segreti e siano noti solo a coloro che devono conoscerli

II. i dati relativi ai clienti siano mantenuti segreti e noti solo a coloro che devono conoscerli tra cui l'impiegato che gestisce l'ordine e gli analisti che calcolano statistiche

III. il rilascio di qualunque informazione sensibile necessita il consenso dei dirigenti e/o degli avvocati dell'azienda

Organizzazione dell'Azienda

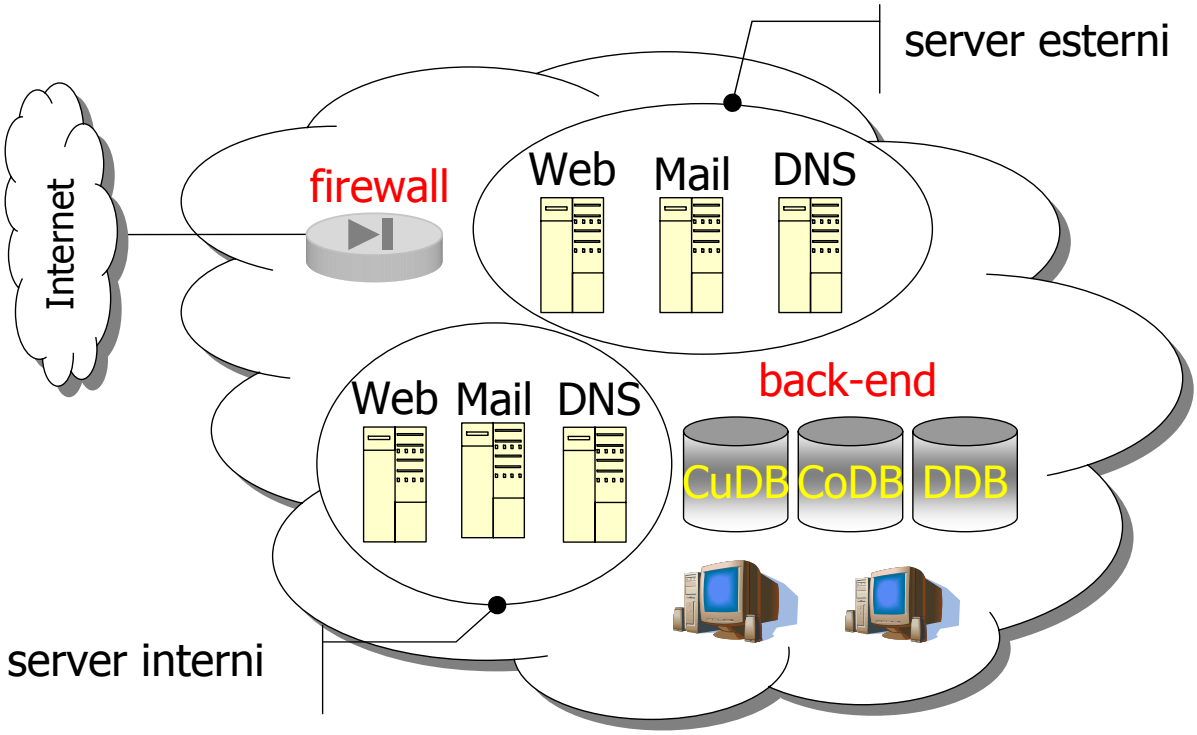
Caso di Studio: Dribbles Co.

L'azienda è organizzata in gruppi/dipartimenti

- Il **Customer Service Group** (**CSG**)
  - che costituisce l'interfaccia tra i clienti/fornitori e l'azienda;
  - che gestisce tutte le informazioni, riservate e non, relative ai clienti
- Il **Development Group** (**DG**)
  - che progetta, sviluppa, modifica e mantiene i prodotti
  - che interagisce con CSG per avere informazioni sui gusti dei clienti
- Il **Corporate Group** (**CG**)
  - che è costituito da dirigenti e avvocati (corporate officers)
  - che gestisce tutte le informazioni aziendali di carattere finanziario e legale (investimenti, acquisizioni, cessioni, cause, brevetti, …)

Identification of Assets

Caso di Studio: Dribbles Co.



Identification of Assets

Caso di Studio: Dribbles Co.

- Dati pubblici (PD): disponibili sul Web server esterno
- Dati relativi prodotti esistenti (DDEP): memorizzati nel database DDB
- Dati relativi a prodotti futuri (DDFP): idem
- Dati Aziendali (CoD): memorizzati nel database CoDB
- Dati sui clienti (CuD): memorizzati nel database CuDB

Threat Identification

Caso di Studio: Dribbles Co.

- **minacce da parte di un avversario esterno**
  - accesso ai back-end DB
  - "defacement" del web server esterno
  - accesso alle comunicazioni interne
  - …
- **minacce da parte di un avversario interno**
  - accesso alle comunicazioni interne non destinate a lui
  - accesso ad aree dei back-end DB non destinate al suo utilizzo
  - …

Risk Assessment

Caso di Studio: Dribbles Co.

- Confidentiality
  - La preoccupazione maggiore dell'azienda è la protezione della confidenzialità di CoD, DDFP e di CuD
- Integrity
  - Anche l'integrità è molto importante per l'Azienda perché una perdita di informazioni può comportare una perdita di tempo.
- Availability
  - Internamente, l'azienda utilizza la rete principalmente per R&D. Perciò è sufficiente che la rete interna sia "su" il più delle volte.
  - Esternamente, siccome l'Azienda utilizza il Web e l'email per attestare la propria presenza in Internet, è sufficiente che il web server ed il mail server siano "su" la maggior parte del tempo

Risk Assessment

Caso di Studio: Dribbles Co.

Asset	Confidentiality	Integrity	Availability
Back-end DB	5	3	2
Ext. Web Server	2	2	5
Internal LAN	4	2	2
Internet connectivity	2	2	4

Per ogni minaccia, a ciascun asset si assegna un rating da 1 (non importante) a 5 (molto importante) che costituisce una misura della sua risk exposure

Security Policy Definition

Caso di Studio: Dribbles Co.

Access Policy

- Gli accessi sono strettamente controllati. Tutti gli accessi sono vietati a meno che non sia specificato diversamente
- L'accesso ai back-end è consentito solo ai dipendenti e solo dalle postazioni della rete interna. L'accesso da ogni altra postazione sarà proibito.
- Gli accessi saranno su base "as-needed". L'accesso agli asset sarà permesso a certi gruppi di utenti e negato a tutti gli altri
- La decisione di permettere l'accesso ad un dipendente sarà presa dal supervisore insieme al Chief Security Officer

Alcuni principi di progettazione

- Principio del minimo privilegio (Principle of least privilege)

  Ad ogni soggetto devono essere dati i minimi privilegi necessari per portare a termine il proprio compito

- Principio della separazione di poteri (Principle of separation of privilege)

  Un sistema non deve concedere un permesso basato su di una singola condizione

- Principio della progettazione aperta (Principle of open design)
  - La sicurezza di un meccanismo non deve basarsi sulla segretezza del suo progetto o della sua implementazione

Privacy & Integrity: visione statica

Caso di Studio: Dribbles Co.

Soggetti — **privilegio**

Oggetti

	ESTERNI	SVILUPPATORI	DIRIGENTI	IMPIEGATI
PD	read	read	read	read
DDEP		read	read	
DDFP		read, write	read	
CoD			read, write	
CuD			read	read, write

Matrice degli Accessi

Privacy & Integrity: visione dinamica

Caso di Studio: Dribbles Co.

Lo spostamento di un dato da una classe all'altra deve essere autorizzato da almeno due utenti (principio di separazione dei poteri)

From \ To	PD	DDEP
PD		
DDEP	CSG, CG	
DDFP		DG, CG
CoD	CG, CG	
CuD		