Network Security
Controllo delle violazioni e delle intrusioni

 1

Breve storia

Novembre 1988 – Morris Worm (>60K computer, danni $10M);

Gennaio 1990 – Crash dell'infrastruttura dell'AT&T (9 ore, 70M di telefonate bloccate);

Natale 1994 – Kevin Mitnick vs. Tsutomu Shimomura (danni $290M)

Febbraio 2000 – DDoS (Yahoo!, Amazon.com, CNN, eBay, Buy.com, e*Trade, etc. danni ~$50M)

Marzo 2001 – Frodi a siti di E-Banking ed E-Commerce (>1M carte di credito rubate, >40 siti)

Estate 2001 – Internet Worms - Code Red, etc. (>250.000 host coinvolti in 9 ore)

 2

Se non esistessero rischi da cui difendersi, non vi sarebbe alcuna ragione per parlare di Intrusion Detection.

Sfortunatamente esistono diverse tipologie di rischi e di attacchi che un sistema informativo puo' subire.

Ci occupiamo dei rischi, e di conseguenza delle intrusioni, realizzate attraverso Internet.

Morris Worm -> errori, interdipendenza dei sistemi, relazioni di fiducia tra host;

Crash AT&T -> vulnerabilita' dell'infrastruttura. Gerarchia DNS?

Mitnik -> vulnerabilita' TCP/IP, dimostrazione di studi teorici.

DDoS -> nuova tipologia, controllo coordinato di centinaia di macchine via Internet;

Frodi E-Commerce -> vulnerabilita' dei nuovi servizi e piattaforme, target reale di atti illeciti;

Internet Worms -> vulnerabilita' piattaforme, diffusione via email, potenziale controllo dei PC privati. Connessioni Always-On?

Solo una percentuale ridotta degli incidenti relativi alla sicurezza informatica vengono resi pubblici.

Molti dei casi resi noti sono eclatanti ma non per questo riflettono le tipologie di rischio piu' gravi.

E' comunemente ritenuto che i casi effettivamente piu' gravi vengano mantenuti del tutto riservati.

 3

Perche' preoccuparsi della sicurezza dei sistemi informatici?

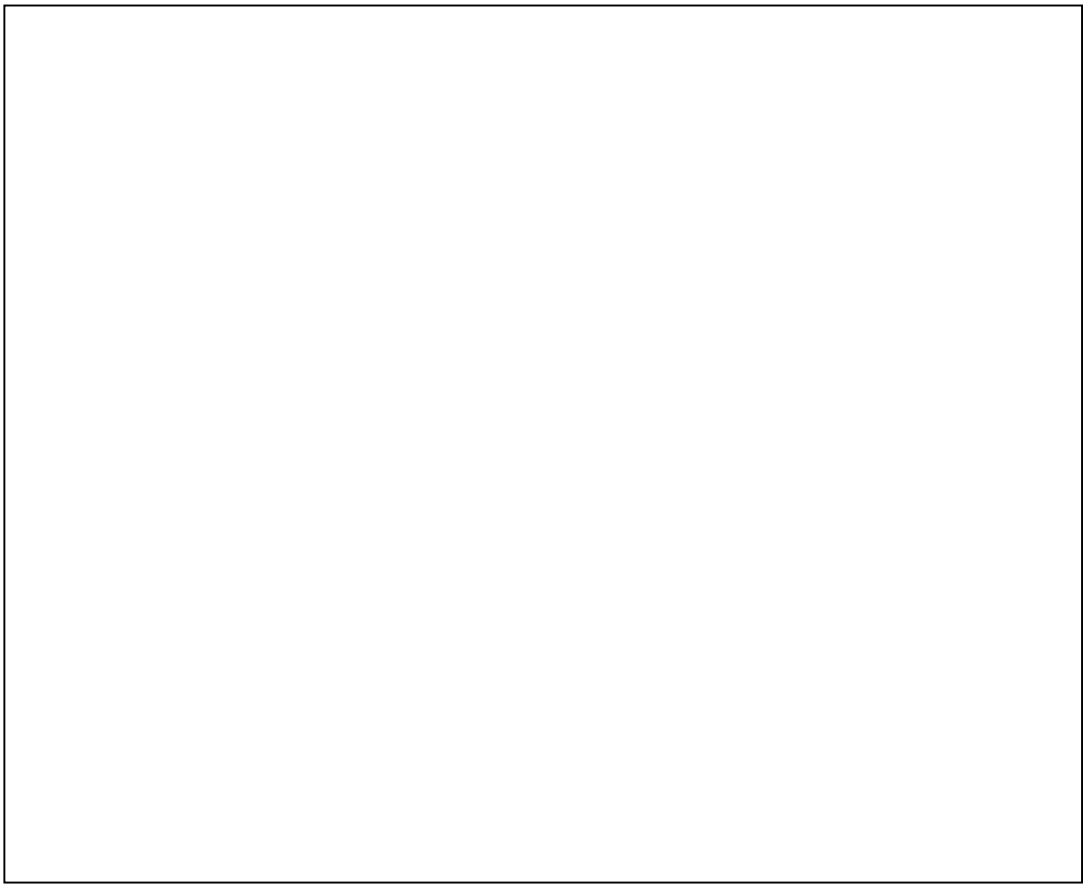
La sicurezza informatica e' uno dei componenti indispensabili per un uso professionale delle tecnologie di Internet

- privacy, identita' degli utenti, integrita' dei dati;
- i limiti della sicurezza informatica coincidono con i limiti dell'uso professionale dei sistemi Internet.

Gli attacchi informatici rendono piu' difficile l'uso di Internet per scopi professionali

- Costi economici, cattiva pubblicita', perdita di efficienza e competitivita', possibile responsabilita' civile/amministrativa;
- Aumentano i RISCHI connessi all'utilizzo delle tecnologie Internet.

 4



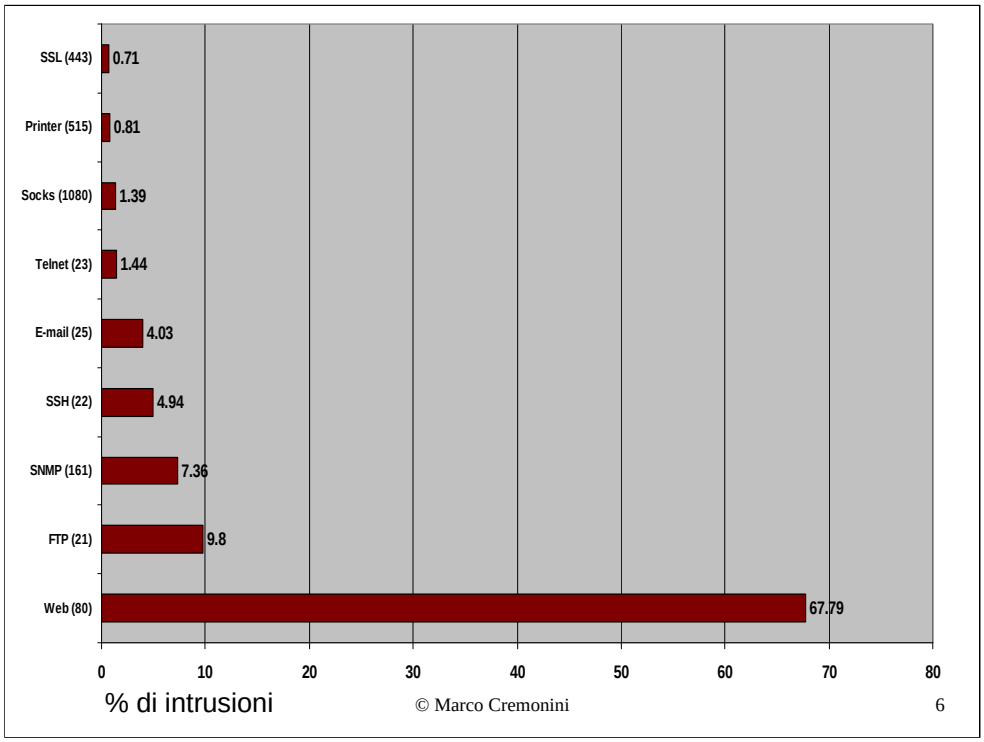
Costi di una interruzione di servizio

- Incidenti di sicurezza informatica causano spesso interruzioni di servizio;
- Un numero crescente di organizzazioni basa la propria operativita', presenza sul mercato e rapporti con partner e clienti sui propri sistemi informativi;
- I costi sono sempre ingenti, per alcune tipologie di aziende possono essere elevatissimi;

Settore Industriale	Costo Orario	Costo Orario per Dipendente
Energia	$2,817,846	$569.20
Telecomunicazioni	$2,066,245	$186.98
Manufatturiero	$1,610,654	$134.24
Finanza	$1,495,134	$1,079.89
Information Technology	$1,344,461	$184,03
Assicurazioni	$1,202,444	$370.92
Commercio	$1,107,274	$244,37
Farmaceutica	$1,082,252	$167.53
Bancario	$996,802	$130.52
Alimentari/Bevande	$804,192	$152.10
Chimica	$704,101	$194.53
Trasporti	$668,586	$107.78
Sanitario	$636,030	$142.58
Elettronica	$477,366	$74.48
Informazione	$340,432	$119.74
Alberghiero	$330,654	$38.62
Valore Medio	$1,010,536	$205.55

 5

Fonte: IT Performance Engineering & Measurement Strategies: Quantifying Performance Loss, Meta Group, October 2000.



Fonte: ISS Internet Risks 12/2001 – 03/2002

2002 CSI/FBI Computer Crime and Security Survey

40% ha riportato intrusioni da Internet;

40% ha riportato denial of service;

85% ha riportato virus/worm;

Sorgente frequente degli attacchi:

Internet: 74% Sistemi interni: 33% Modem: 12%

34% ha denunciato almeno un'intrusione alle autoritá.

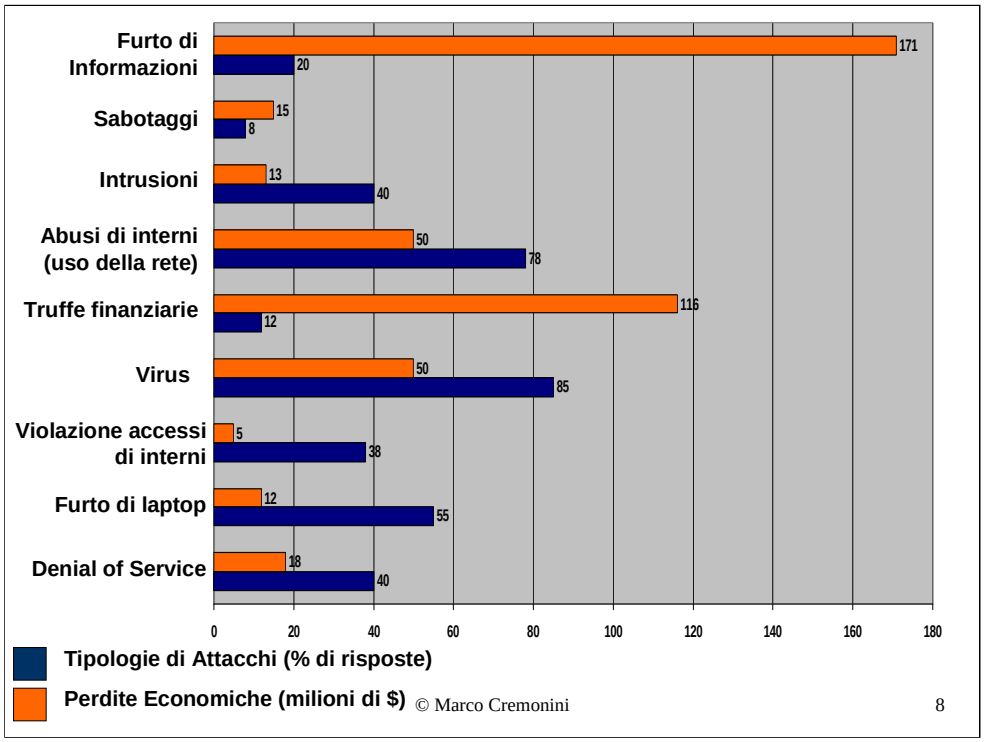
 7

Il rapporto tra attacchi provenienti da Internet e attacchi provenienti dall'interno di una rete si e' capovolto nel corso degli ultimi 2-3 anni.

La percentuale di attacchi denunciati alle autorita', pur rimanendo miniritaria, e' raddoppiato negli ultimi 4 anni.

Gli attacchi di tipo denial of service hanno subito un incremento esponenziale nel corso degli ultimi 3 anni.

Analogamente per la diffusione di virus/worm nel corso del 2000 e 2001.



Notare la differenza evidenziata tra "Furto di informazioni", "Truffe finanziarie" e tutti gli altri.

Come si spiega? Cosa ci mostrano questi dati?

Il reale impatto economico non dipende ne' dal numero di attacchi e neppure dalla opinione comune che identifica spesso nei virus o nei web defacement le principali minacce informatiche.

I rischi reali e piu' severi sono connessi con le attivita' e gli asset critici di una organizzazione: transazioni finanziarie e dati proprietari.

"… coloro che cercano informazioni sono piu' abili grazie a tecnologie e tecniche piu' sofisticate. Due fattori aggiuntivi sono cresciuti drasticamente nel corso degli anni:

1. La consapevolezza che le informazioni detenute dalle organizzazioni hanno un valore rilevante;
2. Il valore delle informazioni stesse.

… Internet ha reso piu' facile il compito di coloro che vogliono impossessarsi di informazioni, le organizzazioni avvertono maggiormente il pericolo di una perdita dei loro dati critici poiche' il possesso di questi si riflette direttamente in vantaggi competitivi, quote di mercato e ricavi significativi. …"

CSI/FBI 2002

 9

Due punti rilevaanti vengono messi in risalto nel commentare la voce "Furto di informazioni":

1) Sempre piu' esiste la consapevolezza del valore e dell'importanza critica dei dati proprietari;
2) Il valore attribuito alle informazioni di proprieta' di una organizzazione cresce.

L'apertura ad Internet rende piu' facile il furto di informazioni proprietarie, cosi' come le tecniche utilizzate per compiere intrusioni si affinano.

Questo viene percepito sepre piu' come un rischio reale e grave dalle organizzazioni.

"… Il volume di transazioni finanziarie condotte per via telematica e' aumentato enormemente nel corso dell'ultimo decennio.

…Le organizzazioni spesso realizzano sistemi che hanno scarsa se non alcuna sicurezza sia nei loro aspetti architetturali che procedurali. Viene spesso annunciato che le misure di sicurezza verranno aggiunte "in seguito", dopo l'implementazione per poter soddisfare I tempi di rilascio, sfortunatamente "in seguito" non arriva mai. …

Le frodi finanziarie non vengono rese pubbliche per paura di cattiva pubblicita'. Questo comporta inoltre che il top management di molte organizzazioni non conosca questi casi ed assuma quindi che tali rischi non esistano. …"

CSI/FBI 2002

 10

Si evidenzia che:

1) Il numero di transazioni finanziarie realizzate elettronicamente ha avuto una crescita esponenziale nell'ultimo decennio;
2) Le organizzazioni realizzano spesso applicazioni con pessima sicurezza, sia a livello architetturale che funzionale; spesso si sceglie di implementare misure di sicurezza 'successivamente' per non ritardare le scadenze (time-to-market) ma in realta' tali misure non vengono realizzate mai;
3) Le truffe legate a transazioni finanziarie spesso non vengono rese pubbliche per paaura di cattiva pubblicita'. Una conseguenza di cio' e' che I responsabili di molte organizzazioni traggono la falsa impressione di che tali frodi non accadano;

Intrusione: Qualunque tipo di accesso o tentativo di accesso non desiderato alle risorse del sistema informativo.

- Prevenzione
- Monitoraggio

} **INTRUSION DETECTION**

Perchè Prevenzione E Monitoraggio?

- Esistono rischi che si vogliono ridurre;
- Nessuna soluzione garantisce l'annullamento dei rischi;
- Indispensabile conoscere sia lo stato del sistema che il contesto.

© Marco Cremonini 11

Ogni metodologia o soluzione utile a **prevenire** intrusioni e' di grande beneficio per un'organizzazione ma nessuna soluzione garantisce la completa inviolabilita'. Per questo, il **monitoraggio** di quanto accade all'interno o sul perimetro del proprio sistema informativo e' indispensabile.

Senza un efficace monitoraggio, ogni soluzione nel campo dell'Intrusion Detection risulta largamente inefficace.

Non esiste alcuna soluzione che garantisce la completa sicurezza.

NETWORK SECURITY

ANALISI DEI RISCHI (risk analysis)

- problematiche, vulnerabilita', metodi

- RIDUZIONE DEI RISCHI (risk mitigation)
  - contromisure gestionali, operative, tecnologiche

LIVELLO DI RISCHIO ACCETTABILE RELATIVAMENTE AL CONTESTO E AL MOMENTO

 12

Sicurezza Informatica:

L'Approccio Tradizionale

- LA TECNOLOGIA RISOLVE I PROBLEMI DI SICUREZZA

  - Crittografia, PKI, firma digitale, autenticazione biometrica, firewall, intrusion detection system, virtual private network, etc.

- LA TECNOLOGIA PUO' RESPINGERE LE MINACCE
- LA TECNOLOGIA RENDE SICURA UNA AZIENDA

 13

Sicurezza Informatica:

***L'Approccio Tradizionale* SPESSO NON FUNZIONA**

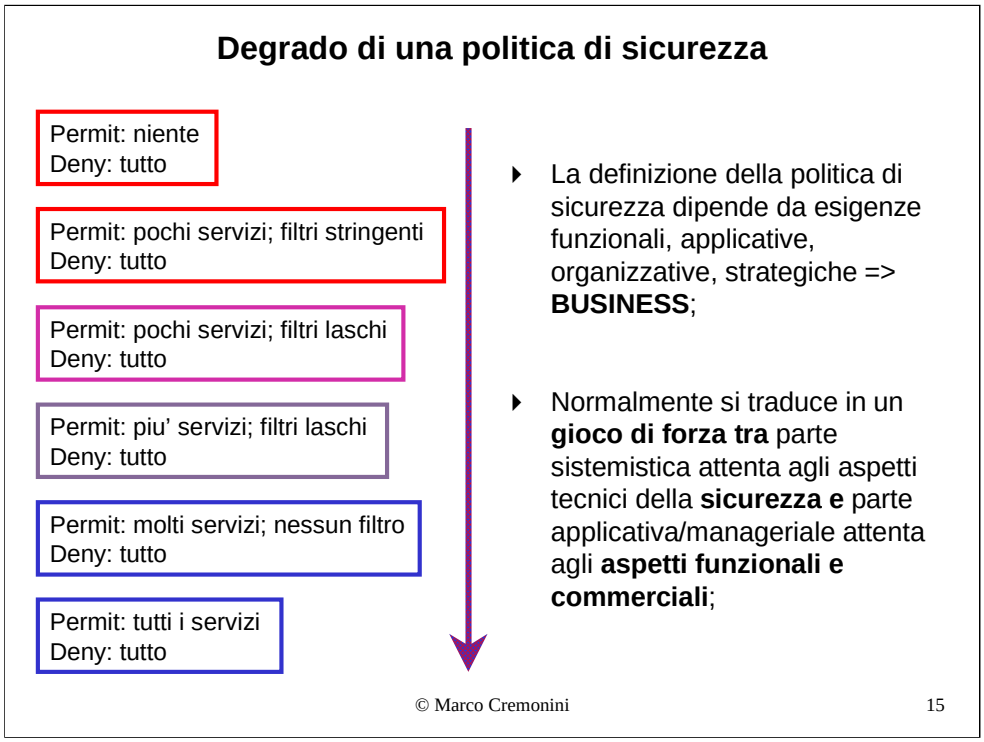
- I RISCHI CONNESSI LA SICUREZZA INFORMATICA SI AGGRAVANO

  - Nonostante le tecnologie per la sicurezza informatica migliorino sempre piu', gli attacchi ai sistemi diventano sempre piu' frequenti, diffusi e gravi nelle conseguenze

- LE PROSPETTIVE FUTURE NON APPAIONO POSITIVE

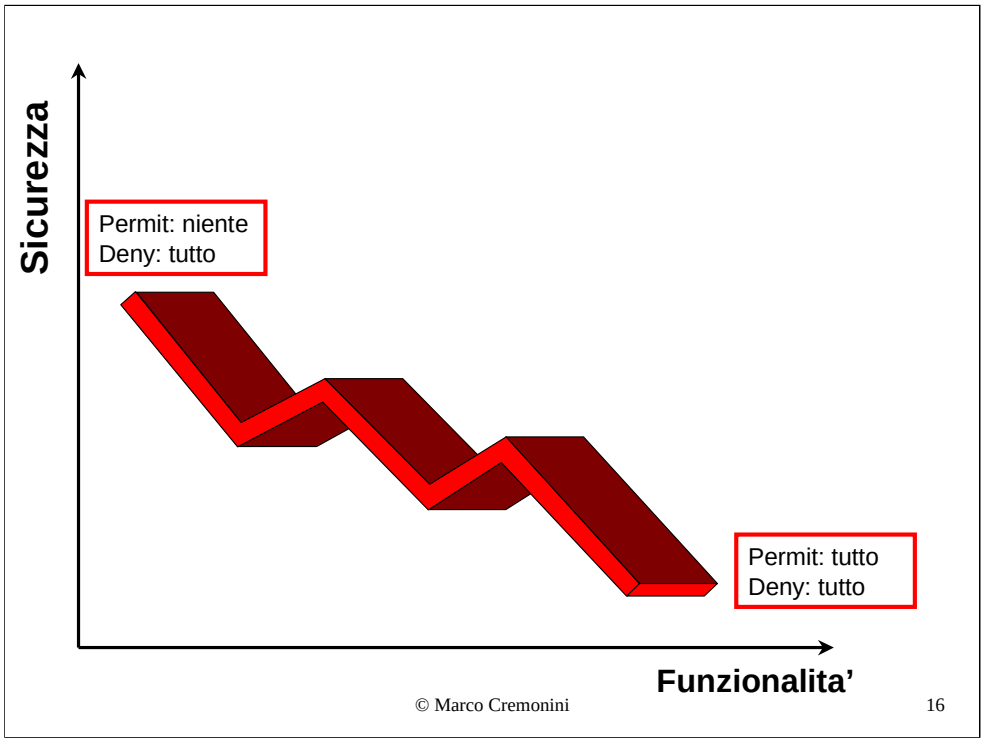
  - maggiore dipendenza dalla tecnologia informatica e dalle reti, pubblico piu' vasto, aumento enorme dei servizi interattivi e delle interconnessioni via Internet

 14



Una politica di sicurezza stringente, molto spesso, tende a venire rilassata sotto la spinta delle richieste di maggiori funzionalita' (applicative, di comunicazione, etc.).

Le decisioni manageriali, commerciali, strategiche di una organizzazione tendono, di norma, a privilegiare l'incremento delle funzionalita', poiche' queste si riflettono immediatamente (breve periodo) in maggiore offerta commerciale, maggiori possibilita' di interoperare, gestione remota, etc.



Le esigenze di business, fino ad oggi almeno, hanno sempre teso verso un incremento continuo e incontestabile delle funzionalita' dei sistemi, dell'automazione dei task degli utenti, dell'arricchimento dell'interfaccia grafica, delle possibilita' di interconnessione e della intuitivita' nell'uso.

Tutto cio', spesso, nonostante le limitazioni che ragioni di sicurezza avrebbero richiesto.

La figura esprime quindi la tendenza "naturale" nell'evoluzione dei sistemi verso un degrado del livello di sicurezza complessivo.

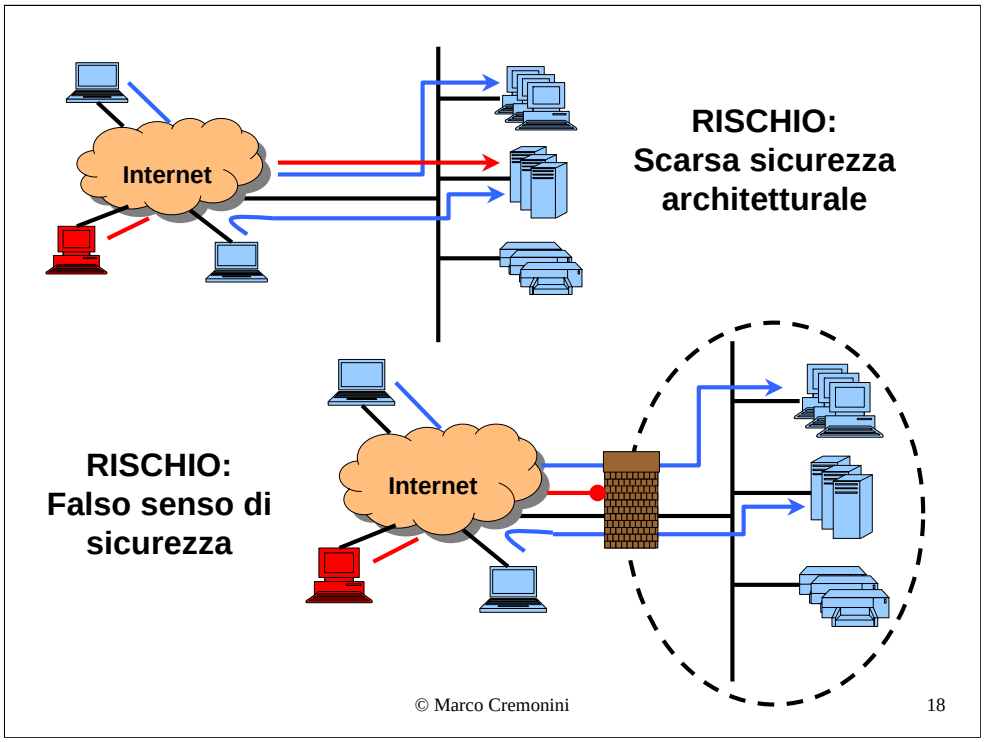
"…Domandiamoci perche' i firewall hanno avuto cosi' successo sul mercato, consideriamo il numero di firewall configurati cosi' male da essere del tutto inefficaci e i molti progetti che avrebbero portato a prodotti molto piu' efficaci e che non hanno avuto alcun successo.

I firewall sono adottati universalmente perche' il mercato ha iniziato a richiedere che le societa' li adottassero. Il costo di non avere un firewall e' di rischiare di non ricevere una certificazione o addirittura essere ritenuti co-responsabili in una causa legale per non essersi adeguati agli standard industriali accettati.

Il risultato e' che cio' che importa e' di poter dichiarare di avere un firewall, qualunque cosa questo possa significare. …."

Bruce Schneier - Counterpane Inc.

 17



Caso 1: Nessuna sicurezza perimetrale

- minore sicurezza, teorica, della rete;

- possibile attenzione alla sicurezza dei singoli host e delle loro interconnessioni (hardening).

Caso 2: Componente di sicurezza perimetrale

- piu' sicurezza, teorica, della rete;

- possibile scarsa attenzione alla sicurezza dei singoli host e delle loro interconnessioni;

- sicurezza della rete delegata interamente alla politica implementata sul firewall.

Possibili conseguenze

Caso 1: livello di sicurezza non ottimale ma attenzione rivolta alla gestione e al monitoraggio.

Caso 2: FALSO SENSO DI SICUREZZA.

Gravita' dei Rischi

FALSO SENSO DI SICUREZZA

E' questo il rischio piu' grave e meno gestibile, l'avversario di ogni tecnologia, progetto e sistema di sicurezza. Questa la reale vulnerabilita' sfruttata dalla grande maggioranza delle intrusioni.

SCARSA SICUREZZA PERCEPITA

Il riconoscimento dell'insufficiente grado di sicurezza rende possibili azioni correttive preventive. Questo diminuisce l'esposizione ed il rischio.

Il falso senso di sicurezza spiega perche', da un lato il 70-80% delle organizzazioni disponga di firewall e sicurezza perimetrale, e dall'altro le intrusioni siano cosi' numerose e talvolta realizzate in maniera molto semplice.

Ancora, per questo motivo non e' sufficiente (anzi e' addirittura controproducente) porre l'attenzione solo sui prodotti e I singoli componenti ma occorra valutare il sistema complessivo, disporre degli strumenti e delle conoscenze per analizzare lo stato di un sistema e prevedere una gestione dell'infrastruttura nel suo complesso.

La sicurezza e' un processo non un prodotto

- Sicurezza di un sistema come catena di molti componenti interoperanti e progettati in una infrastruttura omogenea.
- L'anello piu' debole determina il grado di sicurezza generale.
- Il grado di sicurezza ottimale per un sistema e' il frutto di un bilanciamento tra costi da sostenere e benefici ottenibili.
- Un sistema sicuro e' quello che garantisce che i rischi presenti siano solo quelli ritenuti accettabili.

 20

Come si valuta quindi una infrastruttura di sicurezza? Come si valutano i benefici ottenuti a fronte dei costi sostenuti?

Il prodotto della sicurezza non e' cosi' tangibile come nel caso di altre tecnologie, non ho risultati certi e misurabili.

Se non subisco intrusioni, incidenti, e' grazie ai sistemi di sicurezza oppure no?

Se non ho mai subito gravi incidenti, perche' investire in sicurezza informatica?

Sicurezza informatica:

- costi di gestione, sviluppo, aggiornamento;
- skill;
- modifica dello sviluppo delle applicazioni;

AUMENTO DELLA COMPLESSITA' DEI SISTEMI

⇩

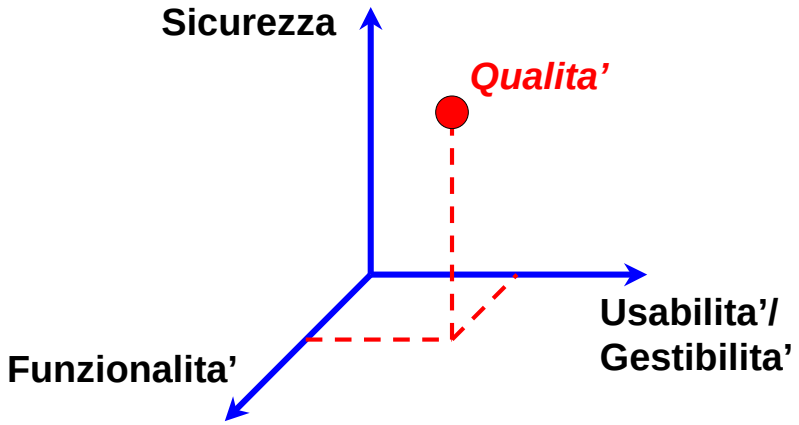
MINORE SICUREZZA INFORMATICA

- maggior numero di errori di progettazione e programmazione
- interconnessione tra sistemi eterogenei, sistemi multi-componenti
- difficolta' di comprensione del funzionamento da parte degli utenti
- difficolta' di analisi, difficolta' di eseguire test accurati
- inefficacia del meccanismo delle patch

 21

PROGETTAZIONE DI UN SISTEMA SICURO

la sicurezza e' una componente essenziale di un prodotto di qualita'



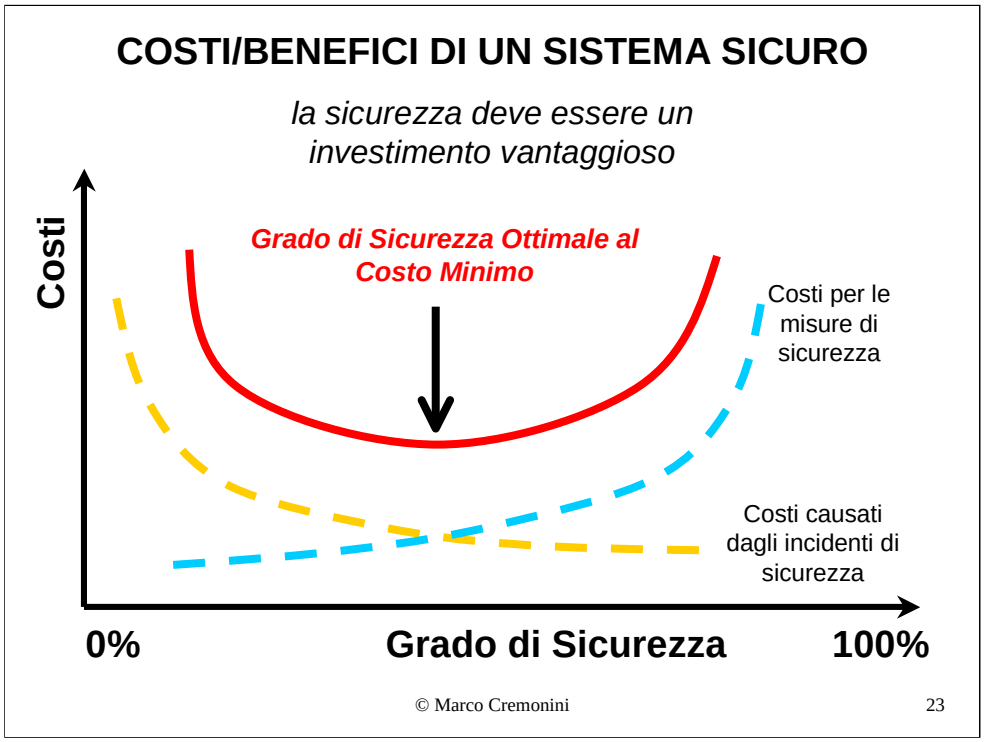
 22

La Sicurezza si aggiunge alle tradizionali dimensioni di Funzionalita' e Usabilita'/Gestibilita'.

(Usabilita': utilizzo da parte degli utenti finali; Gestibilita': gestioone da parte degli amministratori dei sistemi informativi)

La progettazione di un sistema sicuro e' quindi sempre il risultato di un bilanciamento tra questi attributi fondamentali, nessuno dei quali puo' essere considerato isolato dagli altri.

La combinazione delle caratteristiche di Funzionalita', Usabilita'/Gestibilita' e Sicurezza determina la **Qualita'** di un sistema informatico.



La sicurezza TOTALE non e' ne' un risultato possibile da ottenere e neppure un obiettivo conveniente da perseguire

- limiti tecnologici;
- costi non sostenibili.

La mancanza di sicurezza non e' uno stato accettabile

- costi dovuti ad incidenti troppo elevati

La sicurezza deve essere ADEGUATA alle esigenze aziendali:

- permettere lo sviluppo di nuovi servizi, soddisfare utenti/clienti, etc
- permettere un efficace utilizzo della infrastrutture tecnologica
- garantire il corretto uso delle risorse aziendali

Per ogni tecnologia o procedura di sicurezza, occorre quindi sempre domandarsi:

1. **Quali problemi risolve?**
2. **Quanto efficacemente risolve tali problemi?**
3. **Genera nuovi problemi?**
4. **Quali sono i costi, sia economici che sociali?**
5. **Dalle risposte date ai punti precedenti, si conclude che I benefici sono maggiori dei costi?**

 24

1. Quali problemi risolve? Potrebbe sembrare banale ma molti progetti in materia di sicurezza (utilizzo nuove tecnologie, disegno di architetture, progetto di sistemi) vengono proposto senza che siano chiariti quali problemi si vorrebbero concretamente risolvere e addirittura quali siano I problemi esistenti.
2. Quale efficacia ha la soluzione? Molto spesso vengono presentati I problemi da risolvere e a fronte di questi si propongono soluzioni dall'efficacia solo teorica, senza nessun riscontro pratico, senza alcuna analisi dell'efficacia della particolare tecnologia o implementazione.
3. Nascono nuovi problemi? La sicurezza e' un processo complesso nella gestione e strettamente correlato con le infrastrutture e i sistemi in essere. E' facile constatare effetti collaterali non previsti e dannosi a seguito di una riprogettazione o l'adozione di nuove procedure e tecnologie.
4. Costi? I costi sono di generi differenti. Economici (hardware, software, riconfigurazioni, modifiche a sistemi, assistenza, skill, etc.) ma anche sociali (maggiore complessita' gestionale, minore flessibilita', procedure decisionali piu' complesse, necessita' di formazione, monitoraggio, motivazioni del personale, etc.)
5. A fronte di quanto analizzato nei punti precedenti, le decisioni di progetto devono risultare ben ponderate, mai scontate.

"… La network security non e' un problema che la tecnologia possa risolvere. …

Molte organizzazioni investono poco in sicurezza, perche' da un lato, i costi sono rilevanti mentre, dall'altro, i rischi derivanti dall'ignorare la sicurezza sono percepiti come ridotti. Per la stessa ragione economica i produttori di software investono poco nel rendere sicuri i loro prodotti. I costi per progettare un prodotto realmente sicuro sono alti, e il mercato richiede funzionalita' innanzi tutto.

La network security e' quindi un problema economico, e per affrontarlo nelle sue basi occorre concentrarsi sulle motivazioni economiche …comprendere queste motivazioni e' la chiave per comprendere oggi la sicurezza informatica.

Bruce Schneier - Counterpane Inc.

 25