Istituto di Scienza e Teonologie dell'Informazione "Alessandro Faedo"
Politica della Sicurezza Informatica: Analisi generale del rischio

A cura di Carlo Carlesi

Scopo

La sicurezza informatica ha l`obiettivo di garantire, riducendo i rischi, un adegauto grado di protezione del bene informativo costituito dall'insieme delle risorse tecnologiche (personal-computer, server, unita' di rete, applicazioni software etc) e delle informazioni elettroniche (ovvero dei dati mantenuti su supporti elettronici).
E' abbastanza evidente che solo da un analisi dei rischi a cui possono essere sottoposte le diverse componenti del bene informativo che e' possibile individuare l'insieme delle contromisure, fisiche, logiche ed organizzative in grado di abbattere l'entita' di tali rischi.
Tenuto conto che la sicurezza ha un costo, e che questo costo deve essere commisurato al "valore" del bene che si vuole proteggere e' utile definire le componenti del bene informativo e per ciacuna componente un proprio livello di sicurezza, cioe' stabilire l'insieme appropriato delle misure di sicurezza da adottare per rendere accettabile il livello di rischio rimanente.
Definiamo di seguito quali sono le principali componenti oggetto della sicurezza informatica dell'ISTI e quali sono i rischi generali a cui possono essere sottoposti.

Componenti della sicurezza informatica

Come si e' detto, il bene informativo, oggetto della sicurezza informatica e' costituito dall'insieme delle risorse tecnologiche e dalle informazioni elettroniche.

Definiamo risorse tecnologiche le seguenti componenti:

A- i sistemi e le altre risorse hardware:
- Sistemi personali ((Desktop Computer)
- Sistemi Comuni/condivisi (Workstation)
- Server dedicati ad applicazioni intranet
- Server dedicati ad applicazioni internet
- Supporti elettronici per il mantenimento dei dati

B- le risorse di rete:
- Dispositivi di rete locale/internet (hub, router, switch)
- Dispositivi di accesso remoto (terminal server)
- Dispositivi di comunicazione remota (video conferenza)

C- le risorse software:
- Programmi applicativi
- programmi software acquistati
- programmi software "Open Source / Freeware"(in produzione)
- programmi software prodotti internamente
- Sistemi operativi (acquistati/open source)

Definiamo informazioni elettroniche:

D- i.dati/oggetti disponibili su supporto elettronico acquistati e/o prodotti:
- Dati comuni/semplici
- Dati sensibili/personali
- Dati amministrativi
- Dati classificati
    - Confidenziale
    - Riservato
    - Segreto
- Dati soggetti a Copyright

E- le informazioni ottenibili mediante accesso a:
- banche dati elettroniche a pagamento e/o libere

- sistemi informativi esterni pubblici e/o privati
- sistemi informativi interni pubblici e/o privati
- cataloghi pubblici e/o privati

Ai fini del presente lavoro, definiamo inoltre:

- "**Sistema informatico**" il sistema costituito da diversi e piu' componenti indicate ai punti A-E precedenti;
- "**Applicazione**" servizio reso e/o ottenuto mediante l'uso del sistema informatico.;
- "**Sistema Informativo**" l'insieme delle applicazioni integrate con regole organizzative e procedure deputate all'acquisizione, elaborazione, memorizzazione, ritrovamento, scambio e trasmissione delle informazioni.

Rischi informatici

I rischi informatici riguardanti il sistema IT dell'ISTI si possono classificare in:

- rischio di perdita parziale o totale di risorse harduare;
- rischio di perdita parziale o totale di risorse software;
- rischio di perdita parziale o totale di informazioni e dati;
- rischio riguardo le componenti del "sistema informatico";
- rischio riguardo le "applicazioni" e i "sistemi informativi";
- rischio di uso improprio e/o illecito;
- rischio di perdita di immagine a seguito di incidenti informatici.

Il danno economico che deriva, dal verificarsi l'evento del rischio, puo' essere misurato applicando vari parametri; tuttavia ai fini della politica di Istituto si conviene di valutare il danno secondo i seguenti tre parametri:

- valore di mercato dell'oggetto;
- perdita di produttivita' e fruibilita' dei servizi resi e/o ricevuti;
- perdita di immagine.

Mentre e' abbastanza facile misurare il valore di mercato dell'oggetto perso o danneggiato, non sempre e' semplice misurare il valore della "perdita di immagine" o della "perdita di produttivita'" conseguente al ritardo o alla mancanza di uno specifico servizio per un certo periodo di tempo. Queste ultime misure, dipendono ovviamente dall'uso funzionale a cui la risorsa e' destinata e chiaramente come vederemo nel seguito anche le misure di prevenzione e quindi il livello di sicurezza da applicare saranno in funzione della criticita', importanza e valore della risorsa e del contesto strategico in cui la risorsa e' impiegata.

Analisi del rischio

I rischi riguardanti le componenti del "sistema informatico" derivano principalmente dalla possibile perdita parziale o totale di risorse.

Rischi di perdita parziale o totale di risorse hardware

Il rischio della perdita totale o parziale di una apparecchiatura fisica (hardware) e' ovviamente legato alla probabilita' che si verifichi un guasto parziale o totale dell'apparecchiatura stessa che puo' essere dovuto:

- a un fattore esterno quale allegamento, incendio o altro, non prevedibile, fortuito e non intenzionale;
- ad azione dolosa ed intenzionale da soggetti interni e/o esterni all'Istituto;
- all'invecchiamento naturale (fisiologico) della risorsa;
- alla mancanza di una opportuna manutenzione ordinaria,
- ad errore umano non intenzionale e/o a un cattivo uso della risorsa;

- all'accesso fisico e/o virtuale non autorizzato della risorsa (intrusione).

Rischi di perdita parziale o totale di risorse software

Il rischio di perdita totale o parziale di una risorsa software puo' in alcuni casi risultare di difficile valutazione e dipende ovviamente dal tipo di risorsa.
Il rischio prevalente per una risorsa software puo' derivare da:

- guasto e/o danneggiamento del supporto elettronico di memorizzazione (cd-rom, dischetto, nastro, disco etc);
- errori e/o conflitti con altre applicazioni;
- errori e/o conflitti del sistema operativo;
- cancellazione o danneggiamento dovuto a errori umani o del software stesso;
- cancellazione o danneggiamento dovuto a virus o a intrusioni illecite;
- perdita della licenza d'uso e/o rispetto delle norme di "Copyright"

Rischi di perdita parziale o totale di dati e informazioni elettroniche

Il rischio di perdita totale o parziale d'informazioni e/o dati puo' in alcuni casi risultare di difficile valutazione e dipende ovviamente dal tipo d'informazione e/o dato derivano principalmente da:

- guasto e/o danneggiamento del supporto di memorizzazione;
- accesso ed uso non autorizzato a seguito di intrusioni con conseguente:
    - perdita di riservatezza: ovvero, utilizzo indebito di informazioni/dati
    - perdita di integrita': ovvero alterazione e/o manipolazione indebita delle informazioni/dati;
    - perdita di disponibilita': ovvero, perdita dell'accesso controllato alle informazioni/dati.

Rischio riguardo le "applicazioni" e i "sistemi informativi"

I rischi riguardanti le applicazioni e i sistemi informativi oltre a quelli gia' considerati riguardanti componenti specifiche, derivano principalmente da un uso scorretto delle risorse. L'uso non corretto puo' manifestarsi a seguito di azioni involontarie (errore umano) o volontarie ad opera di soggetti interni all'istituto o esterni. In particolare, I sistemi e le applicazioni ched hanno attivita' connesse all'uso di risorse di rete via Internet sono candidate a subire maggiormente attacchi informatici esterni.

Tipologie di attacco ai sistemi informatici connessi alla rete Internet.

Un attacco intenzionale ad un sistema informatico, connesso alla rete Internet, puo' essere lanciato da un qualsiasi posto nel mondo, in un qualsiasi momento. Gli attacchi possono assumere una grande varieta' di forme, e finalita' tra cui citiamo l'accesso illecito al sistema, la diffusione di codice malizioso (virus) e il diniego di servizio ("denial of service"). .
Consideriamo le seguenti tipologie di attacco:

a) *Accesso non autorizzato ai sistemi di informazione*.
Questo tipo di attacco, puo' avere la finalita' di copiare, modificare o distruggere dati, oppure di accedere a servizi con accesso condizionato. Molto spesso, tuttavia, si riscontrano intrusioni anche su macchine che non contengono dati sensibili e di particolare valore, solo per poterle utilizzare in attacchi ad altri obiettivi e rendere il piu' difficile possibile risalire all'attaccante. Le tecniche di intrusione vanno dallo sfruttamento di informazioni interne, all'intercettazione di password di accesso o allo sfruttamento di "bachi" software di talune applicazioni (buffer overflow, etc).

b) *Interruzione del funzionamento dei sistemi di informazione*
Questo tipo di attacco, comunemente indicato come "denial of service" (DoS), mira principalmente ad interrompere l'erogazione dei servizi del sistema attaccato. Ci sono parecchi modi di portare questo tipo di attacco, tra cui quello di saturare il sistema attaccato mediante l'invio continuo e ripetuto di richieste ad opera di piu' sistemi contemporaneamente (molto spesso a loro volta compromessi per questo scopo), o attraverso la distruzione di dati e o parti di programmi del sistema attaccato.

c) *Esecuzione di software "maligni" che modificano o distruggono i dati***.**
Questo tipo di attacco generalmente noto con il nome di "virus", e condotto molto spesso atrraverso il servizio di posta eletrronica, e' tra i piu' diffusi proprio perche' ha la finalita' di replicarsi a macchia d'olio da un sistema all'altro. Ci sono "virus" che creano disfunzioni ma non danneggiano in modo irreversibile il sistema colpito, altri che invece distruggono dati e sistema operativo e talvolta creano anche guasti hardware.

d) *Intercettazione di comunicazioni e falsificazione della propria identita*'.
L'intercettazione dolosa delle comunicazioni ("sniffing"), oltre a compromettere la riservatezza dei dati utente e' spesso utilizzata per ottenere informazioni da utilizzare a fini dolosi, come l'usurpazione dell'identita' di un soggetto ("spoofing") o l'acquisizione di password di accesso su altri sistemi.