Vulnerabilità di un Sistema Informativo

Un Sistema Informativo e le principali tipologie di minacce alla "vulnerabilità" e come le tecniche di backup possono essere utilizzate come contromisure a tali minacce.

F. Donatantonio

Sistema informativo

Il **sistema informativo** è costituito dall'insieme delle informazioni utilizzate, prodotte e trasformate da un'azienda durante l'esecuzione dei processi aziendali. Nei primi anni '80 l'informatica si avvicinò alle medie e grandi imprese con l'avvento dei primi computer, solo successivamente furono sviluppati dei moduli software che qualche anno dopo avrebbero reso i sistemi informativi automatizzati e rispondenti alle esigenze lavorative e dei clienti.

Immaginiamo un'azienda che negli anni '70 si trovava a gestire quotidianamente il proprio magazzino, i prodotti, le attrezzature e i mezzi a propria disposizione. Il mantenimento di questi dati e di tutte le informazioni connesse era riservato esclusivamente ad archivi e faldoni cartacei, gestiti e aggiornati da addetti aziendali. Le procedure di un sistema informativo erano all'epoca più umane ma anche più complesse, sensibili agli errori e come ultimo fattore, non di poco conto, difficili da gestire con l'aumento dei dati. Altro fattore discriminante di un sistema informativo non automatizzato era la poca confidenzialità che questo offriva ai clienti di un'azienda. Difatti i dati e le informazioni interessanti per un cliente erano anch'esse racchiuse in faldoni e cartelle, accessibili tramite un addetto che magari non sempre ricordava la locazione fisica di quest'ultimi.

Le *tecnologie informatiche* offrono invece oggi grandi potenzialità (*informatizzazione del sistema informativo aziendale*):

- consentono alle aziende di controllare, pianificare e gestire in modo integrato tutte le attività;
- consentono di elaborare velocemente una maggiore quantità di dati ed informazioni di quanto fosse possibile in passato.

Sono così entrati a far parte di un sistema informativo: server, database, computer e reti telematiche; modificando radicalmente il modo di operare e di gestire un processo aziendale.

Nonostante qualche ritardo rispetto alle aziende private, anche la **Pubblica Amministrazione** si è dotata di Sistemi Informativi automatizzati senza trascurare i problemi derivanti dalla sicurezza e dal trattamento dei dati. Difatti un ruolo importante all'interno di un sistema lo ricopre la sicurezza informatica e quindi la salvaguardia da minacce, malfunzionamenti, integrità dei dati e loro divulgazione.

Le componenti da proteggere e salvaguardare sono quindi:

- Hardware (server, firewall, supporti di memorizzazione ed apparecchiature varie),
- Software (sistema operativo, DBMS, ERP, firewall, ecc …)
- Dati (file)
- Apparati di rete (router, switch, cavi, ecc …)

Una Pubblica Amministrazione gestisce i dati dei propri dipendenti, degli utenti nonché le informazioni di carattere economico e strategico. Se poi si considera che un servizio pubblico, anche se il più piccolo sul territorio, è per definizione da ritenersi sempre **efficiente**, **funzionale** e **rispondente alle esigenze** della comunità allora è chiaro come il fattore sicurezza incida radicalmente sul processo organizzativo e di sviluppo di un sistema informativo.

La *Sicurezza Informatica* è caratterizzata da:

- *Segretezza/Confidenzialità*: le informazioni possono essere lette solo da chi ne ha diritto.
- *Integrità*: le informazioni possono essere modificate solo da chi ne ha diritto.
- *Disponibilità*: una risorsa deve essere disponibile quando richiesta.
- *Non Ripudio*: un utente che provoca un danno NON deve essere nella condizione di poter negare le sue colpe.

Chi all'interno di un'azienda o di una Pubblica Amministrazione si occupa di valutare il grado di sicurezza deve tener conto dei *beni da tutelare*, delle *vulnerabilità*, delle *minacce* e dei possibili *attacchi*, nonché in ultimo analizzare e gestire i *rischi* ai quali si può incorrere.

Vulnerabilità

Nonostante sia da scongiurare o comunque da evitare è possibile che un sistema informativo sia soggetto ad alcune vulnerabilità.
Una **vulnerabilità** è un *errore* che genera ripercussioni sulla sicurezza.
Spesso le problematiche che risiedono in un sistema sono legati ad errori, tecnicamente chiamati bachi, all'interno del software, anche se possiamo identificare i seguenti tipi di vulnerabilità:

Vulnerabilità dei componenti informatici:

- Vulnerabilità di Sistemi/Applicazioni.
- Vulnerabilità dei Protocolli.

Vulnerabilità strutturali:

- Vulnerabilità legate alle architetture di rete.

Vulnerabilità organizzativo/procedurali:

- Vulnerabilità procedurale.
- Vulnerabilità organizzativa.

Vulnerabilità di Sistemi/Applicazioni:

- Vulnerabilità del Software:
  Overflow: buffer overflow, stack overflow e heap overflow.
  Format String: vulnerabilità delle format function (fprintf, printf, sprintf, etc...)
- Errori di configurazione: configurazioni poco robuste e/o inadeguate, ad esempio utenze non protette.

Vulnerabilità dei Protocolli:

- Debolezze di progettazione: permettono attacchi di tipo Spoofing, Hijacking e Sniffing.
- Errori implementativi dello stack di rete: permettono attacchi di tipo DoS/DDoS.

Un malintenzionato può sfruttare una delle problematiche sopra elencate per corrompere un sistema informativo. E' possibile ad esempio che qualcuno sfrutti un errore del software o un punto d'accesso ad esso (backdoor) per accedere ai dati e alle informazioni. Oppure che qualcuno "spii" le operazioni compiute all'interno del sistema, catturando magari i dati che viaggiano sulla rete (sniffing) oppure verificando il traffico in ingresso e uscita da un particolare computer (port scanning).
In ultimo un haker esperto potrebbe introdurre in rete un programma apparentemente innocuo che invece rende inutilizzabile alcune funzionalità, deturpa, corrompe o distrugge le informazioni sensibili (trojan e virus).

Pensare ai danni che in una Pubblica Amministrazione possano produrre queste problematiche se trascurate spaventano e preoccuperebbero chiunque. Immaginiamo se qualcuno riuscisse a

corrompere un database e venisse a conoscenza delle informazioni personali di migliaia di persone, ad esempio codici fiscali, coordinate bancarie, informazioni sanitarie, contrattuali o dati di fatture.
Peggio ancora se una persona esterna riuscisse ad entrare in un sistema dopo aver spiato i dati di accesso di un responsabile (login e password) e che quindi abbia la possibilità di operare indisturbato con il software per fini poco leciti. Costui potrebbe modificare alcuni valori all'interno della banca dati operando in maniera pulita e quindi difficilmente individuabile ad una prima analisi dei responsabili della sicurezza.

I casi a cui si può andare incontro sono innumerevoli, la cosa certa è che tutti in una maniera o in un'altra portano danni alla sicurezza di un sistema informativo. Risulta quindi necessario porre importante interesse alle tecniche di sicurezza onde evitare che un malfunzionamento o un attacco crei danni anche irreparabili.

Tra le tecniche più utilizzate ci sono:

- *Antivirus*
- *Antispyware*
- *Firewall*
- *Firma digitale, Crittografia*
- *Backup*
- *Intrusion Detection System (IDS)*
- *Network Intrusion Detection System (NIDS)*
- *Sistema di autenticazione*

Backup

La tecnica del **backup** è da ritenersi indubbiamente una delle più utilizzate in qualsiasi ambiente di lavoro, soprattutto nel momento in cui le informazioni presenti in database crescono e si aggiornano rapidamente durante le attività lavorative giornaliere.

Il backup è la copia dei file di un sistema in un'unità rimovibile, allo scopo di recuperare i dati in caso di malfunzionamenti o errori. Con il termine backup si intende sia la copia dei file, sia la procedura necessaria a copiare i dati.
Anche se i motivi per cui si eseguono i backup sono molteplici, si può affermare che il backup serve a *ripristinare i dati persi*. La perdita dei dati può avvenire per svariati motivi, solitamente:

- Cause legate agli operatori e ai sabotatori, persone fisiche (80%)
- Cause tecniche: (14%)
- Cause ambientali: (6%)

Il verificarsi di una qualsiasi delle cause elencate potrebbe significare il blocco dell'intero sistema informatico di un'azienda per un periodo lungo, nonché la perdita di dati importanti.

Immaginiamo ad alcune situazioni cui un'azienda o una *Pubblica Amministrazione* possono andare incontro. Potrebbero ad esempio non essere disponibili i server, costringendo gli utenti a lavorare senza collegamento a Internet, senza posta elettronica, senza fax e senza gestionale. Anche dopo la reinstallazione e riconfigurazione dei server potrebbero esserci disagi, ove non fosse possibile recuperare i file con i dati. Questo potrebbe comportare il reinserimento manuale di tutte le fatture e tutti gli ordini, tutta l'anagrafica clienti e dipendenti e la perdita di tutta la corrispondenza via posta elettronica. Se proviamo solo un attimo a considerare tali situazioni di disagio in un

meccanismo complesso come può essere un'*università* con la perdita di tutti i dati riguardanti studenti, professori, dipendenti; in un attimo verrebbero perse le carriere universitarie, i dati di corsi e esami, nonché la banca dati degli uffici tecnici. E' chiaro come la gravità di fenomeni del genere blocchino per intero anche le più minime funzionalità di un meccanismo che entrerebbe di diritto in uno stato di caos totale.

Le procedure di backup non possono evitare il verificarsi delle cause, ma permettono il ripristino del sistema e il recupero dei dati in periodi brevi (i tempi dipendono dalla politica scelta). Il backup può essere gestito in molti modi differenti e utilizzando supporti diversi, la scelta dipende dai mezzi a disposizione (quanto si vuole spendere in tempo e denaro), dalla priorità di ripristino (per quanto tempo si può permettere di tenere bloccato il sistema informatico?) e da altri fattori analizzati in seguito. Per creare una procedura di backup efficiente è quindi necessaria una attenta analisi del sistema informativo, al fine di definire una strategia di backup adatta alle esigenze aziendali e che garantisca il recupero dei dati persi, in tempi ragionevoli.
Si devono prendere in considerazione molti fattori, i più importanti sono:

- di quali file è opportuno eseguire il backup?
- si esegue un backup di rete o più procedure sui singoli PC?
  frequenza dei backup, quante volte farli? Uno al giorno, uno alla settimana oppure uno al mese?
- quando si deve eseguire la procedura di copia dei dati? Alle otto di ogni mattina, alla sera, etc.
- che tipo di backup eseguire?
- quali tecnologie utilizzare?

La scelta della strategia da seguire dipende essenzialmente quindi dalla natura dei dati da salvare, dalla loro frequenza di utilizzo e aggiornamento. Ad esempio i responsabili della sicurezza potrebbero decidere di effettuare il backup di un determinato archivio ogni pomeriggio sul finire delle attività lavorative dopo aver considerato che tale archivio subisce importanti modifiche ogni giorno (ad esempio i dati di fatture o richieste); d'altro canto su un archivio potrebbe essere effettuato il backup anche mensilmente qualora questo subisca poche modifiche (ad esempio l'anagrafica dei dipendenti).

Entrando nel dettaglio, tra le tecniche di backup comunemente utilizzate si segnalano:

- *Backup a caldo* (o *Hot backup*)
  Backup di un database o sistema di memorizzazione effettuato mentre il sistema è in linea. I dati possono quindi essere modificati mentre il backup è in corso
- *Backup completo* (o *Full backup)*
  Un backup di tutti i file sul sistema.
- *Backup Differenziale*
  Backup cumulativo di tutti i cambiamenti effettuati a partire dall'ultimo backup completo (o full backup). Il vantaggio è il minor tempo necessario rispetto ad un backup completo. Lo svantaggio è che i dati da salvare aumentano per ogni giorno trascorso dall'ultimo backup
- *Backup Incrementale*
  Backup che contiene tutti i file cambiati dall'ultimo backup (completo e incrementale). Il backup incrementale è più rapido di quello differenziale ma richiede tempi di restore più lunghi poiché è necessario partire dall'ultimo backup completo e poi aggiungere in sequenza tutti i backup incrementali
- *Backup Remoto*
  È un servizio di salvataggio dati che sfrutta la connessione internet per trasferire tutti i dati importanti, tramite un software apposito su dei server web

Il responsabile della sicurezza sarà in grado di scegliere la combinazione ideale di tecniche di backup in relazione anche alla disponibilità di supporti di memorizzazione e ai tempi impiegati per effettuare tali operazioni.

Conclusioni

L'evoluzione dei sistemi informativi non può prescindere da uno studio approfondito della sicurezza e della prevenzione dei dati. Con l'avvento dell'era dell'informatizzazione, i rischi sono aumentati in modo esponenziale grazie al fatto che i dati sono accessibili sempre e dovunque tramite la rete. Una pubblica amministrazione deve dal canto suo garantire alla comunità la continuità del servizio, nonché il rispetto degli oneri contrattuali e della riservatezza dei dati, tutti aspetti che pongono in primo piano le strategie di difesa e di ripristino dei dati.
La tecnica del backup è da evidenziare come l'ultima spiaggia in un processo molto più ampio che studi le varie contromisure da adottare in relazione alle diverse esigenze, alla qualità dei dati da preservare e al rispetto delle esigenze e dei diritti del cliente. Effettuare backup giornalieri, programmati o incrementali non pone in sicurezza un sistema, bensì regala un'ancora di salvezza per ripristinare in maniera veloce e ci si augura col minor disagio possibile, una situazione di corruzione del database e del software gestionale. Tale tecnica non può prescindere dalla messa in opera di strategie preventive che permettano di ridurre i rischi alla sicurezza di un sistema informativo, come antivirus, firewall e *antispyware* . Altresì è importante lavorare per ridurre al minimo le vulnerabilità di un sistema, adottando adeguate procedure di verifica e controllo del software utilizzato.