Sicurezza nei sistemi informatici

La sicurezza nei sistemi informatici riguarda sia gli aspetti hardware che gli aspetti software. Considerando le apparecchiature, i principali problemi sono connessi ai guasti che si possono verificare durante il normale funzionamento.
Le applicazioni software non sono soggette a guasti ma solitamente a malfunzionamenti, mentre a livello di sicurezza le preoccupazioni maggiori sono rivolte alla gestione degli accessi ai dati.

• Calamità naturali

Una delle cause che può incidere negativamente, e talvolta in modo irreparabile, sulla sicurezza del sistema informatico di un'azienda nel suo complesso è rappresentata dalle calamità naturali.

Fortunatamente il nostro Paese non è particolarmente colpito da calamità naturali che possono distruggere un'azienda come accade in altri paesi a causa di tifoni o terremoti; le calamità prese in considerazione sono solo quelle connesse a incendi, alluvioni e attentati che sono in genere inferiori rispetto a quelle citate sopra.

Tuttavia alcune aziende hanno sentito il bisogno di dotarsi di procedure particolari che consentano di far ripartire l'insieme delle attività in pochi giorni anche in caso di distruzione totale di un'unità lavorativa composta spesso di migliaia di persone.

Si tratta di costruire norme che definiscano tutte le apparecchiature e tutte le informazioni indispensabili per ripartire, di creare depositi sicuri in cui mettere una copia di tutti i documenti necessari alla ripartenza, e infine di definire quali attività e quali figure aziendali, o esterne all'azienda, devono intervenire secondo una scaletta articolata e prestabilita.

La salvaguardia rispetto a incendi, alluvioni e in qualche misura terremoti, può essere risolta mediante tecniche costruttive particolari, come edifici bunker o comunque che rispettano le norme antisismiche, con un sistema di rilevazione automatica dei fumi collegata ad impianti per la caduta di acqua (in assenza di problemi elettrici) o di polveri sul punto dove sono stati rilevati i fumi.

• Attentati terroristici

Solitamente il blocco del sistema informatico può produrre la paralisi dell'azienda. Il sistema informatico è diventato un elemento fondamentale per l'operatività dell'azienda e per questo può diventare il centro di interesse per chi vuole danneggiare l'attività aziendale. Il sistema informatico può essere al centro di attentati terroristici che possono causare il blocco totale della struttura colpendo un punto, di ricatti da parte della malavita organizzata o più semplicemente da mitomani.

Come risposta le aziende tendono a collocare le principali apparecchiature informatiche in luoghi sempre più protetti al centro delle aziende o in veri e propri bunker, al riparo da chi voglia aggredire con la forza.

• Guasti e interruzioni hardware

Nelle situazioni dove non è consentita l'interruzione dell'attività di un sistema di elaborazione (*downtime*), come per esempio in una banca o in un supermercato, la sicurezza viene garantita nella parte hardware attraverso la duplicazione di parti o dell'intero sistema.

Queste tecniche vengono indicate con il termine **fault tolerance** (tolleranza del guasto) e riguardano principalmente le memorie di massa nei server delle reti e nei sistemi di medie e grandi dimensioni.
Il *fault tolerance* viene realizzato a livelli diversi:

- il metodo più semplice si chiama **mirroring** e consente di avere nelle unità di memoria di massa due copie identiche dello stesso disco (oppure solo di alcuni archivi particolarmente importanti e preselezionati); quando un'operazione di I/O riscontra un errore, l'elaborazione non viene interrotta potendo essa utilizzare la copia alternativa.
- un secondo livello di tolleranza del guasto viene realizzato con la tecnica del **duplexing**, che consiste nella duplicazione dell'unità di controllo dei dischi (*controller*) oltre che dei dischi. L'utente può continuare l'attività di elaborazione anche nel caso di un guasto al controller o al disco, e diminuiscono i rischi di interruzione.
- il terzo livello riguarda la **duplicazione dell'intero sistema**, del server nel caso di reti locali, e del mainframe nel caso di un sistema di grandi dimensioni.
- ci sono a disposizione altre tecniche meno costose rispetto alla duplicazione parziale del sistema, che vengono indicate con la sigla **RAID** (*Redundant Array of Inexpensive Disk*). Questa tecnologia consiste nel distribuire i dati su un insieme di dischi, in modo che sia possibile ricostruire per via matematica tutti i dati eventualmente persi da uno dei dischi.

• Errori del personale

L'enorme sviluppo dell'elettronica moderna consente di accumulare grandi quantità di dati in spazi molto piccoli e secondo modalità che non sono quasi mai simili alle operazioni svolte secondo la gestione manuale, per cui anche errori banali possono produrre disastri.

Le norme per prevenire tali eventualità di solito consistono in:

- una netta separazione tra l'ambiente di esercizio e l'ambiente di sviluppo, per evitare che il programmatore durante le sue prove inquini o peggio distrugga i dati che servono per le procedure aziendali;
- copia periodica di tutti i dati aziendali su supporti di memoria da conservare in luogo sicuro per un successivo ripristino se richiesto: normalmente vengono conservati più salvataggi di giornate differenti al fine di una maggiore protezione;
- intervento di livelli professionali differenti in caso di ripetizione dell'errore in modo da evitare qualsiasi rischio;
- definizione di regole organizzative e figure professionali preposte a verificare tutte le anomalie nei dati di input o di output.

Per ridurre al minimo gli errori del personale operativo si devono prevedere le attività di formazione, tramite corsi di aggiornamento, in modo da sviluppare e consolidare le competenze informatiche delle persone che interagiscono con il sistema informativo aziendale.

• Virus

Tra i problemi di sicurezza che coinvolgono i sistemi software, applicazioni e dati, c'è quello dei virus informatici.

I virus sono programmi chiamati così perché sono stati costruiti con lo scopo di:

- infettare un programma senza alterarne in apparenza il funzionamento;
- rendersi visibili in qualche modo;
- autoriprodursi nell'ambiente in cui sono inseriti creando un'epidemia che può essere dannosa (distruzione di dati e programmi) o solo contagiosa estendendosi a tutti i programmi e a tutti i computer.

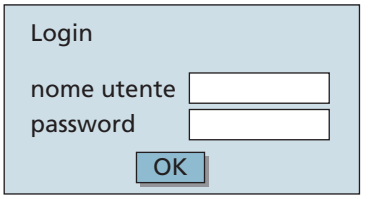
Possono essere prodotti per gioco oppure talvolta con finalità ricattatorie.
Non esiste un modo attraverso il quale distinguere un programma da un virus e quindi un virus diventa tale solo dopo la sua scoperta e la sua denominazione.
La protezione contro i virus può essere realizzata attraverso il controllo sistematico di tutti i supporti che vengono usati. Esistono poi organizzazioni e software house che si sono specializzate nelle identificazioni dei virus e degli effetti che producono, e nella costruzione di programmi vaccino per eliminarli, chiamati **antivirus**.
In alcuni casi la rimozione del virus può richiedere la cancellazione dei programmi danneggiati: pertanto diventa fondamentale il lavoro di filtro sugli accessi, sui dati e sul software, con scopi di prevenzione.
Gli strumenti antivirus devono essere costantemente aggiornati con le definizioni dei nuovi virus scoperti, ma questo non è sufficiente per azzerare le probabilità di essere colpiti da un virus. È quindi opportuno seguire una politica di copie di sicurezza periodiche, in modo tale da poter ripristinare i dati in caso di corruzione o cancellazione da parte di virus.

• Sicurezza e integrità dei dati

La gestione di un sistema di elaborazione ha un aspetto cruciale rappresentato dalla necessità di garantire la **consistenza** dei dati in esso memorizzati, sia nel caso di un computer personale,sia nel caso di sistemi informatici aziendali: i dati devono essere significativi ed essere effettivamente utilizzabili nelle applicazioni. I dati devono quindi essere protetti per impedire perdite accidentali dovute a improvvise interruzioni dell'attività del sistema, guasti hardware o interventi dannosi da parte di utenti o programmi: la protezione deve riguardare anche gli interventi dolosi sui dati dovuti ad accessi non autorizzati con operazioni di lettura, modifica o cancellazione.
In sostanza **sicurezza** significa impedire che il sistema e i suoi dati vengano danneggiati da interventi accidentali e non autorizzati; **integrità** significa garantire che le operazioni effettuate sul sistema e sui dati da parte di utenti autorizzati non provochino una perdita di consistenza ai dati.
Gli archivi elettronici hanno più o meno gli stessi problemi degli archivi cartacei, per esempio un'unità a dischi si può rompere provocando la perdita di tutti i dati in essa contenuti, oppure un errore degli operatori può provocare la cancellazione non voluta di uno o più archivi: pertanto si rende necessaria la copia periodica degli archivi e la conservazione delle copie in posti sicuri.
L'attività di copia di archivi di grandi dimensioni ha durate significative e di solito viene eseguita giornalmente: questa attività si chiama **backup** (salvataggio). L'attività in senso inverso si chiama **restore** (ripristino) e serve per ricaricare su disco tutti o parte degli archivi salvati precedentemente.
L'accesso non autorizzato ai dati rappresenta un altro aspetto di sicurezza legato agli archivi. In un ambiente che comprende tutti i dati aziendali occorre avere una responsabilità centralizzata in grado di distribuire le autorizzazioni e le modalità di accesso.

• Profilazione degli utenti

In generale ad ogni utente viene associato un **profilo** il cui accesso è controllato mediante l'**identificativo dell'utente** (*user ID* o *username*) e la **parola d'ordine** (*password*): il primo rappresenta il nome, che può anche essere pubblico, con il quale l'utente accede alla procedura di riconoscimento (**login**), mentre la seconda rappresenta la parola chiave, di solito scelta dall'utente stesso, che è privata e riservata. Per questo motivo la password dovrebbe essere non banale (nomi di persona, date di nascita, ecc.) e dovrebbe essere frequentemente cambiata. La password deve essere lunga almeno 8 caratteri e deve essere una combinazione di cifre e di lettere.



Al profilo sono poi associati i **diritti di accesso**, cioè le azioni, i permessi e i divieti relativi alle attività svolte dall'utente: quali programmi può utilizzare, quali archivi può consultare, quali permessi su un singolo archivio (solo lettura oppure lettura e scrittura), la possibilità di installare nuovi programmi. Questi controlli vengono realizzati a diversi livelli: gestione delle basi di dati, sistemi operativi, reti di utenti. Essi sono gestiti dall'**Amministratore del sistema** (*system administrator*), che nel personal computer coincide con l'utente stesso, mentre per sistemi più complessi o per le reti è una specifica figura professionale del settore informatico.

• Pirati informatici

Nel linguaggio corrente il termine **hacker** viene usato come sinonimo di *criminale* o *pirata informatico*, anche se il termine corretto dovrebbe essere *cracker.* Esso sta ad indicare persone che si collegano, con sistemi di elaborazione, sfruttando i meccanismi di rete senza avere l'autorizzazione all'accesso: questi inserimenti indesiderati con messaggi o programmi possono anche portare alla paralisi del sistema.

• Crimini informatici e sicurezza

L'Italia si è allineata alle disposizioni comunitarie in materia di provvedimenti legislativi relativi alla sicurezza informatica. La **legge n. 547 del 14 dicembre 1993**, "*Modificazioni e integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica*", stabilisce le pene per **reati informatici** come il danneggiamento di dati e programmi. Ecco alcuni passi significativi della legge. Innanzitutto all'articolo 392 del Codice Penale, dopo il secondo comma è aggiunto il seguente:

> *"si ha altresì violenza sulle cose allorché un programma informatico viene alterato, modificato o cancellato in tutto o in parte ovvero viene impedito o turbato il funzionamento di un sistema informatico o telematico".*

La pena all'art. 420 (*attentato a impianti di pubblica utilità*), si applica anche a chi commette un fatto diretto a danneggiare o distruggere sistemi informatici o telematici di pubblica utilità. Rilevanza penale si ha anche per quanto riguarda la falsità dei documenti informatici.

Art. 615-ter. (*accesso abusivo a un sistema informatico o telematico*).

> *"Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha diritto di escluderlo, è punito con la reclusione fino a tre anni".*

Art. 615-quinquies

> *"Chiunque diffonde, comunica o consegna un programma informatico da lui stesso o da altri redatto, avente per scopo o per effetto il danneggiamento di un sistema informatico o telematico, dei dati o dei programmi in esso contenuti o ad esso pertinenti ... è punito con la reclusione sino a due anni e con la multa sino a euro 10.329"*