Minacce ai dati

Salvaguardare le informazioni

Distinguere tra dati e informazioni.

- I **dati** sono informazioni non ancora sottoposte a elaborazione. I dati possono essere una collezione di numeri, testi o immagini non elaborate. Dall'elaborazione dei dati si ottengono le:
- **informazioni** sono il risultato dell'utilizzo dei dati e della loro eventuale modifica in modo da renderli significativi per la persona che li riceve.

Comprendere il termine crimine informatico.

Il **crimine informatico** è un'attività illegale che avviene utilizzando dei mezzi informatici come la rete Internet o, in generale, un computer. Esempi di crimine informatico includono le frodi informatiche, il furto di identità e l'intrusione nei sistemi informatici.
Le frodi informatiche possono riguardare la riproduzione e/o l'utilizzo di programmi informatici senza la specifica autorizzazione. Infatti, i programmi informatici sono ritenuti opere dell'ingegno e quindi sono tutelati dalla legge sul diritto d'autore. Le frodi informatiche possono riguardare anche la vendita on line di prodotti inesistenti o contraffatti.
I programmi informatici quindi non possono essere usati e duplicati senza autorizzazione.
In generale non è consentito:

1. fare delle copie non autorizzate di un software o di parte di esso;
2. andare a vedere e copiare il modo con cui è stato realizzato;
3. installarlo su diversi computer senza autorizzazione o cederlo ad altri.

Infatti, quando si acquista un programma non si diventa proprietari del software senza alcun vincolo: non si può fare un libero uso del programma, ma si acquisisce soltanto la **licenza d'uso**, detta **EULA**.
EULA o End User License Agreement (accordo di licenza con l'utente finale) è il contratto tra il fornitore del software e l'utente finale. Tale contratto assegna la licenza d'uso del programma all'utente nei termini stabiliti dal contratto stesso. EULA solitamente permette soltanto:

1. di utilizzare il software su un solo computer, salvo diverse indicazioni (contratti multi licenza);
2. la possibilità di fare una ulteriore copia, la copia di sicurezza, del supporto con cui il software è distribuito. È quindi possibile duplicare il cd del programma ma solo per creare la copia di sicurezza.

Quindi è un reato:

1. installare lo stesso programma su più computer, se non è espressamente consentito nella licenza;

2. avere una copia illegale di un programma;
3. scambiare o scaricare tramite internet musica, testi, film soggetti alla tutela del copyright;
4. modificare del software e personalizzarlo per rivenderlo come proprio.

Per riconoscere software regolarmente licenziato si deve verificare il codice del prodotto, il numero di registrazione del prodotto (Product Key) o visualizzare la licenza del software.
Un codice di licenza è una serie di numeri e lettere utilizzata per installare e registrare le versioni del software. Questi codici si possono trovare nella scatola del prodotto, sul supporto con cui è stato distribuito il software, nel certificato di autenticità generalmente riportato sul computer.

Le licenze software quindi sono documenti legali allegati ai programmi. Senza un tale documento, un programma non può essere distribuito né modificato senza l'esplicito consenso degli autori.

Differenza tra Hacking, Kracking e Hacking etico

L'attività di **Hacking** (dall'inglese to hack, intaccare) è svolta da programmatori (hacker) che si collegano e accedono a risorse di rete senza averne l'autorizzazione, solo per gusto di sfidare il computer e i sistemi di protezione. Solitamente un hacker non vuole causare un danno ma usare le risorse del sistema attaccato oppure semplicemente dimostrare di essere riuscito ad accedervi.
Quando la violazione di un sistema da parte di un hacker comporta un vantaggio personale o un uso delle risorse per proprio lucro, si parla di **Kracking**: ad esempio, rubare o alterare dei dati, danneggiare il sistema, ecc. Per kracker si intende anche un programmatore che si dedica alla pirateria informatica, rimuovendo le protezioni dai programmi e distribuendone copie illegalmente a scopo di lucro. Alcuni esempi di attività di kracking sono il **Cracking di password**, cioè il recupero di password, in modo manuale o con appositi programmi, da dati memorizzati o inviati ad un sistema informatico e il **Cracking di software**, cioè la disattivazione o l'eliminazione di alcune funzioni del software come la protezione contro la copia, i numeri di serie, le chiavi hardware, i controlli di data, ecc.

A volte le competenze e le abilità di un hacker possono essere utilizzate “a fin di bene” per testare il grado di sicurezza di un sistema informatico. In questo caso si parla di **hacking etico**: l'utilizzo delle tecniche di hacking per monitorare la sicurezza dei sistemi e delle reti informatiche al fine di evitare l'abuso da parte di malintenzionati. In pratica è permesso l’attacco al sistema di sicurezza di un computer da parte dei proprietari per rilevarne le vulnerabilità.
Un famoso hacker che è diventato un hacker etico è Kevin David Mitnick, nome in codice “Condor”. Negli anni ’90 si è introdotto illegalmente nei sistemi informatici di varie società americane, sia sfruttando i *bug* (letteralmente “bachi”: errori nella scrittura di un software) dei loro sistemi informatici sia utilizzando la tecnica dell’*ingegneria sociale*, cioè acquisendo informazioni riservate direttamente dalle persone coinvolte nei sistemi informatici dell’azienda guadagnando la loro fiducia con l’inganno.
Ha eseguito tra le più ardite intrusioni nei computer del governo degli Stati Uniti. Dopo essere stato catturato e aver scontato diversi anni di carcere ha iniziato ad occuparsi di sicurezza informatica e attualmente è amministratore delegato di una azienda di consulenza e sicurezza.

Riconoscere le minacce ai dati provocate da forza maggiore.

Per **Forza maggiore** si intende una forza superiore o un evento imprevisto che può minacciare la conservazione dei dati. Queste forze o eventi possono essere naturali o generate dall’uomo. Ad esempio incendi, inondazioni, terremoti, guerre, furti, atti vandalici, ecc. In vista di questi frangenti è opportuno adottare delle misure di sicurezza per ridurre al minimo il danno che ne può derivare.
Una buona norma da seguire è assicurarsi che per tutti i dati importanti esista una copia di *riserva*, una copia di *backup*. È consigliabile conservare anche una copia dei software che sono installati nel computer.
Come vedremo nei capitoli successivi fare il backup significa copiare i dati su di un supporto esterno come un hard disk rimovibile, un CD/DVD riscrivibile, una chiave USB, ecc. Esistono dei programmi che creano automaticamente, mentre si lavora, copie di riserva dei dati.
È fondamentale che la copia di backup non sia conservata nelle vicinanze del computer che contiene i dati originari, per evitare che una delle calamità descritte in precedenza porti alla perdita di entrambe le copie.
Esistono servizi in Internet che offrono la possibilità di effettuare dei backup su dispositivi messi in rete: si chiamano **memorie online**, o dischi virtuali. Uno memoria online è come in un magazzino, un hard disk virtuale, uno spazio di memoria in un sito internet che si apre solo se si possiede la password di accesso. È un sistema avanzato di backup per avere una copia dei propri dati immediatamente accessibile anche in caso di emergenza. Basta collegarsi alla rete, dovunque ci si trovi senza avere il proprio computer. Un esempio di questo servizio è Dropbox.
Inoltre può essere utile come spazio per scambio di file tra utenti (chiaramente tutti in possesso della password).

Minacce ai dati provocate da impiegati, fornitori di servizi e persone esterne

I dati privati e personali di un utente, di una azienda, di una scuola, di un ospedale, ecc. sono un bene da proteggere, sia per evitare il furto di know how aziendale sia perché c'è una legislazione sulla privacy dei dati riservati molto rigorosa.

Abbiamo visto a quali rischi possono essere soggette queste informazioni. Ma la sicurezza dei dati di una organizzazione può essere minacciata anche dagli utilizzatori di questi dati o da persone esterne che accedono casualmente ad essi.

Ad esempio, gli stessi **impiegati**, con le loro azioni, possono compromettere le informazioni importanti dell'azienda dove lavorano: in modo accidentale, cancellando o modificando questi dati o per scopi fraudolenti, ad esempio rubando e vendendo alla concorrenza le specifiche dei prodotti.

Anche i **fornitori di servizi**, ad esempio gli addetti alla manutenzione dell'hardware e del software, potrebbero accedere casualmente a informazioni e dati e provocare, in modo volontario o meno, dei danni.

In ultima analisi, se delle **persone esterne** possono accedere al sistema informatico senza alcun controllo, ad esempio nel caso di una rete Wi-Fi senza chiavi di protezione, i dati sono a rischio di furto o danneggiamento.

Per evitare le problematiche esposte è importante che l'incaricato alla conservazione dei dati riservati o elenchi di aziende, di persone o banche dati deve salvaguardarli dall'intrusione di altri soggetti e non divulgarli se non con esplicita autorizzazione. Un modo è impostare una corretta gestione degli accessi attraverso autorizzazioni e password.

Valore delle informazioni

Importanza delle informazioni

Motivi per proteggere le informazioni personali

I motivi per cui è importante proteggere i dati riguardanti le proprie informazioni personali spesso sono abbastanza evidenti. Si pensi alle conseguenze di un accesso al proprio conto corrente bancario da parte di una persona che non sia il proprietario.
Un fenomeno frequente, nel campo della violazione dei dati personali, è il **furto d'identità**. Il furto d'identità consiste nell'ottenere indebitamente le informazioni personali di un soggetto al fine di sostituirsi in tutto o in parte al soggetto stesso e compiere azioni illecite in suo nome o ottenere credito tramite false credenziali.
Le informazioni personali carpite possono essere: nome, cognome, indirizzo, codice fiscale, numero di telefono/cellulare, luogo e data di nascita, numero della carta di credito, estremi del conto corrente, nome dei figli, ecc.
L'attività di carpire informazioni ingannando un utente ed indurlo a rivelare dati sensibili e personali come le credenziali di accesso al proprio conto online è detta **ingegneria sociale**. L'ingegneria sociale si riferisce alla manipolazione delle persone, che vengono portate ad eseguire delle azioni o a divulgare informazioni riservate, invece di utilizzare tecniche di hacking per ottenere le stesse informazioni.
Attraverso operazioni di ingegneria sociale è possibile:

- Raccogliere informazioni riservate o di valore.
- **Realizzare frodi**, utilizzando le informazioni raccolte per commettere atti fraudolenti.
- **Accedere a sistemi informatici** in modo non autorizzato e, di conseguenza, consentendo potenzialmente l'accesso ad altre informazioni riservate.

Il fenomeno dell'ingegneria sociale è cresciuto proporzionalmente al diffondersi della rete internet. Infatti, nell'enorme mare di dati presente in internet è semplice reperire informazioni su una persona o un'azienda.
A tutti coloro che usano internet viene chiesto regolarmente di fornire dati personali per poter accedere a determinati siti o per poter acquistare beni. Spesso queste informazioni viaggiano sulla rete in chiaro e non in modalità protetta.
Un crescente numero di utenti, inoltre, sta fornendo un'elevata quantità di dati personali a social networks come MySpace, Facebook, chat, blog, ecc.
Ci sono poi delle tecniche specifiche di ingegneria sociale tramite internet, quali:

- **Phishing** - Questo termine identifica il furto di dati via mail. Il malvivente invia un'e-mail dichiarando di essere un incaricato di una banca o di una compagnia di carte di credito o di altre organizzazioni con cui si possono avere rapporti, richiedendo informazioni personali. Generalmente l'e-mail chiede di utilizzare un link per accedere ai dettagli del conto della vittima presso il sito della compagnia, adducendo

motivazioni di sicurezza, riscuotere premi in denaro, beni tecnologici, ripristinare password scadute, etc. Cliccando su quel link, tuttavia, l'utente sarà condotto in un sito web solo all'apparenza originale, in cui dovrà fornire informazioni private. I criminali potranno poi utilizzare i dati lasciati in tale sito fittizio per rubare denaro alle loro vittime.

- Questionari on line.
- Ingannare qualcuno a proposito della propria identità durante una chat, in un forum, ecc.
- **Finte promozioni o vincite**: mediante la ricezione di messaggi (SMS, Email) che, con la scusa di promozioni o vincite ad esempio di un telefonino di ultima generazione, portano a un link che porta ad una azione di phishing finalizzata ad acquisire i dati personali.

Ci sono comunque altri metodi, che non comportano l'utilizzo di internet, attraverso cui i criminali recuperano le informazioni necessarie per rubare l'identità:

- **Bin-raiding**. Documenti cartacei che non si ritiene importanti, come bollette del gas, della luce o del telefono, estratti conto e persino lettere personali e le buste in cui sono contenute, forniscono informazioni preziose che possono essere raccolte semplicemente rovistano nei rifiuti.
- **Contatti indesiderati.** Si deve fare molta attenzione a chi ci contatta, anche telefonicamente: spesso i truffatori si dichiarano incaricati di una banca o di un ente pubblico e vi chiedono di aggiornare i vostri dati personali. Accade la stessa cosa con coloro che si presentano come ricercatori di mercato e richiedono informazioni personali.
- **Furto o smarrimento del portafoglio**. Generalmente i portafogli contengono bancomat, carte di redito e documenti di identità come la patente di guida e le tessere di iscrizione a determinate associazioni.
- **Skimming**. Lo Skimming consiste generalmente nella clonazione di una carta di credito attraverso l'apparecchiatura elettronica utilizzata negli esercizi commerciali per pagare i beni acquistati. I dati che vengono raccolti, sono poi trasmessi a organizzazioni criminali.
- **Rubare l'identità di un deceduto**. I malviventi più spietati svolgono le loro attività criminali utilizzando l'identità di persone decedute, ottenendo informazioni sulla loro età, data di nascita ed indirizzo attraverso necrologi e pubblicazioni funebri.
- **Questionari cartacei**. Spesso vengono inviati per posta. Se sono molto lunghi, il compilatore non si accorge che sta fornendo a estranei delle informazioni private.
- **Tramite… noi stessi**. Capita, inconsciamente, di raccontare in pubblico fatti che ci riguardano (nell'anticamera del dottore, al supermercato durante la fila alla cassa, ecc.), non sapendo che per un ascoltatore interessato possono essere una miniera di dati.
- **Shoulder surfing** (letteralmente "fare surf alle spalle"). Designa quella semplice tecnica a metà tra l'informatica e il social engineering finalizzata all'impadronirsi di codici di accesso. Mentre la vittima digita la propria password (oppure il PIN o altri codici), il malintenzionato lo osserva, sia da vicino oppure anche da lontano (mediante lenti particolari o anche le riprese di telecamere a circuito chiuso), e riesce così ad

impossessarsi delle sequenze. Spesso ciò avviene tramite l'utilizzo di terminali POS oppure in luoghi molto frequentati, come ad esempio gli internet cafè.

Sono evidenti i motivi per cui è opportuno proteggere le proprie informazioni personali: se qualcuno entra in possesso di dati riservati, come le credenziali di accesso alla posta elettronica o a una rete sociale, ne può fare un uso illegale facendo ricadere la colpa su di noi (**furto di indentità**).