Sommario

Cap1: Introduzione

Aspetti della sicurezza

La sicurezza di un sistema informatico è l'insieme di accorgimenti che vengono utilizzati per ridurre, o addirittura evitare, tutti i possibili attacchi da parte di un'agente qualunque.

Sicuro è un sistemainformatico in cui le informazioni contenute vengono garantite attraverso misure e sistemi di sicurezza predisposti.

Un sistema informatico per ritenersi sicuro deve predisporre dei seguenti caratteri:

- Affidabilità: deve cioè garantire che il servizio venga erogato tutte le volte che l'utente lo richiede, deve assicurare che i dati per i quali è stato programmato siano sempre presenti.

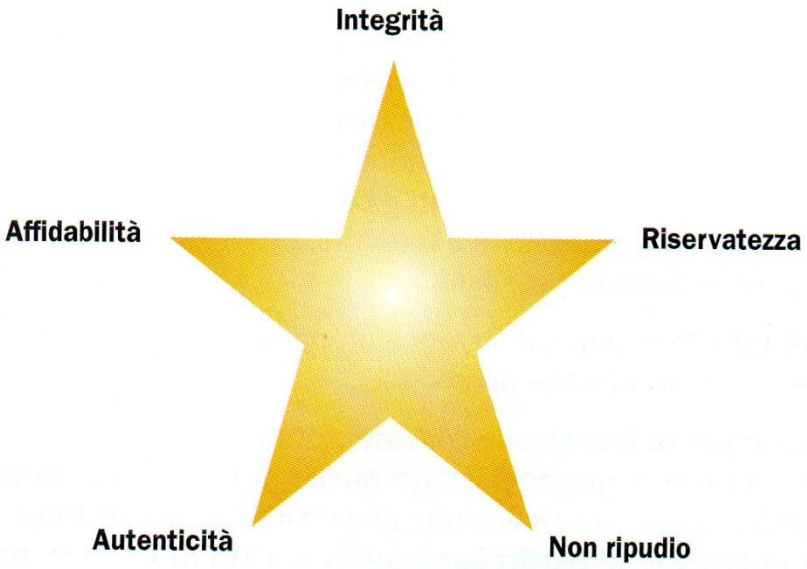
- Integrità: garanzia che le informazioni non subiscano modifiche o cancellazioni a seguito di errori o di azioni volontarie, ma anche a seguito di malfunzionamenti o danni dei sistemi tecnologici.

- Riservatezza: gestione della sicurezza in modo tale da evitare i rischi connessi all'accesso o all'uso delle informazioni in forma non autorizzata. In poche parole: necessità che il dato inviato al destinatario sia visibile solo a quest'ultimo.

- Autenticità: Chi riceve un messaggio deve poterne identificare con certezza la provenienza, ossia **verificare l'identità dell'origine**(il mittente di quel messaggio deve essere effettivamente lui).

- Non ripudiabilità: Chi genera un messaggio non deve poter negare successivamente di averlo generato, né deve poterne negare il contenuto. Allo stesso modo, chi riceve un messaggio non deve poter negare di averlo ricevuto, né deve poterne negare il contenuto. Un esempio di messaggio non ripudiabile sono la PEC e la firmadigitale.

È bene sottolineare che questi 5 caratteri non sono talvolta tutti presenti contemporaneamente nel solito sito. Non è obbligatoria la presenza di tutti e 5 poiché ognuno di loro viene utilizzato a seconda dell'uso che si vuole fare.



Sicuro è un sistema informatico in cui le informazioni contenute vengono garantite attraverso sistemi e misure di sicurezza appositamente predisposti. Contro la violazione degli aspetti relativi alla sicurezza

Il concetto giuridico di sicurezza informatica è collegato a quel complesso di accorgimenti tecnici e organizzativi che puntano a tutelare i beni giuridici della confidenzialità, dell'integrità e della disponibilità delle informazioni registrate.

La normativa in materia di sicurezza di sistemi informatici prevede vari tipi di sanzioni anche penali. Tali norme prevedono una casistica di disastri informatici che costituisce una sorta di elenco, non esaustivo degli attacchi.

Un attacco (accidentale o intensionale) è un'agente.

Classificazione degli agenti

La sicurezza di un sistema informatico, infine, può essere compromessa da alcuni fattori, gli agenti. Quest'ultimi possono essere ***attivi***, alterano la sicurezza e si distinguono in umani e non umani, e ***passivi***, violano la riservatezza e anche questi possono essere umani e non umani.

Si definisce agente **attivo** quell'agente che può violare gli aspetti relativi alla sicurezza, negli attacchi attivi, l'hacker accede a una rete e ai sistemi target connessi ad essa utilizzando delle credenziali rubate. Sono attacchi informatici attivi il masquerade attack,la message modification e il Denial of Service o DoS.

Si definisce invece agente **passivo** quell'agente che può violare solo gli aspetti inerenti alla riservatezza, gli attacchi passivi sono quelli in cui l'hacker si limita a intercettare i traffici di dati che avvengono su una rete e sono spesso propedeutici ad attacchi attivi.

Gli attacchi attivi sono quelli che implicano la manomissione di dati, mentre gli attacchi passivi consistono in attività di intelligence.

Infine, gli agenti sia attivi che passivi possono essere umani o non umani.

La sicurezza di un sistema informatico coincide con l'insieme di accorgimenti che devono essere utilizzati per ridurre tutti i possibili attacchi da parte di un'agente qualsiasi.

Cap2: Attacchi informatici

Malware

Per **malware** (dall'inglese "***malicious software***") si intende qualsiasi tipo di software dannoso o fonte di disturbo, creato per accedere segretamente a un dispositivo senza che l'utente ne sia a conoscenza. Lo scopo dei malware è lucrare illecitamente a spese degli utenti. I malware non possono danneggiare gli hardware fisici di un sistema, ma possono rubare, criptare o eliminare i dati e spiare le attività degli utenti senza che questi se ne accorgano o forniscano alcuna autorizzazione.

Virus

Col termine virus, in ambito informatico, ci si riferisce ad un software(un programma, una macro o uno script) facente parte della categoria dei malware. Un virus viene progettato e realizzato in modo tale da essere inserito al'interno di un dispositivo, senza che l'utente lo sappia o dia la propria autorizzazione. La vita di un virus si svolge tramite una fase di trasmissione dove il file infetta uno o più file del dispositivo, successivamente nella fase di riproduzione si moltiplica contagiando il singolo dispositivo o gli altri nella rete mentre nella sua fase finale di vita ovvero l'alterazione il virus svolge il compito per cui è stato programmato che spesso significa ostruzione o distruzione dei file contagiati.

Vi sono diverse tipologie di virus in base allo scopo da raggiungere e alle componenti da infettare:

- **Virus di file:** sostituiscono interamente o parzialmente ad un programma.
- **Virus di boot:** infettano il settore boot o master boot, ovvero danneggiando l'avvio del sisema.
- **Virus poliformici:** si riproducono in cloni con diverse forme rimanendo difficilmente riconoscibili.
- **Virus stealth:** irriconoscibili dagli antivirus.
- **Virus tsr:** colpisce la RAM del dispositivo.

Worms

Un worm nella sicurezza informatica, è una particolare categoria di malware la cui caratteristica principale è quella di autoreplicarsi. Tipicamente un worm modifica il computer che infetta, in modo da venire eseguito ogni volta che si avvia la macchina e rimanere attivo finché non si spegne il computer o non si arresta il processo corrispondente. Il worm tenta di replicarsi sfruttando la rete Internet. Il mezzo più comune impiegato dai worm per diffondersi è la posta elettronica il Programma maligno una volta che ha infettato accede alle e-mail e invia diverse copie di se stesso senza che serva l'intervento dell'utente .Possiamo dividere gli effetti provocati da un worm in due tipi

- *danni diretti*, causati dall'esecuzione del worm sulla macchina vittima
- *danni indiretti*, derivanti dalle tecniche utilizzate per la diffusione.

La maggior parte dei worm, contiene una parte detta ***payload***, che ha lo scopo di causare dei danni al sistema infettato. Molto di frequente un worm funge da veicolo (**DROPPING**) per l'installazione automatica sul maggior numero di macchine di altri malware,.

Spyware

Lo spyware è uno dei malware in circolazione, il suo obiettivo è quello di accumulare informazioni sensibili degli utenti: Viene definito molto pericoloso perché costituisce una minaccia per la privacy, in quant riesce a ricavare informazioni sul comportamento dell'utente in Internet e i suoi dati come password. Solitamente questi dati raccolti, ricavati ad esempio dalle abitudini online degli utenti, vengono inviati agli hacker che li

utilizzano per realizzare annunci pubblicitari adatti all'utente specifico. Lo spyware riesce anche ad individuare delle falle nei browser. Ed inoltre, è molto difficile da scovare e da bloccare.

Keylogger

Un tipo di malware è il keylogger, formato da “key” (tasto) e dal verbo “to log” (registrare su un diario), si fa riferimento a un “registratore di tasti”.Il keylogger è uno strumento informatico tecnologico che permette di intercettare tutto ciò che viene digitato sulla tastiera di un computer.I keylogger nascono inizialmente come metodi e dispositivi per scopi leciti (come il recuperare password, nomi di user ID, testi non salvati, ecc.) ma con la grande diffusione e importanza dei computer, sono diventati sistemi usati spesso per danneggiare irrimediabilmente la nostra privacy e in modo illegittimo.

Può essere di due tipi:

- Il **keylogger** di tipo **hardware**, solitamente, è un micro dispositivo elettronico a cavetto, dall’aspetto simile a una prolunga, da collegarsi tra il cavo della tastiera e il pc, che riesce catturare e memorizzare in un file di testo tutte le password e qualsiasi altro dato, come ad esempio gli indirizzi web, digitati sulla tastiera.

a

- Il **keylogger** di tipo **software**, invece è un programma spia installato sul computer tra il browser e il web in grado di captare tutte le informazioni all’insaputa dell’utente riguardo le sue attività svolte, e memorizzarle in un file, come ad esempio le schermate video, i messaggi di posta elettronica, i numeri della carta di credito e così via. Queste informazioni registrate vengono poi inviate a un computer remoto spia, pronte per essere, in un secondo tempo, decodificate e usate.

Trojan

Oggi col termine "**trojan**" ci si riferisce ai **malware** ad accesso, composti generalmente da 2 file: il file server, che viene installato nella macchina “vittima”, ed un file client, usato dall'attaccante per inviare istruzioni che il server esegue. Proprio perché i trojan non si diffondono autonomamente come i virus o i worm e non sono in grado di replicare se stessi, essi richiedono un'azione diretta dell'aggressore per far giungere il software maligno al programma.
Il **trojan**, chiamato anche “cavallo di Troia”, nasconde il suo funzionamento all'interno di un altro programma apparentemente utile e innocuo. L'utente, eseguendo o installando quest'ultimo programma, in effetti attiva anche il codice del trojan nascosto.

L'attribuzione del termine "cavallo di Troia" è dato dal fatto che esso nasconde il suo vero fine. È proprio il celare le sue reali "intenzioni" che lo rende tale e in questo modo l'utente, inconsapevolmente, è indotto ad installare il programma.

Inoltre, il virus trojan può essere impiegato da **cyberladri** e hacker che cercano di accedere ai sistemi degli utenti. Una volta attivato, il trojan può consentire ai **cybercriminali** di spiare l'utente, rubarne i dati sensibili e ottenere l'accesso al sistema. Ad esempio: eliminazione, blocco, modifica, copia dei dati o compromissione delle prestazioni di computer o reti. Altre volte gli stessi trojan possono essere usati per diffondere virus all'interno di una rete difficile da attaccare per gli hacker.

I trojan, oggi, sono sempre più diffusi e non tutti sono riconoscibili prontamente dagli antivirus. Per aumentare la loro efficacia possono nascondersi in modo tale che nemmeno l'antivirus sia in grado di eliminarli. Permettendo così di danneggiare il computer. Se questo accade, il trojan può essere individuato e rimosso solo tramite la *reinstallazione* totale del sistema operativo ad opera di un informatico esperto.

Ramsonware

Il Ransomware è un tipo di malware che imposta il blocco all'accesso di un sistema informatico da parte di un criminale informatico, che richiede un riscatto per poter rimuovere il blocco.Il malware può anche criptare i file e renderli in questo modo inaccessibili.
E' dunque necessario un compenso monetario per poter nuovamente accedere ai dati.

Sono attacchi molto pericolosi creati da criminali informatici con ampie conoscenze riguardo la programmazione informatica e spinti ad effettuare questi attacchi per motivi economici appunto. Riescono ad entrare all'interno del client con facilità, mediante magari l'apertura di un sito che è infetto da questo malware oppure con una mail infetta o più semplicemente tramite la rete.

Accorgersi di avere un computer infetto da Ransomware è semplice, poiché non si riesce ad accedervi. Per poter prevenire questi probabili attacchi, si possono installare nel computer degli antivirus e soprattutto effettuare sempre il back-up dei dati, o locale o remoto, al fine di poterli riottenere in qualche modo. Altrimenti se sono di estrema importanza, può dover essere necessario pagare il riscatto, se precedentemente non sono state prese queste misure di prevenzione.

Cryptolocker

Un Cryptolocker è un **ransomware** e può essere installato in un computer impedendo il suo stesso utilizzo.

Questo, infetta i sistemi di Windows , e consiste nel criptare i dati della vittima con lo scopo di riuscire ad estorcere alla vittima stessa un importo di denaro, in genere è solito chiedere il pagamento di una somma di denaro per la decriptazione dei dati.

Un Cryptolocker in genere si diffonde come un allegato di posta elettronica che a primo impatto può sembrare inoffensivo perché magari utilizza il nome di un Istituzione inesistente, ma in realtà è molto più pericoloso di quel che sembra perché dal momento in cui il criminale entra nel computer, si impossessa dei server di comando e di controllo.

Una volta che è si è connesso al server, genera una chiave RSA a 2048 bit e manda una chiave pubblica al computer infetto.

Il computer sembra continui a funzionare ma immagini, documenti e file di ogni genere sono criptati dalla chiave emessa dal criminale informatico che è sostanzialmente

inviolabile.

Adware

Gli **adware** sono una delle infezioni informatiche più comuni. Si tratta infatti di programmi malevoli che generalmente hanno due obbiettivi: spiare il comportamento online degli utenti e mostrare loro determinati annunci pubblicitari: una volta entrati nel sistema tempestano gli utenti con continui banner pubblicitari oppure reindirizzando il traffico web verso siti internet che contengono sempre annunci commerciali.

Essi sono in grado di colpire qualsiasi dispositivo: dai cellulari ai computer.

Il loro principale obbiettivo (conoscendo le nostre caratteristiche e i nostri interessi) è generare più click possibili ai contenuti sponsorizzati.

C'è un modo per proteggersi da questi attacchi?

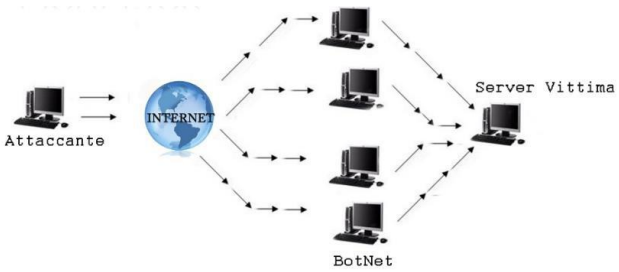
Purtroppo spesso i programmi adware non dispongono di una procedura di disinstallazione e utilizzano tecnologie simili a quelle dei virus (quindi molto avanzate) per operare senza farsi notare.

L'unica cosa che possiamo fare è dunque prevenire l'attacco: questo significa di evitare di scaricare programmi da siti internet non ufficiali e potenzialmente rischiosi. Bisogna fare attenzione anche alle estensioni installate nei browser e soprattutto non bisogna aprire link e allegati email sospetti. Molto importante è tenere sempre aggiornato il computer e gli antivirus.

Ecco come può apparire la presenza di un adware:

Denied of Service

Attacco D. O. S (attacco Denial of Service) è usato per ostacolare l'accesso di utenti ad un sito web, solitamente vengono attaccati i siti web più conosciuti.



Ci sono differenti tipologie di attacchi D. O. S: alcune mirano a impedire l'accesso di un determinato individuo (legittimo) a un sito web, altre cercano di cercano di rallentare o bloccare l'attività di quel determinato server.

Il più comune di questi attacchi consiste in un **allagamento della rete** o della connessione a cui il computer che si vuole attaccare appartiene. I questo caso si attacca una parte del server al quale hanno accesso un numero limitato di utenti, il malintenzionato (utente che attacca) riesce a mandare un numero elevato di richieste informazioni a quel determinato server e facendo così riesce a bloccare l'attività del sito perché appunto ne esaurisce le riserve.

Un altro tipo di attacco colpisce le **caselle di posta elettronica** e consiste nell'invito indesiderato di file di grosse dimensioni o di e-mail con allegati di grosse dimensioni verso un account che si vuole appunto attaccare. La conseguenza di questo fatto è che si esaurisce lo spazio che ogni utente ha a disposizione impedendo così che altre mail possano arrivare a quel determinato indirizzo di posta elettronica.

Backdoor

Una backdoor (dal termine inglese per *porta di servizio* o *porta sul retro*) è un metodo, spesso segreto, per passare oltre (aggirare, bypassare) la normale autenticazione in un prodotto, un sistema informatico, un crittosistema o un algoritmo.

Le backdoor hanno la funzione principale di superare le difese imposte da un sistema, come può essere un firewall, al fine di accedere in remoto a un personal computer, ottenendo per mezzo di un sistema di crittografia un'autenticazione che permetta di prendere il completo o parziale possesso del computer vittima.

Una backdoor può celarsi segretamente all'interno di un ignaro programma di sistema, di un software separato, o può anche essere un componente hardware malevolo come: apparati di rete, sistemi di sorveglianza e alcuni dispositivi di infrastruttura di comunicazione che possono avere celate al loro interno backdoor maligne permettendo l'intrusione di un eventuale criminale informatico.

Una backdoor può essere installata dall'amministratore di sistema per entrare rapidamente in un dispositivo per effettuare operazioni di manutenzione in remoto, oppure, nella peggiore delle ipotesi, da un malware (un qualsiasi programma informatico usato per disturbare le operazioni svolte da un utente di un computer) controllato da un hacker per prendere completamente il controllo di un sistema all'insaputa dell'utente.

È per questo motivo che cerca di nascondersi nel mare magum (grande mare) dei file di sistema assumendo nomi e dimensioni che non diano nell'occhio al punto da insospettire un utente. Chi cancellerebbe mai un file di sistema? Ma, basta un comando in remoto da parte di qualche

cybercriminale per trasformare questo file all'apparenza innocuo in una via di accesso privilegiata al sistema.

Le backdoor permettono il controllo da tutti i processi attivi a quello sulla **webcam**, **mouse** e **tastiera**. Sempre che l'hacker non decida di reclutarlo come "bot" per usarlo, all'insaputa dell'utente , in un attacco DDoS o di altro genere.

È evidente che non c'è nulla di malevolo nell'idea di nascondere una funzionalità di gestione di emergenza a vantaggio del proprietario o del gestore del sistema. Chiaramente, però, la cosa diventa problematica nel momento in cui la backdoor viene scoperta da qualcuno che non è colui a cui la "porta di servizio" sarebbe destinata.

Come difendersi dalle backdoor:

- **Cambiare le password di default**. La maggior parte delle violazioni dei sistemi condotte tramite backdoor, è avvenuto perché venivano usate password deboli o di default. Esistono centinaia di database online che riportano tutte le credenziali di default dei principali apparati. Moltissimi router domestici usano ancora, come password di default della rete wireless, una chiave prodotta a partire dall'ID del dispositivo (MAC Address, BSSID o altro seriale disponibile nell'etere) con algoritmi noti. Esistono addirittura delle app che consentono, semplicemente "sniffando" le reti, di comprendere il tipo e modello di Access Point e restituiscono la password di default di quella particolare rete.
- **Applicare pedissequamente il principio di minimum access**, segregando il più possibile i network ed i flussi dati in maniera tale da avere il traffico di management esclusivamente su una rete dedicata e strettamente sorvegliata. Se vedo traffico IPMI su una rete destinata al traffico standard, di certo c'è un problema. Viceversa, se trovo traffico sulla rete di management destinata a servizi differenti da quelli di gestione, la probabilità diventa una quasi certezza.
- **Non possiamo fidarci pienamente di nessun device** o software che non abbiamo programmato o realizzato noi. Ed anche in questo caso, dobbiamo diffidare dei componenti, per cui diventa fondamentale sfruttare il periodo di test per auditare il sistema e cercare di verificarne il funzionamento nei dettagli.
- **I sistemi IDS/IPS tradizionali difficilmente riescono ad individuare delle backdoor**, mentre i sistemi avanzati di network behavior analysis possono al contrario esserci di estremo aiuto, evidenziando le connessioni inusuali da o verso indirizzi che non dovrebbero parlarsi.

Sniffing

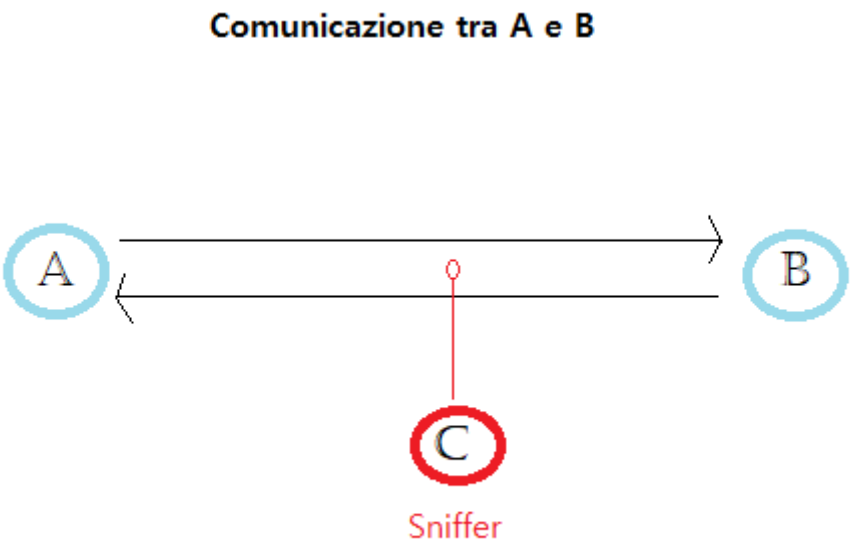
Lo Sniffing è una metodologia di attacco che, tramite l'intercettazione dei dati in transito, raccoglie informazioni chiave utili al fine di compromettere la comunicazione tra client e server.

Tale attività può essere svolta sia per scopi legittimi (ad esempio l'analisi e l'individuazione di problemi di comunicazione) sia per scopi illeciti contro la sicurezza informatica (per esempio l'intercettazione fraudolenta di password).

L'attività dello sniffer, colui che esegue lo Sniffing, consiste nell'intercettare le comunicazioni trasmesse su Internet e inviate da un punto A per raggiungere un punto B (o viceversa).

Dunque, in semplici parole, lo sniffing è un tipo di attacco utilizzato per violare la riservatezza dei dati.

Ci sono diversi metodi per difendersi da un attacco di questo genere, uno di questi consiste nell'inviare i dati sensibili in modo criptato, così che, anche se venissero catturati da uno Sniffer, sarebbero comunque illeggibili.



Spoofing

Phishing

Il **pishing** è una particolare tipologia di truffa che avviene principalmente attraverso i messaggi di posta elettronica. Gli utenti ricevono delle e-mail da apparenti siti che possono essere di banche o società di carte di credito, ricevendo messaggi sui problemi di registrazione o di altra natura. L' utente talvolta è ignaro del fatto che si tratti di una truffa, poiché i truffatori per rendere più credibile il loro tentativo di estorsione inseriscono dei link che rimandano ad un sito identico a quello originale, che è stato accuratamente rielaborato dai malviventi. Nel momento in cui il malcapitato in questione inserisca le proprie credenziali, credendo appunto che si tratti di un sito reale, esse vanno in mano ai criminali. Un pericolo più ingannevole è quello dei virus informatici, anch'essi ricevuti dall'utente tramite allegati di posta elettronica. Essi si attivano nel momento in cui l'utente acceda al link fasullo oppure inserendo le proprie credenziali. Anch'essi sono utilizzati per carpire dati

Hacking Etico

Gli **hacker etici** sono persone che, seguendo una serie di principi etici personali, mettono le loto capacità a servizio di imprese o altri soggetti. La loro attività consiste nel simulare attacchi maligni con lo scopo di trovare, prima di coloro che hanno l'intenzione di attaccare veramente un server, punti vulnerabili, deboli dei sistemi, in modo da poter risolvere gli eventuali problemi e rendere il sistema sicuro.

Il loro scopo è quello di opporsi alle attività criminali degli hacker non etici conducendo azioni guidate da principi etici personali o perché richiesto da contratti di lavoro, pratica sempre più frequente, essi sono quindi una categoria sempre più richiesta da aziende e governi che sono consapevoli della necessità di proteggere in modo efficace i propri sistemi.

Cap3: Meccanismi di protezione

Backup

Il backup è un meccanismo che non protegge dagli attacchi informatici, ma consente che il lavoro non vada perso perché genera copie dei file o dei database (fisici o virtuali) che viene ospitata in un sito secondario. È evidente che, per garantire la strategia, il secondo sito dovrebbe essere geograficamente lontano dal sito primario dove risiedono i dati originali in modo da avere garanzia del fatto che il secondo sito, per qualunque evenienza, non sarà compromesso.

È un'attività fondamentale nei seguenti casi:

- Anomalie e guasti dell'apparecchiatura
- Eventi catastrofici come incendi, allagamenti, terremoti,
- Azioni malevoli come furti, virus e via dicendo
- Errori da parte degli utenti distratti o inesperti

Grazie alla copia di file, applicazioni e sistemi, è possibile recuperare i dati perduti e di tornare alla condizione operativa precedente all'evento negativo; ovviamente, la funzionalità operativa dipende dalla frequenza con cui si effettua. Per lavori intensivi, infatti, la frequenza deve maggiore rispetto ad attività diluite in archi temporali più lunghi.

Può essere:

- **Locale**: ogni computer dev'essere dotato di un hardware che consenta la copia su due hard disk contemporaneamente
- **Remoto**: prevede la copia dei dati su un dispositivo grazie alla connessione di rete (ad esempio google drive o icloud)

Antivirus

L' antivirus è un **software** che consente di proteggere il proprio pc da virus o elementi che potrebbero danneggiarlo. Esso consente di prevenire, individuare e rendere inoffensivi tali codici dannosi. Un buon antivirus deve essere costantemente aggiornato e l'utente deve, in modo regolare, scansionare i propri dispositivi per individuare eventuali virus. L'antivirus è quindi un programma con il compito di scansionare i file alla ricerca di codici malevoli, ha poi il compito di bloccare l'espansione dei virus rilevati e di cercare di ripristinare i file infetti.

Cloud computing

In parole semplici, il **cloud computing** è la distribuzione di servizi di calcolo, come server, risorse di archiviazione, database, rete, software, analisi e intelligence, tramite Internet ("il cloud"), per offrire innovazione rapida, risorse flessibili ed economie di scala. Paghi solo per i servizi cloud che usi e risparmi sui costi operativi, esegui l'infrastruttura in modo più efficiente e ridimensioni le risorse in base all'evoluzione delle esigenze aziendali.

Principali vantaggi del cloud computing

Il cloud computing rappresenta un grande cambiamento rispetto alla visione tradizionale delle aziende in materia di risorse IT. Ecco sette motivi comuni per cui le organizzazioni ricorrono ai servizi di cloud computing:

Costo

Il cloud computing elimina le spese di capitale associate all'acquisto di hardware e software e alla configurazione e alla gestione di data center locali, che richiedono rack di server, elettricità 24 ore su 24 per alimentazione e raffreddamento ed esperti IT per la gestione dell'infrastruttura. I conti tornano in fretta.

Velocità

La maggior parte dei servizi di cloud computing viene fornita in modalità self-service e su richiesta, quindi è possibile effettuare il provisioning anche di grandi quantità di risorse di calcolo in pochi minuti, in genere con pochi clic del mouse. Le aziende possono quindi usufruire di una grande flessibilità senza la pressione legata alla pianificazione della capacità.

Scalabilità globale

I vantaggi dei servizi di cloud computing includono la possibilità di ridimensionare le risorse in modo elastico. In materia di cloud questo significa fornire la giusta quantità di risorse IT, ad esempio una quantità maggiore o minore di potenza di calcolo, risorse di archiviazione e larghezza di banda, proprio quando è necessario e dalla località geografica appropriata.

Produttività

I data center locali richiedono in genere un impegno notevole nell'organizzazione e nell'assemblaggio dei rack, che include la configurazione dell'hardware, l'applicazione di patch software e altre attività di gestione IT dispendiose in termini di tempo. Il cloud computing elimina la necessità di molte di queste attività, consentendo ai team IT di dedicare il proprio tempo al raggiungimento di obiettivi aziendali più importanti.

Prestazioni

I più grandi servizi di cloud computing vengono eseguiti su una rete mondiale di data center sicuri, aggiornati regolarmente all'ultima generazione di hardware, veloce ed efficiente. Questo offre diversi vantaggi rispetto a un singolo data center aziendale, tra cui latenza di rete ridotta per le applicazioni e maggiori economie di scala.

Affidabilità

Il cloud computing aumenta la semplicità e riduce i costi di backup dei dati, ripristino di emergenza e continuità aziendale, grazie alla possibilità di eseguire il mirroring dei dati in più siti ridondanti nella rete del provider di servizi cloud.

Sicurezza

Molti provider di servizi cloud offrono un'ampia gamma di criteri, tecnologie e controlli che rafforzano il comportamento di sicurezza complessivo, grazie alla protezione di dati, app e infrastruttura dalle minacce potenziali.

Tipi di cloud computing

Non tutti i cloud sono uguali e non sempre lo stesso tipo di cloud computing è adatto a tutte le esigenze. Sono disponibili numerosi modelli, tipi e servizi diversi per offrire la soluzione più adatta in base alle tue esigenze.

Per prima cosa, devi determinare il tipo di distribuzione cloud, ovvero l'architettura di cloud computing, in cui verranno implementati i servizi cloud. Ci sono tre modalità diverse di distribuzione dei servizi cloud: in un cloud pubblico, in un cloud privato e in un cloud ibrido.

Cloud pubblico

I cloud pubblici sono di proprietà di un provider di servizi cloud di terze parti, che fornisce le risorse di calcolo, come server e risorse di archiviazione, tramite Internet. Microsoft Azure è un esempio di cloud pubblico. In un cloud pubblico, l'hardware, il software e l'infrastruttura di supporto appartengono al provider di servizi cloud, che li gestisce. Puoi accedere a questi servizi e gestire il tuo account usando un Web browser.

Cloud privato

Un cloud privato si riferisce alle risorse di cloud computing usate esclusivamente da una singola azienda o organizzazione. Un cloud privato può trovarsi fisicamente nel data center locale della società. Alcune

società, inoltre, pagano provider di servizi di terze parti per ospitare il proprio cloud privato. Un cloud privato è un cloud in cui servizi e infrastruttura sono gestiti in una rete privata.

Cloud ibrido

I cloud ibridi combinano cloud privato e pubblico, grazie a una tecnologia che consente la condivisione di dati e applicazioni tra i due tipi di cloud. Grazie alla possibilità di spostare dati e applicazioni tra cloud pubblici e privati, un cloud ibrido offre all'azienda maggiore flessibilità e più opzioni di distribuzione e aiuta a ottimizzare l'infrastruttura esistente, la sicurezza e la conformità.

Tipi di servizi cloud: IaaS, PaaS, serverless e SaaS

La maggior parte dei servizi di cloud computing rientra in quattro ampie categorie: infrastruttura distribuita come servizio (IaaS), piattaforma distribuita come servizio (PaaS), elaborazione serverless e software come un servizio (SaaS). Talvolta si parla di "stack" di cloud computing, in quanto queste categorie sono basate una sull'altra. La conoscenza di queste soluzioni e delle loro differenze semplifica il raggiungimento degli obiettivi aziendali.

Infrastruttura distribuita come servizio (Infrastructure as a service, IaaS)

Si tratta della categoria di base dei servizi di cloud computing. Con una soluzione IaaS, affitti l'infrastruttura IT, ovvero server e macchine virtuali (VM), risorse di archiviazione, reti e sistemi operativi, da un provider di servizi cloud con pagamento in base al consumo

Piattaforma distribuita come servizio (PaaS, Platform as a Service)

PaaS (piattaforma distribuita come servizio, Platform as a Service) si riferisce a servizi di cloud computing che forniscono un ambiente su richiesta per lo sviluppo, il test, la distribuzione e la gestione di applicazioni software. Una soluzione PaaS è progettata per consentire agli sviluppatori di creare in modo più semplice e rapido app Web o per dispositivi mobili, senza doversi preoccupare della configurazione o della gestione dell'infrastruttura di server sottostante, della rete di archiviazione e dei database necessari per lo sviluppo.

Software come un servizio (SaaS, Software as a Service)

SaaS (Software as a Service, software come un servizio) è un metodo per la distribuzione di applicazioni software tramite Internet, su richiesta e in genere in base a una sottoscrizione. Con una soluzione SaaS, i provider di servizi cloud ospitano e gestiscono l'applicazione software e l'infrastruttura sottostante e si occupano delle attività di manutenzione, come gli aggiornamenti software e l'applicazione di patch di protezione. Gli utenti si connettono all'applicazione tramite Internet, in genere con un Web browser nel telefono, tablet o PC.

Usi del cloud computing

Probabilmente stai usando il cloud computing proprio adesso, anche se non te ne rendi conto. Se usi un servizio online per inviare posta elettronica, modificare documenti, guardare film o programmi TV, ascoltare musica, giocare oppure archiviare immagini o altri file, è probabile che tutto questo sia possibile grazie al cloud computing, che agisce dietro le quinte. I primi servizi di cloud computing risalgono appena a

una decina di anni fa, ma già molte organizzazioni, dalle piccole startup alle multinazionali, dagli enti pubblici alle organizzazioni no profit, stanno adottando questa tecnologia per i motivi più vari.

Ecco alcuni esempi di ciò che è possibile fare oggi con i servizi cloud di un provider di servizi cloud:

Crea applicazioni native del cloud

Crea, distribuisci e ridimensiona rapidamente le applicazioni per il Web, i dispositivi mobili e le API. Sfrutta i vantaggi delle tecnologie e degli approcci nativi del cloud, tra cui contenitori, Kubernetes, architettura basata su microservizi, comunicazioni basate su API e DevOps.

Testare e compilare le applicazioni

Riduci i costi e i tempi di sviluppo delle applicazioni usando infrastrutture cloud che consentono di aumentare o ridurre facilmente le prestazioni in base alle esigenze.

Archiviare i dati ed eseguirne il backup e il ripristino

Proteggi i dati razionalizzando i costi e su vasta scala, grazie alla possibilità di trasferire i dati tramite Internet su un sistema di archiviazione cloud esterno accessibile da qualsiasi posizione e da qualunque dispositivo.

Analizzare i dati

Unifica i dati tra team, divisioni e sedi nel cloud. Usa quindi i servizi cloud, come Machine Learning e intelligenza artificiale, per acquisire informazioni dettagliate e prendere decisioni più informate.

Trasmettere in streaming audio e video

Rimani in contatto con i tuoi destinatari ovunque, in qualsiasi momento e su qualunque dispositivo, grazie alle funzionalità audio e video ad alta definizione con distribuzione globale.

Incorporare l'intelligence

Usa modelli intelligenti per coinvolgere i clienti e raccogliere informazioni dettagliate preziose dai dati acquisiti.

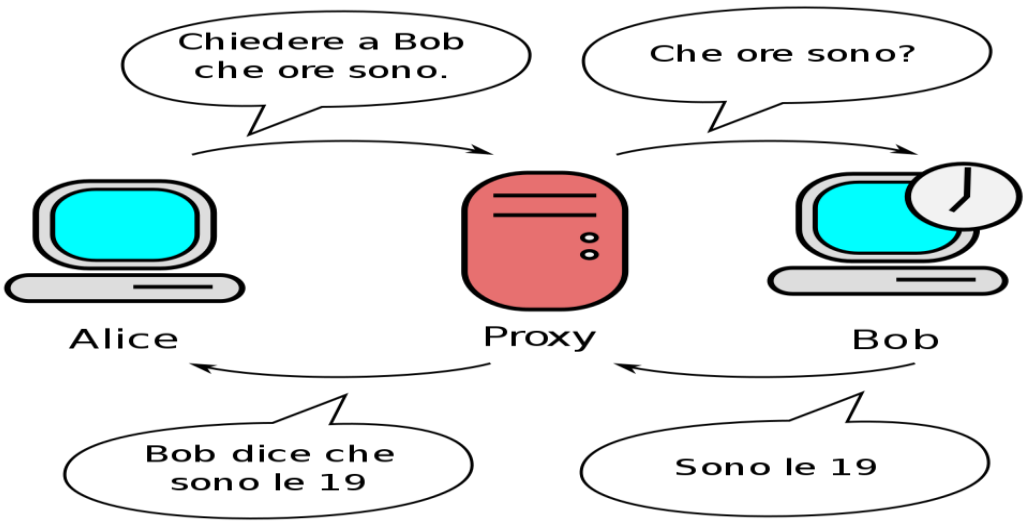
Fornire software on demand

Anche noto come Software as a Service, il software su richiesta ti permette di offrire le versioni e gli aggiornamenti più recenti del software ai tuoi clienti, sempre e ovunque si trovino.

Proxy

Proxy, in informatica e telecomunicazioni, indica un tipo di server che funge da intermediario per le richieste da parte dei client alla ricerca di risorse su altri server, disaccoppiando l'accesso al web dal browser. Un client si connette al **server proxy**, richiedendo qualche servizio (ad esempio un file, una pagina web o qualsiasi altra risorsa disponibile su un altro server), e quest'ultimo valuta ed esegue la richiesta in modo da semplificare e gestire la sua complessità. I proxy sono stati inventati per aggiungere struttura e incapsulamento ai sistemi distribuiti.

Un proxy è un software che si occupa di ricevere le vostre richieste (ad esempio l'accesso a un indirizzo web) e si occupa di elaborare e soddisfare la richiesta. Un proxy si interpone tra voi (che siete il cliente) e il server.



Il client si collega al proxy invece che al server e gli invia delle richieste. Il proxy a sua volta valuta ed esegue la richiesta in modo da semplificare e gestire la sua complessità e si collega al server e inoltra la richiesta del client.

Ad oggi il Proxy vengono utilizzati per svariati impieghi come:

1)Fornire l'**anonimato** durante la navigazione internet

2)Memorizzare una **copia locale** degli oggetti web in modo da poterli fornire nuovamente senza effettuare altri accessi

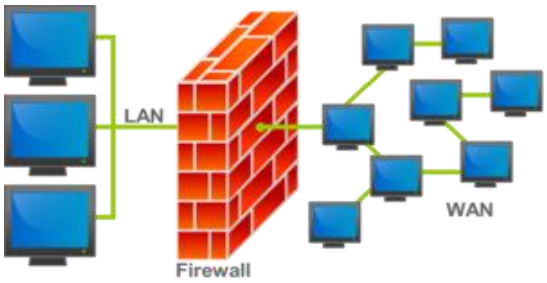
3)Creare una «**barriera di difesa**» agendo da filtro per le connessioni entranti ed uscenti e monitorando, controllando e modificando il traffico interno

Firewall

Il firewall è un sistema di sicurezza informatico che permette di proteggere il computer e la rete da eventuali agenti esterni. Il firewall permette di bloccare e limitare i file e i siti prima che entrino nella rete interna, in base a delle regole predefinite.
Il firewall permette, quindi, di filtrare in base alle eventuali necessità, facendo sì che i dati passino da un

unico punto sia per entrare che per uscire, con l'obiettivo fondamentale di proteggere la rete.

Si tratta di un dispositivo(elemento hardware o un'applicazione software) per la sicurezza della rete che permette di monitorare il traffico in entrata e in uscita utilizzando una serie predefinita di regole di sicurezza o bloccare gli eventi.



Si tratta di una specie di filtro che controlla il traffico di dati e blocca le trasmissioni pericolose o indesiderate in base a una serie di regole specifiche: dispongono di norme standard che possono essere aggiunte altre personalizzate dal'utente.

I firewall utilizza uno di questi criteri generali di applicazione delle regole:

1) **Default-deny**, viene accettato solo ciò che viene autorizzato, il resto viene vietato (più usato, più sicuro)
2) **Default-allow,** viene bloccato solo ciò che viene vietato esplicitamente, il resto viene permesso

In base al tipo di controllo e analisi delle trasmissioni di dati, possiamo distinguere i seguenti tipi di firewall:

Firewall con filtro di pacchetti, analizza i dati contenuti nei pacchetti, le confronta con le regole di filtro impostate. Questa tipo è affidabile ma limitata perché minacciata dallo spoofing

Firewall con analisi dello stato della connessione, analizza sia i pacchetti ma anche la connessione, le porte utilizzate con il computer e i protocolli di trasmissione

Firewall a livello di applicazione, svolgono un'analisi approfondita sulle singole applicazioni che funzionano da intermediari nella comunicazione, e possono bloccare le connessioni in tempo reale

Dmz

Nell'ambito delle reti informatiche e della sicurezza informatica, una demilitarized zone (DMZ, in italiano zona demilitarizzata), è la funzione di un router che permette di dirottare, senza controllarne l'attendibilità, tutto il traffico proveniente dalla rete Internet verso una determinata interfaccia di un apparato di rete, il quale si occuperà poi di gestire e proteggere il traffico.

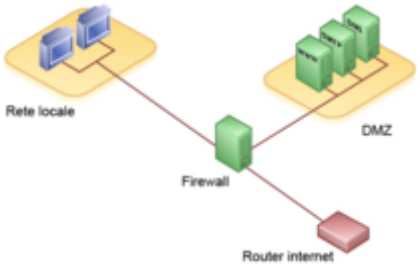
Con DMZ si indica quindi una rete di computer, che funge tra due reti da **intermediario** e le delimita mediante regole di accesso rigide. Una DMZ funziona come una piccola rete isolata posizionata tra internet e la rete interna. Il suo scopo è quello di aggiungere un ulteriore livello di sicurezza ad una rete locale aziendale, dove un nodo appartenente ad una rete esterna può accedere soltanto ai servizi messi a disposizione, senza mettere a rischio e compromettere la sicurezza dell'intera rete.

Una DMZ può essere creata attraverso la definizione di policy distinte su uno o più firewall.

Una DMZ con un solo firewall

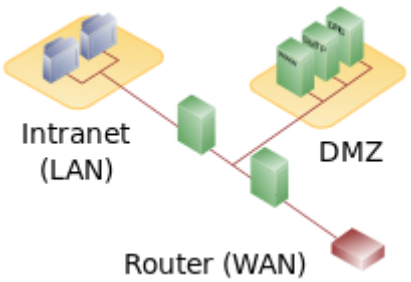
La rete dispone di un singolo firewall con almeno 3 interfacce di rete, le quali forniscono rispettivamente un collegamento con:

- La rete esterna, dalla quale arrivano le richieste internet tramite un router (WAN).
- La rete interna (intranet).
- La DMZ



In una **DMZ** di questo tipo vengono controllate dallo stesso firewall tutte le porte, indipendenti l'una dall'altra. E rappresenta una configurazione poco sicura dovuta proprio alla presenza di un unico firewall. Inoltre, il firewall deve essere in grado di far fronte in una struttura di questo tipo sia al traffico proveniente da Internet sia agli accessi alla LAN.

Una DMZ con due firewall



Un approccio più sicuro consiste nell'utilizzare due firewall per creare una DMZ. La configurazione consiste nell'usare un primo firewall esterno come prima linea di difesa e deve essere configurato per consentire solo il traffico destinato alla DMZ. Il secondo firewall interno che consente solo il traffico dalla DMZ alla rete interna. C'è ancora più protezione se i due firewall usati provengono da due diversi fornitori, perché rende meno probabile che entrambi i dispositivi soffrano delle stesse vulnerabilità di sicurezza. Uno degli svantaggi di questa architettura è che è più costoso, sia da acquistare che da gestire.).

Una **DMZ** può essere creata attraverso la definizione di policy distinte su uno o più firewall. Genericamente i firewall intermedi controllano il traffico tra i server nella **DMZ**, i client interni ed esterni. Le connessioni dalle reti esterne verso la DMZ sono solitamente controllate tramite una tipologia di **NAT** chiamata "**port forwarding**" o "**port mapping**", implementata sul sistema che agisce da firewall che tipicamente sono di tipo **packet filter**. Una configurazione **DMZ** fornisce sicurezza dagli attacchi esterni, ma in genere non ha alcun effetto sugli attacchi interni come lo **sniffing** della comunicazione tramite un analizzatore di pacchetti o attacchi di **spoofing**.

Servizi che implementano una DMZ

Server Web

I **server Web** potrebbero dover comunicare con un database interno per fornire alcuni servizi specializzati. A volte è anche buona norma configurare una **Zona Militarizzata Classificata** (**CMZ**) separata dalla **DMZ**, cioè una zona militarizzata altamente monitorata che comprende per lo più server Web e server simili che si interfacciano con il mondo esterno, cioè Internet. In questo modo proteggiamo i server di database mettendoli in una zona separata dalla **CMZ** essendo quest'ultima pubblicamente accessibile. In genere, non

è una buona norma consentire al server Web di comunicare direttamente con il server database sottostante. Invece, può essere utilizzato un **firewall** dell'applicazione che funge da mezzo di comunicazione tra il server del database e il server web. Ciò fornisce un ulteriore livello di sicurezza, sebbene più complesso. Questo tipo di configurazione ha però uno svantaggio dovuto al fatto che gli utenti della **workstation** non possono usare directory di rete e apportare modifiche direttamente a pagine Web o altri file e quindi costretti ad usare protocolli applicativi come **FTP** per caricare o scaricare le pagine.

Server Email

I messaggi di posta elettronica degli utenti sono confidenziali quindi sono generalmente memorizzati su server a cui non è possibile accedere da Internet, e quindi inserito in una zona LAN. Per far sì che il server di posta interno comunichi con server di posta esterni, viene posto un server ausiliario nella **DMZ**, il quale riceve email in arrivo e le inoltra al server interno principale. In questo modo è possibile controllare la posta in arrivo sulla DMZ ad esempio tramite **sandbox** o **antivirus** prima di inoltrarla.

Server DNS

È possibile avere diverse configurazioni riguardante la posizione e il numero di server **DNS** in una **DMZ**. Se si dispone di un solo set di server **DNS**, sia per la zona interna che esterna, è necessario inserirli nella **DMZ** e consentire così agli utenti locali di accedervi anziché collocarli nella stessa rete interna e configurare nel firewall le richieste **DNS** esterne, la quale è una prassi poco sicura poiché permettiamo ad utenti esterni di accedere alla rete interna. La configurazione più comune consiste nell'usare due set di server **DNS**, un set di DNS interni e un set di server accessibili esternamente collocati nella **DMZ**, che è sicura ma accessibile solo dalla rete pubblica.

Cap4: La Crittografia

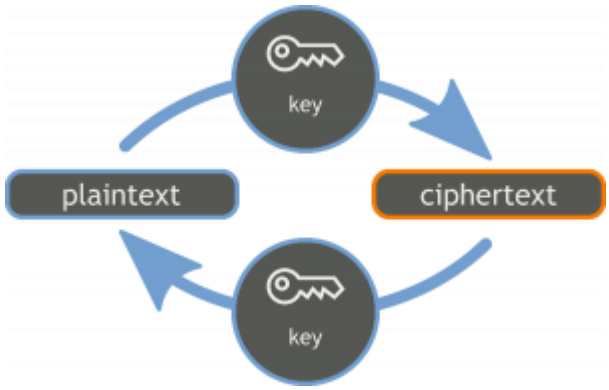
*Erodoto narra (libro V delle Storie) – **Istieo** voleva dare ad **Aristagora** l'ordine di ribellarsi,non aveva alcun altro modo per annunziarglielo con sicurezza, essendo le strade sorvegliate, fatta rasare la testa al più fido degli schiavi, vi impresse dei segni, e aspettò che ricrescessero i capelli. Non appena ricrebbero, lo spedì a **Mileto**, non comandando gli null'altro se non che, quando giungesse a **Mileto**,dicesse ad **Aristagora** di fargli radere i capelli e di guardare la sua testa: i segni impressi ordinavano,come già prima ho detto, la rivolta.*

La crittografia a chiave simmetrica

La crittografia simmetrica utilizza un algoritmo che **converte il messaggio originale in chiaro in un messaggio crittografato con testo cifrato** utilizzando una chiave di crittografia. **La stessa chiave viene utilizzata dal destinatario per convertire il testo cifrato in testo normale.** Applichiamo questo concetto al nostro esempio.

Se Alice vuole inviare un messaggio a Bob, lo crittografa con una chiave simmetrica. Quando Bob lo riceve**, usa la stessa chiave per decifrare il messaggio**. Senza la chiave, gli utenti malintenzionati non possono accedere alla comunicazione crittografata tra i due utenti, e questo la manterrà riservata.

Solitamente, **la chiave simmetrica viene generata a ogni sessione e non è valida per le comunicazioni successive**. Possiamo chiamarla chiave di sessione.



Tuttavia, questo approccio ha degli svantaggi:

1. **Scalabilità:** la nostra soluzione non è scalabile. Se 1.000 utenti vogliono comunicare tra loro, ognuno di loro avrebbe bisogno di 999 chiavi diverse per stabilire un canale sicuro**.**
2. **Distribuzione delle chiavi:** abbiamo ipotizzato che entrambe le parti abbiano accesso alla chiave simmetrica, ma come ottengono questa chiave in primo luogo? Se Alice genera una chiave simmetrica (chiave di sessione) e la invia a Bob, l'utente malintenzionato potrebbe intercettarla e decrittografare qualsiasi altra comunicazione.

Il cifrario di Cesare

La crittografia è usata da secoli ormai nella nostra civiltà, uno dei primi algoritmi di cifratura sembra risalire a uno degli imperatori di Roma, Cesare. Egli studiò un sistema per comunicare senza essere scoperti.

L’algoritmo era a dir poco banale, ma essendo il primo del suo genere ovviamente era difficile capire per il nemico cosa volesse dire quell’insieme di caratteri senza senso. L’algoritmo fu presto ribattezzato Crittografia di Cesare. Questa consisteva semplicemente nello spostare in avanti o indietro le lettere che compongono una parola, di un tot di posizioni già prefisse e note sia al mittente che al destinatario.

Ad esempio spostando di 1 lettera indietro sull’alfabeto, la parola **ciao** otteniamo **bhzn**, il destinatario che riceve quella parola risposta in avanti le lettere e ottiene la parola ciao. I questo caso specifico, il numero di posizioni da spostare in avanti o indietro è detta *chiave di crittografia*.

Il Cifrario di Vigenère

Blaise de Vigenère pubblicò nel 1586 un trattato di cifre nel quale partendo dalla cifra di Bellaso del 1553 proponeva una tavola quadrata come quella dell'abate Tritemio da usarsi con una parola chiave come proposto da Bellaso. Con il nome di tavola di Vigenère è poi entrata nella letteratura crittografica una versione semplificata di quella pubblicata nel trattato. Si tratta della più semplice cifra di sostituzione polialfabetica, e proprio per la sua semplicità ha goduto per secoli di grande popolarità fino ad essere considerata indecifrabile, fama piuttosto esagerata, essendo più debole di altre cifre polialfabetiche precedenti come il disco di L.B. Alberti, o delle cifre del Bellaso essendo più ordinata. Tale fortuna è durata fino a molti decenni dopo che era stato pubblicato un primo metodo di decrittazione: quello del Kasiski; e altri metodi di crittanalisi sono possibili.

Va detto che dal Vigenère possono ricavarsi cifrari molto più sicuri usando alfabeti disordinati, e soprattutto chiavi molto lunghe, che al limite portano al cifrario di Vernam, considerato il cifrario teoricamente perfetto.

Il metodo

Il metodo si può considerare una generalizzazione del cifrario di Cesare; invece di spostare sempre dello stesso numero di posti la lettera da cifrare, questa viene spostata di un numero di posti variabile, determinato in base ad una parola chiave, da concordarsi tra mittente e destinatario, e da scriversi sotto il messaggio, carattere per carattere; la parola chiave è detta anche *verme*, per il motivo che, essendo in genere molto più corta del messaggio, deve essere ripetuta molte volte sotto questo, come nel seguente esempio:

Testo chiaro - ARRIVANOIRINFORZI Verme - VERMEVERMEVERMEVE Testo cifrato - VVIUZVRFUVDRWAVUM

Il testo cifrato si ottiene spostando la lettera chiara di un numero fisso di caratteri, pari al numero ordinale della lettera corrispondente del verme. Di fatto si esegue una somma aritmetica tra l'ordinale del chiaro (A = 0, B = 1, C = 2 ...) e quello del verme; se si supera l'ultima lettera, la Z, si ricomincia dalla A. Matematicamente il Vigenère si riduce a un'addizione modulo 26 (vedi aritmetiche finite).

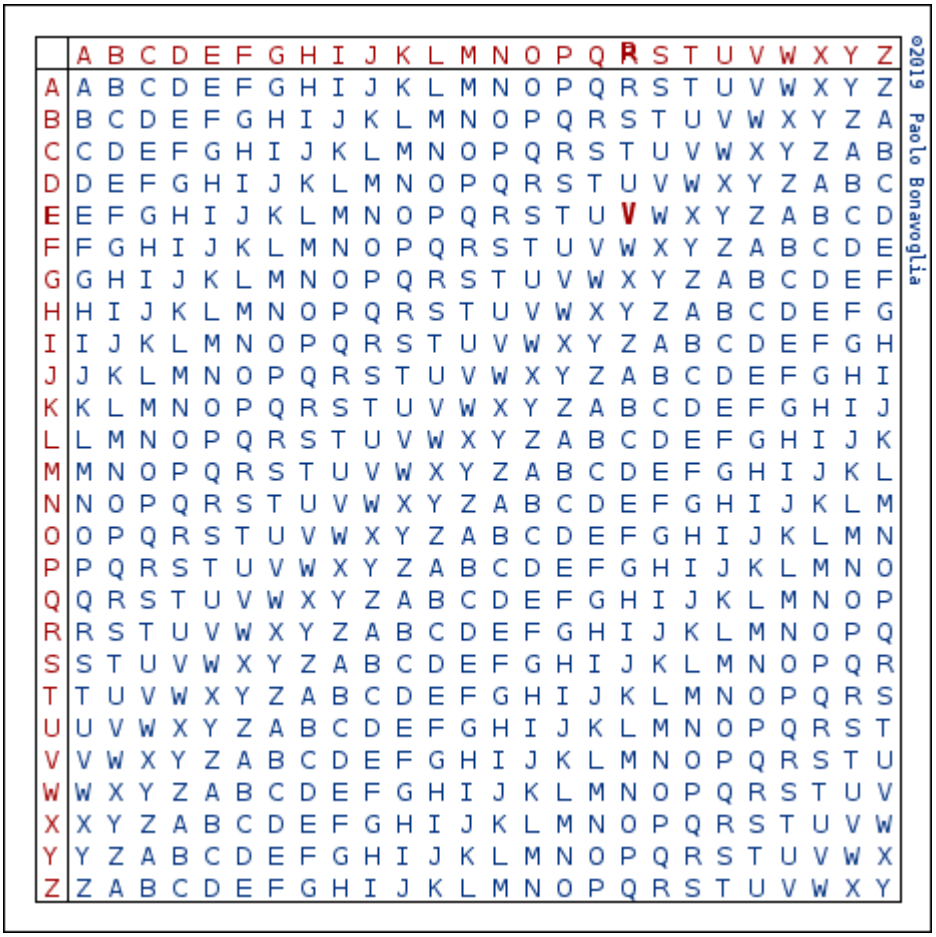
Per semplificare questa operazione Vigenère usa la tavola quadrata del Tritemio, composta da alfabeti ordinati spostati. Volendo ad esempio cifrare la prima **R** di ARRIVANO si individuerà la colonna della **R**, quindi si scenderà lungo la colonna fino alla riga corrispondente della corrispondente lettera del verme (qui **E**); la lettera trovata all'incrocio è la lettera cifrata (qui **V**); la seconda **R** invece sarà cifrata con la lettera trovata sulla riga della **R** di VERME, e cioé con la **I**.

Il vantaggio rispetto alle cifre mono-alfabetiche è evidente: la stessa lettera del testo chiaro non è sempre cifrata con la stessa lettera; e questo rende più difficile l'analisi statistica del testo cifrato e la decrittazione.

Chi riceve il messaggio per decifrarlo deve semplicemente usare il metodo inverso (sottrarre invece che sommare); riferendosi all'esempio di sopra si avrà:

Testo cifrato - VVIUZVRFUVDRWAVUM Verme - VERMEVERMEVERMEVE Testo chiaro - ARRIVANOIRINFORZI

si potrà decifrare la seconda **V** ricercandola nella riga della corrispondente lettera del verme, la **E**; la colonna dove si trova la **V** ha al primo posto in alto la lettera chiara, la **R**.



Varianti

Basandosi su queste semplici regole è possibile creare cifrari personalizzati, ad esempio usando come chiave di cifratura la data di oggi, o del compleanno di qualcuno. Oppure un'altra parola sfruttando il numero della posizione che occupa il singolo carattere nell'alfabeto e migliaia ancora di variabili.

Questi metodi sono detti a chiave unica o **crittografia simmetrica**, e sono stati utilizzati per anni nell'informatica. Hanno dato vita a cifrari di tutto rispetto come ad esempio il cifrario di Rijndael scelto per il prossimo standard del famosissimo AES (Advanced Encryption Standard). Utilizzato per la crittografia delle connessioni Wi-Fi, andrà presto a sostituire l'ormai vecchio DES (Data Encryption Standard).

Questi sistemi hanno però un grande problema, cioè quello che in un modo o nell'altro la chiave usata per cifrare il messaggio deve essere condivisa con il nostro destinatario. Quindi si corre il rischio che venga intercettata e si comprometta così l'intero sistema crittografico

Operazione Colossus, la lotta contro Enigma.

Figura 1 : Enigma

Allo scoppio della Seconda Guerra Mondiale, le operazioni di decifrazione britanniche furono spostate da Londra a Blechtley Park. Una delle figure più importanti che lavorò in questo dipartimento spionistico fu senza dubbio il matematico Alan Turing, il cui lavoro fu reso noto solo molti anni dopo, quando cadde il segreto militare sulle tecniche di crittoanalisi sviluppate durante la guerra.

La figura di Turing costituisce un baluardo per lo studio della calcolabilità logico-matematica, lo strumento da lui utilizzato è oggi noto come Macchina di Turing, un calcolatore in grado di leggere le informazioni da un nastro, eseguire un algoritmo e restituire un output su un altro nastro.

Le comunicazioni tedesche erano cifr ate con una macchina chiamata Enigma, uno dei più sofisticati cifrari a rotore (sostituiti poi dai più moderni e innovativi cifrari elettronici,che hanno letteralmente sconvolto il mondo della crittografia).Enigma era però sprovvisto di una stampante, i risultati apparivano illuminati su un'apposita tastiera e dovevano essere trascritti su un foglio di carta: fu così che gli Inglesi entrarono in possesso di un "known plain text", "testo in chiaro noto", ribattezzato in seguito in crib. Ciò, unito alla reversibilità del processo, permise a Turing di scoprire l'algoritmo stesso e di costruire un meccanismo automatico di decrittazione: la **Bomba di Turing**.

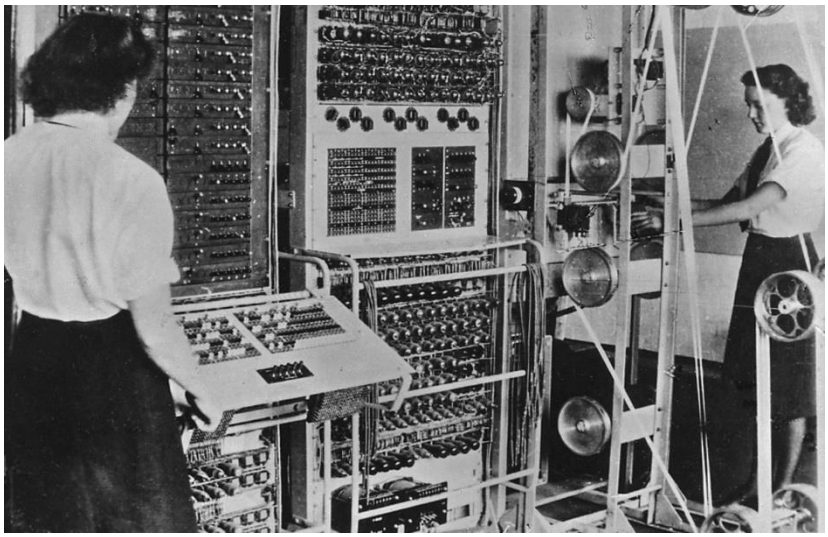


Figura 2 : Colossus

Lo scopo del suo workgroup, formato da circa settemila persone tra militari,civili, matematici, giocatori d'azzardo, era quello di rompere Enigma: a questo fine, Turing si servì di **Colossus**, una gigantesca macchina inventata da un esperto di centralini telefoni ci, che può essere considerata un predecessore dei successivi calcolatori elettromeccanici. Grazie al **Colossus**, la "Bomba", Turing era in grado di trovare i codici nazisti in pochi minuti, per intercettare le comunicazioni italo-tedesche. In questo modo gli alleati poterono cambiare letteralmente il corso della guerra,prendendosi un grande vantaggio sulla stessa marina italiana sconfitta a capo Matapan nel 1941. Tutti gli esemplari di Colossus vennero smantellati alla fine della guerra.

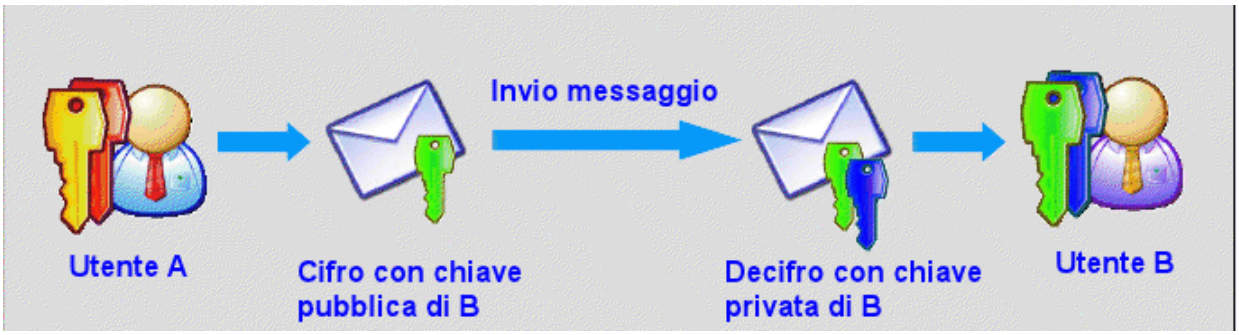
Dal canto loro gli Americani, nel tentativo di ottenere comunicazioni vocali "sicure", avevano sperimentato il linguaggio degli indiani Choctaws, che già era di per se criptato. Dopo la guerra questo tipo di comunicazione venne ulteriormente perfezionato, tramite l' uso del linguaggio Navajos. Questo tipo di comunicazioni, chiamati comunemente NAC (Native American Codetalkers) non è mai stato infranto.

La crittografia a chiave asimmetrica

Si utilizza una coppia di chiavi diverse: una **diretta** e una **inversa**, collegate da una relazione matematica: le due chiavi assumono il nome di chiave privata (posseduta solo dall'ente o dalla persona che crea la coppia di chiavi, quindi di natura estremamente personale) e chiave pubblica (posseduta da chiunque ne abbia bisono, per tanto di dominio pubblico).

Le caratteristiche matematiche della coppia di chiavi fa si che un messaggio cifrato con la chiave privata possa essere decifrato **SOLAMENTE** utilizzando la chiave pubblica. Tale principio vale anche al contrario, posso cifrare un messaggio con la chiave pubblica e decifrarlo solamente con la chiave privata.

Caso 1



1. B genera le due chiavi e pubblica la sua chiave pubblica
2. A preleva la chiave pubblicata da B
3. A usa la chiave per cifrare il messaggio
4. A può mandare il messaggio

B è l'unico a poter decifrare il messaggio con la chiave privata. Immaginate che B sia ad esempio "Amazon", voi ovviamente siete "A" e il messaggio è il numero della vostra carta di credito che usate per acquistare dal sito. Ora capite perché siamo ragionevolmente sicuri che nessuno ruberà il nostro "dato sensibile" e l'unico che avrà la possibilità di leggere il numero di carta sarà "Amazon".

Caso2

In questo caso, tutti possono leggere il messaggio cifrato da A. Quindi è ovvio che non stiamo proteggendo la riservatezza del messaggio. Tuttavia pensate a chi può aver cifrato il messaggio con la chiave privata di "A" ? Solamente "A". Quindi in questo modo siamo sicuri che il mittente è chi dice di essere, e stiamo proteggendo l'autenticità del mittente oltre che garantire il non ripudio del messaggio.

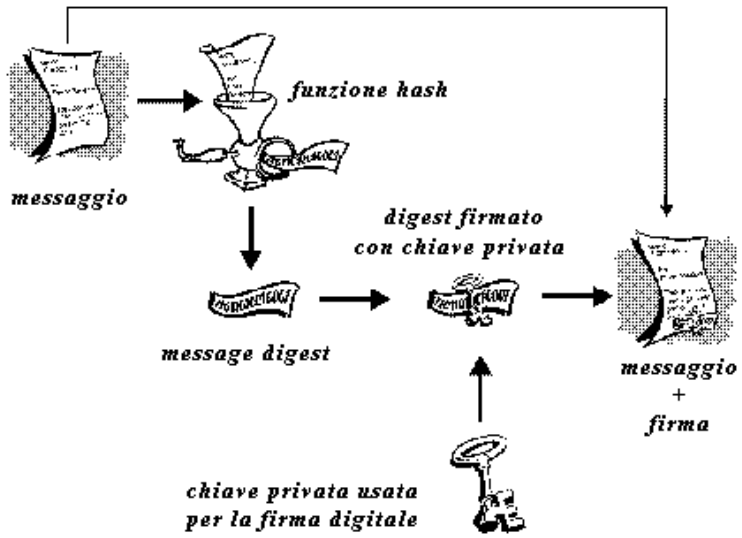
Applicazioni della crittografia (firma digitale)

La firma digitale è un metodo matematico che serve a dimostrare l'autenticità di un messaggio inviato attraverso un canale non sicuro, facendo diventare ad esempio dei semplici documenti a documenti con un valore legale.

Essa è basata su un sistema di chiavi asimmetriche a coppia, una pubblica e una privata, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di verificare la provenienza e l'integrità di un documento.

Questo procedimento è basato su 3 concetti fondamentali:

- Integrità, ovvero la condizione che mi garantisce che i miei documenti non subiscono modifiche, non vengono corrotti o rovinati, nel tempo.
- Autenticità, la quale ci garantisce che chi ha firmato il documento è veramente chi dice di essere.
- Non ripudio, secondo il quale chi ha firmato il documento mediante firma elettronica non può poi disconoscerlo.



Nella firma digitale una persona firma un documento usando la sua chiave privata, mentre le altre persone, che vogliono controllare l'autenticità e l'integrità usano la chiave pubblica. A partire dal documento, viene generata un'impronta, cioè una sequenza binaria di lunghezza fissa (128 o 160 bit) che rappresenta un "riassunto" (digest) del documento. L'impronta viene generata usando la funzione hash, con la garanzia che a partire da documenti diversi si ottengono impronte diverse. Questa impronta viene poi codificata utilizzando la chiave privata e il risultato rappresenta la firma digitale.