ROMA TRE UNIVERSITÀ DEGLI STUDI
Corso di Laurea in Matematica
Dipartimento di Matematica e Fisica

Sistemi per l'elaborazione delle informazioni

8. Sicurezza dei sistemi informativi

Dispense del corso IN530 a.a. 2019/2020

prof. Marco Liverani

Sicurezza dei sistemi informativi

- In ambito IT garantire la sicurezza di un sistema informativo significa garantirne:
  - **riservatezza delle informazioni** (*confidentiality*): solo chi è autorizzato deve poter accedere all'informazione;
  - **integrità delle informazioni** (*integrity*): le informazioni non devono essere danneggiate o modificate per caso o con intenzioni malevole;
  - **disponibilità delle informazioni** (*availability*): le informazioni devono essere sempre disponibili a chi è autorizzato ad utilizzarle
- Occuparsi di sicurezza informatica significa quindi predisporre **politiche**, **processi**, **controlli** e **contromisure informatiche** in grado di **contrastare le minacce** che rischiano di compromettere la riservatezza, l'integrità e la disponibilità delle informazioni
- Nell'ambito della sicurezza informatica l'oggetto più prezioso da proteggere è l'**informazione**, il **dato**, o il **servizio di business** erogato con il supporto del sistema informatico (es.: il valore di un computer non è dato solo dal suo prezzo di acquisto, ma soprattutto dall'importanza del dato che gestisce e del servizio che eroga)

Sicurezza dei sistemi informativi

- Perché si adottano delle misure di sicurezza? Da cosa ci si vuole proteggere?
- Le **minacce per un sistema informativo** sono di diversi tipi:
  1. **catastrofi naturali** e **incidenti** imprevisti
  2. **aggressione da parte di hacker**, ossia da parte di soggetti esterni intenzionati a compromettere la sicurezza del sistema informativo: per danneggiare l'azienda sottraendo informazioni, compromettendo le informazioni o rendendole indisponibili e in questo modo impedendo la corretta erogazione di un servizio di business o la realizzazione di un prodotto
  3. **software malevolo**, come virus o malware, in grado di danneggiare i dati o i sistemi informatici, anche solo deteriorandone le performance
  4. **attività scorrette e illecite** da parte di personale interno all'organizzazione aziendale, dipendenti e collaboratori dell'azienda, talvolta effettuate inconsapevolmente
- Tali minacce sono in grado di provocare un danno al business aziendale, attraverso:
  - la **compromissione dei sistemi informatici** che consentono all'azienda di erogare un servizio ai propri clienti;
  - la **fuga di notizie riservate**, che potrebbero danneggiare direttamente l'azienda (es.: dati commerciali o brevetti) o i suoi clienti (es.: numeri di carte di credito o informazioni sanitarie)
  - la **modifica o la cancellazione di dati rilevanti** (es.: spostamento di valori economici sui conti bancari o su conti assicurativi o previdenziali)

Domini tematici della Sicurezza IT

(ISC)² – *International Information Systems Security Certification Consortium*, ha definito 8 domini tematici della sicurezza IT: questa suddivisione rappresenta una buona classificazione degli ambiti di intervento della sicurezza informatica (CISSP *knowledge domains*)

1. Security and Risk Management
Confidentiality, integrity, and availability concepts; Security governance principles; Compliance; Legal and regulatory issues; Professional ethic; Security policies, standards, procedures and guidelines

2. Asset Security
Information and asset classification; Ownership (e.g. data owners, system owners); Protect privacy; Appropriate retention; Data security controls; Handling requirements

3. Security Engineering
Engineering processes using secure design principles, Security capabilities of information systems, Security architectures, designs, and solution elements vulnerabilities, Web-based systems vulnerabilities, Mobile systems vulnerabilities, Cryptography, Physical security

4. Communication and Network Security
Secure network architecture design, Secure network components, Secure communication channels, Network attacks

5. Identity and Access Management
Physical and logical assets control, Identification and authentication of people and devices, Third-party identity services, Access control attacks, Identity and access provisioning lifecycle

6. Security Assessment and Testing
Assessment and test strategies, Security process data, Security control testing, Test outputs, Security architectures vulnerabilities

7. Security Operations
Investigations, Incident Management, and Disaster Recovery, Logging and monitoring activities, Patch and vulnerability management, Change management processes, Recovery strategies
Disaster recovery processes and plans
Business continuity planning, Physical security

8. Software Development Security
Security in the software development lifecycle, Development environment security controls, Software security effectiveness, Acquired software security impact

The Map of Cybersecurity Domains

Alcuni tipi di attacco informatico

- Attacchi in grado di sfruttare specifiche **debolezze di un programma software**
  - **Exploit**: sfruttando un bug o una "vulnerabilità" del software, l'attaccante riesce a far eseguire il codice di un programma al target sotto attacco, in modo da danneggiare le informazioni, comprometterne la riservatezza o acquisire privilegi elevati sulla macchina
  - **Shell code**: è un attacco che mediante un exploit riesce ad eseguire una shell del sistema operativo sulla macchina target
  - **Buffer overflow** (anche stack overflow, heap overflow): è un attacco che, saturando un'area di memoria della macchina, sovrascrive la memoria adiacente, compromettendo il corretto funzionamento del programma o dell'intero sistema; tipicamente sono dovuti ad una inadeguata gestione dell'input da parte del programma, che accetta quantità di dati in ingresso tali da saturare la memoria dedicata al processo
  - **Cracking**: modifica software con l'obiettivo di rimuovere un codice di protezione di un programma o di accedere ad aree protette del sistema; viene effettuato eseguendo il *reverse engineering* del codice binario di un programma

Alcuni tipi di attacco informatico

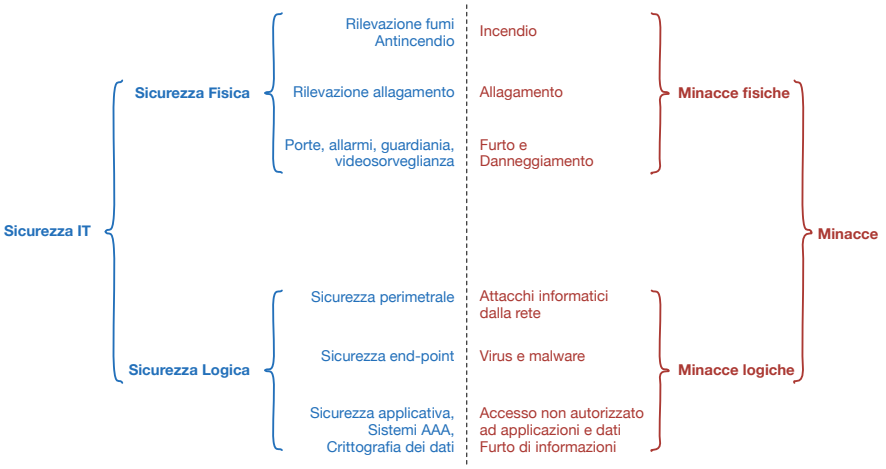
- Attacchi in grado di sfruttare **connessioni di rete** e porte TCP di accesso al sistema target o di intervenire sul traffico di rete
  - **Backdoor**: è una tecnica di attacco ad un sistema informatico che sfrutta porte "nascoste", ma lasciate aperte da chi gestisce il sistema per eseguire più agevolmente operazioni di manutenzione del sistema; una backdoor può anche essere attivata mediante un programma "trojan" che crea una porta di accesso via rete al computer attivando un servizio non autorizzato in ascolto su una specifica porta TCP o UDP
  - **Port scanning**: scansione di tutte le possibili porte TCP/UDP aperte su un host, al fine di studiarne la configurazione e individuarne delle debolezze o dei punti di attacco
  - **Sniffing**: intercettazione dei pacchetti che viaggiano sulla rete a cui è connesso il computer dell'attaccante; l'obiettivo è quello di carpire informazioni riservate trasmesse "in chiaro"
  - **Keylogging**: intercettazione (mediante software malware o dispositivi hardware collegati al computer attaccato) dei dati digitati sulla tastiera dall'utente durante una normale sessione di lavoro
  - **Spoofing**: si tenta di accedere ad un host, falsificando l'identità del computer dell'attaccante (indirizzo IP, MAC address, hostname DNS, ecc.)
  - **DoS**/**DDoS**: *Denial of Service*/*Distributed Denial of Service*, sono attacchi provenienti da uno (DoS) o più computer (DDoS) collegati alla rete, che, utilizzando porte di connessione del server sotto attacco, note e aperte per l'erogazione di servizi, mirano a saturarne le risorse (es.: numero di connessioni contemporanee gestibili dal server) fino a rendere non più fruibili i servizi erogati dal server

Alcuni tipi di attacco informatico

- Attacchi condotti con l'utilizzo di **software malevolo** (malware, virus, ...)
  - **Malware**: è genericamente un software che opera con l'intenzione di violare la protezione delle informazioni presenti su un computer per eliminarle o trafugarle
  - **Trojan Horse**: è un software che viene eseguito inconsapevolmente dall'utente sul proprio computer e, così facendo, provoca l'apertura di una porta TCP che viene sfruttata dall'attaccante per accedere al computer
  - **Virus**: sono software che danneggiano i dati presenti sul computer e che hanno la capacità di attivarsi agganciandosi ad un programma non malevolo, modificandone il codice binario; ogni volta che il programma "contagiato" viene eseguito, viene eseguito anche il virus
  - **Spyware**: software che inviano a destinatari esterni e non autorizzati, informazioni presenti sul computer su cui è installato lo Spyware
  - **Ransonware**: software che limita l'uso del sistema eseguendo la cifratura dei dati e richiedendo un riscatto per ottenere la chiave con cui decifrare i dati (o l'intero filesystem del computer)
- Attacchi di **social engineering**, con l'obiettivo di sfruttare la scarsa consapevolezza della riservatezza delle informazioni apparentemente non critiche da parte del personale di un'organizzazione, per accedere ad informazioni riservate
  - Le tecniche di social engineering prevedono anche l'acquisizione di **materiale di scarto** (fogli stampati, dischetti, CD, DVD, hard disk dismessi, per acquisire informazioni utili a portare a termine un attacco al sistema informativo
  - Altre tecniche consistono nel fornire **strumenti dotati di Trojan** che vengono poi inseriti inconsapevolmente dagli utenti sui loro computer
  - Tecniche di social engineering/social hacking sono usate per compiere **furti d'identità**, trafugando le credenziali di un utente (a sua insaputa), per poi accedere al sistema attraverso canali standard

Sicurezza dei sistemi informativi

- La sicurezza si occupa di predisporre contromisure idonee a contrastare minacce di tipo "**fisico**" e di tipo "**logico**": le prime riguardano l'integrità dei sistemi (computer, reti, ecc.), le altre riguardano minacce e contromisure di tipo software



Sicurezza fisica di un sistema informativo

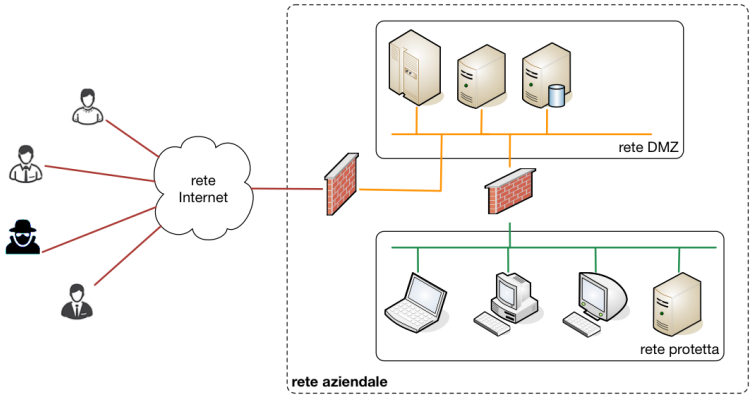
- La sicurezza fisica del sistema informativo riguarda prevalentemente:
  - **sicurezza dell'edificio** che ospita il sistema informativo:
    - guardiania
    - telecamere di videosorveglianza e sistemi di registrazione video
    - locali ad accesso riservato con porte blindate
  - controlli di **accesso delle persone** all'edificio
    - guardiania e personale di portineria
    - sistemi di identificazione e di controllo degli accessi delle persone (con badge personale o dati biometrici)
    - processi di accertamento dell'identità e rilascio di chiavi o badge di accesso
    - sistemi antifurto o di rilevazione della presenza in locali riservati
  - sistemi **anti-incendio** e **anti-allagamento**
    - rilevatori di fumo e fiamme
    - sistema automatico di allarme e dispositivi anti-incendio
    - porte, pareti, materiali, armadi ignifughi
  - sistemi di **business continuity** e di **disaster recovery**
    - gruppi di continuità elettrica e procedure di spegnimento sicuro dei sistemi in caso di prolungata assenza di energia elettrica
    - sistemi di climatizzazione dei locali CED al fine di garantire la corretta temperatura di esercizio dei sistemi
    - sistemi di ridondanza elettrica, di componenti hardware informatiche, di connessione di rete
    - piano di ripristino dei sistemi e delle attività in locali diversi e distanti da quelli del "sito primario" in caso di disastro ("sito secondario" o "sito di disaster recovery")

Sicurezza logica di un sistema informativo

- **Sicurezza perimetrale**
  - l'insieme degli strumenti e delle tecniche utilizzate per impedire accessi non autorizzati alla rete aziendale dall'esterno o attacchi informatici che possano compromettere l'erogazione di servizi
  - in questo ambito le contromisure sono strumenti che analizzano i pacchetti che viaggiano in rete bloccando quelli sospetti o attivando degli allarmi in loro presenza
- **Sicurezza degli end-point**
  - l'insieme degli strumenti e delle tecniche usate per proteggere i computer e gli altri dispositivi di tipo "end-point", ossia le foglie del grafo della rete informatica aziendale, costituite dai personal computer e dagli altri dispositivi connessi in rete
  - in questo ambito si opera attraverso apposite configurazioni del sistema operativo della macchina end-point (*hardening* della configurazione, cifratura dei volumi), attraverso l'aggiornamento software continuo, l'applicazione di patch di sicurezza e mediante l'installazione di software anti-malware e anti-virus
- **Sicurezza applicativa**
  - tecniche di scrittura di software sicuro, limitando il rischio di presenza di vulnerabilità, tecniche di verifica (*vulnerability assessment*, *application penetration test*)
  - strumenti di tipo AAA (*Authentication*, *Authorization*, *Accounting*) integrati con tutte le applicazioni del sistema informativo aziendale

Sicurezza perimetrale

- Obiettivo:
  - rendere accessibili dalla rete esterna i servizi offerti dal sistema informativo aziendale
  - proteggere il sistema informativo (e i suoi dati) da accessi non autorizzati dall'esterno
  - contrastare attacchi informatici condotti attraverso la rete (DoS/DDoS, port scanning, spoofing, ...)



Sicurezza perimetrale: firewall

- Il principale strumento di sicurezza perimetrale è il **Firewall**
  - È un computer dotato di **due o più interfacce di rete** e svolge il ruolo di gateway tra due o più reti
  - Gestisce le **regole che determinano il traffico** che può passare da una rete ad un'altra
- Tipicamente collega tre reti distinte:
  - **la rete esterna**, fuori dal perimetro del sistema informativo aziendale (es.: la rete Internet)
  - **la rete interna**, la rete aziendale vera e propria, a cui sono connessi gli end-point degli utenti interni; questa rete generalmente non è accessibile dall'esterno, ma i nodi di questa rete possono aprire connessioni verso nodi della rete esterna su alcuni protocolli applicativi e verso alcuni indirizzi esterni
  - **la rete DMZ** (*demilitarized zone*), la rete del sistema informativo aziendale a cui sono connessi gli host che erogano servizi verso l'esterno e che quindi devono essere accessibili dalla rete esterna (mail server, web server, DNS, ecc.)
- Processo operativo:
  - Valutazione della direzione del traffico (rete sorgente, rete destinazione) e selezione delle policy di sicurezza impostate
  - Valutazione della raggiungibilità dell'indirizzo di destinazione (eventualmente tramite NAT) dall'indirizzo di origine
  - Valutazione della raggiungibilità della porta TCP/UDP del server richiesta dal client sulla base delle policy di sicurezza impostate
  - Attivazione della connessione, oppure "drop" del pacchetto

Sicurezza perimetrale: IDS / IPS

- I sistemi **IDS** (*intrusion detection system*) sono apparati hardware o programmi software dedicati ad analizzare il traffico di rete in ingresso per rilevare sequenze di dati che siano riconoscibili come accessi non autorizzati dall'esterno
- I sistemi IDS si basano sull'applicazione di regole euristiche per stabilire se una connessione è illecita, un tentativo di intrusione (riuscito) non autorizzato
- I sistemi **IPS** (*intrusion prevention system*) sono, al contrario, sistemi che, analizzando il traffico di rete, identificano un tentativo di intrusione dall'esterno non autorizzato e non ancora eseguito e lo bloccano (*drop* del pacchetto di rete)
- Ad esempio i sistemi IDS e IPS sono in grado di identificare (IDS) e di bloccare (IPS) un port scan dalla rete esterna
- Spesso questi dispositivi sono una componente implementata nel software del Firewall

Sicurezza perimetrale: Content Filtering e Proxy Server

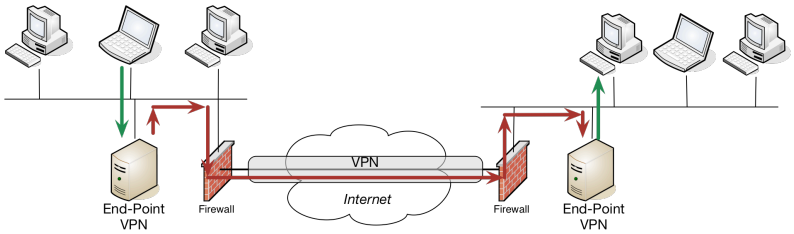
- Un **proxy server** è una componente (hardware o software) che riceve richieste dalla rete interna (tipicamente HTTP/HTTPS), modifica i pacchetti IP impostando come indirizzo IP client il proprio indirizzo esterno, ed inviando il pacchetto a destinazione; la risposta del server viene così ricevuta dal Proxy Server che provvede a girarla al client
- Lo scopo di un proxy server (ad esempio un HTTP proxy) è quello di:
  - rendere accessibile una risorsa esterna anche tramite un client con un indirizzo privato
  - non stabilire una connessione di rete diretta tra client (interno) e server (esterno): la connessione è intermediata dal proxy in modo del tutto trasparente per i due interlocutori
  - rifiutare connessioni verso siti presenti in una *black list* gestita nella configurazione del proxy (es.: siti pornografici, siti di "*fishing*", siti i cui contenuti contravvengono all'etica aziendale, ecc.)
- Un **content filter** è una sorta di proxy che attua le proprie regole di raggiungibilità o irraggiungibilità di un sito, sulla base del contenuto presente nel traffico di rete dall'esterno verso l'interno
  - Anche un sistema antivirus o antispam installato su un mail server, è una sorta di content filter: entra nel merito del contenuto delle mail e stabilisce se trasmetterle o eliminarle dalla coda

Sicurezza perimetrale: VPN – Virtual Private Network

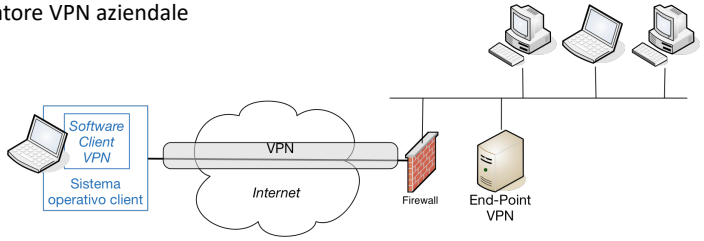
- Una VPN è una **connessione di rete privata** basata su una **infrastruttura di trasporto pubblica** (es.: Internet)
- La VPN è basata su due componenti, gli **end-point della VPN**, che svolgono il ruolo di gateway per il traffico che passa da un nodo all'altro della rete:
  - l'end-point VPN della rete a cui è connessa la sorgente della trasmissione, riceve i pacchetti destinati ad un computer connesso all'altro capo della VPN, li cifra con una chiave nota all'altro end-point e lo inviano
  - l'end-point VPN della rete a cui è connesso l'host di destinazione, riceve il pacchetto cifrato, lo decifra e lo inoltra all'indirizzo di destinazione
  - in questo modo il traffico che passa sulla rete pubblica è cifrato e, se anche venisse intercettato da un attaccante, non sarebbe facile decifrarne il contenuto
- la rete VPN può essere di tre tipi:
  - **VPN site-to-site**: due nodi delle due reti (siti) che devono comunicare in VPN (es.: due filiali della stessa azienda) sono end-point VPN; gli altri nodi della rete utilizzano la VPN in modo trasparente
  - **VPN client-to-site**: uno dei due end-point è un computer client, che deve connettersi alla rete aziendale in modalità sicura; sul client viene installato un software che svolge il ruolo di terminatore VPN
  - **VPN client-to-client**: la VPN viene stabilita via software (con due agent installati sui due computer) tra due computer client

Sicurezza perimetrale: VPN – Virtual Private Network

- **VPN site-to-site** (il terminatore VPN può essere realizzato dal firewall)



- **VPN client-to-site**: il client è connesso ad una rete aziendale o direttamente alla rete pubblica e dispone di un client VPN che si occupa della cifratura del traffico scambiato con il terminatore VPN aziendale



Sicurezza degli end-point

- La protezione delle **postazioni di lavoro** e dei **server**, i cosiddetti "end point" del sistema informativo aziendale, può essere attuata su quattro linee principali:
  - Hardening, aggiornamento continuo con patch
  - Sistemi Antivirus
  - Personal firewall
  - Sistemi Data Loss Prevention

- **Hardening della macchina**
  - Consiste nella applicazione di **configurazioni del software di base** e del software applicativo che riducano il rischio di creare i presupposti per attacchi dall'esterno (es.: disabilitazione di servizi inutili o non utilizzati, impostazione di password non banali, definizione di profili di autorizzazione per gli utenti della macchina che limitino la loro operatività, ecc.)
  - Una componente fondamentale dell'hardening è l'installazione di tutte le **patch di sicurezza** disponibili per il software di base e per il software applicativo; l'impostazione di politiche di aggiornamento automatico continuo del sistema operativo delle postazioni di lavoro è una buona prassi

Sicurezza degli end-point

- **Software Antivirus**
  - È buona norma installare su tutte le postazioni di lavoro un software antivirus
  - Sono programmi che analizzano in tempo reale il contenuto di file e programmi nel momento in cui questi vengono acquisiti dall'esterno (via mail, via trasferimento file dalla rete, mediante memoria di massa removibile, ecc.) e **identificano dei pattern nelle sequenze di byte**, riconducibili a quelle che caratterizzano software infettato da virus: quei programmi vengono eliminati o copiati in un'area del filesystem detta di "quarantena"
  - Gli antivirus **eseguono valutazioni euristiche basate sui pattern** (le "**firme**" dei virus) aggiornati continuamente dai laboratori di ricerca e sviluppo dei produttori dei software antivirus: è buona norma quindi configurare il software antivirus per scaricare quotidianamente gli aggiornamenti delle firme dei nuovi virus scoperti dal produttore dell'antivirus

- **Personal firewall**
  - Come componente del sistema operativo sono spesso presenti dei software che consentono di attuare sul personal computer o sul server delle politiche di accettazione o di rifiuto di connessioni provenienti dalla rete, analoghe a quelle definite sui firewall
  - Questo genere di strumento non può sostituire un firewall vero e proprio perché per riuscire a valutare le richieste di connessione dall'esterno, la macchina deve comunque accettarle: pertanto il personal firewall non è in grado di evitare che la macchina *end-point* venga attaccata, ma può limitare in modo significativo la probabilità che l'attacco abbia successo

Sicurezza degli end-point

- **Sistemi di Data Loss Prevention (DLP)**
  - Sui personal computer, ma anche sui file server, sono presenti molte informazioni anche critiche o riservate, in forma "destrutturata": si tratta di dati importanti contenuti su documenti Microsoft Word, tabelle Microsoft Excel, documenti elettronici in formato PDF o Microsoft Powerpoint, ecc.
  - Tali informazioni non sono gestite mediante un programma che ne limiti l'accessibilità da parte degli utenti sulla base di specifiche autorizzazioni: quei file possono essere facilmente distrutti, stampati, condivisi con altri, anche con chi non ha il permesso di accedere a tali informazioni
  - La riservatezza, l'integrità e la disponibilità delle informazioni presenti sui file prodotti con strumenti di office automation, dipendono dalla consapevolezza dell'utente
  - I sistemi DLP arricchiscono il sistema operativo della macchina di **funzionalità evolute di protezione delle informazioni non strutturate**:
    - permettono di definire e di attuare policy di **cifratura** dei file
    - policy di **protezione** da danneggiamenti
    - policy per la **condivisione** dei file stessi (es.: impediscono la stampa o la condivisione via e-mail di documenti che rispettano un determinato formato o contengono specifici pattern riconducibili ad informazioni riservate, ecc.)

Sicurezza degli end-point

- **End-point threat detection (EDR – End-point Detection and Response)**
  - Mediante programmi «agent» installati sui singoli end-point vengono analizzati parametri di funzionamento interno della macchina (processi attivi, utilizzo della CPU, utilizzo della rete, operatività sui file) al fine di rilevare operazioni potenzialmente anomale o che violano le policy di sicurezza definite centralmente
  - Gli agent sono in grado di intervenire sui processi e le funzionalità di basso livello della macchina per bloccare attività identificate come pericolose (es.: terminazione di processi, interruzione delle comunicazioni in rete, ecc.)
- **Sistemi anti-malware, anti-SPAM e sandbox**
  - Un veicolo di trasporto di programmi *malware* e di azioni di *phishing* è la **posta elettronica**
  - Sui sistemi di posta elettronica (mail server) vengono predisposti **programmi anti-malware**, **anti-spam** in grado di analizzare il contenuto di tutte le mail in entrata e in uscita e di bloccare quelle contenenti allegati potenzialmente dannosi
  - Il blocco di una determinata e-mail viene segnalata all'utente che, nei casi incerti, può prelevare comunque il messaggio e-mail posto in un'area di «**quarantena**»
  - È possibile anche configurare sui mail server dei programmi denominati «**sandbox**» in cui un allegato potenzialmente dannoso può essere ***detonato*** (eseguito) in un ambiente protetto, al fine di valutarne gli effetti

Sicurezza applicativa

- Consiste nell'adottare metodologie e strumenti per rendere sicure le applicazioni informatiche mediante cui gli utenti autorizzati accedono ai dati presenti nel sistema informativo aziendale:
  - **progettazione e sviluppo di software intrinsecamente sicuro** e resistente ad attacchi informatici
  - **adozione di componenti architetturali in grado di offrire servizi di protezione applicativa** ben ingegnerizzati e indipendenti dalla codifica dei programmi (servizi "AAA")

Metodologie di progettazione e sviluppo "sicure"

- Progettazione e sviluppo di software sicuro
  - anche grazie alle contromisure adottate per il controllo degli accessi al sistema informativo e la messa in protezione dei dati, la maggior parte degli attacchi informatici sono indirizzati direttamente verso le applicazioni
  - gli obiettivi degli attacchi sono le vulnerabilità presenti all'interno delle applicazioni software
  - sono state sviluppate numerose metodologie per aumentare il livello di qualità nel processo di progettazione e sviluppo del software, al fine di ridurre non solo la difettosità funzionale dei programmi, ma di curare anche la progettazione di software esente da vulnerabilità intrinseche

Metodologie di progettazione e sviluppo "sicure"

- **Security Development Lifecycle** (SDL): definito da Microsoft per ridurre la vulnerabilità dei propri prodotti

- Si articola su sette fasi principali:
  1. **Training**: formazione dei programmatori sulle tecniche di sviluppo sicuro del software
  2. **Requirements**: definizione dei rischi relativi alla riservatezza dei dati e alla sicurezza
  3. **Design** (progettazione): nella definizione dei requisiti del software devono essere considerati anche i requisiti inerenti la sicurezza; devono essere definiti scenari di attacco al software, in modo da realizzare requisiti che si pongano come contromisure efficaci
  4. **Implementation** (sviluppo): utilizzo di tool di sviluppo verificati e approvati dal responsabile dello sviluppo software, attivare opzioni e utility di warning sulla compilazione del software, effettuare verifiche "statiche" sul codice software prima della sua compilazione
  5. **Verification** (verifica e validazione del software attraverso test e verifiche di piani di attacco): test dinamici anche mediante tool software, test "fuzzy" mediante l'introduzione di input casuale, revisione della "superficie di attacco" del software (l'insieme degli aspetti che possono essere oggetto di un attacco informatico)
  6. **Release** (rilascio): preparare piani di risposta ad incidenti informatici in modo da produrre tempestivamente correzioni e patch, eseguire test finali di sicurezza sulla release software oggetto di rilascio
  7. **Response**: a valle del rilascio del software, attuare piani di risposta alle segnalazioni di incidenti informatici

Metodologie di progettazione e sviluppo "sicure"

- Il modello **CLASP** (*Comprehensive, Lightweight Application Security Process*) fornito dal progetto **OWASP** (*Open Web Application Security Project*) fornisce un approccio strutturato all'integrazione di attività di sicurezza in ogni fase di un ciclo di sviluppo software
- È basato su cinque punti di vista (*view*)
  - Concepts view
  - Role-based view
  - Activity-Assessment View
  - Activity-Implementation View
  - Vulnerability View
- Altre metodologie:
  - Capability Maturity Model Integration (CMMI)
  - Systems Security Engineering – Capability Maturity Model (SSE-CMM)
  - Software Assurance Maturity Model (SAMM)
  - Building Security in Maturity Model (BSIMM)

Metodologie di progettazione e sviluppo "sicure"

- Le minacce a cui è sottoposto un software possono essere classificate secondo il modello **STRIDE** definito da Microsoft:
  - **Spoofing**: attacchi basati sulla falsificazione dell'identità (es.: web spoofing: falsificazione dell'identità di un server web per far credere ad un utente di essere connesso ad un certo server mentre è connesso ad un server malevolo)
  - **Tampering**: l'informazione in transito viene modificata o rimpiazzata prima di raggiungere il destinatario (es.: modifica di un ordine, di un movimento bancario, ecc.)
  - **Repudiation**: ripudio delle informazioni prodotte dal sistema
  - **Information disclosure**: divulgazione di informazioni riservate gestite dall'applicazione
  - **Denial of Service**: il servizio erogato dal software attaccato viene reso indisponibile agli utenti, inviando al software una quantità di richieste tali da saturare la sua capacità di risposta
  - **Elevation of privilege**: incremento dei privilegi dell'utenza con cui viene eseguita una determinata applicazione, al fine di violare l'integrità o la riservatezza dei dati

Crittografia

- È un insieme di algoritmi il cui scopo è quello di rendere incomprensibile il contenuto di un messaggio (un testo) che potrà essere compreso solo decifrandolo attraverso una chiave
- **Crittografia simmetrica**: la chiave per cifrare e decifrare i messaggi è la stessa e deve quindi essere nota sia al mittente che al ricevente del messaggio
  Lo scambio della chiave di cifratura tra il mittente e il destinatario è un momento estremamente critico in un crittosistema simmetrico
- **Crittografia asimmetrica**: ogni utente ha una coppia di chiavi: la **chiave pubblica** e quella **privata**, rilasciate da un'autorità terza di certificazione (***certification authority***)
  Le due chiavi (pubblica/privata) possono essere utilizzate per decifrare un messaggio cifrato con l'altra chiave (es.: messaggio cifrato con la chiave pubblica e decifrato con quella privata)
- In un sistema crittografico asimmetrico gli utenti non devono scambiarsi entrambe le chiavi: solo la chiave pubblica può essere condivisa con altri (anzi, può essere resa pubblica), mentre la chiave privata verrà conservata e mantenuta segreta dall'utente
- Per cifrare un messaggio destinato a Bob, Alice utilizzerà la chiave pubblica di Bob per cifrare il messaggio; in questo modo solo Bob, con la sua chiave privata, potrà decifrarlo

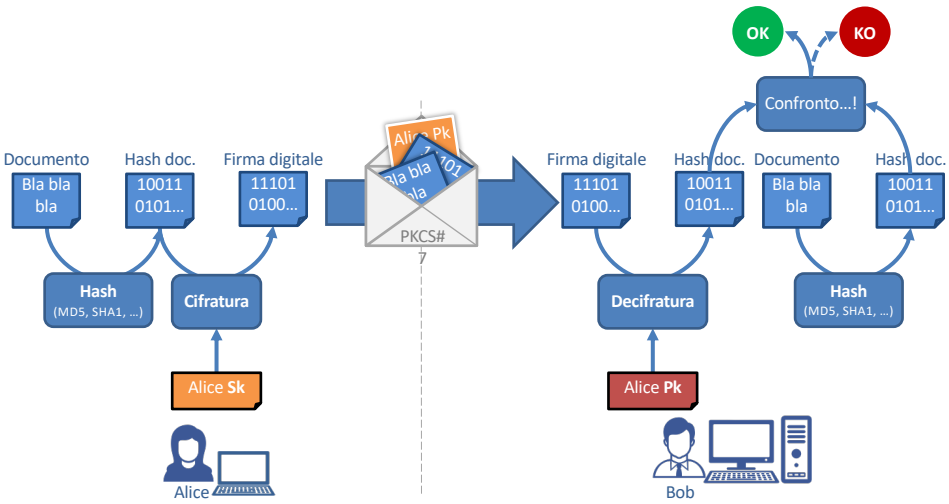
Hash

- Un **hash** (o «**impronta**») di un file è una stringa di caratteri ottenuta dal file originale, applicando un algoritmo di codifica non reversibile
- Gli **algoritmi crittografici di hash** (MD5, SHA1, ecc.) sono progettati per garantire con alta probabilità che due file differenti vengano rimappati su due hash differenti
- In questo modo, sebbene da un certo *hash* non è possibile ricavare direttamente il file da cui è stato prodotto, l'uguaglianza di due file molto lunghi può essere verificata confrontando fra loro i corrispondenti *hash* (prodotti con il medesimo algoritmo)
- Le funzioni *hash* sono molto usate in crittografia e nell'analisi forense, per certificare l'integrità di un documento

Firma digitale: gli obiettivi

- La firma digitale (firma elettronica qualificata, nel nostro ordinamento) è uno strumento ormai molto diffuso per la semplificazione dei procedimenti amministrativi nella PA e nelle relazioni tra la PA e i cittadini e le imprese (*a Roma Tre la usiamo anche per firmare i verbali d'esame!*)
- È uno strumento formidabile per soddisfare le seguenti esigenze:
  - **Autenticazione**: è possibile verificare/certificare l'identità del mittente
  - **Integrità**: è possibile verificare che il documento non sia stato alterato dopo la firma
  - **Non ripudio**: il mittente (il firmatario) non può disconoscere il documento

Firma digitale: un'applicazione della crittografia



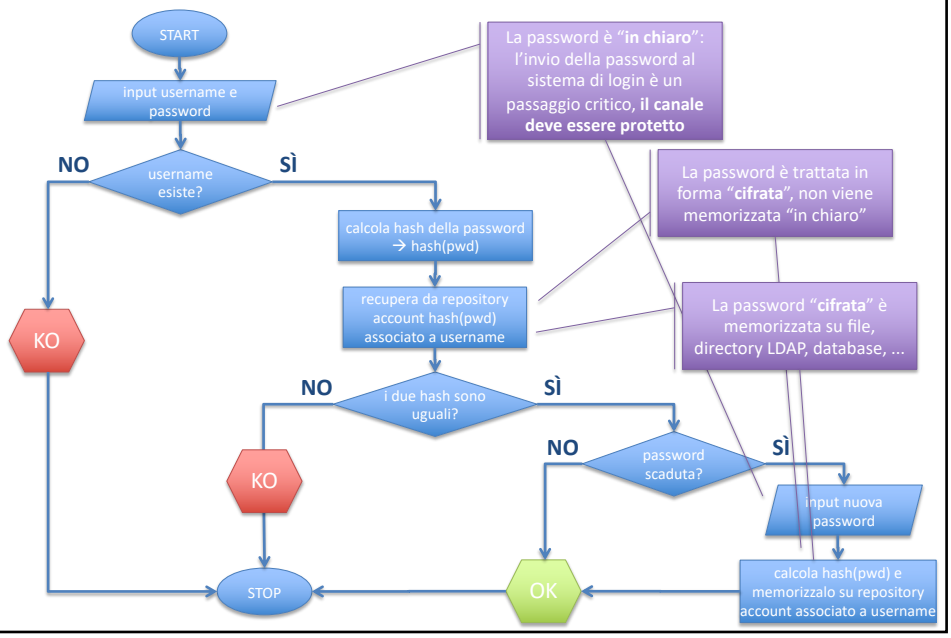
Sistemi AAA: *authentication, authorization, accounting*

- Sul sistema informativo vengono introdotte delle componenti infrastrutturali che offrono servizi di autenticazione, autorizzazione e *accounting* degli utenti delle applicazioni
  - **Autenticazione**: meccanismi per accertare l'identità dell'utente (o per "autenticare" la dichiarazione di identità fatta dall'utente)
  - **Autorizzazione**: meccanismi di verifica e attuazione delle regole di autorizzazione assegnate ad un utente per l'esecuzione di una determinata funzionalità applicativa o per l'accesso ad un dato o tipo di dato
  - **Accounting**: meccanismi di responsabilizzazione dell'utente, anche attraverso il tracciamento delle operazioni svolte sui dati mediante le applicazioni o gli altri strumenti resi disponibili sul sistema informativo
- Se offerte come servizio, le funzioni devono solo essere richiamate dalle applicazioni, attraverso appositi protocolli o funzioni di libreria:
  - in questo modo si **semplifica lo sviluppo del software**: non devono essere progettate e implementate le funzioni di autenticazione, autorizzazione e accounting in tutte le applicazioni
  - si garantisce **maggiore sicurezza**: le funzioni sono sviluppate una volta per tutte (o sono basate su un prodotto di mercato) e integrate con le applicazioni e i sistemi; non si corre il rischio che le stesse funzioni possano essere implementate in maniera differente da un'applicazione all'altra
  - si garantisce **maggiore flessibilità**: la sostituzione di una funzione di tipo AAA con un'altra può essere fatta centralmente, senza dover modificare ogni applicazione

Autenticazione

- L'autenticazione di un utente nei confronti di un'applicazione (o di un'applicazione nei confronti di un'altra applicazione) si basa su una delle seguenti informazioni:
  - **qualcosa che si conosce**: ad esempio una password o un PIN;
  - **qualcosa che si possiede**: ad esempio un badge, una chiave, un token;
  - **qualcosa che si è**: ad esempio l'impronta digitale, il modello della retina dell'occhio, ecc.
- La fase di **login** su un'applicazione o su un sistema informatico è quella in cui l'utente dichiara la propria identità (ad esempio attraverso uno *username* univoco) e l'applicazione o il sistema lo autenticano attraverso la verifica di una *password* segreta (nota solo all'utente) inserita contestualmente dall'utente
- Da quel momento in poi viene aperta una **sessione di lavoro** entro cui l'utente può operare sull'applicazione o sul sistema senza doversi autenticare nuovamente
- Più sistemi possono stabilire relazioni di fiducia tra di loro per consentire ad un utente di autenticarsi su un sistema senza poi doversi autenticare nuovamente anche sugli altri (anche se gli account sono diversi): ***single sign-on***

Autenticazione



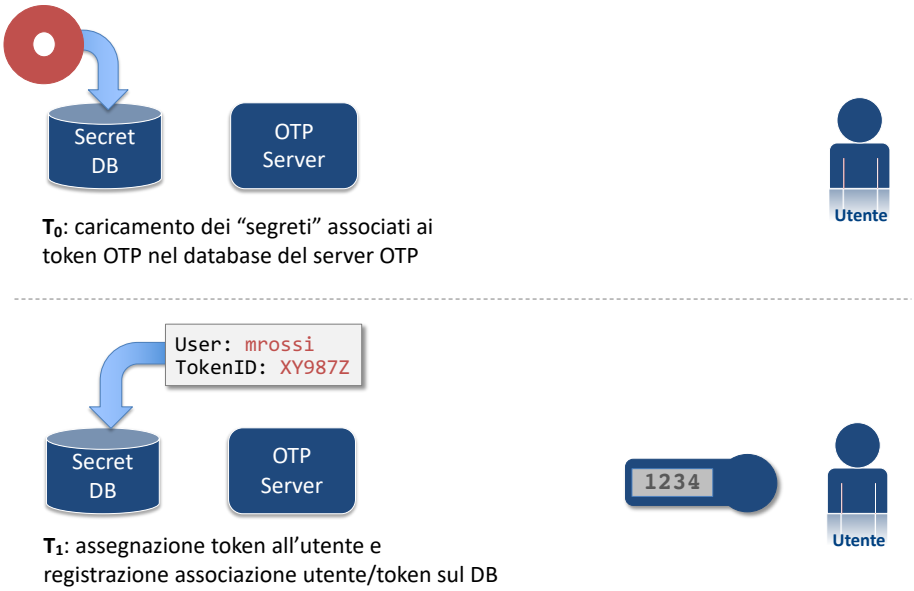
Autenticazione forte

- Si parla di **autenticazione forte** (*strong authentication*) quando il meccanismo di autenticazione è basato su due dei tre fattori
  - es.: per autenticare l'utente che dichiara la propria identità attraverso uno username, si fornisce una password e un codice generato da un token assegnato all'utente stesso
- **Autenticazione forte con certificati digitali**
  - L'utente è dotato di una *smart-card* con a bordo una coppia di chiavi crittografiche; il server di autenticazione possiede la chiave pubblica dell'utente
  - Il passo critico è la generazione delle chiavi crittografiche e l'assegnazione agli utenti: questa fase deve essere protetta e gestita con un processo ben definito e verificato
  - Algoritmo "*challenge/response*":
    1. il server genera un codice e lo sottopone all'utente che ne produce una cifratura asimmetrica con la propria chiave privata
    2. Se il server riesce a portare in chiaro il codice utilizzando la chiave pubblica dell'utente, allora avrà compiuto la sua autenticazione: solo con la chiave pubblica dell'utente si può riportare in chiaro il codice cifrato con la sua chiave privata; il codice è noto al server che può quindi verificarne l'uguaglianza con quello generato al passo precedente

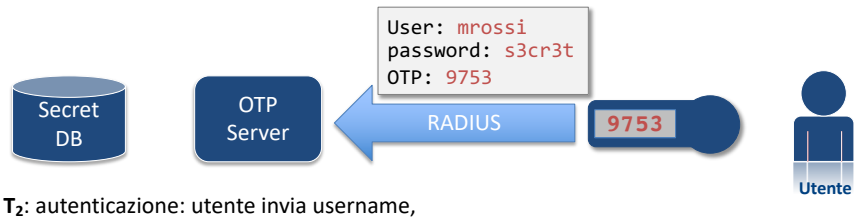
Autenticazione forte

- **Autenticazione forte con OTP** (*one time password*)
  - Un algoritmo genera in tempo reale una password che **può essere utilizzata dall'utente una sola volta**: anche se intercettata da un attaccante la password non sarà più utile per autenticarsi a nome di un altro utente
- Tre tipi di algoritmi principali per la generazione di OTP:
  - Algoritmi basati sulla **sincronizzazione temporale** tra server OTP e client che fornisce la password (le OTP sono valide solo per un breve periodo di tempo, es.: 30")
  - Algoritmi basati su una **catena di password** legate tra loro e generate per via algoritmica, in base anche ad un "seme" associato al client OTP assegnato all'utente: il server e il client generano una nuova password in base alla password precedente
  - Algoritmi di tipo **challenge/response**: il server genera un numero casuale e lo invia al client che restituirà un codice basato su quel numero casuale e sul "seme" associato al client OTP dell'utente

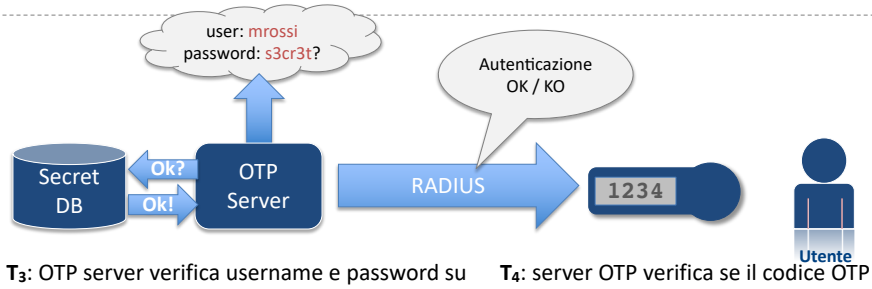
Autenticazione forte con OTP



Autenticazione forte con OTP



T_2: autenticazione: utente invia username, password e OTP generata dal token sul momento



T_3: OTP server verifica username e password su un sistema di autenticazione (anche esterno)

T_4: server OTP verifica se il codice OTP può essere generato dal token XY987Z assegnato all'utente mrossi

Autorizzazione

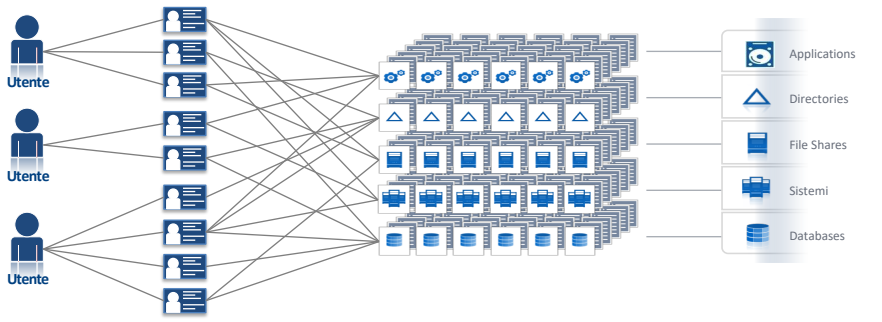
- Le applicazioni, i sistemi applicativi, i sistemi operativi sono strumenti attraverso cui l'utente (o un altro programma) può accedere alle informazioni e gestirle eseguendo delle operazioni di lettura, scrittura, modifica e cancellazione
- A garanzia della sicurezza delle informazioni (riservatezza, integrità e disponibilità), i sistemi applicativi implementano meccanismi di **autorizzazione** degli utenti per l'accesso ai dati attraverso le funzionalità messe a disposizione dal sistema stesso
- Partendo dal presupposto che l'utente non può in alcun modo operare sui dati gestiti dall'applicazione, **un'autorizzazione è il permesso di compiere una determinata operazione** su un certo tipo di dato (es.: inserire una fattura, visualizzare un certificato medico, approvare una richiesta di acquisto, ecc.)
- I sistemi prevedono anche **autorizzazioni necessarie per assegnare o revocare autorizzazioni**: generalmente l'amministratore del sistema è autorizzato a priori a gestire le autorizzazioni degli altri utenti
- L'applicazione delle autorizzazioni permette di implementare un meccanismo di **controllo degli accessi** ai dati:
  - l'utente **chiede di eseguire** una determinata operazione su un dato
  - il sistema **verifica se l'utente è autorizzato** a compiere tale operazione su quel dato
  - il sistema **concede o impedisce l'accesso al dato**: controllo degli accessi
- Per poter **autorizzare** un utente, questo dovrà essere stato **precedentemente autenticato**

Autorizzazione

- Per garantire una corretta politica di autorizzazione degli utenti è opportuno definire un insieme di **ruoli applicativi** che sia possibile attribuire agli utenti
- Ciascun ruolo prevede un **insieme di autorizzazioni** che saranno così attribuite a tutti gli utenti a cui verrà assegnato un determinato ruolo
- Si costruisce un **profilo dell'utente** del sistema informativo basato sui ruoli (e quindi sulle autorizzazioni) che si assegnano all'utente
- Assegnare o rimuovere un ruolo ad un utente significa assegnare o rimuovere un insieme di autorizzazioni allo stesso utente
- In un'organizzazione ben strutturata i *ruoli applicativi* dovrebbero corrispondere ai *ruoli di business* degli utenti
  - Es.: per un'applicazione gestionale in un contesto scolastico o universitario, i profili autorizzativi possono essere costruiti sui ruoli di docente, studente, bibliotecario, ecc.
  - In questo modo un cambio di ruolo nell'organizzazione, porterebbe ad una facile identificazione del nuovo profilo autorizzativo da attribuire all'utente
- **RBAC**: ***role based access control***, è una politica di controllo degli accessi alle informazioni basata sui ruoli assegnati agli utenti

Governance della sicurezza del sistema informativo aziendale

- In un sistema informativo complesso l'implementazione di sistemi AAA porta ad un contesto difficile da gestire

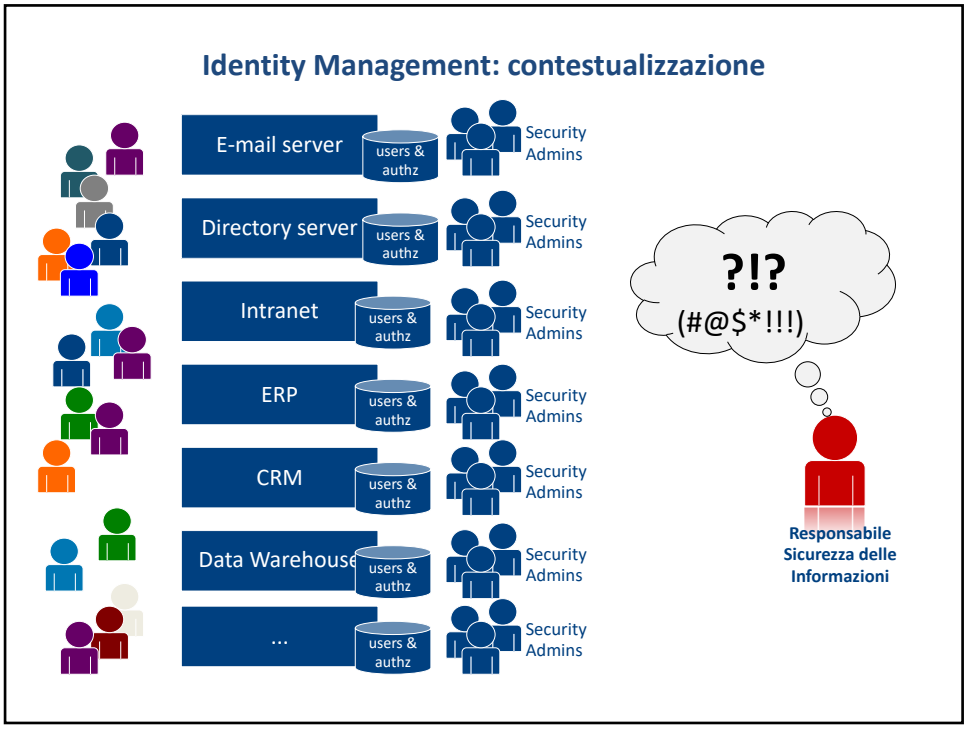


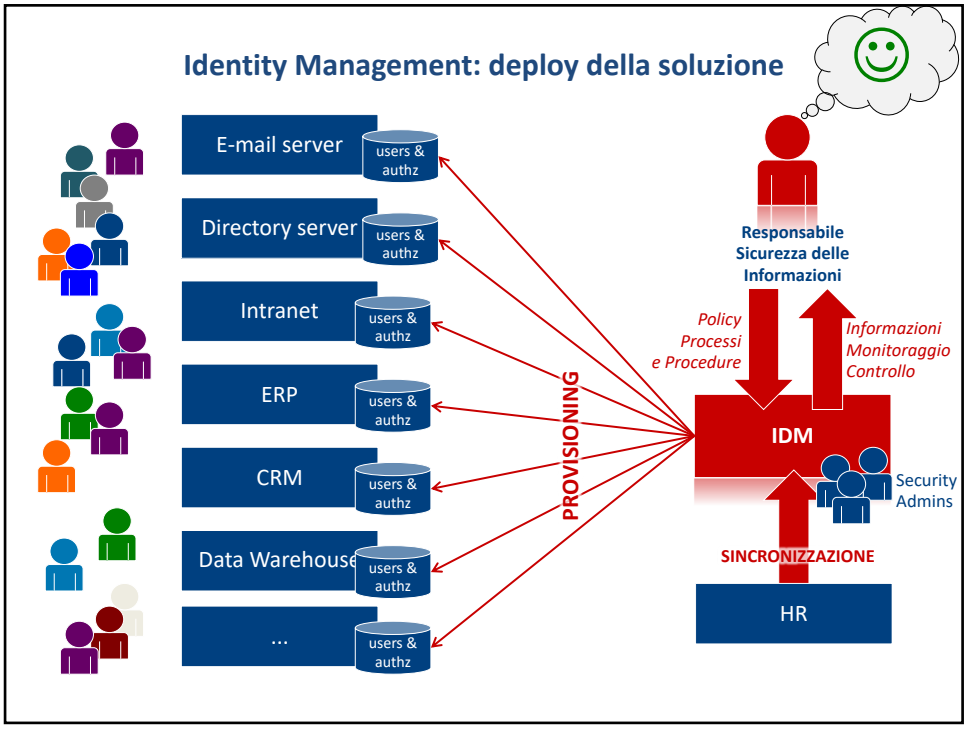
Governance della sicurezza del sistema informativo aziendale

- In particolare diventa complicato attuare una vera ***governance* della sicurezza informatica**
  - definizione e attuazione di **politiche per la sicurezza**
  - definizione e attuazione di **processi gestionali controllati**
  - **raccolta tempestiva di informazioni e dati** per poter controllare e misurare il servizio
  - controllo e misura di eventuali **scostamenti dai requisiti** dettati da normative e regolamenti (***compliance***)
- Alcune domande a cui il responsabile della sicurezza delle informazioni è tenuto a rispondere:
  - A quali informazioni ha accesso Mr X?
  - Chi ha accesso alle informazioni presenti nell'archivio Y?
  - Chi ha autorizzato Mr X ad accedere all'archivio Y?
  - Siamo sicuri che gli utenti del nostro sistema informativo abbiano solo le autorizzazioni necessarie per lo svolgimento del loro lavoro?
  - Siamo sicuri che le autorizzazioni assegnate agli utenti del sistema informativo rispettino le linee guida sulla sicurezza interne e le normative vigenti?
  - Qual è il processo con cui vengono assegnate credenziali ed autorizzazioni ai nuovi dipendenti dell'azienda? E per i consulenti esterni? E per i fornitori? Per i partner con cui condividiamo alcune informazioni o servizi?
  - Qual è il processo con cui vengono modificate le autorizzazioni degli utenti che cambiano sede o ruolo aziendale? E quando cessano la collaborazione con l'azienda cosa succede?
  - Quanto tempo viene impegnato oggi nella gestione del ciclo di vita delle credenziali e delle autorizzazioni assegnate agli utenti?
  - Abbiamo definito criteri di assegnazione delle autorizzazioni basate sulla funzione aziendale degli utenti?
  - Viene posta maggiore attenzione nella assegnazione di autorizzazioni riguardanti le risorse più critiche del sistema informativo aziendale? Quali sono le risorse più critiche?

Governance della sicurezza del sistema informativo aziendale

- Per consentire una effettiva attività di ***governance* della sicurezza** del sistema informativo aziendale è necessario
  - definire delle ***policy***, dei **processi organizzativi** e dei **controlli**
  - **predisporre dei sistemi IT integrati** in grado di automatizzare e guidare gli amministratori e gli utenti nella applicazione delle policy, riducendo possibilità di errore e violazioni delle politiche e delle normative esistenti
- Alcuni dei principali **sistemi di supporto alla *governance* della sicurezza** del sistema informativo:
  - **sistemi di Risk Assessment, Risk Analysis, Risk Management**: supporto all'analisi e alla gestione dei rischi a cui è soggetto il sistema informativo aziendale
  - **sistemi di Identity Management, Identity Governance**: supporto alla gestione del ciclo di vita delle credenziali e delle autorizzazioni assegnate agli utenti del sistema informativo aziendale
  - **sistemi di Access Management, Identity Federation**: centralizzazione dei servizi di autenticazione e autorizzazione, anche su base "federata", ossia estendendo il perimetro del servizio ad altre organizzazioni con cui l'azienda ha stabilito degli accordi di collaborazione (e di fiducia)
  - **sistemi SIEM (*Security Information Event Management*)**: supporto alla raccolta, correlazione e analisi dei log provenienti dalle diverse componenti del sistema informativo aziendale


Identity Management: contestualizzazione
E-mail server
Directory server
Intranet
ERP
CRM
Data Warehouse
...
users & authz
Security Admins
?!?
(#@$*!!!)
Responsabile Sicurezza delle Informazioni


Identity Management: deploy della soluzione
E-mail server
Directory server
Intranet
ERP
CRM
Data Warehouse
...
users & authz
PROVISIONING
Responsabile Sicurezza delle Informazioni
Policy Processi e Procedure
Informazioni Monitoraggio Controllo
IDM
Security Admins
SINCRONIZZAZIONE
HR

Identity Management: caratteristiche principali

- È una componente di sicurezza logica che consente di **gestire centralmente le identità digitali** delle persone abilitate ad utilizzare il sistema informativo aziendale
- Raccoglie in un database unificato tutte le informazioni relative all'identificazione dell'utente sul sistema stesso e su tutte le piattaforme integrate con IDM (***virtual identity*** degli utenti)
  - Conosce il nominativo ed altri dati "anagrafici" per ciascuna persona abilitata ad utilizzare il sistema informativo aziendale
  - Conosce gli account con cui ciascun utente si autentica ed accede sui vari sistemi
- Raccoglie alcune delle informazioni relative alla **struttura organizzativa aziendale**
  - Conosce la collocazione di ogni persona nella struttura organizzativa, al fine di stabilire chi è autorizzato ed è responsabile dell'assegnazione di credenziali e privilegi di accesso ad ogni utente
- Raccoglie le informazioni relative alle **piattaforme informatiche** che compongono il sistema informativo e su cui gli utenti dovranno accedere
  - Conosce le informazioni con cui ogni utente viene identificato su ciascuna piattaforma (più account utente per ogni persona, un account per ciascuna piattaforma)
  - Es.: IBM RACF, Microsoft Active Directory, Lotus Notes, ecc.

Identity Management: caratteristiche principali

- Cosa conosce IDM:
  - Conosce le anagrafiche degli utenti per identificarli univocamente
  - Conosce le piattaforme informatiche presenti nel sistema informativo (Microsoft Windows/AD, Lotus Notes, OS/390-RACF, ecc.)
  - Conosce la struttura organizzativa aziendale (sedi, direzioni, aree, ruoli macroscopici degli utenti)
- Cosa fa IDM:
  - Assegna gli account di accesso per le piattaforme agli utenti
  - Esegue il provisioning/de-provisioning degli account di accesso verso le piattaforme target
  - Acquisisce le anagrafiche degli utenti dal sistema di gestione delle risorse umane
  - Consente una amministrazione delegata basata sulla struttura organizzativa aziendale
- Cosa non fa IDM:
  - Non sostituisce l'anagrafe del personale
    - al contrario: acquisisce i dati dall'anagrafe del personale
  - Non sostituisce il sistema di gestione della struttura organizzativa aziendale
    - al contrario: recepisce la struttura organizzativa nella configurazione e la utilizza come griglia entro cui delegare le attività di gestione
  - Non gestisce l'autenticazione e gli accessi degli utenti ai sistemi informatici
    - al contrario, li controlla: mediante IDM si assegnano, si sospendono e si revocano le credenziali per l'accesso ai sistemi

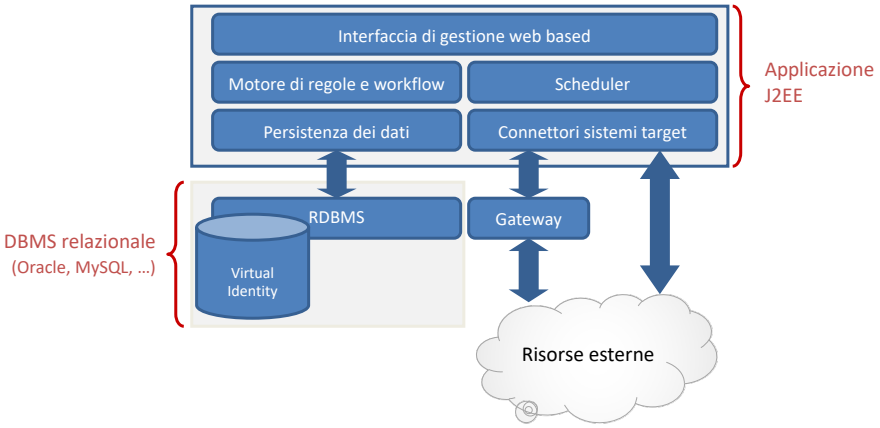
Identity Management: Riconciliazione e Provisioning

- **Riconciliazione** e **Provisioning** sono funzionalità proprie delle piattaforme di Identity Management (IDM)
- **Riconciliazione** e **Sincronizzazione** con altri sistemi
  - È l'operazione che consente di **caricare da sistemi preesistenti le credenziali degli utenti** nel database di IDM (per completare/aggiornare le *virtual identity* degli utenti)
  - Avviene una volta all'inizializzazione del sistema IDM per le piattaforme che dovranno essere alimentate dal sistema stesso (*piattaforme target*)
  - Avviene con continuità per le piattaforme che alimentano la base informativa del sistema IDM e che "innescano" il processo di gestione dell'utente (i sistemi di gestione delle risorse umane e della struttura organizzativa – le cosiddette *trusted sources*)
- **Provisioning** verso le piattaforme target
  - È l'operazione di **trasmissione delle credenziali** utente e delle informazioni identificative dal sistema IDM verso le piattaforme target su cui l'utente dovrà accedere ed essere autenticato per poter operare
  - Avviene ogni qual volta sono modificati i suoi dati sulla piattaforma IDM
  - È soggetta all'**approvazione** dei soggetti preposti a gestire l'ambito delle attività dell'utente (il direttore o il dirigente) e dei soggetti preposti alla gestione delle piattaforme informatiche

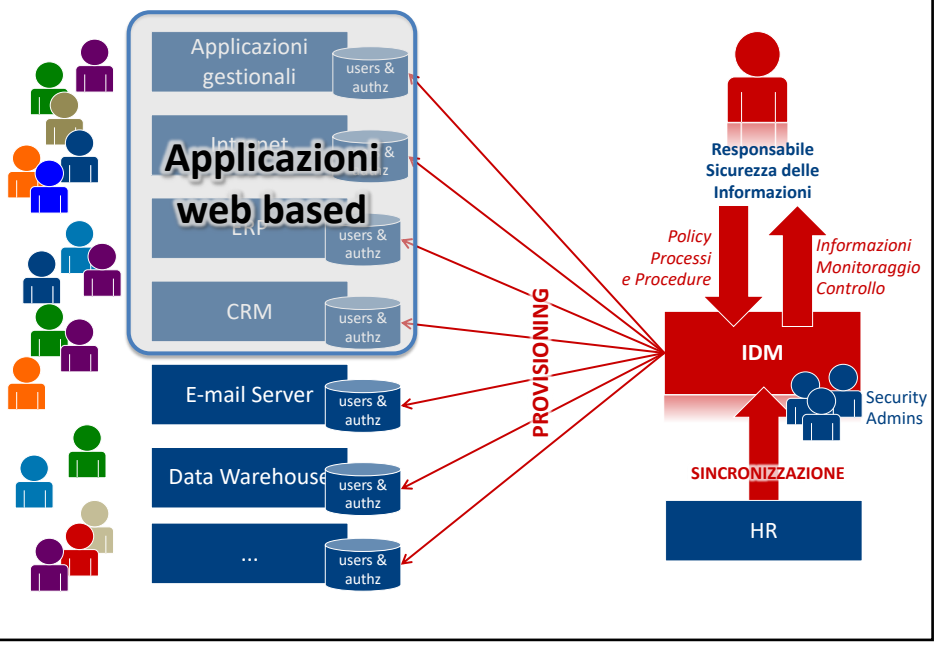
Identity Management: principali benefici

- **Sincronizzazione con una o più *trusted sources*** per automatizzare e rendere tempestivo l'innesco di variazioni nel ciclo di vita delle *virtual identity*:
  - nuovi utenti, spostamenti o modifiche delle funzioni aziendali, conclusioni di rapporti di collaborazione
- **Provisioning verso sistemi target** di autenticazione e autorizzazione degli utenti
  - automazione del processo di creazione, cancellazione e modifica di credenziali di accesso e di autorizzazioni legate alle credenziali
- **Principali benefici**:
  - Attuazione di alcune policy di sicurezza sulle credenziali e sulle autorizzazioni degli utenti (*naming convention*, *password policy*, scadenza delle password, scadenza automatica degli account di accesso, ecc.)
  - Monitoraggio del processo di gestione delle credenziali e delle autorizzazioni (*audit log* delle operazioni compiute sulle credenziali e sulle autorizzazioni assegnate agli utenti)
  - Semplificazione del processo di gestione: il personale tecnico addetto alla gestione delle credenziali e delle autorizzazioni ha uno strumento unificato, *web based*, per effettuare le operazioni di gestione; non è richiesta la conoscenza di comandi o procedure su sistemi operativi o applicativi specifici

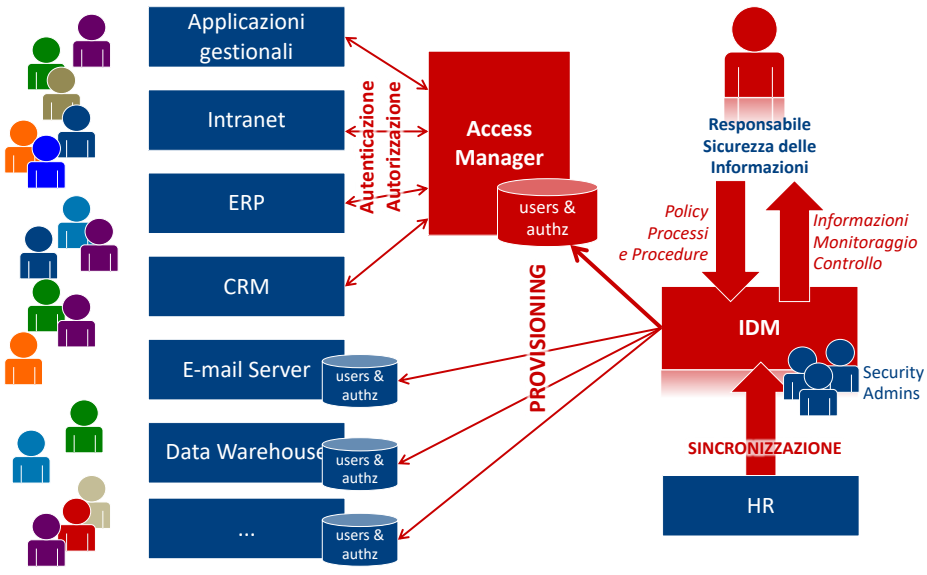
Identity Management: una vista semplificata sull'architettura



Access Management: contestualizzazione



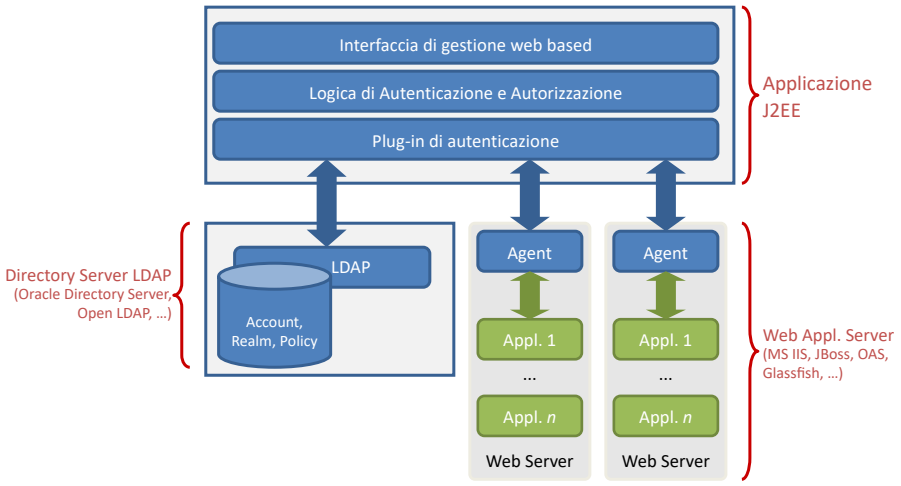
Access Management: deploy della soluzione



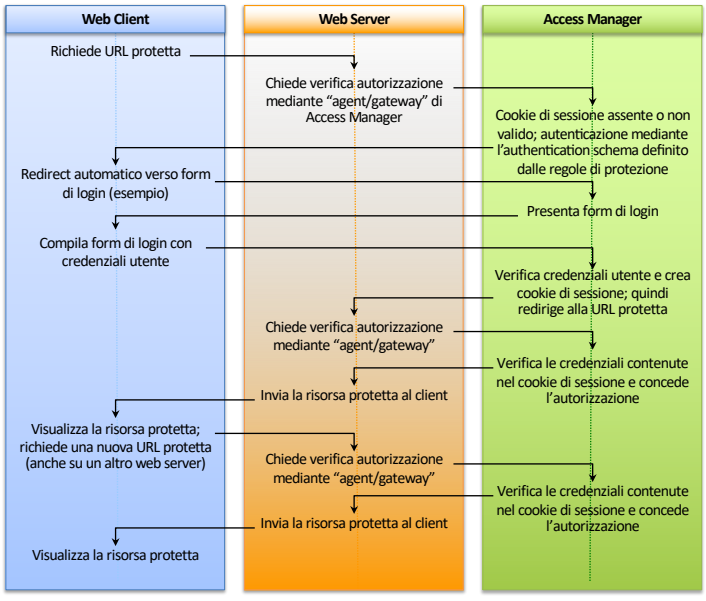
Access Management: caratteristiche principali

- È una componente infrastrutturale di servizio per il consolidamento della sicurezza informatica per le applicazioni web based
- Offre **servizi di autenticazione**, sollevando l'applicazione da tali problematiche e separando in modo netto la logica applicativa di business da quella di autenticazione
  - Autenticazione "password based"
  - Autenticazione "forte" con certificati digitali X.509 o dispositivi OTP
  - Autenticazione "Kerberos" integrata con il dominio Active Directory
  - …
- Offre **servizi di autorizzazione/profilazione**, per l'identificazione dell'utente e per il *single sign-on* che possono essere sfruttati dalle applicazioni
- Offre la possibilità di raccogliere in un log centralizzato le informazioni relative agli accessi (riusciti o falliti) degli utenti sulle applicazioni
- Si integra in modo naturale con i sistemi di **Identity Management** a cui delega la funzione di gestione del ciclo di vita delle credenziali e delle autorizzazioni

Access Management: una vista semplificata sull'architettura

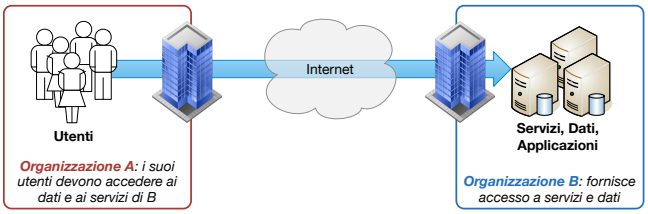


Access Management: processo di autenticazione e autorizzazione



Identity Federation: contestualizzazione

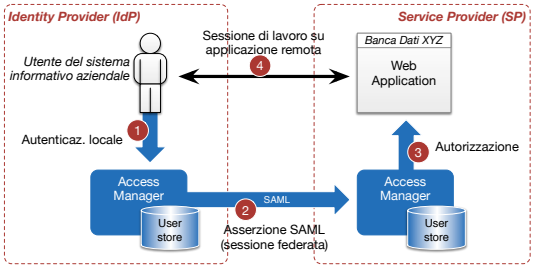
- Tra organizzazioni aziendali distinte spesso intercorrono **rapporti di collaborazione** (es.: due enti pubblici che collaborano su determinati temi, due aziende che operano in modalità di partnership, un'azienda e i suoi fornitori, ecc.) tali da rendere necessario l'**accesso di utenti di uno dei due partner su alcune applicazioni del sistema informativo dell'altro partner**
- In tali casi l'accesso sicuro viene garantito tipicamente assegnando agli utenti dell'organizzazione *A* (fruitore delle informazioni) utenze e autorizzazioni per l'accesso al sistema informativo dell'organizzazione *B* (fornitore di informazioni o servizi)



- La gestione del ciclo di vita delle utenze assegnate da *B* ad *A* è piuttosto difficile per l'organizzazione *B*, perché non ha il pieno controllo sui membri dell'organizzazione *A*

Identity Federation: deploy della soluzione

- Viene definito il ruolo delle due organizzazioni:
  - **Identity Provider (IdP)**: è l'organizzazione che conosce e autentica l'identità degli utenti (A nell'esempio)
  - **Service Provider (SP)**: è l'organizzazione che fornisce servizi applicativi e informativi
- **Identity Federation**: permette di costruire una sorta di "contesto di single sign-on" che mette in comunicazione l'Access Manager di **IdP** con l'Access Manager di **SP**
- Il protocollo **SAML** (*Security Assertion Markup Language*) permette di inviare dei messaggi da **IdP** ad **SP** per aprire una sessione di lavoro federata degli utenti di **IdP** sui sistemi di **SP**:
  1. Access Manager di **IdP** autentica l'utente che conosce (appartiene alla propria organizzazione)
  2. Access Manager di **IdP** invia un'asserzione SAML ad Access Manager di **SP**
  3. Access Manager di **SP** apre una sessione di lavoro, come se l'utente si fosse autenticato sul sistema di **SP**, e lo autorizza ad operare con un determinato profilo sul sistema di **SP**
  4. L'utente di **IdP** accede al sistema di **SP** in modalità sicura e non anonima



SPID: Sistema Pubblico di Identificazione Digitale

- Con il Decreto del Presidente del Consiglio dei Ministri del 24 Ottobre 2014 è stato istituito in Italia il **Sistema Pubblico per la gestione dell'Identità Digitale dei cittadini**
- È un sistema informatico, supportato da una norma di legge, che consente alle Pubbliche Amministrazioni di offrire servizi on-line ai cittadini, utilizzando il sistema SPID come contesto di **identificazione** e di **qualificazione** degli utenti a cui offrire servizi digitali
- SPID opera come un sistema di Identity Federation tra le pubbliche amministrazioni centrali e locali italiane

- Nell'ambito dell'architettura di SPID vengono definiti tre soggetti:
  - **Identity Provider (IdP)**: come nei sistemi di Identity Federation è l'ente pubblico che rilascia al cittadino le credenziali di autenticazione e ne gestisce il ciclo di vita, garantendo le altre pubbliche amministrazioni sull'identità del cittadino associato a tali credenziali digitali
    - Es.: potrebbe essere l'Agenzia delle Entrate che oggi rilascia a tutti i cittadini un Codice Fiscale e una Tessera Sanitaria, oppure il Comune di residenza, che oggi rilascia la Carta d'Identità
  - **Attribute Provider (AP)**: sono gli enti che istituzionalmente possono certificare il possesso di determinati ruoli o requisiti da parte del cittadino dotato di credenziali da un IdP
    - Es.: potrebbe essere la Camera di Commercio che certifica che il sig. Rossi è il legale rappresentante di una certa azienda, o l'Ordine degli Ingegneri, che certifica che il sig. Rossi è un ingegnere iscritto all'Albo
  - **Service Provider (SP)**: sono gli enti che erogano servizi on-line, basandosi sull'identità del cittadino certificata dal IdP e dal ruolo dello stesso cittadino certificato dal AP
    - Es.: potrebbe essere l'INPS che fornisce il servizio di pagamento dei contributi di "maternità" per un dipendente della ditta del sig. Rossi che ne fa domanda on-line

Accounting

- Per responsabilizzare gli utenti nell'uso delle credenziali e delle autorizzazioni che sono state loro assegnate, è necessario tracciare le operazioni svolte dagli utenti tramite le funzioni rese disponibili dai sistemi applicativi
- I sistemi producono delle indicazioni sintetiche sulla sequenza di operazioni svolte nel tempo: tali informazioni vengono chiamati **log**
- I log sono memorizzati su file o su appositi sistemi di raccolta dei log; esistono protocolli (es.: **syslog**) e librerie software (es.: **log4j**) che consentono di semplificare la scrittura di log e di inviare i log prodotti da un sistema verso un sistema di raccolta
- Esistono vari tipi di log:
  - **log di sistema**: informano sullo stato di funzionamento di un sistema e tracciano gli errori avvenuto nel corso del funzionamento del sistema stesso
  - **log applicativi**: informano sullo stato di funzionamento di un programma e sulle operazioni svolte sui dati
  - **log di database**: informano sulle operazioni svolte sui dati; sono utili anche per ripristinare lo stato del database ad un punto precedente all'esecuzione di determinate operazioni di modifica dei dati
  - **log di audit**: informano sulle operazioni svolte dagli utenti mediante un sistema o un'applicazione

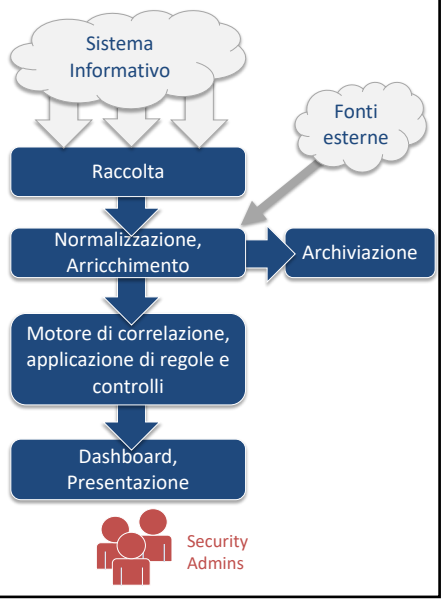
SIEM: Security Information and Event Management

- Le componenti del sistema informativo aziendale producono enormi quantità di dati di log, che dovrebbero essere tenuti sotto controllo dai sistemisti, al fine di rilevare o prevenire malfunzionamenti del sistema
- Spesso i log forniscono anche informazioni o descrizione di eventi che riguardano la sicurezza del sistema informativo o che costituiscono degli indizi di un tentativo di attacco informatico o di un comportamento scorretto da parte di un utente del sistema stesso
- I sistemi **SIEM** consentono di
  - **aggregare** in un unico punto i log provenienti da numerose fonti eterogenee, offrendo così ai sistemisti e agli operatori responsabili della sicurezza uno strumento unico da cui osservare il comportamento di sistemi diversi
  - **correlare** fra loro informazioni provenienti da sistemi diversi o prodotte in tempi diversi da uno stesso sistema: spesso un evento in sé è poco significativo, ma acquista maggiore rilevanza se correlato con altri eventi avvenuto contemporaneamente o a breve distanza di tempo
  - **analizzare** i log sulla base di regole, in modo da portare all'attenzione dell'operatore un numero limitato di eventi o segnalazioni
  - **archiviare** nel tempo in modo sicuro i log, anche per poterli utilizzare come prova in caso di indagini e procedure legali

SIEM: sintesi dell'architettura

Il sistema SIEM è costituito da diverse componenti collegate fra loro

- **Raccolta**: componente per l'acquisizione dei log dai sistemi sorgente
- **Analisi**, normalizzazione: verifica la singola riga di log e la riscrive in un formato standard normalizzato rispetto alla diversità delle sorgenti
- **Archiviazione**: il log in formato originale (*raw*) e normalizzato viene archiviato su uno storage di grandi dimensioni (può essere anche protetto mediante la costruzione di una catena di *hash*)
- **Correlazione e controlli**: i log vengono correlati fra loro e vengono applicati dei controlli per identificare eventi rilevanti per la sicurezza
- **Dashboard**: le informazioni vengono presentate in modalità efficace al personale del **SOC** (*Security Operation Center*)



UEBA: User and Entity Behavior Analytics

- L'analisi del «**comportamento**» degli utenti e delle componenti informatiche (entità) dei sistemi informativi consente di rilevare anomalie che possono essere un indizio di un'attività malevola in corso
- I sistemi UEBA, spesso definiti come estensione dei SIEM, analizzano i comportamenti degli utenti e dei sistemi attraverso l'analisi dei log
- I sistemi UEBA operano sulla base di due fasi distinte, utilizzando algoritmi di *machine learning* per il *clustering* e la classificazione degli utenti sulla base dei loro comportamenti tipici
  1. **Fase di apprendimento**: il sistema acquisisce informazioni circa il comportamento degli utenti ed esegue il partizionamento dell'insieme degli utenti sulla base dei loro ruoli aziendali (acquisiti dai sistemi HR e IAM) e dei loro comportamenti standard
  2. **Fase di rilevazione delle anomalie**: il sistema rileva variazioni significative rispetto ai comportamenti standard degli utenti e segnala, attraverso degli allarmi, tali anomalie al servizio SOC
- Il comportamento dei sistemi (entità) viene rilevato oltre che dai log anche dallo stato interno del sistema (carico della CPU, RAM, operazioni di scrittura su disco, ecc.) e dal traffico di rete originato da tale componente

Threat Intelligence

- Un'attività preventiva nell'ambito della sicurezza informatica è quella di eseguire operazioni di ***threat intelligence*** (indagine sulle minacce), acquisendo tempestivamente informazioni relative a nuove **minacce** di tipo informatico che potrebbero impattare sulle componenti del sistema informativo aziendale
- L'indagine avviene prevalentemente attraverso l'osservazione delle attività e delle discussioni nell'ambito di gruppi di *hacker*, presenti sulla rete Internet su forum e altri sistemi di condivisione e scambio di informazioni tipicamente non facilmente rintracciabili tramite comuni motori di ricerca (*dark web*)
- I **CERT** (*Computer Emergency Response Team*) redigono dei report sulla base delle informazioni raccolte circa le nuove minacce e le vulnerabilità rilevate su prodotti diffusi nel mercato IT (es.: CERT-PA, CERT-FIN, IT-CERT, PICERT, ecc.)
- I report dei CERT vengono diffusi attraverso appositi *feed* di sicurezza che possono essere anche integrati sui sistemi SIEM delle organizzazioni aziendali
- I CERT rilevano anche specifiche «prove» per identificare un incidente informatico, costituite da firme di virus, hash MD5 che identificano un file malevolo, indirizzi IP, ecc. Tali evidenze prendono il nome di **IOC** (*indicator of compromise* / indicatori di compromissione)

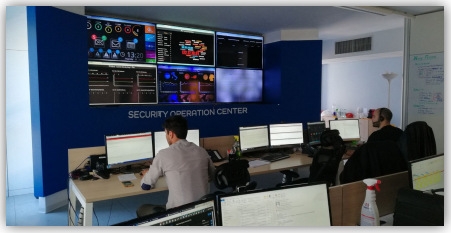
Threat Intelligence

Vulnerability Assessment e Penetration Test

- È buona norma verificare periodicamente lo stato di configurazione dei sistemi, degli apparati di rete e delle applicazioni, anche sulla base di nuove vulnerabilità rilevate mediante i *feed di sicurezza* pubblicati dai servizi CERT (pubblici, open source o commerciali)
- È buona norma definire delle politiche di configurazione e di *hardening* dei sistemi: l'introduzione nel sistema informativo aziendale di un nuovo apparato server o client deve avvenire solo a valle della corretta configurazione (anche dal punto di vista della sicurezza informatica) dell'apparato stesso; la corretta configurazione viene definita mediante linee guida e politiche di configurazione
- La verifica dell'esistenza di vulnerabilità sulle componenti del sistema informativo e sulle applicazioni e la verifica della conformità della configurazione dei sistemi alle linee guida e alle politiche aziendali avviene mediante due processi distinti:
  - **Vulnerability assessment**: verifica la presenza di vulnerabilità note e della corretta configurazione dei sistemi (es.: disabilitazione di porte TCP e di servizi secondo quanto previsto dalle politiche di sicurezza aziendali)
    - È un'attività svolta mediante appositi strumenti che eseguono la scansione automatica delle porte di rete dei diversi apparati alla ricerca dei servizi attivi ed eseguono la verifica della configurazione (software installato, versioni del software, applicazione di patch di sicurezza, ecc.)
  - **Penetration test**: attraverso un'attività manuale o automatizzata attraverso strumenti software automatici, si prova a violare la sicurezza di un'applicazione o di un sistema, verificando la presenza di errori che consentono accessi non autorizzati e modifica o acquisizione di dati riservati

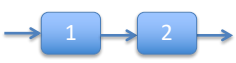
SOC – Security Operation Center

- Un **SOC** è un centro operativo, attivo generalmente 24h x 7 x 365 giorni l'anno, che attraverso strumenti SIEM, UEBA, di system/network monitoring, **controlla la sicurezza** del sistema informativo aziendale e **indirizza le azioni di risposta e di mitigazione** dell'impatto a fronte del verificarsi di attacchi informatici
- Il SOC è composto da **operatori** e **analisti di sicurezza** coordinati da un **SOC manager**
- A fronte di un **allarme** originato da un sistema di monitoraggio (SIEM o altro) gli operatori e gli analisti ne verificano la natura e stabiliscono se tale allarme è un «falso positivo» (un falso allarme) o se è un allarme effettivo che dà luogo, quindi, ad un **incidente di sicurezza**
- L'incidente di sicurezza viene tracciato e gestito attivando anche funzioni dell'organizzazione aziendale esterne al SOC
- Le operazioni di mitigazione attuate o indirizzate dal SOC possono consistere nella modifica di regole su un apparato firewall, isolamento di un sistema compromesso per non «infettare» altri sistemi limitrofi, la disabilitazione di uno o più utenti, la disabilitazione di uno o più servizi, ecc.

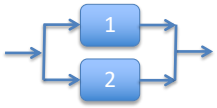


Affidabilità e Disponibilità

- La disponibilità e l'affidabilità di un sistema informatico sono due aspetti legati fra loro e inerenti la probabilità che si verifichino dei guasti o dei malfunzionamenti tali da compromettere il sistema (anche per causa dolosa, come un attacco informatico)
  - **Disponibilità**: esprime la garanzia di essere pronto all'uso in esercizio
  - **Affidabilità**: esprime la garanzia di continuità di uso per un determinato tempo, indipendentemente da quanto duri il tempo di rimessa in esercizio
- Due grandezze importanti da stimare sono
  - **MTBF** (*mean time before failure*): il tempo medio di disponibilità del sistema, prima che si verifichi un guasto
  - **MTTR** (*mean time to recover*): il tempo medio necessario per ripristinare il corretto funzionamento di un sistema guasto
- Disponibilità: $D = \frac{MTBF}{MTBF + MTTR}$
  - Sistemi in serie: $D = D_1 \times D_2$



  - Sistemi in parallelo: $D = (D_1 + D_2) - (D_1 \times D_2)$



(dalla probabilità di guasto, che è complementare alla disponibilità)

Affidabilità e Disponibilità

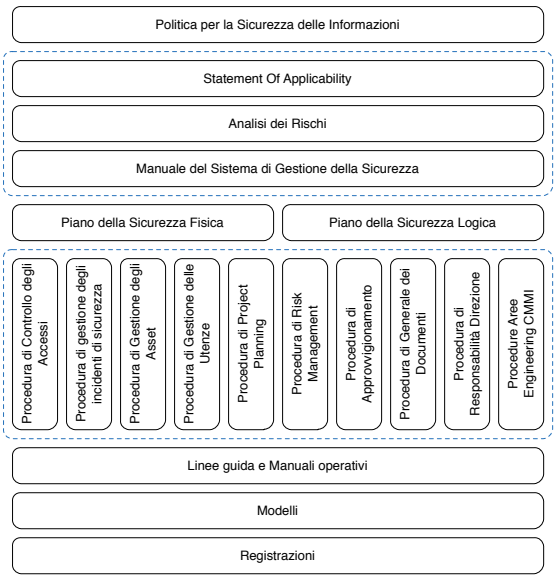
- Caratteristiche che migliorano l'affidabilità e la disponibilità di un sistema:
  - ***Fault tolerance***: capacità del sistema di resistere a determinati guasti di alcune delle sue componenti
    Si ottiene adottando ridondanze hardware e logiche, quali configurazioni master/slave, server in cluster, servizi di *load balancing*, ecc.
  - ***Business continuity***: possibilità di operare senza interruzione almeno per le funzionalità di maggiore importanza, senza quindi interrompere i servizi di business
    Viene perseguita attraverso funzionamenti ed operatività parallele, svolte geograficamente e logicamente in modo indipendente
  - ***Disaster recovery***: possibilità di superare eventi straordinari senza perdite di dati e informazioni rilevanti e riducendo al minimo il periodo di interruzione del servizio di business
    È generalmente raggiunto studiando strategie di distribuzione degli asset e dei sistemi informativi su più "siti" geografici, predisponendo meccanismi di replica delle informazioni su siti differenti e mediante procedure di attivazione dei siti di disaster recovery e di ripristino dei servizi di business

Normative sulla sicurezza IT

- Nell'ambito della sicurezza delle informazioni sono state definite numerose **normative** e **regolamenti** che impongono alle organizzazioni e ai responsabili della sicurezza dei sistemi informativi di adottare **politiche**, **procedure** e **controlli** tali da garantire di aver predisposto contromisure adeguate per tutelare la riservatezza, l'integrità e la disponibilità delle informazioni
- La ***compliance*** alle normative e ai regolamenti è un aspetto molto importante della sicurezza informatica
- Alcune normative sulla sicurezza delle informazioni:
  - **ISO/IEC 27001**: definisce i requisiti per un Sistema di Gestione della Sicurezza delle Informazioni (SGSI o ISMS dall'inglese *Information Security Management System*); include aspetti relativi alla sicurezza logica, fisica ed organizzativa
  - **ISO/IEC 27005**: definisce delle linee guida per la gestione del rischio nell'ambito della sicurezza delle informazioni
  - **GDPR** – ***General Data Protection Regulation***, regolamento UE n. 2016/679 in materia di trattamento dei dati personali e di privacy, operativo dal 25/5/2018
  - **Direttiva NIS** (direttiva UE 2016/1148), misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione
  - **D.lgs 196/2003**: Testo Unico sulla privacy, sulla tutela nella gestione dei dati personali
  - **Amministratori di sistema**: Provvedimento del Garante sulla Privacy per gli amministratori di sistema del 27 novembre 2008
  - **Presidenza del Consiglio dei Ministri, Direttiva 16/1/2002**: Sicurezza informatica e delle telecomunicazioni nelle pubbliche amministrazioni
  - Presidenza del Consiglio dei Ministri, **Piano Nazionale per la Protezione Cibernetica e la Sicurezza Informatica**, 2017

Normativa ISO/IEC 27001

- Come tutti gli standard ISO definisce delle linee guida per la realizzazione di un **sistema**
- **SGSI**: Sistema per la Gestione della Sicurezza delle Informazioni: è costituito da politiche, procedure, documenti, registrazioni ed anche da strumenti di supporto e sistemi di tipo informatico

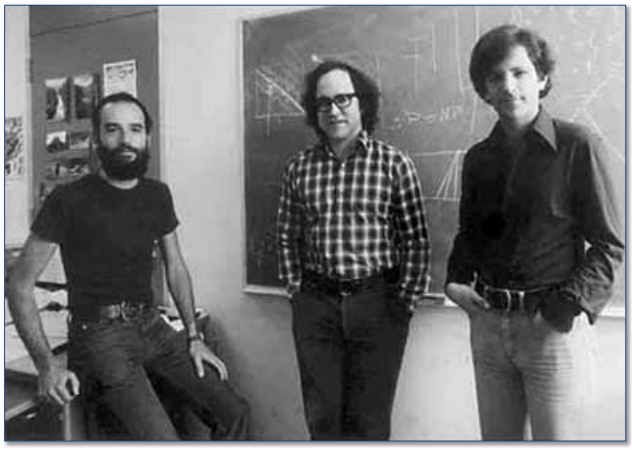


Normativa ISO/IEC 27001

- ISO 27001 propone un insieme di **133 controlli** per verificare lo stato di applicazione delle linee guida e dunque la completezza e l'efficacia del SGSI
- I controlli coprono i seguenti ambiti:
  1. **Information Security Policies** (definizione e revisione della politica per la sicurezza)
  2. **Organization of Information Security** (ruoli, responsabilità, separazione delle competenze, utilizzo di *device* mobili e gestione del telelavoro)
  3. **Human Resource Security** (aspetti inerenti la sicurezza nelle fasi di selezione del personale, gestione del personale, conclusione del rapporto di lavoro con il personale)
  4. **Asset Management** (responsabilità sugli asset, classificazione delle informazioni, gestione dei supporti di memoria)
  5. **Access Control** (gestione delle credenziali e delle autorizzazioni degli utenti)
  6. **Cryptography** (politica nella cifratura dei dati, gestione delle chiavi di cifratura)
  7. **Physical and Environmental Security** (sicurezza fisica, protezione degli asset fisici)
  8. **Operations Security** (change management, threat management, backup, logging, monitoring, ecc.)
  9. **Communications Security** (sicurezza della rete)
  10. **System acquisition, development and maintenance** (approvvigionamenti, sviluppo e manutenzione software, manutenzione dei sistemi)
  11. **Information Security Incident Management** (gestione degli incidenti di sicurezza)
  12. **Information Security Aspects of Business Continuity Management** (business continuity, disaster recovery, ridondanza degli apparati, ecc.)
  13. **Compliance** (rispetto delle normative e dei regolamenti di settore)

GRC – Governance, Risk and Compliance

- La sicurezza del sistema informativo deve essere **governata** attraverso processi, normative, policy, regolamenti esterni e controlli eseguiti con continuità sull'intero perimetro del sistema informativo aziendale
- In particolare, dal momento che un livello assoluto di sicurezza non potrà mai essere ottenuto (la sicurezza informatica di fatto è un processo di miglioramento continuo), è essenziale **misurare gli indici di rischio** a cui è sottoposto il «business» aziendale, rispetto alle vulnerabilità e alle minacce che insistono sul sistema informativo
- Tali **rischi devono essere identificati e misurati** per poi definire dei **piani di mitigazione** del rischio, che portino ad annullarli, trasferirli ad altri o a ridurli sotto a soglie accettabili
  - Il sistema informativo è costituito da ***asset*** (computer, archivi di dati, servizi, ecc.)
  - Gli *asset* possiedono delle **vulnerabilità** che, se sfruttate, possono creare un danno all'azienda
  - Le **minacce** sono le capacità di un soggetto di sfruttare (consapevolmente o meno) le vulnerabilità
  - I **rischi** sono una misura dell'**impatto** di una minaccia su un determinato *asset*
- Le normative e i regolamenti interni ci suggeriscono delle linee guida per ridurre le vulnerabilità o mitigare i rischi; un processo di *compliance management*, attraverso un insieme di controlli, verifica la conformità della configurazione dei sistemi o dei processi aziendali alle normative vigenti (es.: GDPR) e ai regolamenti aziendali
- I **sistemi GRC** supportano l'organizzazione aziendale nelle attività di ***governance*** della sicurezza, ***risk analysis*** e ***risk management*** e di ***compliance management***



Ronald L. Rivest, Adi Shamir, and Leonard Adleman
I tre matematici nel 1978 erano ricercatori al MIT quando inventarono l'algoritmo RSA di crittografia asimmetrica, che permette di cifrare o firmare informazioni. Il modello di crittografia asimmetrica era stato proposto solo due anni prima da Whitfield Diffie e Martin Hellman.