Raccolta di domande V/F

Intrusion Detection System

F dal punto di vista delle intrusioni, osservare quello che avviene all'esterno della mia organizzazione non è particolarmente rilevante.

è importante.

F preparare le politiche di risposta agli incidenti è possibile solo se un'azienda ha un Incident Response Team

sus

F le persone che lavorano in un SOC non dovrebbero occuparsi di vulnerability management e patch management

e invece sì.

Oltre a questo si devono occupare di

- preparazione del personale
- analisi dei trend del cybercrime
- definire il disaster recovery plan
- protezione degli asset/ mitigazione del rischio
- manutenzione dispositivi di sicurezza e loro configurazioni
- vulnerability management e patch management

V un SOC dovrebbe includere anche personale che si occupa dell'analisi del cybercrime per mantenere aggiornata l'analisi dei rischi

F un NIDS è uno scanner di rete che identifica vulnerabilità note

È uno strumento di monitoring del traffico di rete.

V gli honey pot non espongono asset reali agli attacchi

F ? un SIEM (Security Incident Events Management) permette di gestire in maniera automatizzata le reazioni ad attacchi e incidenti

la risposta automatizzata a incidenti di sicurezza non è sempre completamente gestita dai SIEM, che tendono a focalizzarsi più sulla rilevazione, analisi e reportistica. Gli IPS di solito intervengono automaticamente.

F un HIDS è un tool che identifica le vulnerabilità presenti su un determinato host prima che vengano sfruttate.

La sua funzione principale è rilevare attacchi o attività sospette, analizza quindi i log di un singolo host e le configurazioni, per rilevarne dei cambiamenti

V un IPS può permettere di velocizzare ed automatizzare la risposta a specifiche intrusioni rilevate

Un IPS (Intrusion Prevention System) non solo rileva le intrusioni, ma può anche intervenire automaticamente per prevenire l'attacco (ad esempio, bloccando il traffico sospetto), contribuendo a una risposta automatizzata e veloce alle minacce rilevate

V un HIDS può verificare, all'interno di un host specifico, che alcuni file non vengano modificati e analizzare quello che riportano i log dei sistemi informativi

Un HIDS monitora l'integrità dei file (file integrity checking) e analizza i log degli eventi su un host per rilevare cambiamenti o attività anomale, confermando che alcune informazioni non siano state modificate senza autorizzazione.

Protezione del codice

F le tecniche di attestazione del codice impediscono le modifiche al codice garantendo l’integrità

non **impediscono** le modifiche al codice, ma le **rilevano.**

V alcune tecniche di attestazione del codice verificano se i binari sono integri al momento dell'esecuzione o del caricamento in memoria o quando sono salvati su disco

V i ROP sono gadget che terminano sempre con istruzioni RET

i "gadget" sono piccole sequenze di istruzioni che terminano tipicamente con un’istruzione **RET (return)**, che forza il controllo del programma a tornare al chiamante

F le protezioni del software servono a rendere impossibile violare gli asset presenti nel software

V le protezioni del software hanno l’obiettivo di ritardare o rendere meno vantaggiosi gli attacchi del binary machine code di un programma

Le protezioni software, come la crittografia del codice o l’offuscamento, mirano a ritardare o complicare il reverse engineering o l'analisi del **binary machine code**

V la potency è una misura astratta di quanto è buona una tecnica di protezione del software

Collberg ha introdotto l’idea di avere una potency, non c’è un metodo concreto per misurarla: ci sono due approcci:

1. objective metrics
2. esperimenti empirici

F un disassembler genera deterministicamente la rappresentazione in codice assembly del binary machine code di un programma

F la white-box cryptography cifra le chiavi nel codice di un’applicazione per proteggerla da attacchi di reverse engineering

La **white-box cryptography** è progettata per proteggere le chiavi crittografiche in ambienti in cui l'attaccante ha pieno accesso al codice e può tentare di eseguire il reverse engineering. Tuttavia, non si limita a "cifrare" le chiavi nel codice. Invece, combina le chiavi crittografiche con operazioni matematiche offuscate, rendendo più difficile per un attaccante estrarle o identificarle attraverso l’analisi.

F uno shellcode serve per svolgere attacchi di tipo Return Oriented Programming (ROP)

Lo **shellcode** è un pezzo di codice che viene eseguito dopo un exploit per ottenere il controllo di un sistema, come l’apertura di una shell. Gli attacchi **ROP** utilizzano gadget nel codice esistente per eseguire comandi arbitrari, ma non implicano necessariamente l’uso di shellcode. Sono due tecniche distinte, anche se possono essere usate insieme in alcuni scenari.

F uno shellcode è un tipo di gadget; esso rilascia, una volta terminato, il controllo dell'esecuzione alla funzione chiamante e serve quando si attacca un'applicazione mediante Return Oriented Programming (ROP)

un **shellcode non è un gadget**. E soprattutto, serve per eseguire comandi sulla macchina della vittima, quindi non ritorna l’esecuzione alla funzione chiamante.

V la Data Execution Prevention (DEP) vieta l’esecuzione di codice dai segmenti in cui ho privilegi di lettura (o scrittura)

Ciò aiuta a prevenire attacchi come il buffer overflow, in cui un attaccante tenta di eseguire codice in regioni della memoria destinate ai dati.

V abilitando la Data Execution Prevention (DEP) rendo più difficile sfruttare i buffer overflow

V nel paradigma Man-at-the-End, gli attaccanti hanno il controllo completo degli endpoint dove gli attacchi vengono preparati e realizzati.

F nel paradigma Man-at-the-End, gli attaccanti prendono il controllo degli endpoint delle vittime

l'**attaccante non prende necessariamente il controllo degli endpoint delle vittime**, ma piuttosto ha **accesso fisico o locale** a una copia del software o del dispositivo e cerca di manipolarlo o analizzarlo.

Gestione del Rischio

V vulnerability management e patch management, secondo il NIST, sono attività che dovrebbero essere svolte da personale informatico specializzato in cybersecurity.

non serve che sia specializzato in cybersecurity, ma il NIST consiglia che siano svolte da personale specializzato.

V durante la fase di risk monitoring potrei dover cambiare tutte le formule che mi permettono di stimare il rischio aziendale.

V secondo il framework RMF del NIST, la fase di framing include l'identificazione degli asset e la valutazione del loro valore

Il **Risk Management Framework (RMF)** del NIST è un insieme di linee guida e best practice sviluppato dal National Institute of Standards and Technology (NIST) per gestire e mitigare i rischi informatici all'interno di un'organizzazione. Si divide in 4 fasi:

1. **Risk framing**: si descrive proprio sistema aziendale, identificando gli asset e valutando il loro valore
2. **Risk assessment**: identifico minacce e debolezze
3. **Risk mitigation/ Respond**: studiano e implementano le possibili soluzioni e mitigazioni
4. **Risk Monitoring**: monitorare continuamente il nostro sistema in maniera tale da valutare l'efficacia delle soluzioni che abbiamo pensato ed implementato nello step precedente

F le CVSS definiscono in maniera fissa e assoluta caratteristiche e severità delle vulnerabilità notificate al MITRE

framework che permette di valutare il livello di sicurezza in base a 3 metriche che sono:

Base: pericolosità intrinseca della vulnerabilità.

Temporal: come cambia al passare del tempo.

Environmental: quanto è rilevante per un dato ambiente.

F OWASP è uno standard che serve (anche) per la valutazione del livello di sicurezza delle applicazioni web

OWASP (Open Web Application Security Project) è una iniziativa che ha come obiettivo quello di rendere chiaro a tutti che la sicurezza dei siti web è precaria. Non è un tool bensì una organizzazione formata da esperti di sicurezza che, utilizzando diversi dati provenienti da varie aziende, hanno stilato una serie di report e Top10 di problemi e vulnerabilità in ambito web.

Standard

V L'orange book è un documento redatto dal DoD il cui titolo completo è Trusted Computer System Evaluation Criteria.

V Gli standard possono permettere di stimare quando alcuni prodotti di sicurezza possono essere considerati sicuri senza fare test propri

V I Common Criteria non includono una metodologia di valutazione, la valutazione è trattata da un ulteriore standard (CEM)

I Common Criteria **non** implicano, né fanno riferimento a

- processi di sviluppo
- metodologia di valutazione

- regolamentazioni/leggi

V I Common Criteria non fanno riferimento ad un processo di valutazione perché questa è trattata dalla Computer Evaluation Methodology

V Il Mandatory Access Control funziona confrontando le etichette (label) delle risorse e degli utenti che ne fanno richiesta e concedono l'accesso secondo modelli formali

? Il Mandatory Access Control previsto dalla casse B di TCsec usa modelli formali per stabilire quando garantire l'accesso alle risorse.

Dovrebbe essere il livello A che ha verifica formale tramite modellazione matematica del sistema.

Il **Trusted Computer System Evaluation Criteria (TCSEC)**, noto come **Orange Book**, classifica i sistemi informatici in base al loro livello di sicurezza. Le classi principali sono:

Classe D: Minimal Protection

- Sistemi che non soddisfano i requisiti di sicurezza delle classi superiori.

Classe C: Discretionary Protection

- Sistemi con **Discretionary Access Control (DAC)**, dove gli utenti possono controllare l'accesso ai propri file.
  - **C1**: **Discretionary Security Protection**
    - Controlli minimi, il sistema offre protezione discrezionale agli utenti e agli oggetti.
  - **C2**: **Controlled Access Protection**
    - Maggiori controlli di accesso, inclusi audit trail e separazione di utenti e dati.

Classe B: Mandatory Protection

- Sistemi con **Mandatory Access Control (MAC)**, basati su modelli formali di sicurezza.
  - **B1**: **Labeled Security Protection**
    - Sistemi che etichettano dati e utenti con classificazioni di sicurezza e applicano MAC.
  - **B2**: **Structured Protection**
    - Sistemi con una sicurezza più rigorosa, audit dettagliati e protezione di tutti i canali di comunicazione.
  - **B3**: **Security Domains**
    - Sistemi che implementano domini di sicurezza con maggiore isolamento tra processi e strutture di auditing più avanzate.

Classe A: Verified Protection

- Sistemi con il massimo livello di sicurezza, che utilizzano tecniche di verifica formale.
  - **A1**: **Verified Design**
    - Sistemi in cui la sicurezza è **formalmente** verificata in tutto il ciclo di vita del sistema, inclusa la progettazione e l'implementazione.

Questa classificazione del TCSEC è stata sviluppata per valutare e certificare la sicurezza di sistemi informatici, specialmente in contesti militari e governativi.

V In una valutazione di sicurezza ai fini della standardizzazione, la correttezza della soluzione deve tener conto anche del processo di sviluppo.

Nella valutazione della sicurezza, la **correttezza** del sistema riguarda anche il **processo di sviluppo**. Questo include come il sistema è stato progettato, sviluppato e testato per garantire che siano state seguite le pratiche di sicurezza appropriate.

V Anche in Italia abbiamo un Common Criteria Evaluation Scheme, perché questi organisimi di valutazione funzionano su base nazionale.

Ogni paese che adotta i **Common Criteria** può istituire un proprio organismo di valutazione nazionale.

F La *strength of mechanisms* dichiarata permette di distinguere i prodotti sicuri da quelli che lo sono meno.

La **strength of mechanisms** si riferisce al livello di robustezza di un meccanismo di sicurezza rispetto a vari parametri che stabilisco a priori. Se i parametri per cui voglio valutare la robustezza del mio sistema non parametri "scarsi", il risultato è un'alta efficacia rispetto però a situazioni poco a rischio. Questo significa che la valutazione *basic, medium, high* non è un parametro assoluto, ma va sempre relativizzata a ciò che sto valutando.

F Una *strength of mechanisms* dichiarata alta indica che il prodotto può ritenersi molto sicuro

è solo uno degli aspetti che determinano la sicurezza complessiva di un sistema o prodotto.

F Un Protection Profile dei Common Criteria definisce la procedura di valutazione per security target specifici (es. metodologia di valutazione per smart card, sistemi operativi)

Il **PP** specifica gli **obiettivi di sicurezza** e i **requisiti** che un prodotto deve soddisfare, mentre la **procedura di valutazione** viene definita separatamente in base al contesto (di solito tramite lo standard CEM).

F Un Protection Profile è un modo per definire in maniera semplificata come verrà gestita la procedura di valutazione per security target specifici

Il PP è una **specifica formale dei requisiti di sicurezza.**

F ITSEC non supporta la ri-valutazione di un precedente processo di standardizzazione.

ITSEC consente la revisione e la ri-certificazione di prodotti esistenti, specialmente se ci sono stati aggiornamenti o modifiche che potrebbero influenzarne la sicurezza.

V durante la fase di risk monitoring potrei dover cambiare tutte le formule che mi permettono di stimare il rischio aziendale

V l'information gathering è un processo essenziale per la valutazione dell'esposizione delle aziende ai rischi informatici

Certificati

V per fidarmi di un certificato, oltre alla verifica crittografica della firma della CA che l'ha emesso, devo aggiungere la fiducia esplicita nei confronti della root CA.

F SHA-3 è l'algoritmo scelto dopo che SHA-2 è stato deprecato dal NIST.

SHA-2 non è stato deprecato. **SHA-3** è stato sviluppato come una famiglia di algoritmi hash alternativi per offrire opzioni diverse rispetto a SHA-2 e per fornire una diversa base crittografica, non perché SHA-2 fosse obsoleto o compromesso.

V il protocollo ESP di IPsec v2 è un esempio concreto di Authenticated Encryption with Associated Data.

ESP (Encapsulating Security Payload) in IPsec fornisce sia confidenzialità che autenticazione

F in RSA, può essere scelto qualunque esponente pubblico 'e', senza alcun effetto negativo né dal punto di vista della sicurezza, né dal punto di vista computazionale

e va scelto tale che $1 < e < \phi(n)$ con e e $\phi(n)$ coprimi, dove $\phi(n) = (p-1)(q-1)$

e di solito vale 3, 17 o **65537**. Lo standard dice di scegliere 65537 perché è il più grande numero primo di Fermat noto e ha soltanto due bit ad 1 nella sua codifica binaria.

F con l'On-line Certificate Status Protocol posso chiedere ad un server creato appositamente (es. disponibile via internet) se un determinato certificato, identificato dal suo serial number, è valido in un preciso momento del presente o passato.

Solo nel presente.
Per verificare lo stato di un certificato in un momento passato, si dovrebbero usare altri metodi, come i **Certificate Revocation Lists (CRL)** storiche.

F l’uso di Key Derivation Function è tipicamente sconsigliato perché sono funzioni lente ed inefficienti nella gestione della memoria.

Le **Key Derivation Functions (KDF)** sono progettate per essere lente e resistenti agli attacchi di forza bruta. La loro lentezza è un vantaggio per aumentare la sicurezza, non uno svantaggio. Sono utilizzate precisamente per questo motivo, e la loro gestione della memoria non è generalmente un problema significativo.

Si tratta di una delle applicazioni della crittografia asimmetrica e serve per trasformare una psw in una chiave crittografica fatta di numeri random (es: PBKDF2).

V DH e ECDH sono basati su problemi matematici “difficili” diversi ma gli attacchi noti sono (computazionalmente) equivalenti.

Diffie-Hellman (DH) e **Elliptic Curve Diffie-Hellman (ECDH)** si basano su problemi matematici diversi (rispettivamente, il problema del logaritmo discreto e il problema del logaritmo discreto su curve ellittiche), ma entrambi hanno analoghi tipi di attacchi basati sulla complessità computazionale, come gli attacchi di forza bruta o l'uso di algoritmi per risolvere i problemi in tempo sub-esponenziale.

V La firma digitale di un documento è il risultato di un’operazione che coinvolge l’uso di un parametro asimmetrico segreto e del digest del documento stesso.

Sicurezza di canale

F Se il client presenta un session-id valido, il server deve accettare di eseguire l’Handshake ridotto, computazionalmente molto più leggero e con meno scambi di pacchetti e idoneo a client con poca capacità computazionale (IoT).

Il server può rifiutare l’uso del session-id dopo un tot di tempo oppure in assoluto.

V se il client presenta un session-id, il server potrebbe decidere di saltare (buona parte del)la fase di Handshake e indicare di iniziare a proteggere direttamente i dati di canale a partire dai segreti negoziati in uno dei precedenti Handshake

V OpenVPN è un protocollo che può essere usato in alternativa ad IPsec per creare Virtual Private Network.

F L’uso della porta 443 per erogare un servizio web implica che la connessione è protetta con TLS

La porta **443** è tradizionalmente utilizzata per **HTTPS**, che è TLS/SSL. Tuttavia, la porta 443 può essere utilizzata anche per altri protocolli non sicuri, quindi non è una garanzia assoluta che la connessione sia protetta con TLS senza conferma esplicita.

F SSH usa certificati X.509 semplificati per trasmettere la chiave al server.

SSH non utilizza certificati di alcun tipo. Utilizza chiavi pubbliche e private per l'autenticazione, a chiave pubblica, non essendo associata ad un certificato di una CA, deve essere nota alla controparte per poter essere verificata ⇒ mantiene un DB delle chiavi conosciute.
I certificati X.509 sono tipicamente usati in contesti TLS/SSL, non in SSH.

V TLS numera i pacchetti per evitare attacchi di tipo Replay

TLS utilizza numeri di sequenza per ogni pacchetto, che aiutano a prevenire **attacchi di replay** (dove un attaccante riproduce pacchetti di dati precedenti per ottenere accesso non autorizzato).

F TLS usa una sliding window per evitare (parzialmente) attacchi di tipo Replay

La **sliding window** è un meccanismo utilizzato in vari contesti, tra cui le reti e la crittografia, per gestire e controllare l'ordine e la validità dei pacchetti o dei messaggi, ma non è presente in TLS (si usa invece il numero di pacchetto per evitare attacchi replay).

V DTLS funziona con UDP ma non con TCP

V TLS 1.3 usa un Handshake Protocol diverso da quello usato fino al TLS 1.2.

TLS 1.3 introduce un nuovo protocollo di handshake rispetto a **TLS 1.2**, migliorando la sicurezza e riducendo i tempi di handshake.

F TLS 1.3 è perfettamente interoperabile con TLS 1.2

V la versione più recente di TLS non usa più la compressione

TLS 1.3 non usa più la compressione perché computazionalmente onerosa, e si preferisce “sprecare” banda.

V la cyphersuite TLS_DHE_RSA_WITH_AES_128_CBC_SHA indica la volontà di firmare con RSA i parametri effimeri per lo scambio di chiavi.

F la ciphersuite TLS_DH_RSA_WITH_AES_128_GCM_SHA256 indica la volontà di usare SHA256 per calcolare il MAC nel Record Protocol

Il MAC viene calcolato già con GCM, quindi SHA256 viene utilizzato per generare le chiavi a partire dalla premaster secret.

F Nel caso venga scelta la ciphersuite TLS_DHE_RSA_WITH_AES_128_CBC_SHA, l’uso di algoritmi effimeri impone che SHA1 sia usato solo per generare la Master Secret (e successivamente le 4 chiavi usate per proteggere il canale).

SHA1 viene utilizzato anche nell’HMAC.

V la ciphersuite TLS_DHE_DSS_WITH_AES_128_CBC_SHA indica la volontà di firmare con DSS i parametri effimeri per lo scambio di chiavi

DSS (Digital Signature Standard): standard per le firme digitali che usa come algoritmo DSA. In questo caso lo uso per firmare i parametri effimeri.

V L’utilizzo di meccanismi “effimeri” nello scambio della premaster secret garantisce la proprietà di *perfect forward secrecy*

Ottimo nel caso in cui attaccante ha interesse a intercettare la comunicazione e conservarsela, perché se per caso poi trova la chiave privata RSA del server poi può decifrarsi tutta la comunicazione passata. Però se non c’è questo pericolo, non serve usare i meccanismi effimeri perché comunque computazionalmente sono più pesanti.

Attacchi

F dato un keyed-digest calcolato come kd = H (K || M), esiste un attacco che permette di ottenere la chiave K a partire da kd

Non esiste un attacco che permetta di ottenere la chiave K.
Un possibile attacco potrebbe essere
length extension attack se K viene concatenata direttamente a M. In HMAC ho una costruzione più robusta, quindi questo non succede.

V le tabelle delle connessione di un server protetto con un SYN interceptor non sono a (elevato) rischio di saturazione

Prima che la connessione sia completamente stabilita, il server non alloca alcuna risorsa o memoria nella sua tabella delle connessioni.

F lo Smurfing attack può essere evitato richiedendo l'autenticazione del target

Lo **smurfing attack** (o **Smurf attack**) è un tipo di attacco **Denial of Service (DoS)** che sfrutta i protocolli di rete per inondare un obiettivo con un'enorme quantità di traffico, sovraccaricandolo e rendendolo inutilizzabile. L'attacco sfrutta principalmente il protocollo **ICMP (Internet Control Message Protocol)**, utilizzando pacchetti **ICMP Echo Request** per amplificare il traffico verso la vittima.
Contromisure:
per pacchetti dall’esterno → rifiutare broadcast IP
per pacchetti dall’interno → identificare il responsabile tramite strumenti di network management

Variante: **Fraggle attack**. Usa pacchetti UDP invece di pacchetti ICMP.

V il particolare tipo di attacco usato da ettercap richiede che siano costantemente inviati messaggi che servono a mantenere le vittime "avvelenate"

V con l'attacco Heartbleed si possono leggere dati confidenziali e altri segreti

L'attacco **Heartbleed** è una grave vulnerabilità scoperta nel 2014 nel software di crittografia **OpenSSL.** La vulnerabilità, identificata come **CVE-2014-0160**, consente a un attaccante remoto di leggere porzioni di memoria del server o del client, potenzialmente esponendo dati sensibili come chiavi private, password, token di sessione e altre informazioni critiche e sfrutta il fatto che l'utente dichiara la dimensione del buffer e il server non la verifica.

F l'attacco di Kaminsky può essere evitato usando IPsec

Kaminsky DNS Cache Poisoning Attack, è una vulnerabilità scoperta da **Dan Kaminsky** nel 2008 che colpisce il sistema di risoluzione DNS (Domain Name System). Questo attacco è progettato per compromettere i server DNS e reindirizzare il traffico degli utenti verso siti web malevoli o falsificati. È considerato uno dei più gravi attacchi di **cache poisoning** DNS.
Il DNS lavora a livello 7, mentre IPsec lavora a livello 3

F con il FIN scanning posso distinguere filtri di livello applicativo da packet filter stateful

Il **FIN scanning** è una tecnica di scansione di porte utilizzata per determinare quali porte su un sistema target siano aperte, chiuse o filtrate. Questo tipo di scansione fa parte delle **scansioni stealth** (perché non stabilisce una connessione completa, il flag FIN viene usato per chiudere una connessione TCP) e viene utilizzato per cercare di evitare il rilevamento da parte dei firewall e dei sistemi di rilevamento delle intrusioni.

F un attacco basato su Optimal Asimmetric Encryption Padding (RSA-OAEP) può avere successo se si usa un "small encryption exponent"

Quando uso RSA non prendo il messaggio così com'è e lo elevo a e , ma devo "scorrelarlo". RSA-OAEP prende il msg e lo concatena a un pezzo random (padding). Questa tecnica serve per mitigare gli attacchi che sfruttano i messaggi di errore troppo precisi, non c'entra con il small encyption exponent.

F il port scanning è il metodo di information gathering con cui posso identificare con certezza i servizi in base al numero di porta su cui i servizi stessi sono in ascolto

V conoscere il numero di sequenza che un host userà nel corso del prossimo tentativo di connessione TCP è utile agli attaccanti per fare spoofing

Se un attaccante può prevedere o conoscere il numero di sequenza che un host utilizzerà, può creare pacchetti che sembrano legittimi e inserirli in una sessione TCP esistente. Questo è possibile perché TCP si basa sui numeri di sequenza per garantire l'ordine e l'integrità dei dati.

Sicurezza di Messaggio

V i messaggi clear-signed sono visibili su qualunque strumento per la gestione delle mail e anche da web perché firmati con firma detached

F il metodo STARTLS è usato per trasmettere in maniera confidenziale messaggi di posta elettronica

Il canale sicuro con TLS serve per l'autenticazione del client

F il protocollo SMTP permette di autenticare gli utenti prima di inviare mail solo con metodi deboli come LOGIN, PLAIN e CRAM-MD5

Può aprire una connessione sicura con TLS.

F il formato PKCS#12 è un metodo ottimizzato per trasportare firme digitali

Si tratta di una struttura dati per il trasporto di materiale crittografico e identità digitale di un utente.

F il greylisting è uno strumento molto efficace per decidere se rifiutare o accettare mail da un MTA Open Relay

F il CMS è l'evoluzione del formato PKCS#12 per la rappresentazione di dati crittografici

CMS è l'evoluzione del formato PKCS#7

F HTTP-S è un'implementazione obsoleta che protegge messaggi HTTP usando strutture S/MIME

S-HTTP è obsoleta, non c'entra con S/MIME.

F la firma digitale di S/MIMEv4 ha sempre valore legale perché dalla versione 4 è uno standard IETF e usa crittografia asimmetrica che permette il non ripudio

La firma digitale di **S/MIMEv4** (Secure/Multipurpose Internet Mail Extensions) **non garantisce automaticamente valore legale**, e il fatto che utilizzi la **crittografia asimmetrica** non è sufficiente per assicurare il **non ripudio** con valore legale.

F un server Open Relay permette di inviare mail senza restrizioni ai soli utenti interni

Un server Open Relay è un server di posta elettronica configurato in modo da consentire a chiunque di inviare mail tramite di esso.

V S/MIME usa il meccanismo standard di MIME per gestire gli allegati per inserire oggetti crittografici

Sicurezza di Documenti

V Il Time Stamp è, in pratica, la firma digitale di una stringa di testo o di un intero che rappresenti un valore temporale e del digest di un documento

F L'Advanced Electronic Signature può essere usata in tribunale

No. La QES ha valore in tribunale perché basata su QC (Qualified Certificate).

V Per avere una Qualified Electronic Signature la chiave pubblica deve provenire da un Qualified Certificate

F Un dispositivo di firma sicuro può essere ritenuto sicuro se è tamper proof e usa algoritmi ritenuti sicuri

No, può essere soggetto a molti attacchi diversi.

F Forgiare una firma falsa è più facile se si usano le detached signature

Non c'entra niente.

V Cambiando l'ordine di una delle firme sequenziali può far fallire la verifica di qualche firma digitale

V Se un documento è firmato da più persone usando firme parallele, è possibile rimuovere una firma senza che gli altri firmatari se ne accorgano

F Un Qualified Certificate certifica l'identità usando algoritmi qualificati, riconosciuti dalle entità come più efficaci

Certifica l'identità perché emesso da società specializzate.

Leggi, GDPR e CyberSec Act

V Il Titolare del trattamento dei dati del Politecnico di Torino è il rettore

V I dati relativi allo stato di salute e la razza sono considerati di categoria speciale, sottocategoria di dati sensibili

Lo sono anche: opinioni politiche, religiose, principi filosofici, appartenenza a sindacati, dati biometrici o genetici, info sulla vita, orientamento sessuale

V Per dati personali si intende qualunque informazione che possa mettere in relazione o identificare una persona

F I servizi che usano dati personali devono essere pensati per proteggere questi dati durante tutte le fasi di progettazione ma non si può garantire che lo siano anche durante implementazione

Anche durante l’implementazione.

V Nel GDPR, il principio della privacy by design indica che bisogna usare automaticamente le protezioni più restrittive possibili

F Il GDPR introduce il concetto di minimizzazione, che indica che i dati devono essere collezionati usando il minimo numero di strumenti e resi accessibili al minor numero di operatori

Il concetto di minimizzazione si riferisce al fatto che i dati vanno collezionato in modo adeguato, rilevante e limitato a quanto necessario per lo scopo dichiarato.

F Il principio della Full Functionality del GDPR richiede che i controlli funzionino al massimo livello di sicurezza per garantire la protezione dei dati personali

La Full Funcionality si riferisce al fatto che con la scusa della privacy non posso limitare le funzionalità.

V Il principio della Full Lifecycle Protection significa che i dati devo essere protetti per tutto il loro ciclo di vita

V Un data breach è un incidente informatico che porti alla distruzione, alterazione, diffusione non autorizzata o accesso ai dati personali

V Quando una persona accetta il ruolo di DPO diventa responsabile dei danni causati dai data breach

F Il DPO si occupa di riottenere i dati degli utenti quando avvengono dei data breach

Il Data Protection Officer è un ruolo aziendale e non si occupa di riottenere i dati degli utenti, dichiara solo il data breach al garante.

V La PIA (Privacy Impact Assessment) è l’analogo dell’analisi dei rischi.