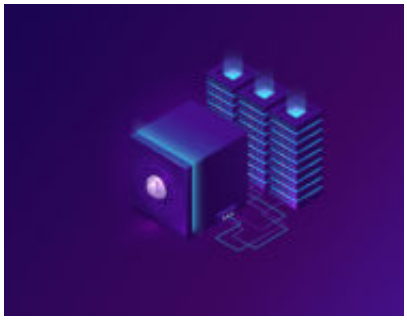
La verifica dei sistemi informatici

Author : Emilio Souberan

Date : 5 Febbraio 2020



Il riscontro dello stato di sicurezza, l'identificazione di vulnerabilità e il perfezionamento delle strutture dedicate alla protezione contro minacce ai sistemi informatici sono richiesti, oltreché dalla recente normativa europea sulla *privacy,* dai più comuni ***framework* di cybersecurity** intendendo, con la stessa, la sicurezza delle informazioni e la protezione dei sistemi informativi.

Nell'odierna società dell'informazione in cui viviamo, le informazioni sempre più a carattere digitale sono parte integrante di qualsiasi nostra attività e la sicurezza è divenuta una componente essenziale da cui l'informazione stessa non può prescindere.

Non è più sufficiente limitarsi ad assicurare la riservatezza ma è necessario garantirne anche la disponibilità e l'integrità.

Il trinomio riservatezza, disponibilità e integrità costituiscono infatti il *target* indispensabile di qualsiasi sistema di sicurezza delle informazioni.

La **riservatezza** consiste nel limitare l'accesso alle informazioni e alle risorse informatiche, alle sole persone autorizzate a farlo.

La **disponibilità** significa che le informazioni devono essere accessibili agli aventi diritto nel momento in cui essi lo richiedano e quindi i sistemi informatici debbono fornire le prestazioni richieste anche in caso di malfunzionamento.

L'**integrità** riguarda il grado di esattezza, coesione e attendibilità delle informazioni, cioè significa che queste non possano venire alterate, cancellate o modificate.

Necessità di un *security audit*

Dal momento che l'informazione è l'essenza di ogni organizzazione aziendale, questa deve adottare tutti i provvedimenti necessari affinché ciò abbia luogo persistendo nel tempo.

Nell’attualità in cui si ha una notevole esposizione ai rischi informatici ed in particolare dove avvengono quotidiane violazioni ai dei sistemi di sicurezza, in capo alle organizzazioni sono posti precisi obblighi di legge, ancora più marcati con l’avvento del nuovo regolamento europeo sulla protezione dei dati n° 679/2016 **(GDPR)**.

Si riporta in questo caso dell’art 32 del citato regolamento là dove: "…*il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio*…”

Ma l’attuare un piano di sicurezza deve tenere conto anche della successiva esigenza di **testare periodicamente i sistemi** posti a protezione delle informazioni stesse. Si parla in questo caso di audit di sicurezza o *security audit*.

Definizione di *security audit*

Un *security audit* può definirsi infatti come una valutazione sistematica della sicurezza del sistema informativo di un'azienda in cui si misura la sua conformità attraverso una serie di criteri stabiliti.

Un controllo approfondito in genere valuta la sicurezza della configurazione fisica e dell'ambiente, del software, dei processi di gestione delle informazioni e delle pratiche dell'utente del sistema.

Gli audit di sicurezza vengono spesso utilizzati per determinare la **conformità normativa**, sulla scia della legislazione privacy - di cui al regolamento europeo che specifica come le organizzazioni devono gestire le informazioni – e anche per confermare l’aderenza alle note norme ISO o framework di cybersecurity.

Gli audit di sicurezza possono essere svolti in prima persona dall’organizzazione (audit interno) cioè con proprio personale oppure da consulenti esterni che valutano il grado di qualità offerto al cliente finale (audit di seconda parte). Esiste poi un altro livello, il cosiddetto livello di terza parte che fa riferimento a professionisti esterni di realtà specializzate nell’erogazione di servizi di auditing le cui attività sono in genere finalizzate al rilascio di una certificazione di qualità.

Un audit di sicurezza informatica è una valutazione tecnica misurabile manuale o sistematica di un sistema o di un'applicazione. E pertanto non può basarsi esclusivamente sulla compilazione di checklist o altra documentazione.

Altrettanto vera è la **differenza tra un penetration test e un security audit**.

Un *penetration test* è un’attività mirata a cercare falle di sicurezza in una risorsa critica, come la rete informatica e, di solito, opera dall'esterno del firewall con informazioni minime al fine di simulare in modo più realistico i mezzi con cui un hacker attaccherebbe l’organizzazione.

Un *security audit* è invece una valutazione tecnica - metodica e misurabile - di come viene utilizzata la politica di sicurezza dell'organizzazione e in questo senso gli *auditor* lavorano con

informazioni privilegiate al fine di comprendere le risorse aziendali da controllare.

I *security auditor* svolgono il loro lavoro anche attraverso interviste personali ma soprattutto attraverso scansioni di vulnerabilità, l'esame delle impostazioni del sistema operativo, le analisi delle condivisioni di rete e i dati storici derivanti dai vari *log* di sistema. Si preoccupano principalmente del modo in cui vengono effettivamente utilizzate le politiche di sicurezza che sono alla base di qualsiasi strategia di sicurezza organizzativa.

Esistono alcuni **punti chiave** a cui gli audit di sicurezza cercano di dare risposta tra cui, a titolo di esempio, possiamo ricordare:

- la presenza di password robuste periodicamente cambiate;
- la verifica di malware nella rete informatica aziendale ivi compresi dispositivi iot e centralini voip;
- il riscontro sulla crittografia applicata ai vari dispositivi di memoria utilizzati dall'organizzazione;
- l'attivazione del controllo di accesso (acl) sui dispositivi di rete per verificare chi ha accessibilità ai dati condivisi;
- l'aggiornamento dei sistemi operativi e dei software;
- l'esistenza di un piano di backup programmato, di archiviazione dei relativi supporti e di verifica attraverso reali *restore*;
- la presenza di un piano di *disaster recovery* e la prova di funzionamento attraverso un vero e proprio di ripristino - simulato - di emergenza.

Si tratta ovviamente di una bozza di verifiche che va calibrata nei confronti dell'organizzazione oggetto di audit; ma che dà già un'idea dell'attività tecnica che manualmente dev'essere esperita durante una verifica di sicurezza.

Conclusioni

Nell'ottica sopraindicata, la necessità di una **coerenza complessiva di sicurezza informatica** dev'essere validamente testata e rivista altrettanto periodicamente, per via della rapida progressione tecnologica dei sistemi informatici e delle minacce correlate.

L'effettuazione di verifiche non può prescindere dall'esecuzione di reali test volti a misurare l'effettiva tenuta del sistema informativo aziendale attraverso idonei strumenti di controllo delle prestazioni e ogni organizzazione dovrebbe dotarsi di un piano di audit periodico per saggiare la tenuta della sicurezza delle informazioni.

Peraltro un *security audit* dovrebbe essere inteso come è uno dei modi migliori per determinare la sicurezza delle informazioni di un'organizzazione senza incorrere in costi e altri danni associati a un incidente di sicurezza, valore aggiunto che dovrebbe far riflettere le organizzazioni soprattutto in un momento in cui incidenti di sicurezza e/o *data breach* sono all'ordine del giorno.

Link utili

https://www.garanteprivacy.it/documents/10160/0/codice+in+materia+di+protezione+dei+dati+personali+%28testo+coordinato%29.pdf/b1787d6b-6bce-07da-a38f-3742e3888c1d?version=1.7

https://cyfor.co.uk/cyber-security/cyber-security-audit/

Articolo a cura di **Emilio Souberan**