Introduzione

Alla base di questo studio sono stati messi in evidenza dei concetti che sono alla base della sicurezza informatica, rappresentando gli standard riconosciuti e che raffigurano per la quasi totalità degli Stati la lingua universale che gli addetti ai lavori devono utilizzare.

E' stato rappresentato l'importante ruolo degli enti di standardizzazione ISO e IEC a cui si ispirano poi la totalità delle associazioni di ogni singolo Stato, in Italia una per tutte è UNI.

Seguono una carrellata di quelle che sono le norme che sono sentite come fossero cogenti quali la famiglia ISO 27000, le Sans, Cobit .

Durante la scrittura dell'elaborato, abbiamo immaginato di sederci accanto ad un hacker, capire cosa potrebbe osservare in un sistema informatico e quindi lo abbiamo esaminato attraverso il modello ISO/OSI e ad ogni livello capito quali attacchi questo può portare avanti.

Poi viene affrontato la normativa che ha portato l'adozione di misure minime all'interno della P.A., raffrontandolo al GDPR .

Capitolo 1.
Che cosa è la cyber security

Capitolo 1.1 paragrafo. Definizione

Con l'avvento dell'informatica tutta la p.a. ha dovuto ridisegnare i processi produttivi, innovare la formazione del personale e si è trovata a gestire problematiche che, se prima erano fisiche (conservazione delle informazioni in archivi), oggi sono anche informatiche in quanto spesso non detiene fisicamente le informazioni ma ci può accedere.

Queste informazioni che sono conservate spesso in banche dati centralizzate a cui dei client si collegano con livelli di privilegi standardizzati in base all' utente o all'ufficio, rappresentano l'asset da gestire e proteggere.

Oggi sempre più spesso i dati della pubblica amministrazione sono attaccati da malintenzionati, spesso organizzati, o addirittura sempre più spesso da hacker assoldati dagli Stati.

I dati si possono immaginare come racchiusi in una cassaforte, di cui non si conosce l'ubicazione, ma a cui tutti possono accedere con una persona che fa da filtro per l'accettazione delle richieste e il ritorno delle informazioni volute.

Nel campo informatico è la cyber security ad occuparsi della sicurezza dei dati che viene attuata attraverso l'adozione di misure idonee a salvaguardare le informazioni sensibili per la sicurezza.

Il suo scopo è quello di difenderci dal

- Cybercrimine: include attori singoli o gruppi che attaccano i sistemi per ottenere un ritorno economico o provocare interruzioni nelle attività aziendali.

- Cyberattacchi: hanno spesso lo scopo di raccogliere informazioni per finalità politiche.
- Cyberterrorismo: ha lo scopo di minare la sicurezza dei sistemi elettronici per suscitare panico o paura.

Le misure sono adottate attraverso delle valutazione quantitative idonee a preservare e mantenere la disponibilità, la riservatezza e l'integrità del dato informativo.

Tra le misure a cui guarda chi redige un piano di sicurezza informatica c'è quello della valutazione del livello delle criticità, le utenze di riferimento, criteri di accesso, restrizioni normative sulla processazione dei dati, l'hardware e il software da adottare. Importanti sono questi ultimi due, insieme al fattore umano, perché spesso rappresentano per i malintenzionati i bersagli prediletti nel caso in cui ci siano degli errori di progettazione, realizzazione degli stessi oppure di non rispetto delle policy per l'uso della rete informatica.

Oggi la definizione classica di sicurezza informatica è "l ' adozione di misure idonee a salvaguardare le informazioni sensibili per la sicurezza."

Capitolo 1. 2. Paragrafo Tipologie

La cyber security viene organizzata, tenendo conto della legislazione vigente, guardando in tre direzioni che sono: sicurezza fisica, sicurezza logica, sicurezza organizzativa.

La sicurezza fisica rappresenta l'adozione di misure atte a controllare gli aspetti fisici ai dati informativi e comunque alle risorse e alle strutture che li ospitano a cui fanno accesso solo le persone identificate ed autorizzate. Questo tipo di sicurezza garantisce l'affidabilità, l'efficienza e la continuità dei dispositivi, delle strutture logistiche, e dei servizi strutturali.

Le misure di sicurezza da prendere in considerazione sono:

- Continuità della corrente elettrica e di altri servizi base;
- Sistemi ridondanti o disponibilità di risorse alternative per l‘immediato ripristino a seguito di guasti hw;
- Presenza di più canali trasmissivi differenziati oltre che dal fornitore anche nel cablaggio;
- Disponibilità di sedi (geograficamente distanti) e risorse alternative per il ripristino, a breve e medio termine a seguito di eventi eccezionali ;
- Controllo del materiale in uscita;
- Controllo del materiale in entrata;
- Controllo degli accessi fisici;
- Adeguatezza degli ambienti rispetto alle caratteristiche del territorio (sismicità, soggetto ad esondazioni o inondazioni, umidità);
- Adeguatezza degli ambienti rispetto a possibili accessi fraudolenti
- Soluzione di rilevamento e gestione incendi;
- Osservazione normative sulla sicurezza luoghi di lavoro;
- Copie di sicurezza.

La sicurezza logica riguarda l‘adozione di soluzioni che controllano gli accessi logici ai dati informativi e alle risorse che li ospita, consentendo l‘accesso alle sole entità identificate e autorizzate. Per accessi logici si intendono gli accessi telematici alle risorse. La sicurezza logica deve gestire la sicurezza dei canali di comunicazione interessati garantendo la riservatezza, l‘integrità e la disponibilità in tutte le fasi in cui vengono scambiate le informazioni. Particolare attenzione viene data al software, alla sua programmazione, alla gestione delle anomalie e alle modalità di utilizzo.

Le misure di sicurezza logiche da prendere in considerazione sono:

- Continuità dei servizi;
- Gestione backup;
- Gestione accessi logici ai sistemi/risorse informative;

- Configurazione della rete;
- Definizione profili e privilegi di accesso;
- Monitoraggio qualità dei sistemi e dei servizi;
- Sistema di monitoraggio allarmi e anomalie;
- Sistemi antivirus;
- Aggiornamenti di sicurezza dei sistemi/software di base o altri applicativi.

La sicurezza organizzativa è data dalla corretta definizione e assegnazione di ruoli e responsabilità nel rispetto della compatibilità di incarichi. Nell‘ambito di questa sicurezza si guarda alla definizione e alla gestione, conduzione e verifica del sistema. Vengono definite le regole da attuare e rispettare.
Le misure di sicurezza organizzativa sono

- Separazione ambiente di test e sviluppo;
- Formazione del personale;
- Regole di policy;
- Definizione di gerarchie , incarichi , responsabilità

.

CAPITOLO 2.
IEC

L'IEC[1] è un'organizzazione globale senza scopo di lucro, ha sede a Ginevra e il suo lavoro riguarda la fornitura di norme tecniche per la progettazione e costruzione di infrastrutture di qualità e per il commercio internazionale di prodotti elettrici ed elettronici.

Facilita l'innovazione tecnica, lo sviluppo di infrastrutture a prezzi accessibili, l'accesso all'energia efficiente e sostenibile, l'urbanizzazione intelligente e i sistemi di trasporto, la mitigazione dei cambiamenti climatici e aumenta la sicurezza delle persone e dell'ambiente.

L'IEC riunisce più di 170 paesi fornendo una piattaforma di standardizzazione globale, neutrale e indipendente a 20.000 esperti a livello globale.

Attraverso 4 Sistemi di valutazione della conformità i membri certificano che i dispositivi, i sistemi, le installazioni, i servizi e le persone funzionino come richiesto. L'IEC ha pubblicato circa 10.000 standard internazionali, insieme alla valutazione della conformità, fornendo il quadro tecnico che consente ai governi e alle aziende di costruire infrastrutture nazionali di qualità. Gli standard internazionali IEC fungono da base per la gestione del rischio e della qualità e vengono utilizzati nei test e nelle certificazioni per verificare che le promesse del produttore vengano mantenute.

Nella struttura dell‘IEC molta importanza hanno i comitati nazionali che forniscono le competenze di gestione e inviano esperti per rappresentare le esigenze nazionali nel campo della standardizzazione e della valutazione della conformità.

Al momento dell'ammissione, a ogni Stato è assegnato un membro IEC che permette di rappresentare pienamente tutti gli interessi nazionali privati e pubblici nel campo elettrico ed elettronico.

L'IEC offre loro un forum internazionale neutrale e indipendente in cui spesso esperti di fama mondiale dell'industria, del governo, del mondo accademico e dei gruppi di utenti, possono sedersi insieme e trovare consenso su soluzioni a grandi sfide tecniche.

Per quanto riguarda i membri sono distinti in membri a pieno titolo o membro associato.

Membro a pieno titolo dell'IEC è qualsiasi paese in grado di dimostrare che il proprio Comitato Nazionale è stato costituito in conformità con gli Statuti e le Regole di procedura dell'IEC. I membri a pieno titolo di IEC, previo pagamento della quota associativa annuale, hanno la possibilità di invitare esperti a partecipare attivamente a qualsiasi comitato/sottocomitato tecnico di loro scelta. Possono anche candidarsi per posizioni e funzioni dirigenziali e hanno diritto di voto nell'Assemblea generale dell'IEC.

Gli individui o le aziende non possono diventare membri dell'IEC. Possono partecipare all'IEC solo attraverso il loro Comitato Nazionale.

Gli individui sono distinti in esperti e delegati .

Alcune organizzazioni che hanno un rapporto formale con l'IEC possono anche nominare esperti in determinati gruppi di lavoro e gruppi di progetto di comitati tecnici (TC) e sottocomitati (SC).

Gli esperti partecipano al lavoro tecnico di IEC a titolo personale e non rappresentano la loro azienda/organizzazione o NC. Le procedure per la nomina degli esperti sono descritte nelle Direttive IEC.

I delegati partecipano ai TC/SC per rappresentare gli interessi di un NC. Ciascun CN designa un Capo delegazione che parli e voti a nome del CN durante la riunione del TC/SC. Gli altri membri della delegazione NC possono parlare ma non votare, ogni paese ha un solo voto.

I membri si raggruppano in Tc (technical committees) e quelli affini al campo informatico sono:

- SyC città intelligenti e aspetti elettrotecnici delle Smart Cities,

- SyC energia intelligente,
- JTC ISO/IEC 1 Tecnologie dell'informazione,
- ISO/IEC JTC1/SC2 Set di caratteri codificati,
- ISO/IEC JTC 1/SC 6 Telecomunicazioni e scambio di informazioni tra sistemi,
- ISO/IEC JTC1/SC7 Ingegneria del software e dei sistemi,
- ISO/IEC JTC1/SC17 Tessere e dispositivi di sicurezza per l'identificazione personale,
- ISO/IEC JTC1/SC22 Linguaggi di programmazione, loro ambienti e interfacce software di sistema,
- ISO/IEC JTC1/SC23 Supporti registrati digitalmente per lo scambio e l'archiviazione di informazioni,
- ISO/IEC JTC1/SC24 Computer grafica, elaborazione di immagini e rappresentazione di dati ambientali,
- ISO/IEC JTC1/SC25 Interconnessione di apparecchiature informatiche, ISO/IEC JTC 1/SC 27 Sicurezza informatica, sicurezza informatica e tutela della privacy,
- ISO/IEC JTC1/SC28 Attrezzatura da ufficio,
- ISO/IEC JTC 1/SC 29 Codifica di informazioni audio, immagini, multimediali e ipermediali,
- ISO/IEC JTC 1/SC 31 Tecniche di identificazione automatica e acquisizione dati,
- ISO/IEC JTC 1/SC 32 Gestione e interscambio di dati,
- ISO/IEC JTC 1/SC 34 Descrizione del documento e linguaggi di elaborazione,
- ISO/IEC JTC 1/SC 35 Interfacce utente,
- ISO/IEC JTC 1/SC 36 Tecnologia dell'informazione per l'apprendimento, l'istruzione e la formazione,
- ISO/IEC JTC 1/SC 37 Biometrica,

- ISO/IEC JTC 1/SC 38 Cloud Computing e Piattaforme Distribuite,
- ISO/IEC JTC 1/SC 39 Sostenibilità, IT e data center,
- ISO/IEC JTC 1/SC 40 IT Service Management e IT Governance,
- ISO/IEC JTC 1/SC 41 Internet delle cose e gemello digitale,
- ISO/IEC JTC 1/SC 42 Intelligenza artificiale,
- ISO/IEC JTC 1/SC 43 Interfacce cervello-computer.

Importante funzione dell'IEC è quella della valutazione di conformità che si riferisce a qualsiasi attività che determina se un prodotto, un sistema, un servizio e talvolta le persone soddisfano i requisiti e le caratteristiche descritte in uno standard o in una specifica. Tali requisiti possono includere, ad esempio, prestazioni, sicurezza, efficienza, efficacia, affidabilità, durata o impatti ambientali come inquinamento o rumore. La verifica viene generalmente effettuata tramite test e/o ispezioni. Ciò può includere o meno la verifica in corso.

Prima che un prodotto possa entrare nel mercato, generalmente deve essere in grado di dimostrare all'acquirente o al regolatore che è sicuro e funziona come promesso in termini di efficienza energetica, affidabilità, sostenibilità e molti altri criteri e proprio a ciò serve la valutazione. La valutazione della conformità fornisce la prova necessaria, basata sugli standard. Con valutazione di conformità:

- I governi possono verificare più facilmente la resilienza delle infrastrutture e sono maggiormente in grado di proteggere le loro popolazioni da rischi inutili;
- Gli assicuratori ottengono la conferma che i rischi sono stati gestiti correttamente e le relative considerazioni sulla sicurezza incluse;
- Gli acquirenti ricevono una prova della sicurezza, delle prestazioni e dell'affidabilità di un prodotto o sistema ;

- Gli investitori possono fidarsi che siano state applicate le migliori pratiche a livello di settore e che il loro investimento sia il più sicuro possibile;
- Gli utenti delle apparecchiature e i consumatori possono essere certi che i dispositivi elettrici ed elettronici siano sicuri da usare e soddisfano le aspettative.

L'IEC fornisce un quadro che supporta tutti i tipi di valutazione della conformità e consente che i test siano trasparenti, prevedibili, comparabili e convenienti. Gli standard internazionali IEC insieme alla valutazione della conformità aiutano a ridurre le barriere commerciali causate dai diversi criteri di certificazione nei diversi paesi. I sistemi di valutazione della conformità IEC (CA) aiutano anche a eliminare ritardi e spese significative per test e approvazioni multiple.

La valutazione di conformità ha tre livelli:

- Primo livello (CA) - autodichiarazione: livello più basso di attendibilità -Il produttore o il fornitore dichiara che un prodotto è conforme a una determinata norma o specifica e rilascia una SDoC (dichiarazione di conformità del fornitore). Questa forma di CA è abbastanza comune per i prodotti a basso rischio. Fornisce ai partner commerciali la certezza che uno standard è stato seguito. È fondamentalmente una forma di informazione. Il marchio CE europeo è un esempio di SDoC. Applicando il marchio CE su un prodotto, il produttore conferma che il prodotto soddisfa i requisiti di sicurezza, salute o ambiente dell'UE e soddisfa i requisiti di valutazione della conformità delle Direttive UE. Questa è la forma più economica e semplice di CA perché non esiste una verifica indipendente; l'affidabilità dipende direttamente dalla credibilità del fornitore;

- CA di seconda parte: livello medio di affidabilità -Una persona o un'organizzazione che ha un interesse diretto a verificare le prestazioni di un prodotto svolge questo tipo di attività di CA. In genere, un cliente molto grande, importante o esigente (governo, importante acquirente o produttore) metterà in atto la propria CA per i prodotti o servizi che acquista. Ciò può includere strutture di prova e speciali procedure di valutazione condotte per verificare la qualità dei prodotti forniti. Lo scopo è solitamente quello di ottenere la garanzia che un fornitore abbia effettuato una CA di prima parte secondo le specifiche del cliente;
- CA di terze parti: alto livello di affidabilità - Questa attività di CA è svolta da una persona o un'organizzazione indipendente dal venditore o dall'acquirente. Questo è solitamente chiamato certificazione e fornisce il massimo livello di garanzia per quanto riguarda lo stato di un determinato prodotto. La CA di terze parti è più costosa della CA di prima parte, poiché gli organismi di certificazione (CB) sono generalmente società a scopo di lucro. L'AC di terze parti viene applicata quando la legislazione lo impone, ad esempio a causa del livello di rischio o quando un mercato è abbastanza grande da giustificare la spesa.

L'IEC supporta tutte e tre le forme di CA e gestisce anche i sistemi di CA IEC, i cui membri forniscono CA di terze parti. Questi sistemi offrono l'unica forma standardizzata a livello globale di valutazione della conformità che copre l'elettrotecnica e rappresentano il più grande accordo multilaterale funzionante al mondo.

La valutazione è fatta dai CAB (Conformity Assessment Board) che si occupa della gestione, anche operativa e finanziaria, delle attività di valutazione della conformità (CA) della Commissione. Il CAB rappresenta la comunità di valutazione della conformità IEC, è un organo decisionale che si riferisce