Seminario 3

Cyber attacchi

Negli ultimi anni, si è registrato un aumento significativo degli attacchi alle infrastrutture digitali, con conseguenti maggiori costi sia per implementare misure preventive che per mitigare i danni causati dagli attacchi stessi.

In risposta a questa crescente minaccia, l'Europa ha introdotto la direttiva **NIS 2** (Network and Information Security), che definisce i requisiti minimi di sicurezza per i sistemi operanti sul territorio europeo. Lo scopo principale della direttiva è rafforzare la resilienza delle infrastrutture e migliorare la capacità di risposta agli incidenti, fornendo linee guida chiare nel campo della **cybersecurity** e nella protezione delle infrastrutture critiche.

Rispetto alla precedente direttiva NIS, la NIS 2 introduce obblighi più stringenti, ampliando le responsabilità per le organizzazioni e garantendo un approccio uniforme e coordinato a livello europeo nella gestione della sicurezza informatica.

Team e Certificazioni

Un team di sicurezza informatica di successo si basa su una forte collaborazione tra i membri e con le parti interessate esterne. È importante disporre di un'organizzazione flessibile con competenze diversificate e capacità di agire rapidamente in caso di minacce.

Le certificazioni di sicurezza informatica, come **ISO 27001**, forniscono linee guida per la gestione della sicurezza delle informazioni e dimostrano l'impegno dell'organizzazione per la sicurezza informatica.

Definizione. ISO 27001 (o ISMS) è uno standard internazionale che fornisce un quadro per la creazione, l'implementazione, il mantenimento e il miglioramento continuo di un **sistema di gestione della sicurezza delle informazioni** (ISMS). Lo standard specifica i requisiti per stabilire, implementare, mantenere e migliorare continuamente un ISMS all'interno del contesto dell'organizzazione.

Le organizzazioni devono affrontare una vasta gamma di minacce informatiche, tra cui attacchi di phishing, social engineering, violazioni dei dati e attacchi ransomware. È fondamentale comprendere il panorama delle minacce e adottare misure preventive per mitigare i rischi.

Protezione della posta elettronica

La posta elettronica è un vettore comune per gli attacchi informatici. È fondamentale implementare misure di sicurezza efficaci per filtrare le e-mail dannose e proteggere le informazioni sensibili.

Consapevolezza, sicurezza OT e regionale

La formazione e la sensibilizzazione sulla sicurezza informatica sono fondamentali per responsabilizzare i dipendenti e promuovere comportamenti sicuri. Simulazioni, newsletter, corsi di formazione e altre iniziative possono contribuire a migliorare la consapevolezza e le competenze in materia di sicurezza informatica.

La sicurezza **informatica OT** (Operational Technology) si concentra sulla protezione dei sistemi di controllo industriale e delle tecnologie operative. Un approccio "defense-in-depth" con interventi a più livelli è essenziale per proteggere le infrastrutture critiche.

Le organizzazioni devono adattare le proprie strategie di sicurezza informatica per soddisfare le esigenze specifiche di diverse regioni e contesti locali. Un team di sicurezza informatica regionale può fornire supporto e guida per migliorare la posizione di sicurezza informatica in diverse aree geografiche (e.g., è il caso delle multinazionali).

Gestione del rischio dei fornitori, tecnologia e fattore umano

Le organizzazioni devono valutare e gestire i rischi per la sicurezza informatica associati alla propria catena di approvvigionamento. È importante stabilire un quadro di governance per garantire che i fornitori soddisfino gli standard di sicurezza richiesti.

La tecnologia svolge un ruolo fondamentale nella sicurezza informatica, ma non è l'unica soluzione. È essenziale scegliere le tecnologie appropriate, gestirle correttamente ed equilibrarle con altri aspetti della sicurezza informatica, come la formazione e i processi.

Le persone sono spesso l'anello più debole nella sicurezza informatica. La formazione, la sensibilizzazione e una cultura di sicurezza informatica possono contribuire a rafforzare il "firewall umano" e mitigare i rischi associati all'errore umano.

Cyber intelligence

La **cyber intelligence** fornisce informazioni sulle minacce emergenti e aiuta le organizzazioni a prevedere e prevenire gli attacchi informatici. È importante rimanere aggiornati sulle ultime minacce e condividere informazioni con partner, esperti e autorità competenti.

Info

La cyber intelligence è il processo di raccolta, analisi e diffusione di informazioni sulle minacce informatiche. La cyber intelligence aiuta le organizzazioni a comprendere il panorama delle minacce, identificare le vulnerabilità e adottare misure preventive per proteggersi dagli attacchi informatici.