BIBLIOTECA

I rischi informatici e le misure di sicurezza negli ambienti digitali

Introduzione

Salve,

oggi parleremo di sicurezza informatica e dei rischi connessi agli ambienti digitali.

Definizione di sicurezza

L'idea di sicurezza, o meglio la percezione di essere al sicuro da eventuali pericoli, cambia profondamente a seconda dell'ambiente in cui ci muoviamo.

Il fattore che più di ogni altro fa scalare la percezione del livello di sicurezza dell'ambiente che ci circonda è la non prevedibilità di quello che può accadere intorno a noi.

La stessa etimologia della parola sicurezza - dal latino "sine cura" cioè senza preoccupazioni - ci aiuta a darne una definizione più corretta: la sicurezza è la "conoscenza che l'evoluzione di un sistema non produrrà stati indesiderati", o più semplicemente la consapevolezza che quello che facciamo e quello che avviene intorno a noi non provocherà danni, né per noi, né per gli altri.

Sicurezza e conoscenza sono dunque due elementi strettamente collegati. Conoscere spazi e regole dell'ambiente con cui interagiamo ce lo rende naturalmente meno pericoloso e più confortevole.

Se questo è vero per gli ambienti fisici, la stessa regola è altrettanto valida anche quando operiamo in ambienti digitali.

Introduzione agli ambienti digitali

In senso lato possiamo considerare ambienti digitali tutti gli spazi virtuali, come la casella di posta elettronica, i social network, i programmi e le applicazioni che utilizziamo, i videogiochi, il web e la stessa rete internet.

Per ambienti digitali si possono intendere, quindi, tutti quegli spazi virtuali accessibili attraverso l'intermediazione di dispositivi digitali, come computer, tablet, smartphone, consolle per i videogiochi o altre tipologie di device.

La crescente centralità economica e sociale degli ambienti digitali li ha resi nel tempo luoghi sempre meno sicuri e sempre più appetibili per chi, mosso da cattive intenzioni, vuole trarne profitto.

Ormai chiunque, possiamo dire, è costantemente connesso attraverso il web, i social network, le community o quant'altro, con la possibilità di accedere in qualsiasi momento a un'enorme quantità di contenuti e servizi. Oltre agli aspetti positivi di tutto ciò, è importante tenere sempre bene a mente che ogni accesso rappresenta un potenziale varco per chi è intenzionato a compromettere la nostra sicurezza.

Sicurezza informatica

In questo contesto di estrema complessità, le misure orientate alla sicurezza informatica degli utenti rivestono un ruolo essenziale per garantire lo sviluppo socio-economico delle moderne comunità.

La sicurezza informatica, intesa come l'insieme dei mezzi e delle tecnologie volti alla protezione dei sistemi informatici, diventa parte integrante dell'infrastruttura che sorregge gli ambienti digitali, consentendo agli utenti di scambiare informazioni e fruire contenuti senza il timore di imbattersi in potenziali pericoli.

Le misure di sicurezza

Le misure di sicurezza informatica per gli ambienti digitali, così come avviene per quelli fisici, possono essere diverse a seconda delle loro specifiche finalità.

Per fare qualche parallelismo, prendiamo ad esempio la sicurezza stradale.

La sicurezza stradale può essere declinata in:

- **sicurezza fisica dell'infrastruttura**, che viene assicurata con la manutenzione delle strade, assicurandosi che siano sempre integre, ben illuminate, con la segnaletica posta in evidenza e dotate di ogni caratteristica che le possa rendere più sicure per gli automobilisti che le percorrono
- **sicurezza dei veicoli** su cui viaggiano gli automobilisti, che devono essere solidi e dotati delle tecnologie che minimizzano i rischi per le persone che li guidano
- e **fattore umano**, relativo non solo alla capacità di guidare in maniera corretta, rispettando i limiti e le disposizioni stabilite dal codice della strada, ma anche alla prudenza che deriva proprio dalla piena consapevolezza dei possibili pericoli

In maniera del tutto speculare, la sicurezza informatica può essere suddivisa in tre principali ambiti di applicazione, integrati l'uno con l'altro per assicurare un presidio più completo possibile degli ambienti digitali:

- **la sicurezza fisica**
- **la sicurezza logica**
- **e il fattore umano**

La sicurezza fisica

La **sicurezza fisica** riguarda le infrastrutture tecnologiche che consentono l'accesso ai dispositivi o, più in generale, a qualunque elemento su cui viaggiano i dati. In questo caso, le misure di sicurezza informatica si rifanno alle misure di sicurezza di qualunque altro ambiente fisico, per cui potrebbe riguardare il presidio degli ambienti che ospitano i server, ad esempio prevedendo l'installazione di porte blindate, oppure un servizio di sorveglianza, o, infine, l'identificazione puntuale del personale che accede alle strutture.

Sicurezza logica

Con **sicurezza logica,** invece, si fa riferimento alle tecniche per mettere al riparo i dati e le applicazioni da accessi non autorizzati.

Questo avviene prevalentemente attraverso le impostazioni di autenticazione (le password, ad esempio) e il tracciamento degli accessi alle piattaforme digitali da parte degli utenti.

Fattore umano

Per quanto riguarda invece il **fattore umano**, questo entra in gioco in riferimento alla **sicurezza degli ambienti digitali**, in quanto ogni utente deve essere in grado di garantirla in totale autonomia.

Abitando gli ambienti digitali, l'utente deve assumere comportamenti in grado di prevenire le possibili minacce e mitigare il rischio di attacchi informatici.

Si parla in questo caso di prevenzione della vulnerabilità dovuta al **fattore umano**, imputabile a elementi come la disattenzione, l'incompetenza, la disinformazione e più in generale all'assenza di **competenze** volte a rendere gli utenti più consapevoli dei pericoli presenti nei sistemi informatici.

In un sistema integrato di sicurezza informatica multilivello, spesso il fattore umano rappresenta l'anello più vulnerabile della catena. Proprio partendo da questa considerazione, la maggior parte degli attacchi informatici sono progettati proprio per colpire innanzitutto l'utente finale, attraverso email ingannevoli o file infetti da malware, ovvero programmi malevoli che si auto-installano sui dispositivi per comprometterne la sicurezza.

Approccio integrato

A fronte di queste considerazioni, diventa sempre più indispensabile per le organizzazioni adottare un modello che includa una strategia complessiva anche per la sicurezza informatica.

Questa strategia deve tener conto anche del livello di consapevolezza dei rischi informatici da parte di tutte le figure coinvolte nei processi di trasformazione digitale.

Per farlo occorrono investimenti non solo in tecnologie, ma anche nello sviluppo delle competenze digitali e trasversali.

E, focalizzandoci ancor di più sul nostro caso specifico, per la Pubblica Amministrazione risulta ancor più necessario garantire la protezione della grande messe di dati che si trova a gestire investendo in risorse

tecnologiche, ma anche umane in maniera proporzionale al valore dell'informazione pubblica in suo possesso.

Conclusioni

Bene, in questa videolezione abbiamo avuto modo con di introdurre i principali rischi e le misure di sicurezza necessarie alla protezione degli ambienti digitali che “abitiamo”.

Non mi resta che augurarvi buon proseguimento!