Fastweb Digital Academy

CIBERSICUREZZA: INTRODUZIONE

Docente
Guglielmo Bondioni

PROTEZIONE DEI SISTEMI INFORMATICI

Gestione delle vulnerabilità tecniche

È la pratica di gestire eventuali falle tecniche nel sistema che potrebbero consentire a un attaccante di aggirare il controllo degli accessi.

Monitoraggio e gestione degli incidenti

È l'insieme delle pratiche e delle tecnologie utili a *rilevare*, *contenere* e *rimediare* a un'intrusione, a un abuso degli accessi al sistema o ad altri attacchi tecnici.

PROTEZIONE DEI SISTEMI INFORMATICI

Controllo degli accessi

È la principale misura a difesa dei sistemi: è ciò che consente solo alle persone autorizzate di accedere e usare uno strumento informatico e/o un dato.

Il controllo degli accessi consiste in:

- **autenticazione**: *accertare l'identità* della persona che intende accedere a un sistema
- **autorizzazione**: *consentire* alla persona autenticata di usare le funzioni *che le sono state precedentemente accordate*;
- **tracciamento**: *tenere un registro* degli accessi e operazioni compiute sul sistema dalle persone

IL RUOLO DELLE PERSONE

Nella gestione delle vulnerabilità tecniche

Impostare e gestire i sistemi di controllo accessi e le altre contromisure.

Nel monitoraggio

Ciascuno di noi detiene le chiavi per accedere a numerosi sistemi informatici

Nel controllo degli accessi

Ciascuno di noi detiene le chiavi per accedere a numerosi sistemi informatici

MISURE TECNICHE DA ADOTTARE

Ciascuno di noi, sui propri dispositivi, ha la responsabilità di:

- Controllo accessi
- Cifratura dei dati (encryption)
- Aggiornamento del software (patching)
- Installazione da fonti note / autorizzate

Fastweb Digital Academy

MISURE TECNICHE: CONTROLLO ACCESSI

Sui computer:

1. creare account utente con credenziali (es. password)
2. impostare il computer per richiedere le credenziali:
   - all'avvio
   - al blocco dello schermo

Su telefoni e tablet:

1. definire un PIN o password
2. opzionalmente abilitare l'impronta digitale o il riconoscimento del viso
3. Impostare il dispositivo per richiedere PIN o impronta:
   - all'avvio
   - al blocco dello schermo

MISURE TECNICHE: CIFRATURA

Sui computer, abilitare la cifratura nativa del sistema operativo:

- Windows: "Crittografia del dispositivo" o BitLocker
- Mac: FileVault
- Linux: dm-crypt ("full disk encryption")

Su telefoni e tablet, basta impostare un PIN per l'avvio.

Fatto questo, la cifratura si attiva automaticamente.

MISURE TECNICHE: AGGIORNAMENTO

Su computer, telefoni, tablet:

1. **Installare gli aggiornamenti** il più presto possibile:
   - per il sistema operativo
   - per software e app
2. **Attenzione:**
   - prelevare gli aggiornamenti solo dalle fonti ufficiali
   - MAI seguire link che propongono aggiornamenti

MISURE TECNICHE: FONTI DEL SOFTWARE

Sui computer:

1. Installare software solo dagli store ufficiali o dal sito del produttore
2. Evitare siti che redistribuiscono software
3. MAI cliccare su link ricevuti via chat o email o trovati per caso: verificare sempre dalla fonte ufficiale

Su telefoni e tablet:

1. Installare app solo dagli store ufficiali
2. MAI seguire link per installare app