Definizioni e Concetti chiave

Security Awareness

Definizioni rilevanti

Vulnerabilità	Una vulnerabilità può essere intesa come una componente di un sistema informatico, in corrispondenza alla quale le misure di sicurezza sono assenti, ridotte o compromesse, il che rappresenta un punto debole del sistema e consente a un eventuale aggressore di compromettere il livello di sicurezza dell'intero sistema.
Minaccia	È l'elemento attivo di potenziale innesco di un rischio. La minaccia è l'agente che, sfruttando una vulnerabilità, potrebbe portare ad un attacco o a un danno al sistema.
Rischio	È il rischio di incorrere in perdite economico/finanziarie in seguito al verificarsi eventi accidentali o di azioni dolose inerenti il sistema informatico (hardware, software, banche dati, etc.). $Rischio = Magnitudo \times Probabilità$
Controlli	Processo di identificazione e valutazione dei rischi e la creazione di un piano che consenta di contenere o tenere sotto controllo quelli individuati e le loro conseguenze ripercuotibili su una azienda.
Asset	Qualsiasi bene di proprietà di un'azienda (macchinari, merci, ecc.), che possa essere monetizzato e quindi usato per il pagamento di debiti.

Definizioni rilevanti

Possono ridurre
o introdurre

Vulnerabilità

Porta ad un

Può sfruttare

Controlli

Minaccia

Aumenta il

Rischio

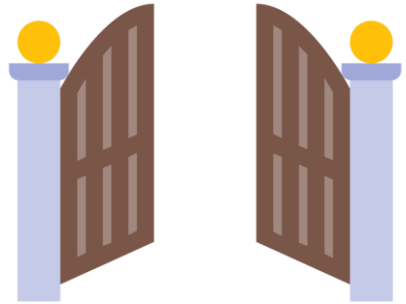
Che si riversa su

Asset

Minaccia vs Attacco

Minaccia

È una potenziale violazione di sicurezza: un cancello aperto è una minaccia, non un attacco.



Attacco

Un attacco è il tentativo, intenzionale o no, di creare una falla nella sicurezza arrecando più o meno danno agli asset di una compagnia.

Può essere di tipo:

- Attivo
- Passivo
- Interno
- Esterno

Un vettore d'attacco è il modo in cui un attacco viene perpetrato.

Categorie di violazioni di sicurezza

Confidenzialità

Cosa è: proprietà delle informazioni di non essere rese disponibili o divulgate a individui, entità o processi non autorizzati

Quando viene meno: lettura non autorizzata di dati riservati.

Integrità

Cosa è: proprietà delle informazioni di non essere alterate nella loro correttezza.

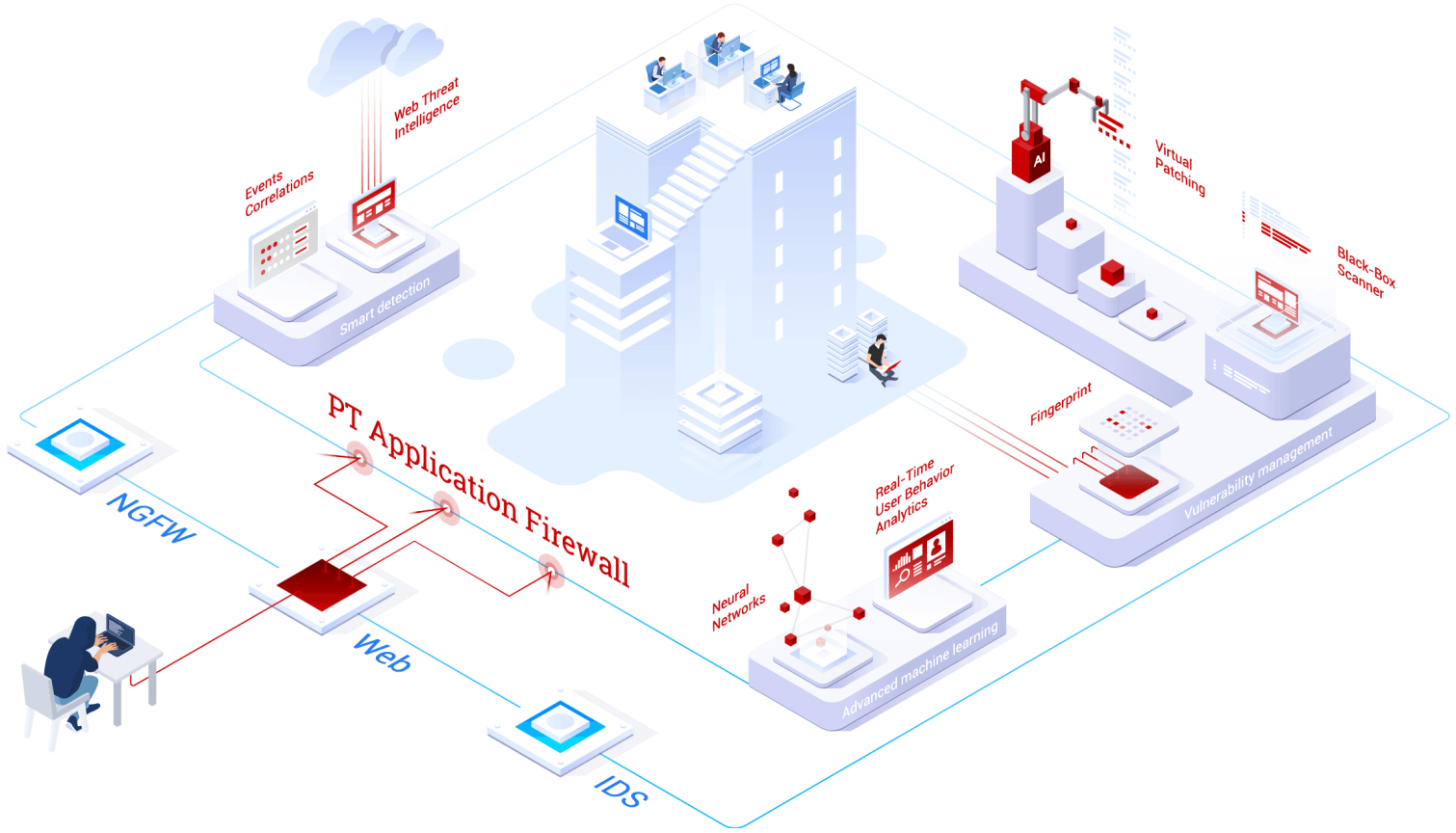
Quando viene meno: modifica non autorizzata di dati.

Disponibilità

Cosa è: proprietà delle informazioni di essere sempre disponibili.

Quando viene meno: non disponibilità dei dati.

Sfide per la sicurezza



In una grande azienda organizzata con un team dedicato alla sicurezza ci si sente sicuri da minacce e rischi.

Next Generation Firewall, Endpoint Protection System e altri apparati di sicurezza fanno il loro lavoro tenendo l'azienda e i suoi dipendendi al sicuro.

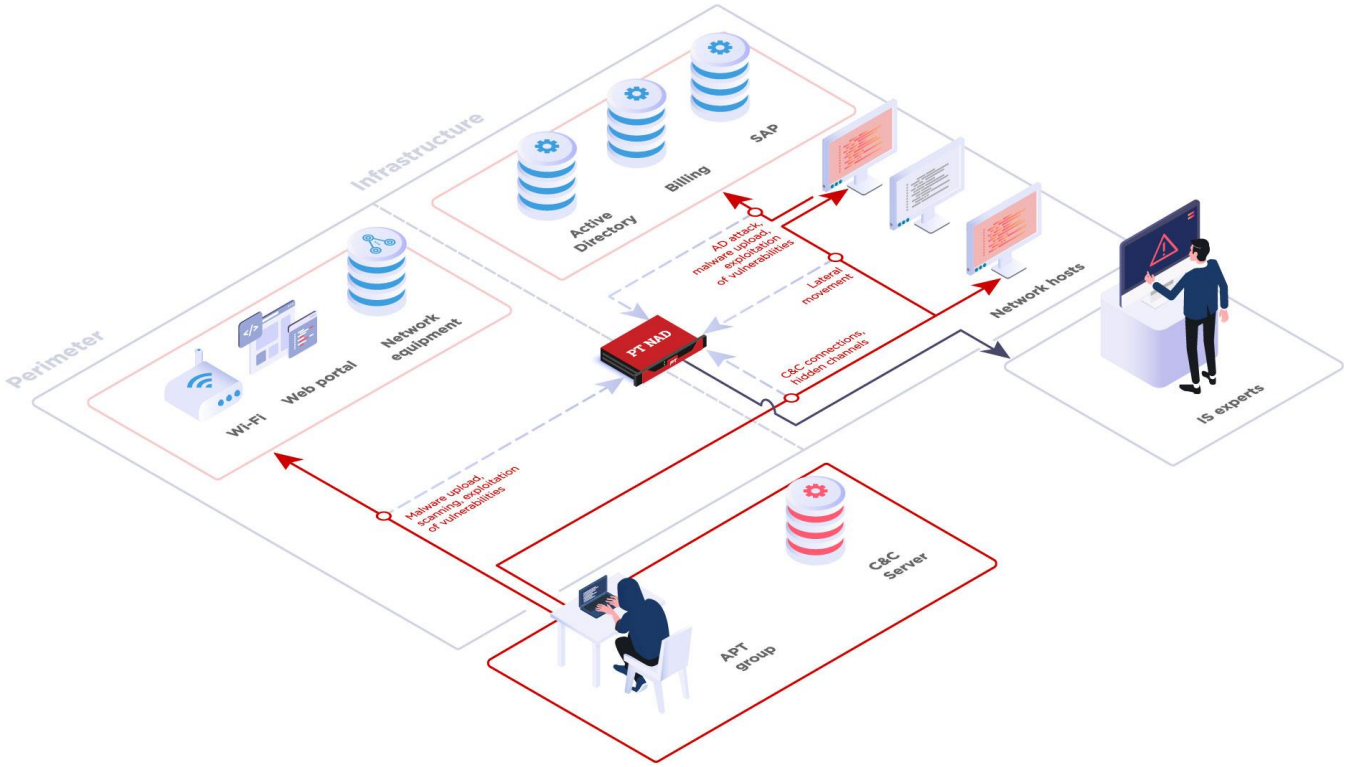
La sicurezza informatica non dipende però solo dalla sicurezza dei protocolli e dell'hardware, ma soprattutto dagli **utenti**.

Sfide per la sicurezza

Ad un generico attaccante basta sfruttare una singola vulnerabilità, mentre al contrario è necessario eliminare (o mitigare) tutti i possibili punti di fallimento della sicurezza, cioè le vulnerabilità.

La sicurezza non è concepita come un beneficio, fin quando non succede un incidente.

La sicurezza richiede continuo monitoraggio, aggiornamento e risorse.



«Meglio un investimento in sicurezza oggi, che inseguire dati persi domani!»

InnovaPuglia S.p.A.

CSIRT PUGLIA