ditech
Improve your performance

SICUREZZA DELLE INFORMAZIONI

VULNERABILITY SCAN

Il servizio Vulnerability Scan risponde all'esigenza di verificare la **presenza di vulnerabilità informatiche conosciute e classificate**, tramite strumenti automatici, con azioni ricorsive.

A COSA SERVE

I repentini cambiamenti e le continue evoluzioni tecnologiche nel campo dell'informazione e della comunicazione hanno cambiato le regole su cui società e mercato avevano sempre vissuto. Poiché non è possibile contrastare o rinunciare all'utilizzo di **nuove tecnologie**, le imprese devono **prendere coscienza dei rischi** che vi sono associati; e per garantire/gestire la sicurezza devono coinvolgere diverse figure professionali, quali sistemi informativi, amministrazione, controllo di gestione, direzione ecc.
Per queste ragioni spesso le aziende non hanno un quadro complessivo, chiaro e condiviso del loro livello di sicurezza e delle relative strategie adottate.
Le aziende, per tutelarsi in modo adeguato, devono **valutare i rischi** e **proteggersi dalle minacce sia esterne sia interne**, evitare usi illeciti e furti di informazioni e garantire l'adeguato supporto ai processi "core". Il primo passo per proteggersi è conoscere i rischi ai quali si è esposti e di conseguenza dotarsi una adeguata strategia di sicurezza per "custodire" e proteggere in maniera appropriata il proprio patrimonio.

A CHI SERVE

Tutti i retailer.

BENEFICI

- Contribuisce a migliorare e mantenere lo stato di sicurezza dei sistemi informativi e la salvaguardia del patrimonio informativo aziendale, grazie al controllo ricorsivo con strumenti sempre aggiornati e grazie al supporto di personale specializzato.
- Fornisce i report formali richiesti dallo standard PCI-DSS (*).

ditech
Improve your performance

COME FUNZIONA

Alla base del servizio vi è un **database** delle vulnerabilità, mantenuto sempre **aggiornato a livello mondiale**, che costituisce il riferimento delle verifiche.

Strumenti automatici, opportunamente configurati, effettuano verifiche confrontando le evidenze rilevate sull'architettura dell'azienda con il database delle vulnerabilità conosciute. Le **attività automatizzate** vengono integrate con **attività manuali** di normalizzazione dei risultati e di verifica di eventuali falsi positivi.

CARATTERISTICHE

Il servizio prevede diverse attività, tra le quali:

- **rilevamento di vulnerabilità** presenti nell'infrastruttura target;
- **ranking** delle vulnerabilità secondo lo schema di valutazione CVSS;
- definizione di **piani di rientro** mirati alla risoluzione delle vulnerabilità e la mitigazione dei rischi;
- definizione di piani per la gestione di **falsi positivi** e del processo di "dispute management";
- predisposizione di un documento di **reportistica** sulle verifiche periodiche di vulnerabilità, richiesto ai fini di conformità al requisito 11.2.2 dello schema PCI-DSS.

Il servizio è erogato in quattro fasi principali:

- **Programmazione**: definizione operativa e tuning sulle esigenze;
- **Setup**: predisposizione e configurazione degli strumenti;
- **Erogazione**: esecuzione del servizio, indicazione sulle attività di "remediation" e gestione dei falsi positivi;
- **Certificazione**: se funzionale al mantenimento o al conseguimento della certificazione PCI, predisposizione della reportistica "Attestation of Scan Compliance" (AoSC) valida ai fini della certificazione PCI-DSS.