

Supporto di gestione per la sicurezza di Active Directory

Just IT fornisce un servizio dedicato a chi ha l'obiettivo di migliorare la **sicurezza dell'ambiente Active Directory** del proprio sistema informatico.

Nella pratica, il servizio si basa sull'esecuzione di vulnerability test su Active Directory: questo processo permette di identificare, quantificare e prioritizzare le vulnerabilità dell'ambiente in uso, e nello specifico viene realizzato utilizzando strumenti automatizzati con l'apporto dell'esperienza di professionisti che possono guidare un'azienda verso il raggiungimento di una gestione ottimale del proprio sistema informatico.

Insieme ai ruoli responsabili delle aziende, risulta agevole discutere i rapporti generati dai test effettuati che raccolgono le informazioni più importanti e stabiliscono una panoramica per una valutazione attraverso l'assegnazione di un punteggio sulla base di un modello e di regole definite, nonché la segnalazione dei Rischi evidenziati.

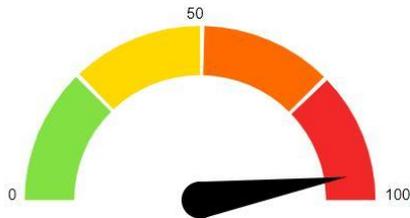
Lo scopo del servizio è quello di identificare le vulnerabilità che potrebbero essere sfruttate per compromettere la sicurezza di Active Directory, quantificare il rischio associato a ciascuna vulnerabilità, prioritizzare le vulnerabilità in base al rischio che rappresentano e pianificare un percorso di attività da intraprendere e di azioni correttive da implementare, sulla base delle indicazioni ottenute dai test effettuati, allo scopo di mitigare le vulnerabilità. Quali sono i vantaggi di utilizzare un servizio come questo? Presto detto:

- Riduzione del rischio di compromissione della sicurezza. Identificando e mitigando le vulnerabilità, è possibile ridurre il rischio di attacchi riusciti.
- Aumento della consapevolezza della sicurezza tra i dipendenti.
- Miglioramento della postura di sicurezza complessiva grazie all'inserimento di un componente importante di un programma di gestione della sicurezza completo.
- Miglioramento della conformità normativa. Molti standard di conformità richiedono l'esecuzione di vulnerability test periodici.

Active Directory Indicators

This section focuses on the core security indicators.
Locate the sub-process determining the score and fix some rules in that area to get a score improvement.

Indicators



Domain Risk Level: 95 / 100

It is the maximum score of the 4 indicators and one score cannot be higher than 100. The lower the better

[Compare with statistics](#)

[Privacy notice](#)



Risk model ?

Stale Objects	Privileged accounts	Trusts	Anomalies
Inactive user or computer	Account take over	Old trust protocol	Audit
Network topography	ACL Check	SID Filtering	Backup
Object configuration	Admin control	SIDHistory	Certificate take over
Obsolete OS	Control paths	Trust impermeability	Golden ticket
Old authentication protocols	Delegation Check	Trust inactive	Local group vulnerability
Provisioning	Irreversible change	Trust with Azure	Network sniffing
Replication	Privilege control		Pass-the-credential
Vulnerability management	Read-Only Domain Controllers		Password retrieval
			Reconnaissance
			Temporary admins
			Weak password

Legend:
■ score is 0 - no risk identified but some improvements detected
■ score between 1 and 10 - a few actions have been identified
■ score between 10 and 30 - rules should be looked with attention
■ score higher than 30 - major risks identified

Questo servizio, coerentemente con ogni altro servizio offerto da Just IT, prevede la calibrazione sulle singole realtà in oggetto: in particolare, la frequenza con cui è necessario eseguire vulnerability test su Active Directory dipende da diversi fattori, tra cui:

- La dimensione e la complessità dell'ambiente Active Directory.
- Il numero di modifiche apportate all'ambiente Active Directory.
- Il livello di rischio associato all'ambiente Active Directory.

In generale, è consigliabile eseguire vulnerability test su Active Directory almeno una volta all'anno, oppure più frequentemente se l'ambiente Active Directory è molto dinamico o se il livello di rischio associato all'ambiente è elevato.

Il servizio di **Supporto alla gestione della sicurezza di Active Directory**, non deve essere considerato la soluzione, ma un supporto per il raggiungimento e il successivo mantenimento di una postura di sicurezza adeguata è quindi **un importante tassello nella gestione della sicurezza dei sistemi informatici basati su soluzioni Microsoft**.

Ma sono molti gli aspetti da considerare e molti anche puramente procedurale: ad esempio è importante

- *Implementare politiche di sicurezza rigide.*
- *Formare i dipendenti sulla sicurezza.*
- *Tenere aggiornati i sistemi operativi e le applicazioni.*
- *Monitorare l'attività dei sistemi in uso.*
- *Implementare sistemi di rilevamento e risposta agli incidenti.*

Su ognuno di questi argomenti, e molto altro in materia di **Cybersecurity**, possiamo dire la nostra: confrontiamoci senza impegno, possiamo mettere a disposizione della tua organizzazione competenza ed esperienza che sicuramente renderanno ogni aspetto più semplice da considerare nell'ottica della salute dei tuoi sistemi e del tuo business.

Scopri come **Just IT** ti può aiutare ad individuare la tua personale strategia di Cyber Security: rivolgiti al tuo commerciale **JustIT** di riferimento o contattaci telefonando al numero **02 80582019** o scrivendo a **commerciale@justit.it**