ICTsystem
integration is now

Network Security Test

Servizio di valutazione e tuning delle infrastrutture di rete wired/wireless e dei sistemi di sicurezza ICT.

Introduzione

La diffusione delle tecnologie ICT, sempre più economiche e semplici da implementare, non è sempre supportata da un'adeguata conoscenza delle tecnologie e dai rischi derivanti da una errata implementazione delle stesse, con il rischio di esporre involontariamente i dati propri e di terze parti al rischio di accessi non controllati e perfino a manomissioni.

Gli errori più comuni sono anche quelli che più facilmente vengono utilizzati da utenti malintenzionati ovvero possono portare utenti inesperti a commettere danni involontari: spesso vengono rilevati account di servizio con password di default o banali, le reti wireless non sono dotate di controllo accessi e/o di crittografia del traffico, parametri di configurazione degli ambienti di sviluppo e test vengono rilasciati in produzione consentendo accessi non adeguatamente controllati.

Il servizio Network Security Test è applicabile ad infrastrutture ICT di varia complessità, sia nell'ambito di un audit più ampio sia nella verifica periodica della consistenza delle impostazioni di sicurezza implementate a seguito di modifica o introduzione di componenti e servizi.

Alcune aree di applicazione sono:

- sistemi di accesso Internet e posta elettronica;
- data center o parti di datacenter con servizi critici;
- reti wireless per l'accesso alla rete aziendale;
- reti wireless outdoor, ad esempio sistemi di video sorveglianza e controllo accessi;
- infrastrutture di interconnessione Intranet ed Extranet.

Descrizione del servizio

Il servizio Network Security Test è un servizio professionale che risponde primariamente all'esigenza di verificare il livello di sicurezza informatica di un sistema ICT o parte di esso.

Attraverso questo servizio è possibile mettere a confronto lo stato della rete sia con gli obiettivi e le politiche aziendali in essere, sia con le normative in vigore, avendo come obiettivi:

- la verifica del grado di adeguatezza ed applicabilità delle politiche di sicurezza aziendali per il sistema ICT in esame;
- la verifica dell'adeguatezza delle politiche implementate rispetto ai requisiti minimi imposti da norme legislative e regolamentazioni;
- la verifica del grado di efficacia, efficienza e robustezza delle contromisure tecnologiche adottate nei sistemi di sicurezza;
- la definizione delle eventuali contromisure necessarie per mitigare i rischi evidenziati durante l'attività di verifica.

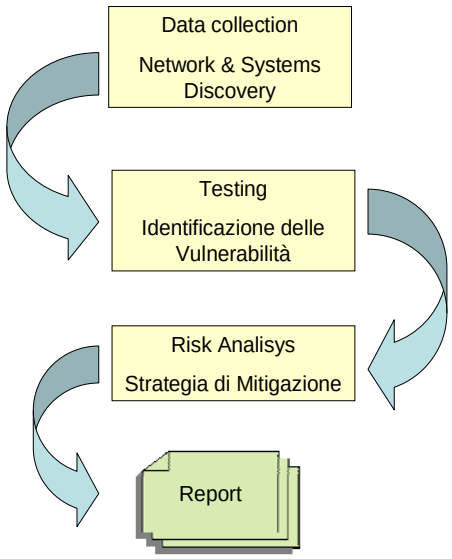
Il servizio Network Security Test consiste nell'analisi, on-site e/o remoto da Internet, delle

infrastrutture definite nell'ambito del contratto.
L'analisi viene realizzata con appositi strumenti software che rilevano eventuali vulnerabilità dovute a errate configurazioni, carenza di aggiornamenti software e/o firmware, presenza di eventuale codice malware.

I risultati vengono elaborati e verificati, con ulteriori test ad-hoc, dai nostri specialisti in collaborazione con il cliente, per individuare le possibili contromisure ed eventuali errori di impostazione dell'architettura del sistema informativo nel suo complesso.

Le procedure applicate nell'esecuzione del servizio sono state sviluppate dai nostri consulenti nel corso di diversi anni di attività nell'ambito di audit di sicurezza, in base agli standards di auditing NIST, ISACA, SANS, PCI-DSS.

Le macro fasi delle attività eseguite sono riassunte nel flusso rappresentato in seguito:



Durante le attività di test e verifica non vengono di norma eseguiti test che possono implicare rischi di Denial of Service (blocco dei servizi) o modifiche ai dati utente e di sistema. Le attività che possono comportare un rischio di disservizio potranno essere eventualmente effettuate secondo modalità concordate per evitare gli impatti sui servizi.

Al termine dell'attività viene rilasciato un report ufficiale che evidenzia il dettaglio delle reti/sistemi testati, vulnerabilità e rischi evidenziati, l'analisi delle criticità riscontrate, riportando le possibili azioni correttive (tecniche, architetturali, organizzative).

Il report è logicamente suddiviso in due sezioni distinte:

- Executive Report, esposizione riassuntiva dei rischi rilevati e delle relative azioni di mitigazione proposte.
- Technical Report, esposizione dettagliata delle attività svolte, rischi rilevati e relative azioni di mitigazione proposte.

Esempio di tabella riassuntiva nel Technical Report:

Sommario Vulnerabilità per Sistema

HOST	IP	Open Ports	LOW	MEDIUM	HIGH
ESIL40-BE	172.20.106.68	2	7	0	0
ESIL42-BE	172.20.106.69	2	6	1	1
ESIL44-BE	172.20.106.70	1	6	0	0
ESIL40-FE	172.20.106.36	2	10	0	1
ESIL42-FE	172.20.106.37	2	10	0	1
ESIL44-FE	172.20.106.38	1	6	0	0
ESIL40	172.20.106.4	3	10	3	1
ESIL42	172.20.106.5	3	10	3	1
ESIL44	172.20.106.6	2	7	0	0
Totale			**72**	**7**	**5**

Per ulteriori informazioni contattare:
info@ictsystem.it