BLS CONSULTING
Consulenza e sviluppo informatico

VULNERABILITY ASSESSMENT & ANALISI DEL RISCHIO

La Vulnerability Assessment e l'Analisi del rischio sono sistemi di scannerizzazione che rilevano le vulnerabilità e i rischi cui le infrastrutture informatiche aziendali sono soggette.
Richiedi ora una Vulnerability Assessment e Analisi del Rischio e pianifica gli interventi che ti permetteranno di evitare problemi futuri.

VULNERABILITY ASSESSMENT

Questa analisi rileva le vulnerabilità presenti sui sistemi Informatici del Cliente con dei metodi molto raffinati.
Tutti i software e gli hardware presentano delle Vulnerabilità che, opportunamente sfruttate, possono portare a un furto di dati, al danneggiamento di un servizio o ad altre gravi disfunzioni.
Contro la maggior parte delle Vulnerabilità i fornitori rilasciano periodicamente delle Patch e degli aggiornamenti che consentono di "tappare" le falle del sistema.
Perché è necessario, allora, effettuare un'analisi di questo tipo?
Perché spesso per le aziende è difficile restare al passo con tutti gli aggiornamenti dei numerosi sistemi che compongono la loro rete.
Può succedere che una nuova Patch sfugga al responsabile IT, dal momento che certe Patch non vengono fornite direttamente.

PROBLEMI DELLE PATCH

Accade spesso che nonostante si sia ricevuto un aggiornamento si sia restii a installarlo in quanto certe Patch possono causare disfunzioni. Immaginate di dover installare una Patch che richieda uno o più riavvii su un Server sul quale girano degli importanti servizi per la vostra azienda. Potreste dover interrompere il Servizio, magari per un tempo prolungato (certi server possono richiedere fino a 30 minuti per riavviarsi). Inoltre, spesso le Patch vengono fornite aggregandole in un unico aggiornamento che risulta molto corposo e causa ovvi problemi alla rete.

SOLUZIONI ALTERNATIVE ALLE PATCH

Per fortuna, esistono dei sistemi alternativi alle Patch per proteggere le proprie vulnerabilità.
In alcuni casi, se il Servizio Vulnerabile non è particolarmente necessario, lo si può semplicemente disabilitare.
In altri casi, si possono implementare i cosiddetti "Walk Around", cioè lievi modifiche alla configurazione che permettono di superare la vulnerabilità senza necessariamente installare la Patch.

ALTRO TIPO DI VULNERABILITA'

Esistono inoltre delle Vulnerabilità di altro tipo, la cui pericolosità non dipende dall'esistenza o meno di una Patch.
Ad esempio, la presenza di Password di Default che per dimenticanza non vengono personalizzate e sono facilmente sfruttabili da chi volesse violare il sistema.

ANALISI DEL RISCHIO

L'analisi del rischio è un ampio studio sui rischi che corre l'infrastruttura informatica dell'azienda.
Include ad esempio l'analisi dei rischi fisici, come l'allocazione dei server aziendali in stanze soggette a rischi di allagamento o non ventilate correttamente, così come la presenza di gruppi di continuità.
Verifica inoltre l'esistenza e l'efficacia dei sistemi di Backup presenti in azienda.
Include infine una valutazione dell'educazione del personale all'utilizzo della rete e alla divulgazione di dati sensibili (Social Engineering).
Dal 2003 l'analisi del rischio non è più solo uno strumento essenziale per la gestione delle informazioni, ma è diventato, ai sensi del Testo Unico sulla Privacy (D. Lgs. 196/2003), una misura minima di sicurezza che deve essere adottata contestualmente alla redazione del Documento Programmatico sulla Sicurezza.

BLS CONSULTING
Consulenza e sviluppo informatico

VULNERABILITY ASSESSMENT & ANALISI DEL RISCHIO

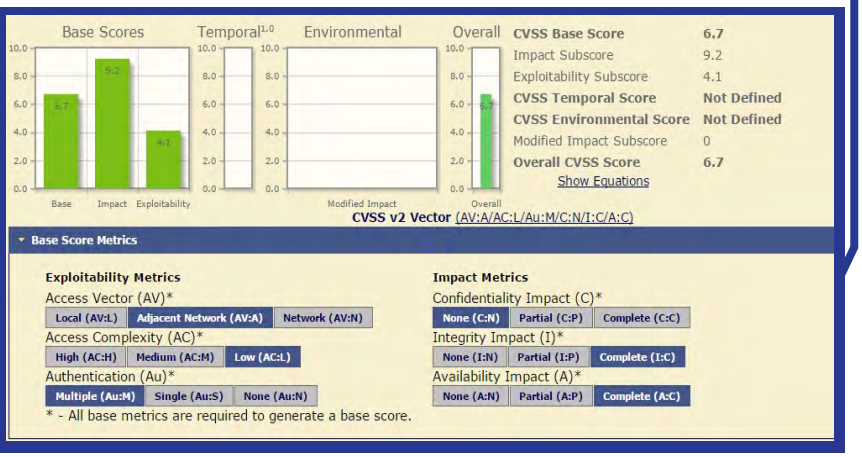
L'ANALISI DI BLS

RILEVAZIONE DELLE VULNERABILITA'

Utilizzando Nessus, software leader nella rilevazione delle vulnerabilità, BLS scannerizza gli Host della vostra rete aziendale.
Nessus si basa, per la sua analisi, sul National Vulnerability Database (NVD), il più grande e aggiornato elenco di Vulnerabilità disponibile al mondo, frutto della cooperazione delle maggiori agenzie di IT Security degli Stati Uniti aggregate sotto la guida del National Institute of Standards and Technology (NIST).
Nello stesso Database sono elencate le Patch disponibili e Nessus ne dà comunicazione nel suo report. Infine, nessus effettua dei test sulle vulnerabilità non legate alle Patch, per le quali i tecnici di Bls mettono a disposizione la loro pluriennale esperienza nel proporre e implementare misure di Walk Around.
Ovviamente l'analisi di BLS include anche altri strumenti per un risultato più completo.

VALUTAZIONE DELLE VULNERABILITA'

Tramite il NVD, Nessus riporta un valore base della pericolosità delle Vulnerabilità rilevate basandosi sul Common Vulnerability Scoring System (CVSS), standard industriale internazionale.
Questo valore viene calcolato basandosi su vari parametri quali il livello di accesso di rete necessario per sfruttarla (se è possibile farlo da remoto o soltanto se autenticati sulla rete aziendale), la complessità di tale accesso, il numero di autenticazioni necessarie per accedere al servizio. Inoltre, considera l'impatto che la vulnerabilità può avere sulla Confidentiality dei dati (se permette di accedere e divulgare dati riservati), sull'Integrity (permette di modificarli) e sulla Availability (se sono dati o servizi fondamentali per il lavoro dell'utente).
Quest'ultima parte di analisi viene ripresa dai tecnici BLS, adattandola ai casi specifici del cliente, cioè verificando l'importanza soggettiva che viene data ai servizi su cui è presente la Vulnerabilità.
Al punteggio base, i tecnici di BLS aggiungono un'analisi Temporale, cioè verificano l'esistenza di Exploit (programmi in grado di sfruttare le vulnerabilità per fare danni, vengono elencati su Security Focus, altro Database Internazionale) e l'effettiva installazione delle Patch sui sistemi del cliente. Come già accennato, BLS verifica congiuntamente con il cliente l'impatto che le Vulnerabilità riscontrate avrebbero sui suoi sistemi.



ANALISI DEL RISCHIO

All'interno della normativa Italiana non è presente un'indicazione precisa sulle modalità di svolgimento dell'analisi del rischio.
Il Decreto Legislativo 196 del 2003 incoraggia genericamente all'"adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta" senza ulteriori specifiche sulle modalità.
BLS effettua l'analisi basandosi sullo standard Canadese ITSG-04, tra i più dettagliati e completi al mondo.
L'obiettivo di tale analisi è quello di identificare e valorizzare gli asset aziendali, identificare le vulnerabilità e le minacce per il proprio sistema informativo, così come l'efficacia dei sistemi di sicurezza.
Tale analisi permette di avere una fotografia esatta del proprio sistema informativo, mostrando qual è l'indice di rischio cui gli asset sono sottoposti e proponendo le misure di sicurezza necessarie per diminuire tale rischio.

BLS CONSULTING
Consulenza e sviluppo informatico

VULNERABILITY ASSESSMENT & ANALISI DEL RISCHIO

RAPPORTO FINALE

Al termine delle analisi BLS presenta un elenco dettagliato delle Vulnerabilità e dei rischi scoperti con una valutazione della gravità e dell'urgenza di contromisure. Alle vulnerabilità scoperte allega delle proposte di soluzioni, basandosi sulle esigenze del cliente affinché siano semplici da implementare e causino il minor disagio possibile.
Su richiesta, BLS effettua successive scansioni specifiche per verificare l'effettiva adeguatezza delle contromisure adottate.

BENEFICI

I benefici che trae l'azienda dall'effettuare periodicamente un Vulnerability Assessment sono molto interessanti.

MIGLIORAMENTO PRODUTTIVITA'

Le procedure proposte da BLS al termine della V.A. non solo migliorano la sicurezza dei sistemi informatici aziendali ma tendono a ottimizzare e razionalizzare l'impiego di risorse.
Esempio di questo sono l'impiego di sistemi antispam e di controllo della posta elettronica, i controlli nei download, la procedura di comunicazione tempestiva al responsabile IT dell'allontanamento di un collaboratore che magari era in possesso di credenziali di accesso a dati aziendali preziosi.

IMMAGINE

La solidità e sicurezza del sistema informatico aziendale, certificata e periodicamente aggiornata col V.A. effettuato da un ente terzo specializzato e competente come BLS concorre ad attestare l'affidabilità dell'azienda.
Da tale attestazione l'azienda trae un sensibile guadagno di immagine nei confronti dei propri stakeholder, dei clienti e dello stato.

CONFORMITA' ALLA LEGGE ITALIANA

La V.A. è uno strumento utilissimo per adeguare la propria azienda alle normative vigenti.
In particolare, l'attestazione della conformità agli standard di sicurezza informatica ottenuta tramite l'analisi delle vulnerabilità e dei rischi va a integrare il Modello Organizzativo aziendale normato dal Decreto Legislativo 231/01.
Tale modello è richiesto sempre più spesso alle aziende che vogliano partecipare a bandi pubblici ed è fondamentale per l'esenzione dalla responsabilità dell'Ente e dei suoi dirigenti nel caso i crimini informatici descritti nella stessa legge vengano commessi dall'interno dell'azienda.
La nostra analisi aiuta inoltre a verificare l'uniformità dell'azienda ai dettami del Codice sulla protezione dei dati personali normato dal Decreto Legislativo 196/03, che raccomanda l'implementazione di procedure di gestione delle credenziali di autenticazione, l'utilizzo di un sistema di autorizzazione, la protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti, ad accessi non consentiti e a determinati programmi informatici, l'adozione di procedure per la custodia di copie di sicurezza e per il ripristino della disponibilità dei dati e dei sistemi, l'adozione di tecniche di cifratura o di codici identificativi.

BLS CONSULTING
Consulenza e sviluppo informatico

VULNERABILITY ASSESSMENT & ANALISI DEL RISCHIO

TIPI DI ANALISI
BLS effettua due tipi di analisi:

BLACK BOX

Include dei test effettuati dall'esterno della rete del cliente, e identifica dunque le vulnerabilità che potrebbero venire sfruttate solo da un esterno che non abbia informazioni sulla struttura della rete, ad esempio un Hacker.

NETWORK DISCOVERY

Analisi degli Host Attivi, identificazione delle linee di comunicazione e dell'architettura di rete, analisi delle informazioni pubblicate su internet.

NETWORK PORT AND SERVICE IDENTIFICATION

Identificazione da remoto delle porte aperte, dei servizi associati e della versione del software utilizzato.

VULNERABILITY SCANNING

Identificazione delle vulnerabilità del software e dell'hardware

PASSWORD CRACKING

Identificazione di login name e password (tramite dictionary attack, brute force, common passwords)

SOCIAL ENGINEERING

Test di recupero di informazioni sensibili dal personale

ULTERIORI TEST SPECIFICI A SECONDA DEI SERVIZI DEL CLIENTE

Ad esempio: Dns poisoning (attacco , Openproxy (attacco al sistema di mail)

PENETRATION TESTING

Impiegando le informazioni recuperate nei test precedenti e gli Exploit pubblici (recuperabili su Security Focus e altri siti dedicati) si verifica il livello di accesso che si può ottenere alla rete aziendale: si verifica la presenza di sistemi di Intrusion Detection, la facilità di accesso a risorse interne, sniffing del traffico…

WHITE BOX

Include test all'interno del perimetro aziendale.
Questi test suppongono la possibilità di accesso di chi già detenga informazioni sulla rete, ad esempio un ex impiegato o semplicemente chi sia riuscito a sottrarre dati di accesso.

PATCH ANALYSIS

Analisi delle Patch applicate e identificazione di quelle mancanti

FILE SYSTEM ANALYSIS

Analisi delle autorizzazioni impostate sul filesystem e sulle eventuali condivisioni

ARCHITECTURE ANALYSIS

Identificazione di eventuali vulnerabilità nell'architettura del sistema, nel firewall o nel proxy

EMAIL SYSTEM ANALYSIS

Verifica di eventuali sistemi di Sender Accreditation, valutazione del sistema di Sender Reputation dell'ente e dei suoi sistemi di sicurezza nella ricezione di email.

B.L.S. Consulting S.r.l
P. IVA 01606500187
email: info@bls.it

Sede
Via Gramsci, 25 -27100 PAVIA (PV)
Tel. 0382/413800-Fax 0382/413820

Commerciale
Tel. 0382/413825
commerciale@bls.it

www.bls.it