SERVICE DESCRIPTION
Vulnerability Assessment
Ver. 1.1 - Aggiornamento del 20/11/2021

Sommario

1. Descrizione generale

Il servizio di Vulnerability Assessment (di seguito V.A.), prevede la scansione degli indirizzi IP pubblici e/o privati, indicati dal cliente, per trovare falle nei sistemi informatici.

Sielco userà dei software che provvederanno a rilevare tutte le possibili vulnerabilità note sui sistemi accessibili tramite gli IP oggetto del servizio.

In alcuni casi Sielco potrebbe inviare un'appliance (dispositivo informatico) con già pre-installato il software necessario.

Sielco potrebbe avvalersi di società terze a cui affidare il servizio.

Il risultato della scansione è un report con indicate le vulnerabilità che verrà discusso assieme al cliente.

NON è oggetto di questo servizio un eventuale piano di remediation (piano per eliminare le vulnerabilità rilevate) che può essere concordato a parte.

Prerequisiti:

- A seconda del tipo di scansione potrebbe essere necessario avere a disposizione l'utente "amministratore" dei sistemi.

Qualora venissero a mancare i prerequisiti il Servizio non potrà essere erogato.

L'installazione dell'appliance può avvenire ad opera del personale Sielco o direttamente per mano del cliente. Nel primo caso il servizio dovrà comprendere gli oneri di trasferta.

2. Condizioni per l'esecuzione del servizio

- Il cliente dichiara di essere titolato a richiedere questo tipo di servizio sugli indirizzi IP che indicherà
- Il cliente, con la sottoscrizione dell'offerta, autorizza Sielco ad effettuare analisi di rete e/o di individuazione di vulnerabilità da effettuarsi nei tempi e nei modi concordati, al trattamento dei dati ed agli accessi ai propri sistemi necessari all'espletamento dei servizi oggetto del presente incarico
- Il cliente, con la sottoscrizione dell'offerta, dichiara di essere a conoscenza ed accettare che verrà tenuta registrazione dei momenti e dei tempi degli accessi ed in tal senso autorizza espressamente Sielco e i suoi fornitori. Ai sensi e per gli effetti delle norme in materia di protezione dei dati personali, Sielco dichiara che le registrazioni appena

citate saranno trattate solo per finalità correlate alla prestazione del presente servizio e conservate per il tempo necessario a dare evidenza della qualità dello stesso.

- Il cliente, con la sottoscrizione dell'offerta, dichiara di essere consapevole ed accettare, che le vulnerabilità sono in continua evoluzione e pertanto a quelle che verranno segnalate potrebbero a breve aggiungersene di ulteriori.
- Il cliente, con la sottoscrizione dell'offerta, dichiara di essere consapevole ed accettare che l'analisi delle vulnerabilità non comporta l'eliminazione delle stesse

3. *Fasi del servizio*

Le fasi per l'avviamento del servizio sono le seguenti:

A. Definizione del perimetro (quali e quanti indirizzi IP) di scansione delle vulnerabilità
B. Preparazione, presso la sede Sielco, dell'appliance con un indirizzo statico della rete del cliente (MASK, DF GW) o in alternativa installazione di una virtual machine sui sistemi del cliente o in alternativa configurazione di una VPN (solo per la scansione di indirizzi ip privati)
C. Spedizione dell'appliance al cliente o installazione (collegamento alla rete) a cura del personale Sielco (solo per la scansione di indirizzi ip privati)
D. Scansione (può durare anche diversi giorni a seconda del perimetro)
E. Generazione del report
F. Discussione del report col cliente

Queste fasi potrebbero subire variazioni a seconda delle condizioni operative in cui si trova il cliente.

4. *Limitazioni di responsabilità*

Si informa espressamente il cliente che l'esecuzione del presente incarico comporta il rispetto delle seguenti condizioni operative da parte del committente stesso:

1. Che sia nominato, prima dell'inizio dell'attività di Vulnerability Assessment, un responsabile interno cui fare riferimento;

2. Che i sistemi di backup siano in perfetto funzionamento;

3. Che il responsabile interno esegua un backup di tutte le risorse prima dell'inizio dell'attività di Vulnerability Assessment;

4. Che sia presente in azienda una procedura di recupero dati e ripristino sistemi da backup testata ed efficiente.

5. Che non si sia già a conoscenza di criticità relative alla sicurezza informatica dei sistemi;

6. Che siano attivi i sistemi antivirus, firewall e più in generale i sistemi di sicurezza dell'infrastruttura informatica del committente;

7. Che l'infrastruttura informatica sia protetta dal gruppo di continuità;

Il committente, con la firma della presente, accetta di assumere a proprio carico i rischi che possano derivargli dall'attività di V.A., a causa del mancato rispetto delle condizioni operative sopra indicate e solleva Sielco Srl. da ogni responsabilità per tutti i danni diretti od indiretti, concomitanti e/o conseguenti alle attività di V.A. ivi compreso, a titolo esemplificativo ma non esaustivo, perdite di produzione e di profitti, violazioni trattamenti di dati accidentali, perdite di dati ecc. .

5. Informazioni Aggiuntive

Per informazioni aggiuntive dettagliate si rimanda alla sessione "Documenti a corredo" presente sul sito SIELCO alla pagina
https://sielco.it/condizioni_contrattuali/