AVVISO PUBBLICO NELL'AMBITO DELL'ANALISI COMPARATIVA EX 68 CAD FINALIZZATA ALL'INDIVIDUAZIONE DI UNA PIATTAFORMA DI NETWORK SECURITY POLICY MANAGEMENT - NSPM (APIM_19_008).

INFORMAZIONI COMPLEMENTARI

Si porta a formale conoscenza di tutte le Imprese interessate all'indagine in oggetto le richieste di chiarimenti pervenute, con le rispettive risposte:

DOMANDA 1

In relazione all'avviso in oggetto richiedo i seguenti chiarimenti relativi ai Punti 2,3 e 4 utili al Dimensionamento della Soluzione.
Punto 2. N. di firewall CED (compresi i virtuali) 30

Punto 3. N. di firewall remoti (branch office) 20

a) *DOMANDA: sia per il CED che per i Branch è possibile avere il dettaglio di quanti firewall sono Fisici e quanti virtuali e quanti Stand alone e quanti in Cluster?*

Punto 4. Numero di nodi di rete (L3) – compresi bilanciatori 100

b) *DOMANDA: è possibile avere il dettaglio di quanti sono i Router, quanti gli Switch e quanti i Bilanciatori?*

RISPOSTA 1

a) Per il CED sono da considerare 5 cluster "active – passive" fisici. Su alcuni di questi sono stanziati firewall virtuali (virtual systems).
Per i branch i firewall sono da considerare tutti fisici di cui almeno 6 casi di cluster.
Nessun branch ha firewall virtuali a bordo.
Il CSI accetta anche soluzioni che prevedano il solo licencing del FW Primario da evidenziare nella documentazione, indicando le eventuali limitazioni di funzionalità del prodotto nel caso di failover da un firewall all'altro.

b) Per quanto riguarda i bilanciatori questo sono 3 Cluster fisici "active/passive" su cui sono configurati da 4 a 10 bilanciatori virtuali per cluster.
Si aggiunge poi un cluster completamente virtuale.
Per quanto riguarda switch/router si è fatta una stima di "massima" di apparati L3 (sia locale che geografici) ma non è ancora stato definito il perimetro esatto.

DOMANDA 2

In relazione all'avviso in oggetto richiedo i seguenti chiarimenti relativi ad alcuni punti utili al Dimensionamento della Soluzione.

a) *DOMANDA*: RF10 e RF19: In quali dispositivi vengono utilizzati profili di tipo L7?

b) *DOMANDA*: RF25: La verifica avviene mediante integrazione con un vulnerability scanner presente (Nessus, Rapid7, Qualys o altro tipo)?

c) *DOMANDA*: RF27: In presenza di un SIEM / SOAR, la soluzione può essere utilizzata per alzare o abbassare il livello di criticità di una nuova vulnerabilità, rispetto alla esplorabilità della stessa da diversi punti dalla rete, aiutando a innescare una azione automatica come aprire un ticket di remediation e realizzando enforcement?

RISPOSTA 2

a) I profili di livello 7 vengono implementati sui firewall (policy per utente di dominio e per applicazione), pertanto il modulo di change deve poter permettere all'utente di richiedere una policy utilizzando anche questi dati e non solo "indirizzo IP-porta".

b) No. Si richiede che sia la soluzione proposta ad effettuare la verifica di vulnerability.

c) Si richiede che la soluzione proposta sia in grado di fornire un elenco di vulnerabilità ordinate per priorità/gravità. Indicare se eventualmente la soluzione proposta puo' fare enforcement.

Torino 22/7/2019

Il RUP
Firmato digitalmente
(S. Lista)