Vulnerabilità Zero-Day

Negli ultimi tempi alcuni casi di vulnerabilità del software sono balzati agli onori della cronaca per gli ingenti danni provocati. Tra questi citiamo i più famosi: "**Heartbleed**", una vulnerabilità della libreria OpenSSL, e "**Shellshock**", una vulnerabilità degli ambienti Linux. Si è trattato di cosiddette vulnerabilità "**Zero-Day**" e quindi di attacchi che hanno sfruttato dei buchi software non ancora conosciuti, che hanno colpito le organizzazioni aziendali quando queste risultavano ancora prive di adeguate difese.

L'obiettivo di tutte le organizzazioni è quello di ridurre al massimo l'esposizione a questo tipo di vulnerabilità, e di uscire da questo stato a partire dal cosiddetto "**Day-One**", cioè dal giorno in cui la vulnerabilità viene identificata e registrata nel **National Vulnerability Data Base**, pubblicato dal NIST. Da quel momento in poi le organizzazioni dovrebbero essere in grado di mettere in atto delle adeguate contromisure, fino all'applicazione della specifica "**patch**" in grado di superare definitivamente lo stato di vulnerabilità.

Tutte le organizzazioni devono però fare i conti con la **complessità** dei sistemi e del software Enterprise. Un singolo software affetto da una determinata vulnerabilità, potrebbe essere diffuso in una miriade di dispositivi aziendali e registrato con un'ampia gamma di nomi diversi. Nel caso di "Heartbleed", il software OpenSSL può essersi diffuso in una realtà Entrprise in almeno 2000 forme diverse, e questo tenendo conto delle numerose combinazioni possibili rispetto al nome del fornitore, al nome del prodotto, al nome del file e alla versione.

Con questo livello di complessità, uscire dallo stato di emergenza attraverso un processo manuale di riconoscimento può richiedere un tempo troppo elevato, una finestra temporale non tollerabile rispetto alle esigenze del business. E' quindi necessario essere dotati di strumenti che riescano a normalizzare e allineare le informazioni relative alle risorse IT, così da ottenere una completa visibilità rispetto al software implementato in azienda, indipendentemente dalla varietà di nomi e delle caratteristiche con cui questo software si è diffuso all'interno dell'architettura Enterprise. **Solo in questo modo sarà possibile pensare di chiudere lo stato di vulnerabilità "Zero-Day", a partire dal "Day-One"**.

Come uscire dallo stato di Vulnerabilità "Zero-Day" a partire dal "Day-One"

Questo è proprio uno dei valori aggiunti delle soluzioni BDNA, in modo particolare dell'architettura **BDNA Technopedia**, il più vasto catalogo di prodotti hardware e software, dotato di funzioni avanzate per il discovery e da un sistema di normalizzazione delle informazioni collezionate. Le soluzioni BDNA rendono possibile l'obiettivo "Day-One", perché consentono di automatizzare il processo di superamento della vulnerabilità, rendendolo rapido e soprattutto ripetibile. Questo processo si attiva nel momento stesso in cui la vulnerabilità viene registrata nel Data Base del NIST.

Tanto per fare un esempio legato al caso "Heartbleed", le soluzioni BDNA sono in grado di **normalizzare le oltre 2000 forme e varietà in cui si presenta la libreria OpenSSL** (a volte "impacchettata" all'interno di programmi eseguibili o funzioni generali come il "Windows Add/Remove Program") assegnando a tutte un nome univoco di identificazione (nel caso specifico OpenSSL). Questo sistema di classificazione normalizzato consente a qualsiasi organizzazione di identificare in pochi minuti tutti i punti in cui è diffusa la vulnerabilità.

Il ruolo di prevenzione e reazione delle soluzioni BDNA rispetto alle vulnerabilità è ancora più ampio, perché consente di controllare ulteriori parametri, come la "**fine del ciclo di vita**" di una determinata versione di un software, che corrisponde al momento in cui il produttore non garantisce più il supporto della stessa. In questi casi infatti, anche a fronte di vulnerabilità riscontrate, non verrà rilasciata alcuna forma di correzione. Questo indicatore consente quindi alle organizzazioni aziendali di intervenire con un processo di upgrade per evitare quella che è una potenziale esposizione o comunque per uscire dallo stato di vulnerabilità.

BDNA ha recentemente rilasciato un'estensione di contenuto (**Content Packs**) del suo catalogo Technopedia che permette di integrare le informazioni contenute nel catalogo con quelle relative agli standard di sicurezza **CPE/CVE**, utilizzando i campi prelevati dal National Vulnerability Database pubblicato dal NIST. Questa integrazione permette di rilevare le principali criticità legate alle vulnerabilità hardware e software della propria infrastruttura tecnologica e quindi di intervenire ove necessario per ridurre i rischi connessi con le vulnerabilità rilevate.

Gruppo Daman

Le soluzioni BDNA sono distribuite in Italia dal **Gruppo Daman**. la cui missione è quella di selezionare prodotti innovativi e sofisticati mirati al mercato dell'ICT, per la successiva distribuzione sul territorio italiano.