Datemi una Injection ed una RCE e vi solleverò il mondo

Author : Massimiliano Brolli

Date : 8 Gennaio 2019

Archimede di Siracusa (matematico ed inventore greco), molto tempo fa, tramite un metodo rigorosamente empirico basato sulla meccanica dell'equilibrio dei corpi solidi, scoprì i principi di funzionamento delle leve e un bel giorno si narra che esclamò la famosa frase: "*datemi una leva e vi solleverò il mondo*".

Ma il titolo di questo articolo, cosa vuol significare con tutto questo?

Cosa sono le vulnerabilità di Injection e Remote Code Execution (RCE)?

Si tratta delle più pericolose minacce presenti sui siti web, capaci, qualora sfruttate, di generare data-breach gravi in termini di profondità e furto dei dati sensibili.

Mentre altre vulnerabilità sono spesso sfruttabili da rete interna, questo genere di vulnerabilità introdotte da una cattiva pratica nello sviluppo sicuro del codice o da carenze nel processo di patching-management, sono subdole e alle volte di difficile rilevazione.
Inoltre, nel caso di tutte le carenze di "depurazione degli input", la loro rimozione è demandata ai team di sviluppo sempre più concentrati ad essere veloci e reattivi (ancora più oggi lavorando in logica a micro-servizi e devops), ma ben poco concentrati a produrre codice sicuro e di qualità.

La superfice di rischio Internet

Il problema serio che questo tipo di vulnerabilità presenti generalmente sulle web application (sfruttabili anche in modo anonimo) sono spesso utilizzabili da big-internet, superficie di rischio "notoriamente" vasta e critica, soggetta a pressioni e scansioni di ogni tipo.
La superficie di rischio... già, … alle volte si tende a concentrare i controlli sul cyberspace interno per paura di esfiltrazione di dati da parte di consulenti e dipendenti interni infedeli, del personale tecnico specialistico. Ma abbiamo mai fatto due semplici conti matematici su quale sia il rischio potenziale di un attacco informatico su queste due diverse direttrici?

Dalle ultime stime, su internet sono interconnessi circa 4.000.000.000 di utenti/devices. Chi ha un cyberspace interno esposto ad oltre 10.000 utenti è già considerata una big-company di livello internazionale, ma vogliamo fare una semplice proporzione? Dicendolo in un altro modo, stiamo parlando che per ogni potenziale aggressore da rete interna, ce ne possono essere 400.000 su big-internet e questo dato deve far riflettere su quanto sia più importante concentrare le forze “fuori” rispetto che a “dentro”.

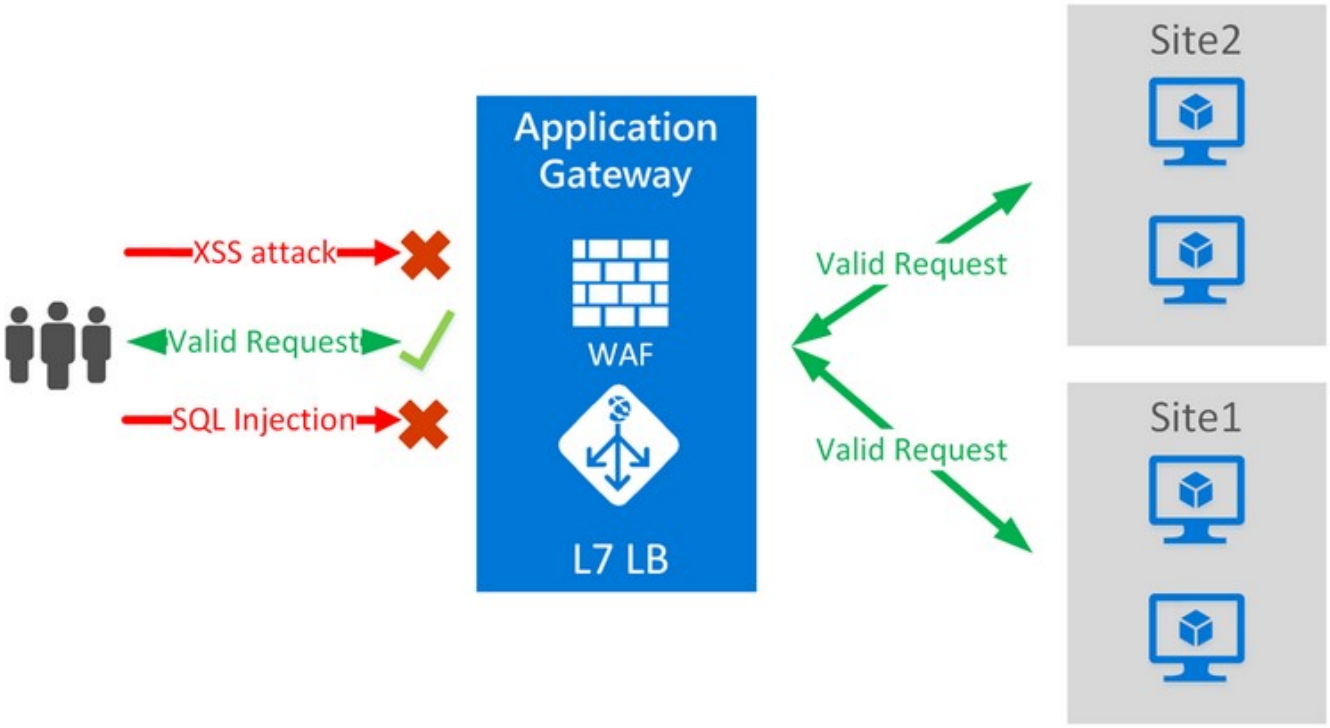
Anche perché spesso “dentro” ci sono protezioni perimetrali e processi aggiuntivi in grado di identificare o prevenire un attacco come i sistemi di identity management, sistemi di sicurezza fisica, firewall, sistemi di tracciamento, IDS, IPS, ecc… In questo caso anche il tracciamento comincia ad essere un elemento importante da valutare da chi vuole attaccare i sistemi.

Fuori è possibile mascherare le identità in infiniti modi oltre a sfruttare la stessa sicurezza per rendere le attività fraudolente ben nascoste (come ad esempio per le sql-injection) che viaggiano anch’esse, come le richieste lecite, in un “tunnel cifrato”.

Un paradosso nella sicurezza informatica

Sembra un paradosso, ma una sql injection o un payload dannoso contenuto all’interno di un canale cifrato (SSL, TLS, ecc…) non risulta osservabile in chiaro proprio perché tale flusso, per questioni di sicurezza e riservatezza, deve risultare offuscato.

Qualora non siano disponibili infrastrutture di terminazione SSL (ad esempio dei security gateway abbinati a dei Web Application Firewall/IDS) il traffico contenuto non risulta leggibile in chiaro in modo da analizzarlo preventivamente e quindi adottare le corrette mitigazioni del rischio durante un attacco.



Purtroppo le soluzioni di terminazione dei canali cifrati non sempre sono conosciute e adottate nelle grandi aziende e questo pregiudica l'utilizzo di strumenti indispensabili ai Security Operation Center per garantire una corretta "detection" degli eventi anomali e agire durante l'attacco e non solo dopo il data breach.

Esistono infatti molte applicazioni web che non utilizzando questo approccio in quanto i canali cifrati terminando direttamente sui server, questo modello deve garantire una sicurezza allo stato dell'arte che può risultare poco gestibile.

Ma allora cosa occorre fare?

Lo spazio internet in molte aziende (e anche in molte big Company) è cresciuto nel tempo in modo esponenziale, anarchico e confuso, cosa che oggi non è più sostenibile anche in considerazione dei danni di business, di immagine e del Gdpr (in ottica delle possibili sanzioni a valle di un ipotetico data breach).

Occorre quindi uno sforzo da parte di tutti per indirizzare al meglio la "Governance dello spazio internet", definendo regole, strumenti e strutture che consentano un corretto presidio e una riduzione drastica della superficie di rischio.

Si perché è proprio questo il reale problema, l'efficacia delle attività di controllo diminuiscono all'aumentare del Cyberspace.

Alcuni spunti possono essere:

- Definire una "***Governance dello spazio internet***" che svolga differenti mansioni come ad esempio:

    Linee guida e procedure sullo spazio internet
    Matrici tecnologiche di componenti software da utilizzare
    Gestione del ciclo di vita del software open source
    Supporto e validazione dei disegni architetturali dei sistemi
    Gestione delle infrastrutture internet (ad es. DNS, Reverse proxy, firewall, WAF, DDoS protection, Ida, IPS, ecc…)
    Classificazione e gestione delle risorse sul RIPE

- Attivare un piano di Assessment mirato a “ridurre” e “accorpare” le risorse esposte su internet soprattutto armonizzando l’esposizione attraverso Reverse Proxy e Security Gateway per consentire la terminazione dei canali di cifratura dei servizi web. Monitoraggio e gestione del corretto aggancio ai sistemi SIEM per consentire una efficace “detection” degli eventi anomali da parte dei Security Operation Center.
- Attivare Assessment ricorsivi su tutta la superficie esposta con la latenza più vicina sostenibile, sia attraverso scansioni infrastrutturali e sia attraverso scansioni delle componenti web (ad es. utilizzando tool addizionali sulla base delle tecnologie utilizzate come Drupal Security Scanner, Joomla Security Scanner, scansioni dinamiche con tool Acunetix like, ecc ...)
- Avviare un’efficace "***Data Breach Prevention***" attraverso attività di Penetration Test ricorsivi mirati alle web application più critiche per verificare potenziali data breach e rimuoverli in regime di Task Force.
- Avviare cicli di "***Awareness Security***" per simulare campagne di phishing verso i dipendenti e a danno dell'azienda per monitorare la “consapevolezza al rischio”, avviare corsi di formazione online per consentire ai singoli di comprendere il rischio derivante da un abuso dei dati sensibili esposti su internet, pillole di sicurezza, ecc… (anche se tutto questo ricade nella gestione classica della cybersecurity aziendale).
- Attivare il processo di "***Responsible discolsure***" tenendo sempre in considerazione che un vero ladro non vi dirà mai che sa dove lasciate la chiave della vostra cassaforte che trova nascosta sotto il tappetino, perché sa che il giorno dopo non la ritroverà più.
- Attivare una “***Threat Intelligence***” efficace mirata a verificare nel deep-web e nel clear-web la diffusione di vulnerabilità nelle community underground che possono affliggere i nostri sistemi verificando anche la presenza di servizi acquistabili in criptovalute per richieste specifiche e di dati sensibili della vostra azienda. Valutare anche nei tempi successivi al lancio di nuovi servizi, cicli di verifica Osint per comprendere con tempismo l'evoluzione delle minacce in modo da bonificarle prima che transitino in modo incontrollato sul clear-web

Conclusioni

Abbiamo visto alcuni spunti che possono essere valutati per poter organizzare al meglio una corretta gestione della superficie esposta su internet che sia sostenibile in termini di costi e di

miglioramento della sicurezza informatica.

Seppur questa esigenza è conosciuta da anni, con le nuove tecnologie emergenti (Cloud, IoT, 5G) e soprattutto con l'avvento del GDPR si rende necessario avviare piani di recovery per poter evolvere una gestione “artigianale” e poco strutturata con una gestione “organica” che consenta di avere sotto controllo lo spazio internet.

Per avere successo nella nuova digital-transformation, le organizzazioni devono saper essere resilienti e avere nel proprio Dna la “capacità” e la “cultura” di ridurre il proprio cyberspace internet.

Con il tempo, questa capacità di adattamento consentirà grandi ritorni in termini di investimenti ICT oltre che a massimizzare l'efficacia in termine di controlli di sicurezza informatica.

Articolo a cura di **Massimiliano Brolli**