

# La sicurezza del software è un processo collaborativo

Non tutti i consigli sono necessariamente buoni. Al netto delle migliori intenzioni, coloro a cui ci rivolgiamo in cerca di aiuto spesso finiscono per suggerirci percorsi che, sebbene abbiano funzionato per loro, non sono pensati per noi; e quando si tratta di sicurezza, accettare cattivi consigli può avere conseguenze devastanti.

La cronaca quotidiana ci ricorda che, laddove i cyber criminali riescono a sfruttare le vulnerabilità contenute nei software, ormai indispensabili strumenti di business, possono fare di tutto: violare la nostra proprietà intellettuale, sottrarre informazioni relative a dipendenti e clienti o svuotare i conti aziendali, potendo arrivare a minare la sicurezza fisica di un edificio e perfino – di solito tramite attacchi *ransomware* – a bloccare il flusso operativo dell'organizzazione.

## Come costruire la fiducia nel proprio software

Oggi qualsiasi attività è in qualche modo basata sul software; e il software, di conseguenza, va incluso fra i principali fattori di rischio per il business.

Per sopravvivere in questo ambiente ostile è necessario usare molta cautela al momento di scegliere a chi rivolgerci in cerca di consigli, nonché di decidere se seguire o meno le indicazioni che ci vengono date.



Synopsys, MOVING FROM EMERGING TO MATURING

Più che sollecitare i feedback dei nostri colleghi, sarebbe più utile avere sempre a portata di mano informazioni

dettagliate provenienti da centinaia di loro: sapere quali soluzioni hanno funzionato, quali no e – forse ancor più importante – cosa è stato modificato e come hanno reagito a tali cambiamenti, al fine di costruire una maggiore fiducia verso il proprio software.

Ecco perché, ad oggi, oltre 130 fra le più note organizzazioni a livello mondiale si sottopongono ad un'analisi BSIMM

## **Cos'è e a cosa serve un Building Security In Maturity Model (BSIMM)**

Sin dal 2008, BSIMM – acronimo per *Building Security In Maturity Model* – analizza 250 progetti di *software security* in quattro ambiti (*Governance, Intelligence, SSDL Touchpoints, Deployment*) esaminando come le organizzazioni inseriscano la sicurezza nei processi di sviluppo al fine di contrastare un panorama di minacce in rapida evoluzione. Attraverso questa osservazione *data-driven*, quindi, stima la maturità del *software security group* di un'organizzazione realizzando un prospetto di riferimento utile a valutare la maturità complessiva dei programmi di sicurezza in uso.



Synopsys software security framework

BSIMM mette anche a disposizione delle aziende una comunità digitale con la quale potersi confrontare, realtà analoghe che permettono di condividere riflessioni e *best practice*, oltre a incontri fisici che favoriscono occasioni di dialogo e collaborazione B2B.

Il programma BSIMM produce anche un report annuale – giunto alla sua tredicesima edizione – che mette in luce i principali trend osservati in ambito di *software security*, per aiutare la comunità dei responsabili della sicurezza a pianificare, implementare e valutare le relative attività. Comprendere le tendenze di settore, infatti, contribuisce significativamente a migliorare la propria pianificazione strategica.

# I principali trend nella sicurezza del software

BSIMM13 (l'ultimo report pubblicato) espone i trend di *software security* in evoluzione negli ultimi 12 mesi presso le organizzazioni affiliate al programma, sottolineando gli sforzi volti a mettere in sicurezza oltre 145.000 applicazioni nella cui realizzazione e manutenzione sono coinvolti circa 410.000 sviluppatori.

Fra le principali tendenze si rileva la **crescente attenzione verso l'*open source* e alla sicurezza della *software supply chain***, visti fino a pochi anni fa come temi marginali ma oggi considerati prioritari da più della metà (51%) delle organizzazioni osservate.

Si pone naturalmente grande **attenzione verso il software di terze parti**, che sia di provenienza *open source* oppure commerciale, poichè figura pressoché in ogni *codebase* e ne rappresenta spesso la componente maggioritaria, come rileva un ulteriore report di Synopsys dal titolo Open Source Security and Risk Analysis.

Di conseguenza, una delle tendenze più incoraggianti che emergono da BSIMM13 è che il **73% dei *cybersecurity teams* esaminati ha incrementato i propri sforzi per mettere in sicurezza la propria *supply chain***. A tale scopo, una delle possibili strade è utilizzare strumenti automatizzati di software composition analysis (SCA) che aiutano a identificare le componenti *open source* presenti in una *codebase*, unitamente alle vulnerabilità note e ad eventuali questioni relative alle licenze d'uso.

Un'altra strada prevede la creazione di un software Bill of Materials (SBOM), che individua il software di terze parti all'interno delle *codebases* affinché si possa reagire rapidamente nel caso siano scoperte delle vulnerabilità in una o più componenti. La ricerca mostra un **aumento del 30% delle**

**organizzazioni che ricorrono allo SBOM**, sintomo di un'accresciuta consapevolezza dei rischi legati alla *software supply chain*.

## **Non solo esperti di sicurezza all'interno dei *security champions programs***

BSIMM13 evidenzia poi una tendenza persistente circa il valore apportato dai cosiddetti "*security champions programs*", i quali prevedono team che non sono formati solo da esperti di sicurezza ma coinvolgono sviluppatori, *QA testers*, *architects* e *DevOps engineers* per renderli "*software security champions*", così permettendo ai team di sicurezza di crescere e potenziare i propri sforzi senza dover coinvolgere risorse esterne. Come rilevato da BSIMM13, le realtà che applicano programmi di questo tipo mostrano punteggi superiori del 35%, sulla media degli *assessments* BSIMM, rispetto a quelle che non ne fanno uso.

Ma forse il dato più interessante che emerge dal report è che **nessuno dei *software security group* in forza alle 130 organizzazioni partecipanti presenta la medesima struttura.**

Non esiste, infatti, una sola modalità per dotarsi di un valido *software security program*, né si può stabilire con certezza quale sia la migliore. Ma l'obiettivo è lo stesso per tutti: garantire l'affidabilità del software impiegato e distribuito.



Synopsys, TO WHOM THE CISO REPORTS

Se da un lato è certamente possibile "navigare a vista", dall'altro è innegabile come poter contare su un piccolo aiuto ci consenta di farlo meglio e – soprattutto – in modo più sicuro.

Ecco perché **il report BSIMM è paragonabile a una mappa:** anziché proporre alle aziende un'unica strada da seguire,

fornisce a ciascuna di esse informazioni utili per tracciare il percorso più adatto al proprio profilo di rischio e alle proprie specifiche esigenze di difesa.

Articolo a cura di **Emanuele Burali d'Arezzo**, Regional Sales Manager di Synopsys

Condividi sui Social Network:

<https://www.ictsecuritymagazine.com/notizie/la-sicurezza-del-software-e-un-processo-collaborativo/>