Dal codice al cliente: il processo che assicura la sicurezza dei nostri prodotti

Introduzione

Man mano che il mondo diventa sempre più interconnesso, cresce l'esigenza di potersi avvalere di tecnologie sicure e affidabili e di garantire la massima sicurezza ai prodotti stessi. Le soluzioni di sicurezza si evolvono parallelamente al settore di ricerca delle vulnerabilità e si trasformano, nella struttura e nelle finalità, in funzione della crescente complessità del panorama delle minacce.

Lo sviluppo del software è un processo poliedrico, con molte fasi lungo il percorso che porta dal codice al cliente. A differenza della maggior parte degli altri software, i prodotti di sicurezza sono costituiti da numerosi componenti, alcuni talmente integrati nel sistema operativo da rendere ancora più importante la risoluzione dei problemi: in caso contrario, l'intero sistema potrebbe essere compromesso.

Una delle maggiori sfide nello sviluppo del software consiste nell'evitare uno scenario basato sull'improvvisazione, che determina il ripetersi costante degli stessi problemi. Questa situazione è inefficiente e pericolosa,

ma può essere evitata strutturando correttamente l'architettura dei componenti del software. Inoltre, se la sicurezza viene posta al centro di ogni processo di sviluppo, l'architettura diventa ancora più sicura. Kaspersky Lab ha adottato un approccio strategico che implica collaborazione tra team, diverse fonti informative interne ed esterne e una formazione continua.

Abbiamo perfezionato l'intero processo e il risultato è sicuramente il modo migliore per integrare la sicurezza nei nostri prodotti e fornire protezione ai nostri clienti. Continuate a leggere per scoprire come riusciamo a conseguire questo obiettivo.

Dal codice al cliente: il processo che assicura la sicurezza dei nostri prodotti

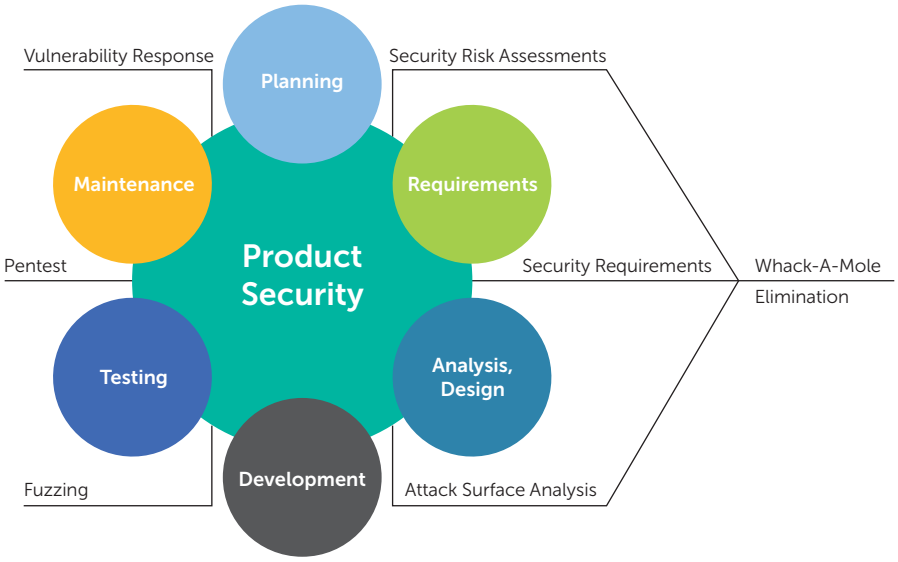
Noi di Kaspersky Lab prendiamo sul serio il ruolo di vendor di sicurezza leader del settore. Nel processo di sviluppo dei nostri prodotti, siamo costantemente alla ricerca della soluzione perfetta in termini di innovazione e usabilità. A differenza di altri software, i prodotti di sicurezza sono costituiti da molti componenti, alcuni talmente integrati nel sistema operativo da rendere cruciale la risoluzione dei problemi.

Sono passati oltre due decenni da quando abbiamo sviluppato la nostra prima soluzione antivirus e in questo periodo abbiamo imparato sul campo a rispondere rapidamente ed efficacemente alle nuove e crescenti sfide del settore della cybersecurity. Le soluzioni di sicurezza, così come gli altri software, si evolvono parallelamente al settore di ricerca delle vulnerabilità e si trasformano, nella struttura e nelle finalità, in funzione della crescente complessità del panorama delle minacce, con miglioramenti e nuove funzionalità a ogni rilascio.

Comprendiamo il collegamento diretto tra la maggiore complessità di un prodotto e il numero di potenziali vulnerabilità riscontrabili. I nostri product team e il nostro intero processo di sviluppo hanno come obiettivo quello di garantire la massima sicurezza dei nostri processi di software engineering. L'integrazione dei massimi livelli di sicurezza nei nostri prodotti è al centro del nostro operato.

Le fondamenta come punto di partenza

Se l'architettura dei componenti software è correttamente strutturata, è possibile evitare uno scenario basato sull'improvvisazione, in cui i problemi continuano a ripresentarsi. Lo stesso si applica anche alle correzioni delle vulnerabilità. I nostri product team lavorano a stretto contatto con il security team per garantire la sicurezza dell'architettura.



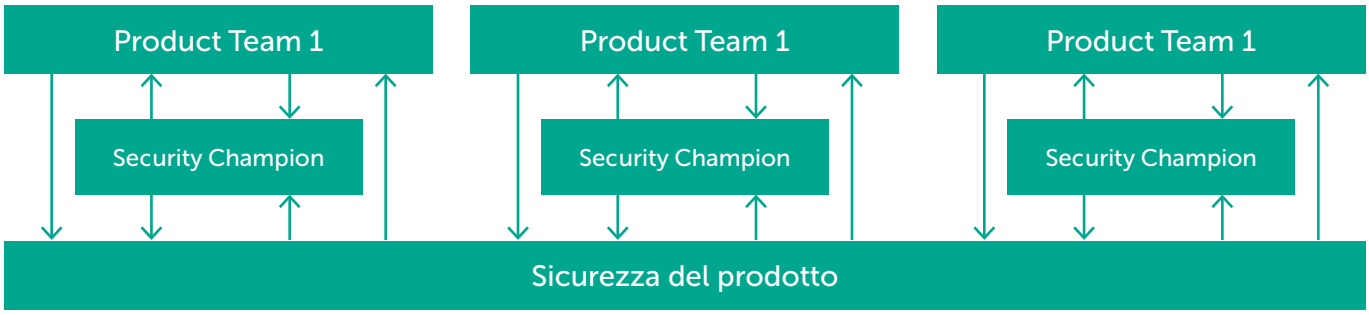
Monitoraggio del processo di sviluppo. I primi tre step in particolare (pianificazione, analisi dei requisiti e design) contribuiscono a evitare risoluzioni improvvisate.

Questo approccio ci ha permesso di evitare i problemi evidenziati dalla "Security Princess" di Google Parisa Tabriz nel suo discorso di apertura al Black Hat USA 2018. Tabriz ha analizzato una questione nota a tutti gli sviluppatori: la frustrazione di ricevere report su vulnerabilità che erano state precedentemente risolte o che sono una banale variante di un bug conosciuto o persino un sintomo di una condizione sottostante o di un errore di processo noto ma mai affrontato.

In Kaspersky Lab, è qui che entra in gioco il Secure Development Lifecycle (SDL), vige un approccio volto a dare priorità alla sicurezza durante il processo di sviluppo di un prodotto. Eliminando il fattore "improvvisazione" durante lo sviluppo dell'architettura non solo si eliminano i problemi ricorrenti legati alle stesse vulnerabilità, ma si liberano anche risorse da ridistribuire nello sviluppo di altri prodotti e nella manutenzione di quelli già rilasciati. Il risultato è un'architettura sicura con numerosi vantaggi, tra cui:

- Riduzione delle vulnerabilità che richiedono modifiche a livello di componenti core dell'architettura durante la manutenzione del prodotto
- Numero maggiore di risorse disponibili per la manutenzione
- Riduzione della quantità di aggiornamenti necessari.

Modalità di interazione tra il prodotto e i security team. Il security champion è un livello aggiuntivo che garantisce la corretta applicazione delle informazioni di sicurezza del prodotto.



Il nostro security team è il punto di riferimento, all'interno del dipartimento R&D, per tutte le questioni relative ai rischi di sicurezza dei prodotti e delle infrastrutture. Il team è responsabile di numerosi task critici, tra cui la stesura dei requisiti iniziali, l'audit del codice, il vulnerability assessment e la relativa remediation, l'analisi dei rischi, la distribuzione di funzionalità di mitigazione, l'integrazione di tecniche di fuzzing, i penetration test e altro ancora. Durante questi step, il nostro team Anti-Malware Research (AMR) è in grado di fornire informazioni cruciali aggiuntive.

Fonti di informazioni sulle vulnerabilità

Anche se il product team investe molto tempo ed energia nella scrittura del software e si attiene strettamente agli standard di sicurezza, un hacker può trovare un punto debole nel prodotto o nel suo ambiente e comprometterlo. Per questo motivo, utilizziamo diverse fonti di informazioni sulle vulnerabilità per ottimizzare la sicurezza dei nostri prodotti.

Tra le fonti che prendiamo in considerazione sono incluse: vulnerabilità divulgate pubblicamente in un sistema operativo che in qualche modo potrebbero interessare i nostri prodotti, vulnerabilità in librerie o software di terze parti utilizzati nei nostri prodotti, report di ricercatori su vulnerabilità pubbliche, report del nostro portale Bug Bounty, report inviati dagli hacker alla nostra casella di posta (vulnerabilities@kaspersky.com), report inviati dai ricercatori tramite il nostro modulo online e vulnerabilità segnalate privatamente dai nostri ricercatori, progettisti e penetration tester.

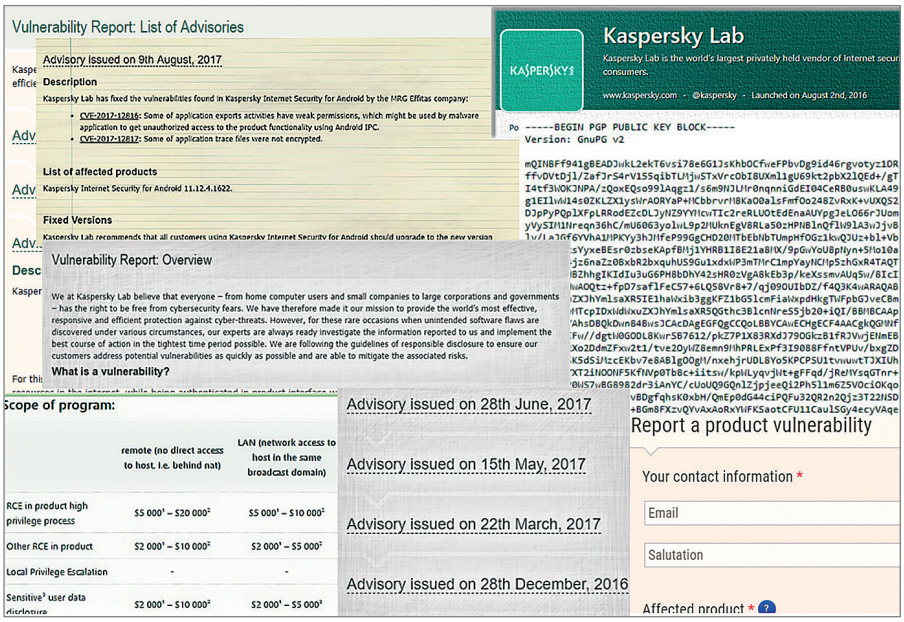
Le diverse fonti di intelligence sulle vulnerabilità che Kaspersky Lab riceve

Le vulnerabilità non corrette tramite patch e divulgate pubblicamente rappresentano una criticità perché possono essere utilizzare dagli hacker per attaccare i nostri clienti. A seconda della valutazione CVSS (Common Vulnerability Scoring System) e del potenziale impatto sui clienti, la correzione di queste vulnerabilità diventa la nostra massima priorità. Anche la correzione delle vulnerabilità presenti nei sistemi operativi e nei software di terze parti integrati nei nostri prodotti è ugualmente importante.

La piattaforma di **segnalazione delle vulnerabilità HackerOne** ci fornisce uno strumento flessibile e articolato per l'analisi dei report provenienti dai ricercatori. Il flusso di lavoro per l'elaborazione dei report inizia dalla classificazione delle criticità e include l'assegnazione di ricompense (bug bounty) ai ricercatori e l'analisi dei rischi legati alla divulgazione di informazioni sensibili su una particolare vulnerabilità (un hacker può richiedere la completa o parziale divulgazione delle informazioni su una vulnerabilità dopo la sua correzione e il rilascio della stessa al pubblico).

Alcuni utenti preferiscono inviare le proprie segnalazioni direttamente a noi tramite la **casella di posta dedicata** all'indirizzo vulnerabilities@kaspersky.com. Per l'invio di queste informazioni sensibili consigliamo di utilizzare la crittografia tramite la nostra chiave PGP pubblica, una pratica comune per salvaguardare questo tipo di condivisione dati.

Fonti dei report sulle vulnerabilità



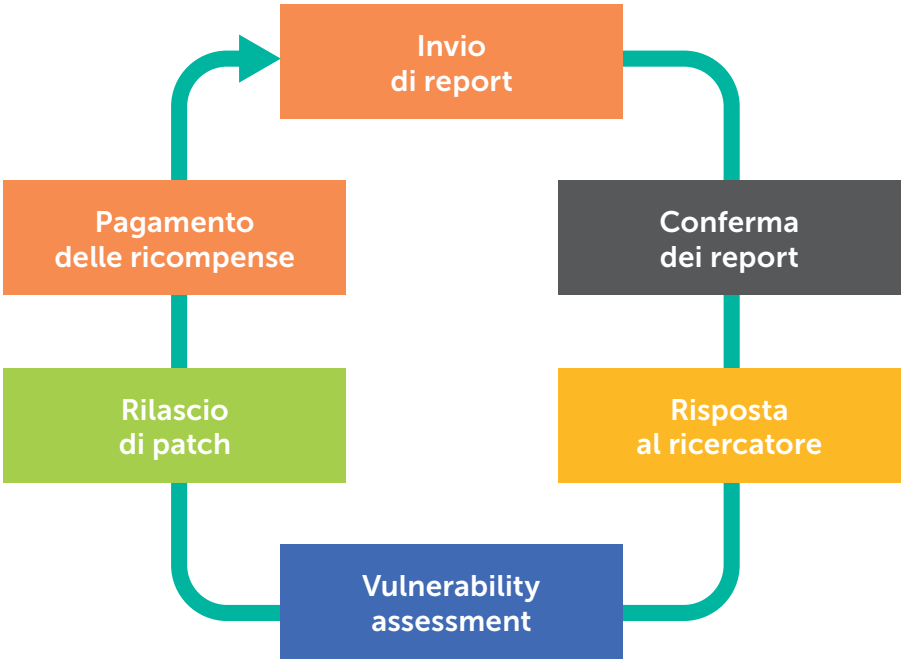
Risposta ai report

La risposta ai report sulle vulnerabilità è un processo separato con un flusso di lavoro specifico. Tale processo inizia quando riceviamo informazioni su una potenziale vulnerabilità che potrebbe interessare i nostri prodotti. A volte riceviamo un report che fa riferimento a una vulnerabilità presente in uno dei nostri prodotti, ma in realtà si riferisce al punto debole di un sistema operativo. In questi casi, forniamo anche un aggiornamento per mitigare l'evento.

Il coinvolgimento di Kaspersky Lab nel programma di ricompense Bug Bounty su HackerOne è pensato per rispondere alle crescenti sfide nel settore della sicurezza. Naturalmente abbiamo progettisti e ricercatori altamente specializzati all'interno della nostra azienda, ma riconosciamo il valore aggiunto che possono fornire i ricercatori esterni e indipendenti. Inoltre, permettendo ai ricercatori esterni di testare i nostri prodotti, li rendiamo ancora più sicuri e affidabili.

Siamo anche convinti che utilizzare le segnalazioni di hacker dietro pagamento sia un approccio intelligente e realista: se non lo facessimo, potrebbero essere tentati di vendere le loro informazioni ai cybercriminali. I loro report devono soddisfare requisiti molto severi, che includono una descrizione dettagliata della vulnerabilità segnalata, dettagli tecnici ed esempi di exploit efficaci o di Proof of Concept.

Flusso di lavoro dell'elaborazione delle vulnerabilità in uno scenario Bug Bounty



L'ambito del nostro programma Bug Bounty al momento copre Kaspersky Internet Security 2019 Beta e Kaspersky Endpoint Security 11. Gli exploit delle vulnerabilità devono essere applicabili a Windows 8.1+ e le ricompense vengono assegnate per vulnerabilità Remote Code Execution (RCE), Local Privilege Escalation (LPE) e Information Disclosure (ID); quest'ultimo è limitato a dati utente sensibili come password, dati di pagamento e token di autenticazione. Per un report dettagliato e un esempio di exploit della vulnerabilità <<unicorn>>, che consente all'autore dell'attacco di eseguire da remoto codice malevolo all'interno di un processo con privilegi elevati tramite il vettore "man-in-the-middle", la ricompensa può arrivare a $ 100.000

	Anello 3 (bassi privilegi)	Anello 3 (alti privilegi)	Anello 0	Anello -1
Aggiramento dell'antivirus				
Information Disclosure (ID)				
Local Privilege Escalation (LPE) (escalation di privilegi)				
Vulnerabilità Remote Code Execution (RCE)				

Tipi di vulnerabilità individuati nei prodotti antivirus. Gli autori degli attacchi aggirano l'antivirus per eludere le funzionalità principali della protezione di un prodotto. Più il cubo è scuro, maggiore è il grado di pericolo

- Nella Modalità utente (**Anello 3**) vengono eseguiti il servizio antivirus e i processi GUI: l'antivirus è un processo ad alta priorità, mentre il processo GUI ha bassa priorità.
- I driver dell'antivirus vengono eseguiti in **Modalità kernel** (**Anello 0**) e ottengono l'accesso al kernel Windows e a tutti i processi nella memoria virtuale. Questo tipo di exploit è molto pericoloso perché l'Anello 0 è quello con più privilegi e, se l'attacco avesse successo, l'intero sistema sarebbe compromesso.
- Alcuni prodotti antivirus contengono speciali componenti che operano a livello di hypervisor (noto come **Anello -1**). Questi componenti controllano le operazioni della memoria virtuale e proteggono dallo screenshotting. L'exploit di una vulnerabilità a questo livello compromette le macchine virtuali e può anche bypassare le misure di sicurezza integrate (come Device Guard e Credential Guard).

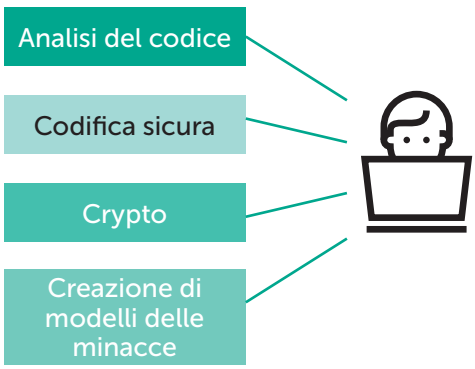
Mai smettere di imparare

A nostro avviso, la costante integrazione di best practice all'interno del nostro SDL non è sufficiente a garantire la sicurezza; è anche necessario che i nostri sviluppatori e progettisti ricevano una formazione approfondita. Utilizziamo le competenze acquisite dal nostro dipartimento R&D in materia di sviluppo e le arricchiamo con i dati forniti dal nostro security team, impegnato ad aggiornare costantemente le "practice" in uso e a testarne di nuove Il risultato è l'implementazione dei seguenti vettori nei nostri programmi formativi sulla sicurezza del prodotto:

Formazione sulla sicurezza per sviluppatori, ingegneri e progettisti

Questo approccio è estremamente vantaggioso per i nostri sviluppatori e per l'intera azienda (per maggiori informazioni, fare riferimento all'immagine riportata di seguito). Non solo incoraggia gli sviluppatori a considerare molteplici ambiti di sicurezza che potrebbero altrimenti essere ignorati, ma aiuta anche a ridurre il costo totale degli interventi di manutenzione del software e a consolidare la nostra reputazione.

Vantaggi della formazione continua per sviluppatori

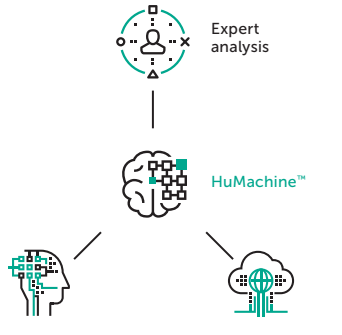


Vantaggi

- Minori spese per problemi di aggiornamento
- Numero maggiore di risorse disponibili per il supporto dei prodotti
- Miglioramento della reputazione dell'azienda
- Miglioramento delle competenze degli sviluppatori

La sicurezza è al centro del nostro operato

Il processo di creazione di un software sicuro non è semplice, soprattutto quando si tratta di soluzioni e prodotti complessi. Per offrire livelli di protezione ottimali, la sicurezza deve essere al centro di ogni fase del processo di sviluppo e manutenzione del software: la stesura dei requisiti di sicurezza, l'assessment dei rischi, l'analisi della superficie di attacco, il fuzzing, i penetration test, vulnerability response e la formazione degli sviluppatori. Questo è esattamente ciò che facciamo in Kaspersky Lab. Il risultato? La sicurezza più testata e premiata al mondo.



Kaspersky Lab
Trovate il partner più vicino: **www.kaspersky.com/buyoffline**
Kaspersky for Business: **www.kaspersky.com/business**
Enterprise Cybersecurity: **www.kaspersky.com/enterprise**
Novità sulla sicurezza IT: **business.kaspersky.com/**
Il nostro approccio unico: **www.kaspersky.it/true-cybersecurity**

#truecybersecurity
#HuMachine

www.kaspersky.it