WHITE PAPER

Secure by Design: integrare la cybersecurity fin dalle fondamenta

Perché questa filosofia è importante e come riduce la superficie di attacco dall'interno

SOPHOS

Riepilogo

Secure by Design è una filosofia di sviluppo del software basata sul considerare la sicurezza come un requisito fondamentale, non un extra da aggiungere dopo.

Anziché realizzare prima un prodotto e aggiungere misure di sicurezza in un secondo momento, l'approccio Secure by Design esige l'integrazione degli aspetti relativi alla sicurezza in ogni fase del ciclo di vita di sviluppo: da architettura e progettazione, fino a codifica, test, distribuzione e manutenzione.

L'idea di fondo è semplice: creando un sistema sicuro fin dalle fondamenta, gli utenti saranno protetti automaticamente, e non solo quando sanno come configurare le giuste impostazioni o quando le lacune di sicurezza vengono risolte a posteriori.

In termini pratici, questo significa adottare principi come l'assegnazione di meno privilegi possibili (concedere a utenti e processi solo l'accesso minimo di cui hanno bisogno), l'uso di impostazioni predefinite sicure (fornire prodotti con la configurazione più sicura fin dal primo utilizzo), una difesa in profondità (che applica controlli di sicurezza a più livelli, in modo che nessun singolo errore possa avere conseguenze catastrofiche) e l'eliminazione di intere categorie di vulnerabilità attraverso linguaggi, framework e modelli di progettazione più sicuri.

L'idea di fondo è semplice:

creando un sistema sicuro fin dalle fondamenta, gli utenti saranno protetti automaticamente, e non solo quando sanno come attivare le giuste impostazioni o quando le lacune di sicurezza vengono risolte a posteriori.

Qual è il motivo per cui è stato introdotto l'approccio Secure by Design?

Per vari decenni, molti player nel settore delle tecnologie hanno adottato un modello di tipo "Rilascia subito, correggi dopo". Una conseguenza ereditata da questa approccio è il fatto che la sicurezza informatica può essere vista semplicemente come un "centro di costo", ovvero come un fattore che rallenta i rilasci e genera frustrazione tra gli sviluppatori. L'impatto di questa mentalità si sta manifestando in tempo reale: continue segnalazioni di vulnerabilità, patch di emergenza rilasciate in fretta e furia, nonché violazioni che costano alle aziende diversi miliardi e che allo stesso tempo mettono a rischio i dati personali di centinaia di milioni di persone.

Le vulnerabilità di Ivanti Connect Secure, l'exploit di Log4Shell in un'onnipresente libreria open source, e le vulnerabilità di MOVEit Transfer sono tutti casi che hanno dimostrato come una sicurezza reattiva non sia in alcun modo in grado di tenere il passo con cybercriminali estremamente determinati.

Consapevole di questo squilibrio, nel 2023 la Cybersecurity and Infrastructure Security Agency (CISA) degli Stati Uniti, in collaborazione con partner internazionali, ha pubblicato linee guida ufficiali su Secure by Design, esortando i produttori di tecnologie ad assumersi la responsabilità dei risultati di sicurezza dei propri clienti.

I principi di Secure by Design stabiliscono che la responsabilità della sicurezza deve ricadere sui produttori che realizzano i prodotti, non sugli utenti finali che li implementano. Questo ha cambiato il modo in cui i produttori considerano la sicurezza dei prodotti tecnologici, spostando il dibattito dalla responsabilità individuale ("gli utenti devono applicare tempestivamente le patch") alla responsabilità del produttore ("i produttori devono commercializzare prodotti sicuri fin dal primo utilizzo").

Perché l'approccio Secure by Design è fondamentale per gran parte delle soluzioni di cybersecurity

È un monito emblematico di come a volte anche gli strumenti di sicurezza possono diventare il punto di accesso di un attacco. Eppure, ciò accade con una regolarità allarmante.

Questo mette in luce un punto debole critico per molte organizzazioni: una volta che un dispositivo perimetrale viene compromesso, gli autori dell'attacco continueranno a colpirlo ripetutamente, finché non sarà stato protetto in modo completo. I firewall e altri sistemi perimetrali possono rimanere vulnerabili anche dopo che è stato reso disponibile un fix. Considerando tutte le vulnerabilità soggette a exploit che sono state confermate nell'ambito di recenti analisi di incidenti risolti da Sophos, il tempo mediano trascorso tra la pubblicazione di un avviso o di una patch da parte del produttore e l'exploit di tale vulnerabilità da parte di un criminale è stato di 322 giorni: quasi un anno intero di opportunità per gli autori degli attacchi. I produttori di soluzioni di cybersecurity non possono presumere che gli utenti applichino immediatamente le patch.

Il problema della posizione privilegiata

Gli strumenti di sicurezza informatica si trovano nei punti più sensibili dell'infrastruttura aziendale. Gli agenti di rilevamento per gli endpoint vengono eseguiti con accesso a livello di kernel. Le piattaforme SIEM acquisiscono log da tutti i sistemi. I provider di identità custodiscono le chiavi di ogni account. I firewall sono situati al confine tra reti attendibili e non attendibili.

Quando i prodotti di sicurezza costituiscono il fulcro delle difese di un'organizzazione, si caricano di una maggiore responsabilità al momento di applicare i principi di Secure by Design. I produttori che operano del nostro settore svolgono un ruolo fondamentale nella tutela dei clienti, e tale fiducia comporta delle aspettative sul modo in cui vengono progettati i prodotti.

Questa posizione privilegiata implica che una vulnerabilità in un prodotto di sicurezza non espone solo quel prodotto, bensì tutti i sistemi che era stato costruito per proteggere. Un cybercriminale che compromette un agente EDR (Endpoint Detection and Response) non accede a un semplice strumento: ottiene il controllo dell'endpoint con i privilegi più elevati. Una vulnerabilità in un'appliance VPN non compromette soltanto l'accesso remoto, ma offre a un criminale un tunnel diretto che elude tutti i controlli perimetrali.

Cosa succede quando Secure by Design viene ignorato?

Le conseguenze della mancata osservanza di Secure by Design sono ben documentate: se questi principi non vengono seguiti correttamente, le aziende, gli utenti e l'intera Internet diventano meno sicuri.

- **Costi sempre più elevati in caso di violazione.** Quando le vulnerabilità vengono individuate dopo il rilascio di una soluzione, applicare fix risulta esponenzialmente più costoso rispetto alla loro risoluzione in fase di sviluppo.

- **Perdita di fiducia.** Clienti, enti normativi e partner perdono fiducia nelle organizzazioni che subiscono incidenti di sicurezza ripetuti. I danni alla reputazione possono protrarsi per anni dopo la risoluzione dei problemi tecnici.

- **Rischi normativi e legali.** I governi di tutto il mondo stanno inasprendo le normative in materia di sicurezza informatica. Il Regolamento sulla ciberresilienza dell'Unione Europea, ad esempio, imporrà requisiti di sicurezza obbligatori per i prodotti dotati di componenti digitali venduti in Europa. Le organizzazioni che ignorano i principi di Secure by Design rischiano di risultare non conformi alle normative, di incorrere in sanzioni e di essere escluse dal mercato.

- **Rischi per la sicurezza nazionale.** Le infrastrutture critiche, quali reti elettriche, impianti di trattamento dell'acqua, e sistemi sanitari, dipendono sempre di più da dispositivi e sistemi connessi a Internet. I prodotti con impostazioni predefinite non sicure in questi ambienti creano possibilità di intrusione per cybercriminali e autori di ransomware sponsorizzati da governi, con conseguenze potenzialmente in grado di sconvolgere la vita quotidiana delle persone coinvolte.

- **Stress da applicazione perpetua delle patch.** Senza basi solide, le organizzazioni rimangono intrappolate in un circolo vizioso di reattività: individuano le vulnerabilità, stabiliscono le priorità delle patch, testano gli aggiornamenti e distribuiscono fix. E il tutto si ripete all'infinito. Questo comporta un dispendio di risorse che potrebbero invece essere destinate a indagini di cybersecurity più approfondite.

Come scegliere un firewall Secure by Design

Nel valutare il tuo prossimo firewall, assicurarti che sia veramente Secure by Design deve essere una priorità assoluta. Tuttavia, può risultare difficile vedere oltre le strategie di marketing delle aziende produttrici e comprendere quali siano le funzionalità effettivamente offerte da una soluzione. I criteri indicati di seguito ti aiuteranno a identificare le caratteristiche essenziali da considerare quando scegli un firewall basato sui veri principi dell'approccio Secure by Design:

1. Architettura con protezione avanzata

Come abbiamo visto, è fondamentale che l'architettura del firewall sia progettata, dal codice fino al nucleo del sistema, secondo i principi di Secure by Design. Naturalmente, però, è molto difficile sapere quali misure abbia intrapreso un determinato produttore di firewall per incrementare la sicurezza della sua soluzione. La maggior parte dei produttori sostiene che i propri prodotti siano sicuri, ma in ultima analisi saranno i risultati recenti a rivelare la verità.

Ecco alcuni degli aspetti più ovvi da verificare:

- Supporto dell'autenticazione multifattoriale (MFA) in tutti gli ambiti del firewall (amministrazione, VPN, portali).
- Supporto integrato di Zero Trust Network Access (ZTNA), che consente di eliminare la necessità di una VPN di accesso remoto.
- Gestione remota sicura che NON richiede né l'uso di SSH, né l'accesso remoto al dispositivo da Internet.
- Portali utenti con protezione avanzata, e containerizzati se sono esposti a Internet.
- Aggiornamenti recenti riportati nelle note di rilascio, che indicano che vengono adottati i principi di Secure by Design.

2. Applicazione automatica di patch alle vulnerabilità, senza bisogno di tempi di inattività

Uno dei principali vettori di attacco contro l'infrastruttura di rete è costituito dalle vulnerabilità alle quali non sono state applicate patch. Una volta individuata una vulnerabilità, possono passare diverse settimane prima che venga effettivamente corretta. Molti utenti soffrono di stress da applicazione delle patch, poiché sono costretti ad applicare continuamente nuove patch e a dover gestire i tempi di inattività che implicano.

Semplificati la vita e automatizza l'applicazione tempestiva di patch ai tuoi sistemi, collaborando con un produttore che offra aggiornamenti automatici over-the-air senza bisogno di tempi di inattività. Non lasciarti ingannare dalle promesse di marketing di presunti "aggiornamenti automatici": verifica cosa viene inteso esattamente con questa definizione. Se un aggiornamento richiede comunque un riavvio e un periodo di inattività, non è per nulla "automatico".

3. Controllo automatico dei rischi di configurazione

Un altro fattore che contribuisce frequentemente agli incidenti di sicurezza sono gli errori di configurazione del firewall. Purtroppo, la maggior parte dei firewall non segnala eventuali errori di configurazione, lasciando così esposte vulnerabilità che potrebbero essere sfruttate. Il tuo prossimo firewall deve garantirti controlli automatici e continui delle configurazioni più importanti, e deve mettere in evidenza le impostazioni ad alto rischio per permetterti di correggerle facilmente.

4. Monitoraggio proattivo da parte del produttore

Quando la maggior parte dei firewall subisce un attacco, spesso il cliente non se ne accorge finché non è troppo tardi. Fortunatamente, non tutti i firewall sono così. Scegli un produttore di firewall che monitori i propri prodotti da remoto, raccogliendo dati di telemetria per rilevare i segnali di compromissione che si manifestano nelle fasi iniziali di un attacco. I produttori devono essere disposti e in grado di intervenire tempestivamente qualora vengano rilevate attività anomale, contattando immediatamente te o il tuo partner di cybersecurity per aiutare a identificare e sventare l'attacco.

5. Un produttore che adotta l'approccio Secure by Design

Benché possa apparire scontato, se hai letto fino a questo punto è probabile che tu abbia già in mente un produttore che dimostra un chiaro impegno nei confronti dei principi di Secure by Design. Ma non basarti solo sulle sue affermazioni. Valutane la storia recente, leggine i report sui progressi e le note di rilascio per comprendere esattamente quanto sia impegnato a garantire la tua sicurezza.

L’impegno di Sophos nei confronti dei principi di Secure by Design

L’8 maggio 2024, Sophos è diventata una delle prime aziende ad aderire all’iniziativa Secure by Design della Cybersecurity and Infrastructure Security Agency (CISA) degli Stati Uniti, che si concentra su sette pilastri fondamentali della sicurezza delle tecnologie e dei prodotti:

1. Autenticazione multifattoriale.
2. Password predefinite.
3. Riduzione di intere categorie di vulnerabilità.
4. Patch di sicurezza.
5. Policy per la comunicazione della presenza di vulnerabilità.
6. CVE.
7. Prova di intrusioni.

In linea con i nostri valori aziendali di base, fondati sulla trasparenza, il principio Secure by Design è stato per noi un punto di riferimento essenziale nel nostro processo di valutazione e miglioramento continuo delle pratiche di sicurezza.

Abbiamo pubblicato i dettagli del nostro impegno formale per il miglioramento e condividiamo pubblicamente i progressi che stiamo compiendo nell’ambito dei sette pilastri fondamentali del framework Secure by Design. Naturalmente, la cybersecurity è in continua evoluzione e il lavoro non è mai concluso. Il continuo perfezionamento e miglioramento dell’applicazione dei principi di Secure by Design nella nostra intera linea di soluzioni costituisce una parte fondamentale e costante della nostra filosofia aziendale.

Sophos si distingue da altri produttori perché offre diverse funzionalità importanti, basate sull’approccio Secure by Design, che migliorano in modo significativo il profilo di sicurezza di Sophos Firewall, e che allo stesso tempo semplificano notevolmente il tuo lavoro. Sophos Firewall è l’unico firewall sul mercato che offre patch di sicurezza effettivamente automatiche e distribuite over-the-air, senza alcun periodo di inattività. Inoltre, siamo l’unico produttore che monitora attivamente l’intera base installata di firewall dei clienti, per individuare eventuali segnali di attacco, in modo da poter intervenire rapidamente per aiutare il tuo team e il tuo partner di cybersecurity a risolvere il problema, e garantire protezione immediata contro attacchi simili anche a tutti gli altri clienti.

Conclusioni

In linea con i nostri valori aziendali di base, fondati sulla trasparenza, il principio Secure by Design è stato per noi un punto di riferimento essenziale nel nostro processo di valutazione e miglioramento continuo delle pratiche di sicurezza.

L'ultima versione (v22) di Sophos Firewall estende ulteriormente le proprie funzionalità Secure by Design, migliorando significativamente il profilo di sicurezza del firewall. Queste funzionalità includono:

- Una nuova opzione di Controllo dello stato di integrità, che riduce il rischio che un errore di configurazione possa potenzialmente causare un attacco.
- Un piano di controllo completamente nuovo, riprogettato per garantire massima sicurezza e scalabilità, che elimina un'intera categoria di vulnerabilità.
- L'introduzione di un Sophos XDR Linux Sensor che ottimizza il monitoraggio in tempo reale dell'integrità dei sistemi di tutti i tuoi clienti da parte dei nostri team di sicurezza, che consente di identificare gli attacchi e reagire più rapidamente.
- Aggiornamenti del firmware crittografati e dotati di certificate pinning, per garantirne l'autenticità.
- Un upgrade all'ultima versione del motore antimalware di Sophos, che offre rilevamento avanzato, zero-day e in tempo reale delle minacce emergenti.

La nostra attività nell'ambito della campagna Pacific Rim ci ha permesso di osservare da vicino come operano cybercriminali determinati e dotati di ottime risorse, nonché di comprendere quali sono le misure necessarie per difendersi dai loro attacchi. La campagna ha confermato che gli active adversary non attendono passivamente che emergano vulnerabilità, ma sono attivamente alla ricerca di errori progettuali, vulnerabilità di configurazione e sistemi privi di patch nell'infrastruttura globale. L'esperienza che abbiamo acquisito ha influenzato direttamente il nostro approccio Secure by Design.

Ha messo in evidenza il fatto che le moderne strategie di difesa devono partire dalla riduzione della superficie di attacco a livello di prodotto, integrando impostazioni predefinite sicure, inasprendo i percorsi di autenticazione ed eliminando le possibilità di utilizzo improprio, ben prima che una vulnerabilità possa emergere.

La strada da percorrere

Secure by Design non elimina completamente le vulnerabilità, e non esonera le aziende dal dovere di mantenere una vigilanza costante. Ciononostante, è diventato un pilastro fondamentale della cybersecurity per ridurre la superficie di attacco. La questione non è più se Secure by Design sia una buona idea, ma con quanta rapidità viene adottato.

È ora di valutare il tuo programma di cybersecurity.

Parla subito con un esperto Sophos.

Vendite per l'Italia
Tel: (+39) 02 94 75 98 00
E-mail: sales@sophos.it