Kaspersky mette in sicurezza le Blockchain in-house

Set 04, 2019 Kaspersky Kaspersky Partner Space 0

Kaspersky ha lanciato un nuovo servizio per aiutare le organizzazioni a proteggere le applicazioni basate su blockchain sviluppate in-house.

Kaspersky Enterprise Blockchain Security include l'assessment delle applicazioni che lavorano su un'infrastruttura blockchain e un audit del codice degli smart contract. Il nuovo servizio aiuta le aziende a individuare e correggere i problemi di sicurezza e le discrepanze nella business logic degli smart-contract, mentre il progetto blockchain passa dall'innovazione interna a parte dei processi aziendali.

Rispettando le previsioni dell'International Data Corporation (IDC), secondo cui la spesa mondiale per le blockchain raggiungerà gli 11,7 miliardi di dollari entro il 2022[1], le aziende stanno considerando questa tecnologia come supporto per la realizzazione di progetti data-driven, su vasta scala in grado di garantire maggiore trasparenza ed efficienza. Ad esempio, nell'aprile 2019, la Société Générale SFH, controllata di covered bond della Société Générale, ha emesso la prima obbligazione garantita del valore di 100 milioni di euro, come security token in una blockchain pubblica[2]. Nel settore farmaceutico, la blockchain viene utilizzata per tracciare il trasferimento dei farmaci dal produttore al consumatore finale, garantendo maggiore chiarezza sulla supply chain[3].

Sebbene nelle innovation division interne delle aziende, i progetti sulle blockchain siano in una fase iniziale di sviluppo, la loro sicurezza non figura ancora tra le priorità dei Chief Information Security Officers. Infatti, l'indagine di Kaspersky sui CISO ha evidenziato che solo il 15% ritiene che la blockchain possa diventare la tecnologia con il maggiore impatto nel settore IT. Nonostante ciò, ad un certo punto, queste applicazioni che trattano dati sensibili si integreranno con altri sistemi business-critical. Quando questo accadrà, le persone a capo dei team di innovazione interna dovranno eseguire controlli di sicurezza e dare approvazioni e questo potrebbe avere ripercussioni sulle scadenze o mettere a rischio il lancio dei progetti.

Kaspersky Enterprise Blockchain Security consiste in una gamma di servizi tra cui Smart Contract / Chain Code Audit e Application Security Assessment. Il servizio garantisce la corretta configurazione delle logiche aziendali degli smart contract e delle operazioni di sicurezza delle applicazioni blockchain.

Smart Contract / Chain Code Audit rivela la non conformità di comportamenti documentati e le possibili vulnerabilità, nonché errori nella logica di business. Quest'ultima può ostacolare l'adempimento delle operazioni (ad esempio, se il chain code utilizza dati errati della blockchain) o conduce a risultati errati causati dall'errore di uno sviluppatore o da intenzioni malevole. Come risultato di questa audit del chain code, le aziende possono avere la certezza che gli smart contract funzionino correttamente come indicato nella documentazione e che i dati non vengano sottratti.

L'**Application Security Assessment** è stato progettato in modo tale da rivelare le vulnerabilità presenti all'interno delle applicazioni che lavorano nell'infrastruttura blockchain, per garantire che non abbiano un impatto sull'integrità della stessa. Questo processo omnicomprensivo utilizza una combinazione di test: white-box (basati sull'analisi del codice sorgente) grey-box (che emula il lavoro di utenti legittimi), e black-box (che emula un attaccante esterno esperto) per garantire che non vengano trascurati potenziali rischi o vulnerabilità. I risultati della valutazione sono riportati in un report che descrive nel dettaglio i risultati tecnici delle eventuali vulnerabilità identificate e le relative raccomandazioni per appianarle. Ciò permette alle aziende di fronteggiare i rischi alla sicurezza prima che possano provocare dei danni.

"Da un paio di anni le aziende stanno lavorando allo sviluppo di applicazioni blockchain e adesso queste innovazioni sono pronte per essere implementate all'interno delle infrastrutture aziendali. Tuttavia, i team responsabili

dell’innovazione e di queste tecnologie potrebbero incontrare ulteriori ostacoli in termini di risk management e sicurezza IT. Questi timori non sono affatto infondati: con l’aumentare del numero di applicazioni blockchain a livello aziendale è probabile che diventino più frequenti anche gli attacchi. C’è una crescente domanda di assessment della sicurezza informatica da parte dei team di sviluppo delle blockchain che vogliono preservare i propri progetti. La nostra nuova offerta è volta a soddisfare questa esigenza”, **ha dichiarato Vitaly Mzokov, Head of Innovation Hub at Kaspersky**

Maggiori informazioni sui servizi di Kaspersky sono disponibili a questo link.

[1] IDC Worldwide Blockchain 2018-2022 Forecast

[2] https://www.societegenerale.com/en/newsroom/first-covered-bond-as-a-security-token-on-a-public-blockchain

[3] https://www.computerworld.com/article/3412319/how-blockchain-is-being-used-in-enterprise.html#slide3

Condividi l’articolo

Il 50% degli smartphone Android vulnerabili a un attacco via SMS Gli exploit per Android valgono più di quelli per iOS

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/09/04/kaspersky-mette-in-sicurezza-le-blockchain-in-house/