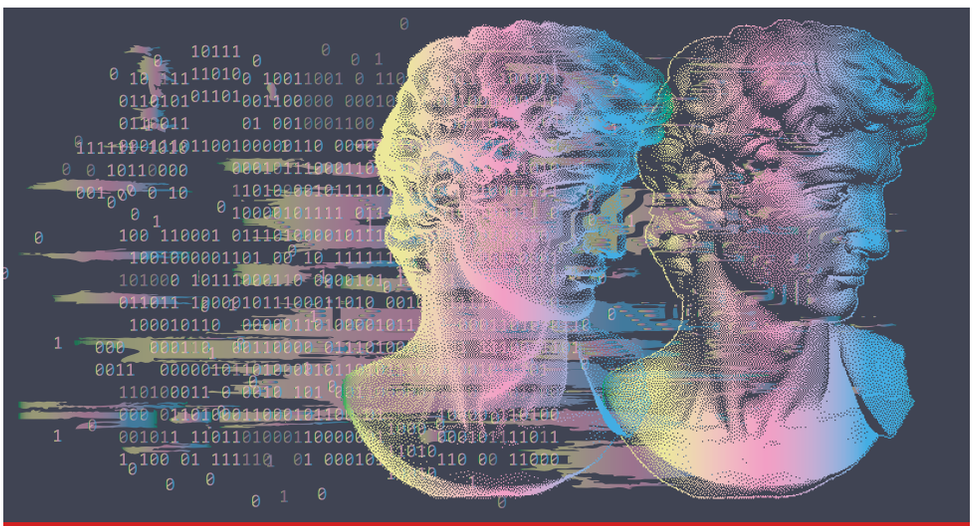
Ilona Simpson

Il digital twin non è al sicuro

Con la diffusione dei gemelli digitali è importante considerare le implicazioni sulla sicurezza informatica di queste tecnologie

Fonte: foto Shutterstock



I sistemi digital twin dovrebbero essere opportunamente segmentati e isolati da altri sistemi e reti per limitare il potenziale impatto di un attacco informatico

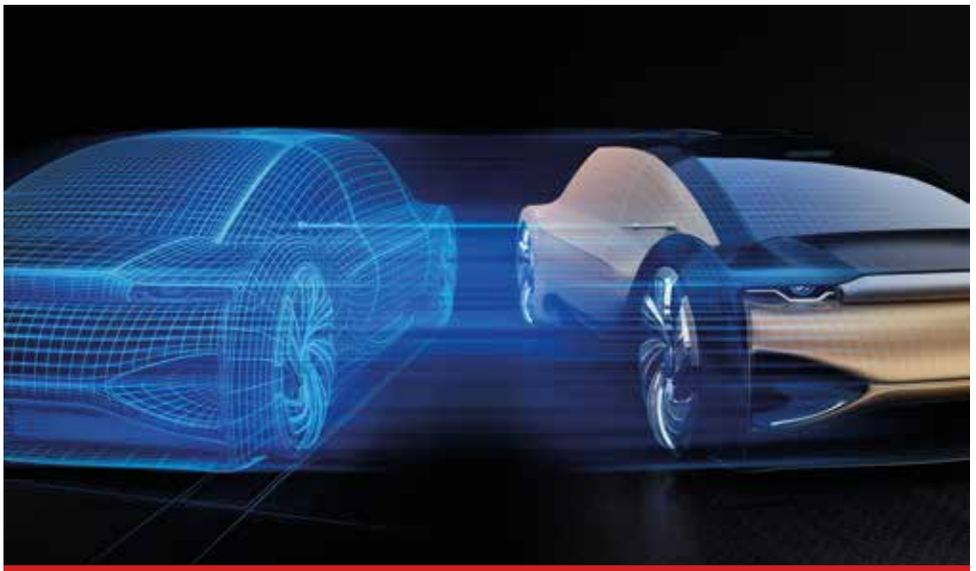
Per digital twin (gemello digitale) si intende una replica virtuale, quindi digitale, di un oggetto, un asset, un processo o un sistema fisico. Viene utilizzato per eseguire simulazioni e analisi per ottimizzare le prestazioni nel mondo reale di questo oggetto, asset, processo o sistema. I digital twin sono diventati sempre più popolari in molti settori, tra cui produzione, assistenza sanitaria e trasporti. Tuttavia, man mano che i gemelli digitali diventano sempre più diffusi, è importante considerare le implicazioni sulla sicurezza informatica di queste tecnologie. Uno dei principali rischi associati ai digital twin è che possono fornire ai criminali informatici un nuovo modo per accedere e sfruttare le informazioni sensibili. Ad esempio, il digital twin di un impianto di produzione potrebbe fornire agli attaccanti informazioni dettagliate su layout, apparecchiature e processi utilizzati nell'impianto. Queste informazioni potrebbero essere utilizzate per pianificare ed eseguire un attacco informatico mirato. I digital twin potrebbero anche essere utilizzati dai criminali informatici come un modo per accedere e attaccare le risorse fisiche su cui sono modellati. Ad esempio, il digital twin di una centrale elettrica potrebbe essere utilizzato per ottenere l'accesso non autorizzato ai controlli dell'impianto, causando potenzialmente danni o interruzioni, negli scenari peggiori interrompendo i servizi essenziali, danneggiando persone, animali o l'ambiente. Per mitigare questi rischi, le organizzazioni devono adottare un approccio proattivo per proteggere i loro digital twin. Questi sistemi sono complessi e non è sufficiente guardarli in modo lineare, come se fossero pezzi isolati cuciti insieme grossolanamente: un tale approccio produrrà sempre protezioni non ottimali. Naturalmente, e come con qualsiasi sistema, l'autenticazione, l'autorizzazione e l'accesso robusti dovrebbero far parte di una cyber hygiene di base, ma la protezione di un digital twin richiede di più.

Identificare le cause

Stamp è un modello per identificare le cause degli incidenti che utilizza la teoria dei sistemi e il pensiero sistemico. Sviluppato da Nancy Leveson al MIT, tiene conto di un'ampia gamma di fattori che possono contribuire agli incidenti, come il software, il processo decisionale umano, le nuove tecnologie, i fattori organizzativi e sociali e la cultura generale della sicurezza. È particolarmente utile per analizzare sistemi complessi in cui questi fattori stanno diventando sempre più importanti. Se utilizzato ai fini della pianificazione degli incidenti con i digital twin, svolge un buon lavoro di analisi del rischio con la consapevolezza che il lato fisico di un digital twin è più di una somma totale di singole parti.

I professionisti della sicurezza che lavorano per proteggere i digital twin dovrebbero assicurarsi di non ignorare lo scopo del sistema e devono anche catturare i peggiori risultati di un potenziale attacco. E questo deve essere fatto prendendo in considerazione domande come: Che aspetto ha la gerarchia dei controllori (sistemi, persone, policy e persino regolamenti) e le loro interazioni? Dove sono le vulnerabilità e come possono essere sfruttate? Quali misure possono essere adottate per evitare/ridurre l'impatto negativo di un incidente? Prevenire è meglio che curare, ma le organizzazioni dovrebbero pianificare entrambe le cose. È essenziale un solido piano

Fonte: foto Shutterstock



Stamp, se utilizzato ai fini della pianificazione degli incidenti con i digital twin, svolge un buon lavoro di analisi del rischio

di risposta agli incidenti che includa procedure per rilevare, rispondere e rimediare agli attacchi informatici. Questo piano dovrebbe essere regolarmente testato e aggiornato per garantire che rimanga efficace in caso di incidente reale. È importante condurre regolari test di penetrazione su sistemi digital twin per identificare e affrontare le vulnerabilità prima che possano essere sfruttate dagli attaccanti. Ciò può essere fatto simulando attacchi informatici ai sistemi digital twin, quindi valutando la risposta del sistema e identificando eventuali punti deboli che devono essere affrontati. E i sistemi digital twin dovrebbero essere opportunamente segmentati e isolati da altri sistemi e reti. Ciò limita il potenziale impatto di un attacco informatico riuscito sui sistemi digital twin e impedisce all'attaccante di spostarsi lateralmente e accedere ad altri dati o sistemi sensibili. I digital twin sono una tecnologia potente e la loro crescente popolarità riflette il valore che possono apportare. Tuttavia, introducono anche nuovi rischi per la sicurezza informatica che devono essere affrontati. Le organizzazioni devono adottare un approccio proattivo per proteggere i loro digital twin e devono implementare solide misure di sicurezza per proteggersi dagli attacchi informatici. In questo modo, possono garantire meglio la sicurezza e la protezione dei loro sistemi digital twin e delle risorse fisiche che rappresentano.

Netskope - www.netskope.com