Previsioni per il 2020: il futuro del cloud, veicoli e dispositivi medici connessi e cybersicurezza

17 dicembre 2019

Peter Galvin | Chief Strategy Officer
Informazioni sull'autore >

Veicoli autonomi. Cloud computing. Dispositivi medici connessi. Violazioni dei dati.

Tra gli argomenti più discussi negli ultimi anni all'interno del settore tech spiccano questi casi d'uso, invenzioni e sfide, che sono destinati a subire una trasformazione significativa nei prossimi 12 mesi.

I motivi di questo cambiamento più che plausibile sono dettati da una combinazione di nuove conoscenze, progressi tecnologici e una migliore organizzazione. Tutto ciò è in gran parte (ma non esclusivamente!) positivo.

Cosa possiamo aspettarci nel 2020 in queste aree rilevanti per il settore? Ecco le mie previsioni.

La strada da percorrere per le auto a guida autonoma diventerà più lunga e limitata

Se anche tu pensi che i veicoli senza conducente appartengano alla fantascienza, sei in buona compagnia: sono in molti a ritenere che le auto che si guidano da sole diventeranno realtà in un futuro piuttosto lontano e in un certo senso, hanno ragione.

Sappiamo tutti che i veicoli autonomi esistono nel mondo reale di oggi, ma ciò non significa che li vedremo presto sfrecciare nel centro delle nostre città. Una volta introdotti nel mercato, infatti, i veicoli a guida autonoma saranno in gran parte soggetti a limitazioni.

Garantire la sicurezza stradale in seguito all'introduzione delle auto senza conducente è una sfida complessa ed è comprensibile che si possa incontrare qualche ostacolo lungo il cammino. Non va dimenticato, inoltre, che tali veicoli hanno causato problemi più gravi del previsto, tra cui una collisione fatale.

La conseguenza? Il lancio di questo tipo di autovetture è molto più lontano di quanto inizialmente ipotizzato e, per questo, assisteremo a un cambiamento nelle modalità di utilizzo. Ad esempio, le auto senza conducente verranno circoscritte a determinati percorsi, sottoposte al rispetto di limiti di velocità specifici e destinate a percorrere solo distanze prestabilite. Proprio come uno skibus, seguiranno un tragitto preciso con responsabilità molto limitate.

L'effetto boomerang favorirà un'adozione generalizzata delle soluzioni multi-cloud e multi-deployment

Secondo le stime di IDC, la spesa globale per il cloud pubblico sarà di 229 miliardi di dollari quest'anno e raggiungerà la soglia dei 500 miliardi nel 2023. Un sondaggio di Gartner indica inoltre che l'81% degli utenti di cloud pubblico collabora con due o più fornitori, ma la società sconsiglia alle aziende di passare in modo troppo precipitoso da un ambiente on-premise a uno multi-cloud. Le varie piattaforme presentano, infatti, piccole differenze che rendono difficile l'interoperabilità tra i servizi, quindi le imprese dovrebbero adottare un approccio graduale alla migrazione per dare al personale interno il tempo di adattarsi alla curva di apprendimento.

Nonostante le sfide, nel prossimo anno mi aspetto di assistere a un'adozione più ampia del multi-cloud, ma ritengo anche che il punto focale del 2020 saranno le tecnologie in grado di supportare gli ambienti cloud on-premise e privati, non solo quelli pubblici. Il merito è dell'effetto boomerang.

Appena un paio d'anni fa, molte organizzazioni stavano pianificando una migrazione completa al cloud pubblico e, in alcuni casi, diverse aziende l'hanno completata per varie applicazioni. In questo processo, molti hanno però riscontrato che il cloud pubblico non costituisce la soluzione più adeguata a tutte le loro esigenze, a causa di problemi di sicurezza, della necessità di riscrivere le applicazioni e di altre difficoltà incontrate. Di conseguenza, alcune app sono tornate a un'implementazione on-premise.

Al giorno d'oggi, le organizzazioni stanno introducendo sempre più ambienti multi-cloud e multi-deployment. La tecnologia avanzata e la sicurezza sono i motivi principali del deployment delle applicazioni, tanto on-premise quanto nel cloud.

A mio parere, continueremo ad assistere a un incremento delle applicazioni aziendali che imitano gli ambienti cloud, anche se di fatto non rientrano nell'ambito del cloud pubblico. Le organizzazioni si occuperanno di creare l'infrastruttura sviluppando un'architettura che consenta di espandere le applicazioni e di attivare/disattivare i carichi di lavoro. Sorprendentemente simili al cloud pubblico, questi ambienti saranno invece creati on-premise o in un cloud privato.

Più assistenza a domicilio con i dispositivi medici connessi

Qualche anno fa, la rivista statunitense WIRED ha pubblicato un articolo dal titolo "Healthcare 2020: The e-Doctor Will See You Now", che prevedeva la probabile diminuzione dei processi cartacei in ambito sanitario. Secondo l'articolo, nel tempo ciò avrebbe contribuito a un maggiore controllo sulla propria salute da parte dei singoli pazienti. L'uso di dispositivi

indossabili, inoltre, avrebbe permesso di monitorare lo stato di salute di ognuno di noi, indipendentemente dal luogo in cui ci troviamo.

Queste tendenze sono già emerse in una certa misura e diventeranno ancora più diffuse nei prossimi 12 mesi.

Nel 2020 assisteremo all'introduzione in ambito domestico di dispositivi medici di grandi dimensioni come i respiratori, che solitamente sono disponibili soltanto nelle strutture ospedaliere. Questi dispositivi saranno più piccoli, connessi a Internet e disponibili per l'uso a domicilio perché collegati alla rete. La possibilità di accedere a questi macchinari a casa propria comporterà un risparmio in termini di tempo e denaro sia per il settore sanitario sia per i pazienti. Questi dispositivi hanno il potenziale di migliorare la salute e salvare vite umane.

Le violazioni dei dati continuano a essere una problematica complessa

L'aumento dei rischi per la sicurezza dei dati è direttamente proporzionale all'incremento del numero di dispositivi collegati alla rete e alla crescente migrazione dei dati personali ai sistemi connessi. Sono questi i motivi per cui, nel 2020, assisteremo a un numero di violazioni uguale o superiore a quello registrato nel 2019.

Molti malintenzionati hanno capito che tali violazioni rappresentano una potenziale miniera d'oro, per cui, dai singoli hacker, le attività criminali sono passate in mano a vere e proprie organizzazioni a caccia di informazioni di identificazione personale.

Particolarmente interessanti per i criminali sono i dati medici, che forniscono informazioni preziose. È emerso, infatti, che una cartella clinica completa può generare fino a 1.000 dollari nel dark web, molto più di un numero di carta di credito o un codice fiscale. Gli utenti non autorizzati violano i dispositivi indossabili e impiantabili per accedere alle cartelle cliniche elettroniche dei pazienti, riuscendo in questo modo a introdursi nel sistema sanitario.

Ma le sfide di cybersicurezza non si limitano a questo scenario: altri fattori che contribuiscono alla complessità della questione includono gli errori umani e la difficoltà delle aziende ad adottare il giusto approccio.

Le organizzazioni devono infatti introdurre meccanismi per il controllo della sicurezza e della privacy, ma disposizioni troppo severe potrebbero allontanare i clienti. Trovare un equilibrio è una vera e propria sfida. Nel prossimo anno, le organizzazioni che introducono misure di sicurezza insufficienti si troveranno nel mirino di attacchi criminali finalizzati alla violazione dei dati.

Visita il sito Web di Entrust per maggiori informazioni sulle nostre soluzioni per la sicurezza e segui l'azienda su Twitter, LinkedIn e Facebook.