RISPONDERE IN MODO RAPIDO ED EFFICACE ALLE MINACCE ODIERNE

Internet rende disponibile in tempo reale una mole di dati senza precedenti che attirano l'interesse di clienti e purtroppo anche di hacker e criminali. Non farti trovare impreparato!

L'utilizzo esponenziale di Smartphone e Tablet aumenta la probabilità di intrusione e amplifica il rischio.
Molte aziende ammettono di non conoscere la reale entità delle minacce che incombono sulle proprie applicazioni, e di non avere le competenze per gestirne l'impatto in autonomia.

Il mondo è oggi interconnesso, tecnologico e intelligente, con imprese che operano a livello internazionale, più complesse e più mobili che nel passato, e quindi l'importanza della sicurezza e dell'adeguamento della protezione per gli endpoint sono continuamente in crescita. Le minacce sono sempre più sofisticate, dinamiche, pericolose e difficili da individuare, pertanto la necessità di trovare un sistema di risposta ad alte prestazioni diventa irrinunciabile.

Il moderno mondo digitale, infatti, non è a prova di errore, si possono sempre presentare incidenti, involontari o volutamente causati. Per ridurre i danni e l'impatto sulle organizzazioni, un'impresa deve saper rispondere rapidamente. Inoltre, al fine di limitare i rischi prima che il danno si presenti, un'organizzazione deve essere in grado di garantire un ottimo livello per la sicurezza, controllando che gli endpoint rispettino gli standard di conformità, automatizzando gli interventi per abbreviare i tempi di risposta e applicando le misure necessarie a controllare le infezioni con soluzioni di quarantena fino all'eliminazione del problema.

Per raggiungere questo grado di agilità sono necessari un controllo complessivo degli endpoint e un'affidabile visualizzazione in tempo reale, non solo per identificare scostamenti dalle regole di conformità, ma anche per riportare rapidamente l'ambiente a un livello stabile. Un sistema di risposta efficiente deve quindi gestire al meglio i dispositivi in remoto - sia in rete che non - con sistemi operativi eterogenei. Deve essere scalabile, per rispondere alle crescenti richieste di rete. Deve saper combinare velocità, rilevamento preciso e tecniche di correzione di altissima qualità, dato che gli attacchi e le minacce risultano sempre più rapidi, sofisticati e difficili da prevenire.

Attacchi all'infrastruttura tecnologica dell'impresa - soprattutto in seguito ad un attacco "zero day", rapido e inatteso - possono comportare gravi perdite a livello di fatturato, produttività, relazioni con la clientela e reputazione.

Grazie al supporto fornito dal team di ricerca e sviluppo IBM X-Force, famoso in tutto il mondo, il portafoglio IBM fornisce soluzioni di security intelligence che aiutano le imprese a proteggere persone, infrastrutture, dati e applicazioni, con soluzioni di identity and access management, database security, application development, gestione del rischio, gestione degli endpoint, network security e molto altro. Tali soluzioni permettono alle imprese di gestire con efficienza i rischi e di proteggere dispositivi mobili, cloud, social media e altre architetture aziendali. Con oltre 6,000 ricercatori, sviluppatori ed esperti impegnati in iniziative di sicurezza, IBM gestisce una delle maggiori organizzazioni al mondo di ricerca e sviluppo in ambito security, e un'altrettanta vasta organizzazione globale per il delivery dei servizi di sicurezza.

IBM X-Force Exchange è una piattaforma di condivisione delle informazioni sulle minacce informatiche basata sul cloud che consente agli utenti di accedere, ricercare ed aggregare rapidamente i dati relativi alle ultime minacce di sicurezza globali, e di collaborare con i propri peers. IBM offre agli utenti collegati l'accesso integrato a tutte le funzionalità del sito: ricerca, inserimento di commenti, raccolte e condivisione, mentre gli ospiti possono comunque ricercare e visualizzare i report.