Bitdefender

Difese extra per rafforzare l'ultimo fronte: crittografia e gestione delle patch

In uno scenario in rapido mutamento, con notizie di attacchi informatici di vaste proporzioni che si susseguono quasi ogni mese, le aziende hanno iniziato a spostare il proprio paradigma in materia di difesa e sicurezza verso l'ottenimento di una maggiore comprensione sul modo in cui si verificano gli attacchi e su come ne diventano bersaglio. Una volta ammessa l'inevitabilità delle violazioni e dopo aver adottato strumenti efficaci di rilevazione e contrasto, gli sforzi dei CISO sono volti principalmente a ridurre al minimo la superficie di attacco e contemporaneamente ad aumentare il livello di protezione della propria infrastruttura. Ed è qui che la gestione delle patch e la crittografia possono fare la differenza.

TENERE FUORI DALLA VISTA LE RISORSE PIÙ PREZIOSE

In base a un sondaggio condotto da Bitdefender tra 1.051 professionisti nel campo della sicurezza IT in Europa e Stati Uniti, quattro CISO su cinque affermano che la crittografia sia il meccanismo più efficace per proteggere i dati, seguito dai software di sicurezza e dalle pratiche di backup. Nei diversi paesi, la crittografia è considerata più affidabile in Italia, nel Regno Unito e negli USA, ma in media solo un'azienda su sei cripta tutti i dati.

Tra i soggetti incaricati di prendere decisioni nell'ambito della sicurezza IT, tre su quattro indicano i costi finanziari e i danni alla reputazione dell'azienda come le peggiori potenziali conseguenze di una violazione avanzata da cui derivi un accesso ai loro "gioielli della corona".
I dati critici riguardanti la proprietà intellettuale devono essere conservati in sede, limitandone l'accesso e la disponibilità esclusivamente al personale autorizzato. Qualsiasi dato archiviato localmente o su cloud dovrebbe essere anche crittografato, in modo da impedire che i criminali informatici possano leggerli in caso di violazione o accesso non autorizzato.

I CISO devono prevenire il rischio di perdita di dati e adeguarsi alla normativa, crittografando completamente il disco rigido dei loro endpoint per dispositivi mobile.

GravityZone Full Disk Encryption protegge i dati di tutto il disco rigido dell'endpoint, utilizzando i sistemi di crittografia forniti da Windows (BitLocker) e Mac (FileVault). Sfrutta la crittografia nativa dei dispositivi, per garantire una completa compatibilità e massimizzare le prestazioni. GZ Full Disk Encryption è integrato nella console e nell'agent di GravityZone e la sua installazione non richiede quindi agent o server di gestione delle chiavi aggiuntivi. L'utilizzo dell'infrastruttura di sicurezza endpoint esistente per la gestione di Full Disk Encryption consente un'implementazione completamente centralizzata, con il minimo sforzo da parte degli amministratori.

RIEMPIRE TUTTI I VUOTI NELLE DIFESE

I sistemi con vulnerabilità non corrette espongono le organizzazioni a possibili incidenti ed epidemie di malware, oltre che a violazioni della sicurezza. La Metà dei CISO intervistati ammette che l'espansione dell'infrastruttura ha causato un aumento della superficie di attacco della propria azienda. Gli esperti di sicurezza raccomandano fortemente ai CISO di mantenere tutti i software aggiornati con le ultime patch. I sistemi di gestione delle patch semplificano ulteriormente questa operazione e aiutano le aziende ad evitare eventi dannosi come le famigerate epidemie WannaCry e GoldenEye.
Il modulo GravityZone Patch Management supporta l'installazione sia automatica che manuale delle patch.

Offre alle organizzazioni una maggiore flessibilità ed efficienza nella gestione delle patch, con la possibilità di creare un inventario delle patch, pianificarne la scansione, limitare l'installazione automatica delle patch alle applicazioni selezionate dagli amministratori, prevedere una pianificazione diversificata per le patch collegate o non collegate alla sicurezza e posticipare i riavvii per le patch che lo richiedono. Nell'attuale scenario, l'installazione di patch per SO e applicazioni è diventata una delle maggiori priorità dei team IT, per garantire sia la sicurezza che la conformità. GravityZone Patch Management permette di verificare l'applicazione di patch in tutta l'azienda, assicurando il pieno rispetto di policy e normative.