Tre problematiche fondamentali incentrate sui dati alle quali devono allinearsi le organizzazioni

Author : Redazione

Date : 8 Aprile 2019

Anche le organizzazioni smart possono essere fuorviate da dati non protetti, dall'evoluzione delle minacce informatiche e dalla conformità al GDPR

I team esecutivi aziendali spesso non sono in contatto con i loro reparti IT e di sicurezza. Mentre il management gestisce questioni aziendali fondamentali, che vanno dalla conformità, allo sviluppo aziendale, all'ufficio legale, al marketing, alle risorse umane e altro ancora, l'IT e la sicurezza tengono aggiornata la rete aziendale con le più recenti tecnologie e la proteggono dalle minacce più recenti. In genere, l'unica volta che questi due gruppi si incontrano è quando qualcosa va storto.

Il divario di conoscenze che ne risulta può dare ai dirigenti aziendali una falsa impressione della preparazione informatica dell'organizzazione. Dato che i dati sono la linfa vitale di qualsiasi azienda, colmare questo divario e adottare una mentalità incentrata sui dati è di vitale importanza.

Sono tre le problematiche fondamentali da affrontare con il management della vostra organizzazione.

La problematica dell'accesso aperto. Le organizzazioni hanno bisogno di sapere quali dati sono sensibili e chi vi accede; devono inoltre monitorare il comportamento degli utenti e l'attività sui file, in modo da sapere quando succede qualcosa di insolito e quando è necessario indagare. Purtroppo, i dati di un'azienda sono spesso del tutto aperti e completamente non monitorati, il che li espone a troppe persone. Per complicare le cose, leimprese hanno perso il controllo dei dati più importanti. I file sono sparsi su server locali, salvati sui PC dei dipendenti, archiviati in cartelle di posta elettronica e ospitati nel cloud.

Immaginate se i dati dei cittadini dell'UE e le informazioni sulle carte di pagamento fossero archiviati in cartelle aperte a tutti i dipendenti dell'organizzazione: anche se allarmante, è pur sempre una possibilità molto reale per molte aziende. Abbiamo scoperto che più del 20% dei

file nella maggior parte delle aziende sono aperti a tutti e molte organizzazioni hanno centinaia di migliaia di cartelle e *milioni* di file esposti in caso di attacco. Quando i dati sono esposti, soprattutto su larga scala, possono essere facilmente rubati da persone interne all'azienda o da aggressori esterni.

Per proteggere le informazioni sensibili è fondamentale rafforzare i controlli globali di accesso sulle condivisioni di file, in modo che solo i gruppi giusti di persone possano accedere alle informazioni di cui hanno bisogno. Molte organizzazioni pensano che mantenere un modello di accesso meno privilegiato sia difficile, ma non deve essere necessariamente così. L'aspetto fondamentale è migliorare il processo di gestione degli accessi alle identità, togliendo il personale IT dalla catena di approvazione per l'accesso ai dati e rimettendo tale decisione ai proprietari dei dati. Una volta fatto questo è possibile implementare un flusso di lavoro per mantenere le autorizzazioni meno privilegiate.

La questione del rilevamento e del blocco delle minacce. Per anni, la sicurezza ha comportato bloccare il perimetro con firewall e antivirus nel tentativo di tenere lontani gli aggressori e il malware. Il numero di attacchi ransomware dimostra che è relativamente semplice per il malware o un avversario superare il firewall e accedere alla rete. Basta che qualcuno faccia clic sull'e-mail sbagliata e all'improvviso può essere lanciato un attacco. C'è di peggio: gli aggressori possono anche lanciare attacchi senza file usando PowerShell su sistemi Windows per eseguire comandi in modo furtivo e cercare di estrarre contenuti preziosi senza sollevare sospetti.

A volte le minacce più grandi provengono dall'interno, poiché i dipendenti interni ostili stanno diventando più abili nel far perdere le loro tracce. Purtroppo, per il team di sicurezza IT che controlla le attività degli hacker, gli attacchi moderni sono molto difficili da individuare, in quanto spesso eludono i tradizionali scanner antivirus e altri sistemi di rilevamento basati sulle firme.

Immaginate se un attacco dovesse avvenire alla fine di una giornata lavorativa subito prima di una lunga vacanza: Potete essere certi che i team giusti sarebbero stati avvisati in tempo per fermare l'attacco? È fondamentale che siano messi in atto controlli migliori per individuare più rapidamente questi attacchi e impedire che provochino danni diffusi. In breve, la difesa tradizionale non è in grado di gestire questo tipo di attacco. Fortunatamente, la tecnologia può individuare in modo efficiente e automatico e inviare un avviso per identificare comportamenti anomali - come gli utenti umani che improvvisamente si comportano come ransomware - che potrebbero indicare una minaccia alla sicurezza.

La questione della conformità al GDPR. Ora che è passato quasi un anno dall'entrata in vigore del GDPR, molte aziende pensano di aver completato tutto il lavoro necessario per conformarsi alla legge. Esse trascurano il fatto che i consumatori stanno iniziando a esercitare il loro "diritto all'oblio" e chiedono che le aziende forniscano tutte le informazioni in loro possesso. Le richieste di accesso da parte degli interessati (DSAR) rappresentano nuove problematiche per le aziende che devono rispettare il GDPR. Non solo devono gestire un flusso di richieste, ma devono anche essere in grado di identificare i contenuti relativi a una persona interessata e farlo entro 30 giorni. Non c'è molto tempo per elaborare le richieste, individuare e raccogliere *tutti i* dati relativi a una persona e rispondere fornendo e/o cancellando i dati.

Privacy e sicurezza vanno di pari passo. Per garantire la privacy, le organizzazioni devono disporre di misure di sicurezza per prevenire gli attacchi e determinare se e quando i dati dei loro consumatori, studenti o pazienti vengono violati. Assicurarsi che i dati non siano esposti, osservare come vengono utilizzati e sapere quando qualcosa va storto renderà il processo molto più semplice. Assicuratevi di monitorare e segnalare le attività sospette sui dati GDPR applicando l'analisi della sicurezza dei dati e i modelli delle minacce all'attività dei file e al comportamento degli utenti.

L'informatica e la sicurezza non sono più problematiche isolate, ma piuttosto questioni commerciali importanti che riguardano ogni reparto di un'azienda. Essere cauti e adottare approcci tradizionali per proteggere le informazioni più preziose non è assolutamente sufficiente: cercate piattaforme integrate che possano porre rimedio agli accessi aperti, facilitare la protezione delle reti dagli attacchi moderni e contribuire a rispettare il GDPR.