Prevenire e rilevare la perdita di dati dovuta a minacce interne

Sei modi per proteggere la fuoriuscita di dati sensibili

Con la possibilità di accedere ai dati sensibili aziendali, come quelli finanziari relativi ai clienti e all'impresa, i dipendenti ricoprono una posizione di fiducia all'interno della propria organizzazione. Questo rende più facile eludere le misure di sicurezza, favorendo la perdita di informazioni confidenziali. Anche se la maggior parte delle perdite di dati sono causate da un errore involontario dell'utente, e non da un intento doloso, l'invio per esempio errato di un'email può avere lo stesso costo e impatto negativo pari a un furto di proprietà intellettuale perpetrato da un dipendente. In entrambi i casi le violazioni interne ai dati sono difficili da identificare e prevenire.

La maggior parte delle organizzazioni si affida a tecniche organizzative per evitare perdite di dati dall'interno, quali politiche di gestione dei dati e training sulla sicurezza. Tuttavia, per dimenticanza o negligenza, gli utenti spesso non seguono le policy aziendali, in particolare se percepiscono queste come un ostacolo ai propri processi di lavoro. Non è possibile prevenire le minacce interne senza prima identificare il livello di sensibilità dei dati, implementare controlli tecnologici sulle policy per prevenire le violazioni e raccogliere informazioni sulle attività degli utenti, per individuare anomalie e rischi legati all'utilizzo dei dati.

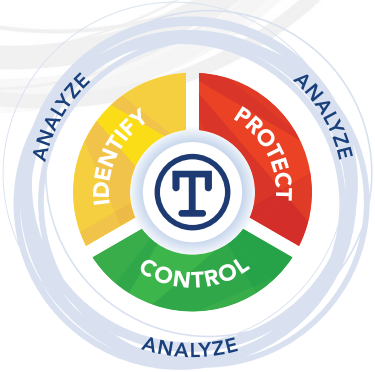
Di seguito sono descritti sei modi con cui TITUS può aiutare le organizzazioni a proteggersi contro la perdita di dati dovuta a minacce interne.

1. Identifica i dati. La sicurezza dei dati inizia dalla loro classificazione. TITUS consente di applicare la classificazione attraverso etichette visive e metadati permanenti, che identificano il grado di riservatezza delle informazioni. Quando l'identità dei dati è conosciuta, diventa semplice per TITUS e per l'ecosistema di sicurezza applicare le policy di controllo, che prevengono l'accesso inappropriato e la distribuzione non autorizzata di file.

2. Cambia il comportamento degli utenti. TITUS può avvisare gli utenti di fermarsi, pensare e prendere in considerazione il valore delle informazioni che stanno trattando. TITUS aiuta ad allineare il comportamento dell'utente finale alle policy aziendali sulla sicurezza e offre un'educazione mirata e interattiva, in modo tale che la sicurezza dei dati diventi una responsabilità di tutti.

3. Aumenta la responsabilità degli utenti. TITUS può stimolare gli utenti a proteggere le informazioni sensibili applicando in modo dinamico informazioni come, ad esempio, il loro nome nelle intestazioni o a piè di pagina, marcature

Struttura minacce interne



Identifica
Cataloga e classifica le informazioni aziendali per determinare il valore dei dati e i rischi associati

Protegge
Una volta identificati i dati, l'ecosistema di sicurezza viene abilitato ad applicare il livello di protezione appropriato

Controlla
Assicura l'accesso da parte delle giuste persone alle corrette informazioni, nel momento e nel luogo appropriato

Analizza
Monitora la classificazione, l'accesso e l'utilizzo dei dati, per tracciare il comportamento degli utenti e il rispetto delle policy

46%

degli incidenti di sicurezza sono causati da personale interno[1]

o altri messaggi, assicurando che essi siano sempre responsabili per le informazioni che condividono e stampano.

4. Previene gli errori e applica le policy. Gli errori degli utenti sono la principale causa di violazione interna dei dati. TITUS utilizza i contenuti dei dati, il contesto e la classificazione per prevenire tali errori. Se un utente cerca di condividere delle informazioni, per esempio via email a un destinatario non autorizzato, TITUS avvisa immediatamente l'utente in modo che questi possa accorgersi e rimediare immediatamente all'errore sul proprio desktop, prima quindi che si verifichi la violazione.

5. Protegge le informazioni. La classificazione TITUS dei metadati può essere utilizzata per potenziare tutto l'ecosistema di sicurezza aziendale dei dati. Invece che affidarsi alla capacità degli utenti di ricordarsi come applicare criteri di crittografia o le funzionalità di Information Rights Management (IRM) ai file sensibili, le classificazioni TITUS possono attivare in modo semplice e automatico queste tecnologie. Allo stesso modo, la classificazione dei metadati consente di fornire ai sistemi di Data Loss Prevention (DLP) la possibilità di riconoscere in maniera certa la riservatezza dei dati, migliorandone così l'accuratezza e l'efficacia.

6. Rileva rischi e minacce. Integrato direttamente con le applicazioni aziendali utilizzate abitualmente dagli utenti, TITUS conferisce agli amministratori la possibilità di monitorare comportamenti anomali o rischiosi altrimenti difficili da rilevare. TITUS fornisce dei report su tutte le attività più importanti eseguite dagli utenti, come il downgrade di un file classificato o l'invio per email di file classificati come "interni" a indirizzi esterni. Combinando i report di TITUS con strumenti di analisi delle minacce, la sicurezza IT può reagire in tempo reale ad attività potenzialmente dannose degli utenti, altrimenti difficili da rilevare.

About TITUS

Le soluzioni TITUS consentono alle organizzazioni di classificare, proteggere e condividere le informazioni in modo sicuro, garantendo inoltre la conformità alle normative vigenti, attraverso l'individuazione e la protezione dei dati non strutturati. Le soluzioni TITUS contribuiscono a prevenire la perdita di dati coinvolgendo gli utenti finali nella classificazione e protezione delle informazioni sensibili contenute nelle email, nei documenti o in altri tipi di file - su desktop, dispositivi mobili e all'interno di ambienti SharePoint. Le soluzioni TITUS sono utilizzate da milioni di utenti in oltre 60 paesi nel mondo. Tra i clienti: Dell, Nokia, Dow Corning, Safran Morpho, United States Air Force, NATO, Pratt and Whitney, Canadian Department of National Defence, Australian Department of Defence e l'U.S. Department of Veterans Affairs.

[1] *(Forrester Research Inc. "Business Technographics Global Security Survey Q2 2014.")*

343 Preston Street, Suite 800, Ottawa, Canada K1S 1N4
Tel: +1 613 820 5111 | info@titus.com