Incidenti di sicurezza nel settore sanitario

Date : 14 settembre 2016

Nel 2015 quasi tre quarti degli incidenti di sicurezza nel settore sanitario hanno riguardato casi di perdita o sottrazione fisica di dati, uso improprio di privilegi da parte di insider ed errori di vari. Se la violazione dei dati avviene generalmente in un minuto o meno, l'individuazione di quest'ultima spesso richiede diversi mesi o più.

L'edizione 2016 del **Data Breach Investigations Report** (DBIR) mostra come la maggior parte degli incidenti di sicurezza possano essere classificati in una delle nove tipologie di violazioni. Solo tre di queste costituiscono il 73% di tutti gli incidenti di sicurezza nel settore sanitario.

Il furto fisico o la perdita dei dati rappresentano la maggior parte degli incidenti in questo settore (ben il 32% del totale). Questo può essere un problema maggiore per il mondo healthcare rispetto a tutti gli altri settori analizzati quest'anno. Scopriamo queste tipologie di minacce in modo più approfondito e come sia possibile migliorare i propri sistemi di difesa.

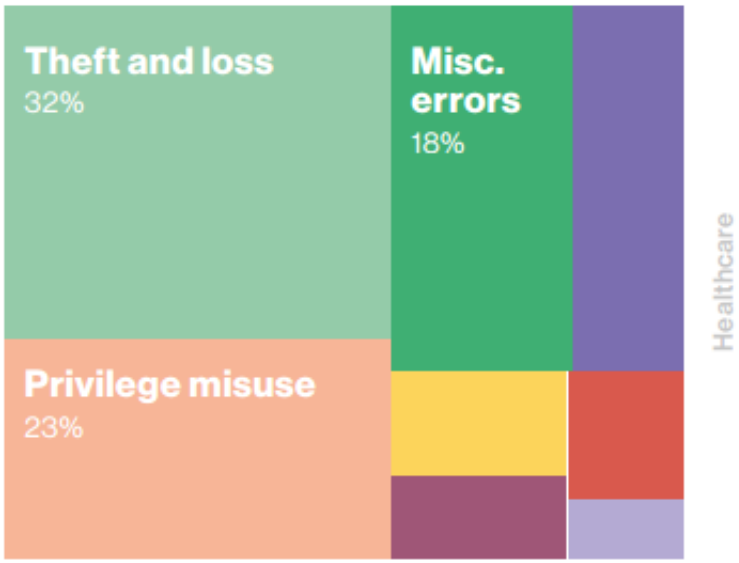

Figure 1: Incidents by pattern

Perdita e sottrazione fisica

Il furto fisico e la perdita degli asset può rappresentare un grave problema del settore sanitario, costituendo quasi un terzo di tutti gli incidenti di sicurezza.

Il furto fisico di dati è un problema costante ogni anno, in tutti i settori. Ma la quota di incidenti che riguarda il settore sanitario è più grande rispetto a qualunque altro settore presente nel dataset.

Tra gli asset rubati o persi rientrano laptop, computer fissi, dispositivi mobili, chiavette USB e documenti cartacei. Considerando tutti i settori, il furto di dati si verifica più comunemente all'interno dell'ambiente di lavoro della vittima (39%) o del veicolo personale del dipendente (34%). Nonostante questo, il rischio più grande in questa categoria deriva dalla perdita di asset da parte dei dipendenti – caso 100 volte più probabile del furto.

Qual è la soluzione?

- **Crittografare i dati:** se i dispositivi rubati sono crittografati, è molto più difficile, per gli hacker, accedere ai dati;
- **Istruire il personale**: sensibilizzare alla sicurezza la propria organizzazione è di fondamentale importanza, introducendo nella formazione continua dei dipendenti un'educazione alla sicurezza fisica dei beni.
- **Ridurre l'utilizzo di documenti stampati:** limitare l'uso di stampanti, stabilire regole per la classificazione dei dati e procedere con la stesura di una policy riguardante le procedure di stampa e il trasporto dei dati sensibili.

Uso improprio di privilegi da parte di insider

Questa categoria costituisce il 23% degli incidenti di sicurezza nel settore sanitario presenti nel DBIR 2016 (16% per tutti gli altri settori). Per il settore sanitario, è la causa principale di violazioni accertate che hanno comportato il furto dei dati.

L'uso improprio di privilegi da parte di insider avviene spesso per opera di dipendenti insoddisfatti o ex-dipendenti che usano le proprie credenziali di accesso per acquisire informazioni confidenziali, a scopo di lucro personale. Ma non mancano casi di collusione tra insider e terze parti, oltre all'uso improprio di privilegi da parte di business partner, come ad esempio vendor.

Qual è la soluzione?

- **Monitorare il comportamento degli utenti:** mettere in atto processi di monitoraggio dell'uso quotidiano del sistema – in particolare di coloro che potrebbero trarre un vantaggio dall'accesso a dati come le informazioni sanitarie protette, dati personali o i dettagli dei conti finanziari.

- **Tracciare l’utilizzo di chiavette USB:** non scoprire che un dipendente ha sottratto dei dati solo dopo che se n’è andato.

Conoscere i propri dati: per proteggere le informazioni, è necessario sapere quali dati si posseggono, dove sono archiviati e chi vi può accedere. Se possibile, potrebbe essere utile limitare l’accesso ai dati a coloro che ne hanno realmente bisogno e assicurarsi di aggiornare gli account degli utenti, in caso di dimissioni degli impiegati o cambiamento della posizione lavorativa.

Errori vari

Gli errori vari, infine, costituiscono il 18% del totale tra le diverse categorie di incidente.

Numerosi incidenti sono stati causati dall’invio di e-mail o documenti da parte dei dipendenti al destinatario sbagliato. Non mancano casi in cui un’informazione è stata divulgata per errore (public disclosure ad esempio).

L'eventuale perdita di dati dei pazienti o di altre informazioni sensibili potrebbe avere un impatto negativo nella relazione tra le aziende sanitarie e i propri pazienti, i partner e il pubblico.

L’errore umano non può mai essere completamente eliminato, ma nella maggior parte dei casi la probabilità che un errore si verifichi può essere notevolmente ridotta, utilizzando i giusti processi e controlli.

Qual è la soluzione?

- **Imparare dagli errori**: stilare un elenco degli errori comuni e usarlo come materiale di training per incrementare la sensibilizzazione alla sicurezza.
- **Mappare gli errori**: definire una mappa con gli errori più comuni. Grazie a queste informazioni, stabilire efficaci controlli per minimizzare la frequenza con cui questi errori si verificano e attenuare i danni quando accadono.
- **Implementare procedure di smaltimento accurate**: nel momento in cui gli asset devono essere venduti o eliminati, è importante assicurarsi che ci sia una procedura documentata di rimozione dei dati sensibili.

Il settore sanitario è lento nel rilevare gli incidenti e le violazioni di sicurezza, là dove il dato è

divulgato. Anche se il 56% degli incidenti è stato scoperto in qualche giorno, nel 39% dei casi ci sono voluti mesi per individuare la violazione. I sistemi sanitari sono stati compromessi nel giro di qualche minuto nel 63% dei casi. Questo permette agli hacker di avere molto tempo per la ricerca di dati sensibili – potenzialmente redditizi – di un paziente. La cosa peggiore è che nel 56% dei casi le violazioni accertate con sottrazione di dati sono state scoperte dopo mesi.

Per ulteriori dettagli: http://www.verizonenterprise.com/resources/reports/rp_2016-DBIR-Healthcare-Data-Security_en_xg.pdf