Gestione ed analisi dell'incidente

Una soluzione garantita.

Le violazioni di dati assumono molteplici forme. Hackers ed insiders sono sicuramente una delle principali fonti di incidenti cyber, ma sapevate che la semplice negligenza è responsabile di un sorprendentemente numero di violazioni?

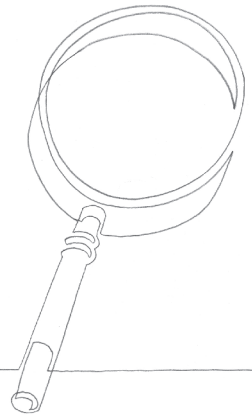
Le violazioni di dati possono costituire una minaccia reale per le persone i cui dati personali sono stati persi o rubati. Alcune violazioni sospette durante le indagini risultano essere falsi allarmi, ma i costi delle analisi di esperti informatici possono essere considerevoli. Anche le caratteristiche settoriali sono critiche – una perdita di cartelle cliniche di un ospedale pone rischi diversi rispetto alla perdita di dati di carte di credito di un commerciante.

In ogni caso BBR Services collabora con voi per stabilire la migliore gestione della crisi, studiata su misura per le vostre esigenze individuali.

Case studies

- Quando il direttore risorse umane di un istituto di credito ha notato utenti falsi nel proprio sistema di payroll BBR Services è intervenuta e ha guidato la banca nell'intero processo di risposta alla violazione, dall'organizzazione di consulenti legali esperti in privacy, attraverso complesse e dettagliate indagini informatiche, al coordinamento del processo di notifica alle migliaia di persone presenti nel database clienti della banca.
- Un rivenditore online di dispositivi elettronici non aveva idea di cosa fare quando ha ricevuto una lettera dalla sua banca che lo avvisava di spese fraudolente pari a $500,000 fatte con 455 carte sul proprio sito web e gli consigliava di avviare immediatamente indagini informatiche e di assumere entro 48 ore un perito approvato dalla Payment Council Industry (PCI).

Il rivenditore ha contattato BBR Services ed il giorno stesso Beazley ha formulato un piano di indagini e di risposta, ed ha organizzato l'intervento di un perito approvato da PCI in 24 ore. Il perito ha accertato che non si fosse verificata alcuna violazione da parte del rivenditore e, su questa base, la banca e la società fornitrice delle carte di credito hanno entrambe chiuso le loro indagini.



Case studies

- Uno studio medico ha scoperto che tutto il suo sistema informatico, inclusa la piattaforma elettronica con le cartelle cliniche, improvvisamente non rispondeva. Diversi tentativi di accedere al sistema erano falliti. Successivamente lo studio ha ricevuto un'e-mail da uno sconosciuto che spiegava che il mittente si era inserito abusivamente nella loro rete, aveva cifrato tutti i dati presenti nel sistema e li avrebbe decifrati solo in cambio del pagamento di un riscatto. I medici erano pronti ad effettuare il pagamento, ma hanno prima contattato Beazley. BBR Services ha formulato immediatamente una strategia di risposta, assumendo un consulente legale esperto in risposta alle violazioni e coordinandosi con le autorità. In tempi rapidi è apparso evidente che l'hacker intendesse semplicemente incassare il denaro del riscatto, rinnegare l'accordo e disseminare ulteriori malware nel sistema. Beazley ha aiutato a coordinare i servizi di cui l'assicurato necessitava per procedere ed inviare notifiche alle migliaia di pazienti, alle autorità di regolamentazione e ai media in merito alla violazione.
- Quando un'e-mail per studenti inviata da una grande università ha incluso involontariamente i codici fiscali di 22.000 studenti nei destinatari, l'università ha chiesto aiuto a Beazley. Oltre a coordinare l'intera risposta alla violazione, inclusi gli aspetti legali, le notifiche e i fornitori di call centre, BBR Services ha fatto in modo, grazie al rapporto privilegiato con Experian, che gli studenti ricevessero una soluzione di monitoraggio del credito.
- Un'organizzazione dedita al furto di identità che operava dalla Malaysia e dalla Russia ha riunito profili di professionisti sanitari di grandi ospedali. L'organizzazione ha utilizzato i dati di dominio pubblico presenti su LinkedIn, nonché i riferimenti di Google relativi alla presenza dei medici a conferenze, per costruire questi profili. L'organizzazione poi ha dato avvio ad una campagna di spear-phishing con e-mail create a regola d' arte che prendevano di mira i medici chiedendo loro di reimpostare alcuni dati relativi alle risorse umane. Numerosi dottori hanno cliccato un collegamento ipertestuale incorporato nell'e-mail. Il link ha registrato i dati di accesso al portale risorse umane, che gli hacker hanno utilizzato per dirottare le buste paga su un conto offshore; tali dati hanno consentito agli hacker di disseminare sofisticati malware nei rispettivi sistemi degli ospedali. Molti ospedali hanno segnalato l'evento a Beazley. BBR Services è stata in grado di coordinare e usare abilmente le risorse per i clienti di questi ospedali in modo tale da ridurre notevolmente i costi di risposta delle conseguenti indagini legali e delle autorità.
- Una società di gestione di hotel aveva server ubicati in diversi luoghi. Uno di questi server è stato infettato. La società ha chiamato Beazley un venerdì sera ed i legali hanno messo in atto un piano nella giornata successiva Hanno agito rapidamente e hanno monitorato la situazione. Si è accertato che non vi fosse stata alcuna violazione di dati.

Gestire una violazione di dati può essere complicato e costoso. Lavorando insieme al team Beazley, la vostra organizzazione sarà guidata e verrà dotata delle risorse necessarie per mettere in atto un piano solido e strategico di risposta alla violazione.

beazley