PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 25 - numero 5437 di Venerdì 21 luglio 2023

Uno studio sugli incidenti informatici

Quando si verifica un incidente informatico, è utile ricorrere ad esperti assicurativi e avvocati? La risposta di quattro università è del tutto negativa!

Non nascondo ai lettori che sono rimasto oltremodo sorpreso da questo studio, convalidato da 69 interviste ad esperti del settore, che dimostra come il coinvolgimento di esperti assicurativi ed avvocati, in fase di gestione di un incidente informatico, può creare più problemi di quelli che potrebbero essere risolti.

La procedura di risposta ad un incidente informatico consente alle vittime di individuare, mettere sotto controllo e ripristinare la funzionalità di apparati, coinvolti in un incidente di sicurezza. Un altro aspetto assai positivo riguarda il fatto che la conoscenza di questi incidenti può aiutare altre aziende a prevenire attacchi similari.

L'esperienza mostra che, per raggiungere questi obiettivi, gli esperti informatici sono sempre più influenzati degli aspetti assicurativi e dagli avvocati.

Il documento, compilato da quattro università, si basa sul risultato di 69 interviste ad esperti del settore, sull'analisi dei dati afferenti a relazioni commerciali e studi on-line di validazione degli eventi.

Lo studio ha mostrato come molto spesso le compagnie di assicurazione per le polizze informatiche mandano sul campo degli esperti informatici, che intervengono con l'assistenza di avvocati, che influenzano le indagini tecniche. La seconda parte di questo studio ha mostrato che l'intervento degli avvocati, nel mettere a punto le politiche di risposta al possibile incidente informatico, introduce delle fasi legali, contrattuali e di comunicazione, che rallentano in modo significativo la risposta all'incidente. Inoltre, spesso gli avvocati consigliano agli esperti, che intervengono in fase di risposta all'incidente, di non scrivere quanto fatto per mettere sotto controllo l'evento e di non produrre rapporti formali. Essi, inoltre, impongono restrizioni significative all'accesso a qualsiasi documento sia stato elaborato.

La situazione è oltremodo sorprendente e preoccupante, soprattutto se viene messa a confronto con la guida per la gestione degli incidenti informatici, pubblicata dal National istitute of standard technology con il codice NIST 800-61, nella quale viene sottolineata l'estrema importanza dell'acquisizione di tutti gli elementi afferenti all' incidente informatico e alla funzione dei soggetti terzi, per evitare che lo stesso problema possa essere presente in altri scenari.

Lo studio di queste quattro università, di qua e di là dell'Atlantico, dimostra le ragioni per cui le chiare indicazioni delle linee guida NIST spesso non vengano seguite. Le interviste hanno confermato come, nella grande maggioranza dei casi, gli avvocati sono assolutamente sfavorevoli alla elaborazione di documentazioni, che descrivono l'evento, e danno indicazioni su testi e contenuti, che potrebbero ridurre la responsabilità dell'azienda coinvolta nell'incidente informatico, mascherando così le cause effettive dell'incidente e rendendo difficile la indicazione di specifiche misure di prevenzione e contenimento.

D'altro canto, le compagnie di assicurazioni, che offrono polizze contro incidenti informatici, tendono ad assumere un atteggiamento protettivo, per cercare di limitare i danni, che l'azienda potrebbe essere costretta a pagare, o per ridurre l'importo delle sanzioni, che, anche nel regolamento generale europeo, sono direttamente legate non solo alla dimensione dell'azienda, ma anche al suo profilo, alle sue dimensioni, nonché ovviamente alla gravità dell'incidente.

Un altro aspetto non trascurabile riguarda poi il fatto che non si desidera che il rapporto interno venga a conoscenza di terzi, per evitare che possa aumentare il numero dei soggetti che possono chiedere un rimborso, in caso di incidente informatico. In casi estremi, non è sufficiente tenere riservato il rapporto interno, perché, soprattutto negli Stati Uniti, gli avvocati interessati potrebbero usare una procedura, chiamata "discovery", che obbliga i soggetti coinvolti a rendere pubblici documenti, come ad esempio rapporti criminologici od una qualsiasi comunicazione scritta tra i soggetti coinvolti. Le uniche comunicazioni che non possono essere diffuse sono protette dall'ormai famoso privilegio avvocato-cliente, che tutela in modo pressoché assoluto lo scambio di comunicazioni tra un avvocato ed il suo cliente.

Un altro problema, messo in evidenza dallo studio, riguarda il fatto che le compagnie di assicurazione delegano gli approfondimenti specifici, in caso di incidenti informatici, a piccole aziende specializzate, utilizzando talvolta il criterio della competenza specifica, ma assai più spesso il criterio del costo più contenuto. Altro elemento che lascia assai perplessi riguarda il fatto che molto spesso queste piccole aziende specializzate vendono anche prodotti di prevenzione e mitigazione di incidenti informatici, che evidentemente trovano un ottimo mercato presso le vittime di questi stessi incidenti.

Inoltre, il rapporto triangolare tra la vittima dell'incidente informatico, uno studio legale e un'azienda specializzata in incidenti informatici fa sì che i ruoli degli ultimi due profili talvolta si sovrappongano, come ad esempio avviene quando l'azienda specializzata in sicurezza informatica viene pagata dallo studio legale, che a sua volta si rivale nei confronti della compagnia di assicurazione.

A proposito della proibizione di diffusione di rapporti interni, vale la pena di citare testualmente la dichiarazione di un avvocato:

"Se sappiamo che con ogni probabilità vi sarà un contenzioso, noi diamo istruzione di non produrre alcun rapporto. Infatti, la controparte potrebbe scatenarsi per cercare di avere copia del rapporto e quindi è molto più semplice rispondere: "siamo spiacenti, ma non vi è alcun rapporto".

D'altro canto, è comprensibile che un avvocato non desideri che un rapporto, nel quale sia presente una frase del tipo: "il server era vulnerabile", possa finire in mano ai legali, che difendono i soggetti danneggiati dall'incidente informatico.

Ecco una citazione letterale tratta dall'intervista ad un avvocato:

"Io sono molto preoccupato quando gli esperti di criminologia producono un documento scritto. In questo documento infatti

potrebbe essere presente una frase del tipo "il vostro esperto esterno ha affermato che voi avreste dovuto fare questo e quello e, non avendolo fatto, vi siete comportati in modo negligente". È evidente che non desidero leggere frasi del genere!".

Non nascondo che lo scenario illustrato ha destato in chi scrive vive preoccupazioni, soprattutto perché la prima regola fondamentale da attuare, dopo un incidente informatico, è la ricostruzione della causa, in maniera da prevenire che tale incidente possa ripetersi. Se la ricostruzione dell'evento è mutilata, come appare da quanto sopra scritto, viene meno un elemento fondamentale di garanzia di miglioramento dei livelli futuri di sicurezza.

Adalberto Biasiotti

www.puntosicuro.it