

WHITE PAPER EASYAUDIT

Segnalare una violazione: tempi più stretti nell'Ue

Ogni giorno le compagnie di servizi informatici segnalano alle autorità competenti la violazione di dati sensibili. Dalla violazione all'effettiva segnalazione però può trascorrere parecchio tempo, rallentando quindi la reazione delle persone coinvolte nell'attacco.

Da tempo il tema era oggetto di dibattito: in Europa infatti non esisteva alcun limite temporale entro il quale i provider erano tassativamente tenuti a segnalare l'attacco, suscitando le lamentele di numerosi clienti.

Non è semplice però stabilire quale sia il termine corretto per far presente alle autorità giudiziarie un'avvenuta violazione: negli Stati Uniti, dove si sono posti il problema in anticipo rispetto a noi, ogni stato fa storia a sé.

Il risultato è una notevole varietà di norme: in certi stati per esempio è sufficiente notificare "prima o poi" l'avvenuto attacco, in altri vi è invece una scadenza intorno ai 45 giorni.

Nei ventotto stati dell'Unione si è quindi deciso di affrontare con forza il problema, imponendo una deadline molto stretta per le compagnie di servizi

informatici: non più di un giorno tra la violazione e la segnalazione all'autorità.

La risposta dei provider a chi ne critica la lentezza nelle notifiche non si è però fatta attendere: operare in tempi troppo stretti è impossibile, dicono, e a farne le spese sarebbe proprio il consumatore. La ragione è la difficoltà nel riconoscere rapidamente un attacco informatico, individuando chi ne sia stato effettivamente vittima.

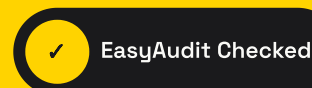
Imporre un limite così stretto, soltanto ventiquattro ore, rischia di rendere impossibile un'autentica comprensione del tipo di minaccia, generando inevitabilmente una serie di falsi allarmi. Sarebbe poi impossibile fornire delle segnalazioni che siano precise e complete.

Todd Hinnen, un partner di Perkins Coie intervistato da SCMagazine, si dice favorevole a un limite temporale massimo per le notifiche, ma a patto che questo non impedisca un lavoro di investigazione congruo. Il tempo giusto della notifica può variare, sostiene, "ma non dovrebbe avvenire comunque oltre le 72 ore".

Vuoi sapere se la tua azienda è davvero protetta?

EasyAudit verifica applicazioni, infrastrutture e piattaforme E-Commerce con un audit chiaro, concreto e pensato per trasformare i rischi tecnici in decisioni semplici.

Richiedi un audit su easyaudit.it



Il segnale visibile di un impegno serio per la sicurezza.