PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 27 - numero 5975 di Lunedì 01 dicembre 2025

Il titolare del trattamento ha l'obbligo di prevenire attacchi informatici

Occorre approfondire fino a che punto il titolare del trattamento di dati personali può e deve adottare misure di protezione dei dati personali. In mancanza, una sanzione di 14 milioni di sterline rappresenta certamente una salata punizione.

Il Garante britannico per la protezione dati personali, ICO - Information Commissioner Office, ha applicato una sanzione di 14 milioni di sterline ad un fornitore di servizi informatici per fondi pensionistici, che non ha adottato appropriate misure di protezione dei dati dei clienti, portando al furto di milioni di informazioni personali dei clienti stessi. In allegato i lettori troveranno l'intero provvedimento, ma una sintesi rappresenta un prezioso aiuto per individuare il rapporto tra rischi e protezioni, che un titolare deve ragionevolmente adottare.

L'attacco informatico è avvenuto nel marzo 2023. Sono state sottratte le informazioni personali di 6, 6 milioni di persone, comprendenti registi pensionistici ed informazioni sensibili, come ad esempio dati finanziari, profili giudiziari e via dicendo.

Il numero straordinario di soggetti coinvolti nasce dal fatto che questa azienda svolge attività informatica al servizio di più di 600 organizzazioni pensionistiche.

L'indagine svolta dagli investigatori dell'autorità garante ha dimostrato che questo titolare del trattamento non solo non aveva adottato adeguate misure di prevenzione dell'attacco, ma ha anche reagito in maniera poco efficace alle immediate conseguenze dell'attacco.

Merita di essere citato il fatto che inizialmente la sanzione era stata ipotizzata attorno ai 45 milioni di sterline, ma successivamente è stata ridotta, perché l'azienda si è attivata incisivamente, anche se tardivamente, per attuare adeguati schemi, in grado di prevenire una possibile ripetizione dell'attacco.

Inoltre l'azienda ha offerto un servizio di assistenza a tutti gli interessati coinvolti e questo fatto è stato apprezzato dall'autorità garante.

Ecco i fatti.

Pubblicità

L'attacco è cominciato quando un file criminoso è stato accidentalmente scaricato da un dipendente sul proprio computer.

Il sistema di allarme del sistema informatico dopo solo 10 minuti ha lanciato un allarme, che però non venne correttamente recepito dai responsabili, in modo che il file criminoso ha avuto a disposizione ben 58 ore per svolgere la sua attività di attacco informatico. L'attaccante ha potuto pertanto operare all'interno del sistema, assumendo la posizione di amministratore di sistema e accedendo a varie aree dell'intero sistema informativo. Infine, il 31 marzo 2023 l'attaccante ha resettato tutte le parole chiave di accesso al sistema, bloccando in pratica l'intera operatività dei dipendenti.

Le indagini degli investigatori hanno permesso di appurare che vi è stato un inaccettabile ritardo tra il momento in cui il sistema ha lanciato un allarme ed i responsabili si sono attivati, per isolare il terminale attaccato.

Il sistema, che trattava milioni di schede personale di interessati, era stato assoggettato a un tentativo di penetrazione soltanto tempo addietro e, al termine della penetrazione, non era stata effettuata una analisi approfondita dei punti di debolezza messi in evidenza.

Negli ultimi tempi il personale addetto alla gestione delle misure di sicurezza si era grandemente ridotto e questo fatto ha indubbiamente compromesso le capacità di reazione dell'intera azienda.

In particolare, gli schemi operativi aziendali prevedevano che la reazione ad un allarme di penetrazione venisse attuata al massimo entro un'ora dal lancio dell'allarme, mentre, nella fattispecie, sono trascorse ben 58 ore, durante le quali, come accennato in precedenza, gli attaccanti si sono completamente impadroniti della gestione del sistema informativo.

Durante la fase di negoziazione, che ha portato ad una significativa riduzione della pur elevatissima sanzione, l'autorità Garante apprezzato il fatto che a tutti i clienti potenzialmente coinvolti sia stato offerto un sistema di monitoraggio costante del credito, in modo da mettere immediatamente in evidenza possibili usi illeciti dei dati personali sottratti.

È un aspetto che tutti i titolari del trattamento dovrebbero avere ben presente, in relazione al fatto che guai possono capitare a tutti, ma le modalità con cui si pone rimedio a questi guai possono avere un'influenza oltremodo positiva sulla valutazione complessiva dell'evento e sulla determinazione della sanzione applicabile.

PENALTY NOTICE - CAPITA PLC - CAPITA PENSION SOLUTIONS LIMITED (pdf)

Adalberto Biasiotti

 Licenza Creative Commons

www.puntosicuro.it