PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 25 - numero 5307 di Venerdì 13 gennaio 2023

Una preoccupante supposizione trova una drammatica conferma

Un esperimento che conferma le perplessità di esperti di sicurezza e protezione dei dati, in merito alle garanzie offerte dalle aziende che effettuano interventi di manutenzione su smartphone e lap top.

In allegato a questa nota i lettori troveranno un documento, pubblicato da studiosi dell'università di Guelph, in Canada, che conferma quanto già da tempo si temeva: state attenti ai vostri dati, quando affidate uno smartphone od un laptop ad un tecnico di manutenzione e riparazione!

Ormai sono sempre più numerosi i negozi che offrono servizi di riparazione e manutenzione per smartphone ed altri apparati elettronici di vario tipo. In Italia, non so perché, la grande maggioranza di queste aziende è gestita da immigrati, provenienti perlopiù dall'India, dal Pakistan e dal Bangladesh.

I compiti che un cliente affida a queste aziende sono per solito la installazione di alcuni applicativi, l'aggiornamento di applicativi esistenti e riparazioni, in caso di necessità.

Quando il cliente consegna questi oggetti alle aziende di manutenzione, spesso riceve anche la richiesta di consegnare le credenziali di accesso, per consentire ai tecnici di intervenire sul cuore del sistema informatico. Appare evidente che la consegna di queste credenziali di accesso può comportare rischi afferenti al fatto che dati personali, presenti sull'apparato, possano venire a conoscenza dei tecnici.

Gli studiosi dell'università canadese hanno sviluppato uno studio, articolato in quattro parti, per misurare il livello di protezione dei dati personali, nell'ambito dell'industria della riparazione di apparati elettronici.

In una prima fase, sono state selezionate 18 aziende ed è stato appurato che nessuna di essa aveva una politica di privacy in essere, né adottava alcun tipo di controllo per salvaguardare i dati personali, presenti sull'apparato da riparare, da accesso indebito da parte dei tecnici.

Nella seconda fase, gli studiosi hanno consegnato degli apparati, debitamente preparati, per interventi di riparazione e manutenzione. Gli applicativi inseriti in questi apparati hanno permesso di raccogliere dati sulla violazione dei dati personali presenti, la copia dei dati e i tentativi di rimozione delle operazioni indebite di lettura o manipolazione dei dati.

Nella terza fase, gli studiosi hanno intervistato un centinaio di clienti, che avevano affidato i propri apparati a queste aziende.

Infine, nella quarta fase, sono state condotte interviste approfondite su un gruppo selezionato di clienti, per verificare fino a che punto essi si erano resi conto dei rischi potenzialmente connessi all'affidamento in manutenzione dei propri apparati.

Lo studio è assolutamente affascinante, anche perché mette in evidenza le cautele prese dagli studiosi, nello svolgere questa indagine. Ad esempio, sono stati sempre usati nomi fittizi, per evitare che i tecnici delle aziende interessate potessero effettuare ricerche su Internet e accorgersi che il nome del cliente corrispondeva ad un tecnico universitario, esperto di sicurezza informatica.

Inoltre, per rispettare specifiche disposizioni in vigore in Canada, tutti i dati presentati sono stati resi anonimi.

Per mettere alla prova la buona fede dei tecnici, alcuni apparati sono stati portati al punto di riparazione solo per la sostituzione della batteria. Anche in questo caso, i tecnici hanno chiesto i codici di accesso e, alle perplessità avanzate dal cliente, hanno risposto che se non ricevevano questi codici di accesso, essi non erano in grado di garantire la qualità del lavoro!

Ma non è finita, perché i tecnici di alcune aziende, dopo aver acquisito le credenziali di accesso, le hanno stampate su un'etichetta auto adesiva, insieme al nome e cognome del cliente, ed hanno applicato l'etichetta sull'apparato.

Alla specifica richiesta del cliente, che voleva essere rassicurato circa il fatto che il tecnico non avrebbe avuto accesso ai suoi dati personali, tutti hanno dato una risposta del tipo: "Dottore, si fidi di me!".

Altrettanto interessante è la descrizione della manipolazione effettuata sugli apparati, prima della consegna per l'intervento di manutenzione. Tutti i laptop avevano installato il sistema operativo Microsoft Windows 10 e i tecnici hanno disabilitato soltanto il driver audio. Si tratta di una riparazione semplicissima, che non richiede alcun accesso ai dati personali presenti nel sistema.

All'interno dell'apparato, i tecnici inserirono tutto una serie di dati personali, con fotografie, contatti di vario tipo e un portafoglio con moneta cripto. Metà degli apparati presentati risultavano appartenere a donne e metà a uomini.

Quando gli apparati sono stati restituiti, gli studiosi dell'università hanno analizzato gli interventi effettuati sugli apparati ed hanno avuto conferma del fatto che molti dati personali erano stati analizzati ed alcuni addirittura copiati. In qualche caso, sono state anche rintracciate prove del fatto che il tecnico aveva cercato di mascherare gli interventi effettuati per estrarre dati

personali.

In conclusione, gli studiosi raccomandano caldamente che tutte le aziende, che effettuano interventi di riparazione e manutenzione su apparati informatici portatili, si dotino di una politica di protezione dei dati personali, debitamente pubblicizzata a tutti i clienti.

Gli studiosi, parimenti, suggeriscono che le autorità garanti per la protezione dei dati personali effettuino periodici controlli in questa particolare area di trattamento dei dati, per verificare il comportamento di queste aziende e intervenire, se del caso, con specifiche prescrizioni e salate sanzioni.

Nel frattempo, state attenti, attenti attenti!

Vedi allegato (pdf)

Adalberto Biasiotti

---

www.puntosicuro.it