Privacy, il 47% dei siti dei comuni italiani è a rischio hacker

A un anno dal Gdpr, numerosi i siti istituzionali ancora senza informativa privacy aggiornata, ma uno studio di Federprivacy evidenzia fenomeno più grave ed esteso: il 47% dei siti web dei comuni italiani utilizza protocolli non sicuri, e il 36% non rende noti i recapiti per contattare il DPO, figura obbligatoria per tutte le pubbliche amministrazioni. Presentazione del rapporto completo la settimana prossima al workshop organizzato da PrivacyLab. Bernardi:"Utilizzo di tecnologie ormai obsolete espone siti dei comuni a potenziali rischi di data breach". Speciale dedicato a cybercrime e violazioni dati sul magazine "Privacy News"

Firenze, 10 aprile 2019 - Ha destato un certo scalpore nei giorni scorsi il **monitoraggio** svolto da Wired che ha individuato una serie di siti web pubblici non ancora adeguati al Gdpr ad un anno dalla sua entrata in vigore, specialmente perché tra questi vi sono portali istituzionali di ministeri, forze dell'ordine, Regioni, e anche di partiti politici. Secondo l'indagine della nota testata online, molti di questi siti non hanno un'informativa privacy aggiornata al nuovo Regolamento Europeo, ma fanno riferimento ancora alle vecchie normative.

Benché si tratti di un cattivo esempio da parte delle principali istituzioni, in realtà si tratta solo della punta dell'iceberg di un fenomeno ben più grave ed esteso che riguarda le pubbliche amministrazioni.

Infatti, uno studio condotto dall'Osservatorio di Federprivacy su ben 3.000 siti dei comuni italiani, tra le varie non conformità ed altre carenze riscontrate, ha rivelato che 1.435 di essi (47%) continuano ad utilizzare connessioni non sicure basate sul vecchio protocollo "http", e per questo sono etichettati come "non sicuri" dai principali browser. Inoltre, 1.079 siti di comuni (36%) non rendono disponibili i dati di contatto del Responsabile della Protezione dei dati (c.d. data protection officer), figura obbligatoria per tutte le pubbliche amministrazioni.

"I risultati emersi dalla ricerca sono alquanto preoccupanti, infatti i siti web con protocolli di connessione non sicuri spianano la strada ad hacker e malintenzionati che mirano ad intercettare e carpire dati personali inviati o ricevuti tramite i form di contatto dei siti dei comuni, e l'utilizzo di queste tecnologie ormai obsolete li espone a potenziali rischi di data breach - afferma Nicola Bernardi, presidente di Federprivacy - Inoltre, la mancata pubblicazione dei dati di contatto del data protection officer impedisce di fatto ai cittadini di esercitare i diritti che sono loro riconosciuti dal Gdpr, a maggior ragione del fatto che vista l'assenza di tali recapiti ci siamo presi la briga di telefonare direttamente a cinquecento centralini dei comuni interessati, ma di questi solo quattro hanno saputo indicarci come rintracciare il loro responsabile per la privacy".

Il rapporto completo della ricerca di Federprivacy sarà presentato ed illustrato mercoledì 17 aprile 2019 a Reggio Emilia durante il **workshop gratuito** "Come gestire i Data Breach", organizzato da PrivacyLab proprio per spiegare agli addetti ai lavori come prevenire e gestire i casi di "data breach", vale a dire per esempio quando si verificano violazioni che comportano la perdita, la distruzione, la diffusione o la comunicazione non autorizzata di dati personali.

Nel frattempo, Federprivacy ha dedicato proprio ai rischi di data breach e ai pericoli del cybercrime un numero speciale del periodico "Privacy News", (vedasi la **versione sfogliabile online**), il magazine che l'associazione invia gratuitamente ai propri associati.

Ufficio Stampa Federprivacy
Email: press@federprivacy.it
Web: www.federprivacy.org
Twitter: @Federprivacy
Mobile: +39 340 2893068