GARANTEPRIVACYITALIA.it

Circolare del 05 Giugno 2020

INDICE

APP 'IMMUNI: VIA LIBERA DEL GARANTE PRIVACY

Il Garante "privacy" **ha autorizzato il Ministero della salute** ad avviare il trattamento relativo al Sistema di allerta COVID-19 (App "Immuni"). Sulla base della Valutazione d'Impatto ("DPIA") trasmessa dal Ministero, **il trattamento** effettuato nell'ambito del Sistema **può essere considerato proporzionato**, **essendo state previste misure** volte a garantire **il rispetto dei diritti e le libertà degli interessati**, che attenuano i rischi.

Tenuto conto della complessità del sistema e del numero dei soggetti coinvolti, il Garante ha ritenuto di dare una serie di **misure volte a rafforzare la sicurezza dei dati** delle persone che scaricheranno la APP.

In particolare, l'Autorità ha chiesto che **gli utenti siano adeguatamente informati** in ordine al funzionamento dell'algoritmo di calcolo utilizzato. Dovranno essere portati a conoscenza del fatto che il sistema potrebbe generare notifiche di esposizione che non sempre riflettono un'effettiva condizione di rischio. Gli utenti dovranno avere la possibilità di disattivare temporaneamente l'app attraverso una funzione facilmente accessibile nella schermata principale.

I dati raccolti attraverso il sistema di allerta **non potranno essere trattati per finalità non previste** dalla norma che istituisce l'app. Dovrà essere garantita la trasparenza del trattamento a fini statistico-epidemiologici dei dati raccolti e individuate modalità adeguate a proteggerli, evitando ogni forma di ri-associazione a soggetti identificabili e adottando idonee misure di sicurezza e tecniche di anonimizzazione. Dovranno essere introdotte misure volte ad assicurare il tracciamento delle operazioni compiute dagli amministratori di sistema sui sistemi operativi, sulla rete e sulle basi dati. La conservazione degli indirizzi IP degli *Smartphone* dovrà essere commisurata ai tempi strettamente necessari per il rilevamento di anomalie e di attacchi. Dovranno essere adottate misure tecniche e organizzative per mitigare i rischi derivanti da falsi positivi.

Particolare attenzione dovrà essere dedicata all'informativa e al messaggio di allerta, tenendo altresì conto del fatto che è previsto l'uso del Sistema anche da parte di minori ultra quattordicenni. Il Garante ha sottolineato infine che il trattamento di dati raccolti, da parte di soggetti non autorizzati, può determinare un **trattamento** di dati personali **illecito**, eventualmente **anche sotto il profilo penale**.

DIPENDENTI DI UN COMUNE RICEVONO EMAIL CON OGGETTO 'INFORMAZIONI SUL CORONAVIRUS', MA È UN RANSOMWARE

Un'altra P.A. colpita da un attacco informatico: stavolta è stato il gruppo di hacker *NetWalker* ha sferrare un attacco ransomware contro il Comune di Weiz, una cittadina dello Stato Federale austriaco della Stiri. Il *Malware* ha compromesso il sistema di servizi pubblici ed ha esposto online dati privati relativi a ispezioni e progetti edilizi.

Secondo quanto affermato dalla società di sicurezza informatica Panda Security, i pirati informatici sono riusciti a **penetrare nei sistemi informatici** del comune **tramite un invio di E-mail di *phishing* legate all'epidemia**, particolarmente ingannevole per una P.A., in quanto le comunicazioni riportavano come oggetto "Informazioni sul Coronavirus", inducendo i dipendenti a cliccare su collegamenti a siti web malevoli, ed innescando così il ransomware.

La Panda Security ha spiegato che si tratta di una famiglia di *Ransomware* relativamente recente: non appena un computer viene infettato, il *Malware* si diffonde rapidamente su tutte le macchine connesse al medesimo network, dopodiché termina i processi e i servizi eseguiti da Windows, cripta i file presenti su tutti i dispositivi d'archiviazione disponibili e infine elimina i *Back-Up*.

Purtroppo quando i bersagli sono Pubbliche Amministrazioni spesso gli *Hacker* trovano terreno fertile, infatti secondo il rapporto dell'Osservatorio di Federprivacy, nel 2019 **il settore più colpito è stato proprio quello della Pubblica Amministrazione**, con il 17% del totale delle multe inflitte in tutti i paesi dell'Unione Europea, e anche in Italia sempre lo scorso anno il 48% delle ingiunzioni del Garante della privacy è stato comminato a carico di Pubbliche Amministrazioni.

IL COMUNE VINCE LA CAUSA CONTRO L'EX DIPENDENTE E NE PUBBLICA LA SENTENZA CON DATI SENSIBILI: CONDANNATO A PAGARE UNA SANZIONE PECUNIARIA

Qualche anno fa un'ex dipendente aveva fatto causa per *Mobbing* al Comune di Urago d'Oglio perdendo in primo grado, e l'amministrazione aveva **pubblicato sul proprio sito l'intera sentenza**, nella quale vi erano dati c.d. sensibili dell'interessato, anche relativi alle sue condizioni di salute, motivo per cui la persona **presentava un reclamo al Garante** per la protezione dei dati personali.

Per le opportune verifiche, l'Autorità avviava un'istruttoria, accertando che nel sito era effettivamente disponibile e liberamente scaricabile il testo integrale della sentenza, che lo stesso Comune motivava di aver pubblicato perché si trattava di informazione "resa pubblica solo per ragioni di trasparenza e di informazione riguardo ad un fatto noto". L'amministrazione si giustificava inoltre che se i dati dell'interessato contenuti nella sentenza erano rimasti pubblicati per mesi, era stato poichè questo non aveva mai fatto richiesta di rimuovere il documento, e che avrebbe potuto invitare l'amministrazione ad oscurarne le informazioni invece di presentare l'esposto al Garante.

D'altra parte, "all'esito del giudizio, ciò che premeva all'amministrazione [..era...] riscattare con dignità il danno all'immagine e al proprio operato pesantemente danneggiato dalle informazioni e dichiarazioni distorte che sono state diffuse attraverso la stampa e i social", **alcune delle quali rilasciate anche dallo stesso ex dipendente**.

Nelle proprie conclusioni, il Garante affermava che **il Comune**, in qualità di "Titolare del trattamento **è tenuto a rispettare i principi in materia di protezione dei dati**, fra i quali quello di liceità, correttezza e trasparenza nonché di minimizzazione, in base ai quali i dati personali devono essere trattati in modo lecito, corretto e trasparente nei confronti dell'interessato" come previsto dall'art. 5, par. 1, lett. a) e c), del GDPR. In particolare, precisava "nel rispetto del principio di minimizzazione dei dati, **anche in presenza di un obbligo di pubblicazione**, i soggetti chiamati a darvi attuazione **non possono comunque diffondere i dati personali eccedenti o non pertinenti**, e in ogni caso, i dati relativi alla salute non possono essere diffusi". Il Garante decideva pertanto di **irrogare una multa di 4.000 euro**, che adesso **l'amministrazione comunale di Urago dovrà pagare** a titolo di sanzione amministrativa pecuniaria.

UNA FINTA EMAIL SU IMMUNI PRENDE IN OSTAGGIO I PC E CHIEDE UN RISCATTO DA 300 EURO

Mentre Immuni fa il suo "esordio" sugli store di Apple e Google, una campagna di *Hacking* prova a sfruttare questo evento. A renderlo noto è l'Agid-Cert, la struttura del governo che si occupa di *Cybersicurezza*. Non si ha contezza, al momento, di quanti cittadini siano realmente coinvolti e a rischio, ma la vicenda è abbastanza emblematica, e necessita di grande attenzione.

A scoprire il tutto è stato un ricercatore. In sostanza, si tratta di una campagna di *Phishing* – quindi attiva con le classiche ***Email-esca***, che puntano a ingannare chi le riceve – che prova a sfruttare l'esordio di Immuni, l'APP per il ***Contact Tracing*** scelta dal governo italiano, che proprio in queste ore è in fase di rilascio.

All'interno della Email infetta, **si prova a convincere l'utente a cliccare su un link** che porta a un dominio creato ad arte per replicare i contenuti della Federazione Ordini Farmacisti Italiani (FOFI.it).

> IN REALTÀ BASTA UN CLICK PER FINIRE SUL FILE ESEGUIBILE "IMMUNI.EXE", CHE AL SUO INTERNO CONTIENE UN MALWARE CHIAMATO FUCKUNICORN.

È un virus di tipo *Ransomware* – di quelli che bloccano i computer e chiedono un riscatto per sbloccarli – che una volta eseguito mostra una finta *Dashboard* con i risultati della contaminazione da COVID-19. E mentre l'utente si trova davanti questa mappa, il *Malware* **provvede a cifrare i file presenti sul sistema** Windows della vittima e a rinominarli assegnando l'estensione ".fuckunicornhtrhrtjrjy".

Alla fine **sullo schermo compare il classico file di testo con le istruzioni per il riscatto**, che ammonta a 300 euro, in bitcoin, per liberare i file cifrati, quindi il PC. Come nella maggior parte dei casi, quando c'è di mezzo un *Ransomware*, pagare il riscatto è del tutto inutile. La transazione è protetta dall'anonimato tipico delle ***Criptovalute,*** E MAI NESSUN *CYBERCRIMINALE* VI VERRÀ IN AIUTO.

LA GESTIONE DEI DATI PERSONALI NELL'AMBITO LAVORATIVO IN PERIODI DI EMERGENZA

Con riferimento al trattamento dei dati personali in ambito lavorativo va precisato che il 14 marzo 2020 è stato sottoscritto il protocollo di sicurezza anti-contagio adottato ai sensi dell'art. 1, n. 7, lett. d) del DPCM 11 marzo 2020, integrato dal più recente protocollo del 24 aprile 2020. Il documento è stato realizzato per agevolare gli Enti e le imprese nell'adozione di protocolli di sicurezza anti-contagio, ovverosia Protocollo di regolamentazione per il contrasto e il contenimento della diffusione del virus COVID 19 negli ambienti di lavoro, ma contiene importanti disposizioni anche in materia di "privacy".

Difatti la rilevazione in tempo reale della temperatura corporea costituisce un trattamento di dati personali e, pertanto, deve avvenire ai sensi della disciplina privacy vigente. Per questo motivo vengono suggerite tutta una serie di **precauzioni da adottare**. In particolare bisogna:

1. Rilevare la temperatura e **non registrare il dato** acquisito. È possibile identificare l'interessato e registrare il superamento della soglia di temperatura solo qualora sia necessario a documentare le ragioni che hanno impedito l'accesso ai locali.
2. **Fornire l'informativa** sul trattamento dei dati personali.
3. Definire le **misure tecniche e organizzative adeguate** a proteggere i dati. In particolare, sotto il profilo organizzativo, occorre individuare i soggetti preposti al trattamento e fornire loro le istruzioni necessarie. A tal fine, si ricorda che i dati possono essere trattati esclusivamente per finalità di prevenzione dal contagio da COVID-19 e non devono essere diffusi o comunicati a terzi al di fuori delle specifiche previsioni normative (es. in caso di richiesta da parte dell'Autorità sanitaria per la ricostruzione della filiera degli eventuali "contatti stretti di un lavoratore risultato positivo al COVID-19).
4. In caso di isolamento momentaneo dovuto al superamento della soglia di temperatura, assicurare modalità tali da garantire la riservatezza e la dignità del lavoratore/soggetto interessato. Tali garanzie devono essere assicurate anche nel caso in cui il soggetto comunichi all'ufficio/unità responsabile di aver avuto contatti con soggetti risultati positivi al COVID-19 e nel caso di allontanamento del lavoratore

che durante l'attività lavorativa sviluppi febbre e sintomi di infezione respiratoria e dei suoi colleghi.

5. Qualora si richieda il rilascio di una dichiarazione attestante la non provenienza dalle zone a rischio epidemiologico e l'assenza di contatti, negli ultimi 14 giorni, con soggetti risultati positivi al COVID-19, si ricorda di prestare attenzione alla disciplina sul trattamento dei dati personali, poiché l'acquisizione della dichiarazione costituisce un trattamento dati. A tal fine, si applicano le indicazioni precedenti e, nello specifico, si suggerisce di **raccogliere solo i dati necessari**, **adeguati e pertinenti** rispetto alla prevenzione del contagio da COVID-19. Ad esempio, se si richiede una dichiarazione sui contatti con persone risultate positive al COVID-19, occorre astenersi dal richiedere informazioni aggiuntive in merito alla persona risultata positiva. Oppure, se si richiede una dichiarazione sulla provenienza da zone a rischio epidemiologico, è necessario astenersi dal richiedere informazioni aggiuntive in merito alle specificità dei luoghi.

Si sottolinea, inoltre, che il Garante per la protezione dei dati personali nelle proprie FAQ pubblicate il 14 maggio 2020 sul sito istituzionale ha specificato che nell'ambito del sistema di prevenzione e sicurezza sui luoghi di lavoro o di protocolli di sicurezza anti-contagio, il datore di lavoro può richiedere ai propri dipendenti di effettuare test sierologici **solo se disposto dal medico competente** o da altro professionista sanitario in base alle norme relative all'emergenza epidemiologica.

> SOLO il medico del lavoro nell'ambito della sorveglianza sanitaria, può stabilire la necessità di particolari esami clinici e biologici. Sempre il medico competente può suggerire l'adozione di mezzi diagnostici, quando li ritenga utili.

Nelle FAQ l'Autorità precisa anche che le informazioni relative alla diagnosi o all'anamnesi familiare del lavoratore **non possono essere trattate dal datore di lavoro** (ad esempio, mediante la consultazione dei referti o degli esiti degli esami). Il datore di lavoro deve, invece, trattare i dati relativi al giudizio di idoneità del lavoratore alla mansione svolta e alle eventuali prescrizioni o limitazioni che il medico competente può stabilire. Le visite e gli accertamenti, anche ai fini della valutazione della riammissione al lavoro del dipendente, devono essere posti in essere dal medico competente o da altro personale sanitario, e, comunque, nel rispetto delle disposizioni generali che vietano al datore di lavoro di effettuare direttamente esami diagnostici sui dipendenti.