**DATA PRIVACY DAY, ITALIA 2ᵃ IN EUROPA PER VIOLAZIONI GDPR (+600% IN UE NEL 2021): ECCO LE 10 MAGGIORI MINACCE PER I DATI DI UTENTI E AZIENDE NEL 2022**

***In occasione della Giornata europea della protezione dei dati personali preoccupa la situazione dell’Italia: il Paese è secondo in Europa per numero di violazioni (83) e terzo per sanzioni (quasi 80 milioni di euro). Nel 2021 in Europa multe per quasi 1,1 miliardi, un incremento vicino al 600% in un anno, e 356 segnalazioni al giorno di data breach. Il cyber crimine spaventa le imprese: se 4 su 10 hanno subìto attacchi informatici negli ultimi due anni, per il 2022 rappresenta la prima causa di preoccupazione per il 44% delle aziende. L’opinione dell’esperto Jacopo Tenconi, GDPR Specialist di Primeur, multinazionale italiana specializzata in data integration: “I dati sensibili sono un asset strategico ma in Italia siamo ancora molto lontani dal creare una cultura del valore della data compliance: l’evoluzione delle infrastrutture IT deve evolvere da cybersecurity a cyber-resilience”.***

La **Giornata europea della protezione dei dati personali** mette in evidenza tutti i **punti deboli dell’Italia** in materia di **GDPR**. Istituita dal **Consiglio d’Europa** nella giornata di oggi (28 gennaio), il **Data Privacy Day** si pone l’obiettivo di sensibilizzare **persone**, **aziende** e **istituzioni** al **corretto uso e conservazione dei dati sensibili**. Una campagna la cui importanza è sottolineata da **dati molto preoccupanti**: secondo un recente report di ***DLA Piper***, infatti, dal 25 maggio 2018 (data di entrata in vigore del nuovo regolamento europeo GDPR), l’**Italia** è **2ᵃ in Europa per numero di violazioni** con **83 interventi** dell’**Autorità Garante** (in testa c’è la **Spagna** con più di 250 sanzioni, segue la **Romania** con **57**) e si pone in **3ᵃ posizione** per **multe complessive** per quasi **80 milioni di euro**. Particolarmente sanzionate sono state le **imprese delle telecomunicazioni** visto che le tre principali multe (rispettivamente di 27, 16 e 12 milioni di euro) sono state comminate dal Garante a società TLC per aver **trattato in modo illecito i dati personali** per **attività di telemarketing e pubblicità**. “Purtroppo sono dati che non sorprendono: **in Italia siamo ancora molto lontani dal creare una cultura del valore della data compliance** – afferma **Jacopo Tenconi**, GDPR Specialist di ***Primeur***, multinazionale italiana specializzata nella data integration – La **corsa alla digitalizzazione** a cui stiamo assistendo sta portando una **nuova consapevolezza nelle persone sul valore e sull’uso dei dati** che sono ormai diventati un **asset strategico per le aziende**: chi sarà in possesso di un’**organizzazione informatica evoluta**, con strumenti automatici di **data integration**, di mappatura e di mascheratura dei dati in grado di **tenere costantemente sotto controllo i dati sensibili gestiti**, trattati e archiviati da un’organizzazione **sarà più competitivo sul mercato**. Questo trend di crescente consapevolezza è un **processo che è iniziato ed è inarrestabile**. Molte aziende, per contro, non sembrano avere acquisito altrettanta coscienza sull’importanza di ottemperare alle richieste GDPR come **parte integrante del servizio ai clienti finali** e alle terze parti: **questo gap di consapevolezza sarà alla base di sempre crescente insoddisfazioni dei clienti**. Le aziende più scaltre hanno capito che essere in linea con la GDPR non significa solo evitare multe salate e acquisire un **vantaggio competitivo cruciale**”.

Tornando allo **scenario europeo**, in testa alla **classifica delle sanzioni** si trovano **Lussemburgo** e **Irlanda**, nazioni dove hanno sede rinomate multinazionali del commercio online e dei social network: proprio all’interno del piccolo Granducato è stata comminata la multa più alta della storia dell’Unione Europea dal valore di **746 milioni di euro**. Complessivamente nel 2021 si è assistito ad un vero e proprio **boom di sanzioni** visto che nel **Vecchio Continente** si è sfiorata la **quota di 1,1 miliardi di euro di multe**: un **dato in crescita del 600%** rispetto allo stesso periodo dello scorso anno dove si sono registrate **violazioni complessive per 158,5 milioni di euro**. Non è migliore lo scenario sulle segnalazioni di **data breach**: il numero di violazioni che comportano l’**accesso**, la **modifica**, la **cancellazione** o la **divulgazione** **non autorizzata di dati personali** è arrivato oltre quota **130mila in Europa nell’ultimo anno**. Si tratta di una media giornaliera di 356 segnalazioni in **crescita del 7,5% rispetto ai dati 2020**. L’**Italia** **cresce a ritmo doppio** rispetto alla media europea: il report individua **1.782 violazioni** di **data breach** negli ultimi 12 mesi, **+13,2%** rispetto alle 1.574 indicate nel 2020 (in testa c’è la **Germania** con oltre **40mila notificazioni** seguita da **Paesi Bassi** e **Polonia**).

L’entrata in vigore del **regolamento europeo GDPR** ha modificato radicalmente lo scenario in materia di **privacy** e **gestione dei dati sensibili**: le aziende e le istituzioni devono **rispettare rigide regole in materia di gestione dei dati personali** che possono includere l'obbligo di notificare alle autorità le violazioni da parte di hacker o pirati informatici entro 72 ore dalla scoperta. Ma **come mai in Italia siamo ancora così indietro rispetto all’Europa?** Secondo **Simone Bonavita**, docente in **Trattamento dei Dati Sensibili** all’***Università degli Studi di Milano*** occorre fare una duplice riflessione: “Da una parte il **Garante Privacy Italiano** ha dei componenti di **comprovata capacità molto attenti alla tutela degli interessi della collettività** e ha intrapreso una serie di **attività di sensibilizzazione sui temi connessi alla tutela dei dati personali**. Dall’altra parte **molte società percepiscono la privacy come un** «**inutile onere**» **invece di un’opportunità di ottimizzazione dei processi**. Ottimizzare un processo significa **aumentare la produttività** e questa funzione efficientistica della privacy rappresenta un **paradigma non molto noto in territorio italiano**. A molte società italiane, inoltre, **manca un approccio**, nella privacy e nella sicurezza, che sia **attento al processo**, **piuttosto che al compito**”.

Uno **scenario in continua evoluzione** che **allarma soprattutto le aziende**: secondo l'***Allianz Risk Barometer*** i **rischi informatici** sono la **principale causa di preoccupazione delle imprese nel 2022 con il 44%** e hanno superato in classifica le difficoltà di approvvigionamento della supply chain, i disastri naturali, il cambiamento climatico e l’evoluzione della pandemia. Altre conferme arrivano dal **Global Cybersecurity Outlook 2022** diffuso dal ***World Economic Forum*** che sottolinea questi timori visto che **4 aziende su 10 hanno dichiarato di aver subito attacchi informatici negli ultimi due anni**. Proprio all’interno del report viene citato il termine “**Cyber Resilience**” come **nuovo modello di sicurezza per le aziende**: le organizzazioni dovranno sviluppare la **capacità di prepararsi**, **rispondere** e **riprendersi** **dagli attacchi informatici** visto che ormai le tradizionali misure di sicurezza non sono più sufficienti per proteggere i dati sensibili dagli attacchi informatici. **Phishing**, **malware** e cyber attacchi vari sono all’ordine del giorno e le aziende devono **lavorare su una strategia che possa ridurre l’impatto degli attacchi informatici** e **garantire la continuità aziendale** in modo tale da **riprendersi più velocemente in caso di futuri shock digitali**: “Ormai ladomanda che si devono porre i reparti IT non è **se ci saranno attacchi informatici ma quando arriveranno** e come sarà possibile **limitarne l’impatto sul business aziendale** – prosegue **Tenconi** –I recenti cambiamenti hanno **creato una dipendenza informatica senza precedenti** e gli **hacker stanno cogliendo ogni opportunità per sfruttare le vulnerabilità delle organizzazioni per predisporre nuovi attacchi informatici**”.

Ma non è tutto. Secondo il bilancio della **Polizia Postale** **2021** sono stati **oltre 5mila gli attacchi informatici a sistemi istituzionali**, infrastrutture critiche informatizzate di interesse nazionale, infrastrutture sensibili di interesse regionale, mentre sono stati **126 i cyber attacchi ai sistemi finanziari di grandi e medie imprese** per un ammontare complessivo di oltre **36 milioni di euro sottratti in modo illecito** (di cui 17 recuperati grazie all’intervento degli investigatori). Il report ha messo in evidenza anche un **importante aumento delle frodi informatiche ai danni dei cittadini**: +**27%** per un totale di **oltre 18.000 furti di dati sensibili**, numeri di carte di credito e chiavi private di wallet di cryptovalute. Il **cyber crimine è in aumento** e per difendersi serve come punto di partenza una **buona organizzazione personale**: “Oltre a **password complesse**, che rimangono la base per prevenire gli attacchi informatici, è il caso di dotarsi di un **programma di gestione delle stesse password** che possa suggerire il **cambiamento con cadenza mensile**. Naturalmente occorre **diffidare da link e allegati provenienti da mail e messaggi provenienti solo in apparenza da banche e uffici postali** e, in ultimo, **evitare di diffondere informazioni o dati personali sui social network. E ricordarsi sempre un vecchio concetto di marketing semplice ma fondamentale: se un servizio è gratis, il prodotto sei tu**”, conclude **Tenconi**.

Ma **quali sono le 10 maggiori cyber minacce che gli utenti dovranno fronteggiare nel 2022**?

* **Social Engineering** –Questa tipologia di attacco informatico studia il comportamento e le interazioni che le persone compiono online per poi ingannare gli stessi utenti con l’obiettivo di carpire informazioni sensibili, estorcere denaro o rubare identità.
* **Ransomware** –È la minaccia che preoccupa maggiormente le organizzazioni: il dispositivo digitale viene infettato da un programma malevolo che blocca l’accesso ai documenti per poi chiedere un riscatto. Recentemente la Regione Lazio ha subito un attacco ransomware che ha mandato in tilt diversi servizi riservati ai cittadini tra cui il portale dedicato alla vaccinazione.
* **Cryptojacking** – La nuova frontiera della truffa informatica. Questo attacco utilizza a insaputa del proprietario il dispositivo elettronico per finalità di *mining* delle valute digitali. A differenza delle altre minacce, l’obiettivo non sono le informazioni personali ma è quello di utilizzare un computer di un’altra persona per eseguire le operazioni di estrazione digitale e accumulare cryptovaluta.
* **Smishing** – L’evoluzione del phishing. Sono sempre di più le minacce che viaggiano attraverso i messaggi di testo: solitamente si tratta di finti istituti di credito o uffici postali che chiedono informazioni finanziarie personali come il numero di conto o quello della carta di credito.
* **Bot** – Si tratta di una rete composta da diversi pc infetti da malware che viene utilizzata per inviare mail nocive contenente spam, virus o con l’obiettivo di rubare i dati personali. Con l’aumento dello smart working e del contestuale utilizzo delle reti domestiche con device lavorativi, questi attacchi sono tornati all’ordine del giorno.
* **BEC, Business E-mail Compromise** – Questa tipologia di attacchi consentono agli hacker di accedere ad un account di posta elettronica aziendale e di fingere di essere il proprietario con l’obiettivo di truffare l’azienda stessa o i fornitori/partner con mail veritiere provenienti da un interlocutore autorevole.
* **Robocall** – Sono in forte aumento le chiamate in arrivo da sistemi automatizzati: questa tipologia di telefonate viene utilizzata sempre di più da società di telemarketing ma in alcuni casi le chiamate hanno l’obiettivo di ottenere in modo fraudolento i dati dell’utente per attivare a sua insaputa contratti non richiesti.
* **Deepfake** – È una tecnologia basata sull’intelligenza artificiale che, attraverso la sovrapposizione di volti su persone reali, permette di falsificare video creando immagini e filmanti altamente realistici. Questa tipologia di truffa viene utilizzata dagli hacker soprattutto per ricattare altre persone soprattutto in ambito della sfera personale.
* **Spyware** – È un malware che viene scaricato su un device elettronico senza il permesso dell'utente e ruba i dati degli utenti per venderli a inserzionisti e aziende esterne. È in grado d’infettare i dispositivi tramite app, collegamenti, siti web e allegati di posta elettronica dannosi.
* **SIM Swap** – La truffa dello “scambio della scheda telefonica” è un furto d’identità dove il criminale riesce ad ottenere i dati personali della vittima: tramite una finta denuncia, la Sim viene duplicata e così il truffatore può iniziare ad operare con l’home banking della vittima ricevendo sul suo cellulare le notifiche per autorizzare le operazioni.