PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 22 - numero 4838 di Mercoledì 16 dicembre 2020

L'agenzia medica europea EMA sotto attacco informatico

Quale debba essere il livello di vigilanza degli esperti di sicurezza informatica viene dimostrato dal recentissimo attacco all'agenzia europea, che si occupa di farmaci.

Questa agenzia dell'unione europea era inizialmente situata nel Regno Unito, ma, alla luce della iniziativa Brexit, la sede è stata trasferita in Olanda. Il compito di questa agenzia è quello di facilitare lo sviluppo dell'accesso a medicine di vario tipo, valutando le richieste di autorizzazione al commercio, tenendo sotto controllo la sicurezza dei prodotti medicinali durante l'intero ciclo di vita e, infine, dare informazioni accurate ed aggiornate sia al pubblico, sia al personale sanitario.

I compiti di questa agenzia sono stati significativamente incrementati a seguito della pandemia di COVID 19, per svolgere le attività legate all'approvazione dei vaccini contro questa malattia.

Gli esperti di sicurezza informatica, già negli Stati Uniti, avevano messo in guardia l'agenzia equivalente, la Food and Drug Administration- FDA, circa la possibilità di attacchi informatici. La stessa allerta era stata data anche all'agenzia europea, ma evidentemente l'allerta non è stata sufficiente per bloccare un attacco, portato a termine pochi giorni fa.

L'agenzia europea ha dichiarato che non desidera dare ulteriori informazioni sulla tipologia dell'attacco, finché le indagini sono in corso, ma ha promesso che quanto prima offrirà un quadro completo dell'accaduto.

Il problema non coinvolge solo la agenzia europea, ma anche le aziende, che stavano sviluppando i vaccini, da sottoporre ad approvazione.

In particolare, un portavoce di BioNTech ha dichiarato che la sua azienda è stata informata che l'agenzia europea è stata vittima di un attacco informatico e che alcuni documenti, che riguardavano la valutazione di accettabilità del vaccino presentato da Pfizer e BioNTech, il vaccino BNT162b2, archiviati su un server dell'agenzia, erano stati esaminati e compromessi. Il portavoce ha tenuto a sottolineare che la violazione riguardava solo i documenti in possesso dell'agenzia europea, mentre nessun documento, in possesso delle aziende produttrici del vaccino, è stato compromesso.

La mancanza di notizie non permette di inquadrare accuratamente la gravità dell'attacco, ma gli esperti ritengono che la sottrazione di questi documenti potrebbe ulteriormente ritardare l'approvazione del vaccino, che già era in attesa di approvazione da qualche tempo e che è stato già approvato in altri paesi.

Al proposito, l'agenzia europea per la sicurezza informatica, nonché l'Interpol, ha fatto presente che un ritardo nell'approvazione di questo vaccino potrebbe aprire la strada ad un ampio mercato per vaccini provenienti da altri paesi, già approvati. È un classico esempio di violazione informatica con riflessi di natura commerciale, ammesso che questa interpretazione risulti alla fine corretta.

Il portavoce dell'azienda produttrice ha espresso il proprio disappunto per il fatto che, mentre la sua azienda si impegnava a fondo per proteggere questi documenti, evidentemente il livello di impegno presso l'agenzia europea non era di pari livello.

D'altra parte, per ottenere l'approvazione l'azienda è obbligata a fornire tutt'una serie di documenti all'agenzia europea e pertanto non avrebbe potuto esimersi.

Questo evento serve da esempio ai titolari del trattamento, che devono comunicare dati di varia natura, anche personali, a soggetti terzi, di esigere perentoriamente che questi soggetti terzi tutelino i dati allo stesso livello di sicurezza e protezione da attacchi informatici, al quale questi dati sono protetti dall'azienda titolare.

Purtroppo, avviene abbastanza spesso che questi dati vengano comunicati a soggetti terzi, senza "pretendere" che questi soggetti terzi garantiscono un soddisfacente ed equivalente livello di protezione, rispetto a quello garantito dal titolare.

Qualora il titolare non ottenga queste garanzie, ed egualmente ceda dati a soggetti terzi, possono ravvisarsi gli estremi per una negligenza da parte del titolare originario ed ecco la ragione per la quale qualsiasi cessione di dati, soprattutto personali, deve essere opportunamente inquadrata.

Ciò vale per una azienda che cede i dati dei propri dipendenti ad un commercialista, che elabora paghe e contributi, ma vale anche, come nella fattispecie, per un'azienda che ceda i propri dati ad un ente pubblico.

È diritto dell'azienda cedente chiedere garanzie di adeguata protezione all'ente pubblico, ed è dovere dell'ente pubblico dare queste garanzie.

Mi auguro che gli esperti di protezione dei dati si ricordino di queste considerazioni, quando saranno coinvolti in cessione di dati, anche personali, a soggetti terzi.

Adalberto Biasiotti

www.puntosicuro.it