Attacchi Hacker e Nuovo Regolamento Europeo 2016/679 - La Difficile Vita della P.A. (non) Digitale

Date : 12 marzo 2018

E’ notizia di meno di 48 ore fa che il portale del Ministero dell’Università e Ricerca (MIUR) sia stato oggetto di un attacco hacker da parte del noto gruppo Anonymous.

La violazione dei sistemi ha portato, sia da quanto è possibile leggete sui comunicati on-line del gruppo di attivisti, sia da conferme ufficiali alla violazione dei sistemi di sicurezza, alla penetrazione all’interno dei server, al prelievo di un elenco di oltre 26000 caselle e-mail, con relativo user-id, password (con note successive il MIUR ha precisato che,in realtà, si trattava non di password vere e proprie bensì solo di codici HASH [*stringa/identificativo generato a seguito di impiego della funzione matematica di HASH rendendo non praticabile il percorso inverso e quindi il recupero dei dati originari in chiaro*]), recapiti telefonici, indirizzi ecc.

La notizia ha suscitato, come era prevedibile, reazioni opposte: da un lato reazioni stile “war games” come già accaduto in occasione di eventi simili (es. Unicredit Banca, UBER, Ministero Giustizia, Ministero Esteri, ecc), dall’altro reazioni da parte di soggetti (addetti ai lavoti) dotati di conoscenze più (o meno) approfondite sull’argomento (cyber security, hacking ecc.).

Se torniamo a qualche pubblicazione/rapporto pubblicato pochi mesi or sono, bisognerebbe rammentarsi che l’anno 2017 era stato più volte etichettato come *l’anno peggiore dal punto di vista degli attacchi informatici* (basti pensare alle ondate di virus cryptolocker che impazzavano – e l’attuale situazione non è certo rassicurante – mietendo vittime anche fra le amministrazioni locali, amministrazioni centrali, aziende sanitarie, aziende pubbliche di trasporto ecc), ma a conti fatti qualcosa è cambiato?... qualcosa, quantomeno, si sta muovendo dopo questo inizio del 2018?

A guardar bene la materia (cyber security, protezione dati, sicurezza infrastrutture di interesse nazionale) è stata, in questi ultimi anni, oggetto di una “pesante” offensiva normativa da parte dei legislatori sia nazionali, che comunitari. Ad esempio possiamo citare:

- **AGENZIA PER L'ITALIA DIGITALE** CIRCOLARE 18 aprile 2017, n. 2/2017 recante: «Misure minime di sicurezza ICT per le pubbliche amministrazioni. (GU n.103 del 5-5-2017);

- **Regolamento Europeo in Materia di Protezione Dati Personali** (REG UE 2016/679) (GUE n. 119 del 4-5-2016)

Leggendo il testo della Circolare n° 02/2017, all'Art. 1 -" ***Scopo***" troviamo : *" obiettivo della presente circolare è indicare alle pubbliche amministrazioni le misure minime per la sicurezza ICT che debbono essere adottate al fine di contrastare le minacce più comuni e frequenti cui sono soggetti i loro sistemi informativi."*

Continuando, all'Art. 5 – ***"Tempi di attuazione"*** – troviamo (perentorio):" *entro il* ***31 dicembre 2017*** *le amministrazioni dovranno attuare gli adempimenti di cui agli articoli precedenti".*

La Circolare è completata dalla Direttive del Presidente del Consiglio dei Ministri – 01/08/2015 – che come parte integrante reca una serie di tabelle utili alle PA per l'effettuazione delle analisi e l'individuazione delle azioni da intraprendere, sulla base della situazione di partenza, delle criticità rilevate e del "***grado di rischio***" assegnato (una sorta di brogliaccio per un discreto risk assessment).

A leggere con attenzione, effettivamente, le analisi e le verifiche previste, a carico delle PA, riguardano praticamente a 360° tutto ciò che ruota attorno all'ICT (es. dall'inventario dei sistemi Hardware e Software, alla verifica dell'utilizzo di sistemi Hardware esterni, la valutazione continua delle vulnerabilità, alle difese contro i malware, alle procedure/modalità inerenti copie di sicurezza, alla protezione dei dati);non si proferisce parola, al contrario, su due punti fondamentali:

1. Chi avrebbe dovuto (materialmente) effettuare quanto previsto nella circolare;
2. Con quali fondi/risorse porre rimedio a quanto di non conforme eventualmente rilevato.

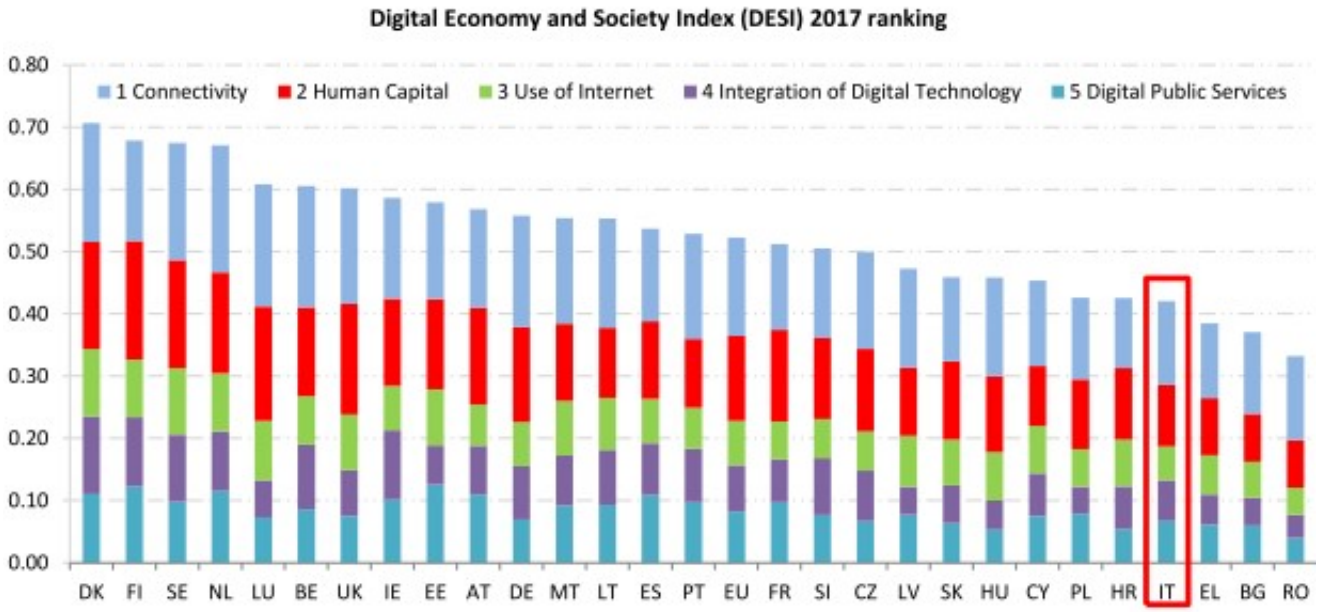
Il fattore "umano" spesso viene sottovalutato, se non ignorato del tutto, in molti settori, ma in un settore come la sicurezza IT, la difesa di infrastrutture critiche, dove notoriamente il è considerato spesso" l'anello debole della catena di sicurezza" su cui fare leva con lo scopo di portare a buon fine un attacco hacker, non prendere assolutamente in considerazione questa variabile potrebbe rivelarsi un errore gravissimo.

Questi due punti assumono una rilevanza ancora maggiore se consideriamo che l'età media dei dipendenti della PA italiana ha ormai oltrepassato la soglia dei 50 anni e che, a ragion veduta, una nutrita fetta di personale possiede un livello di conoscenza tecnica in ambito IT o IT security, minimo o addirittura insufficiente.

Nella nota del MIUR si legge anche che " *probabilmente gli 'indirizzi e-mail con dominio istruzione.it potrebbero essere stati utilizzati per registrarsi a siti o servizi esterni…"*. Se questa affermazione fosse comprovata, sarebbe il primo esempio di una carenza delle basi della sicurezza IT da parte del personale dipendente.

Dalla figura che segue, possiamo evincere come (anno 2017) l'Italia occupasse le retrovie nelle 5 aree analizzate dalla Commissione Europea al fine di valutare all'interno degli Sati Membri lo stato di avanzamento verso una Società digitale. Ovviamente l'Italia è stata classificata con un

lo stato di *slow performing,* che riguarda anche la digitalizzazione dei servizi pubblici.



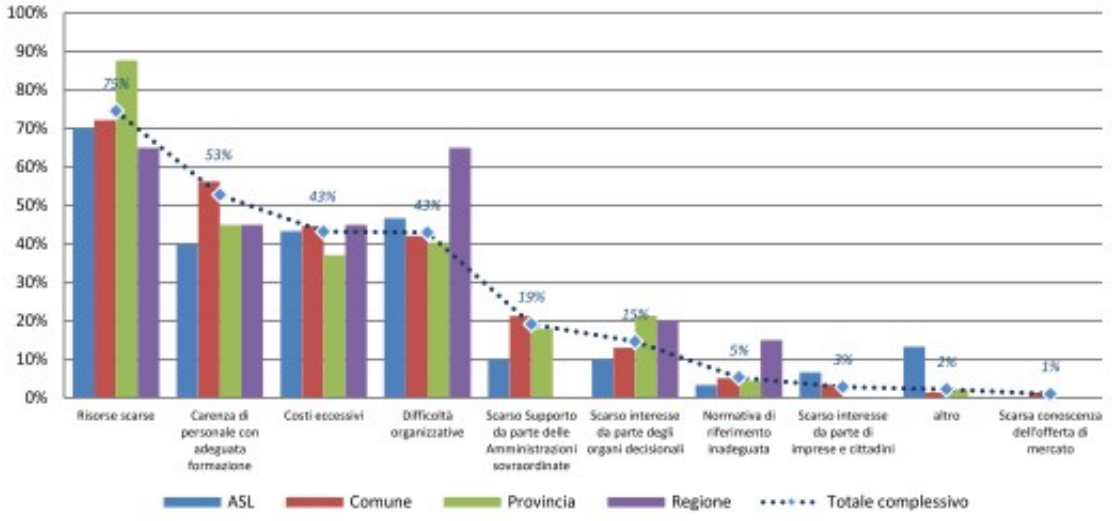
Il Rapporto CLUSIT 2015 sulla sicurezza Ict in Italia, ancora, aveva evidenziato come i siti di molte PA utilizzino versioni obsolete di software esponendosi in questo modo a rischi concreti di furti o perdite di dati. Anche dall'analisi effettuata sui siti di molte amministrazioni locali i risultati non sono stati confortanti: oltre 500 siti web di comuni italiani utilizzano software di gestione dei contenuti (Cms) il cui supporto è terminato nel 2012.

Consultando il rapporto Istat del medesimo anno vediamo come in ambito sicurezza informatica, solo il 48,8% delle PA si è dotata di un piano di *disaster recovery,* mentre solo il 15,6% utilizza tecnologie avanzate, quale *cifratura di dati.*

Risulta ovvio quindi che la PA si trovi ad affrontare ancora oggi una sfida complessa che implica consapevolezza tecnica, gestionale ed organizzativa e richiede competenze tecniche elevate e comprovate da parte delle risorse umane chiamate a gestire processi e infrastrutture tecnologiche.

Determinante ago della bilancia nel processo di innovazione della PA risulta quello legato alla possibilità di effettuare investimenti la cui maggiore rilevanza dovrebbe essere rivestita da quelli per risorse umane e competenze (tecniche). E' plausibile considerare, ad oggi, che carenze organizzative e ritardi accumulati da molte PA nell'utilizzo delle IT possano dipendere dalla impreparazione tecnica e delle risorse umane con competenze non adatte a gestire funzioni di questo ambito specifico.

Banca d'Italia con la sua indagine sull'informatizzazione delle Amministrazioni Locali – 2017, ha fotografato quelli che possono essere i reali motivi ostativi all'utilizzo corretto, consapevole e sicuro delle tecnologie IT all'interno della PA:



I fattori con maggiore incidenza (negativa) risultano anche in questa indagine:

1. Scarsità di risorse assegnate è con percentuali che variano dal 65% al 88%;
2. Carenza di personale con adeguata preparazione è con percentuali dal 40% al 56%.

Non dovrebbero, quindi, lasciare eccessivamente sconvolti eventi come quello accaduto al MIUR dato che nonostante la copiosa produzione di studi, ricerche, indagini e verifiche sul campo ci si continua a limitare a normare su materie come la sicurezza IT dove andrebbero effettuati a monte interventi “strutturali” reali.

In ultima battuta, andrebbe attentamente valutato questo evento se lo stesso fosse avvenuto/stato rilevato dopo il 25 maggio 2018, data in cui diverrà pienamente operativo in nuovo Regolamento Europeo di Protezione Dati Personali (GDPR 2016/679).

Se quanto accaduto al MIUR si fosse verificato post 25 maggio, come il Titolare del Trattamento (o i con-Titolari o i Responsabili del Trattamento- ove ve ne fossero -) avrebbero affrontato l’evento (*data breach*)? Come avrebbero risposto a quanto previsto dalla nuova normativa europea?

Sarebbe comunque interessante conoscere, quali sarebbero le risposte da parte del Titolare del Trattamento ad alcune (naturali) domande che sicuramente sarebbero state poste (ad es.):

- Quando si è avuta conoscenza del data-breach e quando è stata effettuata la comunicazione all’Autorità Garante nazionale (se si è ritenuto di effettuarla)? (Artt. 33 – 34 GDPR);
- Quali misure di sicurezza erano state adottate per la sicurezza dei dati? (Art. 32 GDPR);
- Era stata ritenuta necessaria e, in caso affermativo, era stata effettuata una valutazione d’impatto sulla protezione dei dati? (Art. 35 GDPR);
- Era stato designato un Responsabile della Protezione dei Dati (DPO/RPD)?(Art. 37 GDPR);

- Se nominato, il DPO, era stato messo in grado di assolvere correttamente ai compiti previsti?(Art. 39 GDPR);
- Era stato predisposto e correttamente/costantemente alimentato/aggiornato il Registro delle attività di trattamento? (Art. 30 GDPR).
  ……

Non possiamo sapere se e quali risposte sarebbero arrivate.

Ciò che lascia perplessi è che, nonostante le condizioni in cui versa la PA ad oggi (e sicuramente grossi cambiamenti in un prossimo futuro sarà difficile vederne!- ndr-) siano a conoscenza “di tutti” una reale spinta verso un cambio di rotta non è visibile all’orizzonte.

Con l’attuale scenario, nonostante il grande lavoro fatto fino ad oggi da parte dell’ Autorità Garante nazionale sarà difficile (nella maggior parte dei casi) in caso di verifica, trovare una PA pronta ad adempiere a quanto previsto dal GDPR (es. Artt. 5 – 24 - 30 e segg.) fornendo la documentazione che possa dimostrare(principio di *responsabilizzazione)* la volontà da parte di una PA di raggiungere una piena (o quantomeno accettabile) *compliance* alla normativa europea .

BIBLIOGRAFIA/SITOGRAFIA

- ItalyDESY2017Countryprofile.pdf;
- http://www.agid.gov.it/agenda-digitale/infrastrutture-architetture/cert-pa/misure-minime-sicurezza-ict-pubbliche-amministrazioni;
- Regolamento (UE) 2016/679, http://eur-lex.europa.eu/legal-content/IT/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ITA&toc=OJ:L:2016:119:TOC , ultima consultazione 20/11/2017;
- https://clusit.it/wp-content/uploads/download/Rapporto_Clusit%202015.pdf;
- https://www.bancaditalia.it/media/notizia/indagine-sull-informatizzazione-nelle-amministrazioni-locali/;

A cura di: **Leonardo Scalera**