Nuove minacce informatiche: quale strategia per difendere i sistemi della PA

Prof. Avv. Michele Iaselli

Quadro normativo

Il tema della sicurezza informatica della PA riveste un'importanza fondamentale perché necessaria per garantire la disponibilità, l'integrità e la riservatezza delle informazioni del Sistema informativo della Pubblica amministrazione.

Un'area tecnologica in continua evoluzione, quasi giornaliera, nella quale gli investimenti devono essere rafforzati in continuazione tenendo conto anche dei principi di privacy previsti dall'ordinamento giuridico.

Negli ultimi anni il numero complessivo di attacchi e di incidenti legati alla sicurezza informatica nella PA è aumentato in modo esponenziale. Tutti gli studi e le ricerche che analizzano e studiano questi fenomeni sono concordi nell'affermare una preoccupante tendenza alla crescita.

Le pubbliche amministrazioni, dal punto di vista sicurezza, possono essere considerate come organizzazioni fortemente regolate, in considerazione del fatto che la loro attività si svolge nell'ambito e nei limiti di norme che hanno valore di legge. Il problema è che fino ad oggi sono state poche le norme giuridiche che si siano occupate di cyber security.

Difatti, per quanto, l'art. 51 ("Sicurezza dei dati, dei sistemi e delle infrastrutture delle pubbliche amministrazioni") del CAD, prevede che "Agid attua, per quanto di competenza, il Quadro strategico nazionale per la sicurezza dello spazio cibernetico e il Piano nazionale per la sicurezza cibernetica e la sicurezza informatica..." e che il medesimo organo "coordina, tramite il Computer Emergency Response Team Pubblica Amministrazione (CERT-PA) istituito nel suo ambito, le iniziative di prevenzione e gestione degli incidenti di sicurezza informatici" la delicatezza della materia, forse, impone ancora una maggiore attenzione dal punto di vista normativo.

Proprio per questi motivi è stata pubblicata sulla G.U. (Serie Generale n. 79 del 04/04/2017) la Circolare AgID del 17 marzo 2017 n. 1/2017 contenente le “Misure minime di sicurezza ICT per le pubbliche amministrazioni”successivamente sostituita dalla circolare n. 2/2017 del 18 aprile 2017.

Le stesse misure sono parte integrante del più ampio disegno delle Regole Tecniche per la sicurezza informatica della Pubblica Amministrazione, emesso come previsto dal Piano Triennale per l'Informatica nella PA e dalla Direttiva 1 agosto 2015 del Presidente del Consiglio dei Ministri, che assegna all'Agenzia per l'Italia Digitale il compito di sviluppare gli standard di riferimento per le amministrazioni.

In tale ottica assume rilevanza anche la nuova direttiva sulla protezione cibernetica e la sicurezza informatica nazionale emanata con DPCM del 17 febbraio 2017 (pubblicato sulla GU n. 87 del 13-4-2017) che si pone l'obiettivo di aggiornare la precedente direttiva del 24 gennaio 2013 e di conseguenza anche la relativa architettura di sicurezza cibernetica nazionale e di protezione delle infrastrutture critiche.

Del resto (come si è anticipato) lo stesso art. 51 del CAD specifica che l'AgID attui, per quanto di competenza e in raccordo con le altre autorità competenti in materia, il Quadro strategico nazionale per la sicurezza dello spazio cibernetico e il Piano nazionale per la sicurezza cibernetica e la sicurezza informatica. AgID, in tale ambito:

a) coordina, tramite il Computer Emergency Response Team Pubblica Amministrazione (CERT-PA) istituito nel suo ambito, le iniziative di prevenzione e gestione degli incidenti di sicurezza informatici;
b) promuove intese con le analoghe strutture internazionali;
c) segnala al Ministro per la pubblica amministrazione e l'innovazione il mancato rispetto delle regole tecniche da parte delle pubbliche amministrazioni.

Ma cosa si intende per cyber risk?

La rivoluzione digitale sta portando molti benefici alla nostra società, ma, come spesso accade, bisogna considerare anche il rovescio della medaglia. Difatti, accanto agli innumerevoli benefici, l'uso incontrollato di Internet può comportare una quantità notevole di insidie e problematiche che rientrano nell'ambito di quel fenomeno definito cyber risk "rischio informatico (o ICT)".

Il rischio informatico può essere definito come il rischio di danni economici (rischi diretti) e di reputazione (rischi indiretti) derivanti dall'uso della tecnologia, intendendosi con ciò sia i rischi impliciti nella tecnologia (i cosiddetti rischi di natura endogena) che i rischi derivanti dall'automazione, attraverso l'uso della tecnologia, di processi operativi aziendali (i cosiddetti rischi di natura esogena).

In particolare questi ultimi possono essere:

- danneggiamento di hardware e software;
- errori nell’esecuzione delle operazioni nei sistemi;
- malfunzionamento dei sistemi;
- programmi indesiderati.

Tali rischi possono verificarsi a causa dei cosiddetti programmi “virus” destinati ad alterare od impedire il funzionamento dei sistemi informatici. Ma vi sono anche le truffe informatiche, la pedo-pornografia, il cyberbullismo, i ricatti a sfondo sessuale derivanti da video chat on line e solo una piena consapevolezza del concetto di sicurezza informatica può davvero metterci al riparo da sgradevoli sorprese.

Ogni giorno vengono compiuti migliaia di attacchi informatici attraverso le tecniche più varie e termini come malware, ransomware, trojan horse, account cracking, phishing, sono diventati parte del vocabolario anche per i non esperti.

J. Edgar Hoover, capo dell'FBI (Federal Bureau of Investigation) moltissimi anni fa affermava: "L'unico computer a prova di hacker è quello spento, non collegato ad Internet e chiuso a chiave in una cassaforte". Appena viene riacceso diventa potenzialmente vulnerabile e può essere attaccato, ad esempio durante l'installazione di eventuali aggiornamenti al sistema operativo.

Naturalmente per evitare attacchi informatici, o almeno per limitarne le conseguenze, è necessario adottare delle contromisure; i calcolatori e le reti di telecomunicazione necessitano di protezione anche se come in qualsiasi ambiente la sicurezza assoluta non è concretamente realizzabile.
Il modo per proteggersi è imparare a riconoscere le origini del rischio. Gli strumenti di difesa informatica sono molteplici, si pensi antivirus, antispyware, blocco popup, firewall ecc., ma tuttavia non sempre si rivelano efficienti, in quanto esistono codici malevoli in grado di aggirare facilmente le difese, anche con l’inconsapevole complicità degli stessi utenti.

Gli attacchi provenienti dal web

Quando si parla di attacchi provenienti dal Web non si può fare a meno di pensare ai virus, ma vedremo che non sono gli unici pericoli e tra l'altro non sono tutti uguali.
Un virus informatico è composto da un insieme di istruzioni da pochi byte ad alcuni kilobyte (per rendere più difficile da individuare e facile da copiare), tende ad eseguire soltanto poche operazioni ed impiega il minor numero di risorse, in modo da rendersi il più possibile invisibile.

I virus informatici più semplici sono composti da due parti essenziali, sufficienti ad assicurarne la replicazione:

1. ricercare i file adatti ad essere infettati controllando che non contengano già una copia, per evitare una ripetuta infezione dello stesso file;
2. copiare il codice virale all'interno di ogni file selezionato perché venga eseguito ogni volta che il file infetto viene aperto, in maniera trasparente rispetto all'utente.

Ma quando sentiamo parlare di virus, in genere ricomprendiamo malware, trojan horse, worm mettendoli tutto sullo stesso piano sia per genesi che per effetti, invece, è necessario fare delle precisazioni in quanto esistono delle sostanziali differenze tra queste diverse tipologie di virus.

In primo luogo c'è da precisare che sia i virus, sia i trojan horse che i worm rientrano nella categoria più generale dei malware.

Il termine malware deriva dalla contrazione di due termini inglesi, rispettivamente “MALicious” e “softWARE”, e viene utilizzato per indicare tutti quei programmi realizzati per danneggiare le macchine che li eseguono, da qui il nome di software malevolo. I programmi malware se riescono ad entrare in un computer possono creare dei veri e propri danni impedendone il corretto funzionamento, oppure possono spiare tutto quello che scriviamo, sottrarre dati sensibili, come ad esempio i numeri della carta di credito, per trasmetterli poi ad altri malintenzionati.

Il Trojan horse, letteralmente cavallo di Troia (chiaro riferimento all'inganno della mitologia omerica), può essere definito come un "programma apparentemente utile, ma che contiene funzioni nascoste atte ad abusare dei privilegi dell'utente che lo esegue".
A differenza dei virus non ha la capacità di autoriproduzione e diffusione, ma è l'utente a scaricarlo. Di solito si presenta sotto forma di gioco, screensaver ed altri articoli di interesse, ma una volta eseguito, il trojan installa segretamente il file server sul computer della vittima, compiendo allo stesso tempo tutte le operazioni di "copertura" che si suppone debba compiere.

I Worm sono programmi software dannosi sviluppati per diffondersi il più rapidamente possibile dopo che il PC è stato infettato. A differenza dei comuni virus, non sfruttano la presenza di altri programmi per moltiplicarsi, ma sfruttano i dispositivi di memorizzazione come le chiavette USB, le e-mail o le vulnerabilità nel sistema operativo. La loro propagazione rallenta le prestazioni dei PC e delle reti, diffondono dati all’esterno e possono provocare problemi al funzionamento generale del PC.

Come ultima frontiera dei pericoli digitali non possono essere dimenticati i micidiali “Ransomware” programmi maligni che, utilizzando efficaci tecniche di cifratura dei file, rendono inutilizzabili documenti, archivi, immagini e qualunque altro contenuto venga memorizzato sul disco fisso. L’operazione criminale è il preludio di una manovra estorsiva che si realizza con il rilascio di una salvifica parola chiave a fronte del pagamento di una determinata somma: “ransom”, infatti, è il termine anglofono che identifica il riscatto.

Ultimamente “wannacry” ha creato non pochi danni nel settore pubblico, ma per il passato anche “cryptolocker” è stato l’incubo di molti utenti della rete.

Come difendersi dai virus ed in particolare dalle nuove generazioni di virus (Ransomware)

Prestare la massima attenzione ai messaggi di posta elettronica.

Abilitare la visualizzazione delle estensioni in Windows

Limitare l’accesso alle risorse di rete

Fare copie di backup periodiche dei dati personali su dispositivi fissi o mobili

Utilizzare un buon sistema antivirus eseguendo regolari e giornalieri aggiornamenti del prodotto

Mantenere aggiornato tutto il software

Se possibile, utilizzare un personal firewall