L’Italia ed i Dati “Insicuri”

“Sicurezza dei dati durante la loro trasmissione verso i centro servizi. Resistenze psicologiche e pregiudizi”

Un messaggio forte arriva dall’Unione europea ,grazie alla riforma della protezione dei dati, nel quale viene sancito il diritto fondamentale circa la protezione dei dati.

Intanto gli accadimenti recenti sulla violazione dei dati ha diffuso qualche sconcerto ed ha aumentato la sensibilità circa la questione della sicurezza e privacy anche per il fatto che la dematerializzazione dei dati e la conseguente digitalizzazione si sta sempre più diffondendo.

La diffusione dei servizi in outsourcing obbliga le imprese ad alzare il livello di sicurezza per garantire ai propri utenti una risposta adeguata ai loro timori e nell’immediato futuro la sicurezza delle informazioni creerà competizione tra le aziende e la sicurezza delle informazioni sarà sempre di più un argomento che farà la differenza nell’ambito del business.

La normativa in materia di sicurezza e privacy dei dati oggi è sempre più uno strumento prezioso per consentirci di muoverci nell’era digitale.

La richiesta di servizi digitali in outsourcing obbligano le aziende a rendere sempre più accessibile alle applicazioni interne ai clienti o utilizzatori esterni su soluzioni web.

E’ sempre più in crescita la digitalizzazione delle informazioni ed a esternalizzare servizi che esulano dal core business aziendale, con la conseguente scelta da parte delle aziende che erogano servizi di investire in sicurezza e mentre da una

parte assistiamo ad un incremento di Data Center dedicati dall'altro si tende a prediligere sistemi con tecnologia modulare e virtuale.

Trasferimento dei dati su sistemi cloud, quali gli indici di sicurezza.

Nonostante di recente vi sia stato un incredibile sviluppo del cloud rimane ancora una certa resistenza "psicologica" nei confronti del suo utilizzo e come siano ancora piuttosto radicati, soprattutto in ambito professionale, taluni pregiudizi che etichettano il cloud come uno strumento rischioso ed insicuro.

Il Cloud, questo sconosciuto

La categoria che maggiormente soffre nella scelta di tale tecnologia è da ricercarsi prevalentemente nei dirigenti aziendali e soprattutto nei consulenti.

Su un campione intervistato di 200 professionisti , in una fascia del 50 -55% ha palesato una certa apprensione nei confronti della sicurezza e riservatezza dei dati in transito da e per i sistemi virtuali. Gli elementi negativi più evidenziati sono: perdita di controllo sulle operazioni di trasferimento delle informazioni , atti di pirateria informatica.

La colpa è di Internet?

Internet ormai costituisce uno strumento friendly a livello mondiale che consente l'accesso a tutti ed è per questo motivo che la trasmissione dei dati è rischiosa soprattutto quando sono particolarmente sensibili.

Nonostante le misure di sicurezza siano elevate, sussiste sempre la possibilità che i dati vadano persi o vengano intercettati, manipolati da persone non autorizzate o addirittura da delinquenti che si appropriano della nostra identità o delle informazioni di natura personale.

La tecnologia crittografica protegge i dati che viaggiano su internet?

Nelle operazioni che svolgiamo quotidianamente sulla rete internet è molto comune l'uso della crittografia, per esempio quando facciamo acquisti online i nostri dati vengono garantiti da una connessione VPN cifrata.

Col metodo crittografico il messaggio in chiaro viene convertito in un messaggio cifrato che sarà incomprensibile a tutti tranne al destinatario che con un sistema di decrittografia inverte il processo ottenendo il documento in chiaro, garantendo la riservatezza dei dati in modo che solo chi è autorizzato può leggere il messaggio originale.

A differenza delle tecniche usate nel passato, oggi si utilizzano algoritmi di pubblico dominio e la decrittografia risulta praticamente impossibile se non si conosce la chiave con cui si è cifrato il messaggio. La crittografia viene utilizzata per fornire riservatezza in ambito "Open Systems Interconnection" nelle seguenti fasi:

- **Applicazione**, la crittografia dei dati viene utilizzata per la sicurezza in e-mail, database (Oracle SQL *

  Net) e di messaggistica (Lotus Notes).

- **Sessione**, i dati vengono crittografati utilizzando un protocollo come il Secure Socket Layer (SSL) o

  Transport Layer Security (TLS).

- Rete, i dati vengono crittografati utilizzando protocolli come IPsec.

Stiamo parlando di un sistema sicuro ma un utente malintenzionato può tentare di rompere un algoritmo o testo cifrato usando una varietà di attacchi:

Attacco chosen-plaintext:

in questo caso il crittoanalista è in possesso del solo testo cifrato ottenibile facilmente analizzando i pacchetti in transito sulla rete.

La possibilità di successo di questo tipo di attacco è molto remota e necessita di un'enorme quantità di dati cifrati.

Attacco known-plaintext:

il crittoanalista è in possesso del testo cifrato e del corrispondente testo in chiaro.

Grazie a questo tipo di informazione è possibile risalire alla chiave segreta che

equivale a carpire il “modus operandi” di una determinata persona o azienda che usa crittografare i propri dati, dal momento che di solito una stessa chiave viene utilizzata per diversi documenti e per un certo periodo di tempo, l’acquisizione della chiave equivale quindi a rendere vulnerabile anche altri testi cifrati.

Attacco a forza bruta:

Tutti gli algoritmi di crittografia sono vulnerabili a un attacco a forza bruta. Con questo attacco il crittoanalista tenta ogni chiave possibile per decriptare il testo cifrato.

Generalmente un attacco a forza bruta riuscirà a raggiungere il suo scopo dopo aver provato il 57% di tutte le chiavi possibili.

Per difendersi da questo forma di attacco i crittografi moderni hanno implementato soluzioni di sicurezza tali per cui la quantità di chiavi possibili è talmente grande da richiedere troppo tempo e denaro per provarle tutte.

Un po’ come il tentativo di vincere al gioco del “Lotto”, le combinazioni sarebbero tante e molte più costose della probabile vincita.

Possiamo asserire che la crittografia può considerarsi affidabile quando:

- E’ resistente agli attacchi crittografici sopra descritti
- Permette chiavi variabili, ampie e scalabili.
- Crea un effetto valanga, al variare di un singolo carattere del testo da cifrare il risultato criptato deve
- Essere completamente diverso dal precedente testo criptato
- Non ha limiti sia all’esportazione che all’importazione dagli stati.
- Protegge da letture e modifiche non autorizzate.
- Certezza della sorgente, della destinazione e del contenuto dell’informazione.
- Garanzia che chi trasmette e chi riceve non possano negare di avere rispettivamente inviato e ricevuto il messaggio

Come possiamo descrivere un dialogo sull’autostrada digitale chiamata “Internet”?

Immaginiamo un dialogo tra uno scienziato americano ed uno italiano che intendano comunicare in modo riservato attraverso un canale risultato poi "insicuro" , perché reso tale dalla interferenza della CIA (servizio segreto americano) che ascolta la comunicazione ed ha interesse a capire cosa si dicono i due scienziati per timore di fuga di dati segreti.

Supponiamo che i due scienziati condividano uno stesso pacchetto di messaggi , noto anche alla CIA. Ipotizziamo che i due scienziati parlino la stessa lingua e che i messaggi che si scambiano sono trasmessi in chiaro e quindi comprensibili anche alla CIA.

Ben presto i due scienziati si accorgono di essere intercettati e decidono di falsare i dati trasmessi in chiaro e apparentemente incomprensibili e privi di significato ma che in sostanza sono comprensibilissimi dai due scienziati. Infatti gli stessi scienziati utilizzano un linguaggio segreto concordato in precedenza. In maniera più precisa usano un cifrario attraverso una coppia di

funzioni individuate da una specifica chiave di cifratura che trasforma il messaggio in chiaro in un nuovo messaggio detto "messaggio cifrato". Entrambi gi scienziati usano una chiave di decifratura che riporta il messaggio nelle condizioni di partenza prima della trasmissione.

Possiamo dire che la sicurezza è stata rispettata? , dipende dai punti di vista , forse sarebbe stato meglio da parte dei due scienziati usare fin da subito tecniche avanzate di sicurezza. Consoliamoci alla fine la guerra è stata scongiurata!!

Il Cloud era già conosciuto dagli Indiani? – Un po' di storia –

Gli indiani , popolo saggio, già conosceva i segreti legati alla sicurezza e le tecniche di crittografia.

Chi non ricorda i film tra indiani e le giubbe blu, quando l'ora dell'attacco veniva comunicato da nuvole di fumo sapientemente lanciate nel cielo, eravamo bambini e non sapevamo ancora di assistere ad una geniale tecnica di crittografia in un sistema "cloud".

Perfino nel corso della seconda guerra mondiale gli americani usarono le tecniche indiane per scambiarsi messaggi cifrati. Gli americani preferirono l'uso del linguaggio indiano in particolare Navajo sia perché un linguaggio praticamente

inesistente e sia per l'impossibilità da parte degli asiatici ed europei di accedere alle sue radici idiomatiche.

La tecnologia moderna e la messa in sicurezza dei nostri dati

La necessità di mantenere delle informazioni segrete è da sempre di fondamentale importanza per l'uomo e la tecnologia , l'arte di creare codici ha radici lontane nel tempo che affondano addirittura nel tempo antico quando la comunicazione di dati imponeva una forma che li rendesse illeggibili nel caso fossero caduti in mano ad estranei o addirittura male intenzionati.

In ambito della sicurezza la società digitale e i nuovi modelli d'uso ICT, sia il privato che la Pubblica Amministrazione, sono orientati a strutturare il loro lavoro e il trattamento dei dati, delle informazioni e dei documenti sotto forma digitale, la sicurezza dei sistemi (e quindi dei dati, delle informazioni e dei documenti), pertanto la sicurezza diventa parte essenziale per le aziende che si occupano del servizio in outsourcing.

La continuità operativa e la sicurezza da accessi illeciti è infatti garantita dallo steso art. 97 della Costituzione e poi dal Codice delle privacy e dal nuovo CAD del 2010, secondo anche quanto stabilito dalle nuove regole tecniche convertite recentemente in norma.

Le aziende fornitrici di servizi e le stesse amministrazioni pubbliche, sono costrette ad una verifica strutturale e di processi per definire e realizzare quali siano le soluzioni per la sicurezza informatica, la business continuity e il disaster recovery, anche perché ci troviamo difronte ad uno stringente obbligo di legge che impone , come anche proposto all'Agenzia per l'Italia Digitale, uno studio di fattibilità e un piano per la continuità operativa e la sicurezza.

E' importante prendere consapevolezza e quindi trovare soluzioni idonee per delineare i rischi e benefici dell'adozione dei servizi del tipo tradizionale e anche nell'ambito di una G-Cloud,sia nell'acquisizione di servizi cloud.

La sicurezza dei sistemi informatici, e quindi dei dati e delle informazioni, la ricerca di soluzioni adeguate rispetto alle nuove esigenze di servizi e di continuità

operativa, i nuovi modelli tecnologici come Open data, Cloud e Byod (Bring Your Own Device) sono temi dibattuti in tutti i convegni, soprattutto alla luce dei dati del 2012/2013 che registrano un aumento del rischio dovuto all'incremento del numero e della qualità degli attacchi informatici e dei rispettivi investimenti per l'innovazione tecnologica.

L'importanza della sicurezza e della conservazione della memoria digitale diventa di particolare importanza quando pensiamo all'enorme patrimonio di dati presenti nel Data center della Pubblica amministrazione e anche il patrimonio rappresentato dalle informazioni progettuali delle aziende private.

Oggi si parla di spending rewiev , sacrosante scelta per gli sperperi della Pubblica Amministrazione, allo stesso tempo è importante evidenziare che essa possa generare delle criticità se orientata alla riduzione di investimenti a fronte di una pressante e indispensabile esigenza di innovazione tecnologica.