BUSINESS

I QUADERNI DI FASTWEB

#2

LA PROTEZIONE DEI *DATI*

OBBLIGHI NORMATIVI E OPPORTUNITÀ

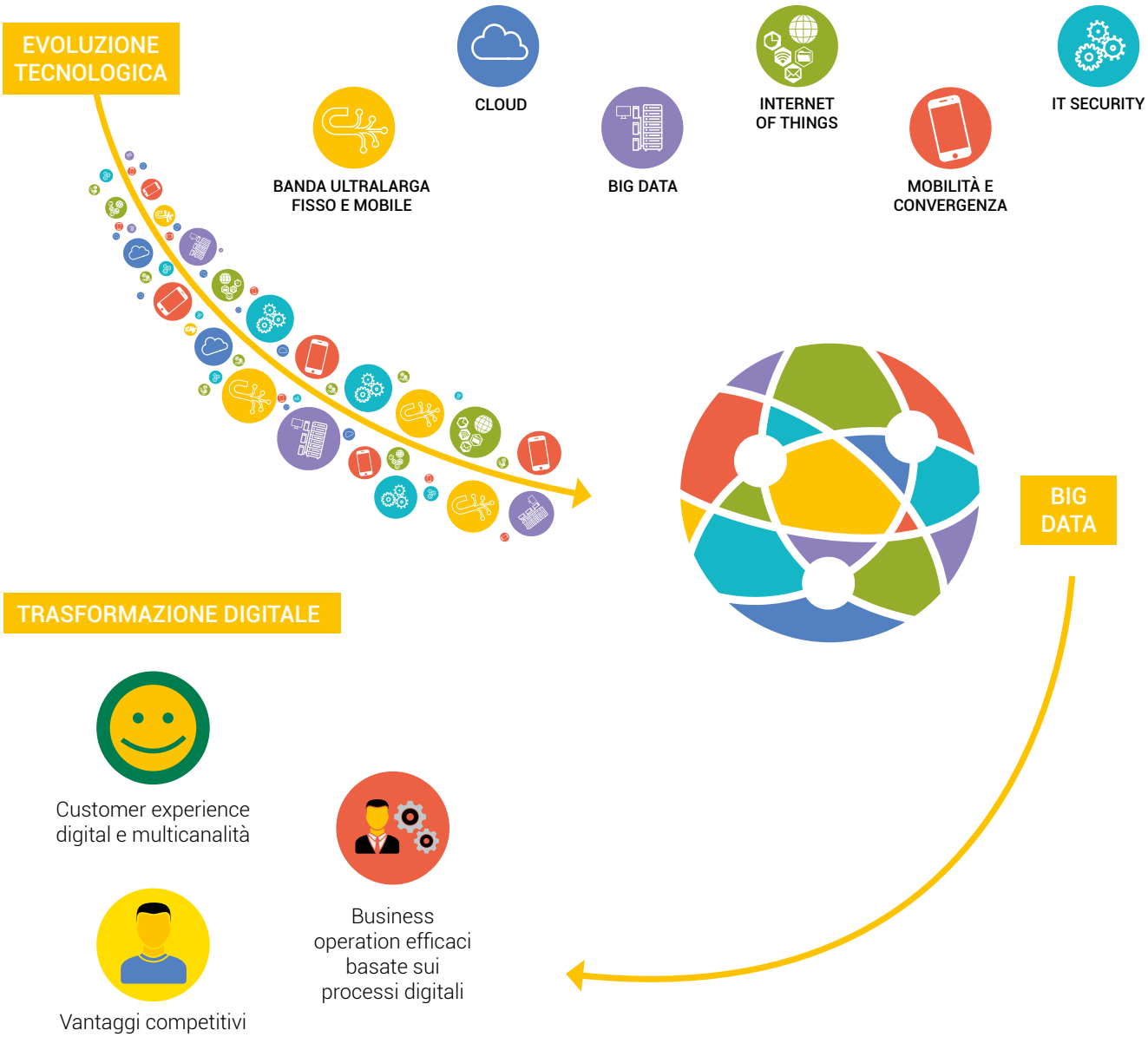
2017

FASTWEB

1 PROTEGGERE I DATI, IL NUOVO PATRIMONIO DELLE AZIENDE

Parlare di sicurezza informatica per le aziende ha sempre significato trattare di temi correlati per lo più alla protezione della propria rete aziendale da attacchi esterni, in larga parte provenienti da internet. Questo rimane certamente ancora un aspetto importante, ma occorre oggi considerare il tema della sicurezza in una prospettiva più ampia che si focalizzi sull'elemento fondamentale che oggi costituisce **il patrimonio di un'azienda: I DATI**.

Viviamo infatti una fase di grande cambiamento che ci coinvolge tutti come utenti e come aziende: siamo sempre più connessi e lo **scambio dei dati è divenuto vitale** perché il **nostro business, grazie alla trasformazione digitale** in atto, **è sempre più intimamente legato alla gestione di informazioni** (inerenti per esempio a fornitori, clienti, ecc.) che ci permettono di essere efficaci nella relazione con i clienti, nelle attività commerciali, nell'ottimizzazione dei processi produttivi ecc.



Governare una mole sempre crescente di dati e garantirne la sicurezza in tutto il loro ciclo di vita implica affrontare sfide importanti dal punto di vista dell'IT Security, una delle quali è il cosiddetto "dissolvimento del perimetro": i dati infatti vengono continuamente generati e utilizzati da personale interno ed esterno all'azienda, attraverso differenti dispositivi, elaborati, trasferiti, archiviati e conservati, spesso in diversi cloud. Evidentemente **non possiamo più limitarci a vigilare sul perimetro**, badando solo alla protezione di ciò che può arrivare dall'esterno (Big Internet) nella nostra rete, ma dobbiamo fare molta attenzione ad almeno altri due aspetti.

Il modo in cui gestiamo e proteggiamo, per l'intero ciclo di vita, il nostro patrimonio informativo, dall'acquisizione dei dati al loro utilizzo: adottiamo processi che ne garantiscano sempre la disponibilità, l'integrità e la riservatezza adeguate?

Il comportamento che adottiamo in azienda come utilizzatori di informazioni: siamo consapevoli ad esempio che, quando apriamo allegati nelle mail, questi potrebbero essere potenzialmente pericolosi perché potrebbero contenere ransomware, ovvero quei tipi di malware che bloccano l'accesso ai dati e richiedono un riscatto in bitcoin? *(cfr."Difendersi dalle minacce Ransomware –Giugno 2017" - https://www.fastweb.it/grandi-aziende/news/articolo/difendersi-dalle-minacce-ransomware*

Se perdessimo i dati che utilizziamo per fare campagne mirate sui nostri clienti? Se un evento disastroso (incendio, alluvione, terremoto) rendesse inutilizzabile il nostro Data Center o un virus si propagasse nella nostra rete bloccando applicazioni o sottraendo dati, rendendo di fatto impossibile evadere ordini o gestire servizi di manutenzione, cosa succederebbe?

La **reputazione dell'azienda** ne sarebbe intaccata pesantemente: i dati persi, o peggio hackerati, potrebbero essere venduti a società concorrenti favorendo così un vantaggio per un possibile competitor (i cybercriminali si sono specializzati in queste attività: l'incremento a livello globale degli attachi di tipo «cyber espionage» è aumentato tra il 2016 ed il 2017 del 47% - fonte: Clusit 2018).
La perdita dei dati renderebbe inoltre **l'azienda poco sicura agli occhi del mercato minando l'efficacia di iniziative commerciali future**. La fiducia dei clienti, la trasparenza delle operazioni che l'azienda effettua, sono alla base del rapporto cliente-fornitore. Mettiamoci nei panni di un cliente: cosa faremmo se da un giorno all'altro venissimo a conoscenza che un nostro fornitore ha perso tutti i dati sensibili dei suoi clienti tra cui i nostri e che in questo momento un hacker, da qualche parte nel mondo, li sta vendendo ad altri soggetti? Riferimenti, credenziali, informazioni bancarie ecc.

Si potrebbe poi innescare anche una **richiesta di danni da parte dei clienti**, in particolar modo se stiamo parlando di **DATI SENSIBILI (*)**, senza contare poi che la regolamentazione impone obblighi e **sanzioni** molto consistenti: il GDPR, ovvero **REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI, impone sanzioni alle aziende non conformi che possono arrivare fino a 20 Mln o al 4% del fatturato annuo**. Sono coinvolte tutte le aziende site all'interno dell'UE che elaborano dati di cittadini dell'UE, anche se i dati vengono processati fuori dall'UE, e aziende con sede al di fuori dell'UE quando elaborano dati di cittadini europei al fine di offrire beni, servizi (onerosi e non) o monitorare il loro comportamento entro l'UE. Il GDPR dal 25 Maggio 2018 sostituisce ed integra la normativa espressa dalla Direttiva 95/46/CE e dal Codice per la Protezione dei Dati Personali – D.Lgs. 196/2003.

I dati sensibili, quindi, costituiscono un insieme di informazioni estremamente strategiche che un'azienda non può permettersi di perdere, ma la situazione è tutt'altro che incoraggiante.

64% **Il 64% delle organizzazioni in Italia è sprovvista al momento di un piano globale per reagire all'impatto del GDPR.**

52% **Solo il 52% delle organizzazioni in Italia è in grado di rimuovere in modo efficace tutti i dati sensibili se viene esercitato dal cliente il "diritto all'oblio".**

58% **Il 58% delle organizzazioni mette a rischio la privacy dei propri clienti non mascherando i dati durante i test.**

(fonte IL SOLE 24 ORE – art. Nuovo regolamento UE sulla privacy: più di due terzi delle aziende in Europa non lo rispettano)

(*) Il D.Lgs. 196/2003 definisce "Sensibili" dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale.

2 LE COMPLIANCE NORMATIVA: UN TEMA CON CUI CONFRONTARSI

IL RISCHIO È TROPPO ELEVATO PER SOTTOVALUTARLO!

La regolamentazione in termini di gestione dei dati esiste da tempo, ma la ragione per la quale adesso è diventato estremamente importante affrontare il tema in maniera organica è dovuta al fatto che **operiamo in uno scenario di rischio sensibilmente diverso**: la trasformazione digitale del business, l'utilizzo quotidiano di dati e informazioni relative a cittadini EU (basta un nome, un numero di telefono o delle coordinate bancarie…), rendono le conseguenze di una non compliance alla regolamentazione estremamente significative. I Cybercriminali che creano i "malware" (virus e non solo) e li utilizzano, non fanno molta distinzione tra le aziende da colpire: il loro scopo è infettare il maggior numero di obiettivi e massimizzare i profitti attraverso la rivendita di informazioni o i riscatti.

OPERARE SECONDO LA NUOVA COMPLIANCE NORMATIVA CONVIENE ALLE AZIENDE

L'insieme delle azioni da mettere in campo, dagli adeguamenti tecnologici dell'IT alla revisione di alcuni processi interni, comporta spesso un'ottimizzazione dei processi stessi, una razionalizzazione della spesa IT e, sicuramente, una consistente riduzione del rischio complessivo e del relativo impatto economico. Infatti, tra le prescrizioni incluse nel GDPR, alcune sono particolarmente significative, sotto questo aspetto.

- L'introduzione della **figura del DPO** (Data Protection Officer) o "responsabile della protezione dei dati" consente di attribuire la responsabilità del governo della gestione dei dati sensibili in maniera certa e non necessariamente tale figura deve fare parte dell'azienda stessa.
- Il **programma di istruzione e formazione permanente** per il personale dell'azienda e l'obbligo di dotarsi di **adeguati processi e tecnologie, aumentano il livello di sicurezza informatica** complessiva e non solo quello relativo ai dati. Infatti l'azienda dovrà adottare misure tecniche (hardware e software) in grado di far fronte alle cyber minacce, oggi sempre più numerose, attraverso sistemi/processi quali Backup, Disaster Recovery, piattaforme di cybersecurity, crittografia dei dati, classificazione delle informazioni ecc.)

Le Aziende si dotano di **efficienti soluzioni per salvaguardare l'integrità, la riservatezza e la disponibilità dei dati e di processi e infrastrutture per garantire la continuità del business** in caso di calamità o cyber attacchi (cfr "Quaderno numero 1 – GARANTIRE LA CONTINUITA' DEL BUSINESS: DISASTER RECOVERY e BUSINESS CONTINUITY nell'era del CLOUD"). Inoltre risulta evidente, anzi "certificato", agli occhi degli utenti, che l'Organizzazione titolare del trattamento dei dati ha messo in campo tutte le procedure necessarie per garantire un corretto utilizzo degli stessi e soprattutto per salvaguardare la privacy degli utenti con **benefiche conseguenze sulla reputazione e la fiducia di clienti e fornitori**.

3 CHE COSA FARE IN PRATICA?

Il percorso di adeguamento alla nuova regolamentazione dovrà prevedere poche ma fondamentali tappe di avvicinamento alla conformità, che hanno l'obiettivo primario di **garantire il governo del ciclo di vita del dato**, dalla sua acquisizione alla sua distruzione: esiste infatti il diritto all'oblio come principio del GDPR ovvero il diritto dell'interessato ad ottenere la distruzione "senza ingiustificato ritardo" dei dati che lo riguardano nei casi previsti dalla normativa (ad esempio a seguito della cessazione di un rapporto contrattuale). Il percorso che generalmente viene adottato prevede le seguenti tappe da affrontare in funzione dell'evoluzione del modello di business, dell'organizzazione e delle condizioni di mercato.

SANITY CHECK

Analisi dell'attuale livello di sicurezza e di tutti processi "business critical": calcolare il livello di rischio su ogni area di business, dare le priorità agli interventi di adeguamento, inventariare i dati processati/trattati.

DESIGN

Adeguamento o ridefinizione dei processi e, se necessario, delle organizzazioni: nominare il Data Protection Officer (DPO), pianificare le attività di formazione interna ecc.

EXECUTION

Implementazione e configurazione degli strumenti tecnologici a supporto, test dei nuovi processi, collaudo e certificazione delle soluzioni adottate.

LA TECNOLOGIA

Da un punto di vista tecnologico, le soluzioni che indirizzano nella maggioranza dei casi i requisiti di compliance e forniscono nel contempo un adeguato livello di protezione sono costituite da infrastrutture e servizi di:

1. **Backup e Disaster Recovery in Cloud** per garantire in ogni evenienza (disastro o attacco informatico) la disponibilità e l'integrità dei dati oltre ad assicurare l'operatività del business.

2. **Controllo delle politiche di accesso ai dati** attraverso la gestione strutturata dei permessi e degli accessi a sistemi e applicazioni IT.

3. **Piattaforme e servizi di cybersecurity** per contrastare in maniera adeguata le minacce principalmente portate dal cybercrime, proteggendo i dati in primis, ma anche l'infrastruttura ICT dell'azienda.

Affrontare però un tema articolato come la protezione dei dati in questa nuova ottica regolamentare, adottando cioè un approccio a 360° che ha impatti su tecnologie, organizzazione e processi, può risultare piuttosto impegnativo se si decide di procedere autonomamente senza ricorrere ad un supporto qualificato. Una soluzione valida per molte imprese invece può risultare quella di rivolgersi a soggetti esterni in grado di mettere in campo competenze e garantire asset adeguati.

Un team di business analyst, con esperienza su diversi contesti aziendali, per elaborare le analisi preliminari, disegnare i nuovi processi a sostegno della nuova organizzazione, **supporto legale e tecnico-specialistico** (team di presale, centri di competenza ICT & Security, team dedicati alla gestione della cybersecurity ecc.).

Soluzioni ad hoc, disegnate sulle esigenze del Cliente e basate su **infrastrutture tecnologiche d'eccellenza in termini di performance affidabilità e sicurezza** (Rete a banda Ultralarga, Data Center Certificati, piattaforme di Cloud Computing e Security allo stato dell'arte): in altre parole **soluzioni e servizi basati su un mix di tecnologia e competenze di alto livello**.

FASTWEB

Con 2,6 milioni di clienti su rete fissa e 1,6 milioni su rete mobile, Fastweb è uno dei principali operatori di telecomunicazioni in Italia. L'azienda offre una vasta gamma di servizi voce e dati, fissi e mobili, a famiglie e imprese. Dalla sua creazione nel 1999, l'azienda ha puntato sull'innovazione e sulle infrastrutture di rete per garantire la massima qualità nella fornitura di servizi a banda ultralarga. Fastweb ha sviluppato una infrastruttura di rete nazionale in fibra ottica di 50.500 chilometri, con oltre 4 milioni di chilometri di fibra. Grazie all'espansione e al continuo potenziamento della rete ultra broadband, Fastweb raggiunge oggi 22 milioni di abitazioni, di cui 8 con rete proprietaria, con velocità di collegamento fino a 1 Gigabit. La società offre inoltre ai propri clienti un servizio mobile di ultima generazione basato su tecnologia 4G e 4G Plus. Entro il 2020 il servizio mobile verrà potenziato, a partire dalle grandi città, grazie alla realizzazione di una infrastruttura di nuova generazione 5G con tecnologia small cells. Fastweb fornisce servizi di telecomunicazioni ad aziende di tutte le dimensioni, dalle start-up alle piccole e medie imprese, dalle società di grandi dimensioni fino al settore pubblico, alle quali offre connettività e servizi ICT avanzati, come l'housing, il cloud computing, la sicurezza e la comunicazione unificata. La società fa parte del gruppo Swisscom dal settembre 2007.

Self-Service Cloud Portal

DISPONIBILITÀ ANNUA
99,997%

RISPOSTA AI GUASTI
automatica senza interruzioni

100 ORE
autonomia energetica

GREEN
PUE 1,25

POTENTE
40 kW/rack

Relativamente ai servizi Data Center e Cloud, Fastweb ha costruito un'infrastruttura dedicata ai clienti Enterprise, basata su un **Data Center di ultima generazione certificato Tier IV da Uptime Institute**. Realizzato secondo gli standard più esigenti in termini di sicurezza e affidabilità esso è in grado di ospitare anche applicazioni e servizi "mission critical" tra i quali vi sono quelli erogati dall'infrastruttura Cloud di Fastweb dedicata alle imprese. Tale infrastruttura è infatti concepita per garantire continuità e performance alle applicazioni di business. In particolare la piattaforma Cloud IaaS (Infrastructure as a service) di Fastweb garantisce la totale segregazione logica e applicativa degli ambienti dedicati ai singoli Clienti in modo da ottenerne il completo isolamento. Grazie ai motori di Orchestration e Automation sviluppati internamente su piattaforma "aperta" Openstack, i sistemi Cloud di Fastweb sono in grado di allocare risorse in maniera scalabile e in tempo reale in funzione del carico e dell'uso applicativo del singolo cliente secondo il modello Software Defined Data Center (le componenti di computing, network, storage e security sono virtualizzate e orchestrate da un'unica piattaforma). Tutta l'infrastruttura Cloud è gestita da team specializzati in centri di competenza e nuclei operativi di gestione dedicati rispettivamente a Data Center, infrastruttura IT e Security, in grado di supportare i Clienti dalla fase di progetto a quella di attivazione ed esercizio.

Per quanto riguarda in particolare i servizi dedicati alla sicurezza, Fastweb rende disponibili alle aziende una serie di servizi e soluzioni di IT Security attraverso il modello di **Managed Security Service Provider**. Tale modello prevede infatti che ciascuna azienda mantenga la totale autonomia nella definizione della Governance dell'IT Security in termini di livelli di rischio e conseguenti priorità di protezione di sistemi e informazioni e demandi invece la gestione operativa dell'IT Security ad un operatore esterno dotato di processi, competenze specifiche e piattaforme tecnologiche adeguate.

Fastweb, oltre a mettere a disposizione un centro di competenza dedicato alla progettazione di soluzioni di IT Security, si è dotata anche di un **Security Operation Center** (SOC Enterprise) dedicato esclusivamente alla gestione dei servizi di sicurezza per le Aziende. Il SOC Enterprise di Fastweb opera in Italia con personale italiano erogando un servizio con copertura H24 7gg/settimana; è dotato di processi conformi alle normative con le certificazioni "ISO 9001 – Quality Management" e "ISO 27001 – Information Security Management", gestisce piattaforme di sicurezza multi-tecnologia sia presso le sedi dei Clienti che centralizzate nell'infrastruttura Cloud di Fastweb, anch'essa con le medesime certificazioni oltre alla conformità alla norma "ISO 27018 – Privacy on Public Cloud". Con il proprio SOC Enterprise Fastweb gestisce direttamente migliaia di apparati e piattaforme di sicurezza operative presso le Aziende Cliente.

Grandi Aziende Fastweb
fastweb.it