GDPR & IT

COME APPLICARE IL GDPR ALLA VOSTRA INFRASTRUTTURA

RELATORE

EMANUEL SAPORITI

SENIOR NETWORK ENGINEER

Premessa:

- Il gdpr impone 4 punti fondamentali per garantire la tutela e l'integrità dei dati:
  - Si deve essere in grado di recuperare velocemente i dati se vengono persi. E vanno anche protetti contro le distruzioni accidentali
    Articolo 32 (Comma 2)
  - Per evitare che attraverso un data breach vengano prelevati dati in maniera indebita può essere opportuno cifrarli.
    Articolo 32 (comma 1b)
  - E' necessario garantire la "confidenzialità dei dati" e l'integrità
    Articolo 32 (comma 1b)
  - Dopo un data breach è necessario avvisare le autorità entro 72 ore dalla scoperta
    Articolo 32 e 33

Un “bigino”:

- Cos’è la crittografia?
  - E un modo per rendere inaccessibili o illeggibili dei dati, senza averne la chiave di lettura, (più è lunga più è sicura), il metro di misura è il bit, quindi se vi parlano di crittografia a 256 bit (siti web come google) ovviamente sarà meno sicura di una a 2048 bit (interconnessioni tra banche o datacenter).
- Pro:
  - Rende le comunicazioni sicure
  - Garantisce la confidenzialità dei dati
  - Attesta l’integrità dei dati
- Contro:
  - Rallenta e appesantisce i sistemi di vecchia generazione
  - In caso di perdita della chiave, i dati non saranno più accessibili

Un “bigino”:

- Cos’è il backup?
  - E’ Il sistema che si occupa della conservazione dei dati contenuti all’interno dei server o dei pc aziendali. Può essere di due categorie, in Cloud o On Site, e in caso di esigenze particolari di integrità dei dati, può essere effettuato in entrambe i metodi.
  - Il backup si suddivide in due ”specie”:
    - Backup: Ovvero, una copia giornaliera dei dati e delle informazioni necessarie
    - Disaster Recovery: è la copia dell’intero server completo di sistema operativo, configurazioni, applicativi.
  - Entrambe le metodologie sono funzionali allo scopo, ma devono essere selezionate in base alle esigenze di tempistiche di ripristino, in quanto il classico backup, impiega molto più tempo per rimettere l’infrastruttura in funzione. Invece un disaster recovery, può ripristinare l’operatività nell’arco di qualche ora. Nulla vieta poi di avere entrambe i sistemi in funzione

Un “bigino”:

- Cos’è il Data Breach?
  - Il Data Breach consiste in una fuga, o inaccessibilità dei dati, che ne può compromettere l’integrità. Un paio di esempi:
    - Cryptolocker: I file non sono accessibili, non si sa bene che fine possano fare, criptati in mano ad un Hacker, magari contenenti dati sensibili o essenziali…
    - Smarrimento: Un dispositivo come uno Smartphone, o un Notebook, senza adeguati sistemi di protezione (crittografia) consente l’accesso a tutte le informazioni contenute e gli accessi a tutto quello che è un browser dove l’utente ha lasciato selezionata la spunta “memorizza password”
    - Furto: il furto di un server, o di un dispositivo di backup senza gli adeguati sistemi di protezione

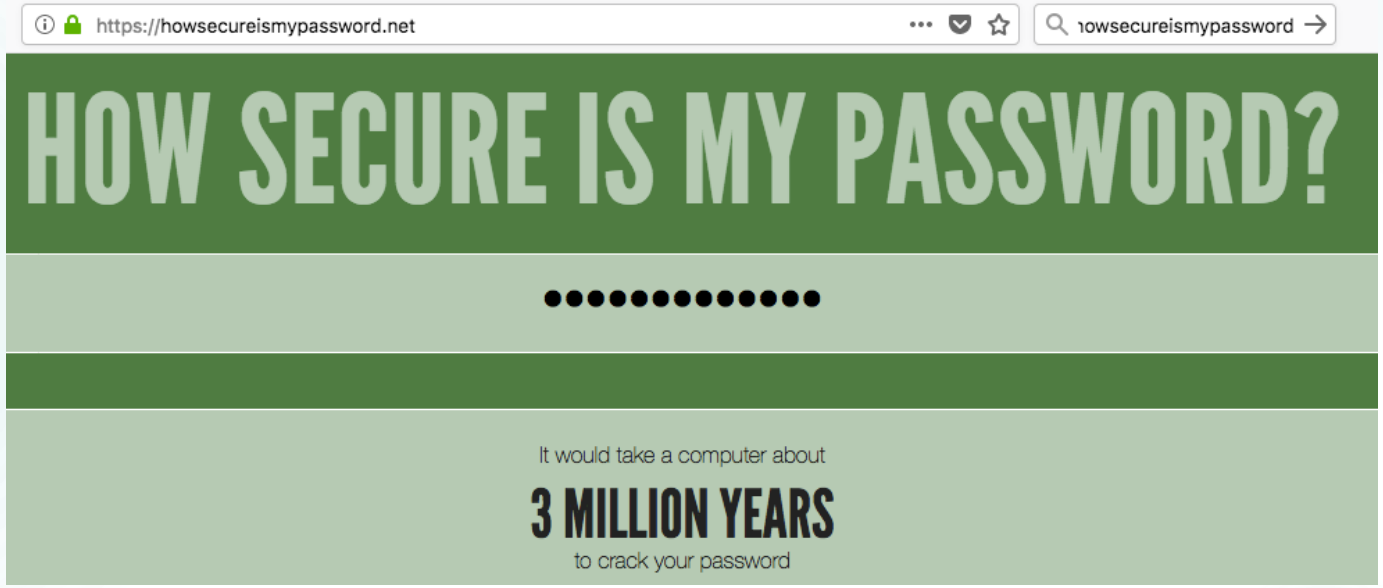
In media un azienda su quattro ha subito un Data Breach negli ultimi 2 anni.
Il 60% di chi lo ha subito si è rassegnato alla perdita completa dei dati.

Parliamo di Sicurezza IT

- Per prevenire tutto quello che può essere una perdita di dati, alla base di tutto ci deve essere:
  - Criteri sulle password: imporre una lunghezza minima, la presenza di caratteri speciali e numeri, nonché una scadenza della stessa.
  - Accesso ai dati: Limitare l'accesso ai dati strettamente pertinenti alla mansione dell'utente.
  - Internet e rete: Possedere un Firewall che consenta l'accesso alla rete dall'esterno solo tramite VPN, evitando di pubblicare porte accessibili da chiunque. Monitorare la navigazione degli utenti o in caso non sia necessaria impedirla completamente.
  - Antivirus & Antispam: Implementati sia sui client che sui server per garantire una protezione ottimale da ogni tipo di minaccia proveniente da web, applicazioni ed e-mail
  - Backup: Monitorati e gestiti correttamente, crittografati e di tipologie diverse (backup e disaster recovery, o backup on site e on cloud)

Password:

Stando al sito www.howsecureismypassword.net
La password “lampadina” è craccabile in soli 2 minuti
Se diventa “Lampadina” il tempo sale a 19 ore
Se aggiungo 123 alla fine il tempo diventa 300 anni
Se in fondo metto un * arrivo a 3 milioni di anni



Password:

- La criticità legata alle password, non è da sottovalutare, in quanto consente di accedere alla rete, alle caselle di posta, ai dati ecc…
  - Posta elettronica: l'indirizzo di posta è una cosa abbastanza "pubblica" e se la password non è adeguata ai criteri di sicurezza, consente di impersonare l'utente della e-mail in oggetto, con possibili comunicazioni fasulle per conto dello stesso. Inoltre può compromettere l'accesso ad altre piattaforme attraverso il reset della password tramite email, per esempio tutti i profili social e dispositivi come smartphone e tablet.
  - Rete aziendale: consente l'accesso a dati e al dispositivo dell'utente, impersonandolo completamente, senza possibilità di riconoscere l'operato di uno e l'operato dell'altro.
  - Credenziali Amministrative di rete: l'80% dei dispositivi connessi su una rete aziendale ha le credenziali di default, ovvero "admin" , una manomissione di questi dispositivi può bloccare completamente una rete aziendale, una stampante, un router, causandone notevoli disservizi, o fughe di dati e accessi indesiderati dall'esterno.

Accesso ai dati:

- Limitare l'accesso delle utenze alle aree strettamente di pertinenza riduce i possibili problemi dovuti a perdite/eliminazioni accidentali/volute e garantisce l' accesso ai dati sensibili solo alle persone incaricate. Inoltre un criterio di blocco schermo con password è un modo utile per garantire la privacy dei dati.
  - Dati Sensibili nell'ufficio personale/paghe: Patologie, retribuzioni, richieste ferie, e un infinità di dati sensibili vengo inviati giornalmente ai responsabili dell'ufficio personale o paghe. Questi dati vanno tutelati con la massima attenzione al fine di evitare sanzioni e richieste di risarcimenti da parte dei dipendenti
  - Dati Sensibili nelle formulazioni/progettazioni: Tutto quello che è un progetto o una formulazione di un azienda, fa parte del suo patrimonio e del suo valore, risulta indispensabile limitare l'accesso alle aree contenenti queste informazioni al fine di evitare sottrazioni volontarie o modifiche/eliminazioni accidentali.
  - Dati Personali: Tutto quello che consente il riconoscimento e l'identificazione di una persona(carte di identità e codici fiscali, patenti, coordinate bancarie, numeri di telefono ecc…) necessitano un ulteriore attenzione, in quanto il furto, lo smarrimento, o la richiesta dell'eliminazione degli stessi (come previsto dal GDPR) obbligano l'azienda a trattarli in maniera particolare, sia per garantirne l'accesso solo ai preposti, che per consentirne una facile eliminazioni a fronte di una richiesta.

Internet e Rete:

- Il web facilita la condivisione dei dati e l'invio degli stessi a terzi. L'accesso alla rete non gestito correttamente rappresenta una minaccia non trascurabile.
  - Accesso ad Internet: Rendere accessibile tutto il web all'interno di un azienda, si presenta come la principale fonte di problemi. I problemi più semplici possono essere legati all'accesso da parte dell'utente a sii malevoli, download di contenuti illegali. La seconda problematica è l'accesso alle web mail personali o ai vari siti di files haring (we transfer/dropbox…), che consentono la trasmissione non monitorata di contenuti sensibili e/o furto di dati aziendali.
  - Rete: Tutto quello che è apparati di networking all'interno di un azienda, sono componenti critici e fondamentali per il funzionamento degli stessi, pertanto una compromissione degli stessi mette a repentaglio tutta la sicurezza dei dati all'interno della rete. Il primo errore da non sottovalutare è legato alle password, il secondo all'apertura di porte per servizi dall'esterno (desktop remoto, telecamere ecc…) e l'ultimo è l'accessibilita di questi dispositivi dall'esterno tramite le porte di management.

Antivirus & Antispam:

- Il primo modo per evitare data breach (cryptolocker), fermi lavoro e contraffazione dell'e-mail è la prevenzione, tramite sistemi in grado di monitorare in tempo reale tutto quello che è il flusso di email e l'accesso al web.
  - Spam & Contraffazione dell'e-mail: Esistono sistemi proattivi in grado di analizzare il flusso di posta che viene ricevuto dall'azienda, e verificarne l'autenticità tramite i parametri spf (verifica della proprietà del dominio).Una successiva verifica dell'esistenza del mittente e una verifica in ambiente sandbox del possibile rischio del contenuto.
  - Antivirus: La presenza di un antivirus risulta ormai fondamentale, tanto da essere uno dei prerequisiti da parte di alcune aziende per iniziare a collaborare. L'antivirus deve essere periodicamente aggiornato e i dispositivi su cui è installato, devono svolgere delle scansioni periodiche. Ovviamente questo non mette al sicuro dall'imperizia dell'operatore o dai virus di ultimissima generazione, ma almeno consente di ridurre queste eventualità.

Backup:

- La questione fondamentale del GDPR è l'integrità dei dati, tanto da prescriverne delle politiche di conservazione. Principalmente i backup vanno monitorati costantemente e sottoposti a verifiche di integrità. Per prevenire l'accesso ai dati sottoposti a backup, il GDPR ha consigliato la crittografia degli stessi. Se un malintenzionato dovesse venire in possesso di una copia del backup, potrebbe estrarne il contenuto senza alcun problema.
  - Backup On Site: il backup fatto in questo modo, necessita di ambienti protetti, preposti a contenere il dispositivo di backup. In caso di dispositivi mobili (hard disk usb o tape) devono essere adeguatamente conservati.
  - Backup On Cloud: si fa riferimento alla normativa sottoscritta con il fornitore del servizio, il quale si impegna solo a garantire l'integrità e l'accessibilità dei dati, ma non prende posizione sulla parte legata al controllo degli accessi al sistema.
- La seconda questione introdotta è la velocità e la sicurezza del ripristino degli stessi, ma in funzione dell'azienda, è ovvio che un ospedale deve essere in grado di garantire il ripristino di una cartella clinica in tempi estremamente rapidi, e che un azienda può impiegare una giornata per ripristinare una cartella.
  - Disaster Recovery: è una questione che va analizzata in ogni singola realtà in base al RTO (tempo previsto per il ripristino) e alle necessità aziendali di fermo utenti. La domanda necessaria a capire se si necessita di un sistema di Disaster Recovery è: quanto tempo può stare la mia azienda senza accendere un computer? E quanto mi costa?

Concludiamo:

- Ogni azienda necessita di un attenta analisi per quanto riguarda la sicurezza dei dati trattati, e le politiche di backup ed eventualmente di disaster recovery.
- Le politiche di accesso ai file devono essere disegnate attentamente al fine di evitare rallentamenti sul lavoro del personale
- La sicurezza di un azienda, inizia dalle password che utilizza e dalla sua infrastruttura di rete, non che dalla presenza di antivirus e sistemi di protezione e prevenzione.