General Data Protection Regulation “G.D.P.R.”
Regolamento Europeo 206/679

Accountability e Compliance dello Studio Notarile
Controlli di Sicurezza

Punti di interesse:

1) Vulnerabilità
2) Gestione Postazioni
3) Sicurezza dei Siti WEB
4) Rischi navigazione e consultazione e-m@il
5) Backup ben strutturato

Consiglio Notarile
dei Distretti Riuniti di Campobasso, Isernia e Larino
Relatore : Luigi De Paola – MCP Microsoft

Premessa 1/2

CYBERSECURITY, DATA-PROTECTION E PRIVACY VIOLATA SONO ARGOMENTI CHE SI DEVONO CONOSCERE, PER EVITARE DANNI IRREPARABILI e/o LA PERDITA DEL PROPRIO PATRIMONIO.

LO SCENARIO TECNOLOGICO IN CUI IL PROFESSIONISTA RIMANE ESPOSTO AI PERICOLI DIGITALI, INFORMATICI ED UMANI.

Il REGOLAMENTO EU, GDPR 2016/679 (pubblicato in Gazzetta Ufficiale UE il 04/05/2016) DETERMINA NUOVE MODALITA' e GARANZIE CHE DEVONO ESSERE APPLICATE AL TRATTAMENTO DEI DATI.

Premessa 2/2

I RISCHI DI NON ESSERE PRIVACY COMPLIANT: QUALI RESPONSABILITA' E QUALI SANZIONI AMMINISTRATIVE.
TRA OBBLIGAZIONI E RACCOMANDAZIONI, COSA FARE?

CAMBIARE LE PROPRIE ABITUDINI, IN UN MONDO CHE CAMBIA DI CONTINUO LE REGOLE DEL GIOCO.
PRIMA DELLA CONFORMITA' DI LEGGE (A CUI SI E' OBBLIGATI), E' BENE ESSERE TUTELATI NEL PROPRIO PERIMETRO LAVORATIVO.
FONDAMENTI, APPROFONDIMENTI E SCHEMI PER LA SICUREZZA FISICA, LOGICA E DIGITALE ALL'INTERNO DEGLI STUDI PROFESSIONALI.
COME COSTRUIRE UN PROPRIO MODELLO (FRAMEWORK) PER ESSERE CONFORMI (COMPLIANT) ALLA NUOVA NORMATIVA "GDPR".

LE DOMANDE DA PORSI SONO:

- SEI CERTO DELLA TUA SICUREZZA DIGITALE, DI QUELLA DEL TUO STUDIO E DEI TUOI COLLABORATORI?
- LA PROTEZIONE DELLE INFORMAZIONI DEVE ESSERE GARANTITA DA CHI LE GESTISCE, COME AGISCE IL PROFESSIONISTA, IN QUALITA' DI TITOLARE (DATA CONTROLLER) ?
- HAI MAI PERSO DEI DATI?
- SEI SICURO DI LAVORARE IN UN AMBIENTE "SALVABILE"?
- QUALI MINACCE INFORMATICHE e NON SOLO, SONO IN ATTO?
- LA TUA IDENTITA' E' DAVVERO PROTETTA?
- SEI ORGANIZZATO PER AFFRONTARE UN EVENTO IMPREVISTO DI QUESTO TIPO NEL TUO STUDIO?

1) Vulnerabilità

La vulnerabilità può essere intesa come una componente (esplicita o implicita) di un sistema, in corrispondenza alla quale le misure di sicurezza sono assenti, ridotte o compromesse, il che rappresenta un punto debole del sistema e consente a un eventuale aggressore di compromettere il livello di sicurezza dell'intero sistema.
Particolarmente importanti sono le vulnerabilità dei sistemi informatici nei confronti di hacker o cracker.

La vulnerabilità non è detta che deve essere per forza informatica, infatti può essere altresì riferita a persone, individui singoli o gruppi di individui (gruppi o comunità di vulnerabili).
In altre parole, una vulnerabilità è una falla che può consentire ad un attaccante di compromettere un sistema o un ufficio, cioè di ridurre il livello di protezione esistente.

Tipologie di Vulnerabilità

Le vulnerabilità si possono presentare a qualsiasi livello di un sistema informatico, ne esistono principalmente di due tipi:

1) Vulnerabilità software (bug software):
Si presenta ovunque ci sia un difetto di progettazione, codifica, installazione e configurazione del software.
2) Vulnerabilità dei protocolli: si manifestano quando i protocolli di comunicazione non contemplano il problema legato alla sicurezza; l'esempio classico di vulnerabilità consiste nel permettere una connessione in chiaro (non crittografata) consentendo a possibili malintenzionati di intercettare le informazioni scambiate.
Le vulnerabilità quindi non compromettono un sistema, ma se utilizzate da quella che viene definita una minaccia (azione indesiderata) possono trasformarsi in un evento indesiderato.

Tipologie di Vulnerabilità

Si possono trovare vulnerabilità anche in ambito hardware. La presenza di umidità, polvere, sporco e supporti di memorizzazione non protetti o malfunzionanti, possono causare perdita di informazioni.

3) In ambito umano e sociale la vulnerabilità può essere definita come segue:

"*la vulnerabilità è un concetto dinamico e relativo, in stretta relazione con la capacità di un individuo o di una comunità di far fronte in un determinato momento a particolari minacce. La vulnerabilità può essere associata a certi elementi specifici della povertà, ma è anche propria di individui isolati, in situazioni di insicurezza ed indifesi da rischi, da shock e stress*".

Cause di Vulnerabilità

Una vulnerabilità può essere causata da:

• Complessità: Sistemi informatici molto grandi e complessi, possono essere causa di falle e involontari punti di accesso.

• Connettività: Più sono presenti porte, protocolli, privilegi, connessioni fisiche e servizi, e più il tempo in cui queste sono accessibili, più è probabile la presenza di un attacco.

• Password: L'utente utilizza password deboli, facilmente soggette a password cracking, oppure utilizza troppo spesso la stessa password o la memorizza nel computer.

• Sistemi operativi obsoleti: Certi sistemi operativi permettono agli utenti e ai programmi un ampio accesso alle risorse, permettendo tutto ciò che non è stato esplicitamente negato. Questa politica, sebbene più funzionale, permette a virus e malware di eseguire comandi anche a livello amministratore creando effetti indesiderati.

Cause di Vulnerabilità

• Navigazione in Internet: Certi siti possono contenere Spyware o Adware che vanno ad infettare il dispositivo, rubando informazioni personali.
• Bug Software: In un programma viene lasciato un bug. Questo potrebbe essere sfruttabile per un possibile attacco all'applicazione.
• Non imparare dagli errori: Quando un programmatore ripete gli stessi errori in nuovi programmi, aumenta la possibilità che questi siano conosciuti e quindi attaccabili.
• Si veda, ad esempio, le vulnerabilità nei protocolli IPv4, scoperte essere ancora presenti nei nuovi IPv6.

Ricerche dimostrano che il punto più vulnerabile di un sistema informatico è il fattore umano (utente, designer, operatore).
L'ingegneria sociale è un problema in continua crescita nell'ambito della sicurezza informatica.

2) Gestione Postazioni

Per postazione, si intende il PC (computer e/o notebook) ma anche l'ambiente dove lavoriamo, dando
Particolare importanza alla scrivania su cui depositiamo i documenti e le cartelline delle pratiche.

Focalizziamo prima l'attenzione a sull'argomento informatico

Misure di sicurezza

La protezione dagli attacchi informatici viene ottenuta agendo a due livelli principali:

- sicurezza fisica;
- sicurezza logica.

Per alcuni esiste anche il livello "organizzativo" costituito da procedure, politiche, autorità e responsabilità, obiettivi e sorveglianza.

Sicurezza passiva (sicurezza fisica)

Per *sicurezza passiva* normalmente si intendono le tecniche e gli strumenti di tipo difensivo, ossia il complesso di soluzioni tecnico-pratiche il cui obiettivo è quello di impedire che utenti non autorizzati possano accedere a risorse, sistemi, impianti, dispositivi, apparati, informazioni e dati di natura riservata.

Il concetto di sicurezza passiva pertanto è molto generale:
ad esempio, per l'accesso fisico a locali protetti, l'utilizzo di porte di accesso blindate, congiuntamente all'impiego di sistemi di allarme e sorveglianza, sono da considerarsi componenti di sicurezza passiva.

Innanzitutto a livello fisico e materiale, ponendo i server ed i sistemi di backup in luoghi il più possibile sicuri.

Spesso il fatto di adottare le tecniche più sofisticate genera un falso senso di sicurezza che può portare a trascurare quelle semplici.

Sicurezza attiva (sicurezza logica)

Per *sicurezza attiva* si intendono le tecniche e gli strumenti mediante i quali le informazioni e i dati (nonché le applicazioni) di natura riservata sono resi sicuri, proteggendo gli stessi sia dalla possibilità che un utente non autorizzato possa accedervi (confidenzialità), sia dalla possibilità che un utente non autorizzato possa modificarli (integrità).

In questa categoria rientrano sia strumenti hardware che software.

Questo livello è normalmente logico e prevede l'autenticazione e l'autorizzazione di un'entità che rappresenta l'utente nel sistema. Le operazioni effettuate dall'utente durante il processo di autenticazione sono tracciate in file di log. Questo processo di tracciamento delle attività è detto accountability. A esso si associa la successiva fase di audit. A volte viene usato il termine *audit* per entrambe le fasi.

La sicurezza passiva e quella attiva sono tra loro complementari ed entrambe indispensabili per raggiungere il desiderato livello di sicurezza di un sistema.

Parametri di protezione

La protezione degli asset informatici è ottenuta attraverso misure di carattere tecnico e organizzativo, sia di prevenzione che di protezione, tese ad assicurare:

- l'accesso protetto e controllato ai dati, a garanzia della confidenzialità delle informazioni trattate (proprietà di *riservatezza*)
- la consistenza dei dati, intesa come completezza e correttezza degli stessi (proprietà di *integrità*)
- l'accesso ai dati nei tempi e nei luoghi previsti (proprietà di *disponibilità*).

Le proprietà di riservatezza, integrità e disponibilità dei dati costituiscono l'assunto base sul quale vengono svolte tutte le successive valutazioni di sicurezza. Tali proprietà sono in genere affiancate anche dalla proprietà di *non ripudio*, ovvero dalla possibilità di attribuire un dato a un mittente o proprietario ben identificato.

Il raggiungimento della disponibilità dipende da diversi fattori che interferiscono tra utente e sistema, quali: robustezza del software di base e applicativo, affidabilità delle apparecchiature e degli ambienti in cui essi sono collocati. Spesso dal funzionamento o meno del sistema informatico dipende anche la sicurezza dei dati in esso contenuti.

Contromisure

Le possibili tecniche di attacco sono molteplici, perciò è necessario usare contemporaneamente diverse tecniche difensive per proteggere un sistema informatico, interponendo barriere fra l'attaccante e l'obiettivo.
Il sistema informatico deve essere in grado di impedire l'alterazione diretta o indiretta delle informazioni, sia da parte di utenti non autorizzati, sia a causa di eventi accidentali; inoltre deve impedire l'accesso abusivo ai dati.
In generale non è buona norma assumere le contromisure adottate in un sistema siano sufficienti a scongiurare qualsiasi attacco.
Per far fronte a evenienze derivanti da possibili guasti o danni fisici, come sicurezza fisica o passiva molte volte si opera in un contesto di ridondanza degli apparati (es. server cluster) ovvero con sistemi distribuiti all'interno di piani di disaster prevention che, assicurando la tolleranza ai guasti (fault tolerance), garantiscano affidabilità e disponibilità, cioè il business continuity del sistema informatico e dell'azienda.

A volte si preferisce agire anche in maniera preventiva tramite piani di disaster prevention. Tra le contromisure più comuni di tipo logico sulla rete locale di un sistema e sui suoi sottosistemi troviamo:

- Sistema di autenticazione: potrebbe rivelarsi utile, in particolare nelle aziende, l'utilizzo di autenticazione sicura con un secondo elemento di autenticazione basato su un insieme di caratteri complessi.
- Gestione utenti e relativi permessi;
- Mandatory Access Control (MAC), tipologia di controllo di accesso a un sistema informatico.
- Firewall: installato e ben configurato un firewall garantisce un sistema di controllo degli accessi verificando tutto il traffico che lo attraversa. Protegge contro aggressioni provenienti dall'esterno e blocca eventuali programmi presenti sul computer che tentano di accedere a internet senza il controllo dell'utente.

3) Sicurezza dei Siti WEB

I siti e le applicazioni Web sono un elemento cardine della comunicazione aziendale; attraverso questi strumenti è possibile promuovere l'immagine aziendale o del professionista, presentare, fornire informazioni o vendere i propri prodotti e servizi.

La presenza nella rete comporta, però, l'assunzione di una chiara responsabilità:

l'adozione di specifiche misure di sicurezza per minimizzare i rischi legati ad attacchi e frodi informatiche, che possono colpire sia l'infrastruttura del sito o l'applicazione Web, così come gli utenti che ne fanno uso.

I rischi per gli utenti e per il business sono molteplici; eccone alcuni esempi:

- oscuramento del sito o dell'applicazione Web in seguito ad un attacco informatico;
- attacco informatico al sito o all'applicazione Web, finalizzato al furto delle informazioni.

BUONE PRATICHE PER LO SVILUPPO DI UN SITO O DI UN'APPLICAZIONE WEB

Valutazione dei rischi: I requisiti di sicurezza adottati devono essere commisurati alle criticità del sito, dell'applicazione Web e dei dati trattati: occorre valutare il rischio, considerando sia gli utenti dell'applicazione, sia le informazioni accessibili. Ugualmente importante è la scelta di un provider affidabile e di software sicuri.

Software aggiornati: Se si gestisce in prima persona il proprio sito Web è importante utilizzare sempre la versione più aggiornata del CMS (*Content Management System*) utilizzato; in questo modo si evita che le vulnerabilità note possano essere sfruttate da eventuali *hacker*.

Autenticazione: Utilizzare password sicure, ricordando che le credenziali di accesso devono avere una scadenza ed essere periodicamente sostituite. Le informazioni di accesso, in particolare quelle di utenti e amministratori, devono essere adeguatamente protette e non devono essere registrate su database facilmente accessibili. E' bene impostare un blocco automatico dell'accesso dopo un dato numero di tentativi falliti.

I cookie: I cookie sono utilizzati per facilitare i meccanismi di autenticazione e di navigazione: essi memorizzano una serie di informazioni utili alla navigazione (es. lingua e aspetto delle pagine Web, dati di navigazione, ecc.). Poiché i cookie sono trasmessi in chiaro, all'interno di essi non devono essere presenti dati sensibili. I cookie contenenti informazioni critiche devono essere protetti mediante crittografia.

Revisione del codice:	Il codice sorgente dei programmi informatici deve essere esaminato per verificare che non siano presenti vulnerabilità che consentano ad un *hacker* di svolgere azioni dolose (es. accessi ad informazioni critiche, frodi, etc).
Backup, Logging e Auditing:	Effettuare periodicamente copie di sicurezza (*backup*), le quali devono essere adeguatamente protette e testate. È buona norma registrare (*logging*) e verificare (*auditing*) periodicamente le seguenti attività: eventi di autenticazione e di autorizzazione, attività degli amministratori, cancellazione o modifica dei dati o dei permessi. I *log* rappresentano informazioni critiche e devono essere adeguatamente protetti contro accessi e/o modifiche non autorizzate.

4) Rischi navigazione e consultazione e-m@il

Internet è considerata il principale vettore di attacchi informatici.
Nello schema che segue sono riassunte le principali “buone pratiche” da utilizzare per minimizzare i rischi legati alla navigazione Web.

CONNESSIONI SICURE

Prima di procedere alla navigazione, assicurarsi che la connessione sia affidabile.
A tal fine:
1) impostare sul proprio router una password sicura subito, evitando di utilizzare il nome utente e la password fornite dal produttore;
2) evitare di collegarsi a reti pubbliche o prive di password, soprattutto quando internet deve essere utilizzato per operazioni che richiedono un certo grado di sicurezza (es. invio o ricezione di documenti aziendali, operazioni bancarie, ecc.).

SCELTA DEL BROWSER

Fondamentale è la scelta del browser; diverse piattaforme offrono diverse opzioni di protezione, che possono (e devono) essere attivate per aumentare la sicurezza dell'utente durante la navigazione.

AGGIORNAMENTO E CORREZIONI (Patch)

La maggior parte degli attacchi informatici sfrutta le vulnerabilità dei sistemi operativi e dei programmi installati sui dispositivi destinatari (*target*); per questo motivo occorre prestare attenzione agli aggiornamenti di sicurezza del software installato (es. sistema operativo, browser, plug-in, ecc.).

È buona norma configurare il proprio computer e, più in generale, tutti i dispositivi connessi alla rete, in modo che scarichino e installino automaticamente le correzioni di sicurezza.

REGOLE DI NAVIGAZIONE

Durante la navigazione, prestare attenzione alla pagina Web visitata.
In tal senso verificare che: nella barra degli indirizzi, il collegamento inizi con https:// invece di http://; nella barra di stato del browser sia presente la classica icona a forma di lucchetto.
L'insieme di questi elementi indica che il sito è sicuro e utilizza sistemi di cifratura.
Nell'utilizzare i *Social Network* è buona norma limitare la visione delle informazioni personali alle sole persone con cui si desidera condividerle, prestando attenzione ai contenuti pubblicati.
Nel caso in cui dovessero apparire pop-up inattesi (es. segnalazioni della presenza di virus sul computer), la prima regola è **evitare di aprire il link e non autorizzare eventuali download**.
Ove possibile è bene utilizzare account con limitazioni (es. divieto di modifica delle impostazioni di sistema o di installare programmi); in questo modo, un eventuale *malware* capace di sfruttare le vulnerabilità del browser utilizzato non sarebbe in grado di infettare il vostro dispositivo.

PASSWORD SICURE

Ogni account deve essere protetto mediante chiavi di accesso sicure e difficili da dedurre.

È bene rispettare le seguenti buone norme per la scelta delle proprie password:

1. evitare di utilizzare nomi di persone o date di nascita;
2. utilizzare nomi di fantasia non presenti in dizionari: in questo modo sarebbe particolarmente complicato utilizzare “attacchi a dizionario” per violare il sistema;
3. non utilizzare password contenenti caratteri sequenziali o ripetuti;
4. la chiave d’accesso deve essere sufficientemente lunga (9 caratteri);
5. utilizzare combinazioni contenenti caratteri normali, speciali, maiuscole e numeri;
6. cambiare le proprie password a intervalli regolari (almeno ogni 3 mesi), evitando di scegliere chiavi d’accesso simili a quelle utilizzate in precedenza (3 versioni);

7. scegliere password facilmente memorizzabili, evitando di scriverle;
8. non usare risposte eccessivamente semplici o facili da individuare nelle opzioni "Domanda segreta".

-- Una soluzione alternativa alle password tradizionali è l'utilizzo di una frase di accesso (*passphrase*) composta da un numero elevato di caratteri molto meno individuabile rispetto ad una password.
I criteri per la scelta di una frase d'accesso robusta sono i seguenti:
lunghezza sufficiente a rendere la frase di difficile individuazione (almeno 20-30 caratteri);
non utilizzare parole o frasi reperibili in un dizionario, oppure celebri;
utilizzare combinazioni contenenti caratteri normali, speciali, maiuscole e numeri;
scegliere frasi di accesso facilmente memorizzabili, evitando di scriverle;
evitare di "salvare" le password sul dispositivo utilizzato.

ACCESSO A SITI INDESIDERATI

In un contesto aziendale può essere necessario impedire agli utenti di accedere a siti Internet non adeguati, dai contenuti offensivi o che potrebbero mettere a repentaglio la sicurezza e la reputazione aziendale; ciò è possibile utilizzando un software per il filtraggio del Web o configurando il proprio browser in modo da permettere l'accesso ai soli siti sicuri, impedendo l'ingresso in quelli classificati come "sconvenienti"

FIREWALL E ANTIMALWARE

Prima di procedere con la navigazione, è bene assicurarsi che sul dispositivo sia installato e attivo un software *anti-malware* in grado di rilevare e disabilitare eventuali programmi dannosi contenuti in email o siti Web non sicuri. I software di sicurezza dovrebbero essere installati come primi programmi in esecuzione e utilizzati per effettuare una scansione completa del sistema con cadenza almeno settimanale.

Occorre utilizzare un *firewall* in grado di proteggere le informazioni critiche (aziendali o personali) e impedire eventuali scambi di dati non autorizzati.

Tutte le applicazioni citate in precedenza devono essere mantenute attive e aggiornate.

GESTIONE DELLA POSTA ELETTRONICA E MISURE DI SICUREZZA

FORMAZIONE E SENSIBILIZZAZIONE DEI DIPENDENTI

La formazione e la sensibilizzazione dei dipendenti è fondamentale per gestire "in sicurezza" la posta elettronica; è necessario coinvolgere i dipendenti per aumentare la loro consapevolezza sui rischi di compromissione delle informazioni aziendali e personali.

MISURE ORGANIZZATIVE

- Normare gli utilizzi (es. divieto di uso privato dell'email poiché la promiscuità avvantaggia i *malware*).
- Formare ed informare circa le responsabilità e le regole da rispettare e le particolarità aziendali.
- Chiarire la perseguibilità individuale in caso di danni dolosi o colposi.
- Assicurare la corretta conformità della gestione delle informazioni distribuite via mail secondo le norme e gli usi anche internazionali (ad esempio, in Germania, la signature DEVE per legge informare su chi è il CEO della società scrivente al momento della spedizione).
- Normare le posizioni aziendali che possono "firmare" mail impegnative.
- Assicurare la conoscenza delle leggi e delle politiche in vigore tramite formazione aziendale.
- Conservare la posta elettronica per DIECI anni, come la normale corrispondenza, e possibilmente avere modo di smascherare le cancellazioni, dolose o colpose, di messaggi, anche a distanza di tempo.
- Decidere tra casella di posta elettronica (*mailbox*) con indirizzi di ufficio o personali (quelli personali meritano riflessioni aggiuntive).

MISURE "MINIME" DI SICUREZZA

Proteggere la posta elettronica da usi impropri con tutti i sistemi disponibili e obbligare al cambiamento frequente delle password.

- Avere copie di sicurezza (backup) frequenti: il *ransomware* passa dalla posta ma i danni li fa a tutto il sistema e non solo al dispositivo colpito.
- Utilizzare *firewall* e software di *mail gateway* adeguati per proteggere il proprio dispositivo da collegamenti non sicuri, virus e altre tipologie di attacco.
- Aggiornare puntualmente tutti i sistemi coinvolti.

5) Backup ben strutturato

Backup può essere tradotto in **copia di sicurezza** o, meglio, **copia di riserva**. Talora si incontra la dicitura "salvataggio" che però si riferisce propriamente alla semplice copia di file o cartelle in un'altra unità e che quindi non è un vero backup, in quanto non utilizza un procedimento attraverso un sistema dedicato.
L'attività di backup è un aspetto fondamentale della gestione di un computer: in caso di guasti, manomissioni, furti, smarrimenti, attacchi da parte di malware, ecc., ci si assicura che esista una copia dei dati, assicurando quindi una ridondanza logico/fisica dei dati.
Se si dispone di un software dedicato o incluso nel proprio sistema operativo l'esecuzione del backup può essere manuale, ossia lanciata dall'utente quando necessita, oppure impostata in maniera automatica: in questo secondo caso è l'applicazione che con una periodicità stabilita (per esempio una volta al giorno o alla settimana) fa partire il processo. Inoltre si possono stabilire altre particolarità avanzate se rese disponibili dal software utilizzato: selezione delle cartelle/file o dei volumi, tipo di file esclusi, e molte altre.

Nelle aziende, il tipo di backup e la relativa periodicità sono solitamente regolati da una procedura aziendale soggetta a verifica periodica e ad altre procedure che comportano un intervento manuale.
Il responsabile della sicurezza è tenuto ad annotare i controlli periodici e gli interventi sui sistemi. I supporti su cui viene effettuato il backup normalmente devono essere di tipo e marca approvati nella procedura ed è necessario che siano periodicamente verificati e sostituiti. Devono inoltre essere conservati in accordo con le politiche di sicurezza aziendale, e legate alla privacy.

Il cosiddetto **piano di backup** programmato consiste nella definizione di cosa salvare (dischi, database, cartelle, utenti, macchine, volumi, ecc.), frequenza, ora di avvio, supporto e percorso di archiviazione, tipo di backup (completo, differenziale, incrementale), modalità di compressione, tipo di log e messaggistica da esporre, tipo di verifica integrità, e molte altre opzioni a seconda della complessità del sistema.

È buona norma eseguire periodiche operazioni di backup anche nei personal computer, operazioni che di solito vengono eseguite dall'utilizzatore del computer stesso che copierà i dati importanti su supporti ottici o magnetici (CD-R, CD riscrivibili, DVD-R, DVD riscrivibili, Digital Audio Tape, cartucce a nastro).
Inoltre si utilizzano hard disk portatili con collegamento esterno USB, le chiavette USB (stick-USB) nonché le memorie flash.

Anche il Tablet e lo smartphone sono diventati importanti strumenti per i lavoratori perché contengono dati fondamentali come la rubrica telefonica e il calendario degli appuntamenti e la posta elettronica, è pertanto diventata buona norma estendere il backup anche a questi strumenti.
Diversi nuovi servizi su internet permettono infine di eseguire il backup degli account e dei dati degli utenti di social network.

Il disaster recovery

Nel caso di un disastro i semplici dati contenuti nel backup non saranno sufficienti al recupero completo delle funzionalità e dei servizi in quanto sono necessari fisicamente dei sistemi informatici (se i sistemi originali in uso sono danneggiati o distrutti) su cui ripristinare i dati e le configurazioni.

Alcune organizzazioni hanno i propri centri di recupero dati, che sono preparati per questo scenario, mentre altre organizzazioni scelgono di utilizzare un centro di recupero di terze parti questo perché un sito disaster recovery è un investimento enorme, generalmente si tende a trasferire i dati periodicamente tra la sede dell'organizzazione e il sito di disaster recovery.

Un modo più rapido sarebbe quello di effettuare il mirroring del disco a distanza, che mantiene i dati del sito il più vicino possibile a quelli effettivamente in uso.

DANNI DERIVANTI DAL FURTO E/O DALLA PERDITÀ DI DATI AZIENDALI CRITICI

PROPRIETÀ INTELLETTUALE

È uno dei danni più insidiosi e più difficili da valutare:

- in primo luogo, non bisogna confondere i costi di ricerca e sviluppo con le perdite dovute a un furto di proprietà intellettuale;
- i n secondo luogo il valore stesso della proprietà intellettuale (soprattutto quando è ancora a livello di ideazione e progetto) è di complessa determinazione;
- in terzo luogo perché, sia a livello di Stato sia a livello di singola azienda, la consapevolezza del furto avviene quasi sempre in un lasso temporale successivo al momento in cui è realmente accaduto.

Sarà difficile avere la certezza dell'entità del danno subito; per esempio, nel caso di un progetto, l'entità del danno dipenderà dal punto in cui si trovava il progetto quando il furto è stato effettuato.

FURTO DI INFORMAZIONI DI BUSINESS E MANIPOLAZIONE DEL MERCATO

il furto di informazioni di business rappresenta la terza fonte di guadagno per il crimine informatico. Tra i più perpetrati c'è il furto di informazioni relative ai clienti dell'azienda quali, ad esempio, il tipo e il numero di ordini effettuati, le modalità e i termini di pagamento.

PERDITA DI BUSINESS

Un attacco informatico può impattare la realizzazione immediata di un affare e aumenta il rischio di allontanare per sempre i clienti. Pensiamo, ad esempio, a un sito di commercio elettronico che subisce un attacco; in questo caso l'azienda non può vendere i propri prodotti/servizi per il periodo in cui il sito non funziona; la fiducia dei clienti verso tale sito viene impattata ed è probabile che questi si rivolgano ad altri attori di mercato per effettuare i loro acquisti.

COSTI DI NOTIFICA

Al costo per la notifica delle violazioni subite, sia ai soggetti che ne sono stati impattati che alle autorità governative competenti (si considerino le spese in call center, comunicazione, eventuali specialisti ingaggiati ad hoc ecc.), bisogna aggiungere le risorse finanziarie e umane necessarie per le azioni da porre in essere in risposta all'incidente di sicurezza subito.

COSTI PER LA PERDITA DI PRODUTTIVITÀ

C'è il costo per la perdita di produttività dei dipendenti interni che vengono distolti o interrotti dalle loro normali mansioni.

IMPLICAZIONI GIURIDICHE

Ci sono i costi per le eventuali cause legali, soprattutto se la violazione ha riguardato il furto di informazioni riservate dei clienti.

SANZIONI NORMATIVE

Bisogna considerare eventuali costi per le sanzioni normative soprattutto in quei settori che trattano dati sensibili e che sono soggetti a regole di protezione stringenti (per es. informazioni sui pagamenti o sullo stato di salute dei propri dipendenti/clienti)

SOLUZIONI POST ATTACCO

Infine si avranno costi derivanti dai nuovi requisiti di sicurezza e di audit per proteggere l'azienda nel rispetto delle disposizioni che regolamentano la protezione dei dati, quali ad esempio l'adozione di processi, procedure e strumenti tecnologici specifici.

BRAND REPUTATION E AWARNESS

E per ultimo ci sarà la ricostruzione della reputazione del marchio (*brand reputation*) e della sua notorietà (*brand awarness*), per riparare al danno d'immagine subito e per riconquistare la fiducia del mercato.

General Data Protection Regulation “G.D.P.R.”
Regolamento Europeo 206/679

Accountability e Compliance dello Studio Notarile
Controlli di Sicurezza

THE END

Relatore : Luigi De Paola – MCP Microsoft