MAST
SOLUTION TECHNOLOGY

WhatsApp
3356694060

MAST di Walter Solati
Via Pertini 9 - 20090 Settala (MI)
Cod.Fis.: SLTWTR65P27F205Z
P.Iva 09210860962 - REA MI 2075970
info@mast.technology - Tel +39 02.95307344

GDPR: la sicurezza informatica nella formazione

consigli per titolari del trattamento

La formazione è una misura organizzativa necessaria al raggiungimento della conformità al GDPR, ma il Regolamento non fornisce alcune indicazione su come farla

Della **formazione** come **misura organizzativa necessaria al raggiungimento e mantenimento della conformità al Regolamento UE 679/16** si è iniziato a discutere relativamente da poco, nonostante essa sia stata individuata da subito come uno dei capisaldi del nuovo corso generato dal GDPR (anche perché implicitamente richiesta dall'art. 32, c. 4, e richiamata dall'art. 39, c. 1, lett. b).

La questione che gli addetti ai lavori si stanno trovando ad affrontare, però, è l'assoluta mancanza di direttive, o almeno linee guida, riguardo ai contenuti di questa formazione. In realtà, non c'è nemmeno tanto da stupirsi, visto che come tutte le misure di sicurezza, **è responsabilità del titolare/responsabile dei trattamenti stabilire le sue particolari necessità**.

Tuttavia, è altrettanto vero che alcune considerazioni di carattere generale, che valgano come aiuto a chi deve preoccuparsi di "progettare" la formazione, si possono fare. Già altri interventi hanno iniziato ad affrontare la parte relativa alla formazione riguardante direttamente la normativa; ed è anche abbastanza chiaro che anche la formazione riguardante i processi del "sistema di gestione privacy", che la conformità di fatto richiede, sia opportuna. Ciò che si nota, a parte qualche accenno qua e là, è invece l'assenza della **formazione in tema di sicurezza informatica**.

La sicurezza informatica nella formazione GDPR: obiettivi formativi

Quando si parla di sicurezza informatica, o cyber security, troppo spesso ci si concentra sugli attacchi provenienti dall'esterno del perimetro che si sta considerando, ad opera dei cosiddetti hacker.

Al contrario, vengono altrettanto spesso ignorate le **minacce interne**, che sono dovute per lo più al fattore umano: ossia i comportamenti sbagliati degli stessi utilizzatori delle risorse informatiche a disposizione, dettati per lo più dalla mancanza di una cultura informatica di base. In questo senso, **lo scopo ultimo della formazione sulla sicurezza informatica deve essere quello di fornire le conoscenze minime** per implementare quello che con una efficace espressione è definito il firewall umano. In sintesi, si tratta di fare in modo che gli utilizzatori siano in grado di:

- riconoscere le **situazioni pericolose e/o non nominali**;
- comportarsi correttamente al loro verificarsi;
- prevenirne gli effetti.

WhatsApp
3356694060

MAST di Walter Solati
Via Pertini 9 - 20090 Settala (MI)
Cod.Fis.: SLTWTR65P27F205Z
P.Iva 09210860962 - REA MI 2075970
info@mast.technology - Tel +39 02.95307344

Modalità formative per la formazione GDPR

Come conseguire l'ambizioso obiettivo? Al di là delle usuali metodologie pedagogiche, assolutamente necessarie, ciò che è necessario è evitare trattazioni teoriche ed astratte e al contrario calarsi nel concreto, utilizzando casi esemplari, il più possibile di vita vissuta, allo scopo di evidenziare le conseguenze di **errori, problemi tecnici e false sicurezze**, e fornendo immediatamente dopo indicazioni su come affrontarle.

Nel far ciò, bisogna evitare di concentrarsi solo sulla salvaguardia della **riservatezza**, come spesso si è portati a fare: al contrario, è necessario affrontare anche, e forse soprattutto, i problemi legati a **integrità** e **disponibilità**. La **resilienza** dei sistemi e dei servizi, anch'essa citata nell'art. 32 (c. 1, lett. a), è normalmente competenza degli amministratori di sistema; tuttavia, nozioni di base potrebbero in qualche caso essere utili anche per gli operatori (dipende dall'architettura delle infrastrutture informatiche, che potrebbero demandare agli operatori alcune precauzioni che impattano sull'affidabilità).

Infine (ma spero sia una raccomandazione inutile), **l'intervento formativo deve essere adattato alla singola realtà alla quale viene proposto**. Nulla vieta comunque di avere un canovaccio standard dal quale partire e di riutilizzare parti di lezioni in contesti simili.

Una parola anche sulla questione delle figure a cui deve essere indirizzata la formazione. Banale ed ovvio: a chi serve. Ciò che nella mia esperienza non risulta né banale né ovvio è che in questa definizione non entrano solo gli operatori, cioè coloro che nella struttura organizzativa occupano i livelli più bassi; ma **devono assolutamente entrare i livelli più alti, che talvolta maneggiano maggiormente i dati** (in termini qualitativi e/o quantitativi)**, e proprio per questo hanno maggior bisogno delle competenze in esame**.

Tutto ciò premesso, analizziamo i temi che dovrebbero entrare a far parte della formazione basilare di sicurezza informatica in ambito GDPR (ma non solo). Come già detto, sta poi al formatore progettare il proprio intervento adattandolo alle reali esigenze dell'uditorio e ovviamente al tempo a disposizione.

La crittografia

La crittografia, oltre ad essere citata direttamente come possibile misura di sicurezza nell'art. 32, c. 1 del GDPR (anche se viene usato il termine *cifratura*), è alla base di molti processi di uso comune anche se spesso non in modo evidente all'utente finale; lo scopo quindi è quello di evidenziarne gli usi che capita di incontrare nelle normali attività, ma anche quello, attraverso la presentazione di quei programmi che ne rendono facile l'utilizzo, di **incentivarne l'adozione** in tutte quelle situazioni in cui è necessario mantenere la riservatezza dei dati.

MAST di Walter Solati
Via Pertini 9 - 20090 Settala (MI)
Cod.Fis.: SLTWTR65P27F205Z
P.Iva 09210860962 - REA MI 2075970
info@mast.technology - Tel +39 02.95307344

Ovviamente, nella trattazione sono da evitare la trattazione dei principi matematici, della storia ecc.; al contrario, bisogna concentrarsi sui concetti indispensabili allo scopo appena descritto:

- crittografia a chiave simmetrica (usata per mantenere privati i dati "statici");
- crittografia a chiave asimmetrica (usata per mantenere private le comunicazioni);
- firma digitale (usata come alternativa alla firma grafica);
- certificati e CA (usati per la verifica dell'identificazione)

Alla parte teorica va assolutamente affiancata una parte più pratica, ossia **la presentazione delle situazioni in cui si utilizzano le metodologie sopra riportate**: il riconoscimento dei siti sicuri, la verifica delle firme sui documenti, la verifica dell'identità delle controparti, la cifratura dei file, la conservazione delle chiavi e via dicendo. Né va dimenticato di proporre una riflessione sui **possibili utilizzi malevoli della crittografia**, per esempio a scopo di riscatto (virus di tipo ransomware).

La posta elettronica

Forse non tutti se ne rendono conto, ma **la stragrande maggioranza dei trasferimenti di dati (anche personali) di piccole dimensioni avviene attraverso la posta elettronica**; semplicemente perché "è comodo". D'altra parte, sicuramente tutti non si rendono conto di quanti pericoli corrono i messaggi. Non mi riferisco solo al protocollo, che è totalmente aperto a facili intercettazioni e a tecniche di sostituzione; ma soprattutto alla **modalità di conservazione**, che espone l'utilizzatore inesperto alla certezza (e non al semplice rischio) di perdita di dati, prima o poi.

In questo senso, un utente di un sistema di posta elettronica dovrebbe essere tenuto a conoscere almeno questo:

- funzionamento del protocollo e dei server SMTP;
- differenza e scelta tra POP e IMAP;
- il sistema PEC e sue differenze con il sistema standard;
- modalità di memorizzazione dei dati (messaggi, contatti) nei client;
- messaggi crittografati;
- riconoscimento di SPAM, phishing, virus.

L'ultimo (non a caso) punto merita comunque una trattazione specifica, nonostante ormai sia probabilmente una capacità abbastanza diffusa, almeno per le minacce più frequenti.

Un altro argomento correlato alla posta elettronica è quello dei sistemi alternativi per l'invio di file, in considerazione sia della maggiore sicurezza (per esempio, attraverso l'utilizzo del protocollo HTTPS), sia del fatto che i diversi server pongono limitazioni sulle dimensioni dei file che non sono note a priori.

MAST di Walter Solati
Via Pertini 9 - 20090 Settala (MI)
Cod.Fis.: SLTWTR65P27F205Z
P.Iva 09210860962 - REA MI 2075970
info@mast.technology - Tel +39 02.95307344

Il social engineering

Così come la posta elettronica, anche le tecniche di social engineering sono una minaccia spesso misconosciuta: eppure, proprio queste tecniche sono quelle utilizzate per **carpire informazioni**, che possono essere utili di per sé stesse, oppure propedeutiche ad attacchi mirati attraverso altre tecniche di hacking più "tradizionali".

In questo caso particolare, la **consapevolezza degli utenti è l'unica arma effettiva**:

- bisogna fornire in primis un elenco, il più esaustivo possibile, delle informazioni critiche che devono essere assolutamente tenute riservate (e verso chi);
- inoltre, è bene presentare una buona dose di esempi, meglio se poi corredata di esercitazioni pratiche, di come queste tecniche vengono messe in pratica.

L'obiettivo finale è inculcare la **cultura del sospetto**, cioè l'abitudine a dubitare di tutto e tutti come atteggiamento predefinito, che si concretizza poi nel compiere i passi necessari di **verifica**, più o meno approfondita a seconda del contesto (tipologia di informazioni richieste, metodo di contatto, grado di conoscenza della controparte ecc.). Tutto ciò si dovrebbe affiancare o integrare (quando applicabile) alla **formazione specifica sulle politiche adottate dall'organizzazione in relazione alla gestione e sicurezza delle informazioni**.

Gestione dei file e backup

Ad una prima lettura, questo potrebbe sembrare un argomento più adatto ad un normale corso di introduzione all'uso del computer, piuttosto che ad una trattazione relativa alla sicurezza; eppure, per coloro (e sono purtroppo molti) che si sono ritrovati ad usare un computer senza ricevere la benché minima informazione in proposito, l'ignoranza in materia genera errori comportamentali che possono portare a **perdita o corruzione di dati**. In questo senso, a differenza degli argomenti precedenti che necessitavano anche di nozioni teoriche, questo necessita più che altro di introdurre alcune linee guida, peraltro utili sempre, riguardo:

- tipi di supporti e tecnologie;
- organizzazione gerarchica (volumi, cartelle, file);
- identificazione delle tipologie di file;
- impostazione di permessi e controllo degli accessi;
- cifratura dei volumi e dei file;
- protezione dai guasti ai dischi e dalla corruzione dei filesystem.

A tutto questo, e partendo dagli ultimi punti, bisogna aggiungere una decisa trattazione della gestione delle copie dei file: obbligatoria, sotto il nome di **backup**, per proteggersi dai rischi di perdita; **ma anche pericolosa, se le copie vengono effettuate in maniera disorganica**, perdendo il controllo delle versioni dei file.

MAST di Walter Solati
Via Pertini 9 - 20090 Settala (MI)
Cod.Fis.: SLTWTR65P27F205Z
P.Iva 09210860962 - REA MI 2075970
info@mast.technology - Tel +39 02.95307344

Metodi di autenticazione

L'autenticazione è spesso il primo scoglio che un utilizzatore di strumenti informatici si trova ad affrontare, rappresentato dalla famigerata coppia username/password. Ma con il progredire dei servizi e delle minacce, i metodi di autenticazione aumentano e diventano (si spera) sempre più sicuri. Quindi è utile, al di là della usuale ma purtroppo necessaria solfa sulla robustezza delle password, spendere due parole sugli altri metodi esistenti:

- autenticazione forte;
- autenticazione a 2 fattori;
- biometria;

nonché sui **rischi relativi ai furti d'identità**. L'obiettivo deve essere quello di sensibilizzare riguardo all'importanza dell'autenticazione, che poi è l'**identificazione certa** della persona che utilizza i sistemi, e ovviamente della protezione dei relativi dati.

Servizi remoti e cloud

Questa tematica non significa tanto sindacare quanto tali servizi abbiano implementate le necessarie misure di sicurezza, quanto deve mettere in chiaro **quali rischi si corrono se non si usano correttamente**. Spesso, infatti, la mediazione delle interfacce utente (browser o all'interno degli strumenti del sistema operativo) rendono l'interazione quasi indistinguibile da quella tipica dei programmi locali al dispositivo in uso, col risultato che **l'utente non si rende conto di dove si trovano effettivamente i dati**; per cui, in caso di malfunzionamento del collegamento di rete, si trova a non avere a disposizione i dati di cui necessita, o anche ad averne a disposizione di **obsoleti**.

In definitiva, è necessario che l'utente sia in grado di riconoscere se un servizio è locale o no, sappia come riconoscere l'assenza del collegamento o il malfunzionamento del servizio stesso, abbia la possibilità di ovviarvi con le copie locali dei dati (eventualmente tramite l'impostazione preventiva della disponibilità offline) e soprattutto sappia come **sincronizzare le diverse versioni dei file** dopo un malfunzionamento.

Dispositivi mobili e reti Wi-Fi

Due sono le questioni da rimarcare: le **conseguenze del furto o smarrimento di un dispositivo mobile**, cioè la facilità di accesso ai dati memorizzati, a meno dell'utilizzo della crittografia, e la pericolosità dell'utilizzo di reti Wi-Fi pubbliche, a causa del fatto che ci si trova di fatto in **potenziale connessione con molti altri dispositivi di cui non conosciamo nulla** e che potrebbero essere fonti di minacce (virus, attacchi generalizzati, cracking della password di rete).