Seminario organizzato da
Ordine Ingegneri di Forlì-Cesena

REGOLAMENTO EUROPEO 2016/679 (GDPR): QUALI IMPATTI SULL'ATTIVITÀ DEI LIBERI PROFESSIONISTI

Cesena, 16 maggio 2018

Ing. Massimo Piceni

Il punto di vista dei sistemi IT

- **I sistemi hardware e software: cosa verificare per essere conformi**
- **La protezione dei dati digitali: dai diritti di accesso alla crittografia**
- **La prevenzione dai rischi di perdita di dati, all'epoca dei cryptolocker**
- **La difesa dei confini: i rischi che possono venire da Internet**
- **La posta elettronica: come usarla responsabilmente**
- **Il Cloud: come e quando possiamo utilizzarlo per contenere dati personali**

I sistemi hardware e software

- **Domanda chiave: quali sistemi hardware e software devono sottostare ai dettami del GDPR ?**
- **Risposta: quelli che contengono, o possono contenere dati, e tutti i sistemi atti a trattarli.**
- **Casi lampanti:**
  - **Il Server che ospita il gestionale è sicuramente da considerare**
  - **Il Server di posta elettronica è sicuramente da considerare**
- **Casi meno evidenti:**
  - **Un computer che controlla un macchinario industriale ?**
  - **Il Server che ospita il sito web istituzionale ?**
  - **Il firewall aziendale ?**

I sistemi hardware e software

- **E il software ?**
- **Sicuramente:**
  - **Gestionale**
  - **Server e client di posta**
  - **Antivirus, antispam e simili (sistemi di protezione attiva dei dati)**
  - **Sistemi di backup (sistemi di protezione attiva dei dati)**
- **Meno evidente:**
  - **Office o similare (lo uso per trattare dati, soprattutto Excel)**
  - **Sistemi operativi server e client (anche se non direttamente, ospitano i dati)**
- **Non si direbbe, ma….:**
  - **Software di compressione (es. WinZIP, WinRAR, ecc.)**
  - **Smartphone e tablet**

I sistemi hardware e software

- **Primo passo: identificazione**
  - **Redigere un elenco dei sistemi hardware interessati e del relativo software installato (elencare anche le versioni)**
  - **Porre particolare attenzione al fatto che i sistemi (soprattutto software) siano sottoposti a manutenzione da parte del produttore o di altri**
  - **Fare attenzione agli aggiornamenti, sia dei sistemi di protezione attiva (antivirus, firewall, backup, ecc.), sia dei sistemi di gestione (sistema operativo e applicativi)**
- **Secondo passo: gestione**
  - **Identificare il modo in cui i sistemi vengono usati per il trattamento dei dati**
  - **Associare ai sistemi i relativi responsabili**
  - **Analizzare i rischi connessi ai sistemi hardware e software**

I sistemi hardware e software

- **Terzo passo: protezione**
  - **Verificare che i sistemi di protezione attiva (antivirus, firewall, backup, ecc.) siano adeguati a rispondere ai rischi individuati**
  - **Definire delle procedure di verifica continua dell'adeguatezza dei sistemi**
  - **Definire delle procedure per individuare eventuali problemi potenziali o in atto**
  - **Definire delle procedure di risposta ai data breach**
- **Quarto passo: documentazione.**
  - **Documentare tutto ciò che si fa per la protezione dei dati, aiuta a**
    - **Una eventuale futura difesa**
    - **Individuare le vulnerabilità**
    - **Responsabilizzare le persone che utilizzano i sistemi**

La protezione dei dati digitali

- **Per rubarmi/distruggermi un oggetto fisico devono venire nella mia azienda. Per rubarmi/distruggermi un dato digitale, non è strettamente necessario**
- **La sola protezione dei sistemi hardware e software non è sufficiente**
- **La protezione assume 2 aspetti:**
  - **Protezione fisica (contro il furto/distruzione di dispositivi che contengono dati)**
  - **Protezione logica (contro il furto/distruzione digitale dei dati)**

La protezione dei dati digitali

- **Protezione fisica:**
  - **Valgono tutti i sistemi di protezione per altri oggetti fisici (antifurto, vigilanza, videosorveglianza, ecc.)**
  - **Principio fondamentale: limitare gli accessi fisici a chi ne ha realmente necessità**
- **La sottrazione di un dispositivo contenente dati, implica più aspetti di rischio sui dati:**
  - **Indisponibilità dei dati**
  - **Perdita dei dati**
  - **Furto dei dati**
  - **Utilizzo non consentito dei dati (anche nei confronti di soggetti terzi)**

La protezione dei dati digitali

- **Protezione logica. Ha una doppia valenza:**
  - **Può tutelare i dati contro accessi non autorizzati, diversi dall'intrusione fisica**
  - **Può tutelare i dati anche in caso di sottrazione del dispositivo che li contiene**
- **Principio fondamentale: limitare gli accessi logici ai dati, a chi ne ha realmente necessità (duale della protezione fisica)**
- **Due tipici metodi di limitazione degli accessi ai dati:**
  - **Diritti di accesso: identifico, informaticamente, ogni utente, e concedo gli accessi in funzione del ruolo di ciascuno. L'ideale è concedere il minimo livello di accesso possibile, nel rispetto delle esigenze lavorative.**
  - **Cifratura dei dati: i dati sono codificati ed accessibili solo a chi dispone della chiave di decodifica. È un concetto diverso dalla condivisione con password. La cifratura avviene sul dispositivo fisico che contiene i dati.**

La protezione dei dati digitali

- **Diritti di accesso:**
  - **Vantaggi: molto semplice da utilizzare; gestibile a livello di amministratore di rete (se cambiano i ruoli, cambio i diritti senza dover fare altro); posso dare livelli di accesso diversi ad utenti diversi; il cambio della chiave di accesso (password, in questo caso) è demandato all'utente**
  - **Svantaggi: non protegge i dati in caso di accesso fisico al dispositivo che li contiene; è vulnerabile in caso di comportamenti errati dell'utente (es. password troppo semplice o condivisa)**
- **Cifratura dei dati:**
  - **Vantaggi: è inviolabile anche in caso di accesso fisico al dispositivo; la protezione è affidata ad una chiave molto complessa**
  - **Svantaggi: più complesso da implementare; chi possiede la chiave può fare tutto (livelli di accesso non definibili); se devo cambiare la chiave, devo ricifrare i dati e ridare la nuova chiave agli utenti; se perdo la chiave, nemmeno l'amministratore di sistema può recuperare i dati**

La protezione dei dati digitali

- **Diritti di accesso e cifratura dei dati possono essere combinati**
- **I diritti di accesso vanno sostanzialmente sempre implementati**
- **I diritti di accesso devono essere gestiti centralmente (tipicamente Active Directory)**
- **La complessità delle password, la loro scadenza e l'impossibilità di riutilizzarle vanno adeguatamente gestite**
- **La cifratura dei dati va implementata se necessaria a mitigare dei rischi individuati**

La prevenzione dai rischi di perdita di dati

- **Falso mito: «il rischio più grande per i miei dati sono i guasti dei dispositivi»**
- **Il rischio principale è diventato il malware informatico (soprattutto cryptolocker). Questo fenomeno è temporaneamente rallentato, ma si attende un ritorno prepotente. Lo spettro delle sanzioni del GDPR potrebbe incentivare gli attacchi di tipo ramsonware**
- **Non esistono misure informatiche, efficaci al 100% per prevenire questo tipo di attacchi**
- **L'assicurazione dei dati contro questo fenomeno, si chiama backup. Attenzione a proteggere adeguatamente le copie**

La prevenzione dai rischi di perdita di dati

- **Falso mito: «I virus/malware posso prenderli solo se uso un PC con Windows»**
- **La maggior parte dei malware è, oggi, multipiattaforma. I malware fatti per rubare dati, spesso, si inseriscono nel browser, a prescindere dal sistema operativo.**
- **I dispositivi, oggi, più a rischio, sono i «non computer», connessi in rete. In particolare i cosiddetti dispositivi IoT**
- **Anche se il dispositivo attaccato non contiene dati, può diventare un cavallo di troia per attaccare, più facilmente, i dispositivi che contengono i dati**

La prevenzione dai rischi di perdita di dati

- **Falso mito: «sono un professionista, sono piccolo, a chi potrà mai interessare attaccarmi?»**
- **Statisticamente, attacchi come quelli di tipo ramsonware, colpiscono maggiormente le piccole realtà**
- **È più probabile che il «piccolo» abbia sistemi di difesa meno sofisticati**
- **È più probabile che il «piccolo» sia carente dal punto di vista dei backup**
- **È più probabile che il «piccolo» paghi il riscatto, magari anche poche centinaia di euro, ma comunque interessanti per l'hacker**

La prevenzione dai rischi di perdita di dati

- **Falso mito: «gli attacchi hacker al mio sistema informativo, avvengono perché qualcuno 'buca' il mio firewall»**
- **Nella quasi totalità dei casi, è l'utente a 'fare entrare' l'hacker, solitamente aprendo un messaggio di posta elettronica**
- **Esistono metodi di intrusione, apparentemente insospettabili, come stampare un PDF**
- **Esistono metodi di furto di dati e credenziali , apparentemente insospettabili, come usare un WiFi free**
- **La prima forma di prevenzione dei rischi informatici è la capacità dell'utente di evitarli => formazione**

La prevenzione dai rischi di perdita di dati

- **Tipici comportamenti pericolosi degli utenti:**
  - **Apertura indiscriminata di messaggi di posta elettronica o siti web**
  - **Utilizzo di password troppo semplici o non cambiate regolarmente**
  - **Scrittura delle password in file di testo o Word/Excel**
  - **Utilizzo della stessa password per più servizi distinti**
  - **Condivisione di password con altre persone**
  - **Salvataggio delle password nel browser**
  - **Mancata sostituzione delle password di default nei dispositivi (NAS, firewall, ecc.)**
  - **Scaricamento indiscriminato di software gratuito**
  - **Installazione di software senza leggere attentamente le indicazioni**
  - **Concessione di diritti di accesso superiori al necessario**
  - **Mancato aggiornamento dei sistemi e degli antivirus**

La difesa dei confini

- **Per evitare azioni indesiderate sui miei dati, devo impedire che malintenzionati si «avvicinino» ad essi (fisicamente o logicamente)**
- **Dal punto di vista logico, il tipico difensore di confine è il firewall**
- **È sostanzialmente obbligatorio (la mancanza non sarebbe motivabile, né difendibile)**
- **Per le realtà più piccole, la combinazione firewall del router + Windows firewall, è un minimo di accettabilità, ma non è ottimale**
- **Sarebbe preferibile un firewall attivo, con abbonamento ai servizi di protezione ed anti intrusione**

La difesa dei confini

- **I log del firewall andrebbero analizzati per intercettare, preventivamente, le minacce (o almeno prima che facciano grossi danni)**
- **L'analisi dei log è attività complessa, spesso fuori della portata di un studio o di una piccola azienda**
- **Il consiglio generale è quello di «chiudere» il più possibile e, preferibilmente, evitare di pubblicare all'esterno servizi di qualsiasi tipo (es. condivisione file del NAS)**
- **Se necessario accedere alle risorse dall'esterno, privilegare la VPN (IpSec o OpenVPN, evitare PPTP o L2TP)**
- **Evitare le VPN in uscita o altri sistemi di anonimizzazione**

La posta elettronica

- **La posta elettronica è, probabilmente, l'applicazione Internet più usata dalle aziende**
- **La posta elettronica è, probabilmente, l'applicazione Internet più insicura. Sotto diversi punti di vista:**
  - **Non c'è garanzia di consegna**
  - **Non c'è garanzia che il mittente sia chi dice di essere**
  - **Non c'è garanzia che il contenuto sia (solo) ciò che si vede**
  - **Non c'è garanzia che il messaggio arrivi proprio al destinatario a cui l'ho spedito**
  - **Non c'è garanzia che altre persone non possano leggere i messaggi che invio o ricevo**

La posta elettronica

- **Falso mito: «il messaggio viene da un indirizzo che avevo considerato attendibile, mi posso fidare»**
- **Far credere che un messaggio arrivi da un indirizzo diverso è una banalità alla portata di qualsiasi tecnico informatico**
- **Falso mito: «conosco bene il sito, posso clickare tranquillamente sul collegamento»**
- **È banale anche mostrare un sito e far puntare il collegamento ad un altro**
- **Falso mito: «ho un antispam costosissimo, se non me lo ha segnalato, il messaggio è sicuro»**

  In media, 1 messaggio malware su 50 passa qualsiasi antispam

La posta elettronica

- **Nel corso degli anni sono stati ideati sistemi per rendere la posta elettronica più sicura, ma nessuno ha mai avuto larga diffusione (tranne la PEC, ma è solo italiana)**
- **La PEC risolve molte delle insicurezze, ma non è infallibile**
- **Falso mito: «il messaggio mi è arrivato via PEC, quindi è affidabile»**
- **La PEC garantisce solo l'attendibilità degli indirizzi e l'avvenuta consegna, ma non garantisce né sui contenuti, né sul fatto che l'indirizzo appartenga ad una certa azienda/persona, e nemmeno la rintracciabilità fisica del mittente**

Il Cloud

- **Il Cloud è una tecnologia che è entrata prepotentemente nelle nostre vite e nelle nostra aziende**
- **In particolare, i Cloud drive, si offrono come la panacea di tutti i mali dei dati digitali**
- **In effetti il Cloud protegge benissimo dalla perdita dei dati e, quasi altrettanto bene, dalla indisponibilità**
- **Quasi sempre è anche più resistente agli attacchi informatici, rispetto ad un dispositivo fisico in azienda**
- **Nessun problema, dunque per la privacy…**

RISPOSTA SBAGLIATA

Il Cloud

- **Falso mito: «non metto i dati in Cloud, perché sono meno sicuri»**
- **In generale, i sistemi Cloud «seri» sono più sicuri, perché gestiti da grandi aziende con molte risorse dedicate alla security**
- **Falso mito: «con le connessioni Internet italiane, se metto i dati in Cloud, gli accessi diventeranno lentissimi»**
- **Quasi tutti i sistemi Cloud hanno dei meccanismi che replicano i dati nel disco locale. Le prestazioni non cambiano**
- **Falso mito: «non uso la posta in Cloud, non è sicura»**
- **La posta elettronica è insicura di suo, e «gira» comunque su Internet. Metterla in Cloud non peggiora la situazione**

Il Cloud

- **Falso mito: «un servizio in Cloud mi costa molto di più, rispetto allo stesso servizio in locale»**
- **Se si confrontano servizi con identiche caratteristiche tecniche e funzionali, questo non è, praticamente, mai vero**
- **Nei costi dei servizi in locale, non consideriamo, quasi mai, i costi di gestione (manutenzione, backup, risoluzione di problemi, energia elettrica, ecc.)**
- **Spesso, non teniamo conto degli aggiornamenti**
- **Quasi mai, teniamo conto delle caratteristiche «nascoste» (affidabilità, continuità di servizio, recupero automatico dei guasti, conformità, ecc.)**

Il Cloud

- C'è Cloud e Cloud…
- Cloud gratuito (ad uso consumer):
  - Mancano funzioni di sicurezza, come le versioni e la crittografia
  - Non viene dichiarato dove si trovano i datacenter. Problema critico per la privacy: se il datacenter è extra-UE, si configura l'esportazione di dati
- Cloud professionale:
  - Dichiara (o è possibile chiedere) dove sono i dati. Posso chiedere che restino in UE
  - Permette il ripristino delle versioni precedenti dei file (se ho sovrascritto dei dati per errore)
  - Permette la crittografia dei dati

Seminario organizzato da
Ordine Ingegneri di Forlì-Cesena

REGOLAMENTO EUROPEO 2016/679 (GDPR): QUALI IMPATTI SULL'ATTIVITÀ DEI LIBERI PROFESSIONISTI

Cesena, 16 maggio 2018

Ing. Massimo Piceni