UNIVERSITÀ DEGLI STUDI DI MILANO
Ufficio di Staff Sicurezza ICT

Gestione dei dati e dei dispositivi

Versione 1.0

Sommario

Premessa

Questo breve manuale definisce dei principi chiave da seguire al fine di proteggere i dati in termini di confidenzialità, integrità e disponibilità. La *confidenzialità* permette di garantire che i dati e le risorse siano preservati dal possibile utilizzo o accesso da parte di soggetti non autorizzati. L'*integrità* rappresenta la capacità di mantenere la veridicità dei dati e delle risorse, e di garantire che non siano in alcun modo modificate o cancellate, se non ad opera di soggetti autorizzati. Infine, la *disponibilità* rappresenta la possibilità di poter accedere alle risorse di cui si ha bisogno per un tempo stabilito ed in modo ininterrotto.
La sicurezza dei dati memorizzati in un dispositivo non riguarda solo intrinsecamente i dati ma anche il dispositivo, con il software in esso installato, e il comportamento dell'utente.
Nella prima parte si affronterà il problema di configurare e gestire sia il sistema operativo che i software applicativi, per minimizzare la probabilità che siano causa di una breccia nella sicurezza del dispositivo. Successivamente, verranno descritte alcune procedure da effettuare sui dati, atte a garantire la confidenzialità, integrità e reperibilità degli stessi. L'ultima parte si focalizzerà su alcune buone norme che l'utente dovrebbe seguire al fine di evitare che soggetti malevoli possano approfittare della disattenzione umana per compiere azioni illecite, come furto dei dati, veicolo di software dannoso, etc.
I temi trattati, sia in termini di numero che di approfondimento, non possono essere considerati esaustivi tenendo conto della vastità del tema trattato, ma devono essere pensati come un buon punto di partenza per mettere al sicuro i dati e il dispositivo che li contiene.
Inoltre, alcuni degli argomenti qui esposti, ove ritenuto necessario, sono stati approfonditi in documenti di natura tecnica reperibili nel portale di Ateneo.

Sicurezza del sistema dal punto di vista software

I. Sistema operativo con licenza valida, aggiornato e aggiornabile

La prima operazione da effettuare al fine di minimizzare la possibilità di incidenti di natura informatica è verificare che il software di base installato sul proprio dispositivo sia ben configurato. Solitamente i dispositivi vengono acquistati dotati di sistema operativo con licenza valida, nel caso si decidesse di cambiare sistema operativo, magari per passare ad una versione più recente, il nuovo sistema dovrà avere una valida licenza, in accordo con le norme sul diritto di autore. Installare la versione più recente di un sistema operativo significa ricevere aggiornamenti e migliorie periodiche di sicurezza fondamentali per diminuire l'esposizione del sistema stesso a vulnerabilità. Si raccomanda di aggiornare il sistema operativo tempestivamente al rilascio di una nuova patch**. Gli aggiornamenti automatici esonerano gli utenti da dover periodicamente controllare il rilascio di nuove patch da parte del produttore del software.**

II. Accounting

Al momento della configurazione dell'utenza si dovrebbe considerare il *principio del privilegio minimo*, fornendo, cioè, all'utente il minimo insieme di privilegi necessari per portare a termine le proprie attività. Solitamente esistono due categorie di tipi di utente: *Amministratore* e *utente standard*. L'account da Amministratore prevede alcuni privilegi che potrebbero compromettere la sicurezza del dispositivo, in quanto alcune operazioni potrebbero modificare la configurazione del sistema operativo. È buona norma configurare il proprio accesso *giornaliero* come utente standard per le azioni che non richiedono alti privilegi. Inoltre, se il dispositivo, contenente dati di proprietà dell'Ateneo, è un notebook, tablet o comunque appartiene alle categorie *mobile*, è bene predisporre una multiutenza, cioè prevedere che utenti diversi possono accedere al dispositivo: un account *lavoro* e uno *personale*, oppure, se necessario, creare un account per amici o familiari di tipo standard. Inoltre, i più diffusi sistemi operativi moderni prevedono l'account *guest* preimpostato che può essere utilizzato da terzi nel caso di accesso temporaneo al dispositivo.

III. Principi base per l'autenticazione

Uno dei principi fondamentali della sicurezza informatica è l'autenticazione. L'utente autenticandosi permette al sistema di verificarne l'identità. Per effettuare tale operazione solitamente si ricorre a qualcosa che si conosce, come una password;

qualcosa che si possiede, come una smartcard, o qualcosa che si "è", come l'impronta digitale. La password è la chiave di sicurezza della maggior parte dei sistemi e delle applicazioni, per cui risulta necessario che essa sia *robusta*, nel senso che sia difficile da indovinare. Buona pratica è creare delle password lunghe, almeno 12 caratteri, da cambiare con sufficiente frequenza evitando di riutilizzare a breve distanza di tempo quelle utilizzate in precedenza. Una scelta migliore per incrementare la robustezza è scegliere una *passphrase*, cioè un insieme di *parole* o di *stringhe alfanumeriche* separati da caratteri non alfabetici come numeri, spazio o caratteri speciali. La differenza tra passphrase e password è solitamente il numero di caratteri utilizzato: la prima risulta essere più lunga, solitamente 20/30 caratteri.
La sicurezza della fase di autenticazione si basa sul principio della segretezza: la password è personale e non va condivisa. Quando si digita la password, è opportuno essere sicuri che nessuno ci stia osservando.
Per poter accedere ai dispositivi è necessario o conoscere la password oppure avere a disposizione il dispositivo dopo che l'operazione di autenticazione sia avvenuta. Quindi non si deve MAI confidare la propria password e non si deve MAI lasciare incustodito il dispositivo dopo aver effettuato l'operazione di login.
Nessuno è autorizzato a chiedere la password per accedere al pc oppure ai servizi di Ateneo al telefono o per email.

IV. Utilizzare un software Antivirus

L'antivirus è un valido strumento software finalizzato a prevenire, rilevare e rendere inoffensivi malware nel dispositivo. I più recenti software antivirus, inoltre, incorporano ulteriori caratteristiche quali antimalware, webcontrol, antispyware, application control, device control, antirootkit. Risulta, perciò, fondamentale configurare il software antivirus in modo da effettuare l'aggiornamento automatico, o almeno programmarne uno giornaliero. Programmare ed eseguire una scansione periodica del proprio dispositivo. L'antivirus dovrebbe essere configurato per rilevare tutti i più conosciuti tipi di malware (come rootkit, cryptolocker e applicazioni potenzialmente sconosciute). La configurazione di **aggiornamenti automatici permette di poter avere uno strumento capace di intercettare anche i malware più recenti.**

V. Installazione di software applicativi

Il software installato deve essere sempre dotato di una licenza valida, e nel caso di software open source deve essere in possesso di licenza OSI. È vietato scaricare e installare software pirata, sia perché tale operazione è illegale sia perché **niente è gratis, questi software sono tipicamente veicoli di malware**. Prima di installare un software è necessario controllare che il dispositivo sia compatibile con le caratteristiche richieste, sia hardware, come quantità di RAM o Hard Disk, che software, come il sistema operativo o che non vi siano eventuali incompatibilità note con altri software applicativi precedentemente installati.
Per ragioni di sicurezza è opportuno installare solo software necessario e disinstallare quello non più utilizzato, disabilitare le estensioni dei software non necessarie per evitare che si trasformino in veicoli di malware (come le Macro di Office). Se il software prevede la definizione di un utente, è buona norma eliminare l'utente di default (solitamente *Admin* con password *Admin*) e creare un'utenza propria, se non necessaria di tipo non amministrativo.

VI. Utilizzare le risorse hardware e software in maniera consapevole

Solitamente quando il dispositivo appare rallentato, la prima cosa che viene in mente è la disattivazione dell'antivirus o di servizi, come il backup automatico, che l'utente ritiene superflui. Per la sicurezza dei dati, in particolare quelli personali, si sconsiglia tale prassi che, inoltre, potrebbe avere come unico risultato quello di esporre il dispositivo ai malware.
Buona norma, invece, è disinstallare le applicazioni non più in uso e fare una pulizia della memoria fisica, spostando su supporto esterno, quei dati che non sono più utilizzati. Inoltre, si raccomanda, quando si installano le applicazioni, verificare che la RAM, lo spazio disco, il sistema operativo, richiesti siano soddisfatti dal dispositivo.

VII. Firewall

La maggior parte dei sistemi operativi moderni è dotato di firewall personali, solitamente con una configurazione di default che permette un medio livello di sicurezza. Non si dovrebbero disabilitare o modificare le impostazioni di default del firewall.

Confidenzialità, integrità e disponibilità dei dati

I. Accesso controllato ai dati

Nel caso di incidente di sicurezza informatica è necessario conoscere la natura dei dati che sono stati danneggiati, distribuiti in maniera illegale o accidentalmente persi. Infatti il nuovo Regolamento Europeo sulla Protezione dei Dati (679/2016, GDPR) si occupa dei dati personali, definiti come *qualsiasi informazione riguardante una persona fisica identificata o identificabile (interessato) che identifichi o renda identificabile una persona fisiche e che possono fornire dettagli sulle sue caratteristiche, le sue abitudini, il suo stile di vita, le sue relazioni personali, il suo stato di salute, la sua situazione economica...* Particolare attenzione deve essere posta nel caso di violazione di dati genetici, biometrici e sanitari (art. 4 679/2016, GDPR).
Per cui è di fondamentale importanza conoscere la categoria dei dati oggetto dell'incidente per effettuare prontamente le azioni corrette: nel caso di dati personali che coinvolgono l'Ateneo, in particolare, è fondamentale contattare immediatamente l'Ufficio di Sicurezza ICT e il proprio Referente di Struttura.

II. Cifratura dei dati

Uno strumento chiave per garantire la confidenzialità dei dati è la cifratura. Questa operazione trasforma i dati da un formato leggibile (*in chiaro*) ad un formato non leggibile (*cifrato*). Per poter visionare i dati in chiaro, dal formato cifrato è necessario conoscere una password o un PIN, senza il quale non è possibile recuperare le informazioni originali. Sarebbe opportuno memorizzare i dati personali in formato cifrato e salvare la password o il PIN in un luogo sicuro, perché la perdita di tale elemento comporterebbe l'impossibilità di reperire i dati in chiaro. Questa operazione risulta di fondamentale importanza quando i dati memorizzati sono *personali*, in accordo con la definizione del Regolamento 679/2016, che sono memorizzati nell'HD del computer, su supporti removibili, o in cloud su sistemi centralizzati.

III. Backup multipli dei dati

Il backup consiste nella duplicazione di un file o di un insieme di dati su un dispositivo esterno, permettendo di avere una copia di ripristino dei dati nel caso di perdita accidentale del dispositivo o infezione dello stesso da un attacco di tipo cryptolocker, che produce la cifratura dei dati.
Il backup previene, quindi, la perdita di disponibilità dei dati. È importante prevedere un backup periodico. Se i dati trattati sono personali (in accordo con la definizione del GDPR), è opportuno effettuare una cifratura del backup e seguire la cosiddetta regola del 3-2-1:

- avere 3 copie indipendenti dei dati: avere almeno 2 backup;
- memorizzare le copie su due differenti dispositivi: conservare le copie dei dati su almeno due tipologie di dispositivo diverse (come un disco rigido interno e una penna USB);
- tenere una copia di backup *off-site*: conservare il backup esterno in un luogo diverso rispetto all'altra (non nello stesso cassetto).

Se i dati trattati sono personali le copie di backup devono essere cifrate.

Comportamento dell'Utente

I. Social engineering

La social engineering, o ingegneria sociale, consiste nell'arte di manipolare le persone in modo da rinunciare ad informazioni riservate, come password o dati bancari, oppure di indurre i soggetti ad installare software dannoso, che tramite il controllo del dispositivo permetterà di avere le informazioni riservate sopra indicate. Gli attacchi di questo tipo stanno diventando non solo comuni ma anche sofisticati.
In genere un attacco di social engineering coinvolge email o altri tipi di mezzi di comunicazione, e si basa sulla naturale inclinazione dell'uomo a fidarsi, sulla creazione di un senso di urgenza o paura che portano a non pensare o ragionare sulle operazioni da fare.
Si suggerisce almeno di:

- *Rallentare*: non lasciarsi influenzare dal senso di urgenza di una mail o di una telefonata, sempre meglio pensare prima di agire;
- *Essere sospettosi di messaggi non richiesti*: è sempre bene verificare che il mittente sia reale;
- Eliminare le richieste di informazioni finanziare o password.

II. Gestione della posta consapevole

La posta elettronica è diventato uno strumento essenziale giornalmente ed è oggetto dell'attacco di social engineering più diffuso: il phishing. La mail è apparentemente innocua, ma contiene collegamenti ad un sito dannoso oppure ha in allegato un file contenente codice dannoso che potrebbe compromettere il dispositivo. Il successo del phishing si basa sul fatto che le mail hanno un aspetto legittimo.
Il primo passo è essere consapevoli dello spam ed adottare precauzioni speciali per l'email che:
Richiede la conferma di informazioni personali o finanziarie con elevata urgenza;

- richiede un'azione rapida minacciando l'utente con informazioni spaventose;
- viene inviata da mittenti sconosciuti;
- viene inviata da mittenti conosciuti ma il testo è *inusuale*.

Inoltre, per proteggersi dagli attacchi veicolati dalla posta elettronica è necessario:

- osservare effettivamente l'indirizzo del mittente;
- passare il mouse sui collegamenti e verificare l'URL (spesso non coincide con quella scritta nella mail);
- prestare particolare attenzione ai collegamenti a siti Web che richiedono informazioni personali, anche se l'e-mail sembra provenire da una fonte legittima, perché i siti Web di phishing sono spesso repliche esatte di siti Web legittimi.
- non scaricare mai gli allegati a meno che non si sappia da dove proviene l'email;
- impostare i filtri antispam del programma di posta elettronica utilizzato;
- non divulgare mai informazioni personali o finanziarie via e-mail.

III. Navigazione sicura

Durante la navigazione sul web, è buona norma prestare attenzione alle notifiche di anomalie da parte del browser, dell'antivirus e/o dal firewall, in quanto potrebbero segnalare la presenza di potenziali componenti malevoli all'interno del sito a cui si vuole accedere. Fornire solo dettagli finanziari su siti Web sicuri, non inserire, in particolare, dati personali su pagine web che non garantiscono la conformità alla legislazione vigente (679/2016, GDPR) o che non dispongono di un sito web protetto (SSL). Attenzione ai pop-up: non inserire mai le informazioni personali in una schermata pop-up o fare clic su di essa.

IV. Buone norme di comportamento

La perdita della sicurezza del dispositivo o dei dati è, nella maggior parte dei casi, dovuta ad una disattenzione da parte dell'uomo. Basterebbe seguire alcune semplici norme di comportamento per rallentare la diffusione di software dannosi, o la perdita della confidenzialità, integrità e disponibilità dei dati, tra le quali ricordiamo: di non lasciare incustodito il proprio dispositivo dopo aver effettuato l'autenticazione, di non fornire informazioni private a terzi per telefono o email, bloccare la propria postazione in caso di assenza, prestare particolare attenzione ai dispositivi mobile e cifrare i dati sensibili in essi contenuti, creare un account ospite nel proprio dispositivo, non rispondere alle mail sospette, aggiornare sempre il proprio dispositivo.

Alcune operazioni sui dispositivi devono essere compiute da un utente esperto. Se non si è Amministratore, è sempre buona norma farsi aiutare dal Referente di Struttura.