Indicazioni generali in materia di cifratura dei dati di Ateneo

Versione 1.0 – 9 novembre 2018

Sommario

Premessa

Vengono fornite, di seguito, **indicazioni di base** utili in materia di **crittografia,** sistema che attraverso la **conversione dei dati salvati "in chiaro" in un insieme di informazioni nuovamente accessibili alla sola condizione di applicare un'apposita chiave di decifratura,** consente di prevenire le conseguenze di una loro diffusione involontaria in caso di incidente.

Per ulteriori approfondimenti ed indicazioni di tipo tecnico di maggior dettaglio rispetto a quelle fornite all'interno del presente documento, si rimanda alla *Guida alla cifratura dei dati* di Ateneo.

L'esecuzione di alcune delle operazioni descritte nel presente documento potrebbero richiedere il possesso di competenze di livello tecnico informatico e/o di privilegi di tipo amministrativo. In tal caso **potrebbe essere necessario richiedere supporto tecnico e/o operativo al referente tecnico preposto (referente di struttura o referente tecnico del servizio) prima di procedere**: l'Ufficio di Staff Sicurezza ICT, che ha curato la stesura del presente documento, non è infatti deputato a fornire assistenza in tal senso.

Ulteriori informazioni utili in materia di sicurezza ICT e protezione di dati personali, in ogni caso, possono essere reperite nella sezione dedicata del portale di Ateneo.

Si specifica, infine, che l'Ufficio Sicurezza ICT non risponde di alcun danno o malfunzionamento derivante dall'applicazione non corretta o non rispondente alle stesse. Si invitano i suoi destinatari delle presenti linee guida consultare periodicamente la sezione dedicata del sito di Ateneo in modo da verificare di disporre di documenti sempre aggiornati.

1. Perché è necessaria la cifratura dei supporti

La diffusione indesiderata di dati non cifrati conseguente alla sottrazione o alla perdita accidentale dei dispositivi in cui sono memorizzati **potrebbe esporre l'Ateneo e gli utenti che li trattano a ripercussioni di rilievo sul piano legale e sanzionatorio**, oltre che a tutte le **conseguenze derivanti dall'occorrenza di un danno di immagine assolutamente evitabile.**

Al fine di scongiurare il rischio di una diffusione di informazioni di cui andrebbe preservata la confidenzialità, pertanto, **si suggerisce di criptare i dati di Ateneo presenti nei sistemi in cui essi sono archiviati attenendosi alle seguenti indicazioni.**

1.1 Software di cifratura offerti dal sistema operativo

È possibile cifrare l'intero *file system* oppure solo una sua parte utilizzando gli strumenti forniti con il sistema operativo in uso o, diversamente, utilizzare software di terze parti anche di tipo *open source*.

1.1.1 Piattaforme Microsoft

Sulle piattaforme Microsoft meno recenti è possibile utilizzare l'*Encrypting File System (EFS),* offerto sul *file system* NTFS per cifrare trasparentemente i file.

Sui sistemi Microsoft più recenti (da Windows Vista Enterprise e Ultimate in poi), è possibile, invece, utilizzare la funzionalità *BitLocker Drive Encryption*.

Ulteriori informazioni sono rese disponibili sul sito web ufficiale di Microsoft, oltre che nei paragrafi dedicati all'argomento della *Guida alla cifratura dei dati* di Ateneo.

1.1.2 Piattaforme Apple

Sulle piattaforme Apple è possibile utilizzare la tecnologia FileVault dalla versione Mac OS X Tiger in poi per cifrare in tempo reale la directory home dell'utente.

Ulteriori informazioni sono rese disponibili sul sito web ufficiale di Apple, oltre che nei paragrafi dedicati all'argomento della *Guida alla cifratura dei dati* di Ateneo.

1.2 Software di cifratura offerti da terze parti

L'utilizzo di soluzioni legate al sistema operativo può comportare limitazioni nella compatibilità dei formati e nel supporto dei file cifrati trasferiti.

Per ovviare a questo inconveniente si possono utilizzare **software di terze parti che, spesso, presentano il vantaggio di poter essere installati su vari sistema operativi e di essere *open source***.

Ad esempio, il software *open source VeraCrypt* (evoluzione del TrueCrypt) è disponibile per sistemi operativi Microsoft, Apple e Linux e consente di effettuare la cifratura in modalità trasparente per l'utente di "contenitori" della dimensione desiderata, che possono essere montati come una normale partizione, oppure di interi dischi o pen-drive USB.

Talvolta la mole di dati da cifrare è piccola ma si desidera averne sempre una copia a portata di mano sulla memoria dello smartphone o di un tablet. In questi casi, è possibile utilizzare strumenti rivolti alla cifratura di singoli file, gruppi di file e cartelle, da utilizzare per effettuare esplicitamente la cifratura diversamente rispetto alle modalità trasparenti viste finora.

Nell'utilizzo di questo tipo di applicazioni l'importante è scegliere un buon algoritmo di cifratura (AES-128, AES-256) e una buona chiave di complessità e lunghezza adeguata.

Un'applicazione *open source* che rientra in questa categoria è *Secret Space Encryptor* che si può installare su varie piattaforme mobile, Android e IOS incluse. Adatto alla portabilità di dati su smartphone e tablet, è altresì compatibile con piattaforme Microsoft, Linux e Mac.

Ulteriori informazioni sono rese disponibili sui siti web ufficiali delle organizzazioni che producono i software a cui si è fatto riferimento, oltre che nei paragrafi dedicati all'argomento della *Guida alla cifratura dei dati* di Ateneo.

2. Scegliere buone password o buone *passphrase*

Le tecniche di cifratura si basano spesso su un sistema di password o di *passphrase* (termine con cui si designa un insieme di parole o di stringhe alfanumeriche da utilizzare per l'autenticazione) per consentire l'accesso ai dati.

Una buona prassi è rappresentata dalla scelta di una password o di una *passphrase* facile da ricordare e comoda da digitare che non sia né banale né facilmente indovinabile.

La complessità delle password e delle *passphrase* va ovviamente commisurata alla criticità dei dati da proteggere: non ha senso proteggere dati banali con *passphrase* esageratamente complicate come non ha senso proteggere dati critici con password deboli.

2.1 Cifratura basata su password

Le password da utilizzare per la cifratura di dati:

- devono essere **univoche, sufficientemente lunghe e basate su parole complesse;**

- devono essere **sufficientemente robuste** e, quindi, comprendere **almeno 8 caratteri** di vario tipo (lettere maiuscole e minuscole, numeri e caratteri speciali);
- non devono rimandare alla sfera privata del possessore del dispositivo (es. date o luoghi noti a persone con cui si collabora ecc.)

Un esempio di password che risponde ai criteri enunciati in precedenza è "Amèmutc3c!!!" (dalla frase: "al mattino è meglio un tè che tre caffè!!!"). Un esempio di password ad essi non conforme, viceversa è "carlotta1961".

2.2 Cifratura basata su *passphrase*

In linea di massima **una *passphrase* offre una protezione maggiore rispetto ad una password: se ne raccomanda, pertanto, l'utilizzo**.

Nella scelta di una *passphrase* si suggerisce di utilizzare frasi facilmente memorizzabili, eventualmente prive di senso o che contengano errori di ortografia (accorgimento utile nel caso in cui capiti di dover digitarle in presenza di altre persone).

A titolo di esempio: "Il cane blu nuota sotto l'albero" oppure "Non mi piace il choccolato".

2.3 Testare la robustezza di una password o di una *passphrase* prestando le dovute cautele

Diversi siti web forniscono strumenti utili a testare la robustezza di una password o di una *passphrase*.

La reale utilità di alcuni di essi, tuttavia, potrebbe essere inficiata dalle finalità malevole dei loro creatori.

In linea di principio, infatti, potrebbero essere stati realizzati per memorizzare password o *passphrase* inserite dagli internauti al fine di consentire a dei malintenzionati di violare il dispositivo in cui i dati sono stati salvati attuando tecniche di *cracking* (es. i c.d. "attacchi a dizionario").

Qualora ci si servisse degli strumenti forniti dal web, **pertanto, si raccomanda di non utilizzare ai fini di test la password o la *passphrase* che si intende utilizzare effettivamente, ma un'altra che sia ad essa assimilabile**.

Si specifica, in ogni caso, che **l'attendibilità delle risposte ricevibili non è assoluta**, ma si può almeno avere un'idea della debolezza, più che della robustezza, della password o della *passphrase* da usare.

3. Effettuare il backup delle chiavi crittografiche

È indispensabile garantire la continua disponibilità delle chiavi da utilizzare per la decriptazione di dati cifrati, poiché **dallo smarrimento della chiave crittografica potrebbe derivare l'impossibilità di accedere nuovamente ad essi**.

Pertanto, **dopo avere eseguito la cifratura dei dati, è fondamentale effettuare una o più copie delle chiavi crittografiche per poi custodirle in un luogo sicuro e distinto da quello in cui risiedono i dati criptati.**

Si specifica che a seconda dei meccanismi di cifratura utilizzati, si dovranno esportare i certificati associati agli utenti, salvare le chiavi crittografiche, le password o le *passphrase*.

La custodia delle chiavi può essere fatta in vari modi: in formato elettronico replicandola su più supporti (per evitare che la corruzione di un supporto causi la perdita della chiave) oppure, ove possibile, anche su carta.

4. Verificare la futura disponibilità dei software *open source*

I software *open source* presentano vantaggi quali la disponibilità dei loro file sorgente e la gratuità della licenza di utilizzo; per contro, **non offrono garanzie in merito alla futura disponibilità del software**.

Stando così le cose si consiglia di:

- **tenere traccia del nome del software e della versione** del programma utilizzato
- di **salvare almeno una copia degli *installer* e dei file sorgente** che lo costituiscono, meglio su più supporti distinti

5. Effettuare il backup dei dati da cifrare e cifrare le copie di sicurezza

I dati dell'università che normalmente risiedono sui dispositivi utilizzati sono perlopiù una copia di quelli che primariamente risiedono sui sistemi di proprietà dell'Ateneo.

In alcuni casi i dati non vengono modificati (perché, ad esempio, servono come input per le elaborazioni o per scopi di consultazione) ed una loro eventuale perdita non rappresenta un problema.

In altri casi, invece, essi subiscono importanti variazioni e può essere importante non perdere **le modifiche effettuate, a loro volta consolidabili solo attraverso la sincronizzazione dei dispositivi che contengono i dati originari con quelli modificati.**

Nel caso in cui l'allineamento non possa avvenire in tempo reale o in un lasso di tempo ragionevole, potrebbe essere necessario effettuare una copia di salvataggio dei dati di partenza.

Stando così le cose, è importante che anche le copie di sicurezza dei dati originari siano cifrate. Se si decide di utilizzare un secondo hard disk removibile o di appoggiare i dati su un *cloud* di Ateneo è opportuno cifrare i dati perché anche la compromissione di una copia di salvataggio rappresenta un rischio per la loro riservatezza e la loro l'integrità.

Su un hard disk esterno si può optare per un salvataggio in chiaro, eliminando quindi la cifratura dei dati, solo se si dispone di un sistema sicuro di conservazione come una buona cassaforte.

Ulteriori indicazioni

L'attenzione agli aspetti di gestione sistemistica e la cura della sicurezza informatica sono molto importanti specialmente per i sistemi mobili.

Per sua natura un sistema mobile è più vulnerabile di quelli collegati ad una rete gestita internamente: si trova spesso ad operare fuori dalla rete di Ateneo, in un contesto informatico e telematico di cui si ignorano gli aspetti relativi alla sicurezza.

È quindi fondamentale, oltre che indispensabile, osservare alcuni semplici accorgimenti che possono fare la differenza in termini di sicurezza dei sistemi e conseguentemente dei dati. A titolo d'esempio**:**

- il sistema operativo utilizzato deve essere recente e supportato dal produttore;
- ***le patch* di sistema operativo e del software utilizzato**, rilasciate dai rispettivi produttori, **devono essere applicate automaticamente e tempestivamente** soprattutto se relative agli aspetti di sicurezza;
- i sistemi devono avere un **antivirus installato, funzionante, regolarmente e automaticamente aggiornato.** Tra i vari antivirus è preferibile utilizzare quello di Ateneo;
- **i sistemi mobili normalmente non devono accettare chiamate da altri sistemi** perché non sono server che erogano servizi in rete.

È opportuno, altresì:

- **disporre di un firewall attivo e configurato per consentire il traffico in uscita ma non in ingresso**. (a tal fine si può utilizzare il firewall presente normalmente su tutti i sistemi operativi);
- **creare sul dispositivo in uso almeno un profilo di utente a cui assegnare privilegi minimi** al fine di utilizzarlo per il lavoro di tutti i giorni, **evitando così di usare quotidianamente l'account di amministratore**. Un'applicazione viene infatti eseguita con i permessi dell'utente che la lancia: se presenta un problema di sicurezza è molto più pericolosa se lanciata dall'amministratore della macchina anziché da un utente semplice (non privilegiato).

Si raccomanda, inoltre, di porre particolare attenzione alle situazioni in cui il computer portatile viene prestato anche per tempi brevi ad un soggetto terzo. In questo caso, sarebbe meglio verificare che sul sistema sia presente un account di tipo "ospite" senza alcun privilegio amministrativo e senza la visibilità dei dati contenuti nel sistema, sebbene cifrati.