PROTEZIONE DEI DATI SU COMPUTER E DISPOSITIVI ELETTRONICI 1.6.1

La diffusione dei sistemi informatici ha condotto le aziende ad affidare a computer e reti interne una enorme massa di dati, alcuni dei quali rivestono particolare importanza per le aziende stesse, mentre altri devono rimanere riservati perché contengono dati personali riguardanti dipendenti o clienti. Per questi motivi qualsiasi azienda, indipendentemente dalla sua dimensione, deve preoccuparsi di gestire i problemi legati alla sicurezza dei dati trattati elettronicamente, problemi che consistono principalmente nella eventualità che persone non autorizzate possano accedere a quei dati e nella possibilità di perdita dei dati stessi, dovuta a disattenzione, malfunzionamenti, virus o altri motivi.

Tra le principali norme da seguire per evitare questi e altri simili rischi, ricordiamo l'adozione di una politica di sicurezza nella gestione dei cosiddetti *dati sensibili*, attraverso la predisposizione di misure necessarie a impedire la perdita di questi dati (in seguito a eventi accidentali, furti, danneggiamento, distruzione) o la loro modifica (specie se si tratta di informazioni riservate). In tal senso sono indispensabili backup periodici dei dati (1.6.1.3) e procedure di monitoraggio che permettano di risalire alle persone che hanno avuto accesso a dati riservati.

Devono, inoltre, essere predisposte procedure per segnalare eventuali problemi di sicurezza, in modo che anche il solo sospetto di danni o di una diffusione impropria di informazioni riservate possa immediatamente attivare le necessarie contromisure. Infine, non va trascurata la preparazione dei dipendenti (anche tramite appositi corsi, se si tratta di aziende di grandi dimensioni), che devono conoscere le proprie responsabilità riguardo la sicurezza dei dati: ciò significa educarli a un uso accorto e riservato delle informazioni in loro possesso, a cominciare dall'utilizzo delle password d'accesso.

Anche per i privati cittadini, la rapida diffusione di computer, smartphone e tablet ha portato a registrare in questi dispositivi molti dati personali (informazioni, documenti, foto, ecc.) la cui importanza si scopre spesso solo nel momento in cui il dispositivo nel quale erano archiviati si rompe o, ancora peggio, viene rubato. Anche in questi casi, dunque, è fondamentale conoscere e rispettare le principali regole per la protezione dei dati.

1.6.1.1

Riconoscere politiche corrette per le password, quali crearle di lunghezza adeguata, con un'adeguata combinazione di caratteri, evitare di condividerle, modificarle con regolarità

Esistono applicazioni in grado di decodificare le password all'insaputa dei loro legittimi "proprietari". Per ridurre questo rischio bisogna evitare che le password corrispondano:

- a dati personali (nome o data di nascita propri o di familiari o di persone care, numeri di telefono, targa della propria auto, ecc.);
- a sequenze prevedibili (del tipo " 123456 ", " 000000 ", " password ", " QWERTY ", " ciao ", ecc.);
- a parole di uso comune (" farfalla ", " segreto ", ecc.).

Meglio utilizzare almeno otto caratteri e inserire nella password sia lettere minuscole, sia lettere maiuscole, sia numeri ed eventualmente

Per saperne di più...
... sulle password, acquisisci l'immagine del QR Code con il tuo smartphone o tablet.

anche simboli: tutto insieme (ad es.: " M@rio673 ", oppure " 3nr1c0*! ", ecc.). Un'altra buona abitudine è quella di cambiare periodicamente le password. Infine, quasi superfluo, ma non certo inutile, è raccomandare di non comunicare a nessuno la propria password e di ricordarla bene, evitando però di conservarla scritta in posti come il retro del tappetino del mouse o un foglietto attaccato al monitor!

più

Alcune applicazioni e siti permettono la memorizzazione della propria password in modo da inserirla automaticamente la volta successiva: abilitate questa funzione solo se siete sicuri di essere gli unici utilizzatori del computer dove state operando.

Le precauzioni riguardanti la scelta e la segretezza delle vostre password sono ovviamente legate all'importanza dei dati che esse proteggono: una password del tipo " elton " può anche andar bene se vi serve per partecipare occasionalmente a una chat, ma è del tutto inadatta se permette l'accesso a dati particolarmente riservati (gestione del proprio conto corrente, della casella di posta elettronica, ecc.).

1.6.1.2 Definire il termine firewall e identificarne gli scopi

Il firewall (pr. *fàir-uòl*) è un sistema di sicurezza con il quale si cerca di evitare che estranei possano accedere a dati presenti in un dispositivo collegato a Internet, o trasmettere virus informatici.

Il firewall può essere sia software sia hardware. Le applicazioni firewall vengono sempre più utilizzate anche da privati, soprattutto da coloro che sono collegati a Internet per parecchie ore al giorno; gli stessi sistemi operativi generalmente comprendono già al loro interno un software di questo tipo. Allo stesso modo, anche i modem-router ADSL integrano spesso al loro interno un firewall.

Il firewall blocca i tentativi di intrusione, impedendo che il computer risponda alle istruzioni esterne. Va detto che molti di questi tentativi non hanno in realtà intenzioni negative e che, comunque, anche il firewall non garantisce al cento per cento l'utente da malintenzionati particolarmente abili.

1.6.1.3 Comprendere lo scopo di creare con regolarità copie di sicurezza remote dei dati

Il termine *backup* (pr. *bekàp*) indica le copie di sicurezza di file (documenti, programmi, ecc.) che vengono effettuate su supporti di memoria rimovibili (ad es. pendrive, dischi fissi esterni, CD, DVD), in modo da poter recuperare i dati in caso di perdita o deterioramento degli stessi. Uno dei guasti più frequenti è il danneggiamento, totale o parziale, del disco fisso: tutto ciò che era memorizzato nei settori danneggiati andrà perduto. Altri rischi derivano da malware, cattivo funzionamento del software e, soprattutto, da errori umani.

Se i dati da conservare sono di particolare importanza è consigliabile realizzare più di una copia di sicurezza, da conservare lontano dalla polvere, dal calore e da fonti magnetiche e possibilmente in un luogo differente da quello dove si trova il computer, nel caso si verifichino eventi straordinari come furti, incendi o crolli. La frequenza dei backup deve essere maggiore se utilizziamo computer portatili, perché sono più esposti a guasti derivanti da accidentali cadute o urti, rischi di smarrimento o furto.

più

A questi eventi sono soggetti anche altri apparecchi elettronici di uso sempre più comune: quali tablet, smartphone e telefoni cellulari. Nei primi due casi è consigliabile effettuare una copia dei dati personali sul proprio computer, dal momento che in genere è possibile realizzare questo trasferimento di informazioni. Nel caso dei cellulari è bene riportare i numeri di telefono che sono stati annotati solo sul cellulare anche in un documento elettronico o almeno su una più tradizionale rubrica cartacea.
In ogni caso, occorre rendersi conto che la sempre maggiore capienza, economicità e potenza dei dispositivi elettronici fa sì che essi contengano spesso molti dati personali di importanza sempre crescente: da numeri telefonici o foto e video estremamente personali, ad appunti, mail e documenti, della cui importanza e segretezza ci accorgiamo a volte solo quando il dispositivo si è rotto, è stato smarrito o rubato.

Sempre in tema di sicurezza dei dati, va ricordato che a molte persone è capitata la brutta esperienza di scrivere al computer qualcosa per ore e ore e – quando si era a poche righe dalla conclusione – è mancata la corrente e tutto il lavoro è andato perso. Infatti, in caso di interruzione dell'energia elettrica o anche di un semplice sbalzo della tensione elettrica, si perde tutto ciò che è memorizzato nella RAM del computer (a meno che non si stia lavorando con un computer portatile o si disponga di un *gruppo di continuità* o *UPS*) e quindi – se non si è avuta l'accortezza di salvare sull'hard disk le modifiche apportate al lavoro che si stava svolgendo – tutto va sprecato. La perdita dei dati avviene anche quando si verifica un guasto al computer, un blocco dell'applicazione o un errore dell'utente.

Perciò, mentre state lavorando a un vostro documento, abituatevi a salvare ogni tanto il vostro lavoro, in modo particolare dopo aver effettuato una aggiunta o una modifica importante. Se state lavorando con uno dei tanti programmi *Microsoft* (*Word, Excel, PowerPoint,* ecc.) e non vi va di staccare le mani dalla tastiera per cliccare col mouse sul pulsante che rappresenta un dischetto, premete contemporaneamente i tasti *Maiusc* e *F12*: impiegherete un secondo assicurandovi contro i rischi di dover passare ore per ricostruire quello che potreste perdere per un banale black out o per un blocco del vostro computer. Potete anche configurare le applicazioni perché facciano questa operazione per conto vostro a determinati intervalli di tempo (a questo proposito consultate la guida in linea dei programmi alla voce "salvataggio automatico").

1.6.1.4

Comprendere l'importanza di aggiornare regolarmente i diversi tipi di software, quali antivirus, applicazioni, sistema operativo

Il mondo dell'informatica è in continua evoluzione, come dimostrano i nuovi software che sono quotidianamente realizzati. Il malware non fa eccezione a questa regola e anche di esso compaiono quotidianamente nuovi tipi, rapidamente distribuiti da Internet in tutto il mondo.

Quando compare un nuovo malware, gli specialisti delle ditte produttrici di antivirus, sistemi operativi e applicazioni che possono essere contagiate, si mettono al lavoro e, in breve tempo, inseriscono nella banca dati le nuove istruzioni e le modifiche per debellarlo.

Ovviamente, se non ci colleghiamo con il sito della casa produttrice (cosa che il sistema fa in genere da solo) l'antivirus, il sistema operativo o l'applicazione non saranno in grado di riconoscere il nuovo malware e di impedirne il suo ingresso nel nostro computer o altro dispositivo elettronico. L'unica cosa da fare, in questo caso, è anche la più semplice: lasciare che il sistema proceda autonomamente a inserire gli aggiornamenti quando il dispositivo è connesso a Internet, cosa che fa da solo senza disturbarci mentre navighiamo da un sito all'altro, se non per avvisarci della disponibilità degli aggiornamenti e della loro avvenuta installazione.