Manuale ECDL Full Standard

Modulo
IT Security

Sommario

Capitolo 1 – Le informazioni personali

Riferimento Syllabus 1.1.1	***Distinguere tra dati e informazioni.***
Riferimento Syllabus 1.1.2	***Comprendere il termine crimine informatico.***
Riferimento Syllabus 1.2.1	***Comprendere i motivi per proteggere le informazioni personali, quali evitare il furto di identità o le frodi.***
Riferimento Syllabus 1.2.3	***Identificare le misure per prevenire accessi non autorizzati ai dati, quali cifratura, password***
Riferimento Syllabus 1.2.4	***Comprendere le caratteristiche fondamentali della sicurezza delle informazioni, quali confidenzialità, integrità, disponibilità.***
Riferimento Syllabus 1.2.5	***Identificare i requisiti principali per la protezione, conservazione e controllo di dati/privacy che si applicano in Italia.***
Riferimento Syllabus 1.3.3	***Comprendere il termine furto di identità e le sue implicazioni personali, finanziarie, lavorative, legali.***
Riferimento Syllabus 1.4.3	***Comprendere i vantaggi e i limiti della cifratura***
Contenuti della lezione	***In questa lezione cercheremo di:*** **renderci conto del valore delle nostre informazioni, proteggere le nostre informazioni personali, lavorative, finanziarie, ..., capire quali sono le caratteristiche fondamentali della sicurezza informatica, analizzare brevemente la legislazione italiana in materia di protezione dei dati personali, descrivere cosa si intende con crimine informatico.**

Distinguere tra dati e informazioni.

Agli albori dell'informatica, si usava molto spesso il termine EDP (Electronic Data Processing), mettendo l'accento sull'elaborazione (Processing) con strumenti elettronici (Electronic) dei dati (Data). Allora, proprio per la rapidissima evoluzione tecnica, si insisteva maggiormente sugli aspetti tecnici. I "dati" la facevano da padrone, con tutti i problemi tecnologici che l'informatica dell'epoca presentava.

Oggi, il termine EDP è pressoché scomparso ma soprattutto l'attenzione si è spostata dai dati alle informazioni. Chi non ha mai sentito almeno uno di questi termini: Tecnologie dell'Informazione e della Comunicazione (Information and Communication Technology – ICT), autostrade dell'informazione, sistema informativo aziendale? Se vi dovesse sfuggire il significato del termine ICT, vi raccomandiamo gli IBUQ *ECDL Computer Essentials* e *ECDL Online Essentials*.

I dati non sono nient'altro che una rappresentazione di proprietà, fatti, caratteristiche, azioni, eventi ... legati a persone, enti, ... o più generalmente oggetti di una rilevazione. Per quanto ci riguarda, tale rappresentazione viene fatta in modalità elettronica e può avvenire attraverso diversi media e formati: testo, disegno, immagine, ... Non necessariamente i dati grezzi appena rilevati sono comprensibili e significativi per una persona diversa da quella che li ha rilevati. Cosa rappresentano i dati riportati in Tabella 1 è noto solo a chi li ha rilevati.

Spesso però i dati non sono proprio grezzi ma almeno "spiegati", anche solo per la comodità del rilevatore. I dati riportati in Tabella 2 sono di più facile lettura e comprensione rispetto agli stessi della tabella precedente.

Il concetto di informazione si spinge oltre, compiendo un passo ulteriore: le informazioni sono dati elaborati (anche soltanto organizzati) in modo da renderli comprensibili e significativi per i loro utilizzatori. Se si precisa che la tabella precedente è relativa ai clienti della nostra azienda, che la colonna "Debito" rappresenta quanto ognuno ci deve ancora pagare in seguito a delle vendite, abbiamo maggiori informazioni sui clienti. Se elaboriamo queste informazioni in un prospetto di sintesi, disponiamo di vere e proprie informazioni sulla situazione finanziaria aziendale.(che tra l'altro, non sembra tanto buona ...) che ci induce a mettere in atto qualche azione di recupero crediti.

50001	03/01/14	5000,00
50002	01/07/14	0,00
50003	31/12/14	3000,00
50004	02/06/14	2500,00
...	...	
50357	01/04/14	0,00

Tabella 1: Dati grezzi

Cliente	Scadenza	Debito
50001	03/01/14	5000,00
50002	01/07/14	0,00
50003	31/12/14	3000,00
50004	02/06/14	2500,00
...	...	
50357	01/04/14	0,00

Tabella 2: Informazioni semplici

In termini di sicurezza informatica, è ben diverso il furto dei dati riportati in tabella Tabella 1 rispetto al furto delle informazioni presenti in Tabella 3.

Malgrado questa differenza concettualmente importante, nell'uso corrente i termini dati e informazioni sono usati pressoché indifferentemente. In questo IBUQ ci adegueremo a questa prassi, tranne in casi specifici.

Situazione clienti al 01/09/2014 (€)	
Scaduti incassati	50.000,00
Scaduti non incassati	145.000,00
Da scadere	23.000,50
Totale	218.000,50
Numero di clienti	320

Tabella 3: Informazioni elaborate

Comprendere le caratteristiche fondamentali della sicurezza delle informazioni, quali confidenzialità, integrità, disponibilità

Proprio per i fondamentali risvolti pratici che assume, la sicurezza delle informazioni è oggetto di numerosi studi e ricerche. Il documento di riferimento che ha strutturato l'argomento, è *ISO/IEC 27002:2013 Information technology - Security techniques - Code of practice for information security controls* (http://www.iso27001security.com/html/27002.html). Questo documento propone il modello CID (Confidenzialità, Integrità, Disponibilità), in inglese CIA (Confidentiality, Integrity, Availability).

Le tre linee proposte da questo modello, divenute ormai standard si ritrovano spesso nelle politiche di sicurezza informatica e hanno trovato riscontro nelle disposizioni di legge:

- *confidenzialità*: le informazioni devono essere protette per impedire accessi e utilizzo a persone non autorizzate. Le stesse autorizzazioni di accesso devono essere limitate alle effettive necessità di consultazione e elaborazione. In un'azienda, ovviamente, tutte le informazioni devono essere protette da accessi non autorizzati, interni o esterni che siano. Inoltre, devono essere previsti sistemi di autorizzazioni per limitare gli accessi alle varie categorie di informazioni agli addetti che ne hanno l'effettiva necessità. Per esempio, gli addetti alla produzione, che per la loro attività non hanno la necessità di accedere ai dati contabili dei clienti, non devono potervi accedere.

- *integrità*: nello stesso modo in cui la consultazione delle informazioni deve essere controllata, deve essere assicurata la conservazione delle informazioni nel loro stato corretto, senza che vi sia la possibilità di modificarle, cancellarle o aggiungerne in modo improprio, accidentalmente, o volontariamente. Questa alterazione deve essere impedita sia per i dati memorizzati nel sistema, sia per i dati trasmessi. Per esempio, in occasione dell'invio di un messaggio di posta elettronica, deve (dovrebbe) essere garantito che il contenuto del messaggio, compresi gli allegati, che giunge al destinatario sia lo stesso di quello inviato dal mittente.
- *disponibilità*: così come le informazioni non devono essere accessibili a chi non è autorizzato, devono essere rese disponibili a chi è autorizzato in modo efficace e tempestivo. Questa caratteristica deve essere garantita sia nell'operatività ordinaria (affidabilità dell'hardware e del software, garanzia di accesso, ...), sia in seguito a fatti accidentali (guasto, malfunzionamento, cancellazione involontaria di dati), sia in caso di azioni dolose (danneggiamento alle apparecchiature, furto di dispositivi o di dati). In tutti i casi, il ripristino della funzionalità del sistema informatico deve avvenire in tempi brevi.

Il rispetto di queste caratteristiche nella messa in opera di politiche di sicurezza coinvolge aspetti tecnici organizzativi e legali, spesso complessi che vanno analizzati caso per caso. Ma, lo vogliamo ripetere, coinvolge aspetti non tecnici che vanno affrontati con opportuna sensibilizzazione e formazione del personale.

Va inoltre detto che nessuna misura di sicurezza elimina completamente i rischi. Si parla quindi di riduzione a livelli accettabili del rischio, livelli da definire tramite un'analisi dei rischi e in funzione del costo accettabile delle misure di sicurezza, dal punto di visto economico e organizzativo.

C'è poi sempre la possibilità di seguire il consiglio di questa citazione per impostare le misure di sicurezza (tratta e liberamente tradotta da http://en.wikiquote.org/wiki/Gene_Spafford):

> *"L'unico sistema veramente sicuro è quello spento, sigillato in un blocco di cemento e chiuso in una stanza blindata sorvegliata da guardie armate - e anche così ho dei dubbi".*
>
> Prof. Eugene Spafford, Purdue University

Comprendere i motivi per proteggere le informazioni personali, quali evitare il furto di identità o le frodi

Nell'IBUQ *ECDL Online Essentials* sono illustrati i principali servizi disponibili oggi su Internet, sempre più numerosi e sempre più adoperati da privati e aziende, Rari sono quelli che non hanno mai adoperato l'*e-commerce* per comprare un biglietto, un libro o qualche bene o servizio oppure quelli che non usano l'*e-banking* per effettuare la maggior parte delle operazioni con la propria banca tramite Internet. Tutti servizi che hanno a che fare con pagamenti e richiedono l'identificazione dell'utente e soprattutto l'inserimento di informazioni utili per il pagamento (tipicamente i dati della propria carta di credito).

Per la maggior parte delle transazioni sono previste misure di sicurezza sempre più efficaci ma anche gli attacchi e le tecniche per carpire informazioni sono sempre più numerose ed efficaci. E' facile intuire quanto sia pericoloso il furto di informazioni il cui uso possa portare ad una perdita di denaro.

Ma il furto delle sole credenziali di accesso alla propria casella di posta elettronica o alla rete sociale che utilizziamo può arrecarci danni significativi, anche se questo non ha un immediato riflesso economico. Furti di identità (approfondito al punto successivo), frodi, danneggiamento della propria immagine o della propria reputazione sono rischi di cui ci dobbiamo rendere conto e che dobbiamo prendere in considerazione. Un uso sicuro di Internet e dei suoi servizi si basa quindi sulla conoscenza di questi rischi di frode e di furto di identità per ridurre i quali è fondamentale tenere riservate e protette queste informazioni personali.

Un'attenzione particolare a queste problematiche deve essere posta dalle aziende, ancora più che dai privati. Per questo le riprenderemo nella parte finale dedicata alle aziende, al punto 1.2.2.

Comprendere il termine furto di identità e le sue implicazioni personali, finanziarie, lavorative, legali

Il furto di identità è un tema di portata generale, che ha dei risvolti informatici particolarmente importanti. A livello generale, il furto di identità (o più propriamente usurpazione di identità) consiste nel fatto di utilizzare l'identità di un'altra persona con lo scopo di compiere degli atti fraudolenti di natura commerciale, civile o penale, come se li avesse compiuti lei.

Anche se, ancora oggi, le statistiche realizzate dagli organismi di controllo e repressione dimostrano che sono prevalenti i furti di identità non informatici (furto di documenti di identità cartacei, falsificazione di documenti cartacei, ...), i furti di identità che coinvolgono strumenti informatici sono sempre più frequenti.

Il furto di identità si basa quindi sull'acquisizione da parte del ladro di informazioni su una persona per potersi sostituire ad essa e far ricadere su di essa i rischi e le conseguenze negative degli atti che esso vuole compiere. Non bisogna pensare che abbiano valore solo informazioni riservate, protette e spesso tenute segrete. I furti di identità organizzati hanno sempre una fase iniziale in cui il ladro acquisisce informazioni apparentemente pubbliche e di scarsa rilevanza (ma sempre personali): nome, cognome, indirizzo, numeri di telefono, data e luogo di nascita, codice fiscale, composizione della famiglia e dati personali dei membri della famiglia, nomi degli animali di compagnia (!), luogo di lavoro e nome del datore di lavoro, hobby, ... Per poi passare a dati più rilevanti quali indirizzi mail, identificativi di servizi Internet, nome della banca, numero della carta di credito. Per poi proseguire la raccolta con informazioni riservate quali password di accesso e compiere effettivamente alla fine di questo percorso le azioni fraudolenti.

Il processo di raccolta delle informazioni dipende ovviamente dalla natura dell'azione illegale che il ladro vuole compiere, non trattandosi sempre di furto di somme di denaro ma di azioni di vario genere: poter documentare diplomi mai conseguiti, sembrare in posizione regolare per l'immigrazione senza esserlo realmente, guidare un veicolo senza averne realmente l'abilitazione, ...

Identificare le misure per prevenire accessi non autorizzati ai dati, quali cifratura, password

Possiamo classificare in due famiglie le misure destinate a prevenire accessi non autorizzati ai dati, diverse per obiettivi e finalità:

- *impedire l'accesso non autorizzato ai dati.* Queste misure sono basilari e irrinunciabili ma non sempre hanno un elevato livello di sicurezza: sono tipicamente l'uso delle credenziali di autenticazione, in generale la password, usate per limitare l'accesso ai soli utenti registrati che hanno la responsabilità della non divulgazione della stessa. All'uso della password si affiancano le misure minime di sicurezza quali il blocco della propria postazione di lavoro in caso di assenza, la custodia della password, ... La password costituisce però una misura di sicurezza debole che richiede l'attivazione di misure di altro tipo per impedire l'utilizzo dei dati da parte di un ladro che sia riuscito ad impadronirsene.

- *impedire l'utilizzo dei dati in caso di furto di dati*. E se non è bastata la password ma sono stati rubati i dati, per esempio asportando un disco o rubando un portatile? I dati non potranno essere utilizzati dal ladro se saranno stati cifrati (detti anche crittografati) prima di registrarli sul disco. In questo caso, anche inserendo il disco in un altro computer - vanificando così la protezione offerta dalla password - non è possibile accedere ai dati senza disporre della chiave usata nella cifratura.

La Notizia

24 luglio 2014

La BCE (Banca Centrale Europea) riconosce un furto di dati dai propri sistemi informatici consentito da una falla di sicurezza in un database di supporto al suo sito web.

https://www.ecb.europa.eu/press/pr/date/2014/html/pr140724.en.html

Per farsi riconoscere da un sistema informatico e poter accedere ai dati, la password può essere affiancata o sostituita da altri sistemi di protezione, più sicuri, per esempio un badge personale da inserire in un apposito lettore. In questo caso, non basta la conoscenza della password ma occorre duplicare (in gergo, clonare) o rubare fisicamente il dispositivo.

Comprendere i vantaggi e i limiti della cifratura

Si parla di cifratura non soltanto per la registrazione dei dati su supporto di memorizzazione, ma anche a proposito della trasmissione di informazioni. In questo caso la trasmissione di informazioni avviene in quattro passi:

1. codifica da parte del mittente dell'informazione da trasmettere
2. invio dell'informazione cifrata
3. ricezione dell'informazione cifrata da parte del destinatario
4. decodifica dell'informazione ricevuta.

Un sistema oggi largamente utilizzato è quello che prende il nome di Crittografia asimmetrica (o crittografia a chiave pubblica). Senza entrare nei dettagli tecnici, ci limitiamo a dire che:

- ognuno dei due interlocutori dispone di due chiavi
  - una chiave pubblica, che deve diffondere, utilizzata da chi vuole mandargli informazioni, per criptarle
  - una chiave privata, segreta, utilizzata dal destinatario per decodificare le informazioni ricevute
- il mittente utilizza la chiave pubblica del destinatario per codificare le informazioni da spedirgli
- il destinatario utilizza la propria chiave privata per decodificare le informazioni ricevute
- la chiave privata non ha bisogno di essere scambiata, in quanto non serve nella cifratura, consentendo un'ulteriore riduzione dei rischi.

In sintesi, nel caso di trasmissione, la cifratura rende molto difficile la lettura dei dati in caso di intercettazione. Nel caso di cifratura di file su supporto di memorizzazione, l'accesso ai dati e il loro utilizzo è possibile solo a chi dispone della chiave di codifica. In caso di furto del file, il ladro non potrà leggere immediatamente i dati.

Ma attenzione, la cifratura non è di per sé una panacea. Nei casi in cui la cifratura di file non avviene automaticamente ma ad opera dell'utente (si pensi per esempio alla cifratura di documenti di LibreOffice, come descritto successivamente al punto 1.4.2), essa presenta due limiti dei quali tener conto:

- in caso di smarrimento della chiave nemmeno il legittimo proprietario può acceder ai propri dati. La chiave o password che permette di decodificare il file deve quindi essere custodita in modo da non compromettere la *disponibilità* dei dati (una delle caratteristiche fondamentali della sicurezza informatica) ma ovviamente in modo riservato
- il livello di sicurezza dipende dalla scelta da parte dell'utente della chiave o password di codifica. Se l'utente sbrigativo non rispetta le buone politiche per le password (illustrate al punto 3.4.2), il file è facilmente decodificabile da parte di qualche malintenzionato che ne venisse in possesso. Lo stesso dicasi se non si rispettano le norme elementari di sicurezza per far conoscere la chiave al destinatario.

Così come si osserva una rincorsa fra creatori di virus e produttori di antivirus, in modo simile si discute sull'inviolabilità delle tecniche di crittografia e periodicamente vengono scoperti metodi di decodifica che rendono inutili sistemi di cifratura ritenuti fino ad ora sicurissimi.

L'importanza della sicurezza informatica è stata recepita dal legislatore italiano già da diversi anni. Si sono susseguite disposizioni di legge in materia di Tutela dei dati personali (detta privacy) che definivano norme minime di sicurezza e incitavano imprese e privati a mettere in pratica comportamenti e regole per proteggere dati personali e dati sensibili, in particolare se gestiti tramite strumenti informatici.

Identificare i requisiti principali per la protezione, conservazione e controllo di dati/privacy che si applicano in Italia

Il Testo unico sulla privacy (D.Lgs 196/2003) e successive modifiche (per esempio il Decreto Legge n. 5 del 9 febbraio 2012 convertito nella Legge n.35 del 4 aprile 2012) è lo strumento che tutela i dati personali dei cittadini italiani, dentro e fuori Internet. Il decreto è entrato in vigore il 1 gennaio 2004 ed è il testo di riferimento in merito alla protezione dei dati personali in Italia. Le finalità della norma sono illustrate all'art 2:

1. *Il presente testo unico, di seguito denominato "codice", garantisce che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali.*
2. *Il trattamento dei dati personali è disciplinato assicurando un elevato livello di tutela dei diritti e delle libertà di cui al comma 1 nel rispetto dei principi di semplificazione, armonizzazione ed efficacia delle modalità previste per il loro esercizio da parte degli interessati, nonché per l'adempimento degli obblighi da parte dei titolari del trattamento.*

L'art 3 del Codice unico contiene l'elenco delle definizioni adottate dalla legge. Vale la pena di soffermarsi su alcune di queste:

- *"trattamento" qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati;*

- *“dato personale"*, *qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale.*
- *"dati sensibili", i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale;*
- *"titolare", la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalita', alle modalita' del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza*
- *"responsabile", la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali;*
- *"incaricati", le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile;*
- *"interessato", la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali.*

L'interessato, cioè colui a cui si riferiscono i dati personali, ha diritto:

- di essere informato sull'esistenza di dati personali e di averne comunicazione in forma intellegibile (art 7, comma 1)
- di conoscere l'origine di tali dati, le finalità e modalità del trattamento, gli estremi del titolare del trattamento e i soggetti ai quali possono essere comunicati tali dati (art. 7, comma 2)
- di ottenere cancellazione, aggiornamento, rettifica e integrazione dei dati (art. 7, comma 3)
- di opporsi, per motivi legittimi, al trattamento dei propri dati e in particolare “al trattamento di dati personali che lo riguardano a fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale.” (art. 7, comma 4).

La gestione dei dati personali è una questione molto delicata, tanto da essere regolata in modo puntuale da specifiche norme. In ottemperanza a quanto previsto dal Testo Unico della Privacy, il titolare del trattamento deve informare l'interessato, per quanto riguarda:

- il motivo, le finalità e le modalità della raccolta
- l'obbligatorietà della raccolta e le conseguenze in caso di rifiuto
- i soggetti terzi a cui potrebbero essere comunicati i suoi dati
- gli estremi del titolare del trattamento e a chi rivolgersi per l'esercizio dei suoi diritti.

Di norma il trattamento può avvenire solo previo consenso dell'interessato, salvo che:

- si tratti di un obbligo giuridico (come nel caso di alberghi e pensioni che devono trasmettere alla questura i dati del cliente)
- sia necessario per la salvaguardia della vita e dell'incolumità dell'interessato (ad esempio per ricoveri urgenti in ospedali)
- sia necessario per difendere propri diritti in sede giudiziaria.

Citando il Garante per la protezione dei dati personali, il consenso è:

> *La libera manifestazione di volontà dell'interessato con cui questi accetta espressamente un determinato trattamento dei suoi dati personali, del quale è stato preventivamente informato da chi ha un potere decisionale sul trattamento (vedi titolare). È sufficiente che il consenso sia "documentato" in forma scritta (ossia annotato, trascritto, riportato dal titolare o dal responsabile o da un incaricato del trattamento su un registro o un atto o un verbale), a meno che il trattamento riguardi dati "sensibili"; in questo caso occorre il consenso rilasciato per iscritto dall'interessato (ad es., con la sua sottoscrizione).*
>
> http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1663787

Dal punto di vista tecnico, altre precisazioni dettate dalla legge riguardano:

- la gestione delle credenziali di autenticazione

- il formato delle password
- il salvataggio e ripristino dei dati
- la protezione contro l'intrusione e il malware
- la periodicità di aggiornamento degli strumenti di protezione dei dati.

Il quadro di riferimento normativo europeo originario è la Direttiva 95/46/CE del Parlamento Europeo e del Consiglio del 24 ottobre 1995 relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati. Il 12 marzo 2014 è stato approvato il nuovo Regolamento sullo stesso tema che tiene conto delle nuove esigenze emerse dal 1995 ad oggi. A completamento del quadro normativo, entro il 2014 dovrebbe essere emanata anche la Direttiva che disciplina la materia per finalità di polizia e giustizia ossia "il trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali".

L'estrema attenzione portata alla sicurezza informatica è dovuta anche alla pericolosità delle azioni fraudolenti che si possono compiere attraverso gli strumenti informatici e alla gravità dei reati che ne derivano. Tant'è che si parla ormai di veri e propri crimini informatici. Vedremo quindi in questo IBUQ cosa rischiano i nostri dati e cosa rischiamo noi se siamo oggetto di questi crimini.

Comprendere il termine crimine informatico

Dando per scontato il significato di "crimine", possiamo concentrarci sulle caratteristiche specifiche del crimine informatico. Con crimine informatico, si intende un atto illecito realizzato attraverso l'uso (improprio) di strumenti informatici, siano essi locali (un personal computer, un dispositivo elettronico) oppure remoti (una rete di computer o Internet stesso). Essere vittima di un crimine informatico è uno dei rischi ai quali è soggetto l'utente di sistemi informatici. Ma chi oggi non è utente di sistemi o strumenti informatici?

Di crimini informatico tratteremo in tutto questo IBUQ., così come esamineremo le tecniche di difesa.

Anticipiamo alcuni esempi di crimine informatico: l'accesso non autorizzato a sistemi informatici, il furto di informazioni, il furto di identità, la distruzione o alterazione di dati ... e i conseguenti furti veri e propri o altri danni di vario genere operati tramite l'uso improprio degli strumenti informatici.

Ma così come ci sono ladri di dati e criminali informatici, esistono diverse istituzioni che fra i loro compiti hanno quello di reprimere i cyber-crimini informatici. A livello europeo, l'EUROPOL (*European Police Office*) - https://www.europol.europa.eu/ è un'agenzia dell'Unione Europea che assicura supporto per la repressione del crimine alle forze dell'ordine dei paesi dell'EU, in collaborazione con una quindicina di paesi extra-europei. A dimostrazione dell'importanza crescente del crimine informatico, ha costituito in gennaio 2013 un apposito centro per la lotta al crimine informatico. Il focus dell'attività di questo centro (European Cybercrime Center - EC3) è proprio sui crimini ad opera di gruppi organizzati a scopo di frode online, l'adescamento in rete e lo sfruttamento sessuale dei bambini nonché gli attacchi a infrastrutture critiche e sistemi informativi dell'UE. Tutti temi che avremo occasione di incontrare in questo IBUQ.

La Notizia

22 settembre 2014

Di fronte alla recrudescenza del crimine informatico, la Federazione delle Banche Europee (EBF) e il il European Cybercrime Centre (EC3) hanno siglato un memorandum d'Intesa per potenziare la collaborazione fra le forze dell'ordine e il settore bancario nell'UE.

https://www.europol.europa.eu/content/european-banks-and-europol-join-forces-fight-cybercrime

Capitolo 2 – Rischi del crimine informatico

Riferimento Syllabus 1.1.4	***Riconoscere le minacce ai dati provocate da forza maggiore, quali fuoco, inondazione, guerra, terremoto.***
Riferimento Syllabus 3.2.1	***Riconoscere le possibilità di connessione ad una rete mediante cavo o wireless.***
Riferimento Syllabus 3.2.2	***Comprendere che la connessione ad una rete ha implicazioni di sicurezza, quali malware, accessi non autorizzati ai dati, mantenimento della privacy.***
Riferimento Syllabus 3.3.1	***Riconoscere l'importanza di richiedere una password per proteggere gli accessi a reti wireless.***
Riferimento Syllabus 3.3.2	***Riconoscere diversi tipi di sicurezza per reti wireless, quali WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected Access), MAC (Media Access Control).***
Riferimento Syllabus 3.3.3	***Essere consapevoli che usando una rete wireless non protetta si rischia che i propri dati vengano intercettati da "spie digitali".***
Riferimento Syllabus 3.3.4	***Connettersi ad una rete wireless protetta/non protetta.***
Riferimento Syllabus 4.2.1	***Comprendere l'importanza di non divulgare informazioni riservate su siti di reti sociali.***
Riferimento Syllabus 4.2.3	***Comprendere i rischi potenziali durante l'uso di siti di reti sociali, quali cyberbullismo, adescamento, informazioni fuorvianti/pericolose, false identità, link o messaggi fraudolenti.***
Riferimento Syllabus 5.2.1	***Comprendere il termine messaggistica istantanea (IM) e i suoi usi.***
Riferimento Syllabus 5.2.2	***Comprendere le vulnerabilità di sicurezza della messaggistica istantanea, quali malware, accesso da backdoor, accesso a file.***
Riferimento Syllabus 6.2.1	***Comprendere il motivo per eliminare in modo permanente i dati dalle memorie di massa o dai dispositivi.***
Riferimento Syllabus 6.2.2	***Distinguere tra cancellare i dati e distruggerli in modo permanente.***

Distinguere tra dati e informazioni

Quelle provocate da forza maggiore (catastrofi naturali, eventi straordinari, ...) si riferiscono prevalentemente alla distruzione, totale o parziale, del sistema informatico, con conseguente perdita dei dati.

Nel caso di catastrofi o eventi straordinari (incendio, inondazione, terremoto, guerra, ...) impedire la distruzione dei dati può essere molto difficile se non impossibile. L'attenzione in termini di sicurezza si sposta quindi sul recupero dei dati in caso di perdita e la riduzione dei danni che ne derivano. Come vedremo, acquistano quindi particolare importanza le procedure di backup o copie di sicurezza e ripristino.

In questi casi, rispetto a quello del furto visto prima: nessuno entra in possesso dei dati ma questi vengono distrutti. Sono quindi rilevanti soltanto i punti 1. e 3.

La Notizia

25 aprile 2011

Un incendio si sviluppa nella server farm principale di Aruba, uno dei maggiori provider italiani, nella zona dei gruppi di continuità (che dovrebbero garantire la fornitura di energia in caso di black-out). I dispositivi anti-incendio scattano regolarmente per spegnere le apparecchiature. Nessun dato viene perso ma ne consegue un'interruzione del servizio di diverse ore.

http://punto-informatico.it/3146710/PI/News/aruba-incendio-nella-farm.aspx
http://punto-informatico.it/3147399/PI/News/aruba-una-giornata-fuoco.aspx

Oggi è pressoché impossibile trovare un personal computer isolato, non collegato a qualche rete. Una rete aziendale, la rete di casa con due o tre personal computer, per non parlare di Internet. In tema di sicurezza, il collegamento ad una rete introduce rischi e difficoltà di protezione aggiuntivi.

Comprendere che la connessione ad una rete ha implicazioni di sicurezza, quali malware, accessi non autorizzati ai dati, mantenimento della privacy

Ma tutti sono collegati ad Internet, non può essere così rischioso!

Il numero di utenti di Internet ha raggiunto dei livelli di tutto rispetto. Secondo Internet World Stats (www.internetworldstats.com/stats.htm), mentre a marzo 2009 erano nel mondo più di 1,5 miliardi, a giugno 2012 erano diventati più di 2,4 miliardi (si veda la tabella inserita nella prima versione di questo IBUQ).

Dati 2012

	Popolazione (Stima 2012	Utenti Internet (Fine 2000)	Utenti Internet (metà 2012)	Penetrazione (% popolaz,)	Variaz. utenti 2000-2012	Utenti %
Africa	1.073.380.925	4.514.400	167.336.676	15,6 %	3.606,7 %	7,0 %
Asia	3.922.066.987	114.304.000	1.076.681.059	27,5 %	841,9 %	44,8 %
Europa	820.918.446	105.096.093	518.512.109	63,2 %	393,4 %	21,5 %
Medio oriente	223.608.203	3.284.800	90.000.455	40,2 %	2.639,9 %	3,7 %
America del Nord	348.280.154	108.096.800	273.785.413	78,6 %	153,3 %	11,4 %
America latina	593.688.638	18.068.919	254.915.745	42,9 %	1.310,8 %	10,6 %
Oceania / Australia	35.903.569	7.620.480	24.287.919	67,6 %	218,7 %	1,0 %
TOTALE	7.017.846.922	360.985.492	2.405.518.376	34,3 %	566,4 %	100,0 %

Certo è che Internet oggi è diverso da com'era alle sue origini. Nato per applicazioni militari, cresciuto nel mondo della ricerca e dell'università, Internet ha oggi una vocazione essenzialmente commerciale. E' diventato lo strumento per eccellenza di diffusione di informazioni e di comunicazione, cambiando anche radicalmente il modello economico di diversi servizi: inviare un milione di lettere per posta ha un costo elevatissimo; inviare un milione di messaggi di posta elettronica ha un costo pressoché nullo. Internet rappresenta quindi una platea di 2,4 miliardi di potenziali clienti.

Dati 2009

	Popolazione (Stima 2008)	Utenti Internet (Fine 2000)	Utenti Internet (Inizio 2009)	Penetrazione (% popolaz,)	Variaz. utenti 2000-2008	Utenti %
Africa	975.330.899	4.514.400	54.171.500	5,6 %	1.100,0 %	3,4 %
Asia	3.780.819.792	114.304.000	657.170.816	17,4 %	474,9 %	41,2 %
Europa	803.903.540	105.096.093	393.373.398	48,9 %	274,3 %	24,6 %
Medio oriente	196.767.614	3.284.800	45.861.346	23,3 %	1.296,2 %	2,9 %
America del Nord	337.572.949	108.096.800	251.290.489	74,4 %	132,5 %	15,7 %
America latina	581.249.892	18.068.919	173.619.140	29,9 %	860,9 %	10,9 %
Oceania / Australia	34.384.384	7.620.480	20.783.419	60,4 %	172,7 %	1,3 %
TOTALE	6.710.029.070	360.985.492	1.596.270.108	23,8 %	342,2 %	100,0 %

Ma non solo di potenziali clienti. Anche di potenziali bersagli di truffe, attacchi, tentativi di spionaggio, di furti di identità, ecc ... La malversazione non è certo nata con Internet, che è soltanto uno strumento di scambio di informazioni ma che per via della sua diffusione ne diventa un canale in grado di amplificarne gli effetti e la portata. Con un numero tale di potenziali bersagli, si può facilmente immaginare che vi sia un numero significativo di attaccanti.

E' di fondamentale importanza adoperare tutte le cautele, mettere in pratica tutte le precauzioni e attivare tutti i sistemi di protezione necessari per ridurre il più possibile i rischi provenienti dalla rete. Collegarsi in rete vuol dire accedere alle sue risorse e ai server che le contengono ma vuol dire anche che dalla rete è possibile accedere al nostro personal computer o direttamente o trasmettendo file in grado di impadronirsi di parte delle funzionalità del nostro personal computer a scopo malevolo.

Sì ma gli attacchi sono rivolti ai server di Internet, alle grandi organizzazioni, non alla mia rete di casa!

Sbagliato! leggete la notizia.

I principali rischi che si corrono collegandosi in rete (non necessariamente Internet, anche una rete locale) sono:

- *ricevere malware*. Il malware è uno dei principali pericoli che possono colpire un sistema informatico. E' l'estensione di quanto una volta veniva chiamato virus. Con il dilagare delle infezioni e degli attacchi in ambito informatico, si usa il termine malware per indicare tutti i programmi dannosi (virus, worm, keylogger, per citare il nome di tre di essi) che si installano all'insaputa dell'utente e arrecano danni al personal computer, ai dati e all'utente stesso. I vari tipi di malware verranno approfonditi al successivo punto 2.1.1.
- *accessi non autorizzati ai dati presenti sul personal computer*. Un sistema poco protetto potrebbe consentire ad esterni di accedere indebitamente tramite la rete a dati presenti sui vari dispositivi di memorizzazione del personal computer. Un computer mal configurato, che per esempio condividesse dei dati con gli altri computer della rete di casa, potrebbe condividerli anche con utenti indesiderati al momento in cui lo si collegasse ad un'altra rete. Oppure un router mal configurato, come visto nella notizia.
- *violazione della privacy*. Fra i dati soggetti ad accesso indesiderato possono naturalmente esserci dati personali o addirittura dati sensibili riguardanti il possessore del personal computer o altri. Non ultimi, anche dati che possono interessare molto i malintenzionati come la cronologia, conservata dal browser, delle pagine web consultate, oppure il file nel quale, presi dalla disperazione per le innumerevoli password da ricordare, si inseriscono tutte le credenziali di autenticazione (codice utente e password) che ci consentono di accedere a tutti i servizi e siti Internet (e-banking, e-commerce, mail, ...).

Come vedremo, questi rischi possono anche avere altre origini, senza richiedere necessariamente di essere collegati in rete. Il malware può arrivare tramite chiavetta USB, i dati possono essere rubati in un momento in cui lasciamo il computer incustodito e non protetto ma sicuramente gli attacchi tramite rete rappresentano un fenomeno consistente.

Ma in che modo ci si connette ad una rete?

Riconoscere le possibilità di connessione ad una rete mediante cavo o wireless

Esistono oggi due modalità principali di connessione in rete: tramite cavo (modalità wired) o tramite onde radio (modalità wireless o Wi-Fi). L'estrema diffusione del portatili e dei dispositivi mobili (smartphone, tablet), tutti previsti per collegarsi in modalità Wi-Fi, potrebbe far pensare che quest'ultima modalità sia quella standard da sempre.

Va ricordato che i primi personal computer (stiamo parlando dell'inizio degli anni '80) non erano collegati in rete. I primi collegamenti in rete sono avvenuti via cavo e per numerosi anni questa è stata l'unica modalità disponibile. Successivamente, con l'avvento dei computer portatili, si è diffuso il collegamento Wi-Fi.

Il collegamento tramite cavo presenta il vantaggio della maggior sicurezza (richiede di collegare fisicamente il computer alla rete accedendo quindi ai locali, rendendo più difficile un'intrusione) e della maggior velocità di trasmissione. Presenta in compenso l'inconveniente del maggior costo di installazione dovuto alla necessità di posare metri o chilometri di cavi di connessione e di effettuare opere murarie. E' usato in prevalenza nella realizzazione delle reti cablate aziendali.

Il collegamento Wi-Fi ha il vantaggio del minor costo di realizzazione della rete e della immediatezza di collegamento di tutti i dispositivi mobili (portatile, tablet, smartphone) e quindi della facilità di uso in mobilità. Presenta in compenso un livello di sicurezza molto minore in quanto vi si può accedere senza essere presente nei locali ma soltanto nelle vicinanze. Spesso una rete aziendale si estende fuori dai muri dell'azienda stessa e tutti gli utenti di un portatile avranno osservato il numero di reti che vengono segnalate, appartenenti ai vicini. Nelle reti domestiche è la modalità prevalentemente utilizzata, per ovvi motivi di praticità (e forse minore sensibilità al tema della sicurezza).

E' sempre più frequente l'uso delle reti wireless, in casa, in azienda o in spazi pubblici. In casa, il modem che assicura il collegamento a Internet gestisce anche una rete senza Wi-Fi, alla quale si collegano prevalentemente personal computer. In azienda, le postazioni di lavoro sono desktop collegati via cavo alla rete ai q2uali si aggiungono reti Wi-Fi nei casi in cui si utilizzano computer portatili e/o smartphone o tablet. Negli spazi pubblici e in condizioni di mobilità (treno, metro, ...) si incontrano prevalentemente dispositivi mobili (smartphone, tablet, ...).

Riconoscere diversi tipi di sicurezza per reti wireless, quali WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected Access), MAC (Media Access Control)

La maggior facilità di collegamento ad una rete Wi-Fi implica una maggior facilità di intercettazione dei dati. Di conseguenza esistono diversi sistemi di sicurezza (o di insicurezza) nelle reti Wi-Fi che, in qualche modo si sono susseguiti nel tempo. Le prime reti Wi-Fi installate erano spesso non protette: era frequente potersi collegare senza formalità al segnale radio di numerose reti. Tant'è che era nata un'attività denominata *wardriving* consistente nel passeggiare per strada con un portatile per individuare reti Wi-Fi non protette per poi censirle inserendo la loro posizione in appositi siti web. il tutto all'insaputa del legittimo proprietario, impresa o privato, della rete.

La coscienza dei rischi e della necessità di protezione ha portato all'inserimento di sistemi di controllo degli accessi, di crittografia e alla quasi scomparsa delle reti a libero accesso.

Si distinguono diversi tipi di reti wireless, a seconda delle restrizioni di accesso e del grado di sicurezza:

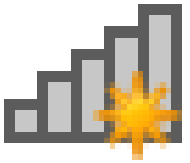
- *aperta*, ossia accessibile a tutti, senza nessuna misura restrittiva. Ci si può collegare addirittura senza password
- *protetta*, ossia resa più sicura da un sistema di crittografia e chiave di sicurezza (password) quale:
  - WEP (Wired Equivalent Privacy), oramai obsoleto e sempre meno diffuso per la sua scarsa sicurezza
  - WPA (Wi-Fi Protected Access) è stato sviluppato per sostituire il sistema WEP, poco sicuro
  - WPA 2 è un'evoluzione di WPA destinata anche qui ad aumentare il livello di sicurezza.

Per aumentare la sicurezza, si può completare i sistemi di autenticazione e crittografia appena visti con un controllo hardware dei computer che si collegano. Ogni scheda di collegamento in rete (wired o wireless) di ogni computer dispone di un cosiddetto indirizzo fisico, detto indirizzo MAC (Media Access Control Address), ossia di un numero che la identifica univocamente a livello mondiale. Un esempio di MAC Address può essere *00:23:32:3e:d5:b9*. Nelle imprese, spesso si censiscono i MAC Address dei computer autorizzati ad accedere alla rete wireless e si configurano i dispositivi di accesso in modo da accettare collegamenti solo dai computer che risultano nella lista. Così facendo, anche se si dispone della password della rete, il sistema non permette il collegamento di computer estranei.

Non fatelo a casa! Non modificate le impostazioni del router che vi assicura il collegamento in rete, tranne se siete sicuri di quello che fate.

E' quindi importante che sia previsto un sistema di cifrature dei dati trasmessi, in modo che chi dovesse riuscire ad inserirsi nella rete non riesca a leggere i dati scambiati, ma questo deve essere preceduto da un sistema di autenticazione che permetta l'accesso alla rete solo a chi dispone della password.

Riconoscere l'importanza di richiedere una password per proteggere gli accessi a reti wireless

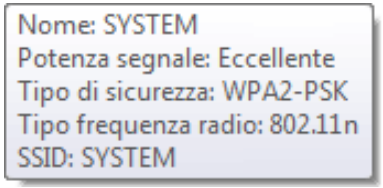


Come visto, le reti wireless non necessitano del collegamento fisico o della presenza nell'edificio per potersi collegarsi. Di conseguenza, una rete senza password consente un facile accesso a eventuali malintenzionati senza che il possessore della rete se ne accorga. Solo un'analisi specifica, non facile in caso di rete di grandi dimensione, potrebbe individuare il collegamento abusivo.

E' pertanto molto importante non attivare, in azienda o in casa, una rete Wi-Fi senza assegnare una password di accesso. Ma l'assenza di password può verificarsi anche nel caso contrario in cui siamo noi a voler acceder ad una rete.

Essere consapevoli che usando una rete wireless non protetta si rischia che i propri dati vengano intercettati da "spie digitali"

Anche se i metodi di protezione degli accessi alle reti wireless sono semplici da attivare e sempre più sicuri, esistono ancora delle reti wireless che non sono protette. Il fatto che siano sempre più rare può far pensare che non tutti quelli che le attivano abbiano intenzioni benevoli ...



E' quindi importante conoscerne i rischi che si corrono collegando un computer ad una rete wireless non

protetta.

Vanno considerati alcuni aspetti:

- rete aperta significa rete accessibile a tutti, compresi i crackers (vedere il punto 1.1.3) o malintenzionati che intendono usarla in modo improprio
- se il computer che utilizzate non è configurato correttamente, alcuni dati presenti sul disco possono risultare condivisi ossia visibili a tutti gli utenti collegati in rete
- se il computer che utilizzate non è protetto, anche se non condividete nessuna cartella esplicitamente, potreste essere oggetto di un attacco che danneggia o sottrae alcuni dei vostri dati
- chi dice collegamento ad una rete wireless dice spesso trasmissione o scambio di dati in rete. Anche se il vostro computer è protetto, potrebbero essere intercettati da malintenzionati non i dati presenti nel vostro computer ma quelli che trasmettete o ricevete durante il collegamento.

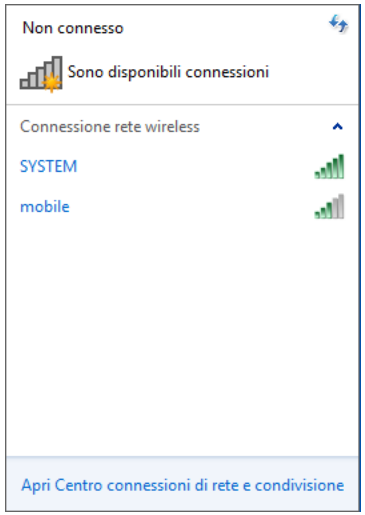


Figura 1: Reti Wi-Fi disponibili

In sintesi, anche se alcuni rischi esistono collegandosi a reti protette, sono molto maggiori i rischi di intercettazione e furto di informazioni collegandosi a reti non protette.

Non si vuole spaventare il lettore demonizzando le reti wireless aperte, che hanno sicuramente contribuito alla diffusione di Internet e alla riduzione dell'ignoranza informatica. Lo si vuole semplicemente sensibilizzare sull'esistenza di rischi e sulla necessità di configurare correttamente il proprio computer per raggiunge un livello accettabile di sicurezza. Occorre quindi non accontentarsi di essere un semplice utente ma è utile *saperne di più*.

Connettersi ad una rete wireless protetta/non protetta.

Il collegamento ad una rete wireless è facilitato dal fatto che il personal computer ricerca le reti disponibili e ne visualizza il nome.

Per collegarsi ad una rete Wi-Fi, occorre:

- cliccare sull'icona delle reti Wi-Fi presente nell'Area di notifica
- nella finestra che compare (Figura 1) sono elencate tutte le reti disponibili
- fare click sul nome della rete desiderata e sul pulsante *Connetti* (Figura 2)

- se la rete è protetta, viene chiesto di inserire la password (Figura 3)
- al termine, è stabilito il collegamento con la rete Wi-Fi.

Con l'aumento della diffusione di Internet, diventa sempre più facile entrare in contatto con persone con le quali altrimenti non si sarebbe mai comunicato. Aumenta naturalmente il rischio che tali persone siano malintenzionate e approfittino dell'immediatezza offerta dallo strumento informatico per commettere qualche reato a danno dell'utente sprovveduto.

E' importante d'altro canto non demonizzare Internet né pensare che sia la causa dei reati che vengono perpetrati per il suo tramite. Internet è solo uno strumento di comunicazione, Così come altri strumenti tecnologici sono stati utilizzati per delinquere quando sono nati (telefono, cassette video, ...) anche Internet viene adoperato agli stessi fini. Truffe e raggiri esistevano ben prima di Internet, così come le prepotenze, le molestie e la diffusione di contenuti proibiti dalla legge.

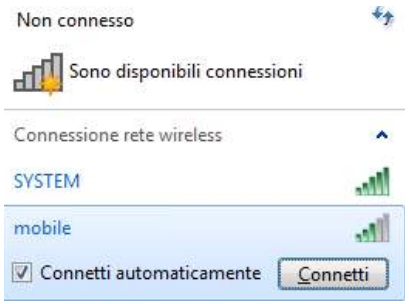


Figura 2: Connessione alla rete Wi-Fi

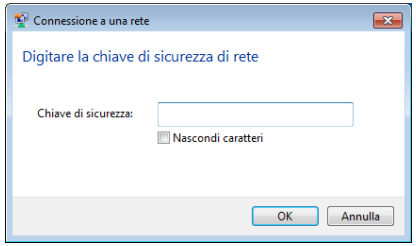


Figura 3: Inserimento della password

Comprendere i rischi potenziali durante l'uso di siti di reti sociali, quali cyberbullismo, adescamento, informazioni fuorvianti/pericolose, false identità, link o messaggi fraudolenti

Ma proprio perché Internet è qualitativamente e quantitativamente più significativo di altri strumenti, è importante conoscere i principali rischi legati all'attività in rete e stare in guardia. I rischi dell'attività in rete non vanno né esagerati né trascurati. Possono essere così esemplificati:

- *cyberbullismo*. Possiamo citare la definizione che *Telefono Azzurro* fornisce del bullismo e del cyberbullismo (www.azzurro.it):

Per bullismo si intendono tutte quelle azioni di sistematica prevaricazione e sopruso messe in atto da parte di un bambino/adolescente, definito "bullo" (o da parte di un gruppo), nei confronti di un altro bambino/adolescente percepito come più debole, la vittima ... Quando le azioni di bullismo si verificano attraverso Internet (posta elettronica, social network, chat, blog, forum), o attraverso il telefono cellulare si parla di cyberbullismo.

Questa definizione va purtroppo estesa anche ai giovani e agli adulti. Caratteristiche del comportamento sono la prevaricazione e il sopruso sistematici e ripetuti. Adoperando mezzi tecnologici di tipo sociale il comportamento può essere reiterato nel tempo e a distanza, con danni ancora più gravi.

- *adescamento*. Tramite le reti sociali, in cui è facile sia nascondere la propria identità sia crearne una finta, i minori - e non solo - sono soggetti a pratiche di adescamento, ossia comportamenti da parte di malintenzionati che cercano di entrare in confidenza con una persona e carpirne la fiducia per coinvolgerli in comportamenti non appropriati. E' un comportamento tipico della pedofilia.
- *informazioni fuorvianti/pericolose*. La pubblicazione di informazioni false, fuorvianti o ingannevoli, per esempio tramite la creazione di appositi siti tematici con possibilità di scaricamenti gratuiti o promesse di premi, può essere un primo strumento messo in opera da chi intende compiere atti di adescamento online o di cyberbullismo, oltre che di frode.
- *false identità*. Per le stesse finalità, possono essere create false identità, complete di tutti i dettagli che caratterizzano quelle vere. Una volta inserita nel profilo di una rete sociale, diventa quasi impossibile distinguerla da un'identità reale. Esistono addirittura siti che permettono di crearne una casualmente, ovviamente assolutamente falsa, scegliendo il paese, il sesso e altre informazioni di base.
- *link o messaggi fraudolenti*. Così come possono arrivarci tramite e-mail, i vari attacchi dei criminali informatici possono anche essere nascosti dietro link che rinviano a pagine web create ad hoc dal criminale informatico. Si parlerà di phishing, di spam, di attacchi basati sull'ingegneria sociale o di altri comportamenti che mirano all'appropriazione indebita di informazioni, tutti temi oggetto di questo IBUQ.

La rete garantisce un elevato livello di anonimato e permette facilmente di assumere le sembianze o l'identità di un'altra persone, anche completamente diversa. E' facile spacciarsi per una persona di aspetto, età o sesso nonché di residenza o nazionalità diversi da quelli reali.

E' quindi importante, se non si conosce effettivamente la persona, non dare per scontato che le

caratteristiche dichiarate siano quelle effettive. Occorre prestare un'attenzione ancora maggiore alle sue intenzioni che non necessariamente sono quelle dichiarate ma possono invece essere più pericolose. E quindi evitare i rischi che possono presentarsi nel passare da una conoscenza virtuale, tramite la rete, ad una conoscenza basata su incontro personale.

Quale utilizzatore di Internet non ha mai ricevuto un messaggio di *spam*, posta elettronica non richiesta, che annunciava che un principe nigeriano decaduto aveva scelto proprio lui per omaggiarlo del suo tesoro di qualche milioni di dollari? Per non parlare di investimenti finanziari senza rischio e ad altissimo rendimento o di proposte di altro genere ma sempre vantaggiosissime per il destinatario della proposta. Ma di questi aspetti parleremo al successivo punto 5.1.4.

Siamo certi che non vi siete lasciato spaventare da questi rischi!

Abbiamo già illustrato il valore che hanno le nostre informazioni e l'esistenza di rischi connessi al furto di dati personali o di malintenzionate "spie digitali" che cercano proprio di impadronirsene. Ma bisogna anche evitare di facilitare loro il lavoro. Non vogliamo farci rubare i nostri dati personali ma non dobbiamo nemmeno regalarli al ladro. Fatto che accade molto frequentemente nelle reti sociali.

E' molto in uso pubblicare le foto delle vacanze in tempo reale. Magari con un testo di accompagnamento.

Testo assolutamente innocuo: "Siamo pallidi da far paura ma dopo tre settimane di sole, vedrete il risultato! Un saluto dalla spiaggia da parte di tutta la famiglia.". Sottinteso: la casa è vuota per tre settimane.

Manca solo un altro messaggio dopo qualche giorno del tipo: "Paola, ricordati di andare a bagnare le piante! E non fare suonare l'antifurto (12345) come la volta scorsa.".

A me non capita! Può darsi, ma le reti sociali sono una miniera di informazioni fra le quali se ne trovano di inutili, personali, sensibili, riservate ...

Comprendere l'importanza di non divulgare informazioni riservate su siti di reti sociali

La partecipazione a una comunità virtuale e/o a una rete sociale spesso fornisce l'impressione di essere all'interno di un circuito protetto a cui possono accedere solo i nostri amici: questo può spingere le persone a rivelare molte informazioni, anche private, su di sé. Così come nella vita reale, anche in rete gli individui possono intendere le amicizie a diversi livelli, e così come possono nascere possono concludersi. Non va inoltre dimenticato che qualsiasi cosa scritta o pubblicata in rete non potrà mai essere cancellata: infatti anche se si cancella quella frase scritta in un momento di rabbia o quella foto imbarazzante, qualcuno potrebbe averla nel frattempo già copiata su un altro server, rendendone molto difficile il reperimento o il controllo della diffusione.

Le reti sociali offrono un accesso gratuito ai propri servizi perché utilizzano le informazioni che ognuno fornisce a scopo di marketing: dichiarare le proprie preferenze o quali acquisti sono stati fatti serve per favorire la diffusione del passaparola che è considerato oggi il modo più efficiente di fare marketing in rete. Alcuni ricercatori hanno inoltre effettuato degli studi per cui l'esplicitazione delle proprie amicizie favorisce lo svelamento automatico e incontrollato anche di informazioni sui nostri amici. Oggi si tende a partecipare a molte reti, e a volte si ha l'impressione di non riuscire a gestirle in modo ottimale: dopo il sovraccarico cognitivo (troppe informazioni equivalgono a nessuna informazione), siamo giunti al sovraccarico da social network.

Di conseguenza va prestata la massima attenzione alle informazioni che si inseriscono - e quindi si fanno diventare di pubblico dominio - sui siti di reti sociali. In particolare va assolutamente evitato di divulgare dati riservati quali credenziali di autenticazione (utente e password), codici di accesso, PIN della carta di credito o del Bancomat (è vero che divulgate soltanto il PIN, che da solo non ha nessun valore, ma magari il ladro si è procurato il numero della carta tramite altri canali). Vanno inoltre tenuti riservati dati quali idee politiche, credenze religiose, orientamenti sessuali ... quelli per esempio che la normativa italiana identifica come dati sensibili. Oltre naturalmente quelli di carattere economico, finanziario o legati alla propria attività lavorativa o relativi al proprio datore di lavoro.

Possono quindi essere utili alcuni suggerimenti per utilizzare le reti sociali e non esserne travolti:

- chiaritevi le idee sul perché iscrivervi e a cosa vi serve
- una volta scelto i network considerati interessanti, cercate di usarli per lo scopo con cui vi siete iscritti, onde evitare di duplicare le informazioni

- definite i vostri confini di utilizzo: se usate Facebook per il tempo libero e Linkedin per i contatti professionali, gestite le richieste di contatto in modo opportuno
- leggete bene le clausole relative alla privacy e al copyright, è sempre meglio essere informati in anticipo.

Comprendere il termine messaggistica istantanea (IM) e i suoi usi

L'*instant messaging* (IM) o messaggistica istantanea può essere visto come un incrocio fra posta elettronica in tempo reale e trasposizione su Internet degli SMS. E' un servizio di comunicazione centralizzato, che permette lo scambio in tempo reale di messaggi di testo fra due o più utenti, previa registrazione presso un fornitore per l'assegnazione di un nome utente e di una password. Diversi servizi gratuiti sono disponibili, come Skype che integra questa funzionalità nel software di telefonia. Al momento dell'accesso al servizio, viene visualizzato l'elenco dei propri contatti che sono collegati in questo momento e con i quali si può comunicare.

Le caratteristiche salienti del servizio di instant messaging sono:

- lo scambio di messaggi testuali
- la comunicazione in tempo reale
- la possibilità di inviare file
- l'estensione a più partecipanti, sotto forma di chat
- la memorizzazione del testo delle conversazioni effettuate
- l'integrazione eventuale con altri sistemi di comunicazione (VoIP, e-mail, ...)
- il costo pressoché nullo.

Naturalmente il sistema richiede la presenza in linea dei corrispondenti. Si tratta di un mezzo di comunicazione che presenta dei limiti nel caso in cui i corrispondenti siano separati da fusi orari molto diversi, in qual caso si privilegia la posta elettronica, rinunciando ad un'interazione in tempo reale. L'IM si sta diffondendo in modo significativo in ambito lavorativo, per le comunicazioni a livello nazionale ed internazionale. E' sempre più frequente, sia per il VoIP, sia per l'IM vedere sui biglietti da visita o sulla carta intestata, oltre al numero di telefono e all'indirizzo e-mail, anche l'identificativo Skype.

La messaggistica istantanea è un servizio nato per scambiarsi (brevi) messaggi di testo. Successivamente, si è arricchita di funzionalità con la possibilità di inserire link a siti web e di inviare file, diventando simile alla posta elettronica in quanto a rischi per la sicurezza.

Comprendere le vulnerabilità di sicurezza della messaggistica istantanea, quali malware, accesso da backdoor, accesso a file

I rischi che si corrono nella messaggistica istantanea sono principalmente i seguenti:

- i file che si ricevono possono contenere malware
- alcuni malware adoperano lo stesso programma di messaggeria per propagarsi ai contatti della rubrica
- così come nella posta elettronica, si possono ricevere messaggi non richiesti (spam) fraudolenti e/o rinviare a siti web pericolosi
- molti programmi di messaggeria istantanea inviano il testo del messaggi in chiaro, facilitandone così l'intercettazione, a scapito della privacy dell'utilizzatore.

La protezione dei dati da furto o da accessi indesiderati è impegnativa dal punto di vista organizzativo e ha un costo. Inoltre può capitare che dati registrati su supporto magnetico, memorie di massa o dispositivi vari non siano più utili: si pensi a vecchie copie di sicurezza o ad archivi molto vecchi e ormai obsoleti. Anche se ormai la capacità dei dispositivi di memorizzazione è tale da non dover liberare spazio per far posto a nuovi dati, può essere opportuno eliminare i dati ormai inutili dai dispositivi di memorizzazione.

Comprendere il motivo per eliminare in modo permanente i dati dalle memorie di massa o dai dispositivi

In questo modo, si semplifica la gestione delle procedure di sicurezza e se ne riduce l'onere. Tale eliminazione può riferirsi a:

- interi supporti: si pensi ad un CD-ROM non riscrivibile
- il contenuto di un intero dispositivo: per esempio, quello di un CD-ROM riscrivibile o di una chiavetta USB
- una cartella: rimuovendo quindi tutte le sotto-cartelle e i file in essa contenuti
- un singolo file: tramite il sistema operativo
- un singolo elemento di un'applicazione: per esempio un messaggio di posta elettronica, cancellato tramite il programma che lo ha creato.

Per non parlare del caso più drastico ma frequente di sostituzione di un personal computer e di vendita o donazione o rottamazione di quello vecchio. Non vorremo certo lasciare sul disco i dati riservati dell'azienda!

Distinguere tra cancellare i dati e distruggerli in modo permanente

Per venir incontro all'utente "distratto" o offrirgli la possibilità di un ripensamento, tutti i sistemi operativi e alcune applicazioni prevedono la presenza del Cestino. Con questa funzionalità, cancellare un elemento non vuole dire distruggerlo ma spostarlo in una cartella particolare, il Cestino. Il file non è più visibile nella sua posizione originaria ma è facilmente recuperabile, in caso di necessità, dalla cartella del Cestino. E' recuperabile fintantoché non lo si cancella dal Cestino o si svuota globalmente il Cestino. Da questo momento, l'elemento cancellato non è più recuperabile dall'utente "distratto" che lo ha cancellato involontariamente.

Ma non si può dire lo stesso che sia stato distrutto in modo permanente. Il contenuto del o dei file cancellati potrebbe infatti, sotto certe condizioni, essere ancora recuperato. Questo perché il sistema operativo non elimina dal disco le informazioni contenute nel file cancellato ma elimina soltanto il riferimento al file dall'indice del disco. Così facendo, lo spazio che il file occupava su disco risulta libero e nuove informazioni

Capitolo 3 – Come vengono sottratti illecitamente i dati

Riferimento Syllabus 1.1.3	***Comprendere la differenza tra hacking, cracking e hacking etico.***
Riferimento Syllabus 1.3.4	***Identificare i metodi applicati per il furto di identità, quali acquisire informazioni a partire da oggetti e informazioni scartati, fingendosi qualcun altro o mediante skimming.***
Riferimento Syllabus 2.1.1	***Comprendere il termine malware.***
Riferimento Syllabus 2.1.2	***Riconoscere diversi modi con cui il malware si può nascondere, quali trojan, rootkit e backdoor.***
Riferimento Syllabus 2.2.1	***Riconoscere i tipi di malware infettivo e comprendere come funzionano, ad esempio virus e worm.***
Riferimento Syllabus 2.2.2	***Riconoscere i tipi di malware usati per furto di dati, profitto/estorsione e comprendere come operano, ad esempio adware, spyware, botnet, keylogger e dialer.***
Riferimento Syllabus 4.1.3	***Essere consapevoli del pharming.***
Riferimento Syllabus 5.1.4	***Essere consapevoli della possibilità di ricevere messaggi fraudolenti e non richiesti.***
Riferimento Syllabus 5.1.5	***Comprendere il termine phishing. Identificare le più comuni caratteristiche del phishing, quali uso del nome di aziende e persone autentiche, collegamenti a falsi siti web.***
Riferimento Syllabus 5.1.6	***Essere consapevoli del rischio di infettare il computer con malware attraverso l'apertura di un allegato contenente una macro o un file eseguibile.***
Contenuti della lezione	***In questa lezione vedremo: la differenza fra hacker e cracker, i metodi usati nel furto di identità, gli attacchi ad opera del malware, phishing, pharming e altri pericoli.***

Comprendere la differenza tra hacking, cracking e hacking etico

Purtroppo, anche se i giornali sono ghiotti di queste informazione, non sempre hanno una visione univoca o completa dei fenomeni che caratterizzano l'informatica e la sicurezza informatica, in particolare se coinvolgono temi legati al software libero e Open Source e alle comunità degli sviluppatori. Un tema spesso oggetto di confusione è quello della figura dei cosiddetti hacker e cracker. Alcuni testi di base disponibili su Internet ci vengono in aiuto per comprenderne la natura e le differenze.

Il *Jargon File* (http://www.catb.org/jargon/), l'approfondito compendio del gergo degli hacker che illustra numerosi aspetti della tradizione, del folklore e dell'umorismo degli hacker, ci spiega che un hacker è:

> *Una persona a chi piace esplorare i dettagli dei sistemi programmabili e scoprirne i limiti, contrariamente a molti utenti che preferiscono imparare soltanto il minimo indispensabile. Il Glossario degli Utenti di Internet (RFC1392) approfondisce: Una persona che si diverte ad acquisire una profonda conoscenza dei dettagli di funzionamento di un sistema, in particolare computer e e reti di computer.*

L'hacking è quindi l'attività svolta dagli hacker che, volendola restringere all'ambito informatico, consiste nello studiare in modo approfondito le caratteristiche tecniche dei sistemi di computer, utilizzarli e sperimentarne le funzionalità, con l'obiettivo di individuarne i limiti e i difetti fino al punto di essere in grado di modificarli e migliorarli. Oggi, tutti i sistemi informatici sono - ad un livello variabile - protetti in modo da riservarne l'accesso ai soli utenti autorizzati. Di conseguenza, una parte importante dell'attività dell'hacker è dedicata ai sistemi di accesso in modo da poter accedere al sistema che vuole studiare anche se questo è protetto. E' naturalmente su questo tema che i crea la confusione nel mondo dei giornalisti e nell'opinione pubblica.

Diversa è l'attività di cracking. In prima battuta il cracker, familiarmente chiamato *black hat (*cappello nero), in contrapposizione a *white hat* (cappello bianco) che si riferisce all'hacker etico, potrebbero essere definito come un hacker malevolo, che ha per obiettivo di intromettersi in un sistema con lo scopo di compiere un crimine informatico: per esempio distruggere dati o rubarli, appropriarsi dati indebitamente tramite l'uso dei sistema sostituendosi all'utente autorizzato., .. Su un altro piano, a chi non è mai capitato di sentir dire "Ho craccato il videogioco" oppure "Ho craccato il codice, la password, ..."? Attività molto modesta che non richiede competenze particolari se non cercare su Internet una password o un codice pubblicato da qualcuno.

Per spiegare la differenza fra un hacker e un cracker, possiamo usare le parole di Eric Raymond, uno dei guru del software libero e Open Source, che nel suo interessantissimo articolo How To Become A Hacker (Come diventare un Hacker), disponibile all'indirizzo http://catb.org/~esr/faqs/hacker-howto.html sintetizza con:

The basic difference is this: hackers build things, crackers break them.

Questa affermazione "La differenza principale è questa: gli hacker costruiscono cose, i cracker le rompono" aiuta proprio a capire lo spirito e l'etica hacker e cosa li differenzia dai cracker.

Si parla di hacking etico a proposito di attività svolta da hacker sotto forma di attacco vero e proprio ad un sistema informatico, in accordo con il suo proprietario, per analizzarne il livello di sicurezza ed individuare eventuali falle o debolezze. Scopo dell'attività è quello di raccogliere informazioni utili per rafforzare la sicurezza del sistema. Il fenomeno dell'hacking etico è diffuso in vari paesi nel mondo (http://www.ilsole24ore.com/art/tecnologie/2013-01-06/sono-hacker-etico-proteggero-081411.shtml?uuid=Ab5XhhHH) e anche in Italia dove Raoul Chiesa ne è uno dei maggiori esponenti (http://www.mediamente.rai.it/mm_it/010307/chiesa.asp).

Il furto d'identità, tema che abbiamo introdotto al precedente punto 1.3.3, può colpire gli individui come le organizzazioni. Vediamo qui i principali metodi applicati per il furto di identità e questi valgono per tutti: imprese, enti privati o pubblici e organismi vari, con conseguenze di portata considerevole.

Identificare i metodi applicati per il furto di identità, quali acquisire informazioni a partire da oggetti e informazioni scartati, fingendosi qualcun altro o mediante skimming

Il furto di identità si basa sull'acquisizione di informazioni di vario genere sulla persona.

Nel caso di furto dell'identità amministrativa, le tecniche maggiormente utilizzate sono il furto di documenti (carta di identità, patente, passaporto, ...) , il furto di corrispondenza, non solo quello della posta elettronica ma anche quella della posta tradizionale. Il furto di corrispondenza nella buca delle lettere può fornire molte informazioni personali soprattutto per l'ingegnere sociale (vedere punto 1.3.1) per esempio carte di credito, estratti conti bancari, fatture, bollette.

Ultimo ma non meno importante, anche perché spesso insospettato dalla persona "sotto attacco", il *dumpster diving* (Figura 4). Sotto questo termine inglese, dalla parvenza tecnico-scientifica (oppure sportiva), si nasconde una tecnica che non ha niente di scientifico e nemmeno di informatico. Consiste nel frugare nella spazzatura in cerca di oggetti o documenti in grado di fornire informazioni su una persona. Si trovano spesso per esempio estratti conti bancari, estratti carte di credito, fatture.

La Notizia

6 ottobre 2008

I quotidiani francesi *Le Figaro* e *Le Nouvel Observateur* commentano i risultati di un'indagine del centro di ricerca Credoc (www.credoc.fr):
- *Furto di identità: le pattumiere sono una miniera d'oro* (Le Figaro)
http://www.lefigaro.fr/actualite-france/2008/10/04/01016-20081004ARTFIG00686-vols-d-identite-les-poubelles-sont-des-mines-d-or-.php

- *Imprese: questi segreti che si trovano nelle pattumiere* (Le Nouvel Observateur)
http://rue89.nouvelobs.com/2008/10/11/entreprises-ces-secrets-quon-a-trouves-dans-les-poubelles

In sintesi:
- 65% delle pattumiere delle imprese contiene almeno un documento confidenziale
- più del 50% di quelle degli enti privati contengono documenti finanziari
- 80% di quelle delle famiglie contiene un documento utile per il furto di identità
- 13% delle pattumiere contenevano tutte le informazioni utili per un furto di identità.

Nel caso di furto di identità digitale, l'obiettivo primario è carpire credenziali di autenticazioni o di autorizzazione. Per gli ATM (Automated Teller Machine), che usano carte di debito o carte di credito, assume particolare importanza lo *skimming*, tecnica fraudolenta che indica il recupero illegale di dati dalla banda magnetica di una carta, tramite duplicazione della carta. Per esempio, nel caso di prelievo di denaro, un dispositivo installato dal ladro legge la banda magnetica della carta quando viene inserita nel distributore (a volte anche nell'apri-porta del locale dove si trova il distributore). Successivamente, il PIN viene carpito o tramite una telecamera o tramite una tastiera falsificata o direttamente dal ladro osservando la digitazione dei numeri sulla tastiera. Anche se i casi di skimming si sono ridotti in seguito all'inserimento del chip sulla carta, vi sono ancora molti paesi in cui si fa largo uso della sola banda magnetica delle carte.

Trasversale a questi metodi, vanno tenuti in considerazione le tecniche già citate di ingegneria sociale spesso applicate in conversazioni telefoniche con l'ingegnere sociale che, grazie a informazioni rubate ad un terzo, si fa passare per qualcun altro ed è così in grado di ottenere informazioni riservate dal corrispondente.

Un altro metodo di attacco è quello basato sul *malware*. Il termine deriva dalle due parole inglese *malicious* e *software*. Letteralmente, significa programma malevole (e non malizioso come a volte si sente o si legge).

Comprendere il termine malware

Una volta si parlava di virus. Oggi, visto il dilagare di pericoli informatici che minacciano i computer in generale e il nostro personal computer in particolare, si è ampliato il concetto con il termine *malware.* Parlando di infezioni in ambito informatico, si userà quindi il termine malware per indicare tutti i programmi, installati senza il consenso dell'utente che hanno per scopo di arrecare danni al sistema informatico e all'integrità dei dati che gestisce. Spesso vengono classificati in base alle modalità di propagazione, al meccanismo di entrata in azione e all'azione che compiono.

Alla grande famiglia del *malware* in costante evoluzione appartengono, fra gli altri:

- *trojan*. Come il più famoso Cavallo di Troia (enorme cavallo di legno regalato dai Greci agli abitanti di Troia, all'interno del quale soldati greci si erano nascosti per entrare nella città) questi programmi si nascondono dentro programmi utili che l'utente installa (Figura 5)
- *rootkit*. Programmi molto pericolosi perché agiscono sul sistema operativo del PC e sono molto difficili da rimuovere perché spesso invisibili agli antivirus. Hanno prevalentemente il compito di nascondere altri malware in modo da renderli invisibili all'utente e al sistema operativo

Figura 6:

Figura 7:

Figura 6: Skimming: la tastiera autentica è coperta da una fasulla per ingannare il cliente
https://www.europol.europa.eu/content/image/b2-card-skimming-genuine-keypad-covered-fake-dupe-customer-839

Figura 7: Particolare dell'installazione di uno skimmer di carte in un ATM
https://www.europol.europa.eu/content/image/b3-part-criminal-card-skimmers-installation-atm-841

Figura 9:

Figura 8:

Figura 8: Un investigatore rimuove un dispositivo per lo skimming delle carte da un ATM.
https://www.europol.europa.eu/content/image/b1-investigator-peels-away-card-skimming-setup-front-genuine-atm-837

Figura 9: Dispositivi usati dai criminali nelle frodi con carte di pagamento e strumenti adoperati dalla polizia scientifica nelle indagini
https://www.europol.europa.eu/content/image/b4-payment-card-fraud-tools-used-criminals-well-forensic-support-tools-847

Fotografie riprodotte per gentile autorizzazione da EUROPOL European Police Office
https://www.europol.europa.eu/

- *backdoor*. E' une funzionalità, inserita nel computer all'insaputa dell'utilizzatore, che permette a terzi di accedere in modo nascosto al computer. Quando è presente una backdoor in un programma, questo può diventare un trojan, mettendo a disposizione di terzi le funzionalità del computer stesso.

A questi si possono aggiungere:

- virus. Il virus propriamente detto (Figura 10), una volta eseguito ha la caratteristica di infettare altri file in modo da riprodursi facendo copie di sé stesso, senza farsi identificare: la caratteristica saliente di un virus è quindi la capacità di replicarsi. I virus possono provocare danni al PC, arrivando fino a provocare la cancellazione di tutti i dati dal disco, ma non sono necessariamente maligni. Alcuni infatti non danneggiano il sistema infettato ma si limitano a produrre suoni e immagini fuori dal controllo dell'utente: appartengono comunque al malware perché si installano senza l'autorizzazione dell'utente e sono difficili da rimuovere. Il virus solitamente provoca danni quando è eseguito e si trova residente nella RAM: a questo punto inizia a riprodursi. Un virus è a tutti gli effetti un programma di dimensioni molto ridotte, per consumare poche risorse e rendersi invisibile: di solito colpisce file eseguibili, inserendosi fra le prime istruzioni, entrando in azione quando il programma infettato viene eseguito.
- *worm*. Modificano le impostazioni del sistema operativo per assicurarsi di venir eseguiti tutte le volte in cui l'utente accende il computer. Non infetta necessariamente file e si propaga sfruttando debolezze del sistema operativo o di programmi applicativi. Spesso sfrutta i contatti di posta elettronica presenti nella rubrica per propagarsi. su altri computer. Un caso famoso è avvenuto nel 2000 quando il worm ILOVEYOU (noto anche come Love Letter) ha colpito decine di milioni di computer basati su Windows, spedendo una mail avente per oggetto "ILOVEYOU" e per allegato un file LOVE-LETTER-FOR-YOU.txt.vbs che nadcondeva un programma dannoso scritto in Visual Basic. Il worm sfruttava una debolezza del programma di posta elettronica Microsoft Outlook, che apriva gli allegasti anche senza aprirli ma visualizzando solo il messaggio. I danni provocati da questo worm sono stati stimati in 5 miliardi di dollari.

L'infezione di un PC a causa di un malware avviene sempre per contagio esterno, occasionato da operazioni che l'utente del PC compie, in modo consapevole o inconsapevole. Anni addietro il principale veicolo di infezione da virus era l'utilizzo dei floppy disk. I programmi dannosi si trasferivano, spesso all'insaputa dei proprietari, da un dischetto all'altro e da un PC all'altro. Anche se oggi la stessa cosa è possibile scambiandosi altri supporti come le chiavette USB, il vero pericolo viene dalla diffusione della posta elettronica e dal web.

Essere consapevoli del rischio di infettare il computer con malware attraverso l'apertura di un allegato contenente una macro o un file eseguibile

Infatti uno dei modi più frequenti in cui si rischia di introdurre malware nel proprio personal computer e di diffonderlo agli altri, è la posta elettronica. Più precisamente l'infezione può avvenire tramite gli allegati ai messaggi.

Potendo allegare qualsiasi file ad un messaggio, a parte eventuali limitazioni imposte da alcuni sistema di posta elettronica, si rischia di ricevere fra i messaggi non desiderati degli allegati che contengono istruzioni eseguibili sul personal computer, suscettibili di arrecare danni. I due casi più frequenti sono:

- *file eseguibili*: contengono istruzioni, in linguaggio macchina o in altri linguaggi, che possono essere eseguite direttamente su un particolare sistema operativo. Nel caso di Windows, sono tipicamente file con estensione .exe (ma non solo). Come appena visto nel caso di ILOVEYOU, anche .vbs.
- *file contenenti macro*: come visto al punto 1.4.1, si tratta di documenti che oltre ai dati contengono anche delle istruzioni che possono essere eseguite, per esempio quando vengono aperti.

In tutti e due i casi le istruzioni potrebbero essere inserite proprio per introdurre qualche forma di malware all'interno del personal computer, in grado di arrecare danni di vario genere.

Purtroppo il livello di rischio è molto difficile da percepire da parte dell'utente non esperto: non solo la vulnerabilità dei programmi di posta elettronica è cambiata nel tempo e quindi dipende dalle versioni ma certi sitemi operativi sono meno attaccabili di altri o meno "accompagnati" di malware di altri: gli esperti segnalano un maggior numero di malware e una maggiore vulnerabilità dei sistemi operativi Windows rispetto a Linux o Mac OS X. Non solo ma file con estensione diversa da .exe possono contenere istruzioni eseguibili in Windows e, ultimo ma non meno grave, si può nascondere l'estensione dei file e farli sembrare innocui all'utente non esperto.

Per ridurre il rischio di infezione tramite allegati di mail,si possono seguire alcune linee guida quali:

- disporre di un programma antivirus, costantemente aggiornato che controlli anche la posta elettronica
- non aprire mai allegati, né salvarli su disco, che risultino visibilmente file eseguibili, anche se

(apparentemente) inviati da corrispondenti noti
- è buona norma non trasmettere per mail file eseguibili. E' frequente che gli ISP blocchino certi tipi di allegati, come quelli con estensione .exe o .zip
- se sussiste proprio l'esigenza di inviare o ricevere file di questo tipo, si consiglia di concordare con il destinatario o il mittente il sistema alternativo da adoperare
- se malgrado tutto ricevete un allegato sospetto e il vostro antivirus non controlla automaticamente la posta elettronica, effettuate esplicitamente una scansione dell'allegato.

E' sempre sconsigliabile aprire file allegati alle mail che arrivano da sconosciuti: i virus possono essere praticamente all'interno di qualsiasi tipologia di file. Purtroppo alcuni virus simulano anche che il messaggio arrivi da indirizzi della nostra rubrica. Non vanno sottovalutati anche altri sistemi di comunicazione come i sistemi di messaggeria istantanea: i virus sono in grado di assumere l'identità dei vostri amici e invitarvi a visitare dei link che infetteranno il vostro PC. Altre indicazioni sono illustrate al successivo punto 5.1.4.

Riconoscere i tipi di malware usati per furto di dati, profitto/estorsione e comprendere come operano, ad esempio adware, spyware, botnet, keylogger e dialer

Come abbiamo visto, alcuni tipi di malware mirano ad arrecare danni alle funzionalità del computer, modificandone le impostazioni, oppure ad adoperare le risorse del computer per fargli compiere azioni malevoli (inviare messaggi, auto-replicarsi in rete, ...). Altri sono in qualche modo "specializzati" nel furto di dati e nella violazione della privacy. Fra questi si possono citare:
- *adware*. Il nome deriva dalle parole inglesi *advertising* (pubblicità) e *software*. Sono software che visualizzano messaggi pubblicitari per procurare un reddito al suo autore. Spesso incorporati in altri programmi si incontrano nei giochi e ultimamente in modo significativo nei programmi per smartphone (le app). L'autore può percepire un reddito tutte le volte in cui l'utente clicca sul banner pubblicitario visualizzato. Alcuni possono, senza che l'utente se ne accorga, inviare ad un server delle informazioni personali quali siti visitati o abitudini di consumo, anche visualizzando falsi banner pubblicitari allo scopo di carpire informazioni sulle preferenze dell'utente per inviargli successivamente pubblicità mirate.

- *spyware*. Non ci sono dubbi sul significato del termine: si tratta di "programmi spia" che hanno lo scopo, sempre all'insaputa dell'utente del computer, di raccogliere informazioni personali ed inviarle al ladro di informazioni, trasmettendoli ad un server remoto. In questi casi, si va dai siti visitati alle credenziali di autenticazione (codice utente e password), ai dati finanziari, ...
- *botnet*. Contrazione delle parole *robot* e *network*, è letteralmente una rete di robot. Si tratta - quando il termine si riferisce ad una versione malevole della rete - di un insieme di computer connessi in rete, preventivamente infetti sfruttando qualche debolezza del sistema operativo, che vengono adoperati per disporre di una capacità di attacco distribuita molto importante. Questa rete, i cui computer sono controllabili a distanza, viene adoperata per compiere azioni non autorizzate quali invio massiccio di posta non richiesta (spam) o per compiere un attacco multiplo ad un server tramite l'azione combinata e simultanea dei computer infetti.
- *keylogger*. L'invio dei dati in rete è sempre più frequentemente cifrato ed è quindi sempre più difficile carpire password intercettando le trasmissioni in rete. La maggior parte dei collegamenti ai servizi sensibili di Internet (e-banking, e-commerce) sono crittografati dal browser adoperando il protocollo https al posto di http (come vedremo al successivo punto 4.1.2). Appena l'utente ha digitato la password, questa viene cifrata e spedita in rete. Il keylogger supera questa protezione intervenendo prima ancora che la password sia cifrata. Il keylogger è un tipo di malware che registra i tasti che vengono premuti sulla tastiera, registrando carattere per carattere quanto viene digitato, prima di qualsiasi elaborazione, compresa l'eventuale cifratura. Trasmettono poi all'esterno i dati registrati fra i quali si trovano - in chiaro - le credenziali di autenticazione.
- *dialer*. Nel caso in cui si utilizzi un collegamento del computer ad una linea telefonica tradizionale tramite modem, il dialer modifica il numero da chiamare (all'insaputa dell'utente) sostituendolo con un numero a tariffazione particolare, molto elevata, consentendo al ladro di incassare una percentuale sul traffico generato. Questo particolare tipo di malware non opera sulle linee ADSL o sui collegamenti diretti ad Internet ma soltanto su linee commutate in cui occorre comporre un numero di telefono per attivare la connessione. Con il diffondersi della banda larga, si riduce il pericolo e la diffusione stessa dei dialer.

Comunicato Stampa

10.04.2014

Indagine Kaspersky Lab: nel 2013 sono stati 28 milioni gli attacchi di malware finanziari

L' Italia è seconda in Europa per numero di attacchi finanziari. Nel 2013 il numero di malware di questo tipo è aumentato del 20,49% rispetto all'anno precedente.

Secondo il 'Financial cyber threats 2013', uno studio condotto da Kaspersky Lab, i cybercriminali puntano sempre più ad accedere ai conti online degli utenti. L'anno scorso, infatti, il numero di attacchi informatici preposti al furto di dati finanziari è aumentato del 27,6% rispetto al 2012 raggiungendo i 28 milioni di attacchi.

I programmi progettati per rubare informazioni finanziarie includono Trojan bancari, keylogger e due nuove classi di malware - una adibita al furto dei portafogli virtuali di **Bitcoin** e l'altra al download di software che generano criptovaluta. L'attività combinata di programmi che hanno come obiettivo i Bitcoin è diventata uno dei principali fattori alla base della crescita degli attacchi informatici finanziari nel 2013 cosi come la scoperta di un numero di vulnerabilità pericolose sfruttate dai criminali per condurre attacchi informatici tramite la popolare piattaforma Java.

Nel 2013, **le soluzioni di sicurezza Kaspersky Lab** hanno protetto 3,8 milioni di utenti da attacchi finanziari (con un incremento del 18,6% su base annua). I programmi malware quali i trojan bancari, tra cui i noti Zbot, Carberp e SpyEye, hanno rappresentato i due terzi del malware finanziario. Tuttavia, rispetto al 2012 la quota di questo tipo di malware è diminuita a causa di un aumento di attività da programmi nocivi destinati a Bitcoin. La percentuale di keylogger - programmi nocivi che intercettano la digitazione - è diminuita perché i criminali sono passati da questi programmi, altamente specializzati, ai Trojan che hanno una vasta gamma di funzioni.

I paesi in cui la **percentuale di criminalità informatica** finanziaria è maggiore sono: Afghanistan, Bolivia, Camerun, Mongolia, Myanmar, Perù, Turchia ed Etiopia. Si tratta dei paesi in cui questo tipo di minaccia rappresenta oltre il 12% di tutti gli attacchi malware.

Per quanto riguarda in particolare l'Italia, da questo studio emerge che il nostro paese si trova al secondo posto in Europa, dopo la Germania, per numero di attacchi finanziari, con una percentuale che nell'anno tra il 2012 e il 2013 è stata del 25,20%. Se invece confrontiamo i due anni, nel 2013 il numero di malware finanziari ha avuto un incremento del 20,49% rispetto all'anno precedente.

Paesi	Malware finanziari	%
Germania	1499994	25,77%
Italia	1466562	25,20%
Regno Unito	1139062	19,57%
Francia	497889	8,55%
Spagna	452803	7,78%
Olanda	174087	2,99%
Portogallo	157212	2,70%
Svizzera	147285	2,53%
Austria	128424	2,21%
Belgio	120986	2,08%
Svezia	26032	0,45%
Danimarca	9750	0,17%

Nel 2013 i cybercriminali hanno rivolto parte della loro attenzione anche al segmento del **malware mobile**, proprio durante questo anno si è vista una crescita esponenziale del numero di applicazioni mobili in grado di rubare denaro dai conti bancari degli utenti. Il numero di questi tipi di minacce è cresciuto di quasi 20 volte durante l'anno. La stragrande maggioranza degli attacchi erano mirati agli utenti con smartphone Android.

Il documento è riprodotto per gentile autorizzazione di Kaspersky Lab.

Essere consapevoli del pharming

Tutti quelli che hanno letto l'IBUQ *ECDL Online Essentials* (e superato l'esame ECDL relativo) sanno cos'è il DNS. Per gli altri, o in caso di vuoto di memoria, ricordiamo che il DNS (Domain Name System) è un servizio di Internet incaricato di tradurre il nome utilizzato per un server (per esempio google.it) nel suo indirizzo IP (173.194.40.120) con il quale è identificato su Internet, permettendo così agli utenti di adoperare nomi in chiaro per identificare i server o i siti web anziché sequenze di numeri difficili da ricordare. Il sistema di gestione del DNS non è centralizzato ma distribuito su molti computer, tant'è che molte aziende e organizzazioni private e pubbliche dispongono di DNS propri.

Il pharming è una tecnica (complessa) che consiste nel dirottare il traffico destinato ad un sito verso un altro sito, Prevede:

- la manipolazione di uno o più server DNS per abbinare il nome di un sito all'indirizzo IP del sito fraudolento
- la realizzazione di un sito fraudolento che imita il più possibile quello originario, in particolare nell'aspetto grafico.

Quando un utente digita il nome del sito al quale vuole accedere (per esempio quello della sua banca) viene dirottato sulla home page del sito fasullo, dove la prima cosa che gli viene chiesta è di autenticarsi digitando codice utente e password che vengono così rubati dal criminale informatico. Quando messo in pratica manomettendo un server DNS, il pharming colpisce un elevato numero di utenti.

Esistono versioni "light" del pharming consistenti nella manomissioni di particolari apparecchiature di una rete (router) che colpiscono gli utenti di quella rete. O addirittura di un singolo utente.

Ovviamente è più facile modificare un file sul proprio computer che fare pharming a livello mondiale ma il principio è lo stesso: avete modificato il vostro DNS locale e, quando volete andare sul sito www.aicanet.it, il vostro computer è convinto che vi deve instradare all'indirizzo 137.129.43.129.

Comprendere il termine phishing. Identificare le più comuni caratteristiche del phishing, quali uso del nome di aziende e persone autentiche, collegamenti a falsi siti web

Il *phishing* è uno dei tentativi di frode via posta elettronica più moderno. Il termine è una variante della parola *fishing* che in inglese significa pescare proprio perché illustra una tecnica che ha per scopo di carpire informazioni riservate all'utente ignaro, principalmente nome utente e password di siti di home banking.

Il tipico attacco di fishing avviene nel seguente modo:

1. l'utente riceve un messaggio di posta elettronica che sembra provenire dalla propria banca, da un gestore di carte di credito, dalle Poste Italiane, ... In tutti i modi da aziende reali
2. il messaggio invoca la necessità di controllare le credenziali del servizio (di home banking, di gestione della carta di credito, ...) oppure segnala la loro prossima scadenza e la necessità di rinnovarle
3. il messaggio di posta elettronica contiene un link, che l'utente è invitato ad attivare, che lo porterebbe sul sito della propria banca per compiere l'azione "necessaria"
4. il link porta invece ad un sito il cui nome è molto simile a quello della banca e la cui grafica rispecchia fedelmente quella del vero sito della banca
5. autenticandosi su questo sito, non ci si collega alla propria banca ma i propri nome utente e password sono memorizzati per essere utilizzate in modo fraudolente successivamente.

Anche se questo è uno dei tentativi di social engineering più subdoli, è facile riconoscerlo:

- nessuna banca o gestore di carte di credito invia mail per chiedere di digitare credenziali di autenticazione
- molte banche non usano proprio la posta elettronica per comunicare con i clienti
- l'indirizzo del sito è simile ma non uguale a quello reale (verificate sempre nella Barra di navigazione).

Se non bastasse, si potrebbe anche osservare che il messaggio di phishing:

- contiene un link ad un sito web al quale chiede di andare
- spesso contiene una scadenza prossima o segnala un qualche carattere di urgenza
- l'autore ha spesso delle difficoltà con la lingua italiana! Anche se va detto che ultimamente arrivano dei messaggi di phishing scritti in un italiano abbastanza corretto

- arriva in modo automatico, indipendentemente dalla banca presso la quale disponiamo di un conto corrente. Se non sono cliente della banca che sembra scrivermi, sarà facile individuare il messaggio come phishing (e sarà difficile - anche volendo - inserire nome utente e password).

Essere consapevoli della possibilità di ricevere messaggi fraudolenti e non richiesti

La comodità e la gratuità della posta elettronica fa sì che praticamente tutti gli utenti di Internet abbiano una casella (o più) di posta elettronica. Più la si usa, più la si pubblica in pagine web o la si diffonde in siti di reti sociali e più aumenta la possibilità di diventare bersaglio di attacchi via e-mail. Anche se questi attacchi sono di vario genere, sono tutti riconducibili a quello che prende il nome di *spam*, ossia di posta elettronica indesiderata o non sollecitata. Nello stesso modo in cui troviamo la nostra cassetta delle lettere di casa piena di volantini pubblicitari non richiesti, troviamo la nostra casella di mail piena di messaggi non sollecitati. Ma mentre la quantità dei volantini rimane contenuta per via del suo costo, la quantità di messaggi di e-mail fraudolenti o non richiesti cresce ogni giorno di più.

Mettere chi legge in guardia contro lo spam può sembrare un insulto alla sua intelligenza o al suo buon senso. La reazione più logica è di chiedersi chi ci può mai cascare. Visto che ancora adesso, nel 2014, numerose persone ci cascano, forse non sono proprio inutili queste poche righe.

Anche se il tasso di successo dei messaggi di spam è bassissimo, essendo nullo il costo di invio in massa dei messaggi di e-mail, continuano a diffondersi e svilupparsi al punto che oggi più della metà dei messaggi di posta elettronica nel mondo sono messaggi di spam, avendo così superato il numero di quelli di natura personale o professionale. Lo scopo delle mail non sollecitate è molto diversificato. Si va dalla raccolta di indirizzi e-mail attivi, alla vendita di prodotti, al furto di identità, alla diffusione di malware fino alla frode vera e propria, per citare solo quelli più frequenti.

Alcuni accorgimenti aiutano nel ridurre i rischi derivanti dai messaggi non richiesti:

1. diffidate dalle proposte allettanti. Possibile che la lotteria di quel paese esotico alla quale non avete mai partecipato abbia individuato proprio voi come vincitore del primo premio?
2. diffidate dai messaggi scritti in dubbio italiano. E' vero che l'uso corretto della lingua tende a perdersi, ma chi vi manda un messaggio di cinque righe con cinquanta errori di ortografia e grammatica non merita risposta
3. non rispondete mai ad un messaggio di spam, nemmeno se vi chiede di rispondere per interrompere l'invio di mail. Aiutereste solo il mittente a raccogliere e vendere il vostro indirizzo individuato come sicuramente attivo
4. cancellate immediatamente e definitivamente ogni messaggio dubbio. Ridurrete così il rischio di lasciare sul vostro computer un virus, ossia cancellatelo e rimuovetelo dal Cestino di Mozilla Thunderbird
5. utilizzate le funzionalità di gestione della "posta indesiderata" del vostro programma di posta elettronica. Thunderbird possiede interessanti funzionalità di riconoscimento e filtro dello spam
6. attivate la vostra casella di posta presso un ISP che abbia sui propri server un efficace programma antispam.

Valgono due regole nel considerare i messaggi ricevuti per posta elettronica:

1. diffidate dei messaggi inviati da mittenti sconosciuti o in generale di dubbia provenienza
2. diffidate dei messaggi inviati da mittenti conosciuti, amici, colleghi, ...

In sintesi diffidate. Se disponete di un buon antivirus regolarmente aggiornato, potete essere leggermente meno diffidenti, ma non abbassate mai la guardia.

La maggior parte dei virus penetra nel sistema tramite la posta elettronica (un'altra parte consistente tramite web) ed alcuni virus sono specializzati nell'installarsi su un computer, accedere alla rubrica di posta elettronica e spedire e-mail agli indirizzi trovati come se fossero stati spediti dall'utente stesso. Quindi se ricevete un messaggio da un vostro corrispondente abituale, non è detto che sia stato proprio lui a spedirvelo ma magari il virus gentilmente ospitato sul suo computer.

Anche se in alcuni casi, con certi programmi di posta elettronica poco sicuri, la sola visualizzazione del messaggio può (o poteva) infettare il computer, il pericolo maggiore proviene dagli allegati che, se sono programmi malvagi, possono venire eseguiti al momento in cui sono aperti (basta un doppio click).

Si ribadisce quindi vivamente di non aprire allegati di posta elettronica di dubbia provenienza, anche se hanno nomi allettanti ma di effettuare tutti i controlli possibili di provenienza, di possibile infezione con l'antivirus, tenendo conto che alcuni virus si propagano anche all'interno di documenti, come abbiamo visto al punto 5.1.6.

Il pericolo da evitare è ovviamente di infettare il proprio computer ma anche, di riflesso, di propagare il virus agli altri computer della rete alla quale siamo collegati o ai nostri corrispondenti di posta elettronica.

Probabilmente, se avete letto fin qui, vi sarà più chiaro come operano i criminali informatici e avrete preso coscienza dell'importanza della sicurezza informatica. Prima di passare ad esaminare come possiamo difenderci, una notizia che che conferma che non si è mai abbastanza prudenti ... e questo vale anche per le imprese.

La Notizia

15 febbraio 2012

CSO è una società che effettua ricerche e pubblica notizie e analisi sulla sicurezza e la gestione del rischio. Nell'articolo *Le 15 peggiori falle di sicurezza del XXI secolo* (*The 15 worst data security breaches of the 21st Century*) trovate una rassegna di falle di sicurezza sfruttate da attacchi informatici a vittime eccellenti: imprese di notevoli dimensioni, alcune molto famose, alcune addirittura specializzate nei prodotti per la sicurezza informatica ...

http://www.csoonline.com/article/2130877/data-protection/the-15-worst-data-security-breaches-of-the-21st-century.html

Non è vero che lo spam è odiato da tutti. Qualcuno lo apprezza e ci trova una fonte di ispirazione artistica! Gli artisti Joana Hadjithomas e Khalil Joreige hanno svolto dal 1999 ad oggi un lavoro di ricerca su più di 4000 mail di spam, con particolare interesse per lo scam, rivolto alle truffe. Risalendo alle origini storiche (Le lettere di Gerusalemme, della fine del XVIII secolo) e a volte risalendo agli autori delle mail, hanno trasformato i risultati del loro lavoro in installazioni artistiche. L'esposizione J*e dois tout d'abord m'excuser… I Must First Apologise…* (Prima di tutto mi devo scusare ...) a Villa Arson (Nizza, Francia) dal 6 luglio al 13 ottobre 2014 illustra i loro lavori.