CERTIFICAZIONI

ECDL IT Security

Marina Cabrini[1], Paolo Schgör[2]

[1] mcabrini@sicef.ch - Membro del gruppo di lavoro ECDL presso la ECDL Foundation – Dublin

[2] p.schgor@aicanet.it - Responsabile certificazioni presso AICA – Milano

Azioni quotidiane come recarsi in un negozio per fare acquisti, prelevare delle banconote a un bancomat, cercare delle informazioni turistiche a uno sportello automatizzato, acquistare un biglietto del treno a una biglietteria automatica e in generale guardarsi intorno, permettono di vedere che i computer sono ormai entrati a far parte del panorama urbano, e che la loro presenza non solo non è più una novità, ma viene anzi data per scontata, al punto da stupirsi della loro mancanza in quelle aree del mondo che non sono ancora pesantemente digitalizzate. Per certi versi, questa familiarità con i sistemi informatici può essere vista sia come un vantaggio, sia come un problema. E' un vantaggio in quanto il computer è diventato ormai uno *strumento* di uso comune, e non più una sorta di *status symbol* fine a se stesso. Allo stesso tempo, però, proprio questa familiarità di uso lo rende vulnerabile a rischi legati a un utilizzo normale

e disinvolto.

Per questi motivi la certificazione ECDL IT Security si propone di intervenire sulla preparazione degli utenti dei vari dispositivi informatici, affrontando le varie problematiche di sicurezza legate al loro uso.

Il malware: strumenti di difesa

Fino a qualche anno fa, prima del massiccio avvento di smartphone e tablet, il *malware* (virus, trojan, adware, e così via) era principalmente orientato ai PC, con una notevole preferenza per i PC dotati di sistema operativo Microsoft Windows. Le indicazioni per proteggersi da tale software malevolo erano abbastanza semplici: usare un antivirus mantenuto costantemente aggiornato, stare attenti a non navigare su siti "strani" e non aprire allegati di mail ricevute da chi non si conosceva. Tuttavia con l'avvento di nuovi dispositivi elettronici, e la loro rapida ed ampia diffusione, era abbastanza facile prevedere che il malware li avrebbe presi di mira. Inoltre, da sempre esistono persone interessate a sottrarre beni (materiali e non), utilizzando tecniche di vario genere. Alcune di queste tecniche si possono raccogliere sotto il termine di *social engineering*, e includono contattare direttamente le persone così da farsi dare in modo truffaldino le informazioni desiderate.

Osservando la casistica dei rischi riportata da Symantec a inizio settembre 2014, si può osservare come il numero di virus e in generale di minacce presenti nel file di definizione dell'antivirus raggiunga ormai i 24.157.365 (http://www.symantec.com/security_response/definitions.jsp), e come molti di questi riguardino dispositivi portatili quali smartphone e tablet, soprattutto quelli dotati di sistema operativo Android. Questo significa semplicemente che non è il caso di abbassare la guardia ora, anche spostandosi verso i dispositivi portatili (tablet, smartphone) per le normali attività di navigazione su Internet e di uso della posta elettronica, rispetto all'impiego di PC fissi e portatili.

ECDL e la sicurezza informatica

La decisione di sviluppare un modulo ECDL dedicato alla sicurezza informatica risale a tre anni fa, quando la Fondazione ECDL decise di affrontare il problema della crescente diffusione di malware sempre più sofisticato. Rispetto alle altre certificazioni ECDL, quali Word Processing o Spreadsheets, la certificazione IT Security affronta tematiche più complesse e generiche, che non possono essere risolte semplicemente chie-

dendo al candidato di sapere quali passaggi deve svolgere per effettuare un'operazione quale, ad esempio, mettere in grassetto una frase di un documento o inserire una formula in una cella di un foglio elettronico.

Quando si affronta la sicurezza in ambito informatico, è importante che chi utilizza i vari dispositivi si renda conto di quali siano i rischi e pericoli che si possono incontrare, e sappia quali comportamenti tenere per restare il più possibile su un terreno sicuro.

Rischiare con la posta elettronica: il "phishing"

Un esempio dei comportamenti "a rischio" di un normale utilizzatore di un computer o di un dispositivo informatico è aprire tutte le mail ricevute e rispondere a quella che segnala problemi con il sito di *online banking* della propria banca, fornendo le proprie generalità e accedendo al sito della banca facendo clic sul link diretto generalmente presente nella mail, e quindi digitando la propria login e password. In realtà il sito a cui si accede è un falso, che si presenta con lo stesso aspetto del sito della banca. La login e la password inserite nel falso sito vengono poi utilizzate da chi ha preparato la trappola per accedere al conto corrente della persona, e non è difficile immaginare cosa può succedere in seguito. Questo tipo di attacco informatico, definito "*phishing*", è sempre più diffuso, ma basterebbe un minimo di consapevolezza da parte degli utenti per evitare di cadere nella trappola e trovarsi senza più soldi sul proprio conto corrente, anche perché questi messaggi sono normalmente scritti in un italiano approssimativo e sgrammaticato, e i link presenti nella mail non portano mai al sito reale. Nell'esempio in Figura 1 sono stati evidenziati sia gli errori ortografici, sia l'indirizzo a cui punta il link "CLICCA QUI PER AGGIORNARE", che non corrisponde a un sito ufficiale della banca.

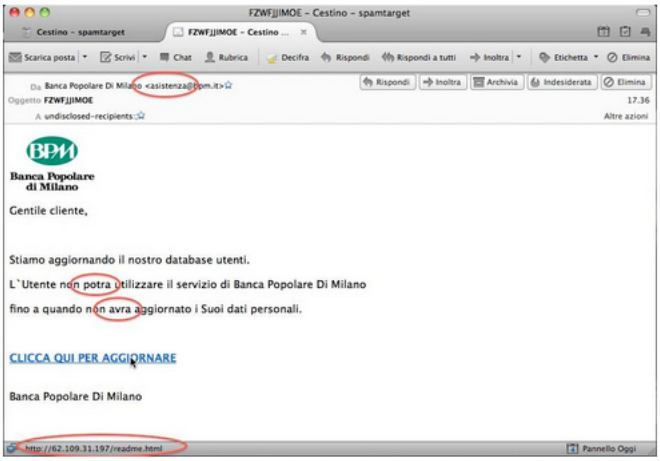

Figura 1 – Esempio di messaggio di phishing

Rischiare scaricando file dalla rete: il "ransomware"

Un altro tipo di attacco informatico che negli ultimi mesi ha visto una notevole diffusione è il *ransomware*. Si tratta di un *trojan* che viene inoculato nel computer attraverso file infetti che vengono scaricati dall'utente, e che agisce cifrando i documenti su cui l'utente lavora. La chiave per decifrare i documenti viene poi inviata a un server di proprietà dei pirati che hanno inviato la mail, e all'utente viene presentato un messaggio in cui si chiede una cifra in denaro per avere la chiave che gli permetterà di riaprire i documenti cifrati. In pratica i documenti dell'utente vengono "rapiti" dai pirati, e vengono rilasciati solo dietro pagamento di un riscatto ("ransom" in inglese). In generale il tempo lasciato a disposizione dell'utente per decidere se pagare il riscatto e riavere i file, o rinunciare a riprendere il controllo dei documenti, è abbastanza breve, ad esempio un paio di giorni.

Anche in questo caso sarebbe sufficiente un po' di attenzione nell'aprire mail provenienti da sconosciuti e mantenere delle copie di sicurezza dei documenti su cui si sta lavorando.

Figura 2 – Esempio di messaggio di ransomware, in questo caso Cryptolocker

Rischiare per ingenuità: le reti sociali

Non sempre gli attacchi informatici possono essere risolti dagli utenti, come dimostra il caso del furto di password dai server di Adobe o della rete dei giocatori di Sony Playstation, ma in alcuni casi l'ingenuità degli utenti lascia davvero senza fiato. Ad esempio, chi penserebbe mai di attaccare un cartello alla porta di casa con le indicazioni di quando si va in vacanza? Eppure sono in molti a scriverlo sui social network, senza valutare che le informazioni date in questo modo permettono a chiunque di risalire senza troppi problemi al loro indirizzo di casa, e di sapere quindi se e quando il padrone di casa è assente e se la casa resta incustodita. Un altro esempio? Il canale Twitter @NeedADebitCard, dove vengono raccolte le fotografie delle carte di credito pubblicate su internet dagli orgogliosi proprietari. Che probabilmente si troveranno alleggeriti di una buona cifra prima ancora di poterle utilizzare per la prima volta.

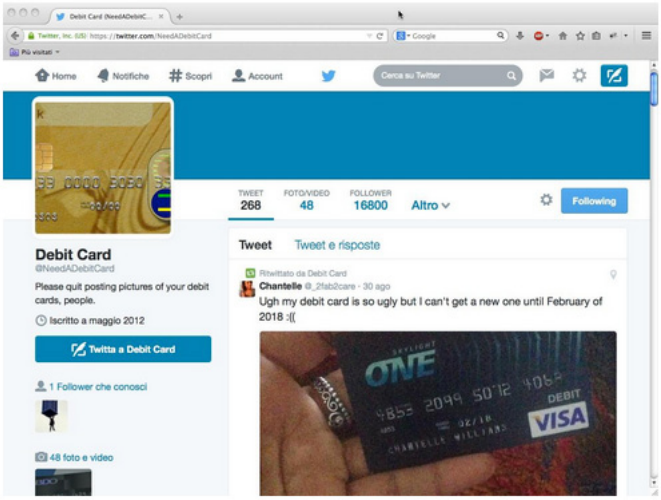

Figura 3 – Il canale Twitter @NeedADebitCard

Rischiare per leggerezza: uso disinvolto dei dispositivi

E' notizia di quest'estate il furto di un numero elevato di foto personali di diverse attrici di Hollywood, che le avevano scattate utilizzando i propri smartphone e le avevano quindi salvate nel loro spazio personale sulla cloud. Al di là del clamore mediatico scatenato dalla pubblicazione di queste foto sulla rete (e dalla richiesta di soldi alle vittime per evitare la pubblicazione delle foto più osé), l'azienda responsabile della cloud da cui sono state sottratte le foto ha avviato un'indagine per stabilire le modalità con cui è stato effettuato il furto. I risultati comunicati ufficialmente dall'azienda (http://www.apple.com/pr/library/2014/09/02Apple-Media-Advisory.html) indicano che anche in questo caso ci si trova di fronte a un uso un po' troppo disinvolto sia dei dispositivi, sia della scelta del meccanismo di protezione del materiale salvato in rete. Uso disinvolto dei dispositivi perché scattare foto intime usando un dispositivo in grado di condividere tali foto sulla rete non è particolarmente furbo, e uso disinvolto del meccanismo di protezione perché se non si vuole mettere a rischio la riservatezza di determinati materiali è il caso di capire bene come funzionano i supporti e i servizi che li ospitano.

Queste osservazioni sono state fatte da molti osservatori sulla rete, come ad esempio Paolo Attivissimo nel suo blog (http://attivissimo.blogspot.it/2014/09/foto-celebrita-violate-apple-smentisce.html), ma

sembra che gli utenti non si riescano a rendere conto di poter essere potenzialmente le prossime vittime dei vari pirati informatici.

In generale, quindi, la certificazione ECDL IT Security ha come scopo quello di aumentare negli utenti la consapevolezza dei rischi corsi adottando comportamenti per così dire "a rischio". O, in altri termini, aumentare il livello di paranoia degli utenti durante l'uso dei loro dispositivi elettronici.

La sicurezza inizia con la consapevolezza

Alla sicurezza informatica si possono riferire concetti analoghi a quelli riguardanti altri tipi di sicurezza, ad esempio quella di un edificio: si può avere una porta blindata tecnicamente avanzatissima, ma se poi si lascia la chiave sotto lo zerbino, ogni accorgimento tecnico risulta vanificato.

In questo senso, anche in campo informatico qualunque sistema di protezione dei dati deve tenere presente il ruolo fondamentale dell'utente: e il livello minimo di preparazione per poter garantire un certo livello di sicurezza è una consapevolezza dei vari rischi a cui si è esposti.

Il modulo ECDL di cui ci stiamo occupando ha appunto l'obiettivo di far comprendere le condizioni per un uso sicuro dei dispositivi digitali nelle attività quotidiane, utilizzare gli accorgimenti per connettersi in rete e navigare senza rischi, oltre a gestire in modo adeguato i propri dati.

L'importanza di questi temi è tale che AICA ha deciso di proporre il modulo sulla sicurezza informatica quale elemento necessario per la nuova certificazione ECDL Full Standard, a tutt'oggi l'unica ad aver ottenuto il riconoscimento da parte di Accredia, l'ente autorizzato dallo Stato a svolgere attività di accreditamento per gli organismi di certificazione.

Al di là delle nostre considerazioni sull'importanza teorica di questi temi, resta il fatto che il modulo IT Security, introdotto in Italia come elemento fondamentale del nuovo programma ECDL, ha già riscosso un notevole successo.

Tanto per dare un'idea dei numeri, in soli due mesi – maggio e giugno 2014 – si sono svolti complessivamente quasi 12.000 esami, ragionevolmente ben distribuiti in tutte le regioni italiane.

Quest'ottima accoglienza da parte del pubblico è la migliore conferma dell'urgenza di approfondire la consapevolezza degli utenti e ridurre quindi i rischi di perdita dei dati o di un loro uso non autorizzato e fraudolento.