NAVIGARE IN SICUREZZA SUL WEB: NON TUTTI I CERTIFICATI SSL SONO UGUALI...

Abstract

Il problema della sicurezza sul web si aggrava sempre più con l'aumentare della quantità e raffinatezza degli attacchi dei malintenzionati. Tra l'altro, si assiste alla continua crescita del *phishing*, agevolato anche dalla difficoltà, per l'utente medio, di distinguere un sito autentico da uno contraffatto. Indipendentemente da ciò, quando si svolgono attività sul web che comportano la trasmissione o ricezione di dati confidenziali è necessario proteggersi da occhi indiscreti, che possono trovarsi anche molto più vicino a noi di quanto pensiamo. Questi problemi sono mitigati dall'uso del SSL: il sistema che permette al browser di controllare se il sito web al quale ci si è collegati è autentico e di crittografare tutti i dati inviati dall'utente e restituiti dal sito. L'attivazione del protocollo SSL richiede un "certificato", da installare sul sito web, che è possibile procurarsi con una spesa modesta. Tuttavia, affinché il browser consideri valido il certificato, questo dev'essere rilasciato da un ente terzo affidabile (una "Certification Authority"); diversamente, il browser mostra un segnale di pericolo che non dovrebbe mai essere ignorato. Una CA può essere trattata come affidabile dal browser se implementa, nella emissione dei certificati SSL, procedure conformi ai requisiti del CAB Forum (l'associazione delle principali CA a livello internazionale) e se mette a disposizione degli utenti un'evidenza di tale conformità. Di solito è richiesto che la CA si sottoponga annualmente ad un audit secondo i criteri WebTrust oppure ETSI TS 102 042. Actalis S.p.A. (gruppo Aruba) è la prima e finora unica Certification Authority italiana ad aver ottenuto lo status di CA "trusted" nei browser, anche grazie all'esito positivo degli audit periodici svolti da valutatori dell'area Security ICT di IMQ, leader italiano nel settore delle valutazioni di conformità. Nel prosieguo dell'articolo si approfondiscono questi temi e si richiamano le best practices del settore.

On the Internet, nobody knows you're a dog...

Una famosa vignetta di Peter Steiner del 1993, quando il web era appena nato e quasi nessuno sapeva cosa fosse un browser, mostra un cane seduto davanti ad un PC che spiega ad un suo simile: "*On the Internet, nobody knows you're a dog!*". Quella vignetta si prestava a diverse letture, ma tutte collegate al problema della scarsa sicurezza delle comunicazioni su Internet, soprattutto per quanto riguarda la vera identità degli interlocutori. All'epoca ciò non era molto grave, in verità, perché i servizi on-line erano pochissimi. Ma da allora, purtroppo, insieme allo straordinario sviluppo che ha conosciuto il web, quel problema si è enormemente aggravato, tanto che oggi è pressoché impossibile, per qualunque professionista del campo, poter affermare di padroneggiarlo in tutte le sue possibili forme e varianti: virus, trojan, worm, spyware, cross-site scripting, spoofing, password cracking, poisoning, mal-

vertising, denial of service, hi-jacking, ... l'elenco sarebbe molto lungo e difficilmente esaustivo.

I criminali che oggi operano su Internet sono sempre più abili ed organizzati, e creano continuamente nuove tecniche per violare la confidenzialità e l'integrità dei dati che circolano sulla rete, compromettere gli elaboratori (inclusi i PC degli utenti) e talvolta bloccare completamente i servizi on-line. Per farsi un'idea dell'entità del fenomeno, basti pensare che i laboratori di ricerca specializzati rilevano globalmente diversi milioni di nuove minacce ogni mese, vale a dire *centinaia di nuovi malware ogni minuto*, con netta tendenza all'aumento (vedere la Figura 1): un ritmo davvero sbalorditivo.

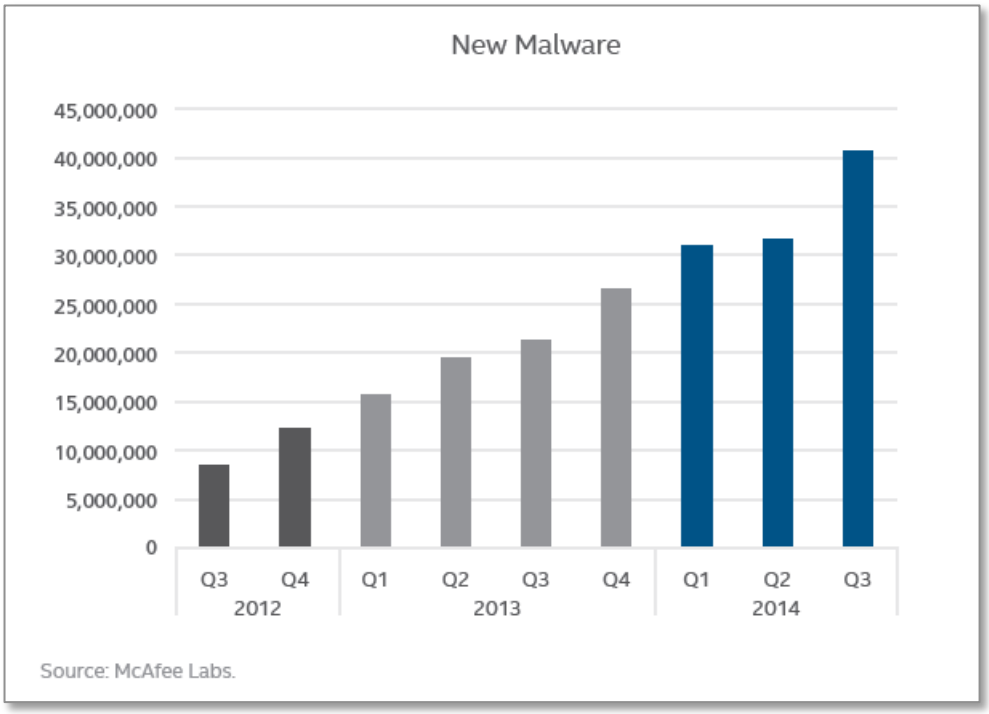

Figura 1: La continua crescita del malware

Una delle tecniche più usate dai criminali di Internet per dare avvio ad un attacco di sicurezza è quella del *phishing*, basata sull'invio (a milioni di utenti) di messaggi di posta elettronica dall'aspetto apparentemente innocuo ma congegnati per ingannare il destinatario ed attirarlo in una trappola. Questo fenomeno, che rappresenta solo una parte dello *spam* (i messaggi indesiderati e molesti che intasano le nostre caselle di posta), è purtroppo in continuo aumento. Un tipico messaggio di phishing (vedere la Figura 2), insieme ad elementi di testo e grafica che mirano a dare un aspetto credibile alla mail, include un *link* ad un sito web che l'utente suppone sia quello della società che *apparentemente* ha spedito la mail (per es. una banca, un portale di commercio elettronico, un social network, un gestore telefonico, ecc.). L'utente ingenuo e impulsivo, notando che il messaggio sembra provenire da una nota azienda, è portato a pensare che quel link lo porterà effettivamente al sito di quell'azienda.

Figura 2: Un esempio di phishing

Quello che invece molto spesso succede, se incautamente clicchiamo su quel link, è che il browser si collega ad un sito che prova subito ad infettare il nostro PC con software malevolo di vario genere (virus, trojan, ecc.). Oppure, più insidiosamente, ci si trova di fronte a quello che *sembra* – ma non è affatto – il sito menzionato nella mail. A quel punto, se si cade nell'inganno, nulla può impedire che i nostri dati più riservati (come password, PIN, numeri di carta di credito, ecc.) finiscano nelle peggiori mani.

Un po' di *sana prudenza ed un buon antivirus/antispam* consentono spesso di evitare questo tipo di tranelli, o perlomeno di non subirne le conseguenze, ma a volte non bastano, perché gli attaccanti si fanno sempre più ingegnosi e le loro trappole a volte sono molto ben dissimulate.

D'altra parte, indipendentemente dal problema del phishing, anche se ci colleghiamo *direttamente al sito* della nostra banca o del nostro commerciante on-line preferito, non per questo siamo protetti dal rischio di intercettazione dei nostri dati da parte dei malintenzionati. Un attaccante, infatti, può essere riuscito a *dirottarci verso un sito fasullo* grazie ad una contaminazione (*poisoning*) delle tabelle di instradamento che il nostro PC consulta ogni qualvolta deve scambiare dati attraverso la rete.

E anche se siamo certi di esserci collegati al sito *autentico*, il rischio di intercettazione dei nostri dati è tutt'altro che scongiurato, perché spesso i canali e gli apparati di trasmissione attraversati sono scarsamente protetti. In altre parole, i nostri dati segreti possono esserci carpiti anche da qualcuno che si trova "in mezzo" tra il nostro PC ed il sito web. In questi casi, si parla di attacchi di tipo *Man-In-The-Middle* (MITM). Questo rischio si corre sia nell'ambiente domestico che in ufficio, come pure nei luoghi pubblici (hotel, aeroporti, ecc). Per giunta, chi intende "sniffare" le nostre comunicazioni può farlo senza spendere denaro

né avere particolari competenze tecniche: esistono infatti numerosi software gratuiti che anche un ragazzino sveglio è in grado di utilizzare.

Perciò, il criminale informatico dal quale dobbiamo difenderci non sta necessariamente "dall'altra parte del filo" (ossia presso il sito web), magari in un lontano paese: può benissimo trovarsi a metà strada o anche molto più vicino a noi di quanto pensiamo.

Mitigare il rischio

Dunque, ogni qualvolta accediamo ad un sito web (ma lo stesso *vale anche per molti altri tipi di servizi on-line* come la posta elettronica, l'instant messaging, il cloud storage, le innumerevoli "app" per smartphone e tablet, ecc.), corriamo il rischio che i nostri dati confidenziali siano intercettati da malintenzionati. In definitiva, tale rischio nasce dalla difficoltà di verificare l'identità del sito web al quale ci siamo collegati e dal fatto che i nostri dati viaggiano "in chiaro", cioè senza alcuna protezione da occhi indiscreti. Per fortuna, *esistono tecnologie che consentono di mitigare* questi problemi (eliminarli al 100% non è materialmente possibile). In particolare - e veniamo così al tema centrale di questo articolo di taglio volutamente divulgativo - è importante la tecnologia nota come Secure Sockets Layer (SSL): un *protocollo sicuro* di comunicazione che tutti i browser possono utilizzare, purché abilitato sui siti web da visitare. In realtà, SSL è il nome che aveva questo protocollo all'epoca in cui fu inventato (a metà degli anni '90). Da allora ha subìto diverse revisioni, cambiando nome in Transport Layer Security (TLS), ma ancora oggi è invalso l'uso del vecchio termine SSL, perfino nei numerosi software che lo supportano, pertanto anche qui adottiamo la stessa convenzione.

Come molti utenti già sanno, per collegarsi col browser ad un sito web usando SSL si deve digitare l'indirizzo del sito iniziando con **https://** (con la "**s**"), come nell'esempio della Figura 3:

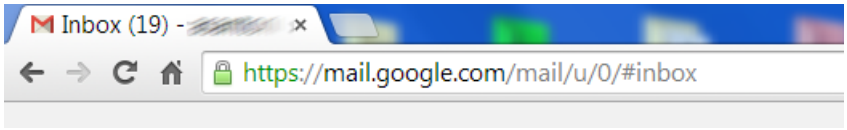

Figura 3: Connessione con SSL evidenziata dal "lucchetto"

Così facendo, dopo qualche attimo di attesa il sito desiderato viene visualizzato e nella barra indirizzo del browser compare l'icona di un *lucchetto* (vedere la Figura 3): questa icona ci segnala che il sito web è "sicuro". Ma in che senso? Vediamo cos'è accaduto "dietro le quinte" durante la breve attesa iniziale:

- il browser ha chiesto al sito web di dimostrare la propria identità;
- il sito web ha inviato al browser il proprio *certificato SSL* (vedremo tra poco di che si tratta);
- il browser ha verificato che il certificato è valido e corretto, dunque il sito web è autentico;
- il browser ha inviato al sito web una chiave di cifratura che solo il sito web può decodificare;

- infine, il browser ed il sito web hanno iniziato a dialogare in modo cifrato, usando la chiave di cifratura condivisa al punto precedente.

In buona sostanza, questo è ciò che accade durante la fase iniziale (detta di *hand-shaking*) del colloquio con SSL tra browser e sito web, quando tutto va per il verso giusto. Non abbiamo ancora detto cos'è il certificato e in che modo il browser lo verifica, ma ci arriveremo tra un attimo. È importante notare, ora, che *cliccando sull'icona del lucchetto* ci vengono mostrate *importanti informazioni* (vedere la Figura 4):

- la conferma che l'identità del sito web è stata verificata con successo ("identity verified"), ossia che il sito sul quale ci troviamo è effettivamente quello che volevamo raggiungere;
- la conferma che la sessione con questo sito web è cifrata ("connection… is encrypted"), ossia che tutti i dati scambiati tra il nostro browser ed il sito sono codificati in modo da essere illeggibili per un eventuale malfattore che dovesse riuscire ad intercettarli.

Inoltre, abbiamo la possibilità di visualizzare i dettagli del certificato ("certificate information").

Tutti i browser più diffusi visualizzano queste informazioni, cliccando sull'icona del lucchetto, anche se l'interfaccia utente cambia tra un browser e l'altro.

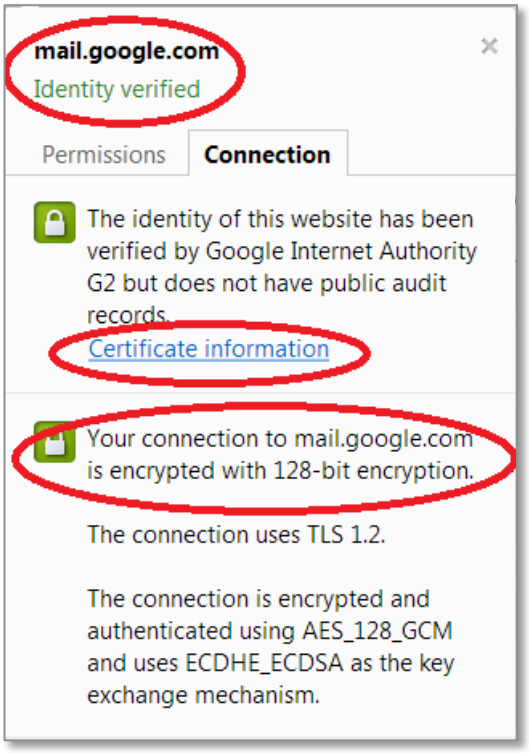

Figura 4: Informazioni sulla connessione SSL

Visualizzando i dettagli del certificato, appare una finestra del tipo mostrato nella Figura 5:

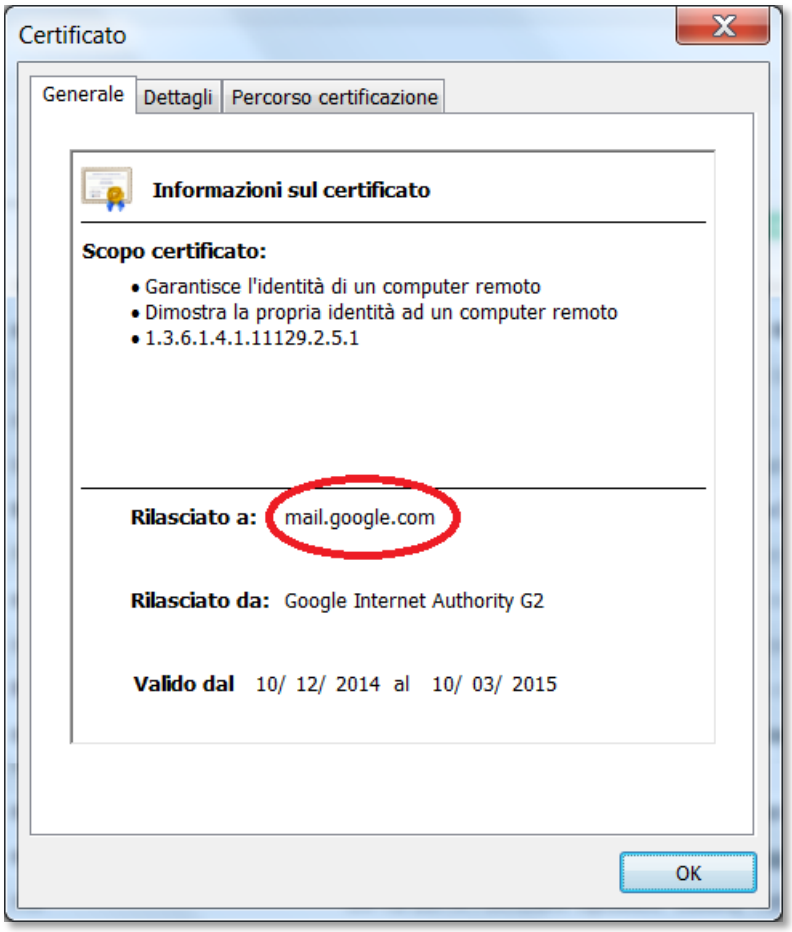

Figura 5: Esempio di certificato SSL di un sito web

Come si può notare, il certificato contiene (tra l'altro) l'indirizzo del sito al quale intendevamo collegarci (mail.google.com): questo ci conferma anche visivamente - dopo che la verifica è stata svolta dal browser in modo automatico - che il sito al quale siamo approdati è quello autentico. Vedremo tra poco in che modo il browser si procura il certificato SSL e come ne determina l'attendibilità.

Riassumendo, non solo il SSL *garantisce all'utente di essersi collegato effettivamente al sito desiderato*, ma effettua automaticamente la *crittografia di tutti i dati che l'utente invia al sito, dal proprio browser, e di tutte le informazioni che il sito web, a sua volta, invia al browser*. Quindi, per esempio, se un sito web protetto con SSL mi chiede di inserire il numero della mia carta di credito, posso contare sul fatto che nessuno "spione" potrà vedere quel numero, tranne il sito web al quale lo sto inviando. Lo stesso vale anche nel senso inverso: se, per esempio, consulto il mio conto corrente bancario attraverso un sito protetto con SSL, posso confidare sul fatto che nessun ficcanaso potrà leggere il valore del mio saldo mentre quel dato è in transito dal sito web verso il mio browser (un attaccante potrà intercettarlo, ma non decifrarlo).

Naturalmente, la funzionalità di crittografia insita nel SSL sarebbe del tutto inutile se il sito al quale mi sono collegato fosse un sito truffaldino, perciò *l'autenticazione del server è il momento più critico* del dialogo su SSL tra browser e sito web. È in quella fase (chiamata

hand-shaking) che entra in gioco il certificato SSL del sito web, sul quale ci soffermiamo di seguito.

Certificati e CA: di che si tratta?

Collegarsi ad un sito web con SSL non è un'opzione sempre disponibile. Per poterlo fare, è necessario (semplifichiamo) che sul sito web sia stato installato un appropriato *certificato SSL*. Fortunatamente, quasi tutti i più importanti fornitori di servizi on-line (come banche, portali di commercio elettronico, social network, enti pubblici, ecc.) già da tempo hanno provveduto, anche se rimangono ancora diverse scoperture e "cattive pratiche". Qui non scenderemo nei dettagli di cosa sia e come funzioni un certificato, per non annoiare troppo il lettore, ma è importante capire almeno a grandi linee di che si tratta. In pratica è un piccolo file che il sito web invia al browser nella fase iniziale della connessione. Il certificato, che non può essere alterato né contraffatto in quanto è *firmato digitalmente*, contiene una serie di informazioni relative all'identità del sito, in particolare il suo indirizzo (come "mail.google.com" nell'esempio della Figura 5) ed eventualmente anche il nome dell'azienda che lo gestisce.

Il certificato viene rilasciato da un ente chiamato *Certification Authority* (CA), dopo aver verificato che il soggetto richiedente abbia realmente *il controllo* del server che risponde ad un determinato indirizzo. Inoltre, secondo la classe di certificato, la CA svolge anche ulteriori verifiche, in particolare sull'identità dell'azienda che gestisce quel sito.

Il presupposto è che *gli utenti di Internet possono avere fiducia nelle CA*, essendo queste ultime delle società indipendenti ed affidabili. E per la proprietà transitiva delle relazioni di fiducia, se una CA affidabile ha emesso il certificato per un sito web, allora possiamo fidarci di quel certificato e dunque del sito web che ce lo presenta. A quel punto, se il certificato contiene l'indirizzo esatto del sito al quale volevamo collegarci, la connessione SSL si instaura correttamente.

Comunque, una CA non è affidabile per il solo fatto di esistere: deve *dimostrare* di esserlo, ottemperando ad una serie di regole tecnico-operative. Anzitutto, deve trattarsi di un'organizzazione ben identificata: non devono esservi dubbi su come si chiama, chi la controlla e dove ha sede. Inoltre, la CA deve pubblicare sul proprio sito un documento (noto come CPS: *Certification Practice Statement*) che illustra in modo dettagliato tutte le caratteristiche del servizio offerto: tipologie di certificati emessi, campi di applicazione, risorse tecniche, procedure operative, misure di sicurezza, formato e contenuto dei certificati, risoluzione dei problemi, obblighi delle parti, ecc. E non si tratta semplicemente di dichiarare il possesso di queste caratteristiche (sarebbe troppo facile!): la CA deve, in realtà, sottoporsi ad un *audit esterno* che lo attesti.

Poiché non è assolutamente detto che una qualsiasi CA risponda ai requisiti sopra citati, il browser non può prendere per buono un certificato SSL se non dopo aver controllato che la CA che lo ha rilasciato sia una CA affidabile. Ecco perché il browser consulta sempre una propria *lista delle CA affidabili* (vedere la Figura 6) quando ci si collega ad un sito web protetto con SSL: si tratta, come si può intuire, di un elenco di organizzazioni che il produttore del browser (per es. Google, Mozilla, Microsoft, Apple, ecc.) ha già vagliato, constatando che ri-

spettano le regole e dunque possono considerarsi affidabili. Si tratta di un elenco sostanzialmente statico, anche se periodicamente viene aggiornato.

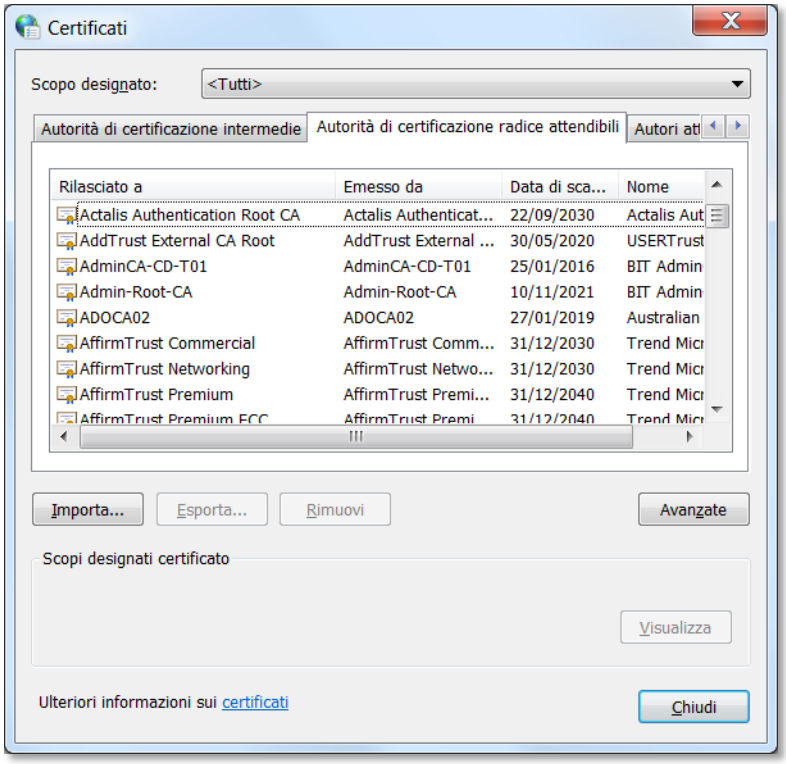

Figura 6: Elenco delle CA affidabili di Windows

Le classi standard DV, OV, EV

Nella fase iniziale dell'acquisto di un certificato, occorre specificare la "*classe*" di certificato desiderata: DV, OV, oppure EV. La classe indica, sostanzialmente, il grado di approfondimento delle verifiche svolte dalla CA, ai fini del rilascio del certificato, e conseguentemente quali informazioni verranno inserite nel certificato, oltre a quella essenziale (l'indirizzo di un sito web gestito dal cliente).

I certificati SSL di classe DV (*Domain Validated*) contengono solamente l'indirizzo del sito web, ossia l'informazione essenziale per poter attivare il protocollo SSL sul sito stesso. Prima di rilasciarlo, la CA verifica solamente che il dominio Internet al quale appartiene il sito sia effettivamente sotto il controllo del cliente; è una verifica poco onerosa per la CA, perciò questi certificati hanno un prezzo molto basso e possono essere erogati molto velocemente.

I certificati SSL di classe OV (*Organization Validated*) includono anche il nome dell'organizzazione (per es. banca, ente pubblico, ecc.) che gestisce il sito web, pertanto la CA deve verificare con attenzione tale dato prima di poter emettere il certificato richiesto dal cliente. Questa verifica è più onerosa per la CA, pertanto questi certificati hanno un costo maggiore e richiedono un tempo maggiore per essere rilasciati. Per contro, il certificato di classe OV permette all'utente di sapere con certezza qual è la società che effettivamente "sta dietro" il sito web (un'informazione non sempre desumibile dal contenuto del sito).

I certificati di classe EV (*Extended Validation*) sono simili agli OV ma hanno, in un certo senso, "una marcia in più". Prima di emettere un certificato di classe EV, la CA ha infatti l'obbligo di svolgere verifiche più meticolose sul cliente e di accertarsi che la richiesta di certificato sia stata autorizzata dal management della società richiedente. Inoltre, questi certificati contengono anche l'indirizzo della sede legale e la Partita IVA della società che gestisce il sito web. Ma i certificati EV hanno un'altra e più nota peculiarità: quando ci si collega ad un sito protetto con un certificato EV, infatti, il browser visualizza automaticamente il nome dell'azienda titolare del certificato, e la barra indirizzo (o una sua parte) appare con sfondo verde (Figura 7):

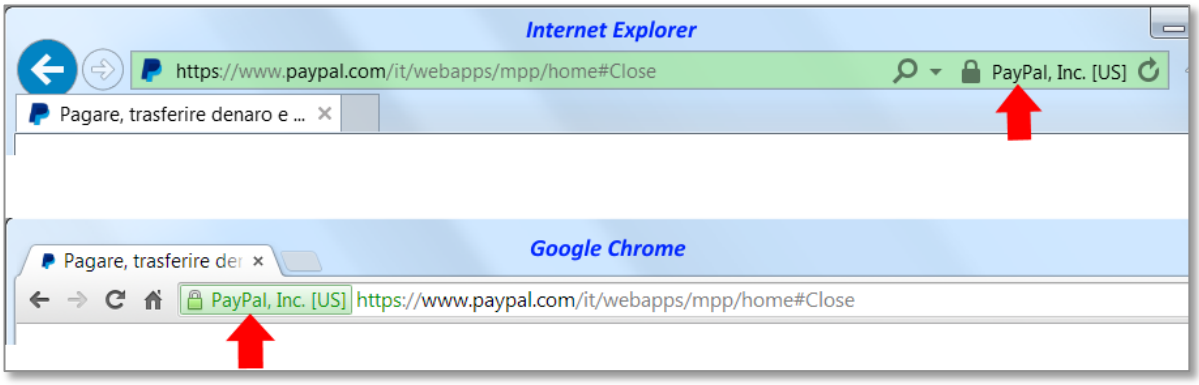

Figura 7: Effetto "barra verde" con certificati EV

Questo effetto tuttavia non è automatico: il browser lo produce solamente se la CA che ha emesso il certificato è inclusa in uno speciale elenco di CA affidabili che hanno dimostrato di rispettare le specifiche regole del CAB/Browser Forum (Cfr. [3]) relative ai certificati di classe EV. Come si può intuire, i certificati EV hanno un costo ancora maggiore dei certificati OV e richiedono più tempo per essere emessi.

Dunque anche in questo senso i certificati SSL "non sono tutti uguali": le tre classi che abbiamo descritto sono infatti caratterizzate da un livello di affidabilità crescente, dal punto di vista dell'utente, per quanto riguarda l'identità dell'azienda che "sta dietro" il sito web. In tutti i casi, comunque, l'utente ha la garanzia di essersi collegato al sito autentico e che il suo colloquio col sito web è crittografato.

Cattive pratiche

Ovviamente il certificato ha un prezzo, perché le CA non sono enti di beneficienza: d'altra parte, l'organizzazione e l'infrastruttura necessarie per erogare un servizio affidabile di CA hanno un costo non trascurabile. Ma in definitiva, l'acquisto di un certificato SSL incide molto poco sui costi complessivi di gestione di un qualsiasi sito web, e la procedura per ottenerlo è abbastanza semplice: ci si rivolge ad una CA tra quelle riconosciute dai browser (la scelta è ampia) e si seguono le istruzioni fornite on-line. Solitamente, il certificato si ottiene nel giro di pochi giorni o addirittura in poche ore (secondo la classe di certificato). Poi, naturalmente, è necessario che il webmaster sia in grado di installarlo correttamente, ma anche

questo è abbastanza facile seguendo le guide che si trovano su Internet: non è necessaria (anche se in verità sarebbe raccomandabile) una formazione specifica.

Quindi, con poca spesa e poco dispendio di tempo, è possibile aumentare in modo netto la sicurezza del proprio sito web, sia quella percepita che quella effettiva. Eppure, incredibile a dirsi, non sono rari i casi di siti web che fanno uso di certificati "fatti in casa". Quando ci colleghiamo ad un tale sito, il browser ci mostra un avviso che ci invita a *porre attenzione* a quello che stiamo facendo, in quanto c'è la concreta possibilità che si tratti di un sito pericoloso:

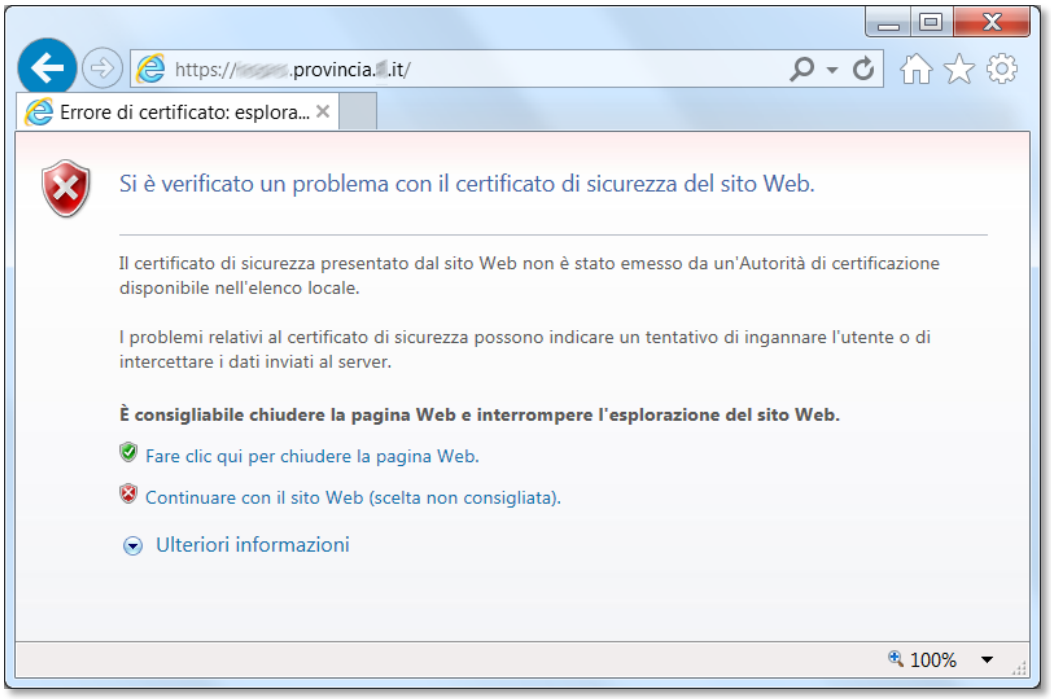

Figura 8: Avviso del browser per problemi nel certificato SSL del sito web

A questo punto, se il sito web è realmente un sito fasullo e pericoloso, l'utente *prudente* ha la possibilità di evitarlo semplicemente fermandosi o tornando indietro. Con le versioni più recenti dei browser questi avvisi sono ormai sufficientemente chiari (vedere la Figura 8), eppure gli utenti spesso li sottovalutano (si veda per esempio lo studio [1]). Talvolta, addirittura, è lo stesso gestore del sito web che invita i propri utenti ad ignorare l'avvertimento del browser. Come a dire: "poiché vogliamo risparmiare, non preoccupatevi se il browser vi segnala un possibile pericolo".

Comunque sia, quando gli utenti si abituano ad ignorare gli avvisi del browser, diventa poi *facilissimo per un hacker avere successo in un attacco di tipo MITM falsificando anche il certificato SSL* (perché anche quello "vero" non è affidabile, e l'utente medio non può notare la differenza tra due certificati entrambi inaffidabili).

Ed è un grave errore di valutazione, per le aziende, pensare che i certificati "fatti in casa" siano una scelta adeguata per gli applicativi ad uso interno (per es. sistemi gestionali, archivi documentali, ecc.), perché sulla intranet aziendale gli attacchi MITM sono ancora più facili che attraverso Internet.

Ecco perché è cruciale, ai fini della sicurezza, *utilizzare solamente certificati emessi da CA riconosciute dai browser*. *Non farlo significa rendere la vita più facile ai malintenzionati,* creando le premesse per attacchi di sicurezza molto gravi. È anzitutto in questo senso che "non tutti i certificati SSL sono uguali", per richiamarci al titolo di questo articolo.

Un ulteriore criterio di confronto tra certificati SSL è quello della "classe" di appartenenza (DV, OV, EV) che abbiamo già descritto.

Le CA "trusted"

Abbiamo già detto, in sostanza, a quali condizioni una CA può essere considerata affidabile dai browser vendor. Più precisamente, è necessario che rispetti le regole definite dal CA/Browser Forum: l'associazione volontaria, fondata nel 2005, che riunisce le principali CA del settore SSL e i principali produttori di browser (Google, Microsoft, Mozilla, Apple, ecc.). Non desta molta sorpresa il fatto che molti membri del CAB Forum siano statunitensi, sebbene non manchino le CA europee ed asiatiche. Un elenco completo delle CA associate si trova su https://cabforum.org/members/

Tornando alle condizioni che permettono ad una CA di essere considerata affidabile dai browser: come minimo, la CA deve rispettare integralmente i "*Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates*": un documento di quasi 50 pagine che detta le regole su tutti i principali aspetti tecnico-operativi di un servizio di emissione di certificati SSL.

Come abbiamo già detto, però, non basta che la CA dichiari di rispettare tali requisiti: è necessario che ciò sia dimostrato da un auditor qualificato e indipendente attraverso lo svolgimento periodico di verifiche sul campo e conseguente rilascio di un'attestazione formale di conformità. L'auditor, pertanto, analizza il *modus operandi* effettivo della CA e controlla che la documentazione del servizio sia coerente con i fatti concreti. Nel compiere tali verifiche, l'auditor deve basarsi su criteri accettati dai browser vendor: si tratta, in particolare, dei criteri *WebTrust* oppure delle norme ETSI TS 102 042 / ETSI TS 101 456.

Già dal 2012 la società milanese Actalis S.p.A. (www.actalis.it) del gruppo Aruba, uno dei principali certificatori di firma digitale accreditati da AgID (http://www.agid.gov.it/certificatori-attivi), è l'unica CA italiana ad aver ottenuto lo status di CA "trusted" nei browser, essendo stata sottoposta con esito positivo ad attività di audit, iniziale e periodico di mantenimento, da parte di auditor dell'area Security ICT di IMQ (www.imq.it), leader italiano nel settore delle valutazioni di conformità. La periodicità delle attività di audit, almeno annuale, permette di valutare la conformità nel corso del tempo ai requisiti dello standard di riferimento [2], anche quando avviene la pubblicazione di una nuova versione dello stesso.

Conclusione

Il protocollo SSL consente di mitigare il rischio di intercettazione dei nostri dati personali durante l'accesso a servizi on-line di ogni genere (es. banche, portali di commercio elettronico, sistemi di pagamento, webmail, social network, servizi di cloud, sanità, ecc.). Tuttavia il

SSL non è un'arma perfetta: la sua efficacia dipende da diversi fattori. Anzitutto, i gestori dei siti web hanno la responsabilità di attivarlo e di configurarlo correttamente sui propri sistemi, partendo dalla scelta di un certificato affidabile.

Fortunatamente, il numero di siti web che supportano il SSL è in costante crescita (cfr. [5]), eppure le competenze sul tema sono ancora insufficienti, non solo da parte degli utenti finali (il che è ovvio e perdonabile: non è il loro mestiere) ma anche da parte delle società che gestiscono i siti. Infatti non basta attivare il SSL sul proprio sito, se non lo si configura in modo appropriato. Spesso il webmaster, per impreparazione o per negligenza, si limita ad accettare la configurazione SSL di "default" del proprio web server, che non sempre è adeguata. Uno dei più comuni errori di configurazione consiste nel lasciare abilitate le "*ciphersuite*" più vecchie, che fanno uso di chiavi di sessione corte (es. 56 bit), ormai facilmente *crackabili* da attaccanti determinati (cfr. [6]).

Non si deve dimenticare, poi, di utilizzare le più recenti versioni disponibili dei browser (per gli utenti finali) e dei web server (per le aziende che gestiscono i siti web), perché le versioni obsolete sono afflitte da "bugs" che possono essere sfruttati dagli attaccanti per eludere o ridurre alquanto le protezioni offerte dal protocollo SSL. In ogni caso resta sempre della massima importanza, per l'utente finale, avere sul proprio PC un buon antivirus, costantemente aggiornato.

Vi sono altri aspetti importanti, in tema di SSL, che per ragioni di spazio non abbiamo qui trattato (per es. i certificati wildcard, la gestione delle revoche, ecc.) e che saranno discussi in un altro articolo.

Riferimenti

[1] Sunshine J., Egelman S., et al.: "Crying Wolf: An Empirical Study of SSL Warning Effectiveness", Proceedings of the 18th conference on USENIX security symposium (August 2009).

[2] ETSI TS 102 042 V2.4.1 (2013-02) – Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates.

[3] Guidelines For The Issuance And Management Of Extended Validation Certificates, CA/Browser Forum V. 1.3. (2010-11)

[4] Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, CA/Browser Forum V 1.1 (2012-09)

[5] http://news.netcraft.com/archives/2014/01/03/january-2014-web-server-survey.html

[6] https://en.wikipedia.org/wiki/EFF_DES_cracker