Top-10 delle cause delle vulnerabilità applicative

di Carlo Simonelli

L'uomo del terzo millennio tende molto spesso a confondere i sintomi con la malattia. Si lamenta dei cattivi politici, ma esalta il suffragio universale; protesta contro la guerra, ma consuma sempre più petrolio; si dispera per i cambiamenti climatici, ma installa nuovi condizionatori in casa e in ufficio..
Gli esperti di sicurezza, che sono a pieno diritto uomini del terzo millennio, non fanno eccezione e tendono molto spesso a pensare che la causa delle vulnerabilità applicative siano le vulnerabilità applicative stesse; che è come dire che la causa del cancro sono le cellule cancerose. È vero, ma è un modo molto miope di affrontare il problema.
Le vulnerabilità applicative non sono funghi, che spuntano da soli nella notte, ma errori di programmazione. Più precisamente, sono errori di *buona programmazione*: non li possiamo considerare dei *bug* veri e proprî, dato che non impediscono il corretto funzionamento del software, ma sono certamente delle abiure alla regola d'arte della scrittura del codice.
In un Mondo in cui la maggior parte dei sistemi informatici è - almeno teoricamente - accessibile a qualunque altro computer del Pianeta, la resilienza ad attacchi esterni dev'essere considerata un requisito indispensabile di qualunque software e i test di sicurezza devono esser resi parte integrante dei test funzionali.
L' OWASP, un'organizzazione *no-profit* internazionale che si prefigge (con buon successo) di diffondere la cultura della sicurezza informatica, pubblica con cadenza triennale una classifica delle vulnerabilità applicative più diffuse, basata sull'elaborazione statistica delle segnalazioni di attacco. Sfortunatamente, però, fra le statistiche è la realtà c'è la stessa, immane differenza che passa fra il sesso fatto dai laureati in statistica e la fornicazione vera e propria; inoltre, dato che questa classifica si basa sui dati comunicati, che sono inevitabilmente un sotto-insieme casuale del totale degli attacchi effettivamente avvenuti, possiamo aspettarci che per le vulnerabilità applicative avvenga ciò che avviene per le violenze domestiche: i dati, terribili, che si possono desumere dalle denunce, sono solo una parte del totale effettivo e si riferiscono solo ai paesi più progrediti.
Da un punto di vista pratico, al contrario, la *Top-10* OWASP è molto utile, perché serve a pararsi il culo. Nessuno può dire con certezza che il suo sistema software sia sicuro al 100%, se non altro perché non è possibile prevedere quali attacchi saranno ideati nel futuro; in compenso, può dire che il suo sistema è protetto dalle vulnerabilità più comuni e utilizzare la Top-10 OWASP come riferimento. È un comportamento perfettamente legittimo, perché la Top-10 OWASP è un elenco accurato e credibile. Approssimato e incompleto, probabilmente, ma è pur sempre la migliore approssimazione disponibile.
Elencare i sintomi, però, pur se in maniera accurata, non ci aiuta a curare la malattia. Questo va bene per chi fa sicurezza, perché gli garantisce un futuro professionale ben remunerato, ma va un po' meno bene per chi deve gestire o utilizzare i sistemi software, perché è solo una cura sintomatica: il naso smette di colare, ma il raffreddore c'è sempre. Se vogliamo davvero rendere i nostri sistemi più sicuri, dobbiamo smetterla di preoccuparci dei sintomi e concentrarci sulla malattia vera e propria.
In quest'ottica, ho deciso di stilare una classifica che riporti quelle che, a mio modo di vedere, sono le *cause* più diffuse delle vulnerabilità applicative. Diversamente dalla Top-10 OWASP, questa classifica può essere facilmente compresa anche da chi non abbia una preparazione specifica nel settore della sicurezza. Non vi troverete davanti definizioni arcane come: *Cross-Site Request Forgery*, o, pure: *Insufficient Transport Layer Protection*; l'unico termine in Inglese è "manager" e ciascuna voce è spiegata in dettaglio per favorire la piena comprensione del problema. Spero possa esservi utile.

Top-10 delle cause più diffuse delle vulnerabilità applicative

1. Committenti Corrotti
2. Programmatori Scadenti
3. Capi-Progetto Inadeguati
4. Commerciali Avidi
5. Mode Passeggere
6. Finti Esperti di Sicurezza
7. Veri Esperti di Sicurezza
8. Manager Impreparati
9. Utenti Tonti
10. Riproduzione Sessuata

Posizione 1: Committenti Corrotti

Prima di *Mani Pulite*, la mazzetta media per gli appalti pubblici si aggirava intorno al 10% dell'importo totale del progetto; dopo Mani Pulite, l'aumento del rischio fece salire la percentuale al 30%.
È sicuramente possibile completare un progetto anche con il 10% in meno di fondi, lo si è fatto per anni; se però dobbiamo scorporare (in nero) il 30%, le cose di fanno più complicate, specie in un mercato che è sempre più affollato e competitivo. Dato che i prezzi sono ormai ridotti all'osso e così pure i margini di guadagno, l'Imprenditore Corruttore, se si aggiudica la gara, ha due possibilità:

a) fa un lavoro quantitativamente inferiore al previsto;
b) fa un lavoro qualitativamente inferiore al previsto.

La prima soluzione è la più remunerativa: l'imprenditore fa solo il 70% del lavoro, poi si ferma - anche perché non ha più i soldi per pagare i fornitori. Se gli dice bene, nessuno se ne accorge e la cosa finisce lì; se invece qualcuno se ne accorge, il corruttore va dal corrotto e gli chiede di affidargli un nuovo progetto, in modo che, con i fondi di quest'ultimo, possa completare il primo. Se il corrotto è sufficientemente potente e/o avido, il corruttore ottiene un nuovo progetto, prende i soldi, decurta l'abituale 30% per il corrotto e completa in maniera raffazzonata entrambi i progetti. O solo uno dei due. O nessuno dei due.
Questo meccanismo perverso è, a mio modo di vedere la causa prima dei problemi del nostro Paese: da un quarto di secolo, lo Stato va a ristorante, paga il un pranzo completo e ottiene, nella migliore delle ipotesi, un piatto di pasta, un contorno e un caffè; la carne e il dolce, se li mangia il cameriere. Se pensate che stia esagerando o che mi stia inventando delle cifre, non avete che da guardarvi intorno: scoprirete che un sacco di opere pubbliche, sono completate al 70%. Nella migliore delle ipotesi.
Se il corrotto non è sufficientemente avido e/o potente da far avere due progetti al suo corruttore, questi è costretto a completare il progetto assegnatogli.Chiaramente, essendo sotto del 30% già da prima di cominciare i lavori, deve fare qualche economia e, non potendo risparmiare sui beni, risparmia sulla qualità dei servizi. Nel caso di un progetto che comporti la produzione di software, risparmia sui programmatori, il che ci porta alla seconda posizione della nostra classifica.

Posizione 2: Programmatori Scadenti

Poniamo che il progetto preveda la fornitura di un programmatore Java J2E al costo giornaliero di 100 Euri (è di più, ma ci semplifica le percentuali). L'imprenditore non ha in casa quel tipo di programmatore, così lo chiede a un'altra società. Chiaramente, sia la società del corruttore che

quella che gli fornisce il programmatore fanno il loro bravo margine sul costo giornaliero del programmatore. Ponendo che il *markup* di ciascuna delle due società sia del 25% (è un'ipotesi ottimistica), otteniamo che il programmatore è pagato, a giornata, poco più di 55 Euri. Inevitabilmente, si tratterà di un programmatore scadente che produrrà software di scarsa qualità.

Posizione 3: Capi-Progetto Inadeguati

Un buon programmatore può diventare, senza grossa fatica, un analista-programmatore; un buon analista-programmatore può diventare, senza grossi sforzi, un buon analista; ma perché un buon analista diventi un buon capo-progetto occorrono tempo e volontà. Programmatore, analista-programmatore e analista, infatti, sono ruoli che prevedono solo delle capacità tecniche; al contrario, un capo-progetto deve saper trattare con il cliente e gestire in maniera efficace le persone del suo gruppo di lavoro - due attitudini che spesso vanno in contrasto con la forma mentale propria del buon tecnico. Per fare un esempio nautico, un uomo che abbia circumnavigato il Globo in solitario potrà essere un ottimo timoniere o un ottimo ufficiale di rotta anche su una nave da crociera, ma per svolgere altrettanto bene il ruolo di primo ufficiale dovrà probabilmente venire a patti con il suo carattere.
Dico tutto ciò con buona cognizione di causa, perché ci sono passato: i miei primi anni da capo-progetto sono stati terribili; guardare indietro a quei tempi e ripensare a ciò che facevo, dicevo e pensavo è sempre un duro colpo, per il mio ego. È l'inevitabile conseguenza del *Principio di Peter*: le posizioni lavorative, in una gerarchia, tendono a essere occupate da impiegati che non hanno competenza adatta ai compiti da svolgere. Questa condizione, tanto paradossale quanto inevitabile, potrebbe essere facilmente risolta se i nuovi capi-progetto fossero affiancati, inizialmente, da colleghi con maggior esperienza, ma dato che allocare un solo responsabile su una commessa costa meno (in teoria) che caricarcene due, i capi-progetto novellini sono lasciati in balìa di sé stessi, con conseguenze che spaziano dal nocivo al disastroso.

Posizione 4: Commerciali Avidi

Quanto ho detto finora non è una novità e non è assolutamente un segreto: è ciò che avviene nel mondo dell'informatica da almeno quindici anni. Ci si potrebbe quindi aspettare che chi gestisce ad alto livello i progetti abbia fatto tesoro dell'esperienza e abbia messo in atto delle politiche preventive, ma non è così. Questo si deve al fatto che i commerciali, coloro i quali propongono ai clienti i prodotti e i servizi delle diverse società informatiche, sono esseri avidi, il cui solo scopo nella vita è di generare fatturato. "Fatturato", badate bene, non "ricavi".
Essendo giudicati in base al fatturato, i commerciali non si curano del fatto che un certo sistema non sia utile al loro cliente o che il personale destinato a realizzarlo non sia sufficientemente capace. Il rapporto che c'è fra commerciali e tecnici è lo stesso che lega i papponi alle mignotte. Per un non pappone, non importa se una mignotta scopa bene o male, se sia sana o abbia l'AIDS: l'importante è che porti soldi. Se la puttana muore, se il cliente muore, poco male: se ne troveranno certamente degli altri.
Questo atteggiamento illuminato potrebbe essere scusabile se fosse applicato esclusivamente nei confronti delle industrie private. Per esempio, se io facessi un pessimo lavoro per la società che commercializza l'acqua minerale Sangemini, potrei sempre pensare: "Chi se ne frega, tanto io, a casa, bevo la Ferrarelle". Ma se lavoro male per lo Stato o per le società para-statali, non posso giustificare il mio comportamento truffaldino con il dovere di offrire un futuro di benessere ai miei figli, perché truffando lo Stato avrò, al contrario, danneggiato il loro futuro e quello di tutte le persone a me care.
Dice: ma è mai possibile che nessuno ci abbia mai pensato, che nessuno, nella gerarchia delle società informatiche non si sia mai reso conto che, in questo modo, si stava scavando la terra sotto ai piedi?
A questa domanda non so rispondere. Posso solo ipotizzare che il manager belga, inglese o americano del nostro Commerciale Avido non sia particolarmente interessato al corretto funzionamento del nostro sistema previdenziale o della nostra amministrazione in genere.
È questo, il bello delle società multinazionali.

Posizione 5: Mode Passeggere

All'inizio dell'estate, le case produttrici di gelati cercano di conquistare nuovi clienti mettendo in commercio nuovi prodotti o nuove versioni dei gelati di maggior successo. Questi gelati, il primo anno, sono molto buoni: la panna sembra effettivamente panna, il cioccolato sa effettivamente di cioccolato e il pistacchio di pistacchio. Già dall'estate successiva, però, si verifica quello che potremmo definire l'*Effetto Cenerentola*: il cioccolato si trasforma in una zucca, la panna in topolini bianchi e il pistacchio in lucertole.
La stessa cosa si verifica nel mondo dell'informatica, solo, con tempi più lunghi. Ciclicamente, appaiono delle novità che diventano in breve tempo l'argomento più trattato negli articoli dei giornali specializzati e nei convegni. Ciascuna di queste novità - sia essa una tecnologia, un paradigma o un linguaggio di programmazione -, viene immancabilmente presentata come la Panacea Digitale, un taglio netto con il passato che rivoluzionerà il nostro/vostro modo di fare o di fruire dei sistemi informatici. *Downsizing*, *Right-sizing*, *Client-server*, *Object-Oriented*, *RAD*, *UML*, *Java*, *Open-Source*, *Agile Programming*, *Cloud*, *Mobile*, *As-a-Service*.. tutte queste innovazioni hanno generato scalpore e fatturati, ma solo alcune di esse si sono dimostrate all'altezza delle aspettative; la maggior parte si è rivelata, alla lunga, un fuoco di paglia.
Questo continuo cambiamento, funzionale solo ai sordidi intenti degli Avidi Commerciali e dei loro padroni multinazionali, ha ostacolato lo sviluppo di un *modus operandi* consolidato, di una regola d'arte informatica: ogni due o tre anni tutto cambia e ciò che si era imparato fino ad allora non serve più. Dopo vent'anni di combattimenti eravamo finalmente riusciti a proteggere i nostri computer da virus e intrusioni, ma l'esplosione del fenomeno *mobile* ha riportato indietro le lancette della sicurezza di almeno dieci anni.
Il pericolo non sono cambiamenti, necessarî e fisiologici, in un settore così giovane e così provvido di sviluppi come l'informatica, ma questa specie di frenesia alimentare che ci porta a provare subito e con cieca fiducia ogni novità offerta dal mercato.
D'altro canto, se uno prova a chiedere consiglio agli esperti..

Posizione 6: Finti Esperti di Sicurezza

Ci sono personaggi che dicono di essere esperti di sicurezza. Conoscono tutti gli acronimi più esoterici, hanno letto tutti i *white-paper* degli IPS e degli IDS di ultima generazione, possono citare a memoria le differenti posizioni delle Top-10 OWASP dal 2004 a oggi, ma non hanno mai scritto né una pagina HTML né una linea di codice in vita loro.
O sono troppo paranoici o lo sono troppo poco. Non hanno mai visto un loro programma schiantarsi per un errore nell'indirizzamento della memoria o andare in *loop* per un errore in un ciclo *while*. Hanno imparato il sesso sui libri e si spacciano per pornodivi. I loro frequenti errori danneggiano i loro malaccorti clienti e mettono in cattiva luce gli appartenenti alla categoria che troviamo alla posizione successiva.

Posizione 7: Veri Esperti di Sicurezza

Qualche tempo fa, ho lavorato con un gruppo di esperti nella sicurezza dei sistemi *mobile*; professionisti molto preparati, con una buona esperienza e una grande passione per il loro lavoro. Da più di sei mesi cercavano, invano, di convincere il responsabile di un sistema a eseguire dei test di sicurezza; io, in meno di una settimana, con due soli messaggi di posta elettronica, sono riuscito ad avere l'autorizzazione a eseguire i test. Abbiamo fatto i nostri controlli, trovato delle vulnerabilità e collaborato alla loro correzione. Alla fine, il responsabile del sistema, quello stesso che da mesi recalcitrava e procrastinava, ci ha inviato un messaggio ufficiale di ringraziamento. Questo drastico cambio di atteggiamento è stato causato da un semplice cambio nella modalità di comunicazione: mentre i miei colleghi avevano esposto il problema in termini tecnici, io lo ho esposto in termini che il responsabile potesse capire. (In pratica gli ho fatto un ricatto implicito, ma a fin di bene..)
Gli esperti di sicurezza, come tutte le categorie ad alta specializzazione, tendono a essere dei circoli chiusi, con il loro gergo e le loro convenzioni lessicali. Come disse, durante un concerto parigino, il cantante *cajun* Clifton Chenier: "*I speak French too, but is a different language*".
Quando un manager si scontra con questa forma di comunicazione così diversa da quella a cui

è abituato (non dimentichiamoci che anche i manager sono una categoria che ha un proprio gergo delle proprie convenzioni lessicali), vive lo stesso imbarazzo che proverebbe un trentenne scapolo se rimanesse intrappolato a un pranzo ufficiale fra due mamme che parlano delle coliche dei loro bambini: sorriderebbe e annuirebbe educatamente, ma non vedrebbe l'ora di alzarsi e andarsene. Perciò, quando un esperto di sicurezza ha la fortuna di riuscire a farsi *ascoltare* da uno o più manager, deve riuscire anche a farsi *capire*. La stessa frase che, in un convegno di hacker, causerebbe diverse occhiate di ammirazione, è molto probabile che infastidisca una platea di dirigenti.
Goethe scrisse che: *Chi vuol capire il Poeta, deve andare nella terra del Poeta*; allo stesso modo, se l'esperto di sicurezza vuole farsi capire dal manager, deve andare nella terra del manager.
Non può aspettarsi che avvenga il contrario.

Posizione 8: Manager Impreparati

Combattiamo guerre da quando l'evoluzione ci ha dato mani in grado di impugnare armi; costruiamo case, strade e ponti da migliaia di anni; sviluppiamo industrie da più di due secoli; gestiamo sistemi informatici globali da poco più di dieci anni e, dalla nascita di Internet a oggi, i cambiamenti si sono susseguiti a velocità così vertiginosa che spesso gli stessi esperti delle società informatiche sono in disaccordo su quali siano i comportamenti da adottare.
In un simile scenario, è perfettamente normale che i manager degli Enti e delle aziende che non appartengono al settore dell'informatica o delle telecomunicazioni abbiano bisogno di aiuto per gestire i loro dati. Sfortunatamente, però, l'aiuto che questi manager ricevono è spesso condizionato da interessi interni dell'azienda che fornisce la consulenza e le soluzioni adottate non sono quelle migliori per il cliente, ma per il fornitore. Da un punto di vista imprenditoriale, quello delle aziende informatiche è un comportamento del tutto coerente - se chiedete a Valentino di rifarvi il guardaroba, non potete aspettarvi che vi consigli una borsa di Gucci - ma, alla lunga, questo stato di cose non può che creare dei problemi, tanto più gravi quanto più importante è il cliente.
Il manager, d'altro canto, non ha scelta: non può basare le sue decisioni su una consuetudine, perché la consuetudine non c'è; non può basarla sulle tendenze generali, perché, come abbiamo detto, le tendenze sono effimere; non può affidarsi a esperti di sicurezza, perché non li capisce.. La sua unica possibilità è scegliere un fornitore di comprovata affidabilità è rimettere a lui ogni scelta di tipo tecnico anche se sa perfettamente che non sempre saranno scelte disinteressate.
Paradossalmente, se il manager ha - o, come più spesso avviene, è convinto di avere - delle competenze informatiche, le cose si complicano, perché si intrometterà nei piani del fornitore con scelte che spesso saranno frutto di mode passeggere o di consigli di Finti Esperti.
Lui li capisce, ma, purtroppo, non li sa distinguere da quelli veri.

Posizione 9: Utenti Tonti

Il Web potrà pure essere alla versione 2.0, ma la maggior parte degli utenti dei sistemi informatici è ancora, indubbiamente, in versione beta: un prototipo instabile con spiccata propensione all'errore.
Gli Utenti Tonti o, più brevemente, gli U*tonti*, sono una delle principali cause delle vulnerabilità applicative perché il loro modo di pensare, il loro stesso approccio all'esistenza - allo stesso tempo furbesco e neghittoso - collidono con i fondamenti stessi della sicurezza informatica.
L'utonto è pericoloso in sé; quando ha un computer a disposizione, la sua pericolosità si estrinseca in forma digitale con conseguenze quasi sempre nefaste. Ciò che maggiormente sgomenta, del comportamento dell'utonto, è che gli basterebbe uno sforzo minimo, per fare le cose in maniera corretta, ma lui, quello sforzo, non riesce proprio a farlo. Non ha una password, apre tutti gli allegati dei messaggi di SPAM, ignora le segnalazioni del suo antivirus, installa qualunque programma o *toolbar* che riesce a procurarsi. La porta USB del suo computer è il corrispettivo informatico di un *glory-hole* nel muro del cesso di un locale gay di San Francisco; il suo motto è: *Stultitia vincit omnia*. Non importa quanto possa essere sicuro un sistema software: se lo si mette in mano a un utonto, state pur certi che lui riuscirà a trovare il modo di renderlo vulnerabile.

L'unico modo per limitare la pericolosità dell'utonto è formarlo, sottoponendolo a forme coercitive di apprendimento che gli inculchino i principii base della sicurezza come riflessi pavloviani. Sfortunatamente, però, se si educassero gli utenti, si venderebbero meno sistemi di difesa (anti-virus, *firewall*, IPS, IDS ecc.) e sarebbero necessarie meno consulenze di sicurezza. Questo è qualcosa che i Commerciali Avidi non possono permettere. Da più di dieci anni, perciò, le società di informatica vedono gli utenti morire di fame, ma, piuttosto che insegnar loro a pescare, preferiscono vender loro del pesce.

Posizione 10: Riproduzione sessuata

Come penso abbiate capito, ciò che determina l'ordinamento di questa mia Top-10 non è la pericolosità dell'elemento, ma, piuttosto, un rapporto di causa-effetto fra le diverse posizioni: la corruzione dei committenti causa la scarsa qualità dei tecnici; l'avidità dei commerciali e le mode passeggere, unite alla scarsa efficacia degli esperti di sicurezza, causano l'impreparazione dei manager e la pericolosità degli utenti.
Un uomo del terzo millennio vi direbbe che finisce qui, e chiuderebbe la classifica alla nona posizione, ma sarebbe l'ennesima confusione fra malattia e sintomo. Io sono - e mi sento - un uomo del secolo scorso: ho visto la televisione in bianco e nero, lo sbarco sulla luna, la Carrà quando ancora era trombabile, i telefoni con il selettore circolare, le audio cassette, i *floppy-disk* da 1.4 Mb, i processori da 100 Mhz, la nascita di Internet, le BBS, i siti porno gratuiti e il *Ping-o-Tronic*. Posso non distinguere il Bene dal Male, ma sono perfettamente in grado di distinguere il male dai suoi sintomi e vi dico perciò che sempre di sintomi, abbiamo parlato, finora.
D'accordo: tecnici, commerciali, esperti e utenti sono la causa delle vulnerabilità informatiche, ma, loro, da *cosa* sono causati La risposta è il titolo di questo paragrafo. Nel mio saggio: *Penetration, un approccio nuovo alla sicurezza informatica*, ho dimostrato come la ritrosia innata delle femmine sia la causa primaria della pirateria informatica; in questa sede voglio fare un passo in più e affermo quindi che è la stessa riproduzione sessuata, il vero problema.
È la riproduzione sessuata, a causare l'avidità dei Committenti Corrotti e dei Commerciali Avidi - convinti, non del tutto a torto, che aumentare il proprio conto in banca significhi anche aumentare le proprie probabilità di accoppiamento. È la riproduzione sessuata incontrollata, che genera un surplus di popolazione, quella genìa che Papini definiva: "uomini che vivevano perché erano nati; che mangiavano per vivere, che lavoravano per mangiare e maledicevano il lavoro senza il coraggio di rifiutar la vita".
Questa gente, una volta venuta al mondo, non la si può più eliminare e gli si deve quindi trovare un lavoro. Quale che sia, tanto, lo faranno comunque male. Quale che sia.
Sono loro, i programmatori scadenti, i capi-progetto inadeguati, i finti esperti di sicurezza e gli utenti tonti. Sono loro, la maggioranza, quelli che votano e mandano al potere i cattivi politici in cambio di un posto di lavoro. E i cattivi politici, una volta al potere, chiudono il cerchio affidando le posizioni di comando ai Committenti Corrotti, che si sdebiteranno dividendo con i loro protettori parte del bottino.

Cosa possono fare, contro questa moltitudine, i pochi, buoni, esperti di sicurezza e i pochi, buoni, manager?