

Responsible Disclosure:

quanto è efficace nel contrastare il fenomeno del Data Leaking?

Marco Ortisi (2011)

Chi sono

- Net Citizen dal 1996
- Lavoro nel campo dell'IT Security dal 1999
 - Penetration Test
 - Vulnerability Assessment
 - Hardening
 - Code Review
 - Malware Reversing
 - (dovevo mettere qualche altra cosa per riempire lo spazio 😊)



Responsible Disclosure: quanto è
efficace nel contrastare il fenomeno
del Data Leaking?

Ho dato una domanda al titolo del talk perché volevo soddisfare una mia curiosità personale, in un periodo dove siamo stati bombardati da casi di Data Leaking:

- **Sony Playstation Network:** 77 milioni di dati personali trafugati (intrusioni multiple) [Aprile 2011]
- **HB Gary:** graaaaaande imbarazzo! [Febbraio 2011]
- **RSA SecurID:** si si, proprio quelli dei token che vi fanno accedere al vostro conto online.. [Marzo 2011]
- **Etc..**

Volendo quindi dare una risposta a questa domanda mi sono chiesto: **ma in Italia come siamo messi?**

C'era una volta...

PC dedicato



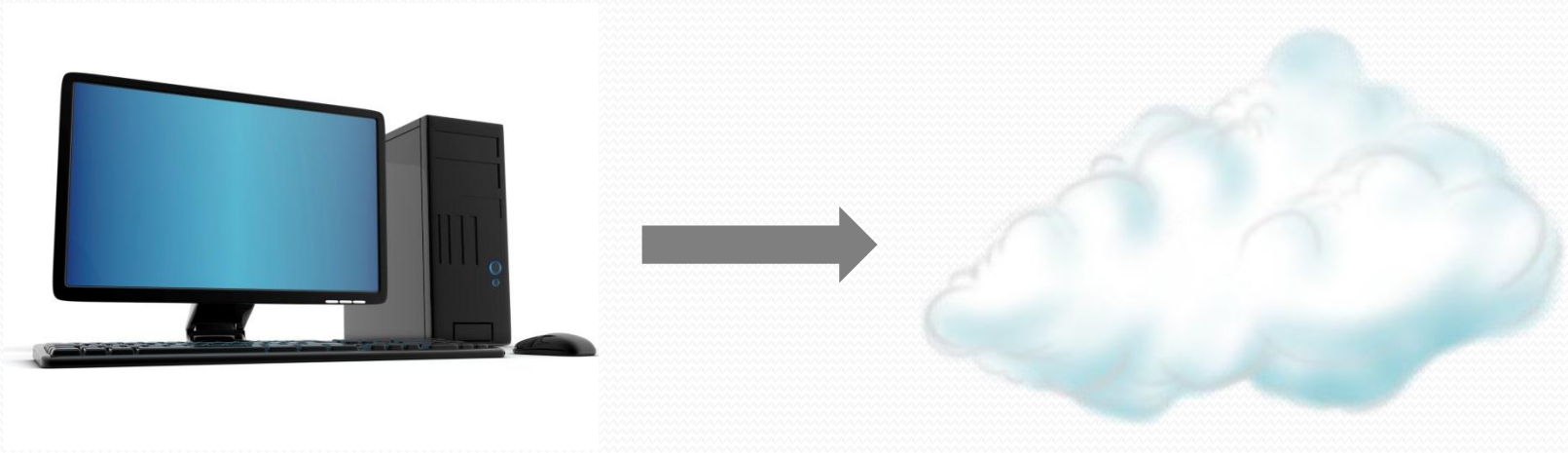
Hard disk locale



Dati memorizzati quasi esclusivamente dentro il PC dell'utente o al massimo in un server della rete locale.

- Volendo operare una disclosure responsabile, se si scopriva la vulnerabilità in un software **locale**, si faceva la segnalazione del problema al **vendor**;
- Il vendor esaminava il caso e se fondato emetteva un bollettino e/o rilasciava una **patch**.
- La patch poteva essere vista come una **forma di democrazia**:
«io vendor faccio conoscere a tutti gli utenti che il mio software soffre di una falla e li metto al corrente del fatto che utilizzando quel software senza patch, un malintenzionato potrebbe arrivare ad estrapolarne i dati contenuti o svolgere altre attività malevole».
- L'utente che aveva installato il software buggato deteneva ancora il controllo dei propri dati e della loro sicurezza (es. poteva decidere se installare o meno la patch).

Oggi tutto è una grande Web Application...




Nella maggior parte dei casi i nostri dati sono quasi sempre online e l'utilizzo dei computer/dispositivi di comunicazione (PC, notebook, netbook, tablet, smartphone, etc..) si è ridotto a strumento volto più a consultarli che memorizzarli. In questo caso per l'utente è difficile avere il controllo dei suoi dati e della sicurezza di quei sistemi che li contengono.

In un mondo perfetto:

- Volendo operare una disclosure responsabile, data una web app vulnerabile che espone i dati di **N** utenti, la falla in questione viene segnalata al gestore del sito o all'azienda responsabile.
- La segnalazione viene analizzata e accertata da chi di competenza così da giungere alla risoluzione del problema (**il rubinetto si chiude**).
- Il responsabile del trattamento dei dati dell'azienda allerta gli utenti coinvolti che vi è stato un problema che ha esposto i loro dati secondo le modalità **X** ed i tempi **Y** (fase di **Incident Handling**, volta anche ad assodare che prima della segnalazione bonaria nessun altro sia effettivamente riuscito ad accedere al DB e trafugare quei dati)
- L'utente, una volta a conoscenza di quanto avvenuto, ha tutti gli strumenti in mano per decidere se esercitare i diritti che gli vengono riconosciuti dalla legge sulla privacy (196/03), ad esempio richiedere la cancellazione dei suoi dati da quell'archivio/DB.



**Ma è davvero così che
vanno le cose?**

- 
- Per darmi una risposta dovevo trovare dei sistemi vulnerabili che esponessero **dati personali** su Internet.
 - Le vulnerabilità trovate dovevano essere semplici, quasi basilari.

Il fine...

- Dare una risposta a queste semplici domande:
 - Era possibile arrivare a dei casi di **data leaking** nostrani sfruttando vulnerabilità banali che non richiedessero grossi sforzi come ad esempio bypassare il meccanismo di autenticazione di una web application? (cioè, sottinteso....**stiamo davvero messi così male?**)
 - Il vendor o l'azienda che riceveva la segnalazione come avrebbe risolto il problema? Seguendo l'iter etico precedentemente mostrato? In caso contrario, quanto ci si sarebbe allontanati da quel modello di riferimento?

Caso 1: Descrizione

- Famoso marchio italiano della moda. Fatturato nell'ordine delle centinaia di milioni di euro.
- **Il problema:** semplicemente visitando la pagina sottostante si ottenevano i dati personali (*nome, cognome, email, indirizzo, nazione, località, provincia, CAP, telefono, data di nascita*) di un utente identificato da un **ID** (segnato in corsivo). Bastava sostituire l'ID dalla query string e si ottenevano i dati di un altro utente:

[http://omissis/zzzz/index.asp?par=B5516OMA11075&ABCDEFGG](http://omissis/zzzz/index.asp?par=B5516OMA<u>11075</u>&ABCDEFGG)

Caso 1: Implicazioni

- Attacco facilmente automatizzabile per estrarre tutte le utenze dal DB (valutati oltre 130 mila record presenti).
- L'attacker avendo in mano decine di migliaia di record che ha estratto dal portale X, conosce quindi le abitudini di quegli utenti ed i loro dati personali, pertanto può personalizzare un attacco su misura (e-mail? telefonata al cell? IM?).
- Solitamente si è molto più credibili quando ci si presenta alla vittima come azienda X, elencando una serie di dati personali che la riguardano e che la vittima stessa sa di aver fornito effettivamente all'azienda X.

Caso 1: La segnalazione (a)

- Trovo il nome del responsabile del trattamento dei dati direttamente dal portale aziendale e cerco di farmelo passare al telefono (questa persona è anche il **CEO**).
- Dalla segreteria, pur spiegando l'impellenza del problema, mi dicono che non me lo possono passare se non ho un appuntamento (figurati se il super boss si espone). Chiedo quindi un appuntamento e lascio l'email ed il mio numero di telefono per essere ricontattato.
- Vengo ricontattato dopo un po' e mi fanno capire che il CEO non mi vuole parlare (devono «filtrare» la chiamata). Mi rimandano quindi ad una sua sottoposta (responsabile del portale) che detta le linee guida e tiene i contatti con la web agency che cura il sito per loro conto.
- Faccio a lei la segnalazione per e-mail, affermando che il loro sito espone i dati di ignari utenti verso Internet e mettendomi a disposizione per una dimostrazione live del problema. Prima reazione: **incredulità, negazione**.

Caso 1: La segnalazione (b)

"Premesso il fatto che la nostra web agency ha adottato le normali best practice per lo sviluppo del sito e del suo backend, quindi non ci sentiamo in difetto in materia di eventuali dati sensibili rilasciati dai nostri utenti, gradirei anzitutto avere una prova di ciò che sta affermando: Le chiedo cortesemente un'estrazione, per esempio, degli utenti registrati in data [omissis] 2011. Lei scrive che chiunque accede al nostro sito può accedere anche "a questi dati e consultarli", ma a noi questo non risulta: da controlli personali e attraverso la nostra agenzia web questo ci risulta impossibile;"

Caso 1: La segnalazione (c)

- Procedo con alcune estrazioni di record dal portale vulnerabile al solo fine di esaudire la sua richiesta e glielo trasmetto un paio per e-mail.
- Poco dopo mi accorgo che tra le estrazioni di prova ho tirato fuori un record con il nome e cognome della responsabile aziendale con cui sto intrattenendo lo scambio di e-mail (anche l'account di posta elettronica coincide).
- La chiamo direttamente al suo cellulare: imbarazzata ma... **adesso mi crede!** 😊

Caso 1: La segnalazione (d)

- Fissiamo un altro appuntamento telefonico per l'indomani.
- Prima di dimostrarle praticamente la falla mi faccio ancora un po' più intraprendente. Le chiedo rassicurazioni circa il fatto che gli utenti vengano messi al corrente delle modalità e dei tempi legati all'esposizione dei propri dati dopo che il problema sarà stato risolto.
- **Reazione:** è possibilista ma è più focalizzata a millantarmi possibili sbocchi lavorativi da cui potrei trarre benefici a conclusione della vicenda.
- Le mostro dove sta il problema e ci lasciamo con la promessa che una volta risolto qualcuno si sarebbe rifatto vivo.

Caso 1: La Post-segnalazione (a)

- Trascorso qualche tempo, nessuno si fa sentire, quindi mi rifaccio vivo io.
- Mi dicono che il problema è stato risolto ma questa volta cambiano i toni: **cercano di minimizzare!**
 - *«anzitutto abbiamo risolto il problema della visualizzazione delle variabili in chiaro (anche se poi c'era un stringa davanti e una dietro quindi non era così immediato accedere ai dati di altri utenti), che erano visibili solamente nel caso di iscrizione dal form della Newsletter [...] e che gli internauti senza particolari conoscenze tecnico/informatiche non avrebbero mai intercettato.»*

<http://omissis/zzzz/index.asp?par=B5516OMA11075&ABCDEFG>

- Insisto sull'avvisare dell'accaduto gli utenti i cui dati sono stati esposti:
 - *«Tu hai visto i dati perché sei un abile tecnico che si occupa di sistemi di sicurezza, ma scusami se faccio un esempio banale... tutti sappiamo che attraverso alcuni strumenti illegali sono riusciti ad entrare addirittura sul server di Google e della Nasa (aziende non proprio delle stesse dimensioni nostre)... »*

Caso 1: La Post-segnalazione (b)

- Paventando a questo punto il timore che i dati potessero già essere stati trafugati vista la semplicità della procedura di estrazione (contrariamente a quanto affermato dal mio interlocutore basta cambiare il numero dalla query string) domando se hanno fatto un controllo sui log.
- La risposta in soldoni è che nessun altro oltre me aveva fatto la segnalazione del problema («*Evidentemente la curiosità di approfondire questa tematica è scaturita solamente da parte tua*»). Quindi secondo lei nessun altro poteva essersi appropriato di quei dati.
- Le spiego che non funziona così: «*se il ladro vuole rubare, non lo comunica di certo prima!*»

Caso 1: La Post-segnalazione (c)

- In realtà nel frattempo mi accorgo che non hanno risolto un bel niente. Gli stessi dati sono infatti raggiungibili da un'altra parte del sito e sempre con una semplice richiesta HTTP GET.
- Decido però a questo punto che è inutile procedere con un'altra segnalazione (è assodato che non avviseranno i propri utenti). Tuttavia gli metto ugualmente la pulce nell'orecchio:
 - *«E se ti dicessi che invece non è stato risolto un bel niente e che il problema è ancora lì...come la prendereste? Avvisereste questa volta gli utenti?? Sareste disposti a mettermelo per iscritto?»*
- **Risposta:** *«dato che io non ho alcun potere decisionale in merito sottoporro la questione al prossimo consiglio d' amministrazione e ti terrò informato»*

Caso 1: Tirando le somme

- Dopo la segnalazione:
 - Non c'è stata risoluzione della falla (il problema è ancora lì)
 - Non c'è stata fase di **Incident Handling**. Deduco ciò dalle loro affermazioni. Se hanno guardato da qualche parte lo hanno fatto nel modo e nel punto sbagliato: «*sul nostro database non ci sono state segnalazioni di intrusioni*»
 - Gli utenti non sono stati avvisati ed i loro dati sono ancora lì alla mercé di chiunque.

Caso 2 e 3: Descrizione

- Aziende del settore Energy & Utilities con partecipazione mista (pubblica/privata) con svariati milioni di euro di capitale sociale. Entrambe S.p.A.
- Il Caso 2 è una situazione simile alla precedente. Senza necessità di autenticarsi, utilizzando la query string sotto, si ottengono i dati personali di un'utenza (*nome, cognome, indirizzo, informazioni sui contatori, etc..*) e lo storico delle bollette fatturate (*importo, se o meno è stato pagato, etc..*)

http://xxxxx/yyyyy/zzzzz/servizi?_servizi_xxxx_action=kkkkk&_servizi_codice=ABCDEFG

- Basandomi sulle possibili iterazioni di **ABCDEFG** calcolo l'esposizione di circa 120 mila record.

Caso 2 e 3: Descrizione

- Il Caso 3 è ancora più eclatante: SQL Injection sulla form di autenticazione con attivazione verbose dei messaggi di errore del DB:

```
Error in statement SELECT * FROM XXXX_UTENTI WHERE  
YYYY_USERNAME = '\' AND KKKK_PWD_HASH = '[omissis]  
ORDER BY CCC_DATA_INIZIO_VAL execution.<br>Array [...][SQL  
Server]Sintassi non corretta in prossimità di 'XXXXX'. [message] =>  
[Microsoft][SQL Server Native Client 10.0][SQL Server]Sintassi non  
corretta in prossimità di 'XXXXX'. ) [...]
```

- Le informazioni che si possono tirare fuori sono sovrapponibili a quelle del Caso 2, con l'aggiunta però di dati finanziari per quegli utenti che hanno deciso di attivare il pagamento automatico delle bollette tramite RID o con carta di credito.
- Un **SELECT COUNT()** rivela che qui ci sono 380 mila record.

Caso 2: Segnalazione (a)

- Contatto un responsabile comunale che fa parte del C.d.A. dell'azienda. Ci incontriamo e gli espongo il problema. Prima reazione: **Menefreghismo**.
- Si prende i miei contatti e mi promette che si farà risentire per fissarmi un incontro con chi tecnicamente potrà gestire la cosa.
- Passano due mesi e nessuno si fa vivo.
- Invio una raccomandata alla sede legale dell'azienda e gli spiego il problema.
- Mi chiamano al telefono qualche giorno dopo e mi fissano un appuntamento con l'amministratore delegato della baracca (avevo chiesto espressamente di parlare con lui nella raccomandata)

Caso 2: Segnalazione (b)

- All'appuntamento porto un paio di estrazioni di prova.
- Quando faccio pressioni ed indico che vi è l'urgenza di avvisare gli utenti circa l'esposizione dei loro dati attraverso Internet il **CEO** cambia discorso e mi **millanta possibili sbocchi lavorativi**:

«mi dia il tempo di fornire queste estrazioni ai miei tecnici e se non riusciranno a capire da soli come individuare e risolvere il problema, licenzierò loro tre ed assumerò lei»

- Se insisto sulla questione etica e sul fatto che quella falla è probabilmente vecchia quanto il portale (3 anni di esposizione attraverso Internet), si mette sulle difensive:

«sono entrati dentro i sistemi della Nasa e di Google quindi ci sta che siamo stati colpiti anche a noi»

Caso 2: Segnalazione (c)

- Ci ridiamo appuntamento dopo due settimane (il tempo che vuole dare ai suoi tecnici per capire il problema e risolverlo).
- Trascorrono le due settimane ma nessuno si fa sentire.
- E' trascorso un mese e mezzo da allora e nessuno si è fatto sentire.
- Ancora oggi il problema è lì...

Caso 3: Segnalazione (a)

- Poiché ho un amico che vive nella zona in cui opera l'azienda del caso 3, chiedo a lui di seguire la cosa e di aggiornarmi sugli sviluppi.
- Gli fornisco i dettagli del problema, quindi lui si mette in contatto con chi di dovere e fa la segnalazione.
- A quattro mesi di distanza la SQL Injection è ancora lì.

Caso 4: Descrizione

- Azienda internazionale operante nel settore telco con pannello di amministrazione del Web Application Server (ce ne sono più di uno in cluster) senza password!
- Il portale in questione chiede esplicitamente di inserire i propri dati (*nome, cognome, email, etc..*) per poter essere ricontattati da un commerciale qualora si fosse interessati ad un prodotto o servizio.
- Numero di record presenti: (?)
 - Per guardare cosa c'è dentro il DB a backend dovrei fare il deployment di un'applicazione e l'operazione diventerebbe troppo invasiva.
- Decido quindi di passare direttamente alla fase della segnalazione del problema.

Caso 4: Segnalazione (a)

- Dopo varie peripezie trovo un contatto tecnico (anche se non diretto) con cui interloquire.
- Mi chiede dove sta il problema e gli rispondo che è **architetturale** e non **applicativo** (come lui pensava) e che desideravo parlare con qualcuno che stesse più in alto di lui (ho imparato che certi discorsi sono inutili se non miri al CEO o al responsabile del trattamento dei dati).
- Mi chiede allora una prova di quello che affermo. Gli trasmetto per email gli indirizzi IP delle macchine interne coinvolte.
- A questo punto chiedo esplicitamente quando gli utenti verranno avvisati. Mi risponde che ha organizzato una conference call per la settimana successiva dove potrò chiederlo direttamente al responsabile del trattamento dei dati che sarà presente.
- La conference call viene ulteriormente spostata ma alla fine riusciamo a farla un paio di giorni dopo. Nel frattempo sono passate 2 settimane dal mio contatto iniziale...

Caso 4: Segnalazione (b)

- Durante la confcall cerco per due volte (la prima un po' più diplomaticamente, la seconda un po' più esplicitamente) di chiedere al responsabile del trattamento come intendesse procedere nell'avvisare gli utenti dell'esposizione dei loro dati.
- Ottengo risposte evasive: «*Ti garantiamo che verrà avviata al più presto un'intera sessione di Assessment sulla piattaforma vulnerabile*». Anche qui ottengo promesse lavorative: «*sono sicuro che si sarà occasione in futuro di collaborare*» mi dirà più avanti nel corso della telefonata.
- Capisco l'antifona e faccio presente dove sta «tecnicamente» il problema. Il responsabile del trattamento mi dice che i sistemisti lo avevano già risolto perché avevano notato nei giorni scorsi un'attività sospetta (in realtà avevano risolto poco prima che iniziasse la conference call, appena in mattinata). Mi viene quindi il dubbio che avessero risolto anche a seguito di alcune mie dritte passate al primo interlocutore (se ti dico che il problema è infrastrutturale non hai bisogno di indagare più di tanto: guardi a front-end). Resta il fatto che avevano riscontrato attività sospetta solo 2 settimane dopo.
- Anche qui in realtà non hanno risolto una mazza. Ci sono altri punti di ingresso che non sono stati coperti.

Caso 4

- E gli sbocchi lavorativi?
- Decido di farmi insistente....
- Nulla di fatto. Come immaginavo è solo il contentino per tenerti buono...

Tirando le somme... (1)

- In Italia siamo pieni zeppi di siti che maneggiano dati personali senza il rispetto della 196/03, malgrado ciò che si legge nelle informative...
- 4 i casi di Data Leaking segnalati...
- Il 50% delle volte si è arrivati all'affermazione da parte dell'azienda colpita di aver risolto il problema. L'altro 50% dopo la segnalazione non si è più fatto vivo...
- Nessuno ha proceduto ad avvisare gli utenti circa tempi e modalità dell'esposizione dei loro dati...

Tirando le somme... (2)

- In realtà le vulnerabilità rimangono anche dopo le segnalazioni...
- In totale sono **ZERO** i casi risolti e più di **600 mila** i record personali (e/o con dati sensibili) ancora facilmente raggiungibili attraverso Internet...
- In questo contesto la **responsible disclosure è inutile**: non accadrà nulla fino a quando non si forzeranno le imprese a rendere pubblici casi di data leaking/esposizione dei dati degli utenti o non vi sarà una legislazione più aperta (chi fa la segnalazione non può nemmeno denunciare l'accaduto pubblicamente se la falla non viene risolta).