DATA security

SANS TOP-20

Versione 8.0 del 28 Novembre 2007

I rischi per la sicurezza SANS Top-20

(Aggiornamento 2007)

Introduzione

Sette anni or sono, il SANS Institute e il National Infrastructure Protection Center (NIPC) presso l' FBI rilasciarono un documento che riassumeva le Dieci vulnerabilità più critiche per la sicurezza in Internet. Migliaia di organizzazioni hanno riposto la loro fiducia in quella lista e sulle liste allargate alle Top 20 che sono seguite negli anni successivi, concentrando quindi i loro sforzi nel correggere in via prioritaria i problemi più pericolosi.

Il panorama delle minacce è molto dinamico e richiede ad ogni cambiamento l'adozione delle misure di sicurezza più aggiornate. Anche prendendo in considerazione solo l'anno appena trascorso, si nota come le tipologie di vulnerabilità sfruttate per attaccare i sistemi siano molto diverse da quelle utilizzate in passato. Ecco alcune osservazioni::

- I sistemi operativi presentano un numero minore di vulnerabilità che possano portare a una diffusione estesa di worm Internet. Per fare un confronto, nel periodo 2002-2005 worm di Microsoft Windows come Blaster, Nachi, Sasser e Zotob infettarono un numero enorme di sistemi affacciati a Internet. Dal 2005 non si sono verificate infezioni di worm mirati ai servizi Windows di scala così ampia. Oggi però possono portare a dei worm vulnerabilità presenti i software antivirus, in applicazioni per il backup o per altri servizi molto diffusi. Il worm più rilevante dello scorso anno è stato quello che sfrutta una vulnerabilità di buffer overflow dell'antivirus Symantec.
- Abbiamo rilevato una crescita significativa del numero di vulnerabilità lato client, tra cui le vulnerabilità nei browser, nei software di office automation, nei lettori multimediali e in altre applicazioni desktop. Queste vulnerabilità sono state scoperte su diversi sistemi operativi e vengono sfruttate intensamente e in modo selvaggio, costituendo spesso terreno fertile per i botnet.
- Gli utenti a cui i datori di lavoro consentono di navigare in Internet sono diventati una fonte importante di rischio per la sicurezza delle loro organizzazioni. Fino a pochi anni fa il compito primario per garantire la sicurezza aziendale era rendere sicuri i server e i servizi di rete. Oggi è altrettanto importante, forse ancora più importante, prevenire la compromissione dei computer degli utenti da parte di pagine web con codici maligni o di altri attacchi diretti ai client.
- Le vulnerabilità in applicazioni web, siano queste derivate da codice personalizzato o open source, rappresentano quasi la metà del numero totale di vulnerabilità scoperte nell'anno appena trascorso. Queste vulnerabilità sono state ampiamente sfruttate per trasformare siti web affidabili in server portatori di maligni exploit per i client e di truffe di phishing
- Le configurazioni di default di molti sistemi operativi e servizi continuano ad essere deboli e continuano a prevedere password di default che non vengono modificate o password troppo semplici da indovinare. Di conseguenza ancora nel 2007 molti sistemi sono stati compromessi attraverso attacchi brute force o da dizionario alle password!
- Gli aggressori stanno escogitando sistemi più creativi per ottenere dati critici dalle varie organizzazioni. Pertanto è ora ancor più fondamentale verificare la natura dei dati presenti ai confini del sistema di difesa aziendale.

La SANS Top-20 2006 è una lista largamente condivisa delle vulnerabilità che richiedono una riparazione immediata. Si tratta del risultato di un processo che coinvolge dozzine dei più importanti esperti di sicurezza mondiali che provengono dalla agenzie governative più impegnate nella sicurezza di Gran Bretagna, Stati Uniti e Singapore, dalle principali case produttrici di software e le più importanti società di consulenza, dai maggiori programmi universitari di ricerca nel campo della sicurezza, dall'Internet Storm Center e da molte altre organizzazioni di utenti. Potete trovare una lista dei partecipanti alla fine del documento.

La lista SANS Top-20 2007 non è "cumulativa." Abbiamo inserito solo vulnerabilità critiche che risalgono all'ultimo anno circa. Se quindi non avete corretto e aggiornato i vostri sistemi da molto tempo è altamente raccomandabile che sistemiate anche le vulnerabilità indicate nella Top-20 2005, oltre che quelle presenti nella lista 2006. Alla fine di questo documento troverete una breve serie di SANS Top-20 FAQ (domande frequenti) che rispondono ai dubbi che potreste avere riguardo il progetto in questione e il sistema con cui la lista viene creata..

La lista di quest'anno si differenzia dalla liste degli anni scorsi che puntavano l'attenzione su vulnerabilità tecniche molto specifiche, risolvibili migliorando una configurazione o applicando una patch. Gli aggressori oggi si muovono molto rapidamente e soluzioni di quel genere sarebbero oggi quasi immediatamente superate. Per tali ragioni la lista di quest'anno si concentra nell'analisi delle aree che gli attacchi prendono maggiormente di mira e per le quali aziende, enti ed organizzazioni hanno bisogno di migliorare le proprie procedure di sicurezza per garantire l'efficace applicazione delle necessarie correzioni tecniche.

La lista SANS Top-20 è un documento in continuo aggiornamento. Contiene istruzioni dettagliate e riferimenti a informazioni supplementari utili per risolvere i problemi di sicurezza. Quando vengono scoperte nuove minacce critiche o sono identificati metodi di protezione più aggiornati o più efficaci, vengono aggiornati la lista delle vulnerabilità e le istruzioni per correggerle; in questo processo il vostro contributo è sempre gradito. Questo documento si basa sul consenso di una intera comunità: la vostra esperienza nel combattere gli attacchi e nell'eliminare le vulnerabilità può aiutare quelli che verranno dopo di voi. Inviate i vostri suggerimenti via e-mail all'indirizzo top20@sans.org

Vulnerabilità lato client in:

C1. Browser Web

C1.1 Descrizione

Microsoft Internet Explorer è il browser per la navigazione del web più diffuso e viene installato per default su tutti i sistemi Windows. Le versioni più datate o non aggiornate di Internet Explorer contengono svariate vulnerabilità che possono portare a problemi di memoria, spoofing (siti web ingannevoli) e all'esecuzione incontrollata di script potenzialmente dannosi. I problemi più gravi sono quelli che portano all'esecuzione di codice in modalità remota senza alcun intervento dell'utente mentre si visita una pagina web o si legge un messaggio email. Il codice per sfruttare molte delle vulnerabilità critiche di Internet Explorer è disponibile pubblicamente. Come se non bastasse, Internet Explorer viene utilizzato come leva per sfruttare le vulnerabilità presenti in altri componenti fondamentali di Windows come l'Help HTML e il Graphics Rendering Engine. Durante l'anno appena trascorso sono state scoperte **centinaia di vulnerabilità in controlli ActiveX** installati da Microsoft o da altri produttori di software. Anche queste vengo sfruttate tramite Internet Explorer.

Mozilla Firefox è il browser web più popolare dopo Internet Explorer e anch'esso raccoglie una parte importante delle vulnerabilità. Nel corso del 2007 ha rilasciato molti aggiornamenti per correggere le vulnerabilità scoperte divenute pubbliche. Come per Internet Explorer, le versioni più vecchie o non aggiornate di Firefox contengono molte vulnerabilità che possono portare a problemi di memoria, spoofing ed esecuzione incontrollata di script o codice dannoso. I siti web che sfruttano le vulnerabilità dei browser di solito ospitano diversi exploit e lanciano di volta in volta gli exploit specifici per il browser che la potenziale vittima sta utilizzando.

Con l'esplosione dei contenuti multimediali nei siti web, un parallelo aumento è stato osservato nel numero di *Browser Helper Object* di terze parti e di plug-in utilizzati per accedere a vari tipi di file MIME, come documenti o multimedia. Questi plug-in spesso si basano su linguaggi di scripting lato client quali Macromedia Flash o Shockwave. Molti di questi plug-in sono installati in modalità (semi)trasparente da un sito web. Gli utenti possono quindi non essere consapevoli del fatto che un *Helper Object* o un plug-in a rischio è installato sul proprio sistema. Questi plug-in aggiuntivi rappresentano delle nuove autostrade per hacker che intendono sfruttarle per compromettere i computer degli utenti che visitano siti web maligni.

Nel mese di ottobre 2007, ad esempio, si è scoperto che i sistemi che eseguono Windows XP e Windows Server 2003 con Windows Internet Explorer 7 non gestiscono correttamente alcuni Uniform Resource Identifiers (URI). Creando un particolare URI in un documento PDF, gli aggressori sono stati in grado di eseguire comandi arbitrari su sistemi vulnerabili

Per quanto alcuni plug-in come Adobe Reader e Quicktime eseguano controlli sulla versione installata e forniscano una funzione di aggiornamento, queste funzioni vengono spesse ignorate o considerate con irritazione dagli utenti. Spesso è poi difficile rilevare la versione installata di un plug-in. Ad esempio, i sistemi possono avere installato diverse versioni di Shockwave per motivi di compatibilità all'indietro, ma l'utente non può facilmente scoprire la versione o le versioni in esecuzione

Queste vulnerabilità sono state largamente utilizzate per installare spyware, adware ed altro software dannoso sui sistemi degli utenti. I problemi di spoofing sono la base per condurre gli attacchi di phishing (la duplicazione di pagine web atta carpire all'utente informazioni personali, finanziarie o semplicemente le sue password). Sono molti anche i casi di vulnerabilità cosiddette zero-days per le quali la patch (la rettifica della parte del software che consente di risolvere il problema) non era disponibile al momento in cui la vulnerabilità è stata resa pubblica. Molti vulnerabilità tra i plug-in sono state ampiamente sfruttate da siti web maligni prima che le patch siano state messe a disposizione dal fornitore. Nel solo 2007, Microsoft ha rilasciato svariati aggiornamenti per Internet Explorer:

- Aggiornamento cumulativo per la protezione di Internet Explorer (939653) (MS07-057)
- Una vulnerabilità in Vector Markup Language può consentire l'esecuzione di codice in modalità remota (938127) (MS07-050)
- Aggiornamento cumulativo per la protezione di Internet Explorer (937143) (MS07-045)
- Aggiornamento cumulativo per la protezione di Internet Explorer (933566) (MS07-033)
- Vulnerabilità in GDI possono consentire l'esecuzione di codice in modalità remota (925902) (MS07-017)
- Aggiornamento cumulativo per la protezione di Internet Explorer (931768) (MS07-027)
- Aggiornamento cumulativo per la protezione di Internet Explorer (928090) (MS07-016)

- La vulnerabilità in Vector Markup Language può consentire l'esecuzione di codice in modalità remota (929969) (MS07-004)

Si noti che il più recente aggiornamento cumulativo per la protezione di Internet Explorer comprende tutti gli aggiornanti cumulativi precedenti. Da notare anche che MS07-017 non elenca vulnerabilità di Internet Explorer, ma la via più comune per sfruttare è. Appunto, tramite Internet Explorer.

C1.2 Sistemi operativi interessati

Per quanto in teoria qualsiasi web browser e qualsiasi sistema operativo sia vulnerabile, i browser web più diffusi tendono ad essere presi maggiormente di mira dagli attacchi. Oggi i due web browser più popolari in Internet sono Microsoft Internet Explorer e Mozilla Firefox.

Internet Explorer 5.x, 6.x e 7 operanti su qualunque versione di Windows sono colpiti.

Firefox operante su qualunque versione dei sistemi operativi compatibili è potenzialmente vulnerabile.

Siccome i plug-in sono generalmente utilizzati per consentire l'accesso a formati di file di terze parti, molte vulnerabilità dei plug-in affliggono tutti i browser compatibili su tutti i sistemi operativi. Qualsiasi browser web che gira su qualsiasi versione di qualsiasi sistema operativo è potenzialmente vulnerabile.

C1.3 Riferimenti CVE

Internet Explorer

CVE-2006-4697, CVE-2007-0024, CVE-2007-0217, CVE-2007-0218, CVE-2007-0219, CVE-2007-0942, CVE-2007-0944, CVE-2007-0945, CVE-2007-0946, CVE-2007-0947, CVE-2007-1749, CVE-2007-1750, CVE-2007-1751, CVE-2007-2216, CVE-2007-2221, CVE-2007-2222, CVE-2007-3027, CVE-2007-3041, CVE-2007-3826, CVE-2007-3892, CVE-2007-3896

Firefox

CVE-2007-0776, CVE-2007-0777, CVE-2007-0779, CVE-2007-0981, CVE-2007-1092, CVE-2007-2292, CVE-2007-2867, CVE-2007-3734, CVE-2007-3735, CVE-2007-3737, CVE-2007-3738, CVE-2007-3845, CVE-2007-4841, CVE-2007-5338

Adobe Acrobat Reader

CVE-2007-0044, CVE-2007-0046, CVE-2007-0103, CVE-2007-5020

I riferimenti CVE per plug-in come i Lettori multimediali sono elencati nella sezione C4.

C1.4 Come stabilire se si è a rischio

Utilizzate un qualsiasi vulnerability scanner per verificare se il vostro sistema è protetto rispetto ai problemi elencati.

Per Internet Explorer prendete in considerazione anche l'uso di sistemi per la valutazione dello stato degli aggiornamenti dei vostri sistemi quali Microsoft Windows Server Update Services (WSUS), Microsoft Baseline Security Analyzer (MBSA), Windows Live Scanner o Systems Management Server (SMS).

Per scoprire quali sono i plug-in usati più di recente da Internet Explorer 7, selezionate *Strumenti -> Opzioni Internet*. Alla sezione *Programmi*, scegliete *Gestisci componenti aggiuntivi*. Potete scegliere diverse viste dei plug-in del browser, compresa quella dei componenti aggiuntivi attualmente caricati, quelli che sono stati usati da Internet Explorer e quelli configurati per essere eseguiti senza richiedere l'autorizzazione dell'utente. Potrete disabilitare ciascuno di questi componenti aggiuntivi sezionando lo specifico plug-in e scegliendo *Disabilita*.

Per Firefox, selezionate *Strumenti -> Opzioni -> Contenuti -> Tipi di File -> Gestione* per vedere come Firefox gestisce i vari formati di file.

Alcune terze parti hanno iniziato a rilasciare strumenti come Secunia PSI (attualmente in versione beta) che analizzano la versione e le patch degli *helper object* che il browser usa.

C1.5 Come proteggersi da queste vulnerabilità

- Se utilizzate Internet Explorer sui vostri sistemi Windows XP, il modo migliore per rimanere sicuri è quello di aggiornarli a Windows XP Service Pack 2. I miglioramenti nella sicurezza del sistema operativo e il Windows Firewall contribuiranno a ridurre i rischi. A coloro che non possono passare a Windows XP con Service Pack 2 è vivamente raccomandato l'utilizzo di un diverso browser.

- Si raccomanda anche il passaggio alla versione 7 di Internet Explorer, che fornisce una sicurezza maggiore rispetto alle versioni precedenti. L'ultima versione di Internet Explorer, IE7, viene distribuita da Microsoft come aggiornamento critico (KB926874)
- Mantenete i sistemi aggiornati con le patch e i service pack più recenti. Quando possibile, abilitate l'opzione Aggiornamenti automatici su tutti i sistemi.
- Per ridurre l'esposizione agli attacchi zero day, prestate attenzione ai Bollettini sulla sicurezza Microsoft e mettete in atto i suggerimenti per ridurre il pericolo prima che la patch sia disponibile.
- Per prevenire la possibilità di sfruttare le vulnerabilità che consentono l'esecuzione di codice in modalità remota a livello di Amministratore, si possono usare strumenti quali Microsoft DropMyRights eseguire Internet Explorer con "privilegi minimi".
- Evitate che componenti ActiveX vulnerabili siano operativi attraverso Internet Explorer con il meccanismo "killbit" (Interruzione dell'esecuzione di un controllo ActiveX in Internet Explorer)
- Molti programmi spyware vengono installati quali Assistente del Browser (*Browser Helper Object*). Un Browser Helper Object o BHO è un piccolo programma che viene automaticamente eseguito ogni volta che si avvia Internet Explorer e ne aggiunge alcune funzionalità. I Browser Helper Object possono essere individuati utilizzando uno scanner Antispyware.
- Utilizzate sistemi di Intrusion Prevention/Detection e software Anti-virus, Anti-Spyware e Malware per bloccare il codice di script HTML dannosi.
- I sistemi Windows 98/ME/NT non sono più supportati per quel che riguarda gli aggiornamenti. Coloro che ancora li usano dovrebbero valutare la possibilità di passare a Windows XP.
- Prendete in considerazione l'utilizzo di browser diversi, che non supportino la tecnologia ActiveX come,. Ad esempio, Mozilla Firefox.

C1.6 Come rendere sicuri i browser web

Per configurare le impostazioni di sicurezza di Internet Explorer:

- Scegliere *Opzioni Internet* dal menu *Strumenti*.
- Scegliere l'opzione *Protezione* e quindi impostare *Livello personalizzato* nell'area *Internet*.

La maggior parte delle vulnerabilità di IE vengono sfruttate attraverso Active Scripting o i Controlli ActiveX.

- Nella sezione *Esecuzione script*, scegliete *Disattiva* per la voce "*Consenti operazioni di copia tramite script*" per evitare che sia possibile vedere i contenuti dei vostri appunti (clipboard). Nota: Disabilitando Active Scripting è possibile che alcuni siti web non funzionino più correttamente.

I Controlli ActiveX sono meno conosciuti, ma sono potenzialmente molto più pericolosi in quanto permettono un maggiore accesso al sistema

- Scegliete *Disattiva* per la voce "*Scarica controlli ActiveX con firma elettronica*". Scegliete *Disattiva* anche per la voce "*Scarica controlli ActiveX senza firma elettronica*" e "*Inizializza e esegui script controlli ActiveX non contrassegnati come sicuri*".

Gli applet Java hanno di solito potenzialità anche maggiori rispetto agli script.

- Sotto *Microsoft VM*, scegliete *Protezione Alta* per le *Autorizzazioni Java*, in modo da mantenere sotto controllo gli applet Java ed evitare un accesso con privilegi al vostro sistema.
- Sotto *Varie*, selezionate *Disattiva* alla voce "*Accesso all'origine dati a livello di dominio"*, per evitare gli attacchi Cross-site scripting.

Controllate anche non vi sia alcun sito sospetto nell'area *Siti attendibili* e nell'*Intranet Locale*, in quanto per queste aree le impostazioni di sicurezza sono inferiori rispetto alle altre.

Microsoft ha pubblicato una guida per migliorare la sicurezza di Internet Explorer (in inglese): "Internet Explorer 7 Desktop Security Guide". Essa prende in esame le nuove funzionalità e le impostazioni che possono essere modificate per ottenere una configurazione della sicurezza più "sigillata" per Internet Explorer 7.

Per configurare le impostazioni di sicurezza di Firefox:

- Scegliere *Opzioni* dal menu *Strumenti*.
- Ulteriori personalizzazioni della configurazione di Firefox si trovano su http://kb.mozillazine.org/About:config.

Per aggiornare i plug-in usati dai browser:

- La maggior parte dei plug-in presentano l'opzione "*Check for Updates*" o "*Controlla aggiornamenti*". Di solito si trova sotto i menu "*Opzioni*", *Preferenze*" o "*Aiuto*".
- Scegliete "*Controlla aggiornamenti* " per controllare che il software sia installato nella sua versione più recente.

C1.7 Approfondimenti

Informazioni sulla sicurezza dei Browser Web US-CERT
http://www.us-cert.gov/reading_room/securing_browser/browser_security.html

Internet Explorer 7 Desktop Security Guide
http://www.microsoft.com/downloads/details.aspx?FamilyID=6AA4C1DA-6021-468E-A8CF-AF4AFE4C84B2&displaylang=en

Microsoft Internet Explorer Weblog
http://blogs.msdn.com/ie/

Mozilla Security Center
http://www.mozilla.org/security/

Vulnerabilità di Firefox
http://www.mozilla.org/projects/security/known-vulnerabilities.html

@Risk: The Consensus Security Alert
https://www.sans.org/newsletters/risk/

C2. Software Office

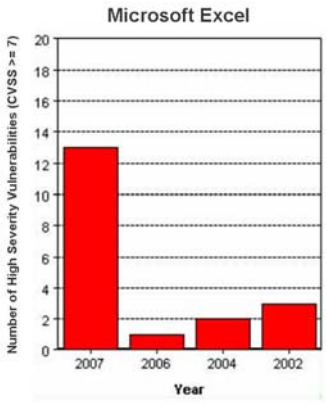
C2.1 Descrizione

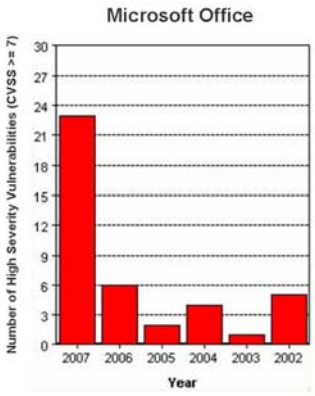
Questa sezione tratta delle vulnerabilità delle suite *office* per la produttività che includono client di posta elettronica, elaboratori di testo, fogli di calcolo, visualizzatori di documenti e applicazioni per la presentazione. Le vulnerabilità presenti in questi prodotti vengono sfruttate tramite le seguenti direttrici d'attacco:

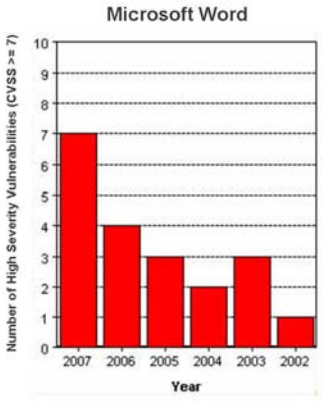
- L'aggressore spedisce un documento *office* con particolari caratteristiche in un messaggio email. Quando l'allegato viene aperto, i contenuti dannosi presenti nel documento sfruttano le vulnerabilità nel software *office*.
- L'aggressore inserisce il documento su un web server o una cartella condivisa e istiga l'utente ad accedere alla pagina Web o alla cartella condivisa. Si noti che in molti casi Internet Explorer apre automaticamente i documenti Microsoft Office, per cui la sola visita alla pagina Web o alla cartella è sufficiente per approfittare della vulnerabilità.
- L'aggressore opera con un server di news (NNTP) o dirotta il flusso di un feed RSS che spedisce documenti dannosi ai client news e RSS.

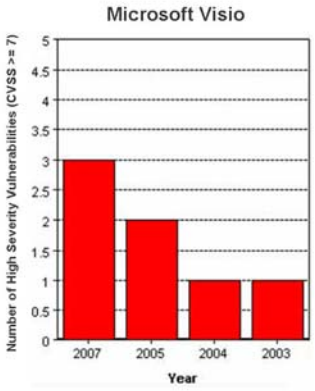
In tutti questi scenari, sul computer della vittima possono essere installati virus, trojan, spyware, adware (software che generano messaggi pubblicitari indesiderati), rootkit, keyboard logger (software che registrano ciò che si digita sulla tastiera) o qualsiasi altro programma predisposto da coloro che hanno avviato l'attacco.

Microsoft Office è la suite per la posta elettronica e la produttività individuale più utilizzata al mondo. Comprende applicazioni quali Outlook, Word, PowerPoint, Excel, Visio, FrontPage e Access. Sono stati riportati numerosi problemi critici per quanto riguarda le applicazioni MS Office e alcune di queste (CVE-2006-5574, CVE-2006-1305, CVE-2006-6456, CVE-2006-6561, CVE-2006-5994, CVE-2007-0515, CVE-2007-0671, CVE-2007-0045) sono state utilizzate nella fase zero-day, ovvero quando il codice per sfruttare la vulnerabilità, i dettagli tecnici della stessa o una dimostrazione della stessa sono stati resi pubblici prima che qualsiasi correzione fosse stata resa disponibile da parte di Microsoft.









I problemi critici rilevati lo scorso anno nei prodotti Office sono:

- Esecuzione di codice in modalità remota in Microsoft Excel (MS07-002)
- Esecuzione di codice in modalità remota in Microsoft Outlook (MS07-003)
- Esecuzione di codice in modalità remota in Microsoft Outlook (MS07-014)
- Esecuzione di codice in modalità remota in Microsoft Office (MS07-015)
- Esecuzione di codice in modalità remota in Microsoft Excel (MS07-023)
- Esecuzione di codice in modalità remota in Microsoft Word (MS07-024)
- Esecuzione di codice in modalità remota in Microsoft Office (MS07-025)
- Microsoft Outlook Express e Windows Mail (MS07-034)
- Esecuzione di codice in modalità remota in Microsoft Excel (MS07-036)
- Esecuzione di codice in modalità remota in Microsoft Excel (MS07-044)
- Esecuzione di codice in modalità remota in Adobe Reader e Acrobat (APSB07-18)
- Cross Site Scripting in Adobe Reader e Acrobat (APSA07-01)

C2.2 Sistemi operativi interessati

Windows 9x, Windows 2000, Windows XP, Windows 2003, Windows Vista, MacOS X sono tutti vulnerabili a seconda del software *office* installato.

C2.3 Riferimenti CVE

CVE-2007-0027, CVE-2007-0028, CVE-2007-0029, CVE-2007-0030, CVE-2007-0031, CVE-2007-0034, CVE-2007-0208, CVE-2007-0209, CVE-2007-0515, CVE-2007-0671, CVE-2007-0215, CVE-2007-1203, CVE-2007-0035, CVE-2007-0870, CVE-2007-1747, CVE-2007-1658, CVE-2007-1756, CVE-2007-3030, CVE-2007-3890

C2.4 Come stabilire se si è a rischio

Sono vulnerabili le installazioni di MS Office che operano senza le patch citate nei Bollettini Microsoft elencati nei record CVE citati qui sopra. Utilizzate un qualsiasi vulnerability scanner per verificare se il vostro sistema è protetto rispetto ai problemi elencati. Prendete anche in considerazione l'uso di sistemi per la

valutazione dello stato degli aggiornamenti dei vostri sistemi quali Microsoft Windows Server Update Services (WSUS), Microsoft Baseline Security Analyzer (MBSA), Windows Live OneCare o Systems Management Server (SMS).

C2.5 Come proteggersi dalle vulnerabilità dei software office

- Mantenete i sistemi aggiornati con le patch e i service pack più recenti. Se possibile, abilitate gli Aggiornamenti automatici su tutti i sistemi.
- Non aprite allegati che provengono da fonti non conosciute. Usate molta cautela anche nell'aprire allegati inaspettati anche nelle e-mail provenienti da indirizzi noti.
- Evitate la pratica del "*click browsing*" per evitare di aprire documenti su siti web sconosciuti. Il *click browsing* è l'abitudine di girare il web cliccando i link presenti nei messaggi e-mail o nei forum online. Se dovete tenere nota di un indirizzo, usate la funzione *preferiti* presente su qualsiasi browser
- Disabilitate la funzione di Internet Explorer che apre automaticamente i documenti Office.
- Configurate Outlook e Outlook Express con le impostazioni di protezione avanzate.
- Usate un vulnerability scanner per verificare il vostro livello di rischio.
- Utilizzate sistemi di Intrusion Prevention/Detection e software Anti-virus e per la rilevazione di Malware per evitare che documenti e risposte del server dannose raggiungano gli utenti finali della vostra rete.
- Utilizzate sistemi di filtro dei contenuti web e delle email a livello di rete per evitare che documenti Office dannosi raggiungano i sistemi degli utenti finali.

C2.6 Approfondimenti

Come rendere sicuro Microsoft Office
http://www.microsoft.com/technet/security/guidance/clientsecurity/2007office/default.mspx

C3. Client di posta elettronica

C3.1 Descrizione

La posta elettronica è una delle applicazioni fondamentali di Internet. Offre significativi vantaggi in termini di tempo, di denaro e di efficienza. Tuttavia, considerata la sua diffusione, si presta ad essere un diffuso vettore di molteplici vulnerabilità.

Sono molti gli attacchi che possono essere realizzati attraverso la posta elettronica:

- diffusione di malfare (virus, Trojan, keylogger, spyware, adware, rootkit ecc);
- phishing – Tentativi di sottrarre all'utente la password o altre informazioni confidenziali;
- spam – posta non desiderata (spazzatura);
- social engineering;
- attacchi denial of service – invio di un ingente numero di messaggi di posta elettronica a una potenziale vittima, server o casella di posta;

Questi attacchi possono provocare:

- danni a applicazioni, dati o sistema operativo;
- diffusione di informazioni confidenziali;
- propagazione di malware;
- l'uso dei sistemi colpiti come "bot" (macchine infette che cadono sotto il controllo di persone diverse dagli utenti legittimi, che le usano come proxy per attaccare altri sistemi o come postazioni di archiviazione e distribuzione di materiale pirata e pornografico);
- carenza di disponibilità dei sistemi e dei servizi;
- perdita di tempo, denaro e lavoro.

Attualmente tutti i sistemi operativi presenti sul mercato possono essere utilizzati come piattaforma per le applicazioni di client di posta.

Al momento, le applicazioni e-mail più diffuse sono:

- Microsoft Outlook (solo Microsoft Windows) e Outlook Express (solo Microsoft Windows; la vecchia versione era disponibile anche per Macintosh);
- Mozilla Thunderbird (Microsoft Windows, Linux, Mac OS X);
- Mail.app (solo Macintosh)

Ci sono altri client di posta (Opera mail, Pegasus, Mozilla SeaMonkey, The Bat!, Eudora ecc), ma la loro diffusione è relativamente bassa.

A prescindere dal sistema operativo utilizzato, è opportuno seguire alcune precauzioni ogni qualvolta utilizzate una applicazione di posta elettronica. (vedi C3.4 Come proteggersi contro le vulnerabilità dei client di posta elettronica)

C3.2 Sistemi operativi interessati

Windows 2000 Workstation e server, Windows XP Home e Professional, Windows Vista, Windows Server 2003, Mac OS X, Linux e Unix sono tutti potenzialmente vulnerabili.

C3.3 Riferimenti CVE

Microsoft Outlook Express, Outlook, Vista Windows Mail
CVE-2006-4868, CVE-2007-0033, CVE-2007-0034, CVE-2007-3897

Mozilla Thunderbird, SeaMonkey
CVE-2006-4565, CVE-2006-4571, CVE-2006-5463, CVE-2006-5747, CVE-2006-6502, CVE-2006-6504, CVE-2007-0777, CVE-2007-0779, CVE-2007-1282, CVE-2007-2867, CVE-2007-3734, CVE-2007-3735, CVE-2007-3845

Eudora
CVE-2006-0637, CVE-2006-6024, CVE-2006-6336, CVE-2007-2770

C3.4 Come proteggersi contro le vulnerabilità dei client di posta elettronica

- Rimuovete il client di posta dai sistemi server, o comunque dove non è necessario.
- Non eseguire nessun client di posta sui server e sulle postazioni di lavoro con informazioni confidenziali.
- Qualora doveste lanciare l'applicazione di posta su un qualsiasi sistema, assicuratevi:
  - di usare l'ultima versione del client di posta e di abilitare la funzione di aggiornamento automatico fornita dall'applicazione o dal sistema operativo.
  - Usate un software antivirus con l'aggiornamento delle firme dei virus. Se possibile, configurate il software antivirus affinché effettui un monitoraggio in tempo reale e aggiorni se quotidianamente le firme dei virus.
  - Non eseguite i client di posta su un account di amministratore, o su altri account con privilegi elevati.
  - Se dovete assolutamente utilizzare la posta elettronica quando siete collegati come Administrator su un sistema Windows, usate software come "Drop My Rights" per ridurre i privilegi disponibili sulle applicazioni di posta.
  - Non aprite nessun messaggio proveniente da mittenti sconosciuti o sospetti.
  - Non rispondete alla posta spazzatura (spam), anche se esiste un opzioni per cancellare l'iscrizione da una lista.
  - Visualizzate i messaggi di posta come testo normale, o con la minima formattazione possibile: HTML e RTF (due schemi di formattazione avanzata per i messaggi di posta) permettono lo scripting e altri metodi di attacco.
  - Non aprite alcun allegato senza averlo precedentemente esaminato con un programma antivirus.
  - Configurate il vostro client di posta in modo che non invii ricevute di ritorno o conferme di lettura.
  - Per lo scambio sicuro di posta utilizzate la firma digitale e/o la crittografia.

Dettagli e impostazioni di configurazione specifici delle applicazioni che possono migliorare la sicurezza del client di posta.

Outlook/Outlook Express/Windows Mail

Outlook Express è compreso nel pacchetto di Internet Explorer ed è installato per default su Windows 98, 2000, XP, 2003. Windows Vista sostituisce Outlook Express con Windows Mail.

- Se Outlook Express non è necessario al sistema è raccomandabile disinstallarlo.
- Se Outlook Express è installato nel sistema, mantenetelo aggiornato.
- Gli aggiornamenti di Outlook Express sono inclusi negli aggiornamenti di Internet Explorer. Se aggiornate Internet Explorer all'ultima versione o al livello più recente di service pack, automaticamente aggiornerete anche Outlook Express.

Parametri di configurazione per Outlook Express

- Outlook Express - *Strumenti - Opzioni – Lettura* – Selezionate "*Leggi tutti i messaggi in testo normale*".
- Outlook Express - *Strumenti - Opzioni - Conferme* - Selezionate "*Non inviare mai una conferma di lettura"*
- Outlook Express - *Strumenti - Opzioni - Protezione* – Selezionate l'area di protezione di Internet Explorer da utilizzare - Selezionate "*Area siti con restrizioni*"
- Outlook Express - *Strumenti - Opzioni - Protezione* – Selezionate "*Avvisa se altre applicazioni tentano l'invio di posta con l'account in uso*"
- Outlook Express - *Strumenti - Opzioni - Protezione* - Selezionate "*Non consentire salvataggi o aperture di allegati che potrebbero contenere virus*"
- Outlook Express - *Strumenti - Opzioni - Protezione* - Selezionate "*Blocca immagini e altri contenuti esterni nella posta elettronica HTML*"
- Outlook Express - *Strumenti - Opzioni - Manutenzione* - Selezionate "*Svuota la cartella Posta eliminate all'uscita*"
- Outlook Express - *Strumenti – Account - Posta elettronica* - Selezionate "*Proprietà*" per ciascun account di posta - *Server* – togliete l'opzione "*Ricorda password*"

Parametri di configurazione per Outlook

Impostazioni per Outlook 2003:

- Outlook - *Strumenti - Opzioni - Preferenze – Opzioni di posta elettronica* – Selezionate "*Visualizza tutti i messaggi standard in formato testo normale*".
- Outlook - *Strumenti - Opzioni - Protezione – Aree di sicurezza - Area* – Selezionate "*Siti con restrizioni*".
- Outlook - *Strumenti - Opzioni - Protezione - Download di immagini - Cambia impostazioni download automatico* – Selezionate "*Non scaricare automaticamente immagini o altro contenuto dei messaggi HTML*".
- Outlook - *Strumenti - Opzioni - Protezione - Download di immagini - Cambia impostazioni download automatico* – Selezionate "*Avvisa prima di scaricare contenuto durante la modifica, l'inoltro o la risposta a messaggi*".
- Outlook - *Strumenti - Opzioni - Preferenze – Posta indesiderata - Opzioni – Seleziona il livello di protezione per la posta indesiderata* – Scegliete "*Basso*", "*Alto*" o "*Solo elenchi indirizzi attendibili*".
- Outlook - *Strumenti - Opzioni - Preferenze – Posta indesiderata - Opzioni* - Selezionate "*Non attivare nei messaggi i collegamenti a siti potenzialmente pericolosi o fraudolenti*".
- Outlook - *Strumenti - Opzioni - Altro* - Selezionate "*Svuota la cartella Posta eliminata all'uscita*"
- Outlook - *Strumenti – Account di posta elettronica* – per ciascun account di posta elettronica togliete l'opzione "*Ricorda password*".

Le stesse impostazioni, o parametri molto simili, possono essere impostati in **Outlook 2007** dal percorso: Outlook 2007 - *Strumenti - Trust Center - E-mail Security*

Parametri di configurazione per Mozilla Thunderbird (versione 2.0 e successive)

- Thunderbird - *Visualizza* – Corpo del messaggio come - "*Testo semplice*"
- Thunderbird - *Visualizza* - Deselezionate "*Mostra allegati in linea*"
- Thunderbird - *Strumenti - Opzioni - Avanzate – Editor di configurazione - javascript.allow.mailnews* – Scegliete nel campo *Valore* "*False*"

- Thunderbird - *Strumenti - Opzioni - Avanzate – Editor di configurazione - javascript.enabled* – Scegliete nel campo *Valore* "*False*"
- Thunderbird - *Strumenti - Opzioni - Avanzate – Editor di configurazione - javascript.options.strict* - Scegliete nel campo *Valore* "*True*"
- Thunderbird - *Strumenti - Opzioni - Privacy – Frodi via posta* - Selezionate "*Avvisa sempre se il messaggio che si sta leggendo è un possibile tentativo di frode*"
- Thunderbird - *Strumenti - Opzioni - Privacy - Anti-Virus* - Selezionate "*Consenti al programma antivirus di mettere in quarantena i singoli messaggi in arrivo*"

C3.5 Approfondimenti

Navigare il Web e leggere le e-mail in sicurezza come Administrator
http://msdn2.microsoft.com/en-us/library/ms972827.aspx

Visualizzazione di tutti i messaggi di posta elettronica come testo normale
http://support.microsoft.com/kb/831607

Panoramica della crittografia in Outlook 2003
http://office.microsoft.com/en-us/ork2003/HA011402871033.aspx

Firma digitale e crittografia (Outlook 2007)
http://office.microsoft.com/en-us/outlook/CH100622261033.aspx

Service Pack (Microsoft Office e Microsoft Outlook)
http://support.microsoft.com/sp/

Download di Microsoft Office
http://office.microsoft.com/it-it/downloads/FX101321101040.aspx?pid=CL100570421040

Bloccare e sbloccare i link nei messaggi sospetti di phishing
http://office.microsoft.com/en-us/outlook/HA011841931033.aspx

Filtro per la posta indesiderata
http://office.microsoft.com/it-it/outlook/CH063564711040.aspx

Personalizzare Outlook Security Features Administrative Package
http://office.microsoft.com/en-us/orkXP/HA011364471033.aspx

Impostazioni relative a sicurezza e privacy (Thunderbird)
http://kb.mozillazine.org/Category:Security_and_privacy-related_preferences

Security Policies (Thunderbird)
http://kb.mozillazine.org/Security_Policies

C4. Lettori multimediali

C4.1 Descrizione

Comunemente vengono scaricati da Internet contenuti multimediali di vario tipo, legati all'intrattenimento, alle notizie, a contenuti di interesse economico o educativo. Per eseguire o visualizzare tali contenuti (musica, video, foto, etc.), a prescindere dalla loro origine, i computer ha bisogno di applicazioni chiamate media player o lettori multimediali.

La maggior parte dei moderni sistemi operativi sono configurati per comprendere automaticamente almeno pacchetto software standard per la lettura di contenuti multimediali. Sono anche disponibili applicazioni di parti terze che eseguono formati di solito non supportati dal set delle applicazioni standard. Tali supporti sono spesso necessari per l'esecuzione di formati proprietari che i fornitori devono concedere in licenza per aggiungere compatibilità alle loro applicazioni multimediali. Queste applicazioni aggiuntive sono di norma installate alla bisogna, a volte anche in modo automatico, per consentire l'esecuzione dei contenuti multimediali che le richiedono. Una volta installate, tali applicazioni possono essere facilmente dimenticate e trascurate dagli amministratori IT responsabili della gestione e del supporto patch, spesso perché questi non sono nemmeno consapevoli della loro esistenza sul singolo sistema.

Durante l'anno appena trascorso sono state riscontrate vulnerabilità per la maggior parte dei lettori multimediali attualmente più diffusi. Per quanto la criticità di tali vulnerabilità sia di vario tipo, tali vulnerabilità possono spesso essere sfruttate per installare malware come virus, applicazioni bot-net, root kit, spy-ware e ad-ware.

Anche se questa lista presenta un panoramica dettagliata dei lettori multimediali più popolari con le relative vulnerabilità, l'elenco non pretende di essere una lista esaustiva che comprenda al suo interno tutti i lettori multimediali e le vulnerabilità a questi associate. Per molte di queste vulnerabilità il codice per sfruttale in un attacco è disponibile pubblicamente e questo codice è continuamente utilizzato in modo selvaggio.

I lettori multimediali per le piattaforme più diffuse sono:

- Windows: Windows Media Player, RealPlayer, Apple Quicktime, Adobe Flash Player, Apple iTunes
- Mac OS: RealPlayer, Apple Quicktime, Apple iTunes, Adobe Flash Player
- Linux/Unix: RealPlayer, Adobe Flash Player

C4.2 Sistemi operativi interessati

- Microsoft Windows
- Linux/Unix
- Mac OS X

C4.3 Riferimenti CVE

RealPlayer
CVE-2007-2497, CVE-2007-3410, CVE-2007-5601

Apple iTunes
CVE-2007-3752

Adobe Flash Player
CVE-2007-3457, CVE-2007-5476

Apple Quicktime
CVE-2007-0462, CVE-2007-0588, CVE-2007-0466, CVE-2007-0711, CVE-2007-0712, CVE-2007-0714, CVE-2007-2175, CVE-2007-2295, CVE-2007-2296, CVE-2007-0754, CVE-2007-2388, CVE-2007-2389, CVE-2007-2392, CVE-2007-2393, CVE-2007-2394, CVE-2007-2396, CVE-2007-2397, CVE-2007-5045, CVE-2007-4673

Windows Media Player
CVE-2006-6134, CVE-2007-3035, CVE-2007-3037, CVE-2007-5095

C4.4 Come stabilire se si è vulnerabili

Può costituire un potenziale problema l'utilizzo di un lettore multimediale sul quale non sono stati installati patch o aggiornamenti della versione più recente. Un buon sistema di rilevamento del software utilizzato revisione e l'utilizzo di pratiche di gestione delle patch aiuta ad essere preparati a fronteggiare le minacce e gli attacchi condotti tramite i lettori multimediali.

C4.5 Come proteggersi dalle vulnerabilità dei lettori multimediali

Di seguito presentiamo alcuni accorgimenti per proteggersi contro le vulnerabilità tipiche dei lettori multimediali:

- Assicurarsi che i lettori multimediali siano regolarmente aggiornati con le più recenti patch. Molti lettori offrono la possibilità di effettuare gli aggiornamenti tramite l'help o il menù degli strumenti.
- Esaminare con cura le installazioni di default dei sistemi operativi e di altri prodotti assicurandosi che non includano lettori multimediali indesiderati.
- Configurare i sistemi operativi e i browser al fine di prevenire installazioni inconsapevoli
- Utilizzare strumenti anti-malvare, come software anti-virus e IDS, sui client desktop in modo da prevenire problemi.
- Sui sistemi che rispondono a una gestione centralizzata, utilizzare il principio dei minimi privilegi e, dove possibile, limitare la possibilità di installazione di software aggiuntivo da parte dell'utente finale. Queste pratiche renderanno la gestione delle patch e delle vulnerabilità molto più semplice e più efficace.
- Quando possibile, implementando un inventario aggiornato del software installato, in modo da identificare i potenziali rischi presenti nell'ambiente operativo.
- Non installare lettori multimediali sui sistemi sui quali non devono essere eseguiti file multimediali (ad esempio sui server)

C4.6 Approfondimenti

La sezione sui lettori multimediali del sito RealNetworks
http://www.realnetworks.com/products/media_players.html
http://www.realnetworks.com/support/updates.html

Home Page di Apple QuickTime
http://www.apple.com/quicktime/
http://www.apple.com/support/quicktime/

Home page di Apple iTunes
http://www.apple.com/itunes/
http://www.apple.com/support/itunes/

Windows Media Player
http://www.microsoft.com/windows/windowsmedia/default.aspx
http://www.microsoft.com/windows/windowsmedia/player/11/security.aspx
http://www.microsoft.com/windows/windowsmedia/player/10/security.aspx
http://www.microsoft.com/technet/security/current.aspx

Homepage di Adobe Flash Player
http://www.adobe.com/products/flashplayer/security/
http://www.adobe.com/downloads/updates/

Security Report e altri link
https://www2.sans.org/newsletters/risk/
http://findarticles.com/p/articles/mi_m0EIN/is_2006_Dec_18/ai_n16912185

Misure di rete generali per mitigare l'impatto delle vulnerabilità lato client:

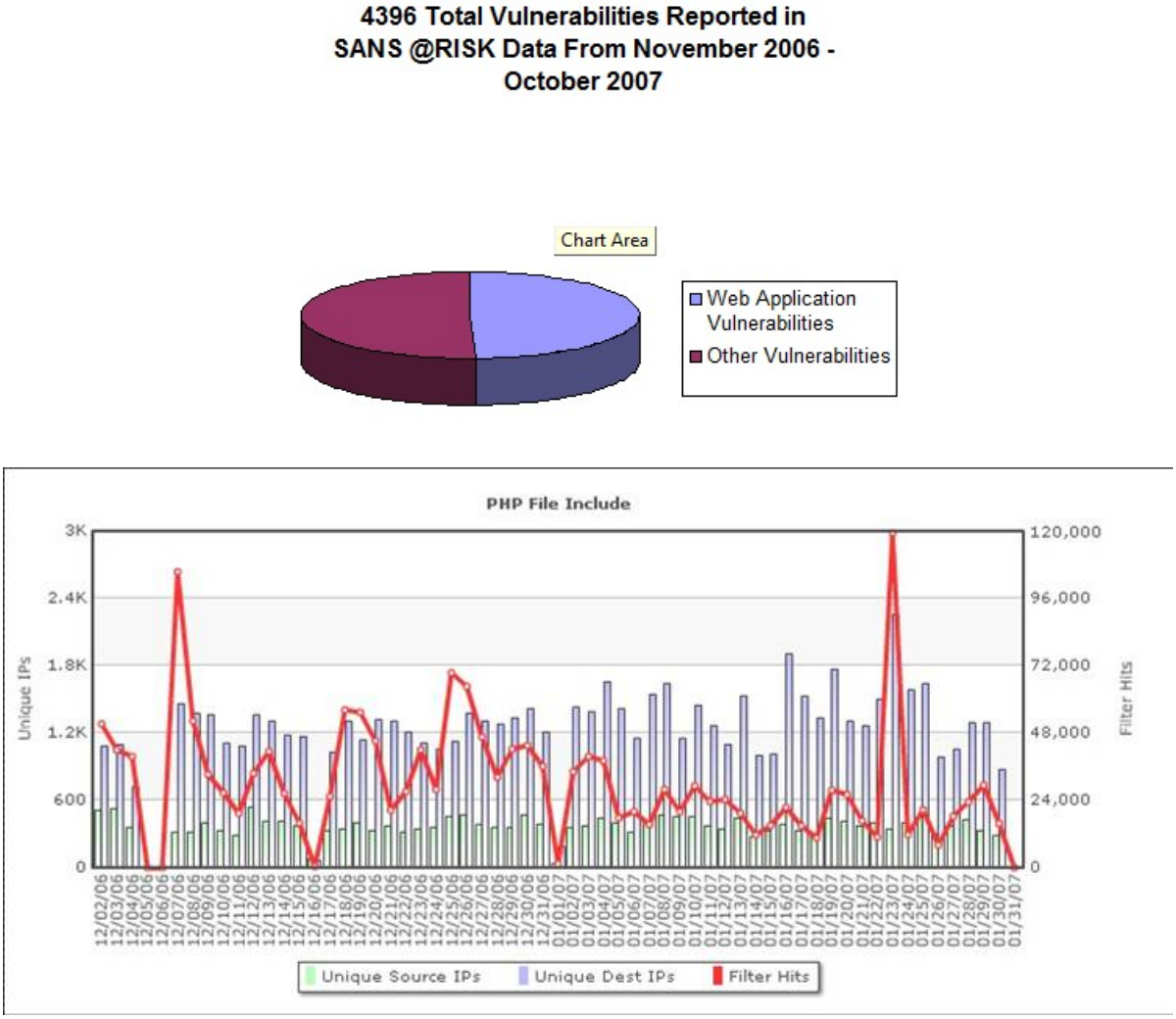
- Agli utenti dovrebbe essere impedita la navigazione verso qualsiasi URL potenzialmente pericoloso utilizzando tecniche di *URL blocking*
  - Il Pentagono, ad esempio, ha bloccato l'accesso a siti di social networking come MySpace e YouTube.
    - Riferimento: http://thelede.blogs.nytimes.com/2007/05/14/pentagon-blocks-myspace-and-youtube/
  - Implementate una soluzione di URL filtering, commerciale o open-source, per evitare che gli utenti visitino siti che diffondono exploit e malware.
    - Riferimenti: http://www.squidguard.org/, http://code.google.com/apis/safebrowsing/
- Il download da Internet di qualsiasi file multimediale da parte degli utenti dovrebbe essere bloccato.
- Agli utenti dovrebbe essere impedito l'accesso SMTP, POP o IMAP alla propria caselle di posta personale. Questa pratica permette di prevenire l'ingresso nella rete aziendale via mail di contenuti potenzialmente non filtrati o non analizzati da sistemi antivirus controllati dall'organizzazione.
- Sarebbe auspicabile l'adozione di soluzioni anti-virus, anti-spyware ad altre applicazioni di scansione del malware presente nelle email a livello di gateway.
- Su un server operativo non devono essere usati browser, client email, lettori multimediali o software office. Quando possibile, bloccate per i server il traffico verso l'esterno attraverso la porta 80/tcp.

Vulnerabilità lato server in:

S1 Applicazioni Web

S1.1 Descrizione

Le applicazioni Web come i Content Management System (CMS), Wiky, Portali, Bulletin Board e forum di discussione sono utilizzate da organizzazioni grandi e piccole. Un grande numero di aziende, inoltre, sviluppa e mantiene applicazioni web personalizzate per il proprio business (in verità per molti casi tali applicazioni *sono* il loro business). Ogni settimana in queste applicazioni, siano esse open source o proprietarie, si scoprono **centinaia** di vulnerabilità, che vengono regolarmente sfruttate per condurre degli attacchi. Da notare che anche le **applicazioni web personalizzate** sono costantemente attaccate e colpite, solo che le vulnerabilità presenti in tali applicazioni non sono censite e monitorate dai database pubblici delle vulnerabilità come @RISK, CVE o BugTraq. Il numero di tentativi giornalieri di attacco per alcuni dei maggiori fornitori di web hosting varia da **centinaia di migliaia fino a milioni**.



Numero di attacchi PHP File Include registrato in una struttura di web hosting da TippingPoint IPS

Tutti gli ambienti web f (PHP, .NET, J2EE, Ruby on Rails, ColdFusion, Perl, ecc) e qualsiasi tipologia di applicazione web è a rischio a causa di problemi di sicurezza delle applicazioni web, che vanno da metodi di validazione insufficienti fino a errori nella logica dell'applicazione. Le vulnerabilità più sfruttate sono:

- **PHP Remote File Include**: PHP è il linguaggio e l'ambiente attualmente più utilizzato per applicazioni web. PHP permette per default l'accesso a risorse su Internet come se fossero file utilizzando una funzionalità chiamata "*allow_url_fopen*". Quando gli script PHP permettono all'utente inserimenti che interagiscano con i nomi dei file, è possibile che si verifichi l'inclusione di file remoti. Questo attacco permette (ma non solo):
  - L'esecuzione di codice da remoto
  - L'installazione di root kit

  - Su Windows, la compromissione totale del sistema attraverso l'uso dei file wrapper SMB di PHP
- **SQL Injection**: Le *injection*, in particolare le *SQL injection*, sono piuttosto comuni nelle applicazioni web. Le Injection sono rese possibili dalla mescolanza di dati forniti dall'utente con query dinamiche o all'interno di procedure mal costruite. Le SQL injection permettono ai malintenzionati di:
  - Creare, leggere, modificare o cancellare qualsiasi dato disponibile nell'ambito dell'applicazione
  - Nel peggiore dei casi, di compromettere completamente il sistema del database e i sistemi correlati
- **Cross-Site Scripting (XSS)**: Il cross site scripting, meglio conosciuto come XSS, è il problema di sicurezza più pernicioso e maggiormente riscontrabile per le applicazioni web. XSS permette agli aggressori di deturpare i siti web, di inserire contenuti dannosi, di condurre attacchi di phishing, di prendere il controllo del browser degli utenti utilizzando codici JavaScript e porta gli utenti ad eseguire comandi non di loro scelta – un attacco conosciuto come *cross-site request forgery*, meglio noto come CSRF.
- **Cross-site request forgery (CSRF)**: CSRF forza gli utenti legittimi ad eseguire comandi senza il loro consenso. Questo tipo di attacco è estremamente difficile da prevenire a meno che l'applicazione non sia esente da vettori cross-site scripting, comprese le *DOM injection*. Con la crescita della diffusione di tecniche Ajax e la conoscenza più approfondita su come sfruttare gli attacchi XSS, gli attacchi CSRF stanno diventando molto sofisticati, sia come attacco specifico attivo, sia come automatismo di worm come il Samy MySpace Worm.

S1.2 Come stabilire se si è a rischio

Gli strumenti di scansione Web possono aiutare a riscontrare queste vulnerabilità, specialmente se si tratta di bug conosciuti. Per trovare le vulnerabilità potenziali è però necessaria una revisione completa del codice sorgente e un *penetration test* dell'applicazione. Queste operazioni dovrebbero essere eseguite dallo sviluppatore prima del rilascio di qualsiasi applicazione web importante.

Controllare come è configurata la struttura della vostra applicazione web e operate le opportune correzioni per la sicurezza.

Gli amministratori del sistema dovrebbero prevedere una scansione periodica dei web server tramite dei vulnerability scanner, in particolare quando questi ospitano una vasta gamma di script diversi forniti dagli utenti, come accade nelle hosting farm.

Nessuno dovrebbe essere incaricato di scrivere una applicazione web se prima non ha superato l'esame del GSSP Secure Software Programming, che riguarda la teoria e gli strumenti di sicurezza essenziali di cui uno sviluppatore avrebbe bisogno per produrre applicazioni più sicure.

S1.3 Come proteggersi dalla vulnerabilità delle applicazioni web

Dal punto di vista dell'hosting e dell'amministratore del sistema PHP:

- Effettuate l'aggiornamento a PHP 5.2, in quanto questa versione elimina molti dei problemi di sicurezza di PHP e permette API più sicure come PDO
- Provate e quindi installate le patch e le nuove versioni di PHP non appena vengono rilasciate
- Si raccomanda l'uso frequente di scansioni web in particolare per gli ambienti ove sono in uso una grande numero di applicazioni PHP.
- Verificate la possibilità di utilizzare le seguenti configurazioni di PHP:
  - *register_globals* dovrebbe essere off (interferirà con applicazioni insicure)
  - *allow_url_fopen* dovrebbe essere off (interferirà con applicazioni che utilizzano questa funzionalità, ma vi proteggerà da un vettore di attacchi molto dannoso)
  - *magic_quotes_gpc* dovrebbe essere off (interferirà con applicazioni insicure meno recenti)
  - *open_basedir* dovrebbe essere abilitato e correttamente configurato
- Verificate la possibilità di utilizzare funzionalità con privilegi di esecuzione molto bassi come PHPsuexec o suPHP
- Prendete in considerazione Suhosin per controllare l'ambiente di esecuzione degli script PHP
- Utilizzate sistemi di Intrusion Prevention/Detection per bloccare o segnalare richieste HTTP sospette. Prendete in considerazione *mod_security* di Apache per bloccare gli attacchi PHP noti

- Come ultima risorsa, prendere in considerazione il blocco delle applicazioni in cui sono state rilevate delle vulnerabilità sfruttate e rallentate i tempi di risposta per risolvere i problemi di sicurezza conosciuti.

Dal punto di vista dello sviluppatore:

- Se usate PHP, migrate rapidamente le vostre applicazioni verso PHP 5.2.
- Per evitare i problemi di codifica illustrati:
  - Sviluppate le applicazioni con la versione più recente di PHP e una configurazione più attenta alla sicurezza (vedi sopra)
  - Convalidate in maniera appropriata tutti gli input
  - Codificate tutti gli output usando *htmlentities*() o meccanismi simili per evitare gli attacchi XSS
  - Migrate la parte dati verso PDO – non utilizzate le funzioni mysql_*() vecchio stile, notoriamente difettose
  - Non usate funzioni in cui gli input dell'utente interagiscano con file, per evitare attacchi di *remote file inclusion*
- Associatevi alle organizzazioni per la codifica sicura come OWASP (vedi riferimenti) per sviluppare le vostre conoscenze e imparare a programmare in modo sicuro
- Provate le vostre applicazioni utilizzando la OWASP Testing Guide con strumenti quali WebScarab, la Web Developer Toolbar di Firefox, Greasemonkey e XSS Assistant
- Misurate le vostre conoscenze usando gli esami GSSP e colmando le lacune del vostro sapere.

S1.4 Approfondimenti

OWASP - Open Web Application Security Project
http://www.owasp.org

OWASP Testing Guide
http://www.owasp.org/index.php/OWASP_Testing_Guide_v2_Table_of_Contents

Guida OWASP Guide – le indicazioni per la codifica sicura
http://www.owasp.org/index.php/Category:OWASP_Guide_Project

OWASP Top 10 – La Top 10 dei problemi di sicurezza delle applicazioni Web
http://www.owasp.org/index.php/Top_10_2007
http://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

Suhosin, un progetto Hardened PHP per controllare l'ambiente di esecuzione delle applicazioni PHP
http://www.hardened-php.net/suhosin/

PHPSecInfo
http://phpsec.org/projects/phpsecinfo/index.html

GSSP Exam blueprints and testing schedule
http://www.sans.org/gssp

S2. Servizi Windows

S2.1 Descrizione

La famiglia dei sistemi operativi Windows supporta una larga gamma di servizi, procedure di rete e tecnologie. Molti di questi componenti sono implementati come SCP (Service Control Programs) sotto il controllo del Service Control Manager (SCM), che viene eseguito come *services.exe*. Le vulnerabilità dei servizi che eseguono queste funzioni del sistema operativo sono una delle strade più battute per gli attacchi alla sicurezza. Alla prima installazione di Windows Server 2003, Windows XP o Windows Vista, alcuni servizi sono installati e configurati per essere attivi automaticamente quando il computer viene riavviato. Su Windows Server 2003 sono attivati quei servizi che corrispondono al ruolo che si è assegnato a ciascun server. In alcuni ambienti qualcuno di questi servizi di default potrebbe essere non necessario, per cui si dovrebbero disattivare manualmente tutti i servizi che non servono in modo da aumentare la sicurezza. I servizi devono collegarsi a risorse di accesso e a oggetti del sistema operativo, ma la maggior parte dei servizi non sono progettati per dare la possibilità di cambiare il loro account di default. Se cambiate la password dell'account predefinito per questi servizi è probabile che il servizio smetta di funzionare. Se scegliete un account che non ha i permessi necessari per collegarsi come servizio, la Microsoft Management

Console (MMC) gli attribuisce automaticamente la possibilità di collegarsi al computer come servizio, anche se questa configurazione automatica non da la garanzia che il servizio partirà davvero. I sistemi operativi Windows prevedono tre account locali preallestiti che vengono usati come account per il logon di vari servizi di sistema:

Account di sistema locale. L'account di sistema locale (*Local System account*) è un account molto potente a cui è riservato pieno accesso al computer ed opera come computer nella rete. Se un servizio usa l'account di sistema locale per autenticarsi presso un controller di dominio, il servizio avrà accesso all'intero dominio. Alcuni servizi hanno come configurazione predefinita la possibilità di usare l'account di sistema locale e questa non si può cambiare. L'account di sistema locale non deve avere una password accessibile all'utente.

Account di Servizio locale. L'account di Servizio locale è un account speciale preallestito che assomiglia all'account di un utente autenticato. Possiede lo stesso livello di accesso alle risorse e agli oggetti di un membro di un Gruppo di utenti. Questo accesso limitato iuta a salvaguardare il vostro computer nel caso che un singolo servizio o uno specifico processo sia compromesso. I servizi che usano l'account di Servizio locale accedono alle risorse di rete con una sessione nulla (*null session*) con credenziali anonime. Il nome di questo account è *NT AUTHORITY\Local Service* e non ha una password accessibile all'utente.

Account di Servizio di rete. Anche l'account di Servizio di rete è un account speciale predefinito che ha caratteristiche simili a un account utente. Come l'account di Servizio locale ha lo stesso livello di accesso alle risorse e agli oggetti di un membro di un Gruppo di utenti , il che aiuta a salvaguardare il vostro computer. I servizi che usano l'account di Servizio di rete accedono alle risorse di rete con le credenziali del computer. Il nome di questo account è *NT AUTHORITY\Network Service* e non ha una password accessibile all'utente.

Alcuni strumenti grafici basati su *Graphical user interface* (GUI) possono essere d'aiuto per gestire i servizi. Le versioni di questi strumenti inserite nelle versioni di Windows precedenti a Windows Server 2003, però, applicano automaticamente i permessi al servizio quando si configura una qualsiasi delle proprietà del servizio. Strumenti come *Group Policy Object Editor* e il modulo *MMC Security Templates* usano la DLL *Security Configuration Editor* per applicare questi permessi. Ad esempio, quando utilizzate il modulo MMC Security Templates per configurare lo stato del servizio all'avvio di Windows XP, la finestra di dialogo seguente mostrerà:

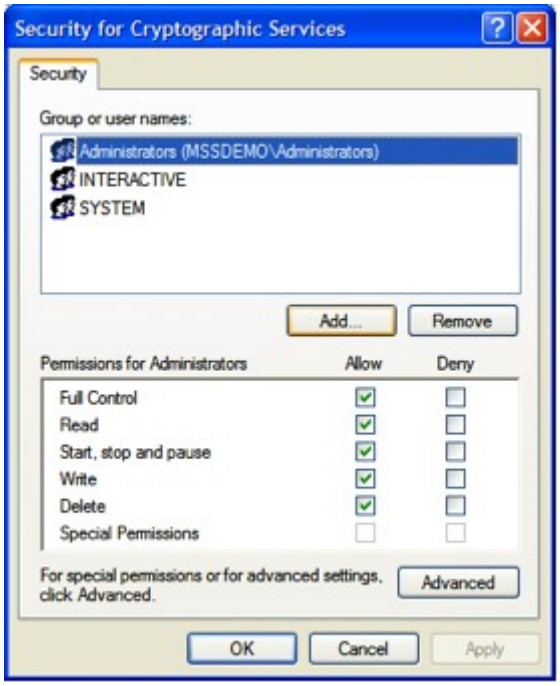


Figura 1. Finestra di dialogo Services Security

A prescindere dal fatto che si selezioni OK o Cancel, i permessi verranno applicati al servizio che è stato configurato. Sfortunatamente i permessi che questa finestra di dialogo propone non corrispondono ai permessi predefiniti per la maggior parte dei servizi inclusi in Windows. In pratica, gestire i permessi dei servizi causa una serie di problemi al funzionamento di molti servizi. Suggeriamo quindi di non alterare i permessi assegnati ai servizi inclusi in Windows XP o Windows Server 2003, poiché quelli impostati per default sono già abbastanza restrittivi. Ci sono diverse linee d'azione che si possono portare avanti in questo scenario:

- Usare il Security Configuration Wizard, un componente opzionale di Windows incluso in Windows Server 2003 Service Pack 1 (SP1). Usate questo approccio quando avete bisogno di configurare filtri per servizi e porte di rete per i vari ruoli di server da assegnare a Windows Server 2003.
- Eseguire i moduli MMC Security Template e Group Policy Object Editor su un serve che esegue Windows Server 2003 con SP1. questo approccio quando avete bisogno di configurare servizi per security template o Group Policy che saranno applicati a Windows XP.
- Usate un editor di testo come Notepad per modificare i security template o le Group Policy su un computer che esegue Windows XP Professional. Questo metodo è il meno desiderabile dei tre, ma in alcuni casi non c'è altra scelta.

Molti dei servizi del nucleo centrale di Windows forniscono punti di collegamento remoti ai componenti del client attraverso le Chiamate di procedura remota (Remote Procedure Calls - RPC). Questi sono esposti soprattutto attraverso le procedure accessibili tramite il protocollo CIFS (Common Internet File System), alcune porte TCP/UDP ben conosciute e in alcuni casi attraverso porte TCP/UDP più transitorie. Storicamente vi sono state numerose vulnerabilità nei servizi Windows che potevano essere sfruttate con utenti anonimi. Quando vengono sfruttate, queste vulnerabilità offrono all'aggressore gli stessi privilegi che ha presso l'host il servizio in quel momento attivo.

S2.2 Sistemi operativi interessati

Sono potenzialmente vulnerabili Windows XP Home e Professional, Windows 2003 e Windows Vista.

S2.3 Riferimenti CVE

CVE-2007-0213, CVE-2007-1748, CVE-2007-0938, CVE-2006-5584, CVE-2006-5583, CVE-2006-4691
CVE-2006-0027, CVE-2006-1314, CVE-2006-2370, CVE-2006-2371, CVE-2006-3439

S2.4 Come stabilire se si è a rischio

- Utilizzate un qualsiasi vulnerability scanner per verificare se il vostro sistema è protetto rispetto ai problemi elencati. Prendete anche in considerazione l'uso di sistemi per la valutazione dello stato degli aggiornamenti dei vostri sistemi quali Microsoft Windows Server Update Services (WSUS), Microsoft Baseline Security Analyzer (MBSA), Windows Live Scanner o Systems Management Server (SMS).
- Potete verificare la presenza della patch corrispondente anche controllando la chiave del registro citata nella sezione Controllo delle chiavi del Registro di sistema presente nel relativo Bollettino sulla sicurezza. È opportuno, inoltre, controllare che le versioni aggiornate dei file citati nel bollettino siano installate sul sistema.
- Per verificare se il vostro sistema sia vulnerabile a un problema presente in un servizio opzionale, dovete prima controllare se il servizio è avviato. Si può fare attraverso la console di amministrazione dei Servizi, che può essere lanciata al menu *Servizi* in *Strumenti di Amministrazione*.

S2.5 Come proteggersi dalle vulnerabilità dei Servizi Windows

- Gli utenti Windows del Governo degli Stati Uniti sono ora obbligati a utilizzare la *Federal Desktop Core Configuration* per Windows XP o Vista. (http://fdcc.nist.gov/). Anche gli altri possono adottare questa configurazione e troveranno la FDCC affidabile e sicura.
- Abilitate il Windows Firewall e/o installate sull'host un firewall di una terza parte. Assicuratevi che siano applicate regole per impedire l'accesso alla macchina Windows a tutte le connessioni ad eccezione di quelle necessarie, esplicitamente indicate. Ad esempio, molte di queste vulnerabilità si trovano sui collegamenti permessi da CIFS e quindi bloccare le porte tcp 139 e 445 è essenziale per prevenire attacchi da remoto. È buona norma anche bloccare le chiamate RPC in entrata provenienti da Internet verso porte superiori alla 1024 per bloccare altre vulnerabilità basate su RPC. In ambienti enterprise i Windows Firewall degli host possono essere configurati con dei General Policy Objects via Microsoft Active Directory.
- In Windows 2003 SP1 e R2, quando possibile utilizzate il Security Configuration Wizard assieme al Windows firewall per ridurre la possibilità degli attacchi.
- Utilizzate filtri in uscita (oltre a quelli in entrata) sui firewall perimetrali come parte dell'architettura di difesa della rete per ridurre i problemi causati da attacchi provenienti sia dall'esterno che dall'interno.
- Mantenete i sistemi aggiornati con le patch e i service pack più recenti. Se possibile, abilitate gli Aggiornamenti automatici su tutti i sistemi.

- Utilizzate sistemi di Intrusion Prevention/Detection a livello di rete e a livello di host come parte della strategia di difesa per prevenire/identificare attacchi che sfruttino queste vulnerabilità.
- Eliminate l'esposizione alle vulnerabilità disabilitando i servizi non necessari. Nei client Windows (XP, 2003 o Vista), dovrebbero generalmente essere disabilitati i seguenti servizi:

Servizio	Nome visualizzato	Client desktop/laptop in reti aziendali	desktop/laptop non in rete
Alerter	Avvisi	Disabilitato	Disabilitato
ClipSrv	ClipBook	Disabilitato	Disabilitato
Browser	Browser di computer	Non definito	Disabilitato
Fax	Fax	Non definito	Disabilitato
MSFtpsvr	FTP	Disabilitato	Disabilitato
IISADMIN	Amministrazione IIS	Disabilitato	Disabilitato
cisvc	Servizio di indicizzazione	Non definito	Disabilitato
Messenger	Messenger	Disabilitato	Disabilitato
mnmsrvc	Condivisione desktop remoto di NetMeeting	Disabilitato	Disabilitato
RDSessMgr	Gestione sessione di assistenza mediante desktop remoto	Non definito	Disabilitato
RemoteAccess	Routing e Accesso remoto	Disabilitato	Disabilitato
SNMP	Servizio SNMP	Disabilitato	Disabilitato
SNMPTRAP	Servizio SNMP Trap	Disabilitato	Disabilitato
SSDPSrv	Servizio di rilevamento SSDP	Disabilitato	Disabilitato
Schedule	Utilità di pianificazione	Non definito	Disabilitato
TlntSvr	Telnet	Disabilitato	Disabilitato
TermService	Servizi Terminal	Non definito	Disabilitato
Upnphost	Host di periferiche Plug and Play universali	Non definito	Disabilitato
W3SVC	World Wide Web Publishing	Disabilitato	Disabilitato

Tabella 1. Servizi Windows disabilitati sui Client Windows

Nelle versioni precedenti dei sistemi operativi Windows, in particolare in Windows NT e Windows 2000, molti di questi servizi erano abilitati di default per la comodità dell'utente. Questi servizi non essenziali aumentano però significativamente l'esposizione agli attacchi. Per le macchine Windows usate come server (es. Server di stampa, file server) fate riferimento alle configurazioni più appropriate descritte nelle guide elencate negli approfondimenti qui sotto e/o usate strumenti automatici come il Windows 2003 Security Configuration Wizard (*Configurazione guidata impostazioni di sicurezza*)per configurare correttamente i servizi.

- In alcuni casi è possibile usare lo stratagemma di impedire l'accesso a sessioni nulle verso l'interfaccia vulnerabile. È buona norma rivedere le vostre impostazioni correnti di RestrictAnonymous e impostarle nella forma più limitativa possibile in base al vostro ambiente di lavoro http://www.securityfocus.com/infocus/1352

S2.6 Approfondimenti

Introduzione ai pericoli e alle contromisure: Impostazioni di sicurezza per Windows Server 2003 e Windows XP
http://www.microsoft.com/italy/technet/security/topics/serversecurity/tcg/tcgch01n.mspx

Guida per la protezione di Windows XP
http://www.microsoft.com/italy/technet/security/prodtech/windowsxp/secwinxp/default.mspx

Guida per la protezione di Windows Server 2003
http://www.microsoft.com/italy/technet/security/prodtech/windowsserver2003/w2003hg/sgch00.mspx

Informazioni su Windows Firewall
http://www.microsoft.com/italy/windows/products/windowsxp/winxp/using/security/internet/sp2_wfintro.mspx

Informazioni sulla Configurazione guidata impostazioni di sicurezza
https://www.microsoft.com/technet/prodtechnol/windowsserver2003/it/library/ServerHelp/eeb7c8c2-3579-47cc-a126-6519321098e6.mspx?mfr=true

Utilizzare gli elenchi di filtri IP IPSec in Windows 2000
http://support.microsoft.com/kb/313190

Blocco di specifici protocolli di rete e porte utilizzando IPSec
http://support.microsoft.com/kb/813878

Configurazione della funzionalità Filtro TCP/IP in Windows 2000
http://support.microsoft.com/kb/309798

S3. Servizi UNIX/Mac OS

S3.1 Descrizione

La maggior parte dei sistemi Unix/Linux include diversi servizi standard nella propria installazione predefinita. Mac OS X spesso soffre delle stesse vulnerabilità dei sistemi Unix, in quanto anch'esso basato su Unix. I servizi non necessari dovrebbero essere disabilitati e i server che si affacciano verso reti pubbliche dovrebbero essere protetti da firewall.

Per i servizi che forniscono login da remoto o comunque servizi da remoto non è possibile bloccare semplicemente il traffico tramite i firewall. Le vulnerabilità di buffer overflow e i problemi nelle funzioni di autenticazione possono spesso diventare un veicolo per l'esecuzione di codice incontrollato, talvolta con privilegi di amministratore, per cui reperire informazioni sulle possibili vulnerabilità e applicare rapidamente le opportune correzioni diventa molto importante. Ogni anno viene scoperta qualche vulnerabilità di buffer overflow nei servizi Unix/Linux.

Questi servizi, anche quando correttamente aggiornati, possono essere l'involontaria causa di danni. **Gli attacchi brute-force contro servizi come SSH, FTP e telnet** rappresentano ancora la più comune forma di attacco diretto a compromettere i server che si affacciano su Internet. Nel corso degli ultimi due anni si è riscontrato un impegno comune da parte degli aggressori ad operare attacchi brute-force verso le password usate in queste applicazioni. Un numero sempre crescente di worm e bot contengono motori per attacchi brute force alle password. I sistemi con password deboli per gli account utente vengono messi in pericolo; spesso attraverso l'escalation di privilegi si riesce ad ottenere un accesso root e ad installare dei rootkit per nascondere le tracce. È importante ricordare che l'attacco brute force verso le password può essere una tecnica valida per compromettere anche quei sistemi che presentano tutti gli aggiornamenti di sicurezza necessari.

Gli amministratori più attenti alla sicurezza utilizzano SSH come sistema per interagire da remoto con i sistemi. Se la versione di SSH è quella più recente e con tutte le patch installate, si considera generalmente il servizio come sicuro. Ciononostante, per quanto sia recente o aggiornato, può essere ancora compromesso tramite attacchi brute-force che ne individuino le password. Per questo si consiglia di usare per SSH meccanismi di autenticazione a chiave pubblica, che sono in grado di evitare questo tipo di attacco. Per quanto riguarda i restanti servizi di interazione, verificate le password per accertavi che presentino una complessità sufficiente a resistere ad attacchi brute-force.

Ridurre al minimo indispensabile i servizi attivi su un host lo renderà più sicuro. Molti servizi sono stati utilizzati per ulteriori exploit e alcune combinazioni di servizi (come ad esempio i server web e server FTP che condividono le directory) sono particolarmente inclini ad essere attaccati.

S3.2 Sistemi operativi interessati

Tutte le versioni dei server Unix/Linux/Mac OS sono potenzialmente a rischio se presentano le configurazioni predefinite o improprie. Tutti questi sistemi operativi possono essere in pericolo se gli account di autenticazione usano password deboli o presenti in un dizionario.

S3.3 Riferimenti CVE

Servizi remoti
CVE-2006-5815, CVE-2007-0882, CVE-2007-2446, CVE-2007-0731, CVE-2007-2791, CVE-2007-1654

Kernel/Librerie
CVE-2007-4995, CVE-2007-5191, CVE-2006-6652, CVE-2007-3641, CVE-2007-5079, CVE-2007-1351

Management Console/Tool
CVE-2007-3093, CVE-2007-3094, CVE-2007-3260, CVE-2007-3232, CVE-2007-2282, CVE-2007-0980

Altro
CVE-2007-2173, CVE-2006-5616

S3.4 Come stabilire se si è vulnerabili

Le installazioni di default (sia che siano effettuate da un produttore o da un amministratore) di sistemi operativi o di applicazioni di rete possono introdurre una vasta gamma di servizi non necessari e non utilizzati. In molti casi l'indefinibilità a priori su cosa avrà davvero bisogno un sistema operativo o una applicazione porta molti produttori e amministratori a installare tutto il software a disposizione nel caso diventi utile in futuro. Questa pratica semplifica significativamente il processo di installazione ma introduce anche una vasta gamma di servizi non necessari e account con password di default, deboli o altrimenti conosciute.

L'uso di un vulnerability scanner aggiornato o di un port mapper può essere molto efficace per la scoperta di qualche vulnerabilità potenziale ereditata dalle istallazioni di default o da servizi e applicazioni non necessarie e/o obsolete. Anche un password cracker può essere utile per evitare l'utilizzo di password deboli o di facile individuazione.

Nota: Non utilizzate mai un password cracker o un vulnerability scanner, neanche sui sistemi per i quali avete un accesso root, senza autorizzazione esplicita e preferibilmente scritta da parte del vostro datore di lavoro. È già accaduto che amministratori di sistema con le migliori intenzioni siano stati licenziati per aver utilizzato strumenti per la determinazione delle password senza autorizzazione.

S3.5 Come proteggersi da queste vulnerabilità

Disabilitando i servizi non necessari

- Analizzate il server con un port scanner o uno strumento di vulnerability assessment per determinare quali servizi non necessari siano attivi sul sistema. Disabilitate i servizi che non sono richiesti da qualche applicazione necessaria.
- Stabilite e applicate procedure affidabili di gestione delle patch
- Installate regolarmente le più recenti patch rilasciate dal fornitore per attenuare le vulnerabilità nei servizi esposti. La gestione delle patch è una parte fondamentale del processo di gestione del rischio.
- Gli strumenti di gestione delle patch sono utili per trovare i sistemi non ancora aggiornati. Applicare costantemente le patch ai server è importante specialmente nelle reti in cui sono attivi molti server, in quanto un solo server non aggiornato può mettere in pericolo l'intera rete.

Utilizzando configurazioni sicure

- Utilizzate i benchmark del Center for Internet Security (www.cisecurity.org) per i sistemi operativi e i servizi che utilizzate. Considerate anche l'utilizzo di Bastille (www.bastille-linux.org) per rafforzare gli host Linux e HP-UX.
- Considerate la possibilità di trasferire i servizi dalla porte di default non appena possibile. Gli scanner automatici tendono ad analizzare solo le porte di default.
- Assicuratevi che i servizi siano protetti da meccanismi di sicurezza forniti dal produttore (come ad esempio SELinux o address space randomization).

Migliorando i log per la difesa e il monitoraggio perimetrale

- Usate firewall hardware o software e IDS/IPS per rilevare e bloccare gli attacchi, proteggendo i servizi necessari. Se possibile, limitate l'accesso e i servizi da remoto a determinati indirizzi IP.
- Nelle reti *mission critical*, utilizzante un sistema di controllo in tempo reale dei log per rilevare immediatamente gli attacchi. Gli strumenti SIM e di gestione dei log sono utili per l'analisi real-time di numerose tipologie di log.

Bloccando gli attacchi brute force

- Non usate le password di default su alcun account.
- Attuate una politica di password robuste. Non permettete l'utilizzo di password deboli o che contengano parole presenti in un dizionario.
- Effettuate delle verifiche per accertarvi che la vostra politica di password sia rispettata.
- Limitate il numero di tentativi di login falliti per i servizi più esposti.
- Limitate gli account che possono accedere attraverso la rete; root non dovrebbe essere uno di questi.
- Proibite l'utilizzo di account condivisi e non utilizzate nomi utente generici come tester, guest, sysadmin, admin, ecc.
- Conservate un registro dei tentativi di login falliti. Un numero alto di tentativi di login falliti a un sistema può richiedere un controllo ulteriore sul sistema vedere se è stato compromesso.
- Prendete in considerazione un sistema di autenticazione basato su certificati.
- Se il vostro sistema UNIX permette l'uso di moduli di autenticazione PAM, implementate i moduli PAM per verificare la resistenza delle password.

Evitando interazioni tra i servizi e configurazioni non corrette

- Dove possibile, limitate le funzioni degli host. Le configurazioni non corrette in diversi servizi possono spesse aumentare i rischi per un servizio.

S3.6 Approfondimenti

Attacchi Brute Force e relative contromisure

http://isc.sans.org/diary.php?storyid=1541
http://isc.sans.org/diary.php?storyid=1491
http://isc.sans.org/diary.html?storyid=3212
http://isc.sans.org/diary.html?storyid=3209
http://isc.sans.org/diary.php?date=2006-08-01

Risorse generali per la sicurezza di UNIX

http://www.cisecurity.org
http://www.bastille-linux.org
http://www.puschitz.com/SecuringLinux.shtml

S4. Software di Backup

S4.1 Descrizione

Il software di backup è un bene prezioso per qualsiasi organizzazione. Di solito questi software agiscono su un gran numero di sistemi di ciascuna azienda. Negli ultimi anni, con la crescita della quantità di dati gestiti, la tendenza è stata quella di consolidare la funzione di backup in pochi server, o anche in un unico server dedicato. Di conseguenza i singoli host che necessitano del servizio di backup comunicano con il server di backup attraverso la rete. Ciò può avvenire in modalità *push* quando il client invia i dati al server o in modalità *pull* quando è il server a connettersi a sua volta con ciascun client, o in una combinazione di queste due modalità. Nel corso del 2007 sono state scoperte diverse vulnerabilità critiche nei software di backup. Siccome i software di backup di solito operano con privilegi piuttosto alti per poter leggere tutti i file del sistema, queste vulnerabilità hanno portato a gravi problemi di sicurezza. Alcune di queste possono essere sfruttate per ottenere il controllo completo dei sistemi che ospitano i server di backup e/o i client di backup. Un aggressore può far leva su questi difetti del software per compromettere tutti i sistemi aziendali e per ottenere l'accesso a dati riservati presenti nei backup. Alcuni exploit sono stati pubblicati in rete e molte vulnerabilità sono state attaccate in maniera selvaggia.

S4.2 Sistemi operativi e software di backup interessati

Tutti i sistemi operativi su cui operano i software per server o client di backup sono potenzialmente vulnerabili agli exploit. I sistemi operativi interessati sono principalmente sistemi Windows e UNIX, in quanto questi sistemi formano la maggioranza dei client e dei server aziendali.

I seguenti pacchetti software di backup molto diffusi sono affetti da vulnerabilità critiche

- Computer Associates (CA) BrightStor ARCServe ha dozzine di vulnerabilità di semplice sfruttabilità, per cui il codice è largamente disponibile.
- Symantec Veritas NetBackup/Backup Exec ha avuto recentemente alcune vulnerabilità riportate.
- Anche EMC Legato Networker ha presentato una vulnerabilità pubblicamente riportata.

S4.3 Nota speciale sulla sicurezza dei backup

I backup spesso contengono tutti o perlomeno una larga parte dei dati di un sistema. Di solito i dati di backup vengono conservati in un luogo centralizzato e spesso non crittati. La sicurezza fisica dei supporti di backup è argomento di estrema importanza, in quanto il furto o l'analisi di un supporto di backup può fornire gli strumenti per l'accesso completo a dati critici senza ulteriori sforzi. Quando possibile, i dati dei backup dovrebbero essere cifrati con crittografia forte e i metodi di decifrazione dovrebbero essere a conoscenza solo di poche persone fidate.

S4.4 Riferimenti CVE

CVE-2007-5332, CVE-2007-5330, CVE-2007-5328, CVE-2007-5327, CVE-2007-5325, CVE-2007-5006, CVE-2007-5004, CVE-2007-5003, CVE-2007-3825, CVE-2007-3216, CVE-2007-2864, CVE-2007-2863, CVE-2007-2139, CVE-2007-1447, CVE-2007-5126, CVE-2007-3509, CVE-2007-2279, CVE-2007-3618

S4.5 Come stabilire se si è vulnerabili

- Usate un vulnerability scanner per scoprire le eventuali vulnerabilità del software di backup
- Aggiornate il vostro software di backup alla versione più recente. Controllate periodicamente il sito del produttore del software e iscrivetevi al sistema di notifica delle patch, se disponibile. Controllate anche nei siti dedicati alla sicurezza come US-CERT, SANS Internet Storm Center se vi sono annunci relativi a vulnerabilità legate al software di backup che avete scelto.
- Controllate gli accessi alle porte TCP e UDP utilizzate dal vostro software di backup. I prodotti di backup elencati utilizzano le seguenti porte:
  - Symantec Veritas Backup Exec
    - TCP/10000 TCP/8099, TCP/6106, TCP/13701, TCP/13721 e TCP/13724 (Una lista delle porte utilizzate dai daemon di backup di Veritas è disponibile qui).
  - CA BrightStor ARCServe Backup Agent
    - TCP/6050, UDP/6051, TCP/6070, TCP/6503, TCP/41523, UDP/41524
  - Sun e EMC Legato Networker
    - TCP/7937-9936

S4.6 Come proteggersi da queste vulnerabilità

- Assicuratevi che le patch più recenti fornite dal produttore del software siano installate sui client e sui server.
- Le porte utilizzate dal software di backup dovrebbero essere protette tramite regole dei firewall dall'utilizzo tramite qualsiasi rete non sicura, in particolare Internet.
- I dati dovrebbero essere cifrati sia quando sono salvati sui supporti di backup, sia quando transitano attraverso la rete.
- I firewall di rete e relativi al singolo host dovrebbero presentare regole che limitano l'accessibilità ai sistemi su cui operano i software di backup in modo che solo l'host di backup corretto possa comunicare attraverso le porte del server di backup.
- Suddividete la vostra rete creando una sottorete VLAN separata per il backup.
- I supporti di backup dovrebbero essere conservati, tracciati e contabilizzati come gli altri asset IT per scoraggiare e individuarne prontamente il furto o la perdita.
- I supporti di backup dovrebbero essere cancellati in modo sicuro o distrutti fisicamente alla fine del loro periodo di utilizzo.

S5. Software anti-virus

S5.1 Descrizione

Il software anti-virus è visto oggi come uno strumento basilare necessario nel corredo per la protezione dei sistemi. I software anti-virus sono oggi installati su quasi tutti i desktop, server e gateway per la lotta contro le infezioni dei virus.

Durante il 2007 gli aggressori hanno spostato la loro attenzione verso i metodi per colpire proprio i prodotti per la sicurezza utilizzati da un grande numero di utenti finali. Tra questi vi sono software anti-virus e personal firewall. La scoperta di vulnerabilità nei software anti-virus non è limitata alle piattaforme desktop e server: sono colpite anche le soluzioni a livello di gateway, e colpire un gateway può provocare un impatto maggiore, in quanto il gateway è il livello più esterno di protezione e spesso l'unico livello di protezione contro determinati pericoli in molte piccole organizzazioni.

Diverse vulnerabilità che consento l'esecuzione di codice remoto sono state scoperte nei software anti-virus fornito da vari produttori quali Symantec, F-Secure, Trend Micro, McAfee, Computer Associates, ClamAV e Sophos. Queste vulnerabilità in questi sistemi possono spesso essere sfruttate per ottenere il controllo completo del sistema dell'utente con interazioni dell'utente minime o nulle.

Si è scoperto che i software anti-virus sono vulnerabili anche ad attacchi "evasion". Creando con tecniche particolari un file dannoso (ad esempio un file HTML con un header eseguibile) può essere possibile evitare la scansione da parte dell'anti-virus. Questi attacchi elusivi possono essere sfruttati per creare un canale attraverso il quale propagare codice dannoso o per bypassare i sistemi che altrimenti limiterebbero la propagazione del malware.

S5.2 Sistemi operativi interessati

Qualsiasi sistema che abbia installata una applicazione anti-virus o un motore di scansione diretto a rilevare codice dannoso potrebbe essere colpito. L'elenco comprende quindi soluzioni installate su desktop, server e gateway. Qualsiasi piattaforma potrebbero essere colpita, incluse Microsoft Windows e tutti i sistemi Unix.

S5.3 Riferimenti CVE

Avast!
CVE-2007-2845, CVE-2007-2846, CVE-2007-1672

AVIRA
CVE-2007-2974, CVE-2007-2973, CVE-2007-2972, CVE-2007-1671

BitDefender
CVE-2007-0391

ClamAV
CVE-2007-4560, CVE-2007-3023, CVE-2007-2029, CVE-2007-1997, CVE-2007-1745

Computer Associates
CVE-2007-2864, CVE-2007-2523, CVE-2007-2522

HAURI
CVE-2006-0864

F-Secure
CVE-2007-3300, CVE-2007-2967, CVE-2007-2966, CVE-2007-2965, CVE-2007-1557

Kaspersky
CVE-2007-3675, CVE-2007-1879, CVE-2007-1112, CVE-2007-0445, CVE-2007-1281

Mcafee
CVE-2007-2152, CVE-2007-1538

Panda
CVE-2007-3969, CVE-2007-3026, CVE-2007-1670

Sophos
CVE-2006-6335, CVE-2006-0994

Symantec
CVE-2007-3699, CVE-2007-0447, CVE-2007-3802, CVE-2007-3095, CVE-2007-3021

Trend Micro
CVE-2007-1591, CVE-2007-0856, CVE-2007-0851

S5.4 Come stabilire se si è vulnerabili

Se si utilizza una qualsiasi versione di un qualunque software anti-virus che non sia aggiornata alla versione più recente, software, vi sono probabilità di essere colpiti.

S5.5 Come proteggersi dalle vulnerabilità dei software anti-virus

- Mantenendo i software anti-virus regolarmente e automaticamente aggiornati.
- Controllando periodicamente i sito del fornitore del software per verificare la presenza di aggiornamenti, patch e avvisi di sicurezza. Una lista di fornitori di anti-virus è fornita nel capitolo seguente. Tale lista può non essere completa.
- Se avete implementato software anti-virus sia sui desktop che a livello di gateway, utilizzate soluzioni anti-virus di fornitori diversi per i desktop e per il gateway. Se una di queste è vulnerabile, almeno sarete protetti dall'altra.

S5.6 Approfondimenti

Ecco una lista di fornitori di anti-virus per controllare aggiornamenti, patch e avvisi di sicurezza.

Avvisi di sicurezza per anti-virus

- https://www2.sans.org/newsletters/risk/display.php?v=6&i=29#widely7 (Symantec)
- https://www2.sans.org/newsletters/risk/display.php?v=6&i=23#widely3 (F-Secure)
- https://www2.sans.org/newsletters/risk/display.php?v=6&i=9#widely2 (Trend Micro)
- https://www2.sans.org/newsletters/risk/display.php?v=6&i=17#07.17.29 (McAfee)
- https://www2.sans.org/newsletters/risk/display.php?v=6&i=24#widely2 (Computer Associates)
- https://www2.sans.org/newsletters/risk/display.php?v=6&i=9#widely6 (ClamAV)
- https://www2.sans.org/newsletters/risk/display.php?v=6&i=22#other1 (Avast!)
- http://www.sans.org/newsletters/risk/display.php?v=4&i=34#other2 (HAURI)
- https://www2.sans.org/newsletters/risk/display.php?v=5&i=19#widely6 (Sophos)
- https://www2.sans.org/newsletters/risk/display.php?v=6&i=31#widely4 (Panda)
- https://www2.sans.org/newsletters/risk/display.php?v=6&i=23#other1 (AVIRA)
- https://www2.sans.org/newsletters/risk/display.php?v=6&i=15#widely3 (Kaspersky)

Problemi di anti-virus evasion

- http://www.kb.cert.org/vuls/id/968818
- http://www.sans.org/newsletters/risk/display.php?v=4&i=43#other4

Altre risorse per anti-virus

- http://www.cert.org/other_sources/viruses.html
- http://www.virusbtn.com/
- http://www.eicar.com/
- http://www.wildlist.org/

S6. Management Server

S6.1 Descrizione

Applicazioni server come i sistemi antivirus e antispam, di directory server e i sistemi di gestione e monitoraggio rappresentano una particolare sfida per la sicurezza; oltre a compromettere i sistemi che li ospitano, forniscono l'opportunità di attaccare altri sistemi.

S6.2 Applicazioni interessate

Le applicazioni interessate al problema possono essere suddivise in diverse categorie:

- **Directory Server** – Utilizzati per gestire informazioni riguardanti gli utenti e i sistemi. Compromettere queste applicazioni può consentire l'accesso a grandi quantità di informazioni, compresi gli username e le password (possibilmente cifrate).
- **Sistemi di monitoraggio** – Utilizzati per monitorare altri sistemi di vario tipo. Queste applicazioni spesso possiedono degli account sui sistemi monitorati, consentendo agli aggressori di accedere facilmente a tali sistemi client.
- **Sistemi per l'aggiornamento di configurazioni e patch** – Questi sistemi sono utilizzati per gestire le configurazioni e le patch dei client. Compromettere questi sistemi offre una via privilegiata per la diffusione di malware.
- **Sistemi antivirus e antispam** – Le vulnerabilità in questi sistemi possono spesso essere sfruttate con interazioni dell'utente minime o nulle, inviando semplicemente un messaggio email appositamente predisposto. Una volta compromesso il sistema, l'aggressore può inviare più facilmente email che contengono spam o virus. Inoltre questi sistemi spesso contengono informazioni critiche, come la casella di posta degli utenti.

Queste applicazioni operano su diversi sistemi operativi, da Microsoft Windows a Solaris, HP-UX, Novell Netware e altri.

S6.3 Riferimenti CVE

CVE-2006-5478, CVE-2006-4509, CVE-2006-4510, CVE-2006-4177, CVE-2006-2496, CVE-2006-0992, CVE-2005-3653, CVE-2005-1928, CVE-2005-1929

S6.4 Come stabilire se si è a rischio

- Usando un vulnerability scanner.
- Tenendo sotto controllo gli annunci di sicurezza del produttore.

S6.5 Come proteggersi da queste vulnerabilità

- Mantenendo i sistemi aggiornati con le patch e i service pack più recenti. Se disponibile, utilizzate un sistema di aggiornamento automatizzato.
- Utilizzando sistemi di Intrusion Prevention/Detection per prevenire/individuare attacchi che utilizzano queste vulnerabilità.
- Controllando che solo gli utenti e i sistemi autorizzati abbiano accesso ai sistemi a rischio.

S6.6 Approfondimenti

Vulnerabilità di ServerProtect Trend Micro
http://archives.neohapsis.com/archives/vulnwatch/2005-q4/0066.html
http://archives.neohapsis.com/archives/vulnwatch/2005-q4/0067.html
http://archives.neohapsis.com/archives/vulnwatch/2005-q4/0068.html

Home Page di Trend Micro
http://www.trendmicro.com/

Buffer Overflow in iTechnology iGateway CA
http://supportconnectw.ca.com/public/ca_common_docs/igatewaysecurity_notice.asp

Home Page CA
http://www.ca.com/

Buffer Overflows remoto in Novell eDirectory iMonitor
http://www.zerodayinitiative.com/advisories/ZDI-06-016.html

Home Page Novell
http://www.novell.com

SQL Injection in Sygate Management Server Symantec
http://securityresponse.symantec.com/avcenter/security/Content/2006.02.01.html

Home Page Symantec
http://www.symantec.com/

Esecuzione di comandi da remoto in OpenView HP
http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c00672314
http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c00671912

Esecuzione di codice da remoto in OpenView Storage Data Protector HP
http://archives.neohapsis.com/archives/bugtraq/2006-08/0273.html

Home Page di OpenView HP
http://h20229.www2.hp.com/

Remote Command Injection in Spam Firewall Barracuda
http://archives.neohapsis.com/archives/bugtraq/2006-08/0093.html

Home Page Barracuda
http://www.barracudanetworks.com/ns/?L=en

S7. Software per database

S7.1 Descrizione

I database danno la possibilità di immagazzinare, cercare e manipolare grandi quantità di dati. Rappresentano degli elementi chiave in molti sistemi, anche se la loro presenza non è sempre direttamente visibile agli utenti. Si trovano praticamente in qualsiasi tipo di business, in applicazioni finanziarie, bancarie, di relazione con il cliente e nei sistemi di monitoraggio.

Siccome nei database sono spesso conservate informazioni molto importanti come dati personali o finanziari, questi sono spesso obiettivo di attacchi e sono particolarmente ambiti dai ladri di identità. I sistemi database sono spesso molto complessi e combinano l'applicazione principale con una serie di altre applicazioni, alcune fornite dagli stessi produttori del database, altre spesso scritte in casa (come le applicazioni web). Un difetto in uno di questi componenti può mettere in pericolo i dati contenuti. Non è sufficiente proteggere il solo database: bisogna mettere in sicurezza anche tutte le applicazioni associate. Le vulnerabilità più comuni nei sistemi database possono essere classificate come:

- Uso delle configurazioni di default con nomi utente e password predefiniti.
- SQL Injection attraverso gli strumenti specifici del database o applicazioni web di front-end aggiunte dagli utenti. Ogni anno vengono annunciate moltissime vulnerabilità di questo tipo.
- Uso di password poco sicure per account con privilegi alti
- Buffer overflow in processi in ascolto su porte TCP/UDP ben conosciute.

Esistono molti sistemi database diversi. Tra i più diffusi vi sono Microsoft SQL Server (proprietario, gira su Windows), Oracle (proprietario, gira su diverse piattaforme), IBM DB2 e IBM Informix (entrambi sistemi proprietari che possono girare su diverse piattaforme), Sybase (proprietario, gira su diverse piattaforme), MySQL e PostgreSQL (entrambi open source e utilizzabili su molte piattaforme).

A tutti i moderni database si può accedere da rete, il che significa che chiunque abbia accesso in rete e strumenti per la generazione di query di semplice reperimento può provare a connettersi direttamente al database. Le connessioni di default più comunemente utilizzate sono: Microsoft SQL attraverso la porta TCP 1433 e la porta UDP 1434, Oracle attraverso la porta TCP 1521, IBM DB2 attraverso la porta 523 e quelle dalla 50000 in su, IBM Informix attraverso le porte 9088 e 9099, Sybase attraverso la porta TCP 4100 o la 2025, MySQL attraverso la porta TCP 3306 e PostgreSQL attraverso la porta TCP 5432.

A causa delle connessioni di rete che forniscono, i database possono inoltre essere colpiti da worm; vi sono stati esempi di worm che hanno colpito Microsoft SQL e Oracle.

Oltre a correggere le specifiche vulnerabilità menzionate in questo capitolo, I tecnici che hanno a che fare con la sicurezza dei database devono esaminare:

- Le implicazioni di standard quali il Payment Card Industry Data Security Standard che richiedono la crittografia per alcune informazioni quali i numeri delle carte di credito o proibiscono lo storage di alcuni tipi di informazione.
- I rischi derivanti dal trasferimento di grandi quantità di dati o interi database verso dispositivi mobili: vi sono state numerose notizie di dati personali smarriti a causa del furto dei laptop in cui erano contenuti.

S7.2 Sistemi operativi interessati

La maggior parte dei sistemi database, sia commerciali che open source, operano su diverse piattaforme. I problemi riguardano indistintamente tutte le piattaforme supportate.

S7.3 Riferimenti CVE

Quelli che seguono sono i riferimenti alle voci che hanno avuto un punteggio CVSS maggiore o uguale a sette dal settembre 2006 in poi. Le vulnerabilità inserite precedentemente possono essere rilevate consultando le edizioni precedenti delle TOP20 SANS. Spesso i problemi non riguardano bachi specifici dei database, ma vulnerabilità nelle applicazioni accessorie, come, ad esempio, le SQL injection nelle interfacce web; questi casi non sono inseriti nel seguente elenco.

IBM DB2
CVE-2007-1086, CVE-2007-1087, CVE-2007-1088, CVE-2007-1089, CVE-2007-2582, CVE-2007-5652.

IBM Informix
Nessuna nel periodo esaminato.

Microsoft SQL Server
CVE-2007-4814

MySQL
Nessuna nel periodo esaminato.

Oracle
CVE-2006-5332, CVE-2006-5333, CVE-2006-5334, CVE-2006-5335, CVE-2006-5336, CVE-2006-5339, CVE-2006-5340, CVE-2006-5341, CVE-2006-5342, CVE-2006-5343, CVE-2006-5344, CVE-2006-5345, CVE-2006-7138, CVE-2007-0272, CVE-2007-1442, CVE-2007-2113, CVE-2007-2118, CVE-2007-5506.

Nota: Oracle pubblica trimestralmente una Critical Patch Update (CPU) che corregge i problemi riscontrati nelle applicazioni database e in quelle correlate. Questa lista contiene vulnerabilità dei programmi fondamentali del database Oracle per le quali esistono informazioni specifiche. Esistono però molte altre vulnerabilità per le quali non vi sono informazioni pubbliche se non l'invito ad applicare la relativa CPU.

PostgreSQL
CVE-2007-0555.

Nota: vi sono altri problemi registrati nelle liste di vulnerabilità come conseguenza di un white paper sulla sicurezza di PostgreSQL, ma gli sviluppatori sostengono che questi non rappresentano dei problemi di sicurezza.

Sybase
Nessuna nel periodo esaminato.

S7.4 Come stabilire se si è vulnerabili

Non basta controllare una semplice lista, mantenuta manualmente, delle applicazioni istallate. Siccome i database sono spesso distribuiti quali componenti di altre applicazioni, capita spesso di installare un database senza rendersene conto. I database possono di conseguenza rimanere privi di patch e aggiornamenti o con le vulnerabilissime configurazioni predefinite.

Eseguite una scansione delle vulnerabilità sui sistemi per stabilire quali software database sono attivi, accessibili e vulnerabili. Oltre ai vulnerability scanner "generalisti", esistono strumenti specifici, sia commerciali che di pubblico dominio; se cercate su un motore di ricerca web "*database security scanners*" troverete diversi strumenti utilizzabili. Questi variano dai semplici servizi di scansione della rete a sistemi che analizzano le password e le configurazioni predefinite, a sistemi che analizzano punto per punto la configurazione dei specifici software database.

S7.5 Come proteggersi dalla vulnerabilità dei database

- Controllate che tutti i DBMS siano aggiornati con le patch più recenti. Le versioni obsolete o non corrette molto probabilmente presentano delle vulnerabilità. Controllate spesso il sito del produttore per le informazioni sulle patch. Tenetevi aggiornati riguardo le vulnerabilità e gli avvisi pubblicati dai produttori:
  - IBM DB2 (http://www-306.ibm.com/software/data/db2/udb/support/)
  - IBM Informix (http://www-1.ibm.com/support/docview.wss?rs=0&uid=swg24009130)
  - Microsoft SQL (http://www.microsoft.com/technet/security/bulletin/notify.mspx)
  - MySQL (http://lists.mysql.com/)
  - Oracle Security Alerts (http://www.oracle.com/technology/deploy/security/alerts.htm)
  - PostgreSQL (http://www.postgresql.org/support/security)
  - Sybase (http://www.sybase.com/support)

- Assicuratevi che i DBMS e le applicazioni siano stati messi al sicuro:
  - Eliminate/cambiate le password di default per gli account di sistema e del database con privilegi alti prima di mettere il sistema in rete. Le liste degli account di default sono facilmente reperibili su Internet.
  - Assegnate i privilegi strettamente indispensabili
  - Quando possibile, usate le *stored procedure*.
  - Eliminate/disabilitate le *stored procedure* non necessarie.
  - Impostate dei limiti alla lunghezza di tutti i campi dei form.
  - Consultate la sezione Approfondimenti seguente, che indica molte risorse utili per rendere sicuri i DBMS.
  - Usate dei firewall o altri dispositivi per la sicurezza delle reti per limitare gli accessi di rete alla porte associate ai servizi database.
  - È ora disponibile un tipo di strumenti che consentono di catturare il traffico di rete verso un database e di esaminare la struttura della query SQL che vengono eseguite. Questi strumenti sono utili per la revisione delle applicazioni, in quanto identificano una serie di query valide per una applicazione e rilevano comportamenti insoliti o modelli comuni di attacco. Possono anche essere posizionate in linea con il database in modo da agire come una sorta di firewall a livello applicativo o IDS/IPS specifico per l'applicazione
  - Prendete in considerazione la crittografia delle comunicazioni tra gli applicativi e il database.
  - Non fidatevi degli inserimenti degli utenti! Assicuratevi che le applicazioni collegate al database effettuino una pulizia sul lato server di tutti gli input per evitare attacchi come le SQL injection (vedi http://www.sans.org/rr/whitepapers/securecode/23.php)

S7.6 Approfondimenti

Risorse generali e per vari database

- La sezione SANS sulla sicurezza dei database: http://www.sans.org/rr/catindex.php?cat_id=3
- La guida DoD sulle tecniche per rendere sicuri i database: http://iase.disa.mil/stigs/stig/databasestig-v7r2.pdf
- http://www.databasesecurity.com/

IBM DB2

- http://www.net-security.org/dl/articles/Securing_IBM_DB2.pdf

IBM Informix

- http://www.databasesecurity.com/informix.htm
- http://publib.boulder.ibm.com/infocenter/idshelp/v10/index.jsp?topic=/com.ibm.admin.doc/admin197.htm

Sicurezza di Microsoft SQL

- http://www.microsoft.com/sql/techinfo/administration/2000/security/default.mspx
- http://www.sqlsecurity.com/
- CIS SQL Server Benchmark Tool: http://www.cisecurity.org/bench_sqlserver.html

MySQL

- La guida passo-passo di SecurityFocus per la sicurezza di MySQL: http://www.securityfocus.com/infocus/1726
- Documentazione di MySQL, sezione sicurezza: http://dev.mysql.com/doc/refman/5.0/en/security.html
- Secure MySQL database design: http://www.securityfocus.com/infocus/1667
- MySQL security overview: http://www.devshed.com/c/a/MySQL/MySQL-Security-Overview/
- http://mysqlsecurity.com/

Oracle

- L’esauriente Checklist SANS per la sicurezza di Oracle: http://www.sans.org/score/oraclechecklist.php
- http://www.oracle.com/technology/deploy/security/pdf/twp_security_checklist_db_database.pdf
- CIS benchmarktool: http://www.cisecurity.org/bench_oracle.html
- http://www.petefinnigan.com/orasec.htm, http://www.petefinnigan.com/tools.htm
- http://otn.oracle.com/deploy/security/index.html
- http://www.red-database-security.com/whitepaper/oracle_security_whitepaper.html

Guide per rendere sicuro PostgreSQL

- http://www.postgresql.org/support/security
- http://www.postgresql.org/docs/techdocs.53

Sybase

- Guida alla sicurezza di Sybase: http://www.niiconsulting.com/innovation/Sybase.pdf

Politiche di sicurezza e personale:

H1. Diritti eccessivi dell’utente e dispositivi non autorizzati

H1.1 Introduzione

Alcuni attacchi non possono essere efficacemente prevenuti dai soli controlli tecnici. Gli utenti imprudenti possono essere attratti verso operazioni poco sicure. Gli utenti più smaliziati possono inventari metodi poco sicuri di eseguire alcuni compiti, esponendo involontariamente loro datori di lavoro a molti rischi. Per prevenire che tali rischi siano sfruttati da attacchi sono necessari controlli organizzativi per completare i controlli tecnici e fisici.

Col passare del tempo, i controlli tecnici possono essere in grado di applicare politiche che precludono alcuni comportamenti degli utenti, ma fino a quando questo risultato non viene raggiunto sono importanti dei controlli periodici al fine di garantire che i controlli organizzativi siano efficaci. È inoltre essenziale istituire un processo rilevi le violazioni alle politiche scelte e garantire che eventuali sistemi non conformi siano riportati a una situazione di rispetto delle politiche scelte in modo efficace.

H.1a Dispositivi infetti e/o non autorizzati in rete

I migliori sforzi per garantire la sicurezza di un sistema informatico diventano inutili se gli utenti connettono dispositivi non autorizzati alla rete o a un computer. Una access point wireless non autorizzato può essere una porta aperta a qualsiasi malintenzionato che vogliono avere un accesso alla rete. Un computer portatile collegato a una rete aziendale può introdurre qualsiasi malware, infettando l’intera rete. I laptop aziendali non protetti che siano stati collegati a reti pubbliche poco sicure possono trasmettere tutti i malware raccolti e condividerli con l'intera organizzazione. Migliaia di computer sono stati compromessi da attacchi in cui il proprietario di un computer portatile è specificamente preso di mira al fine di infettare il laptop con un cavallo di Troia che "chiama casa" una volta collegato alla rete aziendale. Questo permette un accesso completo a un esterno a una rete in precedenza sicura. Lo stesso vale per un esterno in grado di collegare una periferica sconosciuta sulla rete aziendale, sia questa un semplice computer portatile o un più rischioso access point wireless.

Le policy devono quindi affrontare questioni come quelle dei dispositivi non autorizzati e dei sistemi infetti, al fine di garantire una tutela adeguata delle infrastrutture informatiche aziendali, ma senza politiche di verifica sono generalmente inefficaci. Il controllo dell’accesso alla rete è diventata uno strumento importante per affrontare tali questioni. Il monitoraggio continuo dei flussi di dati e delle connessioni di rete può individuare immediatamente i dispositivi non autorizzati. Il sistema di monitoraggio degli accessi alla rete può inoltre identificare il malware, nonché garantire che le patch e le firme malware siano aggiornate. Possono quindi separare i sistemi che non soddisfano i criteri scelti e metterli in quarantena fino a quando non hanno raggiunto gli standard definiti nella politica aziendale.

H.1b Diritti eccessivi dell’utente e software non autorizzato

Il software non regolamentato introduce in azienda diversi rischi. Tale software può contenere vulnerabilità di sicurezza e chi lo usa può essere non sufficientemente informato o motivato per applicare regolarmente le patch. Inoltre gli utenti (o le persone che utilizzano il loro computer senza l'approvazione aziendale come figli o coniugi) possono installare software che, senza che gli utenti lo sappiano, contiene malware che potrebbero portare a compromettere la sicurezza dei dati o della rete. Gli utenti potrebbero anche installare software che forniscono funzionalità tali (ad esempio il file sharing peer-to-peer) da introdurre nuove vulnerabilità nell’ambiente di rete. Chi è responsabile per la sicurezza delle informazioni dovrebbe quindi prendere in considerazione l'attuazione di politiche, e dei corrispondenti controlli correttivi, atte a mitigare tali vulnerabilità

Le organizzazioni sono vulnerabili se agli utenti sono concessi diritti che consentano loro di installare da soli software in una modo incontrollato. Questa libertà può portare anche a software pirata installato sui sistemi aziendali, fatto che apre un'altra serie di questioni da analizzare da un punto di vista giuridico. Per correggere questi problemi è essenziale applicare una politica di limitazione dei diritti dell’utente fino a garantirgli i privilegi minimi indispensabili necessari per eseguire le funzioni connesse alla mansione lavorativa. Una politica di questo tipo nei fatti elimina molti problemi legati ai malware, a programmi potenzialmente indesiderati e a software pirata installato autonomamente dall'utente.

H1.2 Approfondimenti

http://www.isaca.org/Template.cfm?Section=Home&CONTENTID=17170&TEMPLATE=/ContentManagement/ContentDisplay.cfm

http://technet2.microsoft.com/WindowsServer/en/library/e903f7a2-4def-4f5f-9480-41de6010fd291033.mspx?mfr=true

http://www.sans.org/resources/policies/Password_Policy.pdf

http://www.sans.org/resources/policies/Acceptable_Use_Policy.pdf

http://www.cerias.purdue.edu/weblogs/spaf/general/post-30/

H2. Phishing e Spear Phishing

H2.1 Descrizione

Furto d'identità online
Furto d'identità (*Identity Theft*) è l'espressione utilizzata per descrivere una azione in cui una persona usa l'identità di un'altra per ottenere in modo fraudolento credito, beni e servizi o per commettere qualche crimine. Alcuni esempi di questi crimini sono le frodi bancarie e con carte di credito, frode elettronica, frode postale, riciclaggio di denaro sporco, bancarotta fraudolenta e crimini informatici. La diffusione di Internet ha amplificato alcuni schemi tradizionali legati alle frodi, in particolare il cosiddetto furto d'identità online.

La parola "phishing" fu usata la prima volta quando nel 1996 alcuni hacker iniziarono a impadronirsi di account di America On-Line inviando messaggi e-mail agli utenti AOL che fingevano di provenire dalla stessa America On-Line. Gli attacchi di phishing oggi prendono di mira utenti di servizi di online banking, servizi di pagamento come PayPal, di siti di commercio elettronico, di utenti web-mail. Questi attacchi sono rapidamente cresciuti in numero e in sofisticatezza. Le maggiori banche USA, del Regno Unito e dell' Australia sono infatti state vittima di attacchi phishing.

Spear Phishing
Gli autori di questo tipo di frode inviano messaggi di posta elettronica che contengono informazioni che riguardano gli impiegati o gli attuali problemi organizzativi dell'azienda, le quali le fanno apparire attendibili a tutti gli impiegati o i membri di una determinata società, ente pubblico, organizzazione o gruppo. Il messaggio può apparire come inviato dal datore di lavoro o da un collega che avrebbe potuto spedire un messaggio e-mail a tutto il personale, come ad esempio il responsabile delle risorse umane o colui che gestisce il sistema informativo, e può comprendere richieste legate a username o password oppure invitare i destinatari a scaricare allegati dannosi da un sito web infetto. Lo spear phishing è diventato una delle forme di attacco più devastanti presso le organizzazioni militari americane e di altri paesi sviluppati. I phisher guadagnano in questo modo informazioni sugli username e sulle password che utilizzano per intrufolarsi attraverso i sistemi di filtro che proteggono le informazioni militari riservate.

Voice Phishing
Una nuova forma di phishing sostituisce il sito web con un numero di telefono. In questa forma di phishing, una e-mail vi invita a chiamare uno specifico numero dove, installato presso una linea telefonica voce compromessa, trova un interlocutore o un sistema di risposta automatica in attesa di prendere il vostro numero di conto, numero di identificazione personale, la password o altri dati personali di valore. Se vi rifiutate di rispondere alle domande, la persona o il sistema audio dall'altra parte del filo potrebbe sostenere che il vostro conto verrà chiuso o che si potrebbero verificare altri problemi simili.

H2.2 Sistemi operativi interessati

Il phishing è una tecnica di social engineering che prende di mira gli utenti. Per quando esistano varie applicazioni aggiuntive che possono fornire una qualche difesa contro le tecniche di phishing, tutti i sistemi operativi possono essere considerati ugualmente colpiti, poiché l'obiettivo dell'attacco non è tanto il sistema quanto l'utente finale. È un istinto naturale umano quello di fidarsi e i tentativi di phishing tentano di sfruttare proprio questo. Per quanto questi attacchi siano agevolati da difetti nei browser, nei sistemi di posta elettronica e nei DNS, lo sono solo nel migliorare l'apparenza di legittimità del messaggio: alla fine è l'utente finale che viene ingannato se fornisce informazioni al phisher.

H2.3 Come stabilire se si è a rischio

Il phishing per riuscire nel suo intento utilizza principalmente tecniche di social engineering. La consapevolezza di tali tecniche può diminuire la possibilità di essere a rischio in tali attacchi

I ladri di identità possono anche usare le intrusioni nei computer in organizzazioni come quelle degli operatori di business on-line per raccogliere grandi quantità di dati su carte di credito o altre informazioni identificative. Essi possono inoltre cercare di raccogliere informazioni disponibili su siti Internet pubblici: è meglio quindi non esporre troppe informazioni su se stessi e i propri familiari (ad esempio indirizzi e numeri di telefono) in siti di community come MySpace, Facebook e Orkut

H2.4 Come proteggersi dagli attacchi phishing

Dal momento che gli attacchi di phishing sono rivolti a utenti, la sensibilizzazione degli utenti è un elemento fondamentale di difesa. Il più promettente metodo di arresto dello spear phishing è quello di organizzare periodici corsi di formazione per sensibilizzare tutti gli utenti, che può includere anche tentativi simulati di phishing per verificare la sensibilizzazione degli utenti.

Metodi meno efficaci, ma comunque validi sono:

- Evitare di inviare mail comuni ai vostri clienti con link diretti al vostro sito web o a un sito terzo. In questo modo si abitua i clienti ad accettare come normali le e-mail di questo tipo.
- Non usate le vostre credenziali di autenticazione o altre informazioni personali non pubbliche per autenticare la vostra clientela.
- Mantenete un sistema di log per identificare qualsiasi cambiamento di informazioni dell'utente nei sistemi online.
- Assicuratevi che tutti i casi di frode siano denunciati all'autorità competente.
- Software anti-phishing: applicazioni che tentano di individuare i contenuti di phishing nelle e-mail e nei siti web, di solito integrati nei browser web e nei client di posta elettronica. Esistono diverse opzioni:
  - Toolbar NetCraft: disponibile sia per Internet Explorer che per Firefox
  - Google Safe browsing: disponibile per Firefox
  - Ebay Toolbar: disponibile per Internet Explorer
  - Earthlink Scamblocker: disponibile sia per Internet Explorer che per Firefox
  - Geotrust Trustwatch - disponibile per Internet Explorer, Firefox e Flock
  - McAfee SiteAdvisor - disponibile sia per Internet Explorer che per Firefox
- Formazione dell'utente: una delle migliori strategie per la lotta contro il phishing è quello di educare gli utenti ai metodi correnti e a tutte le nuove tecniche di attacco di phishing, e di renderli edotti su cosa fare in caso di un attacco phishing
- Doppia autenticazione (Two Factor Authentication): Prevedere, quando possibile, un diverso meccanismo di autenticazione oltre alla password.

H2.6 Approfondimenti

Anti-Phishing Working Group
http://www.antiphishing.org/

3sharp study Gone Phishing: Evaluating Anti-Phishing Tools for Windows
http://www.3sharp.com/projects/antiphishing/gone-phishing.pdf

VoIP Phishing Scams
http://blogs.pcworld.com/staffblog/archives/001921.html

The Ghost In The Browser; Analysis of Web-based Malware
http://www.usenix.org/events/hotbots07/tech/full_papers/provos/provos.pdf

Phone phishing: The role of VoIP in phishing attacks
http://searchsecurity.techtarget.com/tip/0,289483,sid14_gci1193304,00.html

Phishing and Spamming via IM (SPIM)
http://isc.sans.org/diary.html?storyid=1905

Suspicious e-Mails and Identity Theft
http://www.irs.gov/newsroom/article/0,,id=155682,00.html

H3. Laptop senza crittografia e dispositivi rimovibili

H3.1 Descrizione

La perdita di computer portatili e di supporti rimovibili è diventata un'importante responsabilità per le imprese e gli enti pubblici, oltre che per i privati. Troppo spesso capita che grosse fughe di dati personali o altre informazioni derivino da il furto o lo smarrimento di un laptop o di un supporto di memorizzazione rimovibile.

In passato, i dati personali venivano memorizzati in registri cartacei o in sistemi centralizzati. Con la crescita della capacità di memorizzazione dei computer, è possibile archiviare grandi quantità di informazioni personali su computer portatili, desktop o dispositivi portatili. Questa portabilità provoca un maggiore rischio di perdita o di compromissione dei dati, sia questa dovuta a dolo o a semplice distrazione. Dal momento che i dispositivi di archiviazione rimovibili sono stati progettati specificamente per la portabilità, essi tendono anche ad essere persi o lasciati nel posto sbagliato.

Siccome i dispositivi di memorizzazione portatili sono spesso condivisi tra diverse macchine, rappresentano un potente vettore di propagazione del malware. Gli utenti spesso condividono i dispositivi tra sistemi aziendali e personali o domestici, fornendo un evidente opportunità di diffusione a virus e altri malware, che possono così propagarsi tra reti e ubicazioni fisiche diverse.

Identità messe in pericolo da recenti perdite di computer portatili:

Azienda	ID messe in pericolo dalla perdita di dispositivi senza crittografia
Gap Inc. (San Francisco, CA) http://www.gapsecurityassistance.com/	800,000
New York City Financial Information Services Agency (New York, NY)	280,000
Connecticut Department of Revenue Services (Hartford, CT)	106,000
TSA (Arlington, VA)	100,000
Yuba County Health and Human Services (Yuba County, CA)	70,000
Home Depot (Boston, MA)	10,000
Transportation Security Administration (Arlington, VA)	3,930

Statistiche da: http://www.privacyrights.org/ar/ChronDataBreaches.htm

H3.2 Come stabilire se si è a rischio

Tutte le aziende hanno qualche dato che deve essere protetto: segreti commerciali, informazioni di identificazione personale, dati personali dei dipendenti, dati relativi alle buste paga e alle risorse umane, dati relativi alle vendite, listini, contatti, database dei clienti e via dicendo. In assenza di controlli attivi che assicurino che tutti i dispositivi portatili e i supporti rimovibili siano crittati autorizzati, qualche rischio è sempre presente. Ecco alcune domande che aiutano a determinare il livello di rischio:

- Qual è la politica in materia di dati critici che si spostano su supporti rimovibili o computer portatili?
- Quale sistema di crittografia è installato e utilizzato su portatili, palmari e supporti removibili?
- Quali sono i controlli in atto per monitorare l'accesso ai dati critici che possono determinare il trasferimento non autorizzato dei dati?
- Quali sono i controlli in atto per assicurarsi che tutti i dispositivi di storage siano distrutti (o cancellati in modo sicuro) in modo che i dati non siano più accessibili o recuperabili quando smaltiti?

H3.3 Strategie per ridurre il rischio

- Come minimo è necessaria una policy di sicurezza scritta che riguardi i computer portatili e i dispositivi di memorizzazione removibili. La policy dovrebbe essere controllata ed approvata dai vertici organizzativi. Se la cosa è possibile, nella policy dovrebbe essere indicato l'obbligo di cifrare tutti i dati contenuti sul portatile e sui dispositivi removibili.
- Se dovesse risultare impossibile approvare una politica che introduca sistemi di crittografia completa, si potrebbe provare a introdurre una crittografia a livello di disco o di file system per almeno per alcuni file. Se si applica tale strategia, abbiate cura di farla precedere da una analisi accurata: i sistemi operativi e le applicazioni spesso memorizzano i lavori e dati temporanei in cartelle che potrebbero risiedere al di fuori dell'area cifrata nel sistema. Bisogna evitare un falso senso di sicurezza quando è implementata solo una cifratura parziale.
- Ci dovrebbe essere una policy chiara che identifichi quali sistemi vadano soggetti a cifratura: tutti i sistemi o alcuni sottoinsiemi di sistemi. La policy di sicurezza dovrebbe obbligare a archiviare i dati riservati solo sui sistemi effettivamente cifrati. Naturalmente, dovrebbero essere implementati alcuni metodi efficaci per assicurarsi che i sistemi siano conformi alle policy di sicurezza definite.
- I metodi e gli strumenti per decriptare, incluse le chiavi di crittografia, dovrebbero essere noti solo a un numero molto limitato di individui. Ciò nonostante, in nessuna circostanza la capacità di decifrare i dati dovrebbe essere affidata ad un singolo individuo, poiché la mancanza di quest'ultimo sarebbe catastrofica quanto la perdita dei dati. Dovrebbero essere implementate strategie di condivisione delle chiavi crittografiche e strategie di deposito delle chiavi presso terzi.
- Per quanto riguarda i dispositivi removibili, le policy di sicurezza dovrebbero indicare chi è autorizzato ad utilizzare questi dispositivi, la natura dei dati (tipologia e grado di criticità) che possono essere memorizzati, se possono essere portati al di fuori dell'ambiente aziendale e, possibilmente, gli specifici tipi e modelli di dispositivi removibili utilizzabili.
- Una volta che la policy di sicurezza è presente, l'azienda dovrebbe scegliere il livello e il metodo di controllo da implementare. Si può andare dall'assenza di controlli tecnici (si fa un affidamento esclusivo sulla policy) fino all'impiego di specifici software che limitano le possibilità di utilizzo di dispostivi removibili.
- Dovrebbero essere predisposte misure di sicurezza che notifichino allo staff tecnico il momento in cui dati riservati vengono trasferiti su dispositivi o sistemi removibili. Si tratta di un compito per niente banale, che aiuta spesso a compiere una scelta tra una soluzione di cifratura che interessi l'intero disco o una cifratura parziale.
- Spesso la perdita di dispositivi contenenti dati riservati è colpa di soggetti terzi, come società esterne che effettuano operazioni strumentali, piuttosto che delle organizzazioni proprietarie dei dati. Per ridurre questo rischio è necessario aggiungere specifici requisiti per la crittografia dei dati e dei supporti di storage al momento di stipulare un contratto con società esterne che possono aver accesso a dati riservati.

H3.4 Approfondimenti :

Usare le Group Policy per disabilitare USB, CD-ROM e Floppy Disk
http://support.microsoft.com/kb/555324

Elenco di violazioni dei dati personali
http://www.privacyrights.org/ar/ChronDataBreaches.htm

Elenco delle leggi americane sulla divulgazione dopo la perdita di informazioni personali (PII)
http://www.vigilantminds.com/files/vigilantminds_state_security_breach_legislation_summary.pdf

Perdita di laptop
http://www.numbrx.net/2006/08/19/chevron-employees-data-lost-with-stolen-laptop/
http://www.caslon.com.au/datalossnote3.htm
http://privacy.med.miami.edu/learning_from_others.htm
http://wizbangblog.com/content/2007/08/02/laptop-theft-leaves-verisign-employees-data-exposed.php
http://seattlepi.nwsource.com/business/295769_boeing13.html
http://www.journalinquirer.com/site/news.cfm?newsid=18840780&BRD=985&PAG=461&dept_id=161556&rfi=6

Perdita di chiavi USB
http://www.fcw.com/article97113-12-18-06-Print
http://www.kristv.com/Global/story.asp?S=6667387
http://redtape.msnbc.com/2006/04/military_thumb_.html

http://www.securestix.com/bad_news.php
http://www.nytimes.com/2006/04/14/world/asia/14afghan.html?_r=2&oref=slogin&oref=slogin

Perdita di supporti di backup

In febbraio, Bank of America ha perso una serie di supporti di backup non cifrati che erano stati spediti tramite in aereo di linea; i dati comprendevano dettagli relativi a milioni di clienti.
http://tinyurl.com/4jvbz

In aprile, Iron Mountain ha perso la sua quarta spedizione di nastri di backup dal 2005 - questa volta contenente dati di circa 600000 attuali ed ex dipendenti della Time Warner
http://www.networkworld.com/news/2005/050605-timewarner.html?rl

In giugno, Citigroup ha annunciato che i nastri di backup spediti tramite UPS sono stati smarriti durante il trasporto; i dati al loro interni comprendevano i numeri di Social Security di 3.9 milioni di clienti.
http://www.networkworld.com/news/2005/060605-citibank.html?rl

In novembre, Marriott International ha scoperto la mancanza di supporti nastri di back-up del suo Vacation Club; alla fine dell'anno ha annunciato i nastri smarriti o rubati contenevano dati relativi alla carta di credito e i numeri di Social Security di 206.000 clienti e di qualche impiegato.
http://www.washingtonpost.com/wp-dyn/content/article/2005/12/27/AR2005122700959.html

Abuso di applicazioni:

A1. Instant Messaging

A1.1 Descrizione

L'instant messaging (IM) è un metodo di comunicazione considerato sempre più legittimo sia per uso personale, sia per un uso aziendale. Le applicazioni IM sono disponili per diverse piattaforme, che variano dal tradizionale IM per PC ai telefoni cellulari. L'utilizzo diffuso di messaggistica istantanea L'uso intensivo di messaggeria istantanea, nonostante porti dei vantaggi per gli utenti, può incrementare in modo significativo i rischi per la sicurezza, sia per le aziende che per gli utenti stessi. Gli attacchi comprendono varianti dei worm per e-mail diffusi attraverso l'instant messaging, nuove variazioni nell'installazione e nella diffusione di botnet e l'uso di account di instant messaging compromessi per spingere gli utenti a rivelare informazioni riservate.

Le area generali di rischio correlate all'instant messaging sono:

- Malware – Worm, virus e Trojan diffusi attraverso la messaggistica istantanea. Molti bot sono controllati attraverso i canali IRC.
- Informazioni confidenziali – Le informazioni veicolate attraverso l'instant messaging possono essere soggette a divulgazione in numerose fasi della comunicazione. I messaggi passano di solito attraverso reti e server che non sono sotto il controllo aziendale. Molti programmi IM offrono inoltre anche la possibilità di condividere file. Il processo di condivisione potrebbe lasciare dei duplicati di documenti confidenziali in cartelle condivise da tutti i partecipanti alla conversazione anche dopo che la sessione IM ha avuto termine.
- Reti – Attacchi di denial of service; eccessivo utilizzo della capacità della rete, anche quando l'uso è legittimato.
- Vulnerabilità nelle applicazioni – Le applicazioni di instant messaging possono contenere vulnerabilità che, se sfruttate, possono il sistema colpito. Inoltre, nelle applicazioni IM le possibili vulnerabilità possono comprendere errori nel software di supporto e interfaccia improprie per moduli del software di supporto. Alcune funzionalità delle applicazioni di messaggistica istantanea possono basarsi su moduli provenienti da altri programmi e dal sistema operativo sottostante, ereditando le vulnerabilità presenti in queste programmi. In aggiunta, siccome possono essere chiamati solo moduli specifici, i processi di sicurezza costruiti attorno ai livelli più alti dell'applicazione di supporto possono essere elusi, creando nuove strade per gli attacchi.

Le applicazioni di messaggistica istantanea mobile presentano significativi rischi di sicurezza analoghi a quelli associati a quelle per PC. Dispositivi come i telefoni cellulari con possibilità di instant messaging spesso non hanno protezioni da password o sistemi di cifratura dei dati memorizzati al loro interno. Il risultato è che attacchi *masquerade* verso i contatti e-mail e IM sono di semplice implementazione usando magari dispositivi mobili IM smarriti. La natura wireless dei dispositivi mobili rende inoltre più difficile l'implementazione di un adeguato sistema di sicurezza durante le sessione di messaggistica istantanea.

Le applicazioni di instant messaging più diffuse sono: AOL Instant Messenger (AIM), Gaim, ICQ, Jabber Messenger, Lotus Sametime, Skype, QQ, Windows Live Messenger (WLM), Google Talk, Trillian e Yahoo! Messenger. I protocollo di instant messaging comprendono: IRC, MSNP, OSCAR, SIMPLE, XMPP e YMSG.

A1.2 Sistemi operativi interessati

Le applicazioni di instant messaging sono disponibili per tutti i sistemi operativi più diffusi.

A1.3 Riferimenti CVE

CVE-2007-1680, CVE-2007-2418, CVE-2007-2478, CVE-2007-2931, CVE-2007-3305, CVE-2007-3832, CVE-2007-3928, CVE-2007-4579

A1.4 Come proteggersi dalle vulnerabilità IM e dall'uso non autorizzato dei sistemi di instant messaging

- Istituendo policy per regolamentare l'uso dell'instant messaging e assicurandosi che tutti gli utenti siano sensibilizzati su tali politiche e abbiano compreso chiaramente i potenziali rischi
- Istituendo policy per regolamentare l'so dei dispositivi mobili che comprendano obblighi relativi a password e crittografia.

- Creando degli opportuni standard di configurazione dei prodotti IM che impediscano il trasferimento di file.
- Di regola, agli utenti non dovrebbe essere permessa l'installazione di software. Limitate i privilegi di Amministratore e Power User al personale di supporto e solo nell'ambito della loro attività di supporto tecnico. Se un utente ha bisogno di privilegi di Amministratore o Power User, creategli anche un diverso account con privilegi minori da utilizzare quando svolge le nomali funzioni d'ufficio, la per la navigazione Internet e le comunicazioni on-line.
- Assicurandosi che vengano prontamente applicate le patch del produttore ai software di instant messaging, alle applicazione collegate e ai sottostanti sistemi operativi.
- Impiegando prodotti anti-virus e anti-spyware.
- Non affidandosi a server IM esterni per l'instant messaging interno; affidatevi a un proxy commerciale o a un server IM interno.
- Creando canali di comunicazione sicuri quando si utilizza la messaggistica istantanea con partner commerciali fidati.
- Configurando in modo appropriato i sistemi di intrusion detection/prevention. Bisogna capire che molte applicazioni di instant messaging sono in grado di abilitare comunicazioni associate per mascherare o legittimare in qualche altro modo il traffico prodotto (ad esempio mascherando da traffico http).
- Adottando prodotti progettati specificamente per la sicurezza dell'instant messaging.
- Filtrando tutto il traffico http attraverso un proxy server con autenticazione per ottenere maggiori possibilità di filtro e di monitoraggio del traffico generato dall'instant messaging.
- Bloccando l'accesso a tutti quei server pubblici di instant messaging conosciuti che non siano esplicitamente autorizzati. (Nota: questa misura offre solo una protezione parziale, in quanto è molto alto il numero di potenziali server esterni.)
- Bloccando le porte comunemente utilizzate dall'instant messaging. (Nota: anche questa misura offre una protezione solo parziale, considerando che i protocolli utilizzati e le porte di conseguenza associate sono innumerevoli, oltre al fatto che alcune applicazioni riewscono a eludere le restrizioni relative alle porte.)
- Monitorando tramite un sistema di Intrusion Detection/Prevention gli utenti che creano tunnel per gli IM o eludono i proxy.
- Istruendo i partner con i quali condividete file e insegnando loro a cancellare i file condivisi al termine della sessione di IM.
- Stabilendo degli accordi dettagliati con i partner con i quali dovete condividere documenti riservati, specificando i termini di non divulgazione e le rispettive responsabilità.
- Usando dei controlli di accesso (come le password) per proteggere presentazioni e sessioni di gruppo.

A1.5 Approfondimenti

Phishers hijack IM accounts
http://news.com.com/Phishers+hijack+IM+accounts/2100-7349_3-6126367.html

Instant messaging: a new target for hackers
http://www.leavcom.com/ieee_july05.htm

AIM bot creates "fight combos" to spread
http://www.securityfocus.com/brief/305

Secure Instant Messaging in the Enterprise
http://searchsecurity.techtarget.com/tip/0,289483,sid14_gci1199405,00.html

Remote command execution, HTML and JavaScript injection vulnerabilities in AOL's Instant Messaging software
http://www.securityfocus.com/archive/1/480587

A2. Applicazioni per la condivisione di file Peer to Peer

A2.1 Descrizione

Le reti Peer to Peer (P2P) sono costituite da una serie di computer o "nodi" che funzionano simultaneamente da "client" e da "server" per raggiungere un intento comune. I nodi possono scambiarsi dati, condividere risorse, fornire servizi di directory, sostenere comunicazioni e fornire strumenti per la collaborazione in tempo reale.

Possono essere utilizzate molte architetture di controllo e comunicazione. Talvolta vengono utilizzati dei server di indicizzazione centralizzati che forniscono i servizi di ricerca dei dati e dei servizi disponibili. Nelle rete completamente distribuite ciascun nodo collabora a servizi di indicizzazione e di ricerca ed è del tutto equivalente ad un altro nodo. Le architetture ibride, invece, combinano le caratteristiche dei due modelli in differenti gradazioni: gruppi di nodi possono "scegliere/promuovere" determinati nodi per fungere da server di indicizzazione e di ricerca in una determinata zona.

Molte applicazioni legali usano il P2P. Alcuni produttori di software, tra i quali Microsoft e Sun, propongono diversi strumenti per utilizzarle e incoraggiano lo sviluppo di applicazioni P2P. Tuttavia le applicazioni P2P, come qualsiasi altro strumento per il trasferimento di informazioni, possono portare a usi non corretti o sfruttate per condividere illegalmente materiale soggetto a diritto d'autore, per ottenere dati riservati, per inviare agli utenti materiale non desiderato a carattere pornografico, violento o propagandistico, per distribuire ed eseguire codice dannoso (virus, spyware, bot, ecc.), per sovraccaricare la rete, per tracciare usi e modelli di comportamento degli utenti: tutte azioni che possono comportare una responsabilità nei confronti delle leggi. La responsabilità legale e la conseguente perseguibilità possono in certi casi non essere limitate al singolo esecutore, ma essere estese al promotore, ai sostenitori e ai membri della rete.

Le stesse reti P2P possono essere vittima di attacchi che possono sostituire file legittimi tramite con codici dannosi, seminando questi malware nelle directory condivise, sfruttando errori nel codice o le vulnerabilità insite nel protocollo, bloccando (filtering) il protocollo, eseguendo attacchi di denial of service che portano la rete a funzionare molto lentamente, operando con spamming e attacchi d'identità che portano ad identificare gli utenti della rete per poi perseguitarli. Alcune azioni legali hanno portato alla chiusura di alcune reti molto popolari, colpevoli di aver infranto le normative che regolano i diritti d'autore.

Il Worm Storm usa il protocollo Peer to Peer di eDonkey/Overnet per comunicare con gli host infetti. Si è stimato che esso fosse presente, fino a Settembre 2007, in **un numero di computer infetti e compromessi che va da 1.000.000 a 50.000.000**.

I concetti e le tecniche P2P sono in continua evoluzione e si possono trovare in:

- Reti per la condivisione di file (*file sharing*) — il cui obiettivo primario è quello di condividere risorse quali la memoria e la banda. Queste operano attraverso una rete distribuita di client, condividendo cartelle di file o interi dischi di dati. I client partecipano scaricando i file dagli altri utenti, rendendo disponibili agli altri i propri dati e coordinando per gli altri utenti le ricerche di file
- Cloud Computing — (conosciuto anche come elaborazione distribuita, Grid Computing, o reti mesh) dove "nuvole" di computer sono dedicate a fornire un ambiente virtuale di calcolo per compiere determinate operazioni distribuendo i dati e il carico di elaborazione. Il Cloud Computing inserisce i server in linea a seconda delle esigenze e l'utente finale non sa dove i dati risiedano o vengano elaborati in quel momento. In alcuni casi l'applicazione viene eseguita in parte sui server e in parte sui PC degli utenti. I server cloud possono risiedere fisicamente presso grandi strutture controllate da una organizzazione o in qualunque luogo in Internet. Poiché la potenza di calcolo modulabile si basa sui server virtuali, il proprietario dei dati non sa mai dove questi dati o i sui programmi risiedano fisicamente davvero.

La maggior parte dei programmi P2P usano una serie di porte di default, ma possono essere automaticamente o manualmente configurati per usare porte diverse quando è necessario aggirare sistemi di rilevamento, firewall o filtri in uscita. La tendenza sembra essere quella di andare verso l'uso dei wrapper http e della crittografia per aggirare le restrizioni aziendali.

A2.2 Sistemi operativi interessati

Sono presenti versioni dei software P2P per tutti i sistemi operativi Microsoft Windows attualmente in uso, lo stesso vale per Linux, MacOS e la maggior parte dei sistemi operativi Unix.

A2.3 Rilevare l'attività P2P

Rilevare l'attività P2P sulla rete può risultare impegnativo. È possibile individuare software P2P che girano sulla vostra rete nei seguenti modi:

- Monitorando il traffico su determinate porte TCP/UDP è un metodo che ha efficacia solo per i programmi P2P più datati. Molti programmi più recenti, invece, hanno iniziato ad usare http, https e altre porte che di solito hanno bisogno di essere aperte nei firewall e nei proxy.
- Usando un application layer per protocolli P2P, che può identificare i programmi che usano le porte di solito permesse (come la porta 53 o la porta 80). Anche questo, però, fallisce quando programmi più scaltri usano la crittografia per il traffico che veicolano.
- Usando alcuni intrusion prevention software host based e strumenti di *system change auditing*, che possono prevenire l'installazione o l'esecuzione di applicazioni P2P assieme ad altro codice indesiderato.
- Tramite alcuni sistemi di Intrusion Detection con funzioni di *pattern matching / behavioral*, che possono identificare potenziali membri P2P. I pattern osservati includono la frequenza, il timing e la dimensione dei flussi di comunicazione.
- Effettuando delle scansioni della rete e della memoria dei PC alla ricerca dei contenuti normalmente scaricati dagli utenti P2P, ovvero *.mp3, *.wma, *.avi, *.mpg, *.mpeg, *.jpg, *.gif, *.zip, *.torrent, e *.exe.
- Rilevando i cambiamenti nelle performance della rete, che possono indicare picchi dovuti all'uso di P2P o a infezioni causate da malware.
- Alcuni Firewall e prodotti di Intrusion Detection/Prevention combinano diverse tecniche di detection per rilevare o prevenire il traffico P2P in ingresso o in uscita dalla rete.
- Nelle macchine Microsoft Windows è possibile utilizzare SMS per analizzare gli eseguibili installati nelle workstation. Oltre a ciò, gli amministratori dovrebbero limitare i permessi in modo da impedire agli utenti di installare i software P2P sulle loro postazioni.
- I sistemi compromessi che hanno dei malware installato via file sharing P2P mostreranno gli stessi sintomi rilevati quando sono vittime di malware diffuso con altri metodi.

A2.4 Come proteggersi dalle vulnerabilità che derivano dai software P2P

- Agli utenti standard non dovrebbe essere consentita l'istallazione di software. Limitate i privilegi di Amministratore e Power User al personale di supporto per le loro funzioni tecniche. Se un utente ha bisogno di privilegi di Amministratore o Power User, creategli anche un diverso account da utilizzarsi per il normale lavoro di ufficio, per la navigazione web e la comunicazione on-line.
- Usate strumenti come DropMyRights di Microsoft per rendere sicuri i browser web e i client mail.
- In ambienti Active Directory è possibile usare le *Software Restriction Group Policies* per bloccare l'esecuzione di tipi noti di file binari.
- Sensibilizzate gli utenti riguardo le reti P2P, sottolineando i pericoli del file sharing e illustrando le politiche aziendali in proposito.
- Abilitate i filtri in uscita per limitare tutte le porte non necessarie alle attività aziendali, ma considerate il fatto che molte applicazioni P2P si stanno spostando verso l'http e la crittografia, rendendo meno efficace questa misura.
- Monitorate i log del firewall e degli IDS.
- Per ridurre le infezioni da malware che possono essere diffuse da numerose applicazioni P2P, usate prodotti antispyware e antivirus in tutta l'azienda e assicuratevi che siano aggiornati quotidianamente.
- Usate firewall sugli host oltre ai firewall perimetrali. Windows XP e Windows 2003 includono il Windows firewall che fornisce, se adeguatamente configurato, una buona protezione. Molti firewall *host based* di terze parti (ZoneAlarm, Sygate, Outpost) offrono ulteriori funzionalità e flessibilità. I sistemi Windows 2000, XP e 2003 possono utilizzare anche le policy IPSec, che forniscono una funzione di filtro delle porte rispetto al traffico non necessario sulle VPN. In ambienti Active Directory, le policy IPSec e la configurazione di Windows Firewall (per Windows XP SP2 e Windows 2003 SP1) possono essere gestite in maniera centralizzata tramite le Group Policy.
- Disabilitate la funzione *Condivisione file semplice* (Simple File Sharing) in Windows XP se non assolutamente necessaria [Start -Impostazioni –Pannello di controllo –Opzioni Cartella - Visualizzazione –Deselezionate l'impostazione *Condivisione file semplice* – Applica - OK.]
- Monitorate i sistemi alla ricerca di eseguibili non conosciuti e modifiche non autorizzate dei file di sistema. Si può utilizzare prodotti software come Tripwire o AIDE (c'è una versione commerciale e una open source) per verificare i cambiamenti nei file.

- Le condivisioni basate su Samba possono essere configurate per eseguire dei filtri sull'apertura o sul salvataggio dei file. Un *filetype detector* e un sistema di avvisi possono essere utili per prevenire l'abuso delle condivisioni.

A2.5 Approfondimenti

Voce Peer-to-peer di Wikipedia
http://en.wikipedia.org/wiki/Peer-to-peer
http://it.wikipedia.org/wiki/Peer-to-peer

Worm Storm
http://www.secureworks.com/research/threats/view.html?threat=storm-worm
http://en.wikipedia.org/wiki/Storm_botnet

Sito sul Cybercrime del Dipartimento di Giustizia USA:
http://www.usdoj.gov/criminal/cybercrime

Altri fornitori di software che possono essere coinvolti in problemi legali legati al diritto d'autore
http://www.usdoj.gov/criminal/cybercrime/2006IPTFProgressReport(6-19-06).pdf

Una iniziativa didattica dell'FBI
http://www.fbi.gov/cyberinvest/cyberedletter.htm

The Information Factories
http://www.wired.com/wired/archive/14.10/cloudware_pr.html

Mobile Service Clouds: A Self-managing Infrastructure for Autonomic Mobile Computing Services
http://www.cse.msu.edu/~farshad/publications/conferences/samimi06msc.pdf

Cyber Security Tip ST05-007 –Rischi della tecnologia per il File-Sharing
http://www.us-cert.gov/cas/tips/ST05-007.html

Rischi del File Sharing P2P (Presentazione)
http://www.ftc.gov/bcp/workshops/filesharing/presentations/hale.pdf

Protezione di Windows XP Professional in un ambiente di rete peer-to-peer
http://www.microsoft.com/italy/technet/security/smallbusiness/prodtech/windowsxp/sec_winxp_pro_p2p.mspx

Identificare gli utenti P2P con l'analisi del traffico -Yiming Gong -2005-07-21
http://www.securityfocus.com/infocus/1843

Bot software looks to improve peerage
http://www.securityfocus.com/news/11390

Fermare i bot
http://www.securityfocus.com/columnists/398/1

Blocco di specifici protocolli di rete e porte utilizzando IPSec (MS KB articolo 813878)
http://support.microsoft.com/kb/813878

Utilizzo delle Software Restriction Policy per proteggersi dal software non autorizzato
http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/rstrplcy.mspx

Disponibilità e la descrizione dello strumento Reporter Porta (MS KB articolo 837243)
http://support.microsoft.com/kb/837243

Nuove funzionalità e funzionalità in PortQry versione 2.0 (MS KB articolo 832919)
http://support.microsoft.com/default.aspx?kbid=832919

Log Parser 2.2
http://www.microsoft.com/technet/scriptcenter/tools/logparser/default.mspx

Browsing the Web and Reading E-mail Safely as an Administrator (DropMyRights)
http://msdn2.microsoft.com/en-us/library/ms972827.aspx

Amazon Cloud Computing goes beta
http://www.amazon.com/gp/browse.html?node=201590011

Checkpoint Application Intelligence
http://www.checkpoint.com/products/downloads/applicationintelligence_whitepaper.pdf

Ricerca sul sito Microsoft riguardo il peer-to-peer
http://search.msdn.microsoft.com/search/default.aspx?siteId=0&tab=0&query=peer-to-peer

Vulnerabilità dei sistemi di Instant-Messaging e P2P-per il settore sanitario
http://eziniearticles.com/?Instant-Messaging-and-P2P-Vulnerabilities-for-Health-Organizations&id=232800

Scovare e capire i Rootkit
http://www.buanzo.com.ar/sec/Rootkits.html

Application Layer Packet Classifier for Linux
http://l7-filter.sourceforge.net/

Dispositivi di rete:

N1. Server e telefoni VoIP

N1.1 Descrizione

L'utilizzo delle tecnologie VoIP ha continuato a diffondersi anche corso dell'anno appena concluso. Guidati dal desiderio di adottare rapidamente la tecnologia VoIP per sfruttarne gli indubbi vantaggi economici, molti hanno un po' trascurato, o addirittura del tutto ignorato, gli aspetti di sicurezza. Possono infatti essere presenti vulnerabilità in tutta l'infrastruttura di rete VoIP, nei call proxy mal gestiti o privi di patch, nei media server, negli stessi telefoni VoIP. Sono state individuate vulnerabilità in prodotti come Cisco Unified Call Manager e Asterisk, oltre che in telefoni VoIP di numerosi produttori. Facendo leva quelle vulnerabilità, gli aggressori possono eseguire attacchi di phishing VoIP, di *eavesdropping*, di frodi tariffarie o di denial-of-service. Installazioni mal progettate possono aprire la via verso i dati presenti nelle reti: i ricercatori continuano a scoprire nuove aree potenzialmente attaccabili, come nel caso del cross site scripting attraverso i client VoIP

Siccome molti server VoIP - specialmente quelli presso i service provider VoIP - sono una interfaccia tra SS7 (la segnalazione telefonica tradizionale) e le reti IP, un attaccante in grado di compromettere uno server VoIP vulnerabile potrebbe potenzialmente manipolare la segnalazione SS7 e interrompere i servizi di interconnessione per la Public Switched Telephone Network (PSTN), ovvero la tradizionale linea telefonica.

N1.2 Riferimenti CVE

Asterisk
CVE-2007-1594, CVE-2007-1561

Cisco Call Manager
CVE-2006-5277

Telefoni VoIP
CVE-2007-4459, CVE-2007-2512, CVE-2007-3047, CVE-2007-2270, CVE-2006-7121, CVE-2007-0431, CVE-2006-6411, CVE-2006-5233, CVE-2006-5231, CVE-2006-5038

Avaya
CVE-2007-5556

Cisco IOS
CVE-2007-4291

N1.3 Come affrontare le vulnerabilità del VoIP

- Prendere in considerazione le istanze di sicurezza come parte integrante di qualsiasi installazione VoIP. Ulteriori cautele possono essere necessarie nella fase della selezione dei prodotti da utilizzare, scegliendo quei dispositivi per i quali sia garantita dai fornitori un adeguato supporto nell'applicazione delle patch del sistema operativo non appena queste vengono rilasciate. Molti fornitori di VoIP non forniscono supporto nel caso di patch che loro non hanno ancora approvato e tale approvazione può richiedere parecchio tempo,
- Applicate le patch fornite dal produttore ai server VoIP e al software/firmware del telefono non appena queste diventano disponibili.
- Assicuratevi che i sistemi operativi che girano sui server VoIP abbia installate le patch più recenti, sia quelle rilasciate dal produttore del sistema operativo, sia quelle del prodotto VoIP.
- Effettuate scansioni del server e dei telefoni VoIP per rilevare le porte aperte. Nel firewall chiudete l'accesso da Internet a tutte le porte non necessarie alle operazioni dell'infrastruttura VoIP.
- Utilizzare un firewall che gestisca il protocollo VoIP o un prodotto di Intrusion Prevention per controllare che tutte le porte UDP sui telefoni VoIP non siano aperte alle comunicazioni internet RTP/RTCP.
- Disabilitare sui telefoni e sui server tutti i servizi non indispensabili (telnet, http ecc.)
- Considerate per i vari componenti VoIP l'uso di strumenti specifici come OULU SIP PROTOS Suite per garantire l'integrità dello stack del protocollo VoIP.
- Usate VLAN separate per la vostra rete dati e la rete voce, se la vostra infrastruttura di rete lo permette. Controllate che i server TFTP e DHCP VoIP siano separati dalla vostra rete dati.

- Cambiate la password di default per il login nel pannello di amministrazione di telefoni e proxy.
- Assicuratevi che la VLAN VoIP non possa essere utilizzata in modo tale da poter accedere ad altri servizi critici, come può accedere in caso di VLAN propagate in sedi diverse con qualche macchina come un Call Manager *dual homed*..

N1.4 Approfondimenti

Avvisi di sicurezza per Asterisk
http://www.asterisk.org/security

Avvisi di sicurezza Cisco
http://www.cisco.com/en/US/products/products_security_advisories_listing.html

VoIP Security Alliance
http://www.voipsa.org

NIST 800-58: Considerazioni sulla sicurezza dei sistemi VoIP
http://csrc.nist.gov/publications/nistpubs/800-58/SP800-58-final.pdf

Attacchi Zero Day

Z1: Attacchi Zero Day

Z1.1 Descrizione

Una vulnerabilità zero day si verifica quando un difetto nel codice nel software viene scoperto e sfruttato prima che sia disponibile una patch. Una volta diffuso un exploit funzionante della vulnerabilità, gli utenti del software interessato sono inermi fino a quando non è disponibile una patch o fino a quando non viene adottata una qualche forma di contromisura da parte dell'utente. Nel 2007 si sono registrati numerosi attacchi zero day, quasi il doppio rispetto all'anno precedente. I passi da seguire per mitigare il pericolo e proteggersi da tale minaccia verranno indicati nel corso di questa sezione.

Z1.2. Sistemi operativi interessati

Per tutti i sistemi operativi e per tutte le applicazioni software è possibile scoprire ed eventualmente sfruttare una vulnerabilità zero day.

Z1.3. Riferimenti CVE

Lo scorso anno numerose vulnerabilità sono state sfruttate prima che fosse messa in circolazione una patch ufficiale o studiato un rimedio. Alcuni esempi di voci CVE che riflettono questa tendenza sono:

- Correttore grammaticale Brasiliano Portoghese di Microsoft Office 2003 CVE-2006-5574
- Microsoft Word CVE-2006-6456
- Microsoft Word CVE-2006-6561
- Microsoft Word CVE-2006-5994
- Microsoft Word CVE-2007-0515
- Windows Graphics Rendering Engine (ANI) CVE-2007-0038
- Windows DNS Server CVE-2007-1748
- Adobe Acrobat Reader plug-in CVE-2007-0045
- RealPlayer CVE-2007-5601
- Computer Associates BrightStor CVE-2007-1785

Z1.4. Come proteggersi da queste vulnerabilità

La protezione contro lo sfruttamento delle vulnerabilità zero day è una questione di grande preoccupazione per la maggior parte degli amministratori di sistema. Per ridurre la pericolosità degli attacchi zero day, è opportuno seguire alcune *best practice* quali:

- Adottare una posizione *deny-all* sui firewall e sui dispositivi perimetrali che proteggono le reti interne
- Separare i server con affaccio pubblico dai sistemi interni
- Disattivare i servizi non necessari e rimuovere le applicazioni che non siano richieste da esigenze operative
- Seguire il principio del minimo privilegio possibile nell'impostazione dei controlli di accesso, dei permessi e dei diritti degli utenti
- Impedire o limitare nei browser l'uso di codice attivo come Java script o ActiveX
- Sensibilizzare gli utenti in merito ai rischi connessi all'apertura di file allegati non richiesti
- Disabilitate la possibilità di seguire i link presenti nei messaggi di posta elettronica
- Disabilitate la possibilità di scaricare automaticamente le immagini da Web nei messaggi di posta elettronica
- Gestire internamente (o, se necessario affidare all'esterno) un servizio di gestione degli allarmi e degli avvisi di sicurezza rapido ed efficiente per essere certi di venire a conoscenza degli exploit zero-day exploit non appena diventano pubblici
- Utilizzare soluzioni di gestione end-point per rendere più rapida la distribuzione di patch o di soluzioni alternative appena queste si rendono disponibili
- Qualora si utilizzi Microsoft Active Directory, trarre il massimo vantaggio dai Group Policy Objects per controllare gli accessi degli utenti

- Non fare affidamento esclusivamente sulla protezione di un antivirus, in quanto gli attacchi zero-day spesso non si possono scoprire fino a quando non vengono rilasciate le nuove firme
- Quando possibile, utilizzare su tutti i sistemi protezioni da buffer overflow di terze parti
- Seguire le raccomandazioni dei produttori sulle soluzioni alternative e sulle strategie per la riduzione del rischio fino a quando diventa disponibile una patch

Gli esperti che hanno contribuito a creare la lista Top-20 del 2007

Direttore del progetto: Rohit Dhamankar, TippingPoint, a division of 3Com
Adam Safier, Global Systems & Strategies, Inc.
Alan Rouse, Security Architect, TANDBERG Television
Alan Paller, Director, SANS Institute
Alexander Kotkov, UBS Investment Bank
Amol Sarwate, Manager of Vulnerability Lab, Qualys
Andrew van der Stock, Director, OWASP
Anton Chuvakin, Director of Product Management @ LogLogic
Anthony Richardson, Monash University, Australia
Arturo "Buanzo" Busleiman - Consultor Independiente en Seguridad, Argentina
Cesar Tascon Alvarez, Deloitte, Spain
Christopher Rowe, Elon University
Craig Wright, BDO Kendalls, Australia
Dean Farrington
Donald Smith, Qwest
Ed Fisher, Ingersoll Rand
Edward Ray, Getronics
Gerhard Eschelbeck, CTO, Webroot
Giuseppe Gottardi, Senior Security Engineer, Communication Valley S.p.a, Italy
Jean-Francois Legault, Deloitte & Touche LLP
Jeff Pike, Integrated Team Solutions Facility
Jeremian Grossman, OWASP
John-Thomas Gaietto
John Tannahill, J.Tannahill & Associates
Johannes Ullrich, Internet Storm Center, SANS
Jonathan Rubin, Dominion
Kevin Hong
Koon Yaw Tan, Monetary Authority of Singapore
Leo Pastor, Advanced Consulting and Training, Argentina and Brazil
Marcos A. Ferreira Jr., NX Security, Brazil
Marcus Sachs, SRI International and Internet Storm Center, SANS
Matteo Shea, Senior Security Engineer, Communication Valley S.p.a, Italy
Michel Cusin, Bell Canada
Michele Guel, Cisco Systems
Miguel Guirao A, Telcel
Naoshi Matsushita, NRI Secure Technologies
Olivier Devaux, Webroot
Pedro Bueno - McAfee AvertLabs and SANS Internet Storm Center
Ralf Durkee, Security Consultant
Rhodri Davies, Vistorm, UK
Rick Wanner, Technical Analyst, Corporate Security, SaskTel
Rob King, TippingPoint, a division of 3Com
Russ McRee, HolisticInfosec.org
Sandeep Dhameja, Ambiron Trustwave
Syed Mohamed, Microland Ltd.
Tom Hallewell, Radio Free Asia

Agenzie

Department of Homeland Security (DHS)
Computer Emergency Response Team (CERT)
National Infrastructure Security Coordination Centre (NISCC, UK)
Computer Emergency Response Team, Canada

Hanno collaborato alla localizzazione italiana della SANS Top 20

Luca Springolo, Data Security
Simone Brun, Data Security

Best Practice per prevenire i rischi Top 20

1. Configurare il sistema, fin dal primo giorno, con la configurazione più sicura possibile tra quelle che consentono la funzionalità del vostro business e utilizzare funzioni automatiche per prevenire l'installazione o la disinstallazione di software da parte degli utenti.
2. Utilizzare funzioni automatizzate per controllare che il sistema mantenga una configurazione sicura, sia sempre aggiornato all'ultima versione e con tutte le patch più recenti (e questo significa mantenere sempre aggiornato anche il software antivirus).
3. Utilizzate dei proxy sul perimetro di rete, configurando tutti i servizi client (HTTP, HTTPS, FTP, DNS, ecc.) in modo che debbano passare per i proxy prima di uscire su Internet.
4. Proteggere i dati riservati tramite la crittografia, utilizzando un controllo degli accessi granulare a seconda della tipologia e della criticità delle informazioni, avvalendosi anche di strumenti automatizzati di protezione contro la perdita dei dati
5. Puntare sulla consapevolezza degli utenti e prevedere delle sanzioni chi non rispetta le policy.
6. Tramite i firewall, implementare una adeguata segmentazione DMZ
7. Rimuovete le falle di sicurezza dalle applicazioni web, verificando le conoscenze di sicurezza dei programmatori e analizzando i software alla ricerca delle vulnerabilità.

Le FAQ sui rischi per la sicurezza SANS Top-20 2007

Di Rohit Dhamankar, Direttore del progetto

Per chi è stata scritta la lista?

Negli ultimi anni mi è diventato chiaro che la lista SANS Top 20 è utilizzata da organizzazioni molto diverse tra loro. Alcune organizzazioni di grandi dimensioni utilizzano la lista Top-20 per ricontrollare le loro attività intraprese nel miglioramento della sicurezza, mentre alcune organizzazioni più piccole usano questa lista come strumento esclusivo per guidare tutta la loro attività di rimozione e prevenzione delle vulnerabilità. Così, mentre creavamo la lista abbiamo cercato di servire le due diverse platee.

É ancora rilevante, nel 2007, pubblicare un documento con le peggiori vulnerabilità dell'anno?

Alla luce delle considerazioni che seguono, la risposta non può che essere positiva.

- La scansione dei dati su Internet dimostra che ci sono ancora sistemi affacciati su Internet senza le patch per vulnerabilità che sono state ampiamente sfruttate. Personalmente non ho intenzione di smettere di lavorare a questo progetto fino a quando vedrò un qualsiasi worm come Blaster o Slammer generare un evento in un IDS/IPS nella rete di un cliente.
- Anche se tutte le patch fossero applicate, bisognerebbe vederla ancora con le minacce zero-day! La lista di quest'anno include una serie di difese per le minacce zero-day.
- I professionisti della sicurezza sono così concentrati sulla "sfida del giorno" da aver sempre bisogno di promemoria sulle minacce di volta in volta emergenti, in modo che possano cercare risorse per la lotta contro i nuovi pericoli

Perché la lista si chiama Top 20 quando il numero di vulnerabilità attuale (CVE) è di molto superiore a 20?

- La vita potrebbe essere molto più semplice se si potesse creare una lista di 20 voci CVE critiche e poi sostenere che la protezione contro gli attacchi che sfruttano quelle venti vulnerabilità renderebbe Internet sicuro. La realtà, lo sappiamo, è molto diversa. Se solo uno prendesse gli attacchi settimanali alle vulnerabilità delle applicazioni Web rilevate l'anno scorso, vedrebbe che il numero di vulnerabilità critiche è già superiore a 100! Questo è il numero di vulnerabilità che deriva da centinaia di migliaia di tentativi di attacchi sul web ogni giorno. L'approccio della top 20 è quello di aiutare a focalizzare l'attenzione sulle "classi" di vulnerabilità che vengono sfruttate, e fornire una guida per amministratori di sistema, programmatori e manager su come mitigare ciascuna classe di vulnerabilità.

- La Top 20 raggruppa le vulnerabilità critiche in classi in modo che si possano applicare strategie comuni per la protezione di un intera classe. Per esempio, un largo numero di overflow MS-RPC può essere prevenuto bloccando le porte 139/tcp e 445/tcp sul perimetro di rete.
- La Top 20 aiuta inoltre ad identificare i vettori di diffusione utilizzati da un ampio numero di malware. È triste notare come nel 2007 accada che i malware si diffondano con successo sulle reti usando password identificate con attacchi brute-force!
- Abbiamo mantenuto il nome "Top-20" per conservare la tradizione di un marchio che identifica la continuità del lavoro portato avanti in questo progetto.

Per qualsiasi commento, scrivete a top20@sans.org