Sicurezza ICT

Introduzione alla sicurezza ICT

- La sicurezza è una tematica complessa e articolata che per semplificazione possiamo definire fornendo la risposta alle seguenti domande:
  - Cosa vuol dire “sicuro” in ICT ?
  - Cosa bisogna proteggere ?
  - Contro cosa bisogna proteggere ?
  - Come ci deve proteggere ?
  - Quanto bisogna proteggere ?

Sicurezza ICT

- **Disciplina che attraverso vari processi, azioni, procedure, consente di trattare informazioni e risorse informatiche in modo appropriato in relazione a obiettivi riferiti ai seguenti concetti base:**
  - **Riservatezza**
  - **Integrità**
  - **Disponibilità**
  - **Autenticità**
  - **Non ripudio**

Concetti base della sicurezza

1. RISERVATEZZA: informazioni e risorse devono essere accessibili esclusivamente a coloro che ne sono i legittimi fruitori;
2. INTEGRITA': informazioni e risorse non devono essere modificabili (alterabili) da chi non ne ha diritto;
3. DISPONIBILITA': Gli utenti devono poter accedere e fruire di informazioni e risorse di cui hanno legittimamente bisogno e quando ne hanno l'esigenza;

Concetti base della sicurezza

4. **AUTENTICITA’: E’ necessario poter sempre attribuire in modo certo e univoco una azione, un documento, un messaggio, a colui che ne è il vero autore;**

5. **NON RIPUDIO: E’ necessario impedire il disconoscimento di una azione, di un messaggio o di un documento, da parte dell’autore.**

Scenario di riferimento

Interne ed esterne alla organizzazione

MINACCE

Sfruttano le vulnerabilità presenti per recare danno all'organizzazione ed in particolare alle informazioni

Insieme delle persone, utenti, dei dati, delle procedure e del sistema IT (Assett)

ORGANIZZAZIONE

INFORMAZIONI

strategia di sicurezza

Vengono intraprese una serie di misure a vari livelli volti a mitigare i rischi dell'accadimento di un evento o incidente di sicurezza e a ridurre le vulnerabilità aumentando il livello di sicurezza

Le misure hanno un costo

MISURE

Riduzione del rischio

RISCHI

Diritto e sicurezza informatica

Tante problematiche diverse, tra loro connesse, a rapida evoluzione nel tempo, definiscono un quadro di problematiche tradizionali o si presentano come nuove

- **Crimini informatici**
- **Controllo del lavoratore**
- **Diritti d'autore ed editoria**
- **Amministrazione digitale**
- **Tutela dei dati**
- **Commercio elettronico**
- **Tutela segni distintivi (brand, logo)**
- **Concorrenza sleale**
- **…**

Obiettivi di sicurezza

- **Gli obiettivi di sicurezza sono ciò che ci si prefigge di ottenere per i propri *beni* in termini di *riservatezza, integrità, disponibilità*, etc.**

- **Proteggere un bene significa raggiungere un adeguato livello di *riservatezza, integrità, disponibilità*, etc.**

- **Tale livello è *l'obiettivo di sicurezza* per quel bene.**

Minacce

- Una minaccia è qualsiasi azione, accidentale o deliberata, che potrebbe comportare la violazione di qualche obiettivo di sicurezza;
- Una minaccia dipende sempre da un fattore esterno al sistema che può essere di origine naturale o antropica;
- ESEMPI:
  - Attacco «Hacker»: minaccia deliberata di origine antropica;
  - Smarrimento password: minaccia accidentale di origine antropica.

Vulnerabilità

- **Una vulnerabilità è una debolezza intrinseca di un sistema informatico;**
- **A differenza delle minacce non dipende da agenti esterni ma è una proprietà del sistema stesso;**
- **Se un agente esterno attua una *minaccia* che sfrutta una *vulnerabilità* si ha una violazione di un *obiettivo di sicurezza*;**
- **ESEMPI:**
  - **Errori di progettazione**

Rischio

- Il rischio è il prodotto di due fattori:
  - La probabilità che un evento dannoso si possa verificare;
  - L'impatto (nel senso delle conseguenze) che l'evento dannoso avrebbe sul sistema se si verificasse;

- RISCHIO=PROBABILITA'x IMPATTO

- Il rischio deve essere gestito attraverso azioni mirate a ridurre uno o entrambi i fattori che lo costituiscono.

Contromisure

- Le contromisure di sicurezza sono le scelte progettuali, le azioni, gli accorgimenti, finalizzati a:
  - limitare le vulnerabilità
  - fronteggiare le minacce

- Le contromisure possono essere di vari tipi:
  - fisiche (es. chiudo la sala server)
  - procedurali (politica di aggiornamento del SW)
  - tecniche (sistemi Hardware/software/firmware)

Costo della sicurezza

- Le contromisure hanno un costo, proprio come il verificarsi di un evento dannoso;
- Il costo delle contromisure deve essere proporzionato al valore del bene da proteggere e ai rischi connessi;
- Non è possibile annullare completamente un rischio (costo infinito);
- Occorre stabilire il livello di rischio che è accettabile conservare: compromesso tra contromisure e rischio residuo;

Business Continuity

- Qualsiasi organizzazione o azienda ha nella propria attività la ragione della propria esistenza;
- E' necessario garantire la continuità di tale attività anche in caso di attacchi o disastri;
- La BUSINESS CONTINUTY è l'insieme delle attività necessarie per garantire un adeguato livello di operatività alla propria organizzazione in caso di anomalie o interruzione delle normali funzionalità;
- Si definisce DISASTER RECOVERY il processo di ricostruzione dei propri dati, sistemi o infrastrutture a seguito di un evento dannoso.

Riservatezza

- **Obiettivo:** impedire che dati e risorse possano essere visibili e accessibili a sistemi o persone non autorizzate;
- **Rischio:** persone estranee possono leggere un messaggio;
- **Vulnerabilità:** le informazioni viaggiano apertamente sul mezzo trasmissivo;
- **Contromisure:** Crittografia;

Integrità

- **Obiettivo:** garantire che i dati che giungono al destinatario siano esattamente quelli trasmessi dal mittente, evitando o rendendo manifesti tentativi di alterazione;
- **Rischio:** un malintenzionato potrebbe alterare un messaggio o un documento;
- **Vulnerabilità:** il destinatario non conosce il documento originale;
- **Contromisure:** funzioni di HASH.

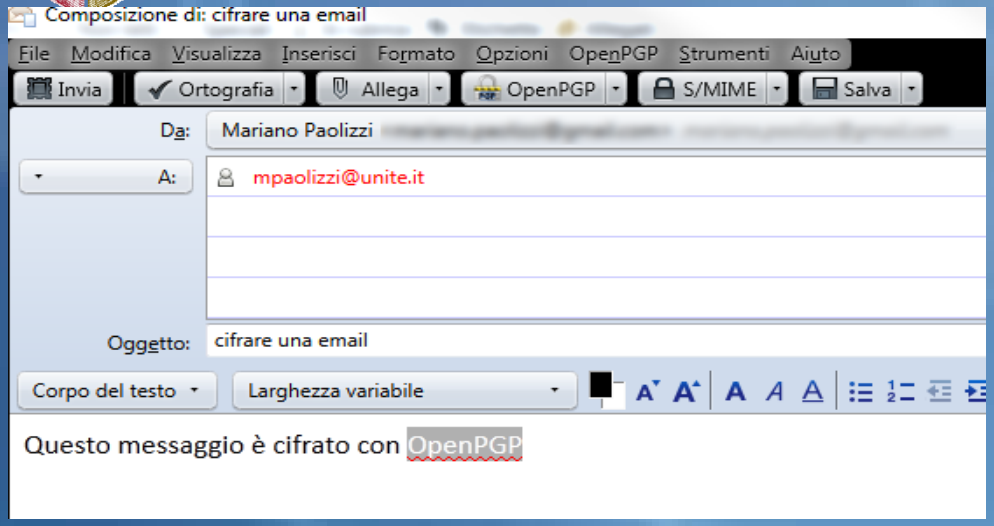
Funzioni di Hash

- Una funzione di hash produce una sequenza di caratteri di lunghezza fissa a partire da un qualsiasi messaggio;
- Tale sequenza dipende in maniera (quasi) univoca dal messaggio stesso di cui costituisce una IMPRONTA (digest);
- Dall'impronta non è possibile risalire al messaggio ed è (quasi) impossibile che due messaggi diversi abbiano la stessa impronta;
- Una piccola modifica al messaggio comporta una grossa modifica all'impronta.

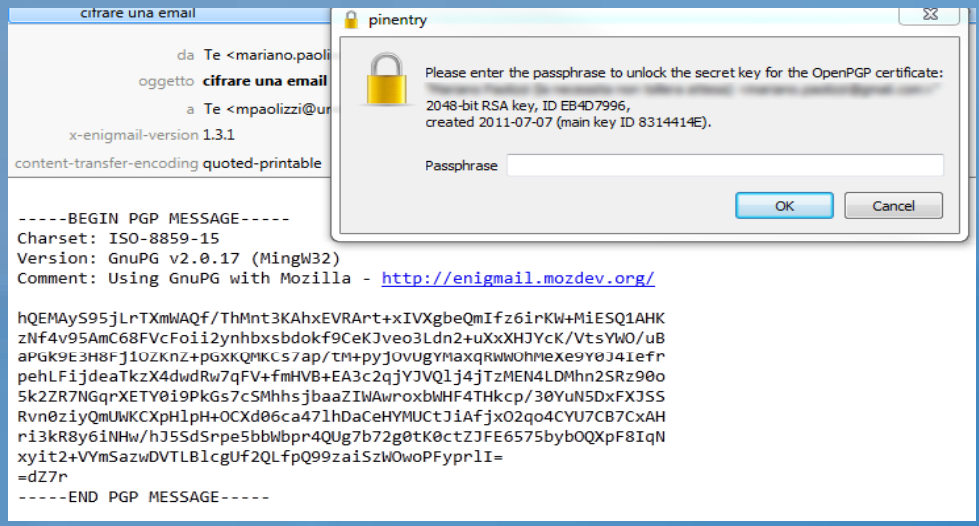
Funzioni di Hash

- Per garantire la integrità:
  - il mittente
    - Scrive il messaggio e ne calcola la impronta
    - Invia messaggio e impronta
  - il ricevente
    - Riceve messaggio e impronta
    - Calcola l'impronta del messaggio ricevuto
    - Confronta la impronta calcolata con quella ricevuta: se coincidono è altissima la probabilità che il messaggio sia integro

ESEMPI



Messaggio email in chiaro



Messaggio email cifrato

Name:	BT5R1-GNOME-64.iso
Size:	2031
Flavor:	GNOME
Arch:	64
Image:	ISO
Download:	Direct
MD5:	13b6bc940a34274675278fd14506a5d2

Hash del file «BT5R1-GNOME-64.iso»

Autenticità e non ripudio

- **Obiettivo:** essere sicuri che un messaggio o un documento provenga da chi ne crediamo l'autore ed impedire che questi possa disconoscerlo;
- **Rischio:** accettare erroneamente un documento come proveniente da un mittente fidato;
- **Vulnerabilità:** Il messaggio non è "firmato";
- **Contromisure:** Firma Digitale.

Firma Digitale

- La firma digitale è una sequenza di byte che associa in modo univoco un documento elettronico all'autore;
- Un documento informatico sottoscritto con firma digitale ha il valore previsto dall'art.2702 del Codice Civile (D.Lgs. N.82 del 07/03/2005 e s.m.i.);
- Si tratta, quindi, dello strumento per eseguire transazioni o stipulare contratti elettronici.

Disponibilità

- **Obiettivo:** garantire “sempre” la fruizione di dati e risorse ai legittimi utenti;
- **Rischio:** una catastrofe naturale o un attacco doloso potrebbero compromettere i dati;
- **Vulnerabilità:** si dispone di una unica copia dei dati in una struttura priva di protezioni;
- **Contromisure:** backup e ridondanza, protezione tecnica da attacchi e codice maligno.

Diritto e sicurezza informatica

SICUREZZA DELLE INFORMAZIONI - NORMATIVE

STANDARD

BS7799

ISO1799

Common Criteria

Linee guida CNIPA

Linee guida NIST, OCSE,…

LEGISLAZIONE

Alcune grandi tematiche:

- Crimini informatici
- Controllo del lavoratore
- Diritti d’autore ed editoria
- Amministrazione digitale
- Tutela dei dati
- Commercio elettronico
- Tutela segni distintivi (brand, logo)
- …

Protezione dei dati personali

Normativa in vigore: Decreto Legislativo 30 giugno 2003 n.196 - "Codice in materia di protezione dei dati personali"

Sostituisce il 675/96 riunendo in un testo unico le disposizioni di legge, normative, regolamenti, codici deontologici emanati nel passati e prendendo in considerazione i provvedimenti del Garante e le Direttive Europee sulla materia.

E' entrato in vigore dal 01/01/04, l'adozione delle misure minime di sicurezza è stata più volte rimandata fino alla data ultima del 31/03/2006.

Un ruolo molto importante è stato assegnato all'Autorità Garante per la privacy

Principali minacce

Le minacce che possono insistere sull'infrastruttura tecnologica di una organizzazione sono molteplici. Le principali sono le seguenti:

- di natura software (malware)
  - Virus e worm
  - Trojan horse, spyware, keylogger, dialer
- Intrusione nei sistemi informativi da interno e da esterno
- Interruzione del servizio (Denial of Service)
- Truffa
- Social Engineering
- Phishing e Vishing
- …molte altre (es. furto, violazione del copyright,…)

Malware – virus e worm

Un malware è un qualsiasi software creato con il solo scopo di causare danni più o meno estesi al computer su cui viene eseguito.

Il termine deriva dalla contrazione delle parole inglesi malicious e software (codice maligno)

I malware tradizionalmente più famosi sono:

- **Virus**: particolare software, appartenente alla categoria dei malware, in grado, una volta eseguito, di infettare dei file in modo da riprodursi facendo copie di se stesso, senza farsi rilevare dall'utente. I virus possono essere più o meno dannosi per il sistema operativo che li ospita, ma anche nel caso migliore comportano un certo spreco di risorse in termini di RAM, CPU e spazio sul disco fisso.
- **Worm**: un worm, letteralmente verme, è una particolare categoria di malware in grado di autoreplicarsi. È simile ad un virus, ma a differenza di questo non necessita di legarsi ad altri files eseguibili per diffondersi

Malware - Trojan horse

Un Trojan Horse è un malware che al momento dell'esecuzione si maschera in modo da sembrare qualcos'altro.

Anche se può pubblicizzare la propria attività dopo l'avvio, questa informazione non è visibile all'utente prima dell'esecuzione.

Il Trojan Horse non replica né copia se stesso ma danneggia o compromette la sicurezza del computer.

Un Trojan Horse può essere inviato o trasportato da un altro programma e può arrivare nella forma di programma burla o applicazione di altro tipo.

Le attività nocive di un Trojan Horse sono indesiderabili per qualsiasi utente informatico poiché comprendono la distruzione dei dati o compromissione del sistema e consentono l'accesso ad altri computer scavalcando i normali controlli di accesso.

Spyware

Uno spyware è un tipo di software che raccoglie informazioni riguardanti l'attività online di un utente (siti visitati, acquisti eseguiti in rete etc) senza il suo consenso, trasmettendole tramite Internet ad un'organizzazione che le utilizzerà per trarne profitto, tipicamente attraverso l'invio di pubblicità mirata.

Gli spyware costituiscono una minaccia per la privacy dell'utente

- carpiscono senza autorizzazione informazioni sul suo comportamento quando connesso ad Internet
- Le informazioni raccolte vengono inviate ad un computer remoto che provvede ad inviare pubblicità mirata sulle preferenze ricavate dall'analisi del comportamento di navigazione
  - Pop-up
  - Banner
  - Spam

Phishing / Vishing

Il phishing è una tecnica rivolta a carpire in maniera ingannevole dati relativi alle carte di credito.

La tecnica si basa sulla realizzazione di un sito web molto simile ad un sito ufficiale di una banca o di altra organizzazione dove vengono attirati gli utenti attraverso delle comunicazioni ingannevoli (via posta elettronica o alterazione di un contenuto di un sito web ufficiale).

Gli utenti, credendo di accedere ad un sito ufficiale, immettono i dati richiesti (in genere relativi alla carta di credito o che consentono l'accesso al proprio conto corrente on-line).

I dati vengono memorizzati e vengono poi utilizzati dai truffatori.

Il vishing è una tecnica simile con la differenza che si usa una comunicazione telefonica e quindi tutte le tecniche tipiche del "social engineering" per ingannare l'utente.

E' un fenomeno che si sta diffondendo moltissimo per via dell'abbattimento del costo delle chiamate.

Intrusione/DoS

Le tecniche di intrusione (tradizionalmente hacking) sono numerose e complesse.

Un hacker generalmente utilizza numerose tecniche per introdursi all'interno di un sistema.

Le intrusioni possono originarsi sia dall'interno dell'organizzazione sia dall'esterno e possono utilizzare vulnerabilità presenti su vari dispositivi (server, apparati di comunicazione, PC,..)

Il Denial of Service è una tecnica usata dagli hacker per rendere inservibili i principali sistemi IT di una organizzazione.

Le tecniche di DoS mirano quindi ad interrompere il servizio sovraccaricando la rete ed i server

Una new entry: lo Scareware

- Lo scareware è una recente forma di malware apparsa su Internet;
- Si tratta di un codice malevolo in grado di imitare gli alert dei browser più diffusi per implementare una forma ingannevole di Web marketing;

- Lo scopo è quello di spaventare gli utenti, paventando il rinvenimento di file pericolosi o infetti sul PC, allo scopo di indurli all'acquisto e all'installazione del software millantato quale soluzione al problema.
- E' opportuno diffidare di messaggi che compaiono durante la navigazione Internet ed invitano ad installare software o plug-in che renderebbero più sicuro il PC in uso.

Vulnerabilità

Le minacce precedentemente elencate sfruttano delle vulnerabilità presenti nei sistemi IT.

Una vulnerabilità è la debolezza di un determinato asset che può essere sfruttata da una minaccia potenziale.

Analogamente alle minacce anche le vulnerabilità sono di varie tipologie ed evolvono nel tempo.

A differenza delle minacce, la gran parte delle vulnerabilità di una organizzazione sono poco note.

Infatti oltre a quelle più comuni, una parte di queste possono essere scoperte o analizzate solamente se precedentemente all'inizio dell'analisi del rischio viene effettuata un auditing accurato

Vulnerabilità WWW

Le più comuni vulnerabilità del servizio WWW sono le seguenti:

- Lacune o bug presenti nel software che implementa le funzionalità di server web
- Lacune o bug presenti nel software che implementa le funzionalità di browser
- Possibilità di far richiedere dal server web al client l'attivazione di script o di codice eseguito direttamente sul PC dell'utente
- Possibilità di far comunicare all'utente informazioni circa la propria navigazione web (es. attraverso "cookies")
- Redirezione ingannevole delle richieste del client su server web distinti e non controllati
- Possibilità di presentare all'utente di servizi web simili ad altri o copie esatte (es. Phishing)

Misure minime del D.lgs 196/03

Misure minime per trattamenti con strumenti informatici:

- **Autenticazione informatica: misure principalmente tecnologica**
- **Adozione di procedure di gestione delle credenziali di autenticazione: misure tecnologica e organizzativa**
- **Utilizzazione di un sistema di autorizzazione: misura tecnologica e organizzativa**
- **Aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici: misura organizzativa**
- **Protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici: misura a prevalenza tecnologica**
- **Adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi: misura tecnologica e organizzativa**
- **Tenuta di un aggiornato documento programmatico sulla sicurezza: misura organizzativa**
- **Adozione di tecniche di cifratura o di codici identificativi per determinati trattamenti di dati idonei a rivelare lo stato di salute o la vita sessuale effettuati da organismi sanitari: misura tecnologica**

Tecniche di protezione

Alcune delle principali tecniche di protezione con associati tool di monitoraggio sono i seguenti:

- Autenticazione
- Antivirus e antispyware
- Antispam
- Content filtering
- Patching
- Firewall

Non sottovalutiamo le minacce…

27.4.2011

Attacco hacker alle Playstation

Rubati i dati di 77 mln di utenti

29/04/2011 09:50

FOTO UFFICIO STAMPA

00:22 - Il blocco del network di quanti giocano … solo l'awisaglia di un problema più grande. Sony … hanno rubato i dati personali di 77 milioni di abbona… l'azienda nipponica sono stati trafugati oltre a i nomi de… le email, le date di nascita, gli username e le password. … escluso la perdita anche dei dati delle carte di credito

Un pirata informatico, definito dall'azienda giapponese come "pr… autorizzata", è riuscito a impossessarsi dei dati personali, nomi, in… codici di avviamento postale, password, e-mail, storia dei pagamenti … bollette, e perfino delle date di nascita dei 77 milioni di persone, tanti so… clienti registrati a questa piattaforma.

Da qui la scelta dello spegnimento la scorsa settimana di ogni attività'. Secondo il comunicato, sinora non ci sarebbe la prova evidente che l'hacker abbia gia' 'rubato' anche tutti i dati riferibili alle carte di credito. Ma si tratta di una evenienza che per ora non si puo' escludere del tutto.

"Al momento - si legge nella nota della Sony - la prudenza è d'obbligo, per cui dobbiamo avvertire tutti che è possibile che l'hacker abbia ottenuto i numeri delle carte di credito e la data di scadenza, ma non il codice di sicurezza".

La casa giapponese, informa il Wall Street Journal, ha già incaricato una grande … informatica di mettersi al lavoro per avviare le indagini su quanto è … il servizio di queste console entro la settimana … internet possono giocare …

Server Aruba fermi a causa di un incendio (update 6)

Un principio di incendio in una server farm Aruba ha portato allo spegnimento dei server con conseguenti disservizi per siti web, email ed altri servizi.

Giacomo Dotta

lunedì 27 settembre 2010 — di *Alfonso Maruccia*

Commenti (76)

Stuxnet, il worm all'assalto del nuclear… iraniano

Esperti di sicurezza presi in contropiede, altissimo livello di sofisticaz… obiettivo apparentemente ben definito sono gli ingredienti dell'affa… …va superstar del variopinto bestiario del malware

…e già ampiamente previsto qualche mese fa, il worm Stuxnet … diatico" capace di impensierire le società di sicurezza e … mainstream, generalmente poco accorta alla prolife… …levolo. Ma Stuxnet fa molto, molto di più oltr… …che da far sorgere più di un dubbio sul … **…o contro il programma nucleare ir…**

Ci sare… servizi segreti israeliani … …ato in …a ma individuato dalla … …o. Il wor… …a di sicurezza, rappresente… …reti di cybe… con lo scopo preordinato di fare da…

…net è un pezzo di … …e estremamente compl… …ano di caratteri… …anzate, …o gli esperti, un malware che … …ace …0 day d… …indows, …delle quali ben… …da più di

La Difesa Usa è in allarme, un virus informatico ha infettato il sistema che controlla i droni

Un virus informatico ha "infettato" i computer della centro operativo dei droni Predator e Reaper, comprendo ogni volta che gli operatori premono i tasti dei computer e altre zone di guerra. A darne notizia è stata la rivista aerei senza pilota impiegati in missioni in Afghanistan e altre zone di guerra. A darne notizia è stata la rivista tecnologica americana Wired, aggiungendo che il virus è stato scoperto un paio di settimane fa dai tecnici della sicurezza della base aerea di Creech, situata nel Nevada, ma finora non ha impedito lo svolgimento delle missioni, né ci sono state al momento indicazioni di fughe di informazioni.

Un altro caso di phishing Poste Italiane

Ringraziamo un nostro gentile lettore che ci ha inviato un caso di phishing ai danni dei clienti dei servizi finanziari di Poste Italiane.

L' e-mail invita l'utente a collegarsi ad un link per verificare il conto che avrebbe subito ripetuti tentativi di accesso; per rendere più veritiera l'e-mail elenca anche alcuni indirizzi IP (ovviamente inventati anch'essi) da cui sarebbero avvenuti i tentativi di accesso.

Come sempre riportiamo il testo integrale dell'e-mail e, a seguire, l'indirizzo internet truffaldino.

Questa E-Mail è Phishing

Posteitaliane

Poste Italiane Caro cliente,

Durante il nostro calendario regolarmente la manutenzione e la verifica che abbiamo rilevato un lieve errore e le informazioni per la fatturazione su file con Poste Italiane.

Ciò potrebbe essere dovuto ad una delle seguenti ragioni:

-- Un recente cambiamento nelle vostre informazioni personali (ad esempio, cambio di indirizzo)
-- L'incapacità di verificare accuratamente selezionata di pagamento, uno errore interno all'interno dei nostri processori.

Recentemente abbiamo notato uno o più tentativi di accesso nel tuo conto Poste Italiane da un indirizzo IP estera e abbiamo ragione di credere che il tuo account e stato dirottato da un terzo senza la sua autorizzazione. Se hai recentemente l'accesso al tuo account mentre viaggia, il log dei [illegible] sopra potrebbe iniziata da voi. Tuttavia, [illegible] fare clic sul link qui sotto, come si prova a [illegible] account.

https://[illegible].poste.it

Corriere della Sera › Scienze › *«Exploit», il Lupin dei virus informatici*

OLTRE 70 MILIONI DI PC SONO GIA' STATI COLPITI E SONO STATI RUBATI DECINE DI MILIONI DI EURO

«Exploit», il Lupin dei virus informatici

Visitando dei siti infetti si rischia di scaricare un componente che s'impossesserà dei nostri dati personali

MILANO - Perché da un po' di tempo non assistiamo a un attacco di un virus informatico su scala? La risposta è semplice. L'attacco è già in corso anche se noi non ce ne rendiamo conto minaccia si chiama «exploit» un termine usato in informatica per identificare un metodo … sfruttando un bug o una vulnerabilità, porta all'acquisizione di privilegi o al denial of serv… computer. Il fenomeno «exploit» ha già infettato oltre 70 milioni di pc nel mondo, cent… migliaia solo in Italia (riferisce Grisoft, società di sicurezza informatica), ma fino ad or… diffuso solo su siti e riviste specializzate.

NUOVA GENERAZIONE - Come mai? Perché l'attuale forma assunta dall'«exploit» … una nuova generazione di attacchi in… virus attivi fino a 4-5 anni fa, che dis… o che bloccavano o cancellavano le … …che non opera secondo le modalità … …hard disk o d…

lunedì 13 febbraio 2012 — di *Alfonso Maruccia*

Commenti (0)

Bucato lo Store di Microsoft India

Il marketplace software di Redmond vittima dei cracker. Tutta colpa delle password salvate in chiaro. E sotto i colpi degli hacker ci finiscono pure i siti hard

Roma – Lo store indiano di Microsoft è stato "abbattuto" da un gruppo di cracker cinesi, i quali sono riusciti a entrare in possesso di tutte le credenziali di accesso degli utenti del sito per di più sbeffeggiando Redmond con il *defacing* della homepage e la pubblicazione, al suo posto, di una maschera di Guy Fawkes (quella del film e del fumetto "V per Vendetta").

La crew cinese responsabile dell'attacco si fa chiamare Evil Shadow Team, e ci ha tenuto a far sapere (sulla homepage deturpata dello store) che "i sistemi insicuri verranno battezzati". Nel caso specifico, è bene sottolinearlo, la responsabilità dell'accaduto non è di Microsoft ma dell'azienda Quasar Media che per Microsoft gestiva lo store.

E di responsabilità Quasar Media sembra parecchie, visto che a quando pare le credenziali di accesso rubate erano state archiviate come testo leggibile in chi… di un'operazione di cifratura. Al momento lo store … almeno sostituita da un messaggio che … possibile".

Facebook: 120 milioni di utenti rischiano di essere infettati dal virus Koobface

Autenticazione

Questa misura di sicurezza prevede che l'utente che accede alle risorse IT dell'organizzazione, dal PC all'applicativo, sia autenticato, ossia sia riconosciuto dal sistema attraverso opportune credenziali.

Le credenziali dell'utente sono in genere costituite da:

- Username
- Password

Queste informazioni sono conosciute dall'utente (ovviamente)

Sistemi di autenticazione più forti richiedono a volte anche qualcosa che sia posseduto dall'utente (es. smart card, token con certificato,...) oltre username e password.

Autenticazione

Nell'ambito dell'autenticazione si inserisce la gestione delle password di accesso ai sistemi IT che devono avere come requisiti le proprietà di essere:

- di almeno 8 caratteri contenenti sia lettere sia cifre sia simboli alfanumerici (!,*,#,@,...)
- cambiate frequentemente (almeno ogni 3/6 mesi)

Antivirus

Un antivirus è un sistema di protezione delle risorse IT dalla propagazione ed infestazione di virus informatici.

Può essere installato:

- **Localmente sui client in modalità stand-alone ossia ogni client è completamente autonomo nella gestione del proprio PC**
- **In maniera centralizzata nei nodi di interscambio dei dati quali ad esempio i sistemi di posta elettronica o di proxy web**
- **Localmente sui client con gestione però da un sistema centrale**

In genere quando si ha un sistema centralizzato Antivirus si riesce:

- **A gestire i client in maniera centralizzata**
- **A eseguire la scansione centralizzata della posta elettronica e del traffico passante attraverso i sistemi di proxy**

Antivirus

Il sistema antivirus possiede un database di firme (in inglese signatures) per il riconoscimento dei virus.

Una firma è una sequenza di caratteri o più in generale la traccia che un virus lascerebbe sul computer se riuscisse ad infettarlo.

L'aggiornamento del database delle firme avviene attraverso una connessione della postazione client ad opportuni server autorizzati.

L'antivirus durante la scansione verifica se ogni file (o quelli specificati) è associato a qualche signatures.

Se sì il virus viene rilevato, vengono effettuate una certa serie di operazioni più o meno impostabili in automatico quali:

- L'avvertimento dell'utente
- La riparazione del file
- La messa in quarantena del file
- L'eliminazione del file

Antivirus

Operazioni durante la scansione:

- **L'avvertimento dell'utente**
- **La riparazione del file**
- **La messa in quarantena del file**
- **L'eliminazione del file**

La riparazione del file è il tentativo da parte del sistema di eliminare il virus dal file.

E' utile quando il virus ha infettato file che sono utilizzati dagli utenti (es. documenti word, excel,...) in quanto, qualora la riparazione non avvenga con successo, il file non sarebbe utilizzabile.

Spesso la riparazione fallisce in quanto il sistema non è in grado di rimuovere il virus dal file. In questo caso il file il sistema chiede all'utente se vuole mettere in quarantena il file per tentare nuovamente la riparazione in un tempo successivo o eliminarlo.

Quando un file viene messo in quarantena, viene posto in un'area del disco ad esclusivo utilizzo del sistema Antivirus e non viene usato dal Sistema operativo e li rimane fino a quando non viene riparato o eliminato.

Antivirus

La scansione è una operazione fondamentale ma allo stesso tempo molto impattante sul singolo PC in quanto dura in genere per molto tempo (anche qualche ora) e consuma risorse di calcolo (la CPU) limitando le performance della macchina.

Innanzitutto una volta installato un sistema AV bisogna configurare il livello di scansione, ossia quanto è dettagliata la scansione, quindi quali file verificare e con quale metodologia, quali operazioni effettuare automaticamente sui file infetti, e quali tipi di scansione far partire automaticamente e quando.

Esempio di scansione:

- File di boot del Sistema operativo
- RAM
- Parziale: es specifiche cartelle del PC (documenti, windows,..), specifiche unità di scrittura/lettura
- Completa: tutto il PC

Antispam

Il fenomeno dello spam, notevolmente diffuso negli ultimi anni, può essere mitigato dotando le postazioni client o il server di posta elettronica di un sistema specifico per il controllo dello spam (es. SpamAssassin, Symantec Bright Mail,..).

Anche in questo caso:

- Scegliere Antispam ben noti che garantiscano un frequente aggiornamento
- Fare attenzione, specialmente durante i primi periodi, a ciò che viene etichettato come spam e come viene gestito (cancellato automaticamente o a mano)

Patching del S.O.

Così come i sistemi precedenti, anche il sistema operativo, la componente software principale del PC necessita di manutenzione e aggiornamenti.

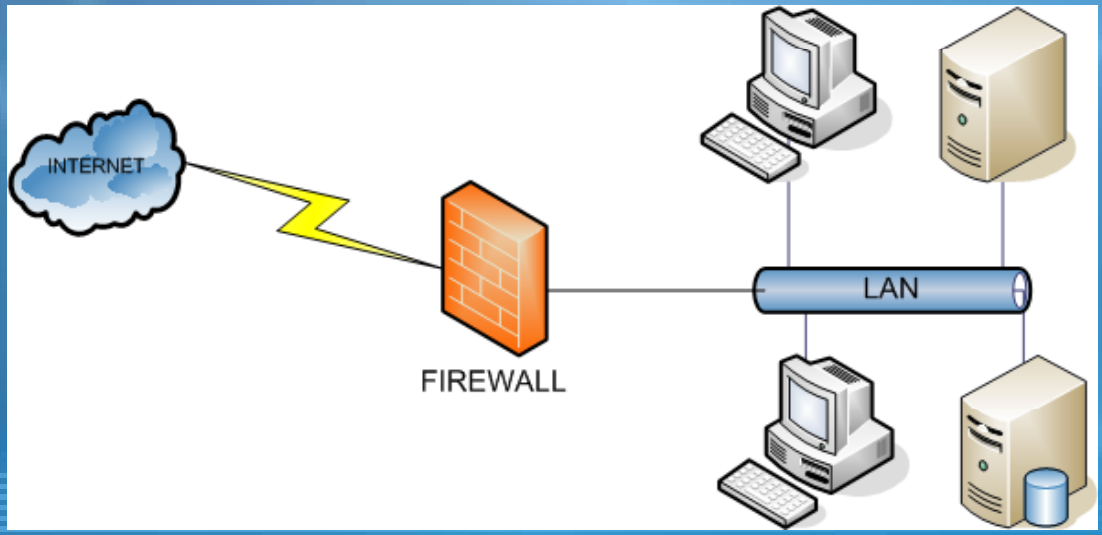
Sia i sistemi Windows sia i sistemi Linux consentono l'aggiornamento del sistema via Internet.

In particolare per i sistemi Windows, il cosiddetto Windows Update, è attivo sin dal S.O. Windows 98.

E' caldamente consigliato attivare i meccanismi di aggiornamento del Sistema Operativo sui PC client.

Firewall

- Si tratta di un dispositivo hardware o di un software (es. firewall personali);
- Isola due porzioni di una rete filtrando e controllando i pacchetti in transito dall'una all'altra;
- Tipicamente viene utilizzato per separare una rete interna "fidata" da una rete esterna (per esempio Internet);
- La funzione del firewall è quella di limitare l'accesso alla rete interna consentendo solo il traffico che possa presumersi "sicuro".



Tecniche di protezione

Consigli e best practices :

Lato utente

- **Possedere un sistema AV ed in genere Anti-malware aggiornabile automaticamente, con schedulazioni almeno settimanali e ben configurato**
- **Aggiornare periodicamente il S.O. anche in maniera automatica**
- **Aggiornare altri prodotti utilizzati (es. suite per Office Automation, Adobe Acrobat,…)**