Sicurezza Informatica

E-Safety

Sicurezza informatica,
protezione dei materiali digitali.

Guido Gelatti – guido.gelatti@itiscastelli.it

Sicurezza Informatica
Definizione

La sicurezza informatica è un processo complesso che richiede una continua analisi dei potenziali rischi al fine di prevedere l'adozione di adeguate contromisure.

Sicurezza Informatica
Definizione

Quando si parla di sicurezza informatica si intende l'analisi delle vulnerabilità, del rischio, delle minacce o attacchi e quindi della protezione dell'integrità fisica (hardware) e logico-funzionale (software) di un sistema informatico e dei dati in esso contenuti o scambiati in una comunicazione con uno più utenti.

Sicurezza Informatica
Definizione

Vulnerabilità

La vulnerabilità può essere intesa come una componente (esplicita o implicita) di un sistema, in corrispondenza alla quale le misure di sicurezza sono assenti, ridotte o compromesse, *il che rappresenta un punto debole del sistema e consente a un eventuale aggressore di compromettere il livello di sicurezza dell'intero sistema*.

Minaccia

Persona, processo o evento con la capacità di causare danni a reti e/o dati. Le minacce possono avere molte forme, ma sono generalmente raggruppate in minacce *umane* e *ambientali*.

Sicurezza Informatica
Definizione

Vulnerabilità

- del sistema operativo
- delle applicazioni
- delle reti

Minaccia

- virus
- spyware
- attacco esterno

$$Rischi = \frac{Minaccia * Vulnerabilità}{contro-misura}$$

Sicurezza Informatica
Definizione

Contromisura

Insieme della azioni con cui si tende a previene o a fronteggiare una situazione sfavorevole.

In generale non è buona norma assumere che le contromisure adottate in un sistema siano sufficienti a scongiurare *qualsiasi* attacco.

Sicurezza Informatica
Definizione

Esempi di Rischio/Contromisura

Rischio:

- accessi non autorizzati ai sistemi informatici

- intercettazione del traffico di rete

- lettura non autorizzata di documenti personali

Contromisura:

- utilizzo di sistemi di autenticazione efficaci

- utilizzo di protocolli cifrati (SSL-HTTPS ecc.)

- cifratura a chiave pubblica dei documenti riservati

Sicurezza Informatica
Importanza

Attenzione!

Un ente pubblico o privato è e sarà sempre più dipendente

- dal suo sistema informativo
- dal sistema informativo dei partner
- dai sistemi informatici/telematici che li collegano

Certificare il rispetto di un qualunque standard o modello (anche non di sicurezza) non è possibile se trascuriamo questa dipendenza.

Sicurezza Informatica
Proprietà

Confidenzialità

Le informazioni possono essere lette solo da chi ne ha diritto

(profilazione account e policy di sicurezza)

Integrità

Le informazioni possono essere modificate solo da chi ne ha diritto

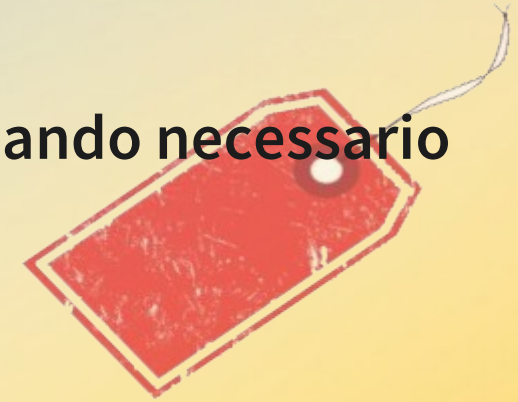
(profilazione account e policy di sicurezza)

Sicurezza Informatica
Proprietà

Disponibilità

Le informazioni devono essere lette/scritte quando necessario

(Procedure di backup e Crash recovery)



Le risorse devono poter essere usate solo da chi ne ha diritto

(Profilazione account)

Sicurezza Informatica
Proprietà

Tracciabilità

poter individuazione di chi ha invocato una operazione

Accountability

poter addebitare l'uso delle risorse

Auditability

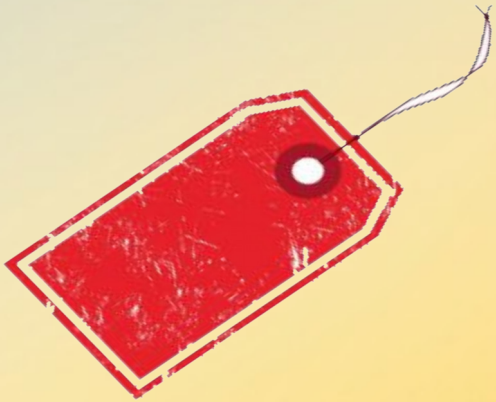
poter verificare l'efficacia dei meccanismi utilizzati

Forensics

Poter provare che certi attacchi hanno avuto luogo

Privacy

Chi/come/se può usare le proprie informazioni personali



Sicurezza Informatica
Comportamenti

Ma la sicurezza implica anche l'adozione di comportamenti "*sicuri*"

- l'utente è elemento "attivo" della rete
- la sicurezza non può essere frutto di soli accorgimenti tecnici
- l'importanza del fattore umano nella sicurezza è strategico

Va osservato che dietro ad ogni tecnologia di sicurezza c'è una persona che deve utilizzarla e che anche il più sofisticato ed apparentemente blindato sistema di sicurezza, sia fisico che logico, può essere vanificato da utilizzatori non addestrati o poco convinti della sua necessità.

Rispetta le policy di sicurezza

Rispetta le regole di sicurezza che la tua amministrazione ha disegnato per te ed i tuoi colleghi. Le policy di sicurezza non sono dettate per "*intralciare il lavoro*" ma per poter far sì che tu "possa continuare a lavorare"

Non utilizzare mai reti pubbliche o Internet point gratuiti per gestire dati sensibili

Sicurezza Informatica
Buone pratiche

Proteggi il tuo computer

Mantieni tutti i software (soprattutto il browser Web) aggiornati

Installa un software antivirus e antispyware

Tieni attivato il firewall e proteggi il tuo router wireless con una password.

Non collegare mai un'unità flash o una chiavetta USB che non conosci al tuo computer: se contiene un virus, potrebbe infettarlo.

Prima di aprire gli allegati o fare clic sui collegamenti contenuti in un messaggio email, un messaggio istantaneo o un social network, chiedi al mittente di confermarne l'autenticità.

Non fare clic su collegamenti o pulsanti in una finestra popup sospetta.

Sicurezza Informatica
Buone pratiche – sicurezza e privacy

Proteggi le informazioni personali sensibili

(sicurezza e privacy molte volte sono legate)

Prima di inserire dati sensibili in un modulo o una pagina Web, verifica la presenza di indicatori che ne attestino la sicurezza, come il fatto che l'indirizzo contenga https (riporti un lucchetto chiuso)

Non fornire mai informazioni sensibili (come numeri di conto o password) in risposta a una richiesta ricevuta tramite un messaggio email, un messaggio istantaneo o un social network.

Non rispondere a richieste di denaro provenienti da "familiari", accordi che sembrano troppo vantaggiosi per essere veri, lotterie cui non hai mai partecipato o altre truffe.

Sicurezza Informatica
Buone pratiche – sicurezza e privacy

Proteggi le informazioni personali sensibili

(sicurezza e privacy molte volte sono legate)

Siate portatori '*irreprensibili*' dell'idea che nel mondo super-connesso di internet la privacy ha un'importanza strategica. Il valore dei nostri dati digitali equivale a quello che nel mondo reale è il valore dei beni all'interno della nostra abitazione.

A chi daremmo le chiavi di casa?

Molte volte regaliamo la nostra vita per poter usare un programma di chat...

Sicurezza Informatica
Buone pratiche – sicurezza e privacy

Proteggi le informazioni personali sensibili

(sicurezza e privacy molte volte sono legate)

Dall'altra parte di Facebook, Google, Bing (ecc.) stanno costruendo (o è già costruito) un avatar commerciale che ci assomiglia come una goccia d'acqua.

Ha i nostri gusti in fatto di cibo e letture. Va in vacanza dove piace andare a noi, ha il nostro reddito, fa i nostri acquisti, ha i nostri amici, legge i nostri stessi giornali…

Avete mai pensato che tutte queste informazioni potrebbero servire a malintenzionati al fine di rubarci l'identità ed agire in nostro nome?

Sicurezza Informatica
Buone pratiche – sicurezza e privacy

Proteggi le informazioni personali sensibili

(sicurezza e privacy molte volte sono legate)

Facciamoci una domanda:

E' proprio necessario condividere tutto?

Proteggi i tuoi account

Proteggere i tuoi account da accessi indesiderati significa proteggere i tuoi dati personali ma anche tutti i tuoi contatti.

Ricorda che se un malintenzionato utilizza le tue credenziali per inviare un allegato malevolo ai tuoi contatti, chi lo riceve si fiderà "*ciecamente*" permettendo al virus di distruggere i dati del tuo contatto (ed i tuoi in maniera speculare).

Sicurezza Informatica
Buone pratiche

Crea password complesse e tienile segrete

Crea password composte da frasi lunghe, contenenti maiuscole, minuscole, numeri e simboli. Usa password diverse per siti diversi, soprattutto se questi ultimi contengono informazioni di natura finanziaria.

Non scrivere le password su un post-it che poi appiccicherai al monitor!

“E' poco sicuro” :-/

Sicurezza Informatica
Buone pratiche

Come utilizzi i social network?

Cerca Impostazioni o Opzioni in social network come Facebook e Twitter per gestire chi può vedere il tuo profilo o le foto in cui sei *taggato*, controlla come gli altri ti possono cercare o fare commenti, e come bloccare le persone.

Quando pubblichi un post, non scrivere nulla che non vorresti vedere in un cartellone pubblicitario.

Cerca di essere selettivo nelle richieste di amicizia che accetti. Valuta periodicamente le persone che hanno accesso alle tue pagine e quello che scrivono su di te.

Sicurezza Informatica
E se non bastasse…

Esagerazione?

"…si consiglia, ad esempio, di non fidarsi mai troppo degli sconosciuti che si incontrano online e di utilizzare la nostra reale identità solo con persone di assoluta fiducia; di utilizzare un laptop per navigare sul web e un altro laptop o computer per lavorare (così da rendere inaccessibili file privati o segreti); memorizzare le proprie password a mente, senza dover ricorrere a foglietti volanti o programmi informatici facilmente hackerabili; di coprire con un pezzettino di nastro isolante la fotocamera frontale dello smartphone, onde evitare di poter essere fotografati via remoto; non utilizzare mai i propri dati per la registrazione nei servizi web, ma inventarne sempre di nuovi per ogni registrazione; se ci si dovesse recare in un luogo che deve restare segreto, togliere batteria e SIM dal cellulare, per essere irreperibili e irrintracciabili."

Forse...

Sicurezza Informatica
Siti web

Se gestisci un sito

- sappi che la necessità di sicurezza va moltiplicata per il numero di utenti che utilizzano il tuo sito

- che potrebbero nascere problemi di privacy se i materiali contenuti possono essere considerati sensibili

- che il tuo sito potrebbe essere usato come “inoculatore” di virus per infettare chi vi accede

Sicurezza Informatica
Siti web

Se gestisci un sito

- la scelta (e la protezione) delle pasword per accedere ai servizi FTP, CMS, MySQL è importantissima
- tieni aggiornato il CMS e tutti i sui componenti
- gestisci attentamente i permessi di accesso dei vari utenti
- effettua backup regolari delle cartelle sull' host e mantienilo in ordine (nel disordine possono nascondersi app abusive)
- attenzione ad utilizzare app java!

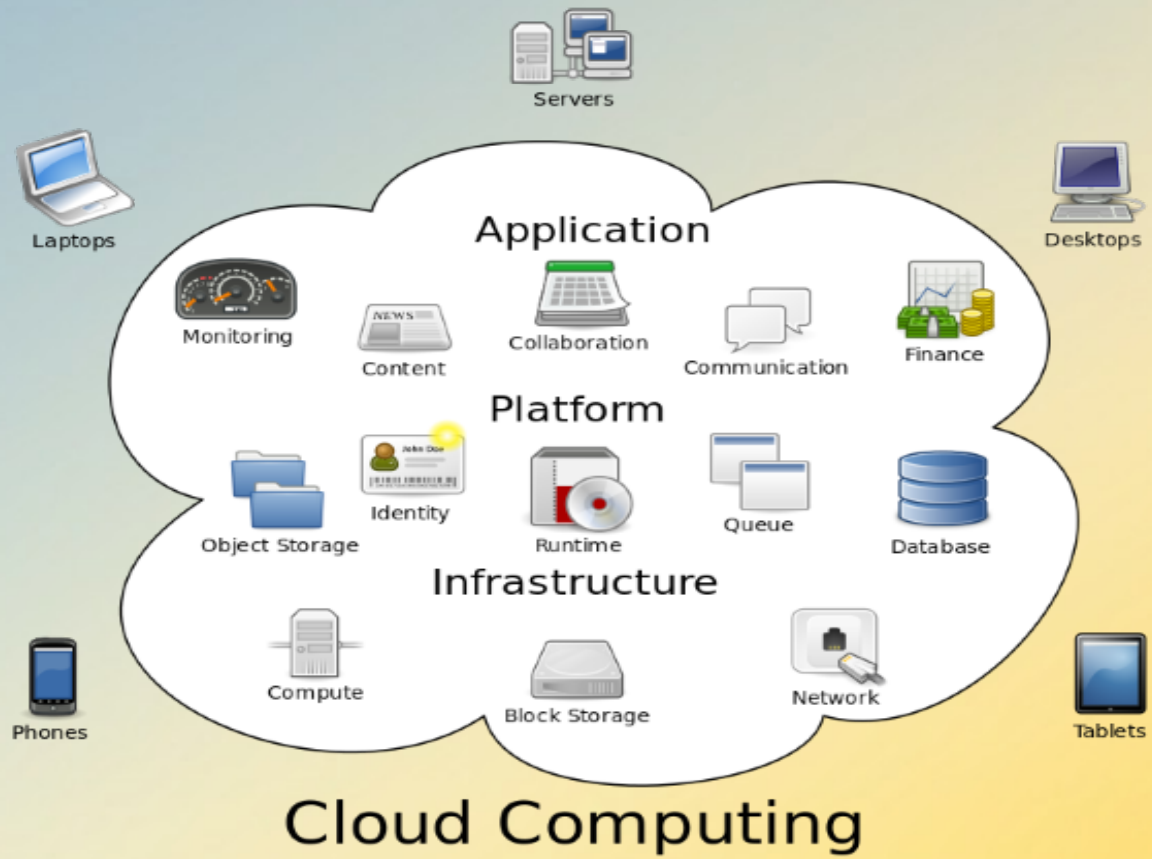
Sicurezza Informatica
Siti web

Cosa può succedere al nostro sito?

- utilizzato per far phishing
- uso abusivo delle cartelle
- ospitare app e/o servizi malevoli
- inviare mail a scopo di spam
- raccogliere dati personali e/o sensibili degli utenti

Sicurezza Informatica
Cloud

E il cloud?



Sicurezza Informatica
Cloud

E il cloud?

Valgono le stesse raccomandazioni legate alle risorse condivise su una rete quindi:

- occhio alle password
- occhio a quello che si pubblica
- occhio ai permessi d'accesso che forniamo ai nostri collaboratori

Sicurezza Informatica
Cloud

E il cloud?

Non sono tutte rose fiori, alcuni esempi:

- DISPONIBILITA' : dipendiamo in tutto per tutto dal nostro fornitore
- DISPONIBILITA' : la rete di connessione ad internet diventa elemento critico
- CONFIDENZIALITA' : il modo in cui i dati vengono gestiti – e protetti – non dipende più da noi
- PRIVACY : la privacy è assicurata? Con che legislazione? Domanda non banale in quanto le risorse nel cloud non hanno confini nazionali

Sicurezza Informatica
Per chiudere

La sicurezza non è mai troppa!

Guido Gelatti – guido.gelatti@itiscastelli.it

Sitografia

- http://www.agid.gov.it/
- http://www.html.it/sicurezza/
- http://www.sviluppoeconomico.gov.it/index.php/it/comunicazioni/internet/sicurezza-informatica
- http://www.garanteprivacy.it/
- https://it.wikipedia.org
- https://www.microsoft.com/italy/sicurezza/
- http://it.ccm.net/contents/833-introduzione-alla-sicurezza-informatica
- http://guide.hosting.aruba.it/hosting/linux/faq/consigli-di-sicurezza-contro-virus-e-malware.aspx
- http://www.hostingtalk.it/sicurezza-hosting-12-consigli/