

# ICT Security:

Aggiornamento: fonti e risorse



<http://www.infosec.it>

[info@infosec.it](mailto:info@infosec.it)

Relatore: Igor Falcomatà – Marzo 2002

# Importanza dell'aggiornamento

- rimanere "up-to-date" con i propri sistemi

- aggiornamenti/patches/hot fixes
- vulnerabilità note
- hardening ed ottimizzazione

I sistemi non mantenuti "invecchiano" rapidamente. Vengono continuamente rese pubbliche nuove vulnerabilità per sistemi operativi ed applicazioni.

- conoscere nuove tecniche e metodologie

- attacco
- verifica
- difesa

Analizzare e capire le metodologie utilizzate negli attacchi per poterle controllare ed arginare.

- assicurare una formazione adeguata allo staff tecnico e all'utenza

Stare al passo con i tempi, confrontarsi e scambiare esperienze...

# Trovare fonti e risorse...

- su Internet

- siti o network
- mailing list, bollettini e newsgroup
- forum, chat e sistemi di messaggistica
- articoli e riviste in formato elettronico
- libri, documenti ed howto
- ...

- "extra-Internet":

- libri
- riviste
- seminari, conferenze e meeting
- corsi
- consulenze
- ...

- ufficiali

- produttori  
Microsoft, Sun, Red Hat, iPlanet,  
Apache, ...

- "semi-ufficiali"

- enti ed organismi  
CERT/CC, NIPC, CIAC, SANS, ...
- siti e società specializzate  
SecurityFocus, @stake, ...

- "ufficiose" o "underground"

- siti "security related"  
PacketStorm, Security Bugware, ...
- "hacker", ricercatori, studenti, ...

# Frammentazione delle risorse

- difficoltà nel trovare le fonti d'informazione e le risorse più adatte al contesto
  - cerco sul sito del produttore?
  - contatto il supporto tecnico?
  - mi rivolgo ad una società di consulenza?
  - cerco su un sito specializzato in security?
  - cerco su un motore di ricerca?
- difficoltà nel reperire le informazioni cercate, anche quando sia stata individuata la fonte a cui fare riferimento
- spesso per una visione "completa" una sola fonte non è sufficiente...
- spesso le informazioni cercate non sono reperibili dove ci aspettiamo...

# Affidabilità delle risorse

- molte informazioni provengono da fonti "non attendibili"
  - fonti "ufficiose"
  - fonti "underground"
  - fonti mantenute amatorialmente o per hobby
  - "voci" o "chiacchiere"
- è sempre possibile che anche informazioni che provengono da canali ufficiali non siano "affidabili" o comunque adeguate alle necessità

Non è cosa rara trovare informazioni molto complete ed approfondite proprio su siti "ufficiosi", siti di gruppi "hacker" o siti "underground".

Esistono però anche numerosissime risorse assolutamente inaffidabili o di scarsa valenza tecnica.

# Completezza ed aggiornamento

- fonti non complete
  - fonti specializzate... in altro
  - "vendor point of view"
  - fonti dal contenuto tecnico scadente od errato
  - scarso interesse per l'argomento da parte dei produttori o dei curatori della risorsa
- informazioni non disponibili
  - informazioni ritenute "di scarso interesse"
  - carenza di ricerca ed informazioni "pubbliche" sull'argomento
  - dettagli od informazioni che i produttori non intendono distribuire
- fonti non aggiornate
  - risorse "abbandonate"
  - risorse non facilmente aggiornabili (libri, riviste, articoli, ...)
- fonti aggiornate "lentamente"
  - necessità per i produttori di verificare le problematiche e trovare le soluzioni
  - necessità di sviluppare, testare e distribuire procedure e/o upgrade
  - scarsa attenzione dei produttori alle problematiche di security
  - risorse mantenute amatorialmente, spesso nel tempo libero

# Come usare le risorse disponibili...

- identificare le esigenze
  - aggiornamento
  - approfondimento
  - notifica, ricerca o verifica di vulnerabilità
  - implementazione di nuove funzionalità
  - ...
- identificare le fonti
  - trovare le fonti disponibili
  - verificarne il grado di affidabilità, completezza ed aggiornamento
  - cercare le informazioni richieste
- analizzare le informazioni
  - comprendere le informazioni ritrovate
  - valutare se siano sufficienti a risolvere le problematiche poste
- verificare le informazioni
  - verificare che siano effettivamente corrette, complete ed aggiornate (in particolar modo se provengono da fonti "non affidabili")
  - testare in un ambiente di prova "isolato" le soluzioni
  - valutare se effettivamente risolvano le problematiche poste
  - valutare l'impatto sull'ambiente di produzione
  - applicare le soluzioni alla produzione
- mantenere le informazioni
  - registrare ed archiviare le soluzioni utilizzate nelle procedure e nella "knowledge-base" aziendali
  - diffondere le informazioni

# Alcuni esempi...

- "information security"
  - google: ~270mila risultati
  - altavista: ~119mila pagine
  - deja: ~58mila risultati
  - yahoo: 616 siti
  - msn: 581 siti
- "firewall"
  - google: ~3 milioni di risultati
  - altavista: ~1,7 milioni di pagine
  - deja: ~1,2 milioni di risultati
  - yahoo: 217 siti
  - msn: 196 siti
  - virgilio: 141 siti
  - arianna: ~8mila pagine
  - securityfocus: 9019 risultati
  - packetstorm: 921 risultati
  - sikurezza.org: 975 risultati
- su yahoo..
  - 588 siti nella categoria  
Computers and Internet > Security and Encryption
  - 678 siti nella categoria  
Business to Business > Computers > Security and Encryption
- su google..
  - 2.615 siti nella categoria  
Computers > Security
- su amazon (sezione libri)..
  - ~13.500 risultati cercando "security"
  - ~7.000 libri con la parola "security" nel titolo
- su securityfocus
  - ~4.300 vulnerabilità catalogate
  - ~3.900 bollettini di sicurezza
  - ~3.800 tra libri, documenti e articoli

# Full disclosure

- una filosofia per affrontare le tematiche di sicurezza (informatica) che recita:
  - un sistema realmente sicuro deve essere in grado di superare una revisione pubblica a tutti i livelli (protocollo, codice sorgente, etc.)
  - i dettagli delle vulnerabilità di sicurezza devono essere accessibili a chiunque
- adottata da quelli che vengono definiti (o si definiscono) "white-hats"
- vantaggi
  - un grande numero di individui può valutare le debolezze di sicurezza del sistema
  - i produttori sono stimolati a fornire le soluzioni in tempo breve
  - programmatori e progettisti possono imparare dagli errori di altri
  - gli utenti possono identificare vulnerabilità simili su sistemi diversi dall'originale
- svantaggi
  - nello stesso momento in cui informi le persone "costruttive" delle vulnerabilità di sicurezza, informi anche i malintenzionati

<http://www.securityfocus.com/popups/forums/bugtraq/faq.shtml>

# No disclosure

- prevede di non diffondere pubblicamente dettagli sulle vulnerabilità di sicurezza..
  - i dettagli vanno comunicati solamente ai vendor o ad organismi preposti ed eventualmente diffusi tra i produttori attraverso canali "riservati"
  - sarà cura del vendor (o dell'ente) decidere se e quali dettagli diffondere pubblicamente
- adottata anche dai "black-hats"
  - ovviamente in questo caso non verranno avvisati i produttori, la vulnerabilità sarà utilizzata per profitto personale dall'individuo o dal gruppo che l'ha scoperta
- vantaggi
  - le informazioni sulle vulnerabilità non vengono diffuse pubblicamente, rendendo più difficile per i malintenzionati ottenere le informazioni
  - i vendor hanno più tempo per studiare soluzioni e contromisure
- svantaggi
  - security through obscurity
  - non è detto, solamente perché l'informazione non è pubblica, che non sia già conosciuta da altri
  - minori sono i dettagli diffusi, più è difficile valutare correttamente l'impatto della vulnerabilità e verificare se sia stata corretta adeguatamente

# Responsable disclosure

- la verità sta nel mezzo?

- i dettagli vanno comunicati ai vendor o ad organismi preposti ed eventualmente diffusi tra i produttori attraverso canali "riservati"
- al vendor verrà lasciato un tempo adeguato per analizzare e risolvere il problema
- qualora il vendor non si dimostri interessato a collaborare oppure una volta che abbia pubblicato le soluzioni al problema, verranno diffusi pubblicamente tutti i dettagli
- molti prevedono che in ogni caso non siano distribuiti pubblicamente attacchi preconfezionati ("exploit") per utilizzare o verificare le vulnerabilità

- vantaggi

- le informazioni sulle vulnerabilità vengono diffuse pubblicamente solamente quando siano state pubblicate anche le adeguate contromisure
- non vengono pubblicati tool pronti per gli "skript kiddie"

- svantaggi

- non è detto, solamente perché l'informazione non è pubblica, che non sia già conosciuta da altri

<http://www.wiretrip.net/rfp/policy.html>

# Anti disclosure

- supportata di recente da una parte del movimento "underground", contrario alla politica "full disclosure":
  - pubblicare informazioni su vulnerabilità o "exploits" giova solamente agli "skript kiddie" e serve a facilitare il compito di società di sicurezza e siti quali SecurityFocus
  - il livello di sicurezza su Internet è comunque più alto quando le vulnerabilità non sono conosciute (o per lo meno non lo sono i dettagli) piuttosto che quando viene adottata la full disclosure

[http://anti.security.is/  
FAQ.php?faq=official](http://anti.security.is/FAQ.php?faq=official)

# I vendor?

- molti produttori adottano/ adottavano una politica "no disclosure"
- molti vendor non considerano/ consideravano la sicurezza come parte integrante del sistema
- i sistemi vengono progettati secondo standard chiusi, "perché garantiscono maggiore sicurezza"
- le vulnerabilità non si conoscono, quindi non ci sono
- meglio non rilasciare uno specifico aggiornamento ed aspettare un normale ciclo di upgrade, piuttosto di dover ammettere pubblicamente una vulnerabilità nel proprio software
- in ogni caso, diffondere meno dettagli possibili e minimizzare l'impatto (sono numerose le vulnerabilità "puramente teoriche" per cui siano usciti attacchi funzionanti..)
- coloro che segnalano le vulnerabilità sono degli scocciatori piuttosto che persone da ringraziare

**Security through obscurity:  
ovvero non diffondere dettagli sul design del sistema, sui protocolli usati, non pubblicare il codice sorgente, non fornire dettagli sulle vulnerabilità per non facilitare il compito agli attaccanti**

# I vendor?

- le cose stanno cambiando, grazie anche a risorse come bugtraq ed alla full disclosure
- i produttori hanno cominciato a considerare la sicurezza come parte importante/fondamentale della loro strategia
- vengono sempre più utilizzati standard aperti, almeno per le componenti critiche
  - protocolli
  - crittografia
  - autenticazione
- creano risorse specifiche per il supporto di security
  - staff specializzati, siti, mailing list, libri, corsi, certificazioni, ....
- utilizzano società specializzate
  - per valutare la sicurezza dei sistemi
  - per analizzare o fare "l'auditing" di protocolli e codice sorgente
  - per sviluppare parti del sistema sensibili ai fini della sicurezza
- adottano un approccio attivo
  - seguono e ascoltano anche risorse "non ufficiali"
  - rivedono il design, le impostazioni ed il codice dei loro prodotti in ottica di sicurezza

# Strumenti utili – Siti web (1/2)

Sito	Descrizione
<a href="http://www.securityfocus.com/">http://www.securityfocus.com/</a>	Portale commerciale dedicato alla sicurezza informatica. E' il sito di riferimento per trovare informazioni sulle vulnerabilità, i tool e le metodologie di attacco e di difesa. Ospita numerose mailing list tra cui Bugtraq (la mailing list più utilizzata e conosciuta dagli esperti di sicurezza e dagli hacker). Aree dedicate per sistemi operativi e tipologie (news, appuntamenti, fondamenti di sicurezza, ids, vpn, vulnerabilità, prodotti, ...)
<a href="http://www.cert.org/">http://www.cert.org/</a>	CERT/CC, risorsa gestita dalla Carnegie Mellon University. Dedicato principalmente alla gestione degli incidenti e alla diffusione di informazioni e advisory di sicurezza.
<a href="http://www.nipc.gov/">http://www.nipc.gov/</a>	National Infrastructure Protection Center, risorsa mantenuta dall'FBI con informazioni su sicurezza informatica, privacy, cyber crime. Interessantei in particolare le pubblicazioni (pdf) periodiche "Highlihts Issues" e "Cybernotes", una vista d'insieme di tutte le informazioni e problematiche di sicurezza divise per periodo.
<a href="http://www.ciac.org/">http://www.ciac.org/</a>	Computer Incident Advisory Capability, risorsa mantenuta dal Dipartimento dell'Energia americano con informazioni su sicurezza (vulnerabilità, tool, "hoaxes", ...) e mailing list periodiche
<a href="http://www.sans.org/">http://www.sans.org/</a>	Il SANS (System Administration, Networking, and Security) Institute è un portale frutto della cooperazione di numerosissimi enti governativi (americani), ditte, istituti di ricerca, associazioni e privati per la diffusione della cultura informatica, in particolar modo quella relativa alla sicurezza. E' una risorsa completissima di informazioni, "how-to" e documentazione varia. Pubblicano bollettini periodici e forniscono servizi di certificazione indipendente.
<a href="http://packetstormsecurity.nl/">http://packetstormsecurity.nl/</a>	Completo repository di tool, attacchi ed informazioni relative alla sicurezza informatica, con possibilità di ricerca e di navigazione per aree tematiche. Molto conosciuto negli ambienti "undergroud".

# Strumenti utili – Siti web (2/2)

Sito	Descrizione
<a href="http://www.safermag.com/">http://www.safermag.com/</a>	Security Alert for Enterprise Resources, pubblicazione (pdf) periodica del Relay Group. Contiene informazioni e news "security related"
<a href="http://xforce.iss.net/">http://xforce.iss.net/</a>	Portale del team "x-force" della ISS, con archivio delle vulnerabilità diviso per piattaforme e generi. Molto completo e di facile consultazione.
<a href="http://cve.mitre.org/">http://cve.mitre.org/</a>	Common Vulnerabilities and Exposures, probabilmente il più grande ed organizzato catalogo di vulnerabilità. Viene spesso utilizzato anche negli advisor, dai programmi che effettuano test di vulnerabilità e dagli IDS (CVE ID: ...)
<a href="http://icat.nist.gov/">http://icat.nist.gov/</a>	Motore di ricerca per vulnerabilità basato sul CVE.
<a href="http://www.atstake.com/security_news/">http://www.atstake.com/security_news/</a>	Security News Network, portale di news "security related" gestito dalla @stake.
<a href="http://www.s bq.com/">http://www.s bq.com/</a>	Rivista on-line "Secure Business Quarterly", gestita dalla @stake.
<a href="http://www.attrition.org/">http://www.attrition.org/</a>	Portale "underground" molto conosciuto, in particolare pubblica "defaced-commentary", un commento sui "defacement" di siti ad "alto profilo" (siti governativi o militari USA, multinazionali, società che si occupano di sicurezza, etc.).
<a href="http://www.alldas.org/">http://www.alldas.org/</a>	Portale di security. Famoso perché tiene un mirror e pubblica le statistiche di tutti i siti che subiscono "defacement".
<a href="http://www.securitybugware.org/">http://www.securitybugware.org/</a>	Security Bugware. Archivio di vulnerabilità diviso per sistemi operativi. Molto utilizzato e conosciuto negli ambienti "underground".

# Strumenti utili – Siti web italiani

Sito	Descrizione
<a href="http://www.sikurezza.org/">http://www.sikurezza.org/</a>	Gestito da volontari (e hostato da Infosec). Ospita le mailing list in italiano moderate ml@sikurezza.org ("security-related") e crypto@sikurezza.org (dedicata alla crittografia). Con archivio on-line.
<a href="http://www.teach.it/">http://www.teach.it/</a> -> "Le liste"	Ospita mailing list in italiano moderate dedicate al networking ed alla sicurezza. Con archivio on-line.
<a href="http://security.dsi.unimi.it/">http://security.dsi.unimi.it/</a>	Italian Computer Emergency Response Team (CERT-IT). In particolar modo ospita la mailing list in italiano unix-security.
<a href="http://security.fi.infn.it/">http://security.fi.infn.it/</a>	Gruppo dedicato alla computer security dell'Istituto Nazionale di Fisica Nucleare.
<a href="http://www.cert.garr.it/">http://www.cert.garr.it/</a>	Il servizio di sicurezza del GARR; in particolare contiene alcuni dei più importanti security alert tradotti in italiano ( <a href="http://www.cert.garr.it/alerts/">http://www.cert.garr.it/alerts/</a> ).
<a href="http://www.darioforte.com/">http://www.darioforte.com/</a>	Sito del giornalista e ricercatore Dario Forte, esperto riconosciuto del settore e membro del Computer Security Institute di San Francisco. Contiene articoli, forum e link utili.
<a href="http://www.andreamonti.net/">http://www.andreamonti.net/</a>	Sito dell'avvocato e giornalista Andrea Monti, esperto in legislazione informatica. Contiene articoli e link utili.
<a href="http://www.interlex.it/">http://www.interlex.it/</a>	Portale dedicato alla legislazione, con particolare riguardo ad informatica, privacy e nuove tecnologie.
<a href="http://www.securityinfos.com/">http://www.securityinfos.com/</a>	Portale in italiano dedicato alla sicurezza, con news e link.
<a href="http://www.ziobudda.net/sicurezza/">http://www.ziobudda.net/sicurezza/</a>	Pagine dedicate alla sicurezza del portale italiano "Linux-oriented".

# Strumenti utili – "riviste underground"

Sito	Descrizione
<a href="http://www.phrack.org/">http://www.phrack.org/</a>	La più famosa e-zine "underground". Pubblica articoli di elevato contenuto tecnico ed è seguita (spesso con terrore :) anche dallo staff di security di numerosi vendor. Molte delle principali tecniche di attacco ai sistemi informatici sono passate "dalla teoria alla pratica" solamente dopo essere state pubblicate e spiegate qui.
<a href="http://www.2600.org/">http://www.2600.org/</a>	Il celebre periodico (cartaceo) 2600. Sebbene i contenuti tecnici non siano eccelsi e la rivista non abbia più i fasti di un tempo, è ancora una rivista molto seguita ed amata per ragioni storiche e per le sue battaglie per le libertà di espressione e diffusione libera delle informazioni.
<a href="http://www.s0ftpj.org/bfi/">http://www.s0ftpj.org/bfi/</a>	Celebre e-zine "underground" in italiano. Probabilmente una delle poche con un contenuto tecnico di assoluto valore.
<a href="http://www.spippolatori.com/nr.html">http://www.spippolatori.com/nr.html</a>	Altra e-zine italiana degna di nota.

# ICT Security:

Aggiornamento: fonti e risorse



<http://www.infosec.it>

[info@infosec.it](mailto:info@infosec.it)

<http://www.infosec.it/progetti.html>  
[igor@infosec.it](mailto:igor@infosec.it)