



Corso di Certified Ethical Hacker

Pordenone 13 - 17 dicembre 2010

**EC-Council - Il mondo degli hackers - Alcuni aspetti del computer crime - Il corso di Ethical Hacking
Profilo di Data Security**

EC-Council

L'International Council of Electronic Commerce ha sede a New York ed opera in 30 nazioni con una struttura altamente qualificata.

È un'organizzazione indipendente, la cui missione è definire standard professionali nel settore della sicurezza e dell'e-business. È formata da professionisti che offrono ai propri clienti le migliori soluzioni finalizzate alla sicurezza del business aziendale e del commercio elettronico.

È membro del NOCA (National Organisation for Competency Assurance) che garantisce che le organizzazioni aderenti siano competenti nel loro settore e che rilascino certificazioni sviluppate nel rispetto dei più elevati standard professionali.

Del NOCA fanno parte anche Prometrics e Pearson VUE.

Attraverso il proprio network mondiale EC-Council ha certificato professionisti appartenenti ad organizzazioni quali:

- FBI,
- CIA, US Marine,
- US Air force, US Army,
- Singapore Police Force, Maritime & Port Authority of Singapore,
- Stock Exchange of Singapore,
- Malaysia's Ministry of Defence,
- Citibank,
- Hewlett Packard,
- IBM,
- VISA, Sony,
- American Express,
- Kodak,
- Fujitsu,
- Federal Express e UPS.

In Italia:

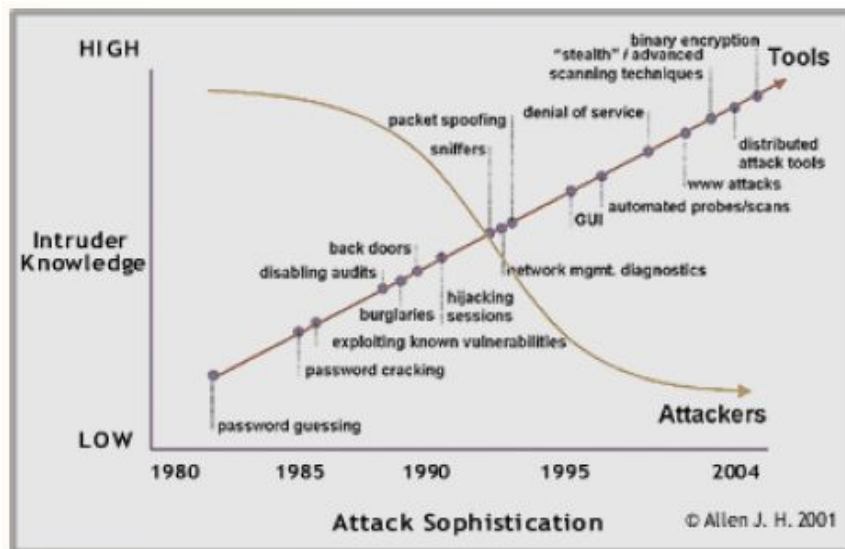
- Vodafone,
- Telecom e alcune banche italiane di primo livello,
- Molte altre aziende ed istituzioni che, per motivi di riservatezza, non desiderano essere citate.

Recentemente alcuni il corso di Ethical Hacker certificato dall'EC-Council è stato scelto ed adottato per formare i professionisti della McAfee/Foundstone, azienda leader nel settore della sicurezza informatica, che propone soluzioni e servizi mirati ad assicurare la sicurezza dei sistemi e delle reti in tutto il mondo.

Il mondo degli hacker

Capacità d'attacco e competenze

Grazie alla disponibilità di strumenti informatici che presentano una curva di apprendimento sempre più bassa, la capacità offensiva degli attaccanti, anche casuali, è in costante aumento facendo, per contro, diminuire la competenza tecnica necessaria anche per gli attacchi più sofisticati.



Anonimato e Gruppi d'attacco

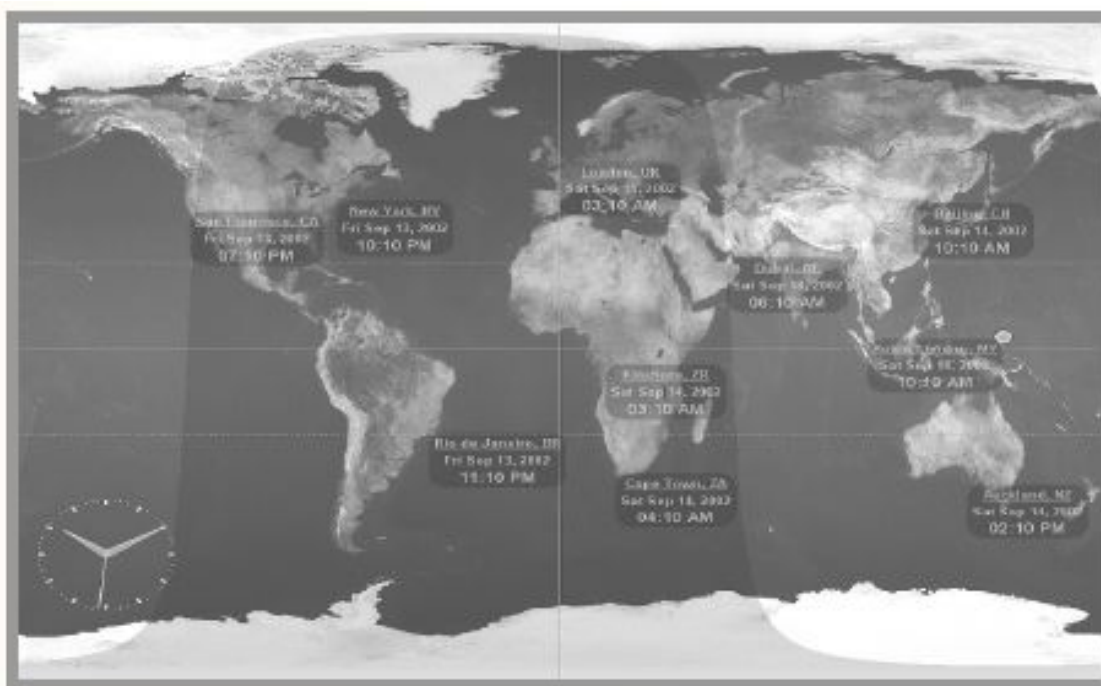
L'uso di tecniche elusive, tanto semplici quanto efficaci, consentono l'anonimato e l'intangibilità degli attaccanti, rendendoli allo stesso tempo onnipresenti ed invisibili. Internet ha facilitato sia la condivisione delle informazioni sia la capacità di aggregazione degli attaccanti. Mentre le organizzazioni hanno strutture più rigide ed una presenza più tangibile, gli hackers utilizzano tecniche simili a quelle della guerriglia, agendo al tempo stesso uniti e distribuiti.

Casualità ed ubiquità dell'avversario

Anche se circa il 50% degli attacchi è perpetrato da personale interno (insiders) molte organizzazioni sono vittime casuali.

Strumenti automatizzati che scandagliano perennemente la rete alla ricerca di host vulnerabili o mail infette inviate in massa ad indirizzi casuali, vanificano il requisito di accessibilità fisica che è proprio degli attacchi più tradizionali.

Tutto ciò rende una potenziale vittima sia l'organizzazione locale sia quella operante nell'emisfero opposto a quello dell'attaccante.

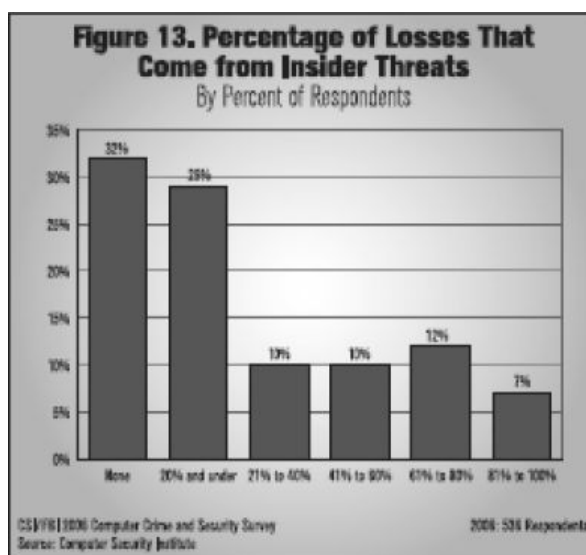


Alcuni aspetti del computer crime

Attacchi ad opera di personale interno

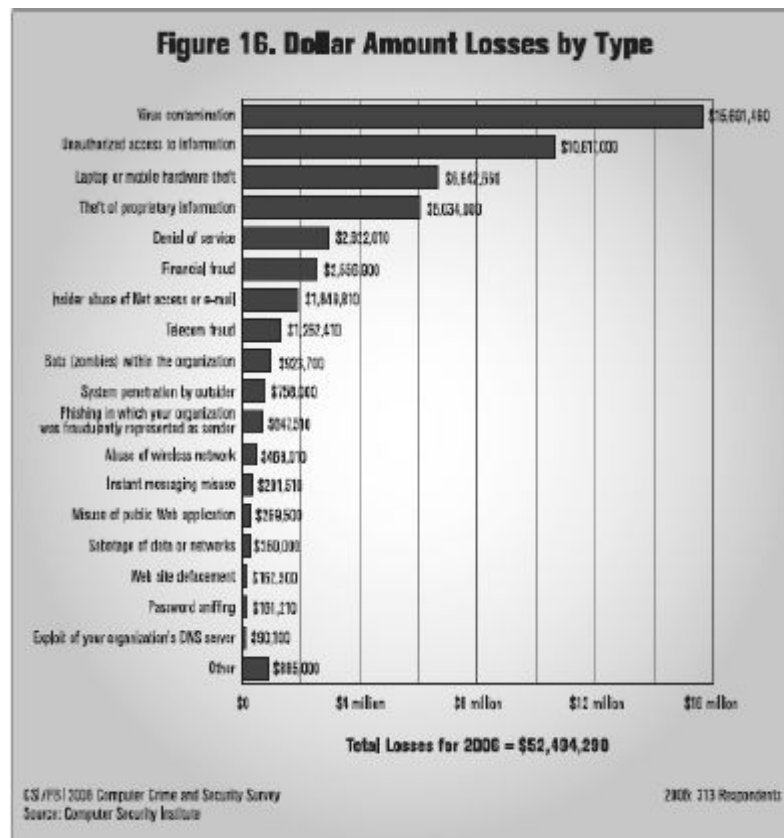
Anche se la maggior parte degli intervistati non considera il personale interno responsabile delle perdite derivate da atti di computer crime, un numero altrettanto significativo ritiene che gli insiders siano comunque responsabili di una parte sostanziale di dette perdite. Una recente indagine italiana ha rilevato che circa il 50% del personale che cambia lavoro, trafuga documentazione riservata da utilizzare al prossimo impiego.

(2006 CSI/FBI Computer Crime and Security Survey)



Perdite Finanziarie

Nel 2006, la media delle perdite finanziarie è stata di circa \$ 170.000 per intervistato. Si ritiene che, rispetto agli anni precedenti, il trend sia in declino grazie al drammatico incremento degli investimenti in sicurezza. Si ritiene comunque che il confronto si sposterà su un livello più alto, rendendo necessari nel medio termine ulteriori investimenti a favore della sicurezza. I problemi di sicurezza maggiormente riportati riguardano la protezione dei dati e la gestione delle vulnerabilità. *(2006 CSI/FBI Computer Crime and Security Survey)*



Vendita di exploit in internet

Zero-day exploit per Windows Vista sono venduti a \$ 50.000 su alcuni siti di hackers. "Ad prezzo variabile tra i \$20.000 ed i \$30.000 è possibile comprare uno zero days exploit. Per \$5.000 è possibile comprare un nuovo Bot o un Trojan. Penso che l'industria del malware stia generando più soldi di quella dell'anti-malware."

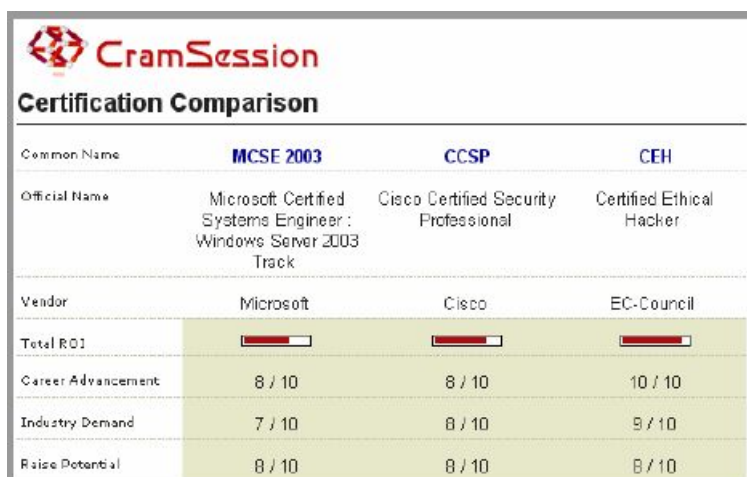
(Raimund Genes, CTO, Trend Micro)




Certified Ethical Hacker, la competenza che serve

I Certified Ethical Hackers (CEH), sono professionisti che hanno sviluppato competenza e consapevolezza propria degli hackers. I Certified Ethical Hackers padroneggiano gli stessi strumenti utilizzati dagli hackers e considerano la sicurezza dal punto di vista dell'attaccante.

CEH la certificazione più richiesta

CEH è la certificazione in maggiore crescita nel comparto della sicurezza. Comparata con altre certificazioni, CEH presenta i migliori risultati in termini di R.o.I. (Return of Investment), sviluppo della carriera, domanda nel settore della sicurezza e sviluppo del proprio potenziale.
(www.brainbuzz.com/certifications/compare-certifications.asp)



Common Name	MCSE 2003	CCSP	CEH
Official Name	Microsoft Certified Systems Engineer : Windows Server 2003 Track	Cisco Certified Security Professional	Certified Ethical Hacker
Vendor	Microsoft	Cisco	EC-Council
Total ROI			
Career Advancement	8 / 10	8 / 10	10 / 10
Industry Demand	7 / 10	8 / 10	9 / 10
Raise Potential	8 / 10	8 / 10	8 / 10

CEH, come affrontare un mondo misterioso

Per vincere le battaglie della sicurezza non bastano solo dei buoni tool. Per fronteggiare il mistero e la magia che circondano il mondo degli hackers ed il caos dell'underground è richiesta una capacità di analisi che lo renda chiaro, netto e comprensibile a chi deve affrontarlo. Durante l'apprendimento, gli studenti beneficeranno di esperienze derivanti da studi dei sistemi complessi (Complex Adaptive Systems) e dalla gestione del Caos (Chaos Management)

Il corso Certified Ethical Hacker

Descrizione del corso

I partecipanti al Corso di Certified Ethical Hacker verranno inseriti in un ambiente interattivo dove verrà mostrato come analizzare, testare, violare e rendere sicuro il proprio sistema. Durante i 5 giorni di formazione, gli studenti familiarizzeranno con strumenti che hanno particolare importanza nel mondo dell'hacking.

Lo scopo didattico di queste sessioni non è quello di presentare gli ultimi tool o zero days exploit, ma far sviluppare al partecipante una concezione della sicurezza che consideri anche la determinazione e la irresponsabilità dell'attaccante. La responsabilità giuridica ed amministrativa sono allo stesso tempo la migliore arma dell'attaccante (che la elude operando anonimamente) ed il peggior handicap del difensore (che invece la deve considerare come parte del mandato ricevuto).

Per questo motivo, gli studenti impareranno sia l'utilizzo di tecniche e strumenti degli hacker, che lo sviluppo di una cultura open mind adeguata all'avversario. In un ambiente controllato, i partecipanti, con l'aiuto di strumenti di analisi ed intrusione messi a loro disposizione, saranno liberi di attaccare e conquistare dei server per rendersi conto che, fondamentalmente, è l'approccio mentale quello che distingue il criminale dal difensore.

Il corso è propedeutico all'esame Council Certified Ethical Hacker.

Chi dovrebbe partecipare

Della partecipazione a questo corso, beneficeranno in modo particolare professionisti e responsabili della sicurezza, security auditors, amministratori di siti e di sistemi e a chiunque interessi l'integrità delle infrastrutture di network.

Durata

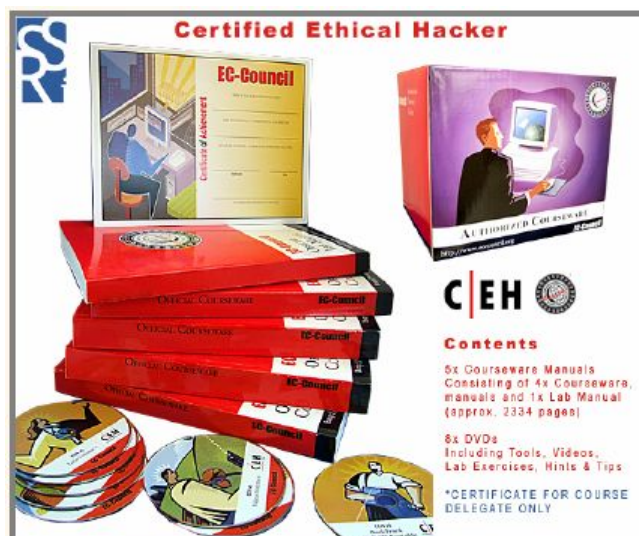
5 giorni consecutivi, dal lunedì al venerdì, dalle 9:00 alle 13.00 e dalle 14.30 alle 17:30.

Certificazione

L'esame EC-Council Certified Ethical Hacker (opzionale), può essere sostenuto nel periodo successivo allo svolgimento del corso Per ricevere l'attestato di certificazione CEH, i partecipanti dovranno superare l'esame erogato in una delle sedi certificate della società Prometric (in modalità on-line).

Materiale didattico

- Ad ogni partecipante verrà fornito un kit didattico composto da:
- 5 libri di testo (tot. 4800 pag.),
- 4 DVD con supporti audiovisivi a completamento della teoria erogata in aula,
- una USB flash memory con tutti i software utilizzati durante il corso.



Componente economica del Corso

La quota individuale per ogni partecipante è pari a € 3.500.00 + IVA ed è comprensiva di tutti gli elementi dell'attività didattica. Nella quota sono compresi i pranzi ed i coffee break presso la sede di erogazione del corso. Sono escluse le spese di per cene ed alloggio.

Alloggio:

I partecipanti potranno alloggiare presso gli alberghi del centro città con i quali DataSecurity ha stipulato convenzioni (costo in convenzione da € 82,00/notte per camere doppie ad uso singolo in alberghi a 5 stelle e, a scendere, fino a € 35,00/notte per sistemazioni più economiche.

Sede di erogazione del Corso

Le attività di formazione sono svolte in attrezzatissime aule presso il Consorzio Universitario di Pordenone.

Il sito dista due chilometri dal centro della città ed è comodamente raggiungibile in autobus o in cinque minuti di taxi.

Come arrivare a Pordenone

Gli aeroporti più vicini sono Venezia (Tessera) e Trieste (Ronchi dei Legionari).

Il collegamento aeroporto/Pordenone, per l'aeroporto di Venezia, è assicurato da un comodo servizio di pullman navetta che compie il tragitto, senza soste, in un'ora scarsa.

La stazione ferroviari dista cinque minuti di passeggiata dal centro.

Organizzazione del corso

Il corso è organizzato in cinque giornate, dalle ore 9.00 alle 17.30 con una pausa intermedia di un'ora e mezza. Al mattino verranno presentate le sessioni teoriche ed al pomeriggio ci saranno degli esercizi guidati di laboratorio. Ogni studente avrà disponibile una propria postazione informatica dotata di diversi sistemi operativi e tutto il materiale didattico, inclusi oltre 300 tool di hacking.

Esame di certificazione

Insieme al materiale didattico, ogni partecipante riceverà un voucher per sostenere l'esame di certificazione.

L'esame finale verrà condotto mediante una prova a carattere individuale basata sulla compilazione di un test di apprendimento inerenti i principali argomenti trattati durante il corso. La durata della prova è di 1 ora.

Alla fine del percorso formativo verrà rilasciato un **ATTESTATO DI FREQUENZA**.

Ottenuto l'attestato di frequenza i partecipanti potranno sostenere opzionalmente e gratuitamente un esame DI CERTIFICAZIONE UFFICIALE in una delle sedi abilitate per conseguire il certificato EC-Council CEH.

Moduli formativi

I moduli sono qui presentati a solo scopo informativo e possono subire delle variazioni senza ulteriore comunicazione.

Giornata 1

MODULO 1 – Introduzione all’Ethical Hacking

- Significato di Ethical Hacker
- Riferimenti normativi
- Ethical Hacking Agreement
- Strategie e benefici

MODULO 2 - Teoria del Penetration testing

- SLA
- NDA
- Engagement
- Report

Giornata 2

MODULO 3 – Preparazione di un client d’attacco

- Servizi su macchina attacker
- Basi di bash scripting
- Utilizzo dei tools (es. netcat)

MODULO 4 – Scanning

- Teoria dello scanning
- Utilizzo di NMAP per effettuare Portscan a Website
- Utilizzo di AngryIP per effettuare Check for Live Hosts
- Utilizzo di altri tools per la scansione di rete (Hping2, NetScan Tools Pro, SuperScan 4, ecc)

Giornata 3

MODULO 5 – Enumerazione

- Teoria dell'enumerazione
- Enumerazione passiva via Web
- Enumerazione attiva (smtp, snmp, nbt, ecc.)

MODULO 6 – Sniffing

- Teoria sul funzionamento degli apparati attivi hub/switch/router
- Utilizzo di tools tipo Wireshark
- Utilizzo di tools tipo tcpdump

Giornata 4

MODULO 7 – Attacchi

- Man in the Middle
- Exploiting (scrittura Buffer Overflow, modifica exploit pubblici, metasploit, ecc.)
- Web Hacking (sql injection, XSS, ecc.)
- Password Cracking

Giornata 5

MODULO 8 – Sicurezza fisica

- Teoria sulla sicurezza fisica
- Documentazione MIT
- Linee guida sulla sicurezza fisica

MODULO 9 – Sicurezza software

- Firewall
- Router
- Antivirus
- Proxy
- ACL

MODULO 10 – Social Engineering

- Teoria del Social Engineering
- Tipo comuni d'attacco
- Attacchi interni
- Phishing
- Online Scams
- Contromisure

Nota: il programma del Corso potrà essere adattato alle specifiche esigenze dei partecipati.

Profilo di Data Security

Data Security è una società specializzata nella gestione della sicurezza e della privacy, in grado di fornire servizi che vanno dall'analisi dei rischi fino all'implementazione e integrazione di sofisticate soluzioni tecnologiche.

Ciò che distingue in maniera significativa Data Security è la capacità di padroneggiare e integrare le componenti organizzative, normative, tecnologiche e di processo per realizzare soluzioni realmente efficaci e in sintonia con l'organizzazione e i sistemi, a costi ragionevolmente contenuti.

Di seguito si riportano i servizi tipicamente erogati da Data Security:

- analisi dei rischi e valutazione delle priorità di intervento;
- analisi costi/benefici e studi di affidabilità tecnologica e prestazionale;
- installazione e configurazione di soluzioni per il monitoraggio e la gestione degli accessi ad Internet;
- consulenza legale, tecnica e organizzativa su Sicurezza, Privacy, Autenticazione, Firma Digitale e Business Continuità;
- collaudo e certificazione dei sistemi e delle procedure di Sicurezza;
- formazione qualificata agli incaricati e ai responsabili del trattamento dei dati, sia presso le strutture didattiche di Data Security sia presso la sede del cliente;
- test di vulnerabilità dei sistemi informatici dall'esterno e dall'interno della rete;
- definizione di regolamenti e policy per la sicurezza e il corretto utilizzo delle risorse informatiche e telematiche;
- consulenza dedicata alla Pubblica Amministrazione per la redazione e l'aggiornamento del Documento Programmatico sulla Sicurezza (D.Lgs. 196/2003), per lo sviluppo del sistema di gestione della sicurezza e per l'implementazione di Firma Digitale, della Carta del Cittadino e della Carta di identità elettronica;
- progettazione di sistemi di Storage, Disaster Recovery e Business Continuity.

Tutto questo con una costante attenzione al rapporto costi/benefici delle soluzioni proposte.

Oltre a ciò Data Security è in grado di fornire, attraverso i suoi partner, le migliori soluzioni tecnologiche per la Sicurezza informatica e di integrarle con i sistemi esistenti.

Data Security si avvale della partnership tecnologica delle più importanti società mondiali nel settore della sicurezza informatica:



Il SANS Institute (System Administration, Networking and Security) è stato fondato nel 1989 come gruppo di ricerca e organizzazione educativa. Con la sua attività permette a più di 160.000 professionisti della sicurezza informatica quali analisti, amministratori di sistema e amministratori di rete, di condividere le proprie esperienze e di trovare le soluzioni ai problemi che, giorno dopo giorno, vengono riscontrati.

Alla base del SANS vi sono molti professionisti di agenzie governative, aziende e istituti universitari di tutto il mondo che investono ogni anno centinaia di ore nella ricerca e nella formazione per aiutare la comunità internazionale a risolvere i problemi della sicurezza informatica.

Data Security, in qualità di partnet, ha appena pubblicato la versione italiana della **SANS Top20 2007 Security Risks**, l'analisi delle venti maggiori vulnerabilità.

La pubblicazione è disponibile nella sezione Top 20 del sito di Data Security.

www.datasecurity.it/top20



QUALYS™

Qualys, Inc., leader nei sistemi gestiti per il Vulnerability Assessment, permette ai professionisti della sicurezza e alle aziende di analizzare automaticamente le reti connesse ad Internet e rilevarne le vulnerabilità. Qualys fornisce inoltre servizi avanzati di security auditing e risk assessment di reti. Data Security offre l'opportunità di verificare l'integrità delle proprie rete e sistema informatico con l'esecuzione di un test on line che genererà, quale output, un accurato report.

Un test gratuito, volto a saggiare la solidità dei propri sistemi rispetto alle Top20, è disponibile ed eseguibile all'indirizzo:

www.datasecurity.it/top20



nCipher è un'azienda leader nel settore della protezione dei sistemi crittografici specializzata nello sviluppo di soluzioni per il miglioramento in termini di sicurezza e di prestazioni delle transazioni basate su crittografia. La partnership con nCipher consente a Data Security di offrire al mercato italiano una componente fondamentale della sicurezza oggi, imprudentemente troppo spesso trascurata.