Incontro di lavoro sul tema : "Sicurezza Informatica"

Interventi della giornata (13 Novembre 2003)

(URL: http://its.isti.cnr.it/Doc/documentazione.html)

Programma

Sicurezza informatica: Principi base
Introduzione generale al problema "Sicurezza"

- **Politiche di sicurezza sugli apparati di rete:**
  L'esperienza dell'area della Ricerca di Pisa
- **Certificazione digitale e PKI:**
  Le iniziative dell'istituto di Informatica e Telematica
- **La sicurezza dei dati in ambiente clinico:**
  L'esperienza dell'Istituto di fisiologia Clinica
- **Trend Micro Enterprise Protection Strategy**
  Strumenti e strategie a supporto della sicurezza

Obiettivo dell'incontro

- **Promuovere la sensibilizzazione alla cultura della sicurezza informatica**
- **Evidenziare i diversi aspetti della sicurezza informatica**
- **Presentare alcune soluzioni/prodotti commerciali proposti da "Trend Micro" per la sicurezza di sistemi connessi in rete**

Agenda

- **Sicurezza informatica: Principi base**

CARLO CARLESI (ISTI)

Responsabile per le "Politiche di Sicurezza" dell'Istituto di Scienza e Tecnologie dell'Informazione "A. Faedo"

- **Concetti generali e aspetti della sicurezza**
  - **Cosa e' la sicurezza informatica, quali sono gli obiettivi, perche' e ' necessaria**
  - **Cosa sono gli incidenti informatici, come si fronteggiano**
  - **Leggi vigenti in materia e le misure minime di sicurezza da osservare**

Agenda

- **Politiche di sicurezza sugli apparati di rete**
  L'esperienza dell'area della Ricerca di Pisa

Dott. Marco Sommani (IIT)

Responsabile del servizio "Reti" dell'Istituto di Informatica e Telematica"

Responsabile della progettazione e gestione della rete dell' Area della Ricerca di Pisa

Membro del Comitato di gestione rete CNR

Membro del Comitato Tecnico Scientifico Consortium GARR

- organizzazione del routing IP in Area
- uso dei router per il controllo e il monitoraggio del traffico
- esperienze maturate attraverso la gestione della rete dell'Area

Agenda

- **Certificazione digitale e PKI**
  Le iniziative dell'istituto di Informatica e Telematica

Ing. Anna Vaccarelli (IIT)

Responsabile della Sezione di Ricerca "Sicurezza dell'Informazione" dell'Istituto di Informatica e Telematica

Membro del consiglio direttivo di Assosecurity

- Nel seminario vengono fornite alcune nozioni di base sugli algoritmi di crittografia e viene descritta la tecnologia della firma digitale. Viene quindi illustrata la funzione delle Public Key Infrastructure (PKI), deputate a rilasciare e gestire certificati digitali, necessari per l'apposizione della firma digitale

Agenda

- **La sicurezza dei dati in ambiente clinico**

  L'esperienza dell'Istituto di fisiologia Clinica

  Dott. Raffaele Conte (IFC)

  Responsabile dei servizi di rete per l'Istituto di Fisiologia Clinica
  Partecipa al progetto "Firma Digitale" in collaborazione con l'IIT per l'applicazione di tale tecnologia ai referti clinici.

  – Saranno discusse le problematiche relative alla sicurezza in ambito sanitario ed in particolare la strategia adottata dall'Istituto nell'affrontare il problema di coniugare l'attivita' di ricerca (tipicamente "*aperta*") con l'attivita' assistenziale (necessariamente "*chiusa*" per la presenza di dati sensibili).

Agenda

- **Trend Micro Enterprise Protection Strategy**

  Strumenti e strategie a supporto della sicurezza

  Dott. Tiberio Molino (Trend Micro spa)

  – **Presentazione multimediale di alcune soluzioni e prodotti "Trend Micro" per la sicurezza dei sistemi informatici.**

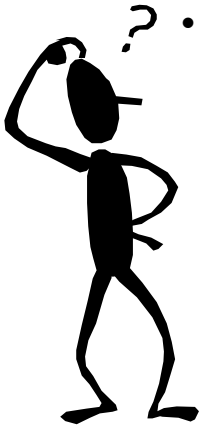
Incontro di lavoro sulla Sicurezza Informatica

Sicurezza Informatica: Principi base

Carlo Carlesi

Istituto di Scienza e Tecnologie dell'Informazione
"Alessandro faedo"

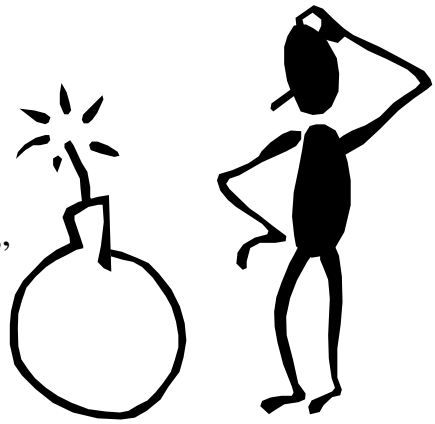
Principi base



- Introduzione alle problematiche di sicurezza informatica
  - Cosa e' la "Sicurezza"
  - Obiettivi della "Sicurezza"
  - Come si attua la "Sicurezza"
  - Perche' la "Sicurezza" e' necessaria
  - Quando la "Sicurezza" e' un obbligo

Concetto di sicurezza

Nel linguaggio corrente per sicurezza si intende una "misura di protezione" e si definisce sicuro "cio' che e' esente da pericoli"



Sicurezza informatica

- Standard ISO e ISO17799
  - Un sistema informatico e' considerato sicuro **quando** e' in grado di garantire determinati requisiti di sicurezza in termini di
    - Disponibilita'
    - Integrita'
    - Riservatezza
    - Autenticita' e non ripudio

Requisiti

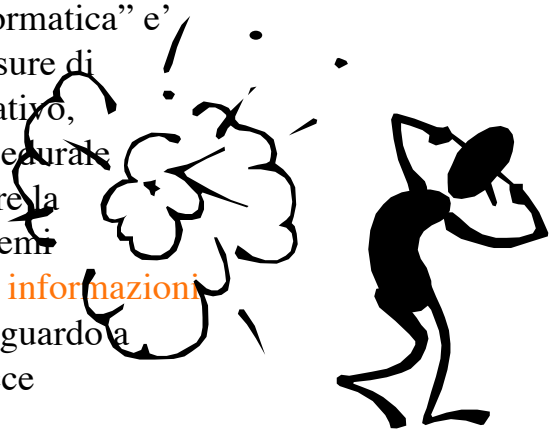
- Requisisto di disponibilita'
  - Il sistema deve garantire la disponibilita' delle informazioni a ciascun utente autorizzato nei modi e nei tempi previsti (politiche aziendali)
- Requisito di integrita'
  - Il sistema deve impedire e comunque rilevare alterazione dirette o indirete delle informazioni da parte di utenti o procedure non autorizzati o a causa di eventi accidentali

Requisiti

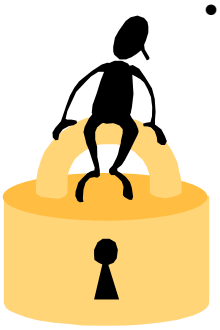
- Requisito di riservatezza
  - Nessun utente deve poter acquisire o dedurre, dal sistema, informazioni che non e' autorizzato a conoscere
- Requisito di autenticita' e non ripudio
  - Avere la certezza che una data informazione appartenga da chi dice di averla generata (autenticita')
  - Chi ha generato una data informazione non deve poter negare di averlo fatto (non ripudio)

Cosa e' la sicurezza

- La "Sicurezza Informatica" e' l'insieme delle misure di carattere organizzativo, tecnologico e procedurale mirate ad assicurare la protezione dei sistemi informatici e delle informazioni in essi contenuti riguardo a determinate minacce



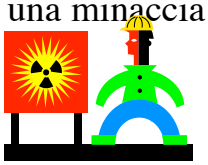
Principi base



- Introduzione alle problematiche di sicurezza informatica
  - Cosa e' la "Sicurezza"
  - Obiettivi della "Sicurezza"
  - Come si attua la "Sicurezza"
  - Perche' la "Sicurezza" e' necessaria
  - Quando la "Sicurezza" e' un obbligo

Obiettivi della sicurezza

- Obiettivo principale della sicurezza informatica e' quello di proteggere i "beni informatici"
  - **Riducendo i rischi**, a cui sono esposti
  - **Limitando gli effetti** causati dall'eventuale occorrenza di una minaccia (rischio residuo)



Beni informatici

- Sistemi + Informazioni + Servizi

- Sistemi (Hardware & Software)
  - Personal computer, workstation, server, main frame, supporti di memorizzazione
  - Apparecchiature di rete (locali e geografiche), sistemi di comunicazione elettronica, router, switch

- Informazioni
  - Banche dati e documenti digitali
    - » Dati memorizzati su supporti elettronici
  - Dati in transito sui sistemi di comunicazione

Servizi
  - Posta elettronica
  - Sportelli elettronici (accessi)

Rischi & Minacce

- Possibili condizioni, azioni o eventi in grado di modificare o alterare le normali funzionalita' di un sistema
- Minacce:
  - Guasti hardware
  - Errori Software
  - Errori umani
  - Cause accidentali ed imprevedibili (allagamenti, incendi, black-out etc)
  - Vulnerabilita' (di infrastruttura, di progetto, di sistema, rete)

- La sicurezza totale nella realta' e' un'astrazione

  Non esiste un sistema informatico totalmente sicuro

Le minacce della rete

- Virus
  - Programmi maliziosi che attaccano una macchina normalmente a seguito di un intervento umano come l'apertura di un allegato di posta, l'inserimento e la lettura di un floppy disk etc.
- WORM (Verme strisciante)
  - Simili ai virus, una volta lanciati, attaccano una macchina sfruttando le vulnerabilita' note e in caso di successo tentano di duplicarsi automaticamente passando ad attaccare altri sistemi in modo incontrollato
- Intrusioni
  - Accesso ed uso non autorizzato di un sistema

Vulnerabilita'

- Windows Systems (Sans Institute 8-10-03)
  1. Internet Information Services (IIS)
  2. Microsoft SQL Server (MSSQL)
  3. Windows Autentication
  4. Internet Explorer
  5. Windows Remote Access Services
  6. Microsoft Data Access Components (MDAC)
  7. Windows Scripting Host (WSH)
  8. Microsoft Outlook and Outlook Express
  9. Windows Peer to Peer File Sharing (P2P)
  10. Simple Network Management Protocol (SNMP)

Vulnerabilita'

- UNIX Systems (Sans Institute 8-10-03)
  1. BIND Domain Name System
  2. Remote Procedure Calls (RPC)
  3. Apache Web Server
  4. General unix Authentication Accounts (with No Passwords or Weak Passwords)
  5. Clear Text Services
  6. Sendmail
  7. Simple Network Management Protocol (SNMP)
  8. Secure Shell (SSH)
  9. Misconfiguration of Enterprise Services NIS/NFS
  10. Open Secure Sockets Layer (SSL)

Principi base

- Introduzione alle problematiche di sicurezza informatica
  - Cosa e' la "Sicurezza"
  - Obiettivi della "Sicurezza"
  - Come si attua la "Sicurezza"
  - Perche' la "Sicurezza" e' necessaria
  - Quando la "Sicurezza" e' un obbligo

Come si attua la sicurezza

- Programma generale di gestione della sicurezza
  - Esprime la volonta' dell'istituzione di perseguire la sicurezza
- Politica della sicurezza
  - Promuove, e individua i criteri generali di sicurezza indipendenti dalla tecnologie in uso e in linea con la "missione istituzionale"
  - Definisce ed assegna in modo chiaro ruoli e responsabilita'
  - Pianifica e provvede le risorse necessarie
- Gestione dei rischi
  - Valutazione periodica dei rischi e identificazione dei beni critici
- Piano opertivo della sicurezza
  - Sviluppa, e applica le misure di sicurezza per l'attuazione della politica

Come si attua la sicurezza

- Controllo e Gestione dei Sistemi & Rete
  - Controllo degli accessi via rete (utenti e procedure/protocolli)
  - Verifica dell'integrita' dei programmi software
  - Aggiornamento e manutenzione dei sistemi
  - Mantenimento regolare delle copie di dati e del software
- Sicurezza fisica
  - Controllo degli accessi fisici alle informazione e a tutti i servizi e risorse informatiche
- Autenticazione & Autorizzazioni
  - Implementazione dei meccanismi di autenticazione e autorizzazione degli accessi a qualsiasi risorsa disponibile, sia dall'interno che dall'esterno dell'organizzazione

Come si attua la sicurezza

- Monitoraggio & Controllo
  - Registrazione e controllo degli accessi e autorizzazioni, verifica della configurazione dei sistemi e rilevamento vulnerabilita'
- Piano di Continuita' Operativa & Recupero (Disaster Recovery)
  - Protezione e garanzia della continuita' dei servizi critici, limitazione dell'impatto degli incidenti
  - Procedure organizzative, normative e risorse per il ripristino di informazioni, servizi e sistemi
- Responsabilita' individuale e formazione
  - Ogni utente deve essere educato e informato sulle politiche di sicurezza e sui rischi connessi alla propria attivita'

Politica della sicurezza GARR

- GARR Acceptable Use Policy (AUP)
  e' il documento che esprime la politica di utilizzo ed accesso alla Rete Italiana dell'Universita' e della Ricerca Scientifica (gestita da INFN dal 1998)
  - Il documento cita : *"L'accesso alla rete GARR e' condizionato all'accettazione integrale delle norme contenute in questo documento."*
- 13 Novembre 2002: Si e' costituito il nuovo organismo autonomo "Consortium GARR" per l'attuazione e gestione della nuova rete ad alta velocita' (Garr-G)

Proteggere il proprio PC

- Suggerimenti base

1. Installare ed usare un programma Anti-Virus
2. Fare attenzione alle E-mail con allegati
3. Mantenere il sistema aggiornato
4. Proteggere l'accesso al pc con password non banali
5. Mantenere copie di Cartelle e File importanti

Proteggere il proprio PC

- Suggerimenti avanzati

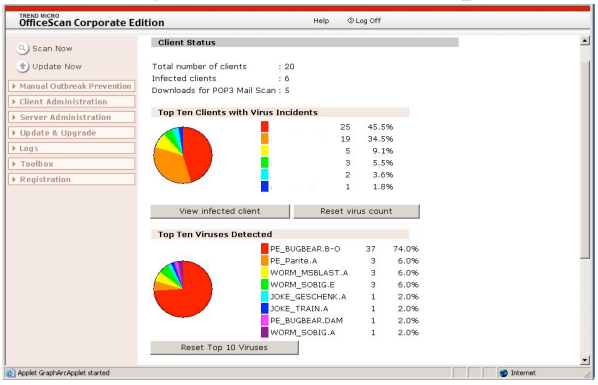
5. Installare ed utilizzare un programma di Personal-Firewall
6. Fare attenzione ai programmi che si installano scaricandoli dalla rete
7. Installare ed utilizzare programmi di controllo degli accessi e di crittografia

Proteggere il proprio PC

- Cosa non fare
  - Non lasciare il proprio pc incustodito (attivare un salva schermo con password)
  - Non lasciare la password scritta su un"post-it" attaccato allo schermo
  - Non istallare programmi di tipo "sniffer" che violano norme etiche e legislative

Antivirus

- Programma di gestione antivirus in prova all'ISTI



Principi base

- Introduzione alle problematiche di sicurezza informatica
  - Cosa e' la "Sicurezza"
  - Obiettivi della "Sicurezza"
  - Come si attua la "Sicurezza"
  - Perche' la "Sicurezza" e' necessaria
  - Quando la "Sicurezza" e' un obbligo

Perche' la sicurezza

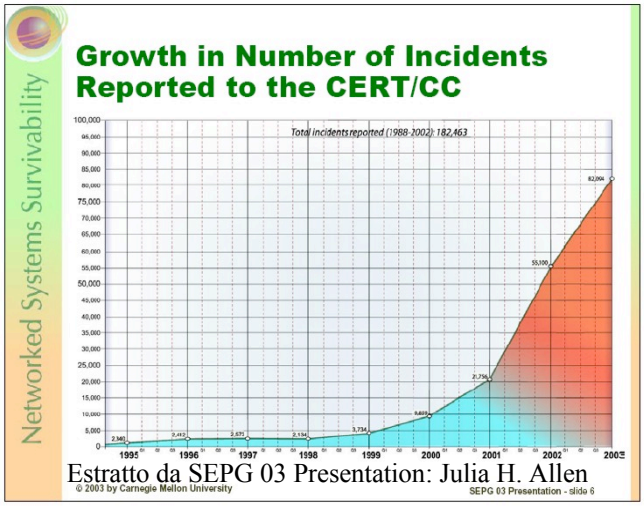
- Limitare i danni e i costi causati dagli incidenti informatici
- Proteggere conservare ed accrescere la qualita' del patrimonio informativo aziendale
- Garantire il rispetto delle disposizioni legislative in materia
- Preservare l'immagine e la missione istituzionale

Incidenti Informatici

- Definiamo incidente informatico qualunque azione o concomitanza di eventi accidentali e/o volontari che porti alla violazione dei requisiti di:
  - Disponibilita'
    - Interruzione non autorizzata totale o parziale di servizi (DOS)
  - Integrita'
    - Perdita di informazioni o modifica non autorizzata di dati
  - Riservatezza
    - Accesso a sistemi (Intrusione) o intercettazione di dati non autorizzato
  - Uso improprio e non autorizzato di risorse informatiche
    - Falsificazione di identita' o di documenti
    - Invio non autorizzato di e-mail (SPAM) (*)

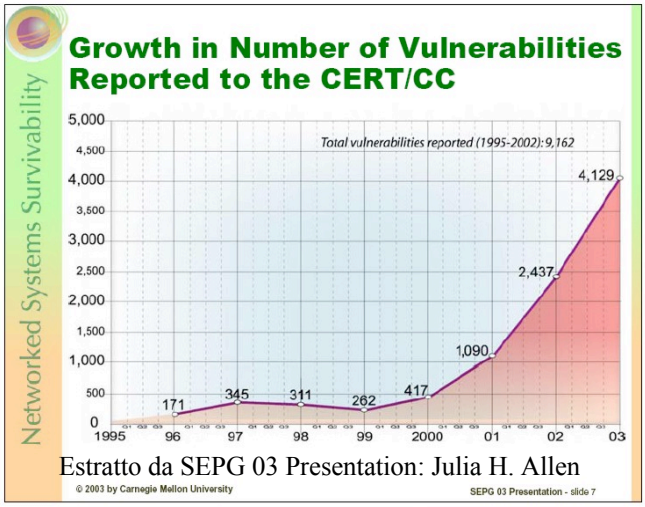
Andamento incidenti

Andamento Incidenti



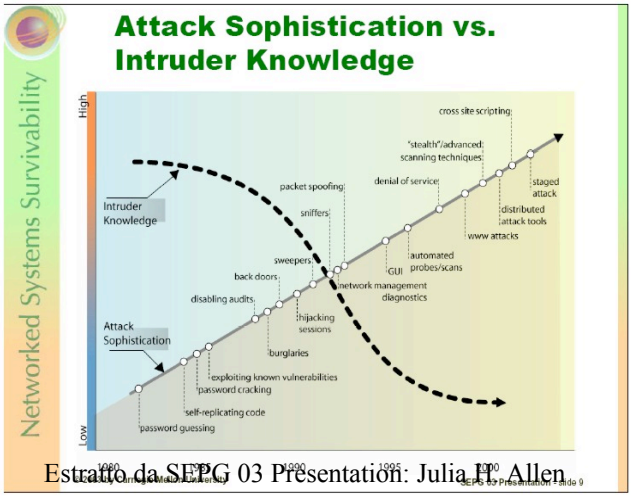
Estratto da SEPG 03 Presentation: Julia H. Allen

Vulnerabilità



Estratto da SEPG 03 Presentation: Julia H. Allen

Hacker & Tecnologie



Estratto da SEPG 03 Presentation: Julia H. Allen

Tipologie di attacco ai sistemi

- a) *Accesso non autorizzato ai sistemi di informazione*.
  - Questo tipo di attacco, puo' avere la finalita' di copiare, modificare o distruggere dati, oppure di accedere a servizi con accesso condizionato. Molto spesso, tuttavia, si riscontrano intrusioni anche su macchine che non contengono dati sensibili e di particolare valore, solo per poterle utilizzare in attacchi ad altri obiettivi e rendere il piu' difficile possibile risalire all'attaccante. Le tecniche di intrusione vanno dallo sfruttamento di informazioni interne, all'intercettazione di password di accesso o allo sfruttamento di "bachi" software di talune applicazioni (buffer overflow, etc).

Tipologie di attacco ai sistemi

- b) *Interruzione del funzionamento dei sistemi di informazione*
  - Questo tipo di attacco, comunemente indicato come "denial of service" (DoS), mira principalmente ad interrompere l'erogazione dei servizi del sistema attaccato. Ci sono parecchi modi di portare questo tipo di attacco, tra cui quello di saturare il sistema attaccato mediante l'invio continuo e ripetuto di richieste ad opera di piu' sistemi contemporaneamente (molto spesso a loro volta compromessi per questo scopo), o attraverso la distruzione di dati e o parti di programmi del sistema attaccato.

Tipologie di attacco ai sistemi

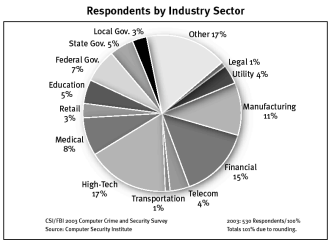
- c) *Esecuzione di software "maligni" che modificano o distruggono i dati*.
  - Questo tipo di attacco generalmente noto con il nome di "virus", e condotto molto spesso atrraverso il servizio di posta eletrronica, e' tra i piu' diffusi proprio perche' ha la finalita' di replicarsi a macchia d'olio da un sistema all'altro. Ci sono "virus" che creano disfunzioni ma non danneggiano in modo irreversibile il sistema colpito, altri che invece distruggono dati e sistema operativo e talvolta creano anche guasti hardware.

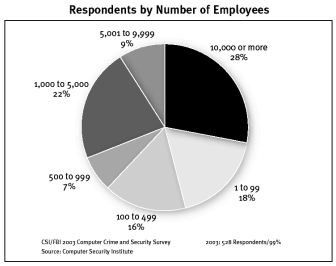
Tipologie di attacco ai sistemi

- d) *Intercettazione di comunicazioni e falsificazione della propria identita'*.
  - L'intercettazione dolosa delle comunicazioni ("sniffing"), oltre a compromettere la riservatezza dei dati utente e' spesso utilizzata per ottenere informazioni da utilizzare a fini dolosi, come l'usurpazione dell'identita' di un soggetto ("spoofing") o l'acquisizione di password di accesso su altri sistemi.

Statistiche 2003

- Studio a cura del
  Computer Security Institute e
  Federal Bureau of Investigation's
  di S. Francisco
  CSI/FBI
  - Risposte basate su un campione di 530 aziende praticanti la sicurezza informatica





Statistica CSI/FBI - 1

Tecnologie di sicurezza utilizzate

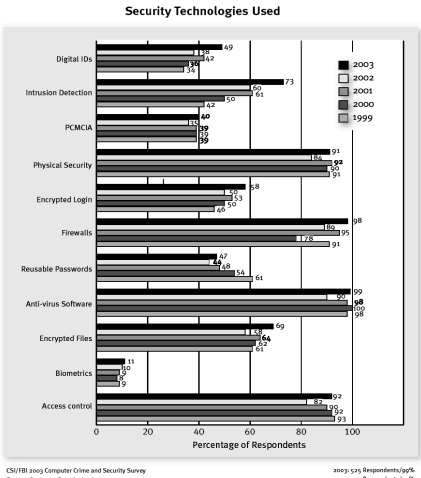
Risposte 99% (525/530)

antivirus 99%

firewalls 98%

sicurrezze fisiche 91%

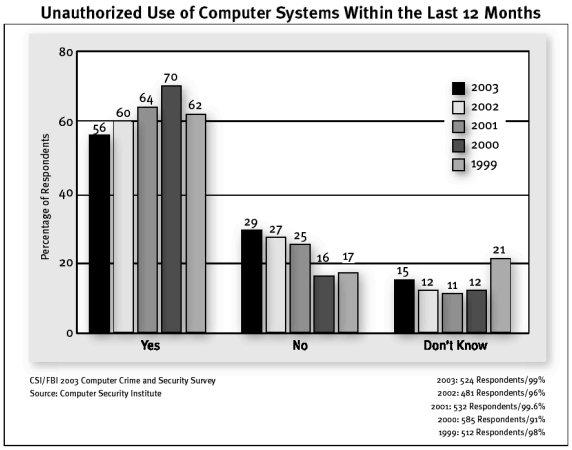
controllo accessi 92%



Statistica CSI/FBI - 2

Uso improprio di risorse

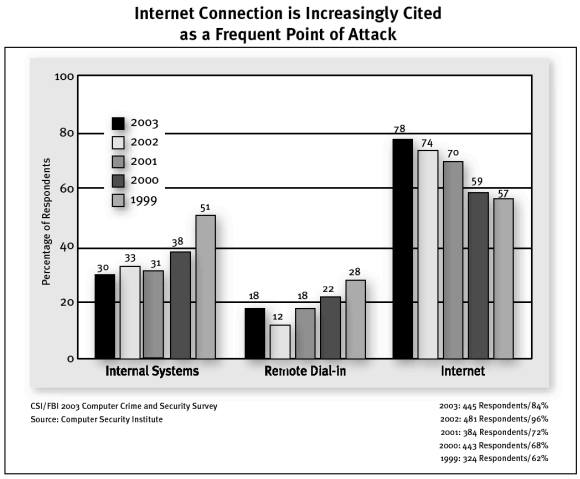
Risposte 99% (524/530)



Statistica CSI/FBI - 3

Provenienza attacchi

Risposte 84% (524/530)



Statistica CSI/FBI - 4

Tipologie di attacchi rilevati

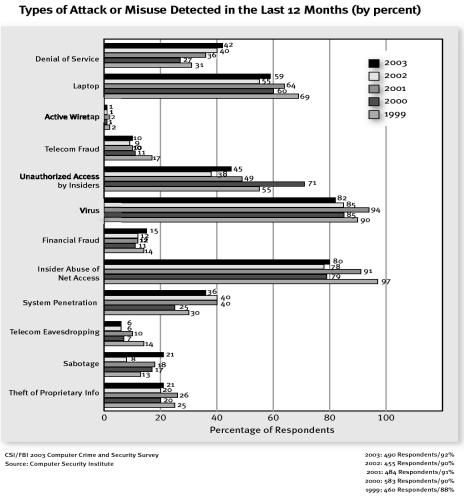
Risposte 92% (490/530)

virus 82%

DOS 42%

Accessi non aut. 45%

Intrusioni 36%



Statistica CSI/FBI - 7

The Cost of Computer Crime

The following table shows the aggregate cost of computer crimes and security breaches over a 48-month period

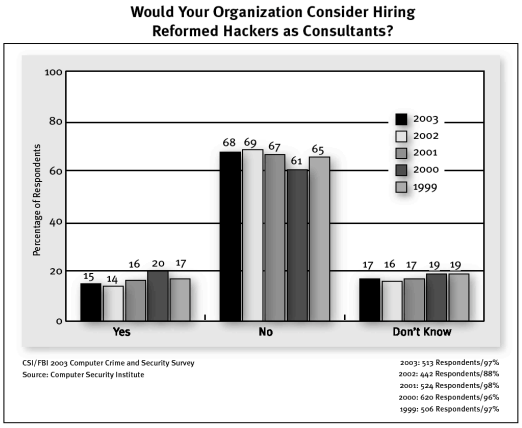
In 2003, 75% of our survey respondents acknowledged financial losses, but only 47% could quantify the losses.

How Money Was Lost

	Lowest Reported				Highest Reported				Average Losses				Total Annual Losses			
	00	01	02	03	00	01	02	03	00	01	02	03	00	01	02	03
Theft of proprietary info.	$1K	$100	$1K	$2K	$25M	$50M	$50M	$35M	$3,032,818	$4,447,900	$6,571,000	$2,699,842	$66,708,000	$151,230,100	$170,827,000	70,195,900
Sabotage of data of networks	1K	100	1K	500	15M	3M	10M	2M	969,577	199,350	541,000	214,521	27,148,000	5,183,100	15,134,000	5,148,500
Telecom eavesdropping	200	1K	5K	1K	500K	500K	5M	50K	66,080	55,375	1,205,000	15,200	991,200	886,000	346,0000	76,000
System penetration by outsider	1K	100	1K	100	5M	10M	5M	1M	244,965	453,967	226,000	56,212	7,104,000	19,066,600	13,055,000	2,754,400
Insider abuse of Net access	240	100	1K	100	15M	10M	10M	6M	307,524	357,160	536,000	135,255	27,984,740	35,001,650	50,099,000	11,767,200
Financial fraud	500	500	1K	1K	21M	40M	50M	4M	1,646,941	4,420,738	4,632,000	328,594	55,996,000	92,935,500	115,753,000	10,186,400
Denial of service	1K	100	1K	500	5M	2M	50M	60M	108,717	122,389	297,000	1,427,028	8,247,500	4,283,600	18,370,500	65,643,300
Virus	100	100	1K	40	10M	20M	9M	6M	180,092	243,835	283,000	199,871	29,171,700	45,288,150	49,979,000	27,382,340
Unauthorized insider access	1K	1K	2K	100	20M	5M	1.5M	100K	1,124,725	275,636	300,00	31,254	22,554,500	6,064,000	4,503,000	406,300
Telecom fraud	1K	500	1K	100	3M	8M	100K	250K	212,000	502,278	22,000	50,107	4,028,000	9,041,000	6,015,00	701,500
Active wiretapping	5M	0	0	5K	5M	0	0	700K	5M	0	0	352,500	5,000,000	0	0	705,000
Laptop theft	500	1K	1K	2400	1.2M	2M	5M	2M	58,794	61,881	89,000	47,107	10,404,300	8,849,000	11,766,500	6,830,500
											Total Annual Losses		265,337,990	377,828,700	455,848,000	201,797,340

CSI/FBI 2003 Computer Crime and Security Survey
Source: Computer Security Institute

Statistica CSI/FBI - 5



Costi della sicurezza

- La sicurezza ha certamente un **costo**
  - Hardware dedicato
  - Software commerciale
  - Costo di progettazione, manutenzione e gestione
  - Riduzione di produttivita' (nuovi vincoli)
  - Formazione del personale
- La **non sicurezza** ha ugualmente un **costo non sempre valutabile**
- Adottare misure di sicurezza non è solo una necessità, ma in alcuni casi un obbligo di legge
  (Codice in materia di protezione dei dati personali)

Gestione Incidenti

- CERT Coordination Center - Organizzazione costituita presso il Software Engeneering Institute (SEI) della Carnegie Mellon University
  - Nata con il compito di coordinare ed assistere gli utenti della rete ad affrontare e rispodere ad un eventuale incidente
  - E' composta da tre gruppi con compiti diversi ma in stretta relazione tra loro:
    - **Operativo**: punto di contatto, assistenza tecnica telefonica, risposta all'incidente e gestione degli archivi delle vulnerabilità, pubblicazione di bollettini circa le vulnerabilità;
    - **Formazione**: aiuto nella creazione di gruppi di risposta, formazione degli utenti, rilascio di documentazione tecnica e dei bollettini forniti dai produttori, organizzazione di seminari;
    - **Ricerca e sviluppo**: creazione di sistemi sicuri, ricerca nel campo della sicurezza, sviluppo di strumenti per la sicurezza

La situazione italiana

In Italia sono attivi diversi CERT:

- **CERT-IT**: http://security.dsi.unimi.it/index.html
  - E' stato creato nel Febbraio 1994 da un gruppo di persone appartenenti allo staff tecnico del Dipartimento di Scienze dell'Informazione dell'Università di Milano. Nel 1995 è entrato a far parte del FIRST;

- **GARR-CERT**: http://www.cert.garr.it/
  - Scopo del servizio è la gestione degli incidenti in cui siano coinvolti enti collegati alla rete GARR;

La situazione italiana

- **IRItaly**: http://www.iritaly.org/
  - IRItaly (Incident Response Italy) è un progetto nato presso il Dipartimento di Tecnologie dell'Informazione dell'Università Statale di Milano, Polo Didattico e di Ricerca di Crema. Lo scopo principale è informare e sensibilizzare la comunità scientifica italiana, le aziende piccole e grandi, gli attori privati e pubblici sui temi dell'Incident Response;
- **SEC-CERT**: http://www.securegroup.it/sec.htm
  - Il primo CERT privato italiano. E' in attesa della comunicazione di ammissione al FIRST
- SSG - Security Service Group Università di Salerno.

Principi base

- Introduzione alle problematiche di sicurezza informatica
  - Cosa e' la "Sicurezza"
  - Obiettivi della "Sicurezza"
  - Come si attua la "Sicurezza"
  - Perche' la "Sicurezza" e' necessaria
  - Quando la "Sicurezza" e' un obbligo

Contesto normativo di riferimento

- Quattro leggi fondamentali costituiscono la griglia di riferimento normativo (fino al 31 12 2003).
  - Dlgs n. 518 del 1992 che modifica il regio decreto n. 633 del 1941, relativo al diritto di autore, integrandolo con norme relative alla tutela giuridica dei programmi per elaboratore.
  - Legge n. 547 del 1993 che modifica il codice penale italiano introducendo i cosidetti "computer crimes".
  - Legge n. 675 del 1996 che disciplina il trattamento dei dati personali.
  - D.P.R. n. 318 del 28 luglio 1999 "Regolamento recante norme per l'individuazione delle misure minime di sicurezza per il trattamento dei dati personali, a norma dell'articolo 15 , comma 2, della legge n.675 del 1996"

Testo Unico

- Il Codice in Materia di Protezione dei Dati Personali entrerà in vigore dal 1/1/04 abrogando la L.675/96 e il DPR.318/99
  - Il nuovo Testo Unico raccoglie l'esperienza passata introducendo un numero esteso di norme (spesso derivanti da determinazioni del Garante), Codici Deontologici e tutta una serie di casi particolari

Testo Unico

- Il DPR 318/99 è sostituito dal Disciplinare Tecnico (Allegato B) che introduce alcune interessanti modifiche rispetto al passato.
- Introduce il "principio di necessita'"
- Rafforza gli :
  - "Obblighi di sicurezza"
  - "Misure minime"

Testo Unico

- PARTE I DISPOSIZIONI GENERALI
  TITOLO I PRINCIPI GENERALI
  - ART. 1 DIRITTO ALLA PROTEZIONE DEI DATI PERSONALI
  - ART. 2 FINALITA'
  - ART. 3 PRINCIPIO DI NECESSITA' NEL TRATTAMENTO DEI DATI
  - ART. 4 DEFINIZIONI
  - ART. 5 OGGETTO ED AMBITO DI APPLICAZIONE
  - ART. 6 DISCIPLINA DEL TRATTAMENTO

Testo Unico

- Art. 3 (Principio di necessità nel trattamento dei dati)
  - 1. I sistemi informativi e i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità.

Testo Unico

- Art. 31 (Obblighi di sicurezza)
  - • 1. I dati personali oggetto di trattamento sono **custoditi e controllati**, anche in relazione alle conoscenze acquisite **in base al progresso tecnico**, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante **l'adozione di idonee e preventive misure di sicurezza**, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

Testo Unico

- Art. 33 (Misure minime)
  - 1. Nel quadro dei più generali obblighi di sicurezza di cui all'articolo 31, o previsti da speciali disposizioni, i titolari del trattamento sono comunque tenuti ad adottare le misure minime individuate nel presente capo o ai sensi dell'articolo 58, comma 3, volte ad **assicurare un livello minimo di protezione dei dati personali**.

Testo Unico

- Art. 34 (Trattamenti con strumenti elettronici)
  - 1. Il trattamento di dati personali effettuato con strumenti elettronici è consentito solo se sono adottate, nei modi previsti dal disciplinare tecnico contenuto nell'**allegato B**), le seguenti misure minime:
    - a) autenticazione informatica;
    - b) adozione di procedure di gestione delle credenziali di autenticazione;
    - c) utilizzazione di un sistema di autorizzazione;
    - d) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;

Testo Unico

- Art. 34 (..segue)
  - 1. Il trattamento (…) è consentito solo se sono adottate (…) le seguenti misure minime:
    - e) protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;
    - f) adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi;
    - g) tenuta di un aggiornato documento programmatico sulla sicurezza;
    - h) **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.**

Testo Unico

- ILLECITI PENALI

ART. 167 TRATTAMENTO ILLECITO DI DATI
ART. 168 FALSITA' NELLE DICHIARAZIONI E NOTIFICAZIONI AL GARANTE
ART. 169 MISURE DI SICUREZZA
ART. 170 INOSSERVANZA DI PROVVEDIMENTI DEL GARANTE
ART. 171 ALTRE FATTISPECIE
ART. 172 PENE ACCESSORIE

Conclusione

- Formazione e Cultura: possono contribuire a trasformare la sicurezza da costo a investimento
  - Educare gli utenti all'adozione di misure di sicurezza
    - comprendere le vulnerabilità, i pericoli, i rischi che si corrono utilizzando servizi in rete e le possibili soluzioni
    - proteggere, conservare ed accrescere il patrimonio informativo aziendale
  - Formare nuove figure professionali di addetti alle misure di sicurezza
    - raggiungere e garantire adeguati assetti di sicurezza logica, fisica e organizzativa,
    - prevenire maggiormente gli abusi, le frodi e gli incidenti ai danni dei sistemi informativi o fatti attraverso i sistemi informatici
    - proteggere, conservare ed accrescere la **qualita'** del patrimonio informativo aziendale