



# **Adaptive Security Management**

## *Un Modello Adattativo per la Gestione della Sicurezza*

Questo documento contiene informazioni proprietarie coperte da copyright. Tutti i diritti sono riservati. Nessuna parte di questo documento può essere riprodotta o fotocopiata senza il preventivo consenso di Primeur e di Primeur IT Security ..

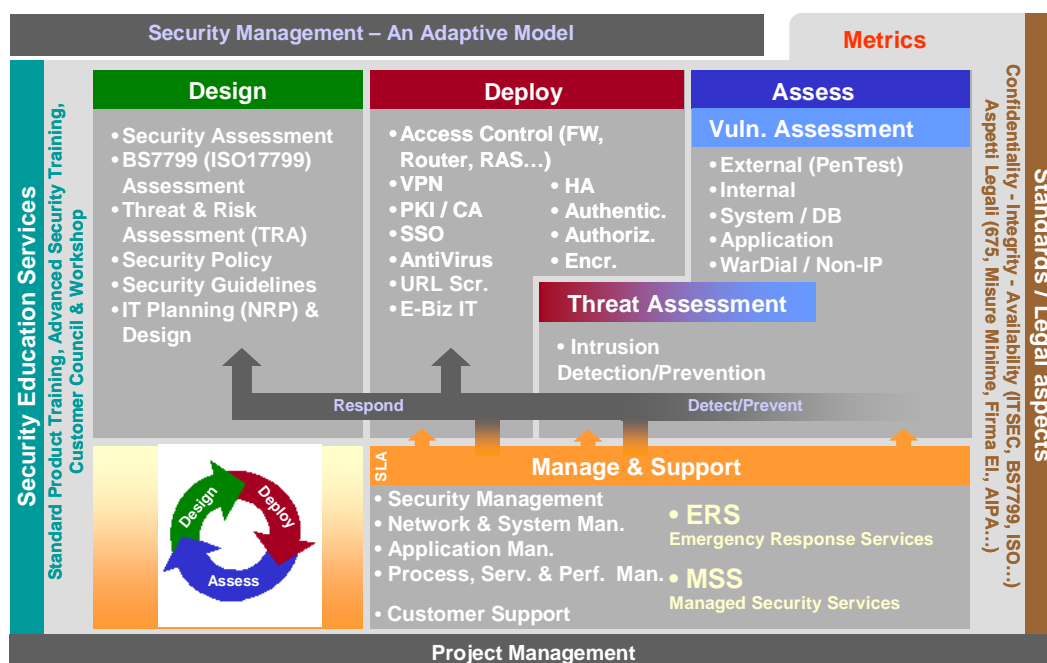


## Sommario

<b>Adaptive Security Management .....</b>	<b>2</b>
Documenti di Riferimento .....	4
Definizioni.....	5
Acronimi e parole Inglesi.....	6
<b>Security Assessment.....</b>	<b>7</b>
Descrizione .....	7
BS 7799 / ISO 17799 .....	13
Threat & Risk Assessment .....	14
RFC 2196.....	14
ICSA.....	16
Riferimenti Legislativi Italiani ed Europei .....	16
Documentazione prodotta .....	20
Pre-requisiti, vincoli e limitazioni.....	20
Deliverables.....	20
Opzioni.....	20
<b>External Security Auditing.....</b>	<b>21</b>
Esecuzione per fasi del Test .....	21
Documentazione prodotta .....	22
Prodotti e strumenti utilizzati .....	22
WarDial .....	23
External Web Application Assessment .....	24
Pre-requisiti, vincoli e limitazioni.....	25
Deliverables.....	26
Opzioni.....	27
Servizi .....	27
<b>Internal Security Auditing.....</b>	<b>28</b>
Documentazione prodotta .....	28
Prodotti e strumenti utilizzati .....	28
Internal Web Application Assessment .....	28
Pre-requisiti, vincoli e limitazioni.....	30
Deliverables.....	30
Opzioni.....	31
Servizi .....	31
<b>System/DataBase Security Auditing .....</b>	<b>32</b>
Documentazione prodotta .....	32
Prodotti e strumenti utilizzati .....	32
<b>Intrusion Detection.....</b>	<b>33</b>
Prodotti utilizzati.....	34
Pre-requisiti, vincoli e limitazioni.....	35
Deliverables.....	35
Nota.....	35
Opzioni.....	36

## Adaptive Security Management

Nuove strategie e tecnologie, nuovi interlocutori e nuove relazioni richiedono più flessibilità e adattabilità alle organizzazioni di oggi. Un'infrastruttura di Information Technology (IT) è caratterizzata da elevata turbolenza ed obsolescenza, e le sue componenti (Reti, Sistemi, Dati e Applicazioni) sono in continua evoluzione. Ciò accade anche per le vulnerabilità di queste componenti, nonché per le minacce alle quali esse sono sottoposte. Nuove vulnerabilità nel Software di base o applicativo vengono scoperte ogni giorno, assieme ai metodi e agli strumenti per sfruttarle a fini illeciti, mentre le minacce si moltiplicano con il crescere dell'utilizzo di infrastrutture pubbliche (come Internet o la rete telefonica) e del valore delle risorse su esse attestata.



**Figura 1**

È necessario quindi non solo gestire, bensì anche rivedere e **misurare** l'infrastruttura di Sicurezza (o meglio: l'intera Infrastruttura IT) nel corso del tempo. Aumentando la complessità di queste relazioni aumenta anche la necessità di esperienza esterna per comprenderne tutte le implicazioni. Infatti, come detto sopra:

- Reti, Sistemi, Dati e Applicazioni sono estesi e complessi, cambiano rapidamente e sono per loro natura affetti da vulnerabilità (vulnerabilities) e sottoposti a minacce (threats) in continua evoluzione. Ciò assume rilevanza sempre maggiore con le nuove Infrastrutture di E-Business.
- Conoscenza ed esperienza radicate nel tempo sono importanti (know-how, background tecnologico, legislazione, enti nazionali ed internazionali, underground ecc.)



- Raccogliere dati è facile, l'analisi e l'integrazione sono più difficili (e richiedono tempo).

Un'Infrastruttura di Sicurezza non può quindi essere considerata come statica: deve essere adottato un Modello **dinamico** (adattativo) per la sua gestione. Alla sua tradizionale parte implementativa (al centro nella Figura 1), mirata solitamente alla cosiddetta "difesa perimetrale", devono essere aggiunte le fasi di Pianificazione (Design, a sinistra nella Figura 1) e di Monitoraggio delle minacce e delle vulnerabilità (Assess, a destra nella Figura 1). Quest'ultima costituisce l'elemento abilitatore del processo di iterazione (freccia grigio scuro Detect/Respond nella Figura 1) che produce le azioni correttive verso le altre fasi.

Questo processo deve infine essere gestito (anche in **OutSourcing**) con i corretti metodi e strumenti (Manage & Support nella Figura 1), e deve comunque soddisfare i Requisiti base proposti dagli Standard (anche di Certificazione) esistenti.

Nella fase di Design vengono enunciati e formalizzati i principi, le politiche e le linee guida che caratterizzano i processi, le funzionalità e l'architettura dell'infrastruttura di sicurezza.

Nella fase di Deploy(ment) l'infrastruttura di sicurezza (Firewall, Router, Access Control, Authentication, Authorization, Encryption ecc.) viene realizzata e posta in esercizio per l'erogazione dei servizi richiesti secondo i criteri di sicurezza precedentemente definiti.

Le attività di monitoraggio delle minacce (Threat Assessment) e delle vulnerabilità (Vulnerability Assessment), infine, costituiscono l'elemento abilitatore del processo di iterazione che produce feed-back e azioni correttive verso le altre fasi, come ad esempio (freccie Detect/Respond nella Figura 1) la ridefinizione della Politica di Sicurezza, la modifica di parti dell'infrastruttura (perché sovradimensionate o sottodimensionate), la scoperta di aree di rischio trascurate, l'avvio di procedure di Incident Handling.

Possono essere addirittura intraprese contromisure automatiche come la riconfigurazione run-time di Firewall e Router a fronte della rilevazione di intrusioni.



## Documenti di Riferimento

Rif. #	Titolo	Data	Autore
RIF1			
RIF2	Esempio di Security Assessment Report		N. De Bello
RIF3	Esempio di Security Auditing Report		N. De Bello
RIF12	Description of the Scheme UKSP01	02/12/1996	UK ITSEC
RIF13	The Appointment of Commercial Evaluation Facilities (CLEFs) UKSP02	03/02/1997	UK ITSEC
RIF14	Developers' Guide Part I (Roles of Developer in ITSEC ) UKSP04/1	07/1996	UK ITSEC
RIF15	Developers' Guide Part II (Reference for Developers) UKSP04/2	07/1996	UK ITSEC
RIF16	Developers' Guide Part III (Advice To Developers) UKSP04/3	07/1996	UK ITSEC
RIF17	Description of the CMS UKSP16 Part I	31/07/1996	UK ITSEC
RIF18	Information Technology Security Evaluation Criteria ITSEC	28/06/1991	UK ITSEC
RIF19	Creating an Information Security Policy	02/11/1998	Tom Peltier, CyberSafe
RIF20	Information Classification Assessment Methodology	02/11/1998	Tom Peltier, CyberSafe
RIF21	Developing a Network Security Checklist	02/11/1998	Tom Peltier, CyberSafe
RIF22	Implementing an Effective Electronic Communication Policy	02/11/1998	Tom Peltier, CyberSafe
RIF23	New Trends in Network Risk Management	02/11/1998	John O'Leary, CSI
RIF24	Secure Single Sign-On: Fantasy or Reality	02/11/1998	Fred Trickey, Columbia University
RIF25	The Self Correcting Network: Security Policy Automation and Reconfiguration	02/11/1998	Jeff Johnson, ISS
RIF26	RFC 2196: Site Security Handbook	09/1997	
RIF27	Information Technology Security Evaluation Manual (ITSEM) Version 1.0		COMMISSION OF THE EUROPEAN COMMUNITIES
RIF28	Guide to Threat and Risk Assessment For Information Technology (TRA Methodology)	11/1994	Canada Government
RIF29	The Role of Data Classification now and in the future (Computer Security Journal, Volume XIV, Number 2)	Spring 1998	Richard Power
RIF30	How to create a Data Classification Program (Computer Security Journal, Volume XIV, Number 2)	Spring 1998	Tom Peltier
RIF31	Intranet Security Guidelines (Computer Security Journal, Volume XIV, Number 4)	Fall 1998	M. Corby, R. E. Johnstone
RIF32	Information Resource Asset Protection (IRAP): A New Technique (Computer Security Journal, Volume XIV, Number 4)	Fall 1998	W. Tompkins, M. Gizzi
RIF33	Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model	05/1998	ISO/IEC JTC 1
RIF34	Common Criteria for Information Technology Security Evaluation - Part 2: Annexes	05/1998	ISO/IEC JTC 1
RIF35	Common Criteria for Information Technology Security Evaluation - Part 2: Security functional requirements	05/1998	ISO/IEC JTC 1
RIF36	Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance requirements	05/1998	ISO/IEC JTC 1
RIF37	BS 7799-1: 1999 Code of practice for information security management	1999	BSI-DISC
RIF38	BS 7799-2: 1999 Specification for information security management systems	1999	BSI-DISC

Note:

- I Documenti da RIF12 a RIF18 possono essere reperiti alla URL <http://www.itsec.gov.uk/>.
- I Documenti da RIF19 a RIF25 possono essere reperiti presso il CSI (Computer Security Institute, [www.gocsi.com](http://www.gocsi.com)), come pure RIF29 e RIF30.
- RFC 2196 (RIF26) sostituisce RFC 1244, che viene così resa obsoleta.
- RIF37 e RIF38 sono disponibili presso UNI.

## Definizioni

In questo Documento vengono usate in maniera interscambiabile le seguenti espressioni:

- “External Security Auditing”, “Internet Security Auditing” e “Penetration Test”
- “Vulnerability(ies)” e “Vulnerabilità”
- “Threat(s)” e “Minaccia(e)”
- “Vulnerability(ies) Monitoring” e “Vulnerability(ies) Assessment”
- “Threat(s) Monitoring” e “Threat(s) Assessment”
- “Planning” e “Pianificazione”
- “Implementing” e “Implementazione”
- “Monitoring” e “Monitoraggio”



### **Acronimi e parole Inglesi**

CSI	Computer Security Institute
ICSA	International Computer Security Association
ISS	Internet Security Systems
ITSEC	Information Technology Security Evaluation Criteria
ITSEM	Information Technology Security Evaluation Manual
ITSEF	Information Technology Security Evaluation Facility
CLEF	Commercial Evaluation Facility
CB	Certification Body
EWP	Evaluation Work Programme
ETR	Evaluation Technical Report
ECITC	European Committee for IT Testing and Certification
ISO	International Organisation for Standardisation
IEC	International Electrotechnical Commission
JTC 1	Joint Technical Committee 1 (ISO/IEC)
CC	Common Criteria
BSI	British Standards Institution
DISC	Delivering Information Solutions to Customers (organo del BSI, cura BS 7799)
UNI	Ente Nazionale Italiano di UNificazione - Italian National Standards Body
IRAP	Information Resource Asset Protection
TRA	Threat & Risk Assessment
VPN	Virtual Private Network
ANS	Adaptive Network Security
NRP	Network Resource Planning
N&SM	Network & System Management
Asset	Qualsiasi risorsa dell'infrastruttura IT
TOE	Target of Evaluation
CIA	Confidentiality, Integrity, Availability
SSO	Single Sign-On
SSSO	Secure Single Sign-On
IDS	Intrusion Detection System
SS o S2	System Scanner
DBS	DataBase Scanner
ITM	Information Technology Management
ITS	Information Technology Security

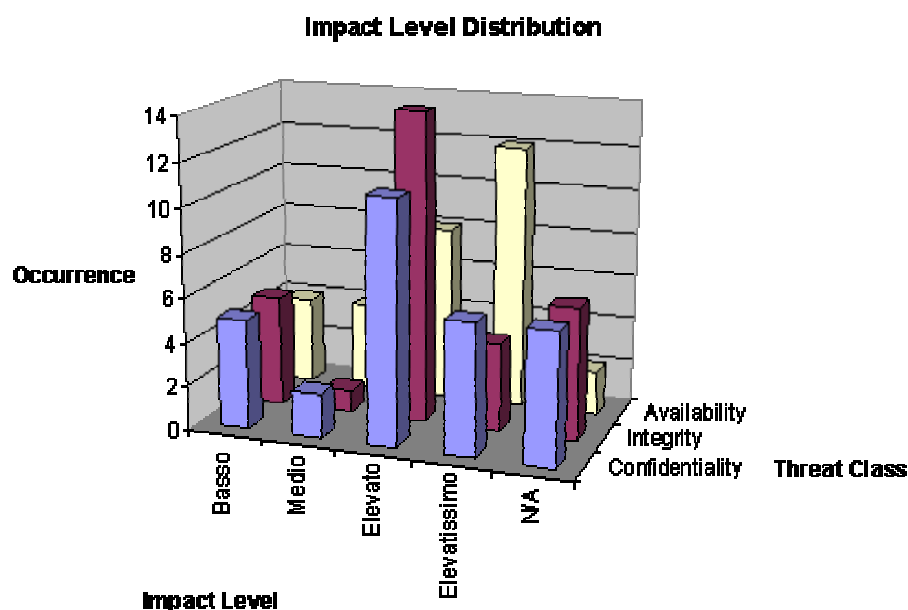
## Security Assessment

### Descrizione

“Le Informazioni e i Dati contenuti nell’infrastruttura IT dell’Azienda, nonché l’infrastruttura stessa, sono risorse di grande valore e costituiscono un importantissimo Patrimonio Aziendale. La continuità del business è pesantemente dipendente dalla **confidenzialità**, dall’**integrità** e dalla continua **disponibilità** di un certo sottoinsieme critico di Informazioni e Dati, nonché dai mezzi tramite i quali questi sono raccolti, memorizzati, processati, trasmessi e presentati. Devono quindi essere intraprese le azioni necessarie per proteggere queste risorse dall’uso, modifica, divulgazione o distruzione non autorizzati, siano essi accidentali o intenzionali.” (BS7799)

L’Attività di Security Assessment ha lo scopo di produrre:

- un’Analisi delle problematiche di Sicurezza relative all’Infrastruttura IT
- una rilevazione delle criticità presenti sia per quanto riguarda le aree esplicitamente richieste che per quanto riguarda eventuali nuove aree evidenziate dall’Analisi stessa
- una valutazione quantitativa (RATING, vedi Esempio in Figura) di dette criticità
- le linee guida per la stesura di Politiche di Sicurezza a copertura delle problematiche/criticità di cui sopra
- un Piano di Azione che suggerisca eventuali contromisure sia statiche (Fase “Implementation” in Figura I) che dinamiche (Fase “Monitoring” in Figura I)





a partire da (vedi sempre Figura 1):

- Principi e Politiche Aziendali esistenti
- Standard esistenti

Per fare ciò si eseguono le seguenti Attività:

- CIA (**Confidentiality, Integrity, Availability**) Requirements
- Asset Classification
- Information/Data Classification
- Threat & Risk Assessment

Queste Attività vengono effettuate nella pratica utilizzando:

- Incontri ed interviste con il personale del Cliente
- Materiale fornito dal Cliente
- Analisi dell'Infrastruttura IT del Cliente con strumenti automatici (vedi Capitoli seguenti)

Tutto ciò viene seguito dalla redazione di un Report DRAFT, da un'eventuale affinamento dell'Analisi e del Report a fronte di *feed-back* da parte del Cliente, e dalla redazione del Report definitivo.

L'Attività di Security Assessment è comunque inserita nel più generale Modello **ASM** (Adaptive Security Management). Si noti che ASM è un Modello Operativo che vuole ottenere due scopi principali:

- Inquadrare le Attività relative alla Sicurezza in un quadro procedurale unico
- Evidenziare l'importantissima, intrinseca caratteristica di iterazione continua di tutto l'insieme (processo *adattativo*)

Esso è comunque il prodotto di quanto esistente attualmente in termini di Standard, Metodologie, Normative ecc.. Si noti però che **NON** vi è allo stato attuale uno Standard universalmente accettato per quanto riguarda le problematiche di Sicurezza qui prese in considerazione, soprattutto per quanto riguarda l'Italia. La Legge 23 Dicembre 1993 n. 547 (Criminalità Informatica) e la Legge 31 Dicembre 1996 n. 675 (Trattamento dei Dati Personali) hanno effettivamente cambiato lo scenario, nel senso che non si può più intendere la Sicurezza come un **COSTO**, ma bisogna invece prevedere **RESPONSABILITÀ per la NON SICUREZZA e COSTO della NON SICUREZZA**. L'Art. 15 della Legge 675 in materia di sicurezza dei dati infatti prevede che: *"I dati personali oggetto di trattamento devono essere custoditi, 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"*. Sembra quindi che i principi minimi ai quali ispirare una Politica Aziendale di Sicurezza Informatica siano:



- Rispetto dei requisiti di “diligenza professionale”, richiesti dall’Art. 2050 del Codice Civile
- Adeguamento preventivo ai contenuti espressi dall’Art. 15 della Legge 675 e quindi alle **MISURE MINIME** DPR n. 318/99 (G.U. Serie Generale n. 216 del 14 settembre 1999)
- Allineamento a Standard riconosciuti a livello Comunitario o Internazionale (ITSEC, BS7799/ISO17799, ISO15408 Common Criteria, ISO Guide 25 e EN45001, Raccomandazioni di ECITC ecc.)

L’adozione dei criteri **ITSEC** sembra, allo stato, adeguata, anche in relazione alle indicazioni emerse in sede comunitaria. Nella raccomandazione 95/144/CE del 7 aprile 1995, il Consiglio dell’UE raccomandava infatti agli stati membri “*che siano applicati, per un periodo iniziale di due anni, i criteri per la valutazione della sicurezza delle tecnologie dell’informazione (ITSEC) nell’ambito delle procedure di valutazione e certificazione, allo scopo di sopperire alle necessità immediate di valutazione e certificazione, legate alla commercializzazione e all’utilizzo di prodotti, servizi e sistemi in materia di tecnologia dell’informazione*”.

Sulla base di tale raccomandazione è prevedibile che le misure minime che saranno individuate dal legislatore italiano non potranno non fare riferimento ai criteri ITSEC. Questa è comunque soltanto una previsione: ITSEC non ha ancora nessuna veste ufficiale per quanto riguarda l’Italia. Anche la sua traduzione in Italiano (vedi <http://www.aipa.it/>) è etichettata dall’AIPA come “non ufficiale”, ed è largamente incompleta. Per ora vi è solo una proposta di legge, la 2515 Camera dei Deputati, in cui si prevede l’istituzione di un sistema di certificazione dei prodotti informatici.

Bisogna anche sottolineare che ITSEC (attualmente alla Versione 1.2) è uno Standard esplicitamente rivolto a questioni di Certificazione:

“The objectives of the Scheme are to meet the needs of Industry and Government for cost effective and efficient security evaluation and certification of IT products and systems. The Scheme also aims to provide a framework for the international mutual recognition of certificates.” (vedi RIF12, Paragrafo 1.2).

Esso è stato ufficialmente sottoscritto solamente (per ora) da Gran Bretagna, Germania, Olanda e Francia, a cui sia aggiungono USA e Canada per quanto riguarda la sua evoluzione nota come ISO/IEC 15408 o “Common Criteria” (attualmente alla Versione 2.0, vedi RIF33, RIF34, RIF35 e RIF36), ed è comunque in “Trial Period”. Nessuna Azienda Italiana può quindi operare ufficialmente sotto l’etichetta ITSEC, per quanto detto sopra e perché essa comunque dovrebbe essere un CLEF ufficialmente approvato dai Governi coinvolti ed operare sotto il controllo di un CB Governativo. Recentemente hanno assunto lo status di CLEF alcuni Enti Governativi e CSQ/IMQ.

C’è infine da osservare che l’Attività qui in Oggetto è un Security Assessment, e come tale per definizione ANTECEDENTE alle fasi e problematiche coperte da ITSEC. Essa serve proprio ad identificare ciò che potrà eventualmente diventare in futuro (usando i termini ITSEC) un Security Target (e quindi un TOE), e ad aprire la

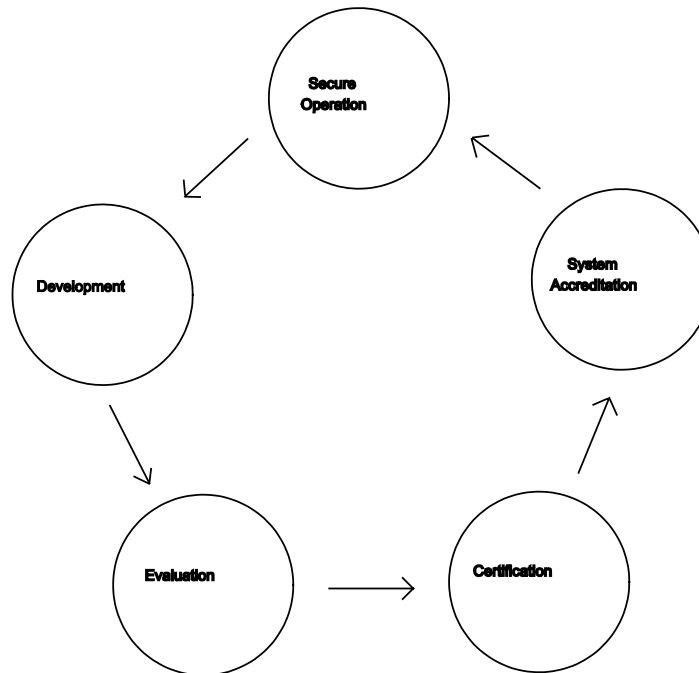


porta alla definizione di Security Policy senza le quali ITSEC non può nemmeno essere preso in considerazione:

“...the procurer of a system may be obliged to seek certification by his Corporate Security Policy.” (vedi RIF12, Paragrafo 3.4)

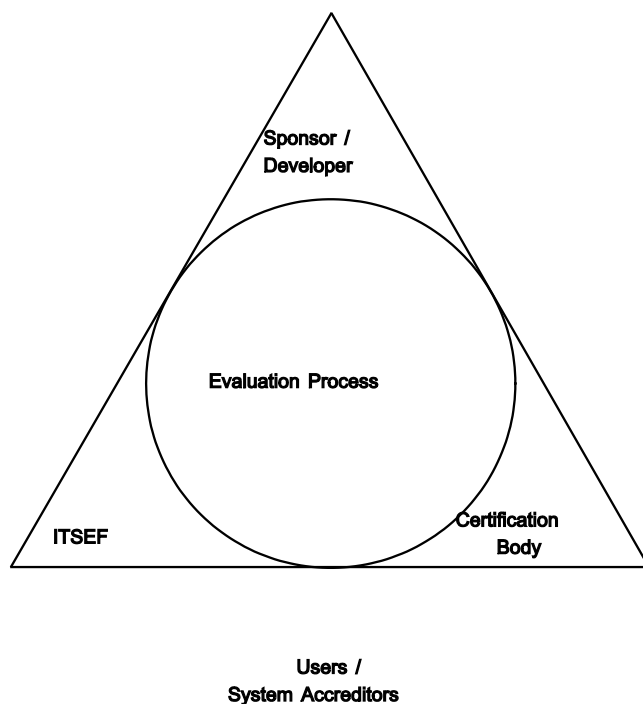
“The Sponsor may employ a security consultant, which may be a CLEF, to assist in determining the Security Target.” (vedi RIF12, Paragrafo 3.11)

Nonostante tutto ciò, si può facilmente notare (consultando da RIF12 a RIF18, RIF27 e da RIF33 a RIF36) che la metodologia qui adottata è perfettamente congruente con gli schemi ITSEC/ITSEM/CC. Innanzitutto, come si vede dalla Figura seguente (RIF27, Figure 1.1.1 Processes in the IT Security Framework) l'aspetto iterativo/adattativo è fondamentale, anche se ovviamente nel caso ITSEC la terminologia è più virata verso questioni di Certificazione.





Anche gli Attori in gioco sono congruenti (RIF27, Figure 1.2.1 Parties involved in, or concerned with, evaluation and certification):



come pure le Fasi in cui il lavoro viene suddiviso (RIF27, Paragrafo 1.2.15 e Capitolo 4.2):

- a) Phase I Preparation;
- b) Phase II Conduct;
- c) Phase III Conclusion.

Il Ruolo di Sponsor/Developer è assunto dal Cliente (con tutti gli obblighi che ciò comporta in termini di fornitura di informazioni), mentre quello di ITSEF (o CLEF) è assunto da Primeur IT Security . Come già sottolineato, non vi è per ora nessun Certification Body.

In questo caso ovviamente sia considera come TOE l'intera Infrastruttura IT del Cliente o qualunque suo sottoinsieme venga preso in esame durante l'Analisi. La congruenza dell'approccio è perfetta leggendo RIF27, Paragrafo 3.3.3:

The security target specifies the security objectives of the TOE, relating **threats** and **assets** to each objective (there must be at least one security objective). An example objective might be:

- a) The TOE shall prevent the disclosure of sensitive information to personnel with insufficient clearance to access that information.
- b) The TOE shall ensure that supervisors charged with cross-checking of customers' data do not abuse their authority in order, for example, to commit fraud.



e la lista dei punti di interesse (RIF27, Paragrafo 3.3.1):

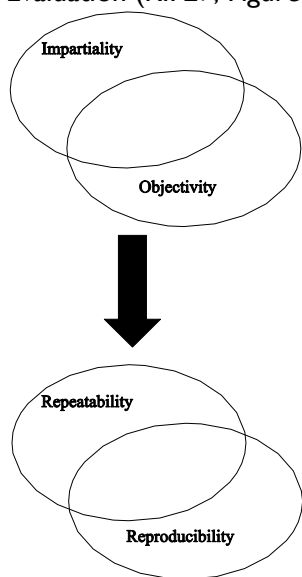
- *security objectives, **assets**, and **threats**;*
- *correctness and effectiveness;*
- *components, functions and mechanisms;*
- *security enforcing, relevant and irrelevant functions and components;*
- *separation of functionality;*
- *refinement, **errors**, and error correction;*
- *construction and operational **vulnerabilities**;*
- *strength of mechanisms;*
- ***exploitable vulnerabilities**;*
- ***penetration testing**.*

Da notare che ITSEC chiama “Penetration Testing” qualsiasi tipo di analisi/attacco/scan automatico del prodotto/sistema sotto esame, attività considerata fondamentale per la valutazione/certificazione. Per quanto riguarda una descrizione dettagliata dello Scan incluso in questo Security Assessment, si vedano i Capitoli seguenti.

Congruenti sono pure i tre Requisiti base che definiscono la Sicurezza (vedi RIF12, RIF37 e RIF38):

- Confidentiality
- Integrity
- Availability

(riassunti dall’acronimo CIA) nonché i quattro principi base di una Security Evaluation (RIF27, Figure 3.4.1 Four Basic Principles in Evaluation):



Si noterà infine una stretta aderenza anche per quanto riguarda le tecniche di valutazione e gli strumenti utilizzati (RIF27, Capitolo 4.5, “Evaluation Techniques and

Tools”) nonché una quasi totale analogia tra la struttura del presente Documento e quello che in termini ITSEC/ITSEM/CC viene chiamato ETR (Evaluation Technical Report, RIF27, Capitolo 4.7 e Figura 4.7.1).

### **BS 7799 / ISO 17799**

Lo Standard BS 7799, a differenza di ITSEC, non si rivolge a problematiche di Certificazione, ma più in generale indica un **“Code of practice for information security management”**, è quindi molto vicino agli argomenti fino ad ora trattati. Esso viene quindi utilizzato da Primeur IT Security come riferimento per le Attività di Security Assessment ovunque sia pertinente (vedi RIF37 e RIF38).

I British Standard 7799 (nel seguito BS) sono frutto di un lavoro congiunto tra *Departement of Trade and Industry* della Gran Bretagna e alcune importanti compagnie ed industrie britanniche. Il risultato di tale lavoro è rappresentato da un documento denominato **“Code of Practice for Information Security Management”**, che è stato avvalorato e pubblicato dal *British Standard Institution* (BSI) come parte I del BS7799. Il **“Code of practice”** è stato in seguito integrato da un secondo documento, **“Specification for information security management system”**, che costituisce la parte 2 del BS7799 ed ha lo scopo di fornire una base guida per il processo di valutazione di un ISMS (*Information Security Management System*).

L'interesse che i BS7799 suscitano a livello mondiale risiede nel fatto che, rispetto ad altri standard quali ITSEC e CC, affrontano il problema della sicurezza dei dati da un punto di vista molto generale. Sono infatti presi in considerazione, non solo gli aspetti tecnologici della sicurezza, ma anche gli aspetti organizzativi e logistici, che rendono i BS7799 adatti ad essere applicati alla gestione della sicurezza di un sistema o di una intera azienda, piuttosto che di un prodotto.

Il **“Code of Practice for Information Security Management”** ha come obiettivo principale quello di fornire una base comune ed una guida per la definizione di un sistema di protezione. Esso è strutturato in dieci sezioni, ciascuna delle quali rappresenta un aspetto della sicurezza. All'interno di ogni sezione sono elencati e descritti una serie di **“controlli”** che riguardano specifiche funzioni di sicurezza a livello tecnologico, organizzativo o logistico. L'ultimo aggiornamento dei BS7799 contiene in tutto 127 controlli di sicurezza. Non tutti i controlli sono applicabili in tutti i contesti, ma vengono segnalati dieci controlli, indicati come **“controlli chiave”**, considerati elementi fondamentali nella costruzione di un sistema di sicurezza. Tra questi citiamo quelli che rendono i BS7799 originali rispetto ad altri standard: assegnazione dei ruoli delle responsabilità riguardo la sicurezza, formazione ed educazione del personale sulle problematiche della sicurezza, definizione di procedure di *disaster recovery*, gestione dei dati personali in conformità con la legge vigente.



Esso è comunque uno Standard inglese, che non ha ancora ufficialità in Italia, anche se, analogamente a ITSEC, sembra ormai essere il punto di riferimento privilegiato. Recentemente (Novembre 2000) esso ha assunto lo status di Standard ISO (ISO 177799), e su di esso si basa la nuova Certificazione “CSQ-Data” rilasciata da IMQ, ente con il quale Primeur IT Security collabora nella definizione della Certificazione.



### **Threat & Risk Assessment**

La Metodologia qua descritta utilizza anche i più attuali risultati nel campo delle Attività di Threat & Risk Assessment, (come ad esempio TRA e IRAP), di Asset/Information Classification e di definizione di Security Policy. Si vedano RIF19, RIF20, RIF21, RIF22, RIF23, RIF28, RIF29, RIF30, RIF31 e RIF32.

Le Form utilizzate nell’Attività contengono i seguenti Campi:

#### Information Classification:

- Information/Data: definizione dell’informazione o del dato
- Sensitivity Label: Public, Internal Use Only, Restricted Internal o Confidential
- Availability: grado di disponibilità dell’informazione/dato
- User: tipo di Utenza
- Access/Attr.: tipo di accesso e altri eventuali attributi
- Storage: dove è memorizzata l’informazione

#### Asset Classification/Threat & Risk Assessment

- Asset: definizione della risorsa IT
- Attributes: attributi (indirizzo IP, nome ecc.)
- Service: tipo di servizio fornito
- Threat: minaccia a cui la risorsa è sottoposta
- Threat Class: categoria della minaccia (Disclosure, Integrity, DoS)
- Probability: probabilità (rischio) che la minaccia accada
- Consequences: conseguenze
- Impact: impatto
- Rating: valutazione numerica finale

### **RFC 2196**

Uno Standard de facto pure molto vicino ad un’Attività di Security Assessment come quella in Oggetto è RFC2196 (vedi RIF26). Quelli seguenti sono tutti estratti da RFC2196, che sottolineano come l’Attività proposta ne segua molto da vicino i dettami.



- Passi da seguire in un Progetto di Sicurezza:
  - (1) Identify what you are trying to protect.
  - (2) Determine what you are trying to protect it from.
  - (3) Determine how likely the threats are.
  - (4) Implement measures which will protect your assets in a cost-effective manner.
  - (5) Review the process continuously and make improvements each time a weakness is found.
  
- Perché una Politica di Sicurezza:

“One of the most important reasons for creating a computer security policy is to ensure that efforts spent on security yield cost effective benefits. Although this may seem obvious, it is possible to be misled about where the effort is needed. As an example, there is a great deal of publicity about intruders on computers systems; yet most surveys of computer security show that, for most organizations, the actual loss from "insiders" is much greater.”
  
- Definizione di Risk Analysis:

“Risk analysis involves determining what you need to protect, what you need to protect it from, and how to protect it.”
  
- Cosa fare per prima cosa:
  - (1) Identifying the assets
  - (2) Identifying the threats
  
- Obiettivi base della Sicurezza:

“For each asset, the basic goals of security are **availability**, **confidentiality**, and **integrity**. Each threat should be examined with an eye to how the threat could affect these areas.”
  
- Possibile categorizzazione degli asset:
  - (1) Hardware: CPUs, boards, keyboards, terminals, workstations, personal computers, printers, disk drives, communication lines, terminal servers, routers.
  - (2) Software: source programs, object programs, utilities, diagnostic programs, operating systems, communication programs.
  - (3) Data: during execution, stored on-line, archived off-line, backups, audit logs, databases, in transit over communication media.
  - (4) People: users, administrators, hardware maintainers.
  - (5) Documentation: on programs, hardware, systems, local administrative procedures.
  - (6) Supplies: paper, forms, ribbons, magnetic media.

- Possibile categorizzazione delle minacce (Threats):
  - (1) Unauthorized access to resources and/or information
  - (2) Unintended and/or unauthorized Disclosure of information
  - (3) Denial of service
  
- Lista delle Problematiche prese in considerazione:
  - *Architecture*
  - *Objectives*
  - *Network and Service Configuration*
  - *Firewalls*
  - *Security Services and Procedures*
  - *Authentication*
  - *Confidentiality*
  - *Integrity*
  - *Authorization*
  - *Access*
  - *Auditing*
  - *Securing Backups*
  - *Security Incident Handling*
  - *Preparing and Planning for Incident Handling*
  - *Notification and Points of Contact*
  - *Identifying an Incident*
  - *Handling an Incident*
  - *Aftermath of an Incident*
  - *Responsibilities*
  - *Ongoing Activities*

## ICSA

La Certificazione di Sicurezza ICSA, denominata “TruSecure”, è volta alla certificazione, nel senso più generale possibile, di ciò che un’organizzazione offre verso Internet. È quindi una Site Certification, che può quindi comprendere Firewall, apparati di rete, Server di vario tipo (Mail, Web ecc.), cioè tutta la parte di Infrastruttura IT che sia visibile da Internet. La sua natura operativa e continuativa la rende uno strumento perfettamente integrabile in qualsiasi accezione la Sicurezza venga vista (ITSEC, BS7799, RFC 2196 ecc.).

## Riferimenti Legislativi Italiani ed Europei

- Legge del 23 dicembre 1993, n.547:

“Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica”.

Questa legge ha attribuito dignità giuridica a comportamenti che, prima della sua approvazione, non potevano essere configurati come penalmente rilevanti. Infatti, nel diritto penale vige il principio secondo il quale la norma può essere applicata solo nei casi in cui il comportamento illecito è espressamente previsto dalla stessa. Tale principio rendeva difficile l’interpretazione e l’applicazione delle norme a causa della



particolarità dei beni informatici. Con la legge 547 il codice penale è stato modificato con la previsione di nuove forme di reato. Sono ora configurabili l'accesso abusivo ad un sistema informatico, l'introduzione di programmi virus, la diffusione di codici di accesso, la frode informatica, i reati contro le comunicazioni informatiche e telematiche e, in generale, tutti quei comportamenti illeciti commessi contro un bene informatico o con l'ausilio di esso.

■ Legge del 15 marzo 1997, n.59 (legge Bassanini):

“Delega al Governo per il conferimento di funzioni e compiti alle regioni ed enti locali, per la riforma della Pubblica Amministrazione e per la semplificazione amministrativa”.

Questa legge stabilisce che “gli atti, dati e documenti formati dalla pubblica amministrazione e dai privati con strumenti informatici o telematici, i contratti stipulati nelle medesime forme, nonché la loro archiviazione e trasmissione con strumenti informatici, sono validi e rilevanti a tutti gli effetti di legge”. I criteri e le modalità di applicazione sono stabiliti con specifici regolamenti.

■ Decreto del Presidente della Repubblica del 10 novembre 1997, n.513.

“Regolamento recante criteri e modalità per la formazione, l'archiviazione e la trasmissione di documenti con strumenti informatici e telematici, a norma dell'articolo 15, comma 2, della legge 15 marzo 1997, n.59”

Il Decreto definisce le regole non tecniche alle quali deve attenersi il documento informatico affinché sia valido e rilevante a tutti gli effetti di legge, secondo quanto stabilito dalla Legge Bassanini del 15 Marzo 1997, n. 59. Anticipa inoltre che le regole tecniche saranno contenute in un decreto del Presidente del Consiglio dei Ministri che dovrà seguire. Definisce quindi i requisiti societari del Certificatore ed i suoi obblighi nei confronti dei clienti e della società civile. Inoltre definisce la Firma Digitale, gli ambiti di valenza, i limiti cui è sottoposta.

■ Decreto del Presidente del Consiglio dei Ministri del 8 febbraio 1999

“Regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici ai sensi dell'articolo 3, comma 1, del Decreto del Presidente della Repubblica, 10 novembre 1997, n.513”

Il decreto contiene le regole tecniche a cui ci si deve attenere nel trattamento di un documento informatico, affinché esso sia valido e rilevante a tutti gli effetti di legge.

Le regole tecniche relative alla firma digitale ad alla coppia di chiavi crittografiche stabiliscono i tipi di chiavi ed i relativi ambiti di valenza, gli algoritmi di generazione delle chiavi e gli algoritmi di hashing utilizzati per l'apposizione della firma digitale. Vengono inoltre stabiliti i requisiti di sicurezza dei dispositivi per la generazione delle chiavi e dei dispositivi di generazione e verifica delle firme, in riferimento allo standard di sicurezza europeo ITSEC.

Le regole tecniche per la certificazione delle chiavi stabiliscono le norme cui devono attenersi i certificatori per ottenere l'iscrizione all'albo dei certificatori tenuto presso l'AIPA. Tali norme riguardano le procedure di gestione dei certificati (dalla generazione alla revoca), i requisiti di sicurezza dei dispositivi di cui sopra, i requisiti di sicurezza del sistema in cui il certificatore opera. In particolare è stabilito il contenuto della documentazione che il certificatore deve produrre al fine di

evidenziare le procedure applicate nello svolgimento della propria attività (Manuale Operativo) e le caratteristiche del proprio sistema di sicurezza (Piano per la Sicurezza).

■ Circolare 26 luglio 1999, n. AIPA/CR/22-Iscrizione all'Albo dei Certificatori

Ai sensi dell'art.16, comma 1, dell'allegato tecnico al decreto del Presidente del Consiglio dei Ministri 8 febbraio 1999, pubblicato sulla Gazzetta Ufficiale del 15 aprile 1999, serie generale, n. 87, la circolare individua le modalità con le quali le società interessate ad esercitare l'attività di certificatore dovranno presentare domanda all'AIPA, per l'iscrizione nell'elenco pubblico dei certificatori di cui all'articolo 8, comma 3, del decreto del Presidente della repubblica 10 novembre 1997, n. 513.

■ Legge del 24 dicembre 1993, n.537

“Interventi correttivi di finanza pubblica”

La legge stabilisce che “gli obblighi di conservazione e di esibizione dei documenti si intendono soddisfatti anche se realizzati tramite supporto ottico”. Le procedure che rendono valide tali modalità di conservazione ed esibizione sono stabiliti con specifici regolamenti tecnici.

■ Deliberazione AIPA del 30 luglio 1998, n.24

“Art.2, comma 15, della legge 24 dicembre 1993, n.537: Regole tecniche per l'uso di supporti ottici”.

La deliberazione definisce i tipi di supporto utilizzabili, gli standard applicabili ed i tipi di documenti archiviabili. Inoltre stabilisce quali devono essere i contenuti obbligatori del supporto di memorizzazione. In particolare per ogni registrazione sul medesimo supporto deve essere memorizzato sul supporto stesso un “file di controllo della registrazione” e dopo l'ultima registrazione effettuata deve essere memorizzato sul supporto un “file di chiusura”. Tali file devono contenere, tra le altre cose, le firme digitali dei soggetti che effettuano le operazioni di registrazione e la firma digitale del pubblico ufficiale che assiste alla chiusura del supporto; ciascuna firma deve essere accompagnata da relativo certificato.

■ Legge del 31 dicembre 1996, n.675

“Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali”.

La legge definisce “trattamento dei dati personali” qualunque operazione (es. elaborazione, conservazione, distruzione ecc.) svolta con o senza mezzi elettronici, relativa a dati concernenti persone fisiche, giuridiche od enti.

La legge istituisce un Garante per la tutela delle persone rispetto al trattamento dei dati personali, i cui compiti principali sono di emanazione di provvedimenti limitativi della diffusione di taluni dati, di vigilanza/ispezione affinché vi sia il rispetto delle norme, di presiedere il ricorso degli interessati con possibilità di irrogare sanzioni amministrative pecuniarie.

La legge stabilisce che è necessario notificare al Garante i trattamenti di dati personali effettuati, in particolare devono essere comunicate anche le misure tecniche ed organizzative adottate per la sicurezza. Se l'azienda, nel suo pur legittimo trattamento di dati personali, cagiona un danno è tenuta al risarcimento, se non



prova di aver adottato tutte le misure idonee ad evitare tale danno (art. 2050 cod.civ. richiamato dall'art. 18 della legge).

■ Decreto del Presidente della repubblica 28 luglio 1999, n. 318

“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 31 dicembre 1996, n. 675.”

Il decreto stabilisce le misure minime di sicurezza, tecniche, informatiche, organizzative, logistiche e procedurali che devono essere previste in un sistema informativo al fine di configurare un livello minimo di protezione nel caso di trattamento dei dati personali o sensibili, effettuato con strumenti elettronici, automatizzati o in maniera differente.

■ Norme del codice civile

Le normative espressamente previste per i beni informatici e per l'utilizzo dei sistemi informatici presuppongono anche una generica responsabilità di carattere civilistico. Riportiamo alcune norme di interesse:

- Art. 2043: “Qualunque fatto doloso o colposo che cagiona ad altri un danno ingiusto, obbliga colui che ha commesso il danno a risarcire il danno”.
- Art. 2049: Responsabilità del datore di lavoro per i danni arrecati da fatti illeciti commessi dai dipendenti nello svolgimento degli incarichi attribuiti.
- Art. 2050: Responsabilità per danni derivanti dallo svolgimento di attività pericolose (è richiamato dal disegno di legge sulla tutela delle persone rispetto al trattamento dei dati personali).

■ Raccomandazione del Consiglio Europeo del 7 aprile 1995, 95/144/CE

“Criteri comuni per la valutazione della sicurezza delle tecnologie d'informazione”. Nella raccomandazione vengono indicati i criteri ITSEC come i criteri da adottare per la valutazione della sicurezza delle tecnologie d'informazione; viene inoltre promossa l'armonizzazione e la normazione internazionale di tali criteri di valutazione.

■ Comunicazione della Commissione Europea COM(1998), n.297

“Proposta di Direttiva del Parlamento Europeo e del Consiglio relativa a regole comuni sulle firme elettroniche.”

La direttiva, proposta nella presente comunicazione, ha lo scopo di creare un quadro giuridico armonizzato ed appropriato relativo all'uso delle firme elettroniche nella Comunità europea, e di definire una serie di criteri che costituiscono la base del riconoscimento giuridico delle firme digitali.

■ COUNCIL OF THE EUROPEAN UNION - Brussels, 15 January 2002

Council Resolution on a common approach and specific actions in the area of network and information security

### Documentazione prodotta

Viene prodotto un Report analogo a quello esemplificato in RIF2.

### Pre-requisiti, vincoli e limitazioni

Il Cliente dovrà rendere disponibili risorse interne nell'ambito IT che siano i riferimenti per la raccolta di informazioni descritta ai Paragrafi precedenti.

L'Attività non comprende parti implementative.

### Deliverables

Come sottolineato nei Paragrafi precedenti, l'Attività comprende:

- Incontri ed interviste con il Cliente
- Analisi del materiale fornito dal Cliente
- Integrazione risultati Scan Automatico
- Produzione del Report
- Consegna ufficiale del Report

Il *Deliverable* ufficiale è quindi il Report di Security Assessment, e si riferisce ad una Infrastruttura IP di max. 500 nodi, costituita da una sede centrale e n sedi periferiche con raggiungibilità IP. Qualora vi sia la necessità di sopralluoghi fisici nelle sedi periferiche, la Quotazione dell'Attività va adattata in funzione di ciò.

### Opzioni

#	Attività	Quotazione
A2.1	Security Assessment come sopra descritto	

## External Security Auditing

La prima tipologia di Auditing (vedi “Adaptive Security Management”) riguarda il monitoraggio delle vulnerabilità dall’esterno. Viene simulato un attacco proveniente dalla rete *untrusted* (Internet), il cui scopo è penetrare nell’insieme delle reti interne *trusted* attraverso gli entry-point commissionati dal Cliente (tipicamente Sistemi Firewall), oppure attraverso altri eventuali entry-point non previsti.

L’avvio di un *Penetration Test* di questo tipo è di solito subordinato ad una attività iniziale di analisi dell’Infrastruttura di Rete, caratterizzata dall’acquisizione della topologia di rete e delle configurazioni dei Sistemi Firewall, nonché dalla catalogazione e caratterizzazione dei sistemi della rete interna ai quali è consentito l’accesso da parte di utenti attestati su reti esterne. Sono questi i sistemi presi in considerazione in dettaglio, assieme ai Firewall, nel test stesso, sebbene l’intera Infrastruttura IT del Cliente (o meglio: la sua visibilità dall’esterno) venga considerata come TOE.

### Esecuzione per fasi del Test

La prima fase del Test (Discovery) riguarda il reperimento di tutte le possibili informazioni disponibili dall’esterno, secondo le seguenti modalità:

- Analisi DNS
- Analisi SNMP
- Analisi routing
- Scan della Rete al fine di rilevare i Servizi aperti, le tipologie di Piattaforme e S.O. ecc.
- Sniffing (se possibile)

In questa fase, prettamente manuale, vengono utilizzati strumenti propri (anche sviluppati all’uopo) e Public Domain (provenienti dalla rete e dall’*underground*), o addirittura le normali utility a disposizione su qualunque piattaforma UNIX (whois, finger, nslookup, ping, traceroute ecc.). Possono anche essere utilizzati strumenti di Discovery SNMP-based. Sarà molto importante, alla fine dell’Attività di Auditing, paragonare i risultati ottenuti in questa fase con i dati forniti dall’Analisi di cui sopra.

La seconda fase del Test (Vulnerability Assessment) riguarda il vero e proprio monitoraggio delle vulnerabilità esistenti in base ai risultati della fase di Discovery. Essa si avvale di strumenti automatici quali gli Scanner di ISS (Internet Security Systems), oltre che di strumenti propri, Public Domain e di provenienza *underground*. Il risultato di questa fase è un Report dettagliato delle eventuali vulnerabilità presenti nell’infrastruttura sotto esame.

La terza fase del Test (Penetration Test) riguarda il tentativo di sfruttamento (*exploit*) delle vulnerabilità eventualmente rilevate nelle fasi precedenti. Appartiene a questa fase anche l’esecuzione degli attacchi DoS (Denial of Service), esecuzione che deve ovviamente essere preventivamente concordata.

### Documentazione prodotta

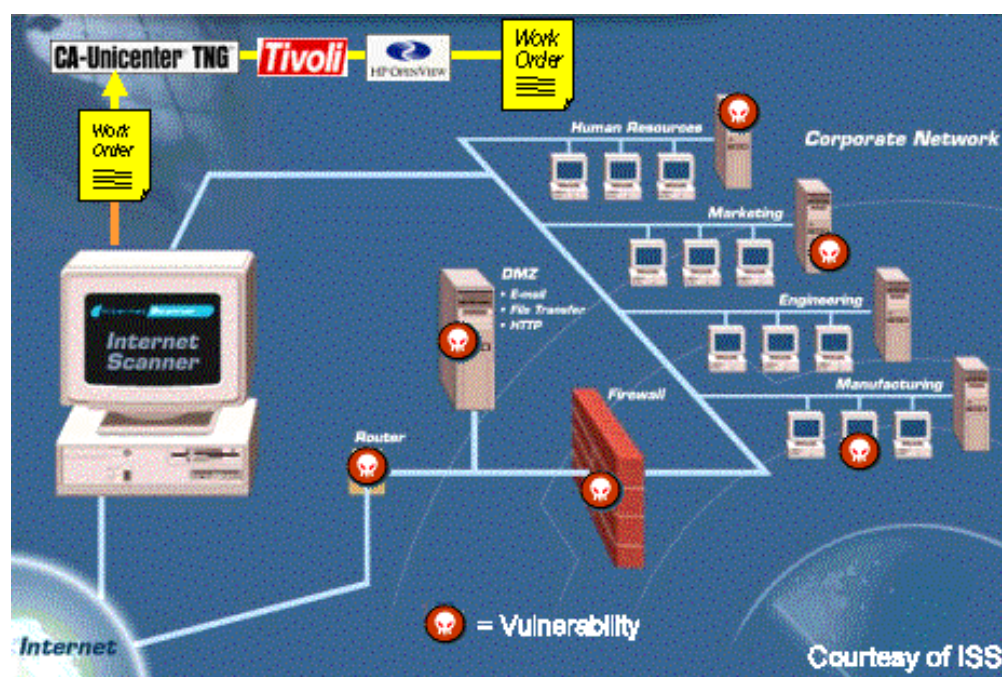
La documentazione dell'attività, oltre a consolidare i dati di analisi iniziale e a paragonarli con i risultati ottenuti, riporterà le modalità operative del test, i risultati, le azioni correttive da intraprendere, le raccomandazioni ed un Piano di Azione consigliato, secondo il seguente Indice:

- Analisi della situazione corrente
- Analisi dei Target
- Definizione della Metodologia
- Sintesi dei Risultati
- Considerazioni
- Piano di Azione
- Dettaglio dei Risultati

Si pone una particolare attenzione alla necessità di un continuo aggiornamento delle informazioni e degli strumenti utilizzati nell'Attività di Auditing, tramite gli enti internazionali preposti (CERT, CIAC, FIRST, ICESA, CSI, ISS X-Force ecc.), le mailing list e i newsgroup dedicati e le risorse dell'*underground*. L'aggiornamento si estende ovviamente anche alle versioni dei prodotti utilizzati, sia per quelli commerciali che per quelli Public Domain e *underground*.

### Prodotti e strumenti utilizzati

Uno degli scopi dell'Attività di Analisi propedeutica al test è quello di individuare la topologia della rete ed i sistemi presenti, anche al fine di poter acquisire le licenze dei prodotti ISS utilizzati nel test stesso. Essi infatti sono licenziati in base agli indirizzi IP target, corrispondenti ad "n" licenze (nodi) del prodotto denominato Internet Scanner Bundle, che può essere utilizzato sia per l'Auditing dall'esterno che per quello interno (vedi Capitolo successivo).





ISS Internet Scanner è disponibile per piattaforme Windows. L'Attività di Scan della Rete e dei nodi *Target* può quindi essere effettuata da qualsiasi stazione (anche portatile) con questa piattaforma. Tutte le principali piattaforme *Target* sono supportate in termini di Analisi delle Vulnerabilità (Windows, tutti i dialetti di Unix, i principali Firewall, i più diffusi Apparati di Rete come ad esempio Cisco, ecc.).



Come già anticipato, lo Scanner di ISS è il principale strumento impiegato, soprattutto per le sue sofisticate caratteristiche di analisi delle vulnerabilità e di reportistica, ma non è certamente l'unico. I suddetti punti di forza, infatti, hanno la massima resa in uno scenario nel quale si siano già accumulate le informazioni topologiche necessarie, mentre un *Penetration Test* parte per definizione da una situazione a *Zero Knowledge*. Le fasi di *Discovery*, di analisi del DNS e delle informazioni SNMP, di indagine sul routing esistente ecc. non possono che essere eseguite con metodologie e strumenti che sono il prodotto di un *know-how* consolidato non solo nell'ambito della Sicurezza, ma in quello più generale del Networking e della Sistemistica. A ciò si aggiungano anche le altre tipiche aree di intervento in un'Attività di Security Auditing (analisi degli applicativi, Social Engineering, esecuzione di exploit e di attacchi DoS ecc.) e risulta evidente come qualsiasi processo legato alla Sicurezza non possa certo esaurirsi in uno o più prodotti.

Alcuni tra gli strumenti utilizzati da Primeur IT Security sono ad esempio:

- DNS: dnswalk, dig ecc.
- SNMP: snmpwalk, snmpprobe, Scotty ecc.
- Discovery: probe Public Domain di vario tipo (nmap, Scotty, Asmodeus ecc.)
- Sniffer: molti sniffer Public Domain (tra cui ad es. Juggernaut), NFR ecc.
- Password: Crack, lophcrack ecc.
- Altro: Nat, Netcat, SATAN, SAINT, NTIS ecc.

ai quali si aggiungono strumenti sviluppati internamente (come ad esempio sofisticati scanner TCP e UDP per il processo di *Discovery*, basati su *Scotty* e sulla *Tnm Tcl Extension* sviluppata all'Università di Braunschweig) o in collaborazione con l'Università di Padova (Facoltà di Ingegneria e di Statistica).

## WarDial

Quanto descritto nei Paragrafi precedenti riguarda l'ambito IP. È possibile completare l'Attività di External Security Auditing effettuando anche un'Analisi degli eventuali entry-point di tipo *Dial-Up*. Possono essere presi in considerazione Sistemi RAS espressamente indicati dal Cliente, o può essere eseguito lo scan (detto "WarDial") di un intero *range* di numerazione telefonica, alla ricerca di accessi in dati (RAS, modem di supporto/manutenzione, modem utente non noti o non permessi ecc.).



La versione *Light* di questa Attività (effettuata con strumenti Public Domain) mira ad individuare la presenza di portanti e a fornire una prima caratterizzazione delle eventuali possibilità di accesso rilevate.

La versione *Full* di questa Attività, invece, ottiene i medesimi risultati della versione *Light* aggiungendo una completa e dettagliata caratterizzazione degli accessi rilevati ed eseguendo per ciascuno di essi il tentativo di *exploit*. Essa si avvale di strumenti HW e SW dedicati, e può essere addirittura prevista una collocazione fisica di detti strumenti presso il Cliente. Ciò vuole ottenere i seguenti risultati:

- Abbattere i costi di chiamata
- Ottenere una gestione centralizzata, anche multi-site
- Consentire di aumentare la frequenza dello scan, dato che la presenza di portanti può essere molto variabile temporalmente (ore del giorno o della notte, periodi dell'anno ecc.)

### External Web Application Assessment

La disciplina di External Web Application Assessment riguarda la verifica di una applicazione web dall'esterno, ossia senza ulteriore conoscenza della sua architettura, o di altre informazioni in aggiunta a quelle normalmente note ad un utente legittimo. Queste possono includere, quando appropriato, credenziali richieste per accedere ad aree riservate. L'applicativo web da analizzare può offrire servizi via protocollo http o https.

Gli obiettivi principali dell'assessment riguardano l'analisi delle seguenti security issues:

- information leakage, cioè l'analisi di dati sensibili che possono essere esposti dall'applicativo (informazioni visibili mediante esame di pagine HTML, script embedded, altri file, o di altro materiale cui si riesca ad ottenere accesso, incluso codice server side che normalmente non è visibile dall'utente; informazioni ottenibili da commenti, messaggi di errore, od eventuali meccanismi di debugging che fossero presenti);
- gestione appropriata delle interazioni con l'utente, allo scopo di individuare possibili debolezze associate a input malformato, buffer overflow, ecc.;
- procedure di autenticazione;
- gestione della sessione, dove appropriato (meccanismi di logout, timeout della sessione, possibilità di introduzione impropria in una sessione da punti di accesso - URL - non verificati, session hijacking, ecc.);
- validazione dei dati (vincoli di integrità);
- alterabilità dei dati;
- interazioni non corrette con database (ad es., possibilità di eseguire comandi non previsti mediante tecniche di SQL injection, includendo query e altri statement SQL nei confronti del database causando l'acquisizione, modifica, cancellazione o introduzione di dati in maniera non controllata né autorizzata; nonché la possibile esecuzione di codice non autorizzato);
- interazioni non corrette o non appropriate con il sistema operativo (ad es., "shell escapes");

- vulnerabilità di Cross-Site Scripting, che consentono l'esecuzione di codice non controllato nel contesto di sicurezza dell'utente dell'applicativo, potendo consentire l'acquisizione di informazioni sensibili e causare, ad es., session hijacking;
- sicurezza dei dati in transito.

Altri controlli possono essere definiti quando ciò risulti appropriato, ad esempio una form web di registrazione può essere verificata nei confronti di uso improprio, race conditions e gestione non corretta di richieste concorrenti, ecc.

L'attività di assessment utilizza strumenti che vengono impiegati per facilitare l'acquisizione di content dal sito web (wget, ed altri), e per simulare interazioni tra client e server, senza richiedere l'utilizzo di un browser, in modo da non effettuare eventuali controlli di integrità implementati sul client (vari tipi di proxies, tra cui @Stake Web Proxy), tool che consentono di programmare interazioni applicative in maniera flessibile quali elza, sniffers, nonché eventuali tool sviluppati ad hoc qualora vi sia la necessità di implementare specifiche verifiche automatizzate (ad es., information gathering via SQL injection).

L'External Web Application Assessment è complementato da un'attività di External Vulnerability Assessment, che può verificare la presenza, con l'ausilio di strumenti automatici, di eventuali vulnerabilità associate all'infrastruttura ed alle componenti software utilizzate, che potrebbero essere sfruttate - ad esempio, ma non solo - per ottenere accesso a dati e/o parti applicative dell'applicativo web normalmente non rese disponibili (come vulnerabilità che abilitano il browsing di web directories e quindi espongono l'esistenza di URL "private" o comunque di content non inteso per la consultazione, vulnerabilità che permettono di esplorare codice sorgente posizionato sul server, vulnerabilità che consentono di oltrepassare barriere di sicurezza e quindi di accedere ad aree altrimenti riservate o non disponibili, ecc.). In generale è comunque sempre consigliabile effettuare un External Vulnerability Assessment per elevare il grado di sicurezza dell'infrastruttura esposta su Internet nel suo complesso.

### Pre-requisiti, vincoli e limitazioni

Il Cliente dovrà fornire il dettaglio dei Target, in termini di:

- Topologia degli Entry-Point
- Reti
- Nodi
- Domini
- Numeri e/o range telefonici in caso di WarDial
- Applicativo web, ed eventuali credenziali utente, nel caso di Web Application Assessment

Potranno essere utilizzate le Form già presenti in RIF2.



La topologia degli entry-point ha lo scopo di chiarire l'ambito sotto esame. Il dato significativo è comunque il numero di nodi Target e i loro indirizzi IP. Lo sforzo di dettaglio verrà indirizzato all'insieme dei nodi Target così caratterizzati, per i quali verrà acquisita (come descritto al Paragrafo 3.3) la licenza del prodotto "ISS Scanner Bundle". Si sottolinea ancora una volta che TUTTA l'infrastruttura IT del Cliente eventualmente visibile dall'esterno viene comunque considerata come TOE, e quindi vengono analizzati (non utilizzando il prodotto citato) anche tutti gli eventuali scenari non previsti. La licenza di "ISS Scanner Bundle" può essere ri-generata in eventuali iterazioni successive.

NOTA: Non viene eseguita l'Analisi approfondita delle Applicazioni visibili (tipicamente via Web). Applicazioni web possono essere analizzate richiedendo l'apposito servizio di Web Application Assessment.

L'Attività non comprende l'implementazione delle contromisure specificate nel "Piano di Azione", che è eventualmente da definirsi a posteriori tipicamente nella forma "Time & Material".

### Deliverables

Come sottolineato nei Paragrafi precedenti, l'Attività comprende:

- Un incontro iniziale per l'acquisizione dei dati forniti dal Cliente
- L'esecuzione da remoto (con tutti gli accordi temporali del caso)
- Un incontro di consegna del Report e presentazione dei Risultati

Il Report avrà la struttura descritta al Paragrafo 3.2, e comprenderà anche tutti i risultati di dettaglio in forma elettronica.

**Opzioni****Servizi**

#	Attività	Quotazione
A3e.1a10	External Security Auditing IP (10 nodi, 1 ripetizione)	
A3e.1a30	External Security Auditing IP (30 nodi, 1 ripetizione)	
A3e.1a50	External Security Auditing IP (50 nodi, 1 ripetizione)	
A3e.2a	External Security Auditing Sistema RAS, 1 ripetizione	
A3e.3a	External Security Auditing WarDial Light (1000 numeri, 1 ripetizione)	
A3e.4a	External Security Auditing WarDial Full (1000 numeri, 1 ripetizione)	
A3e.5a10	External Security Auditing IP (10 nodi, 4 ripetizioni/anno)	
A3e.5a30	External Security Auditing IP (30 nodi, 4 ripetizioni/anno)	
A3e.5a50	External Security Auditing IP (50 nodi, 4 ripetizioni/anno)	
A3e.6a	External Security Auditing Sistema RAS, 4 ripetizioni/anno	
A3e.7a	External Security Auditing WarDial Light (1000 numeri, 4 ripetiz./anno)	
A3e.8a	External Security Auditing WarDial Full (1000 numeri, n ripetiz./anno)	
A3e.9a	Ri-generazione Licenza "ISS Scanner Bundle"	
A3e.10a	Implementazione contromisure come da "Piano di Azione"	
A3e.11a	External Web Application Assessment, un applicativo web, incluso vulnerability assessment sul sistema	
A3e.12a	External Web Application Assessment, un applicativo web, senza vulnerability assessment (ad es., acquistato separatamente)	

**Note:**

- Le Attività A3e.1 e A3e.5 comprendono la licenza perpetua (con 1 anno di manutenzione) del prodotto "ISS Internet Scanner Bundle" (per il numero di nodi indicati), che rimane comunque di proprietà del Cliente.
- L'eventuale quotazione di anni successivi al primo deve seguire la Tabella al Paragrafo seguente, dato che non vi è più l'esigenza di includere il Prodotto. In ogni caso, l'acquisto di 2 anni (3 anni) di Servizio prevede uno sconto del 10% (20%) sul totale.
- Spese incluse.

## Internal Security Auditing

La seconda tipologia di Auditing (vedi “Adaptive Security Management”) riguarda il monitoraggio delle vulnerabilità della rete dall’interno. Il suo obiettivo è quello di esaminare le eventuali vulnerabilità e misconfigurazioni nell’architettura delle reti interne, eseguendo una operazione di scan dei suoi nodi. Le informazioni così ottenute mirano ad elevare il livello di sicurezza e di robustezza dell’architettura di rete nei confronti di un uso non autorizzato delle sue risorse da parte di eventuali intrusori, di utenti interni malintenzionati, o addirittura nei confronti di attacchi provenienti dall’interno.

Le modalità di intervento sono identiche a quelle descritte nel capitolo precedente, con le seguenti precisazioni:

- Più che mirare ad un tentativo di penetrazione (o alla dimostrazione che esso non è effettuabile), si cerca di ottenere un innalzamento del livello di sicurezza e di robustezza dell’insieme di risorse a disposizione sulla rete.
- Viene posta particolare attenzione alle relazioni di tipo trusted hosts presenti tra i nodi sotto esame.
- Il Piano di Azione è di solito principalmente dedicato alla lista di interventi da effettuare per pulire, correggere e consolidare le configurazioni di rete dei nodi sotto esame.
- L’esecuzione dei Test avverrà da una stazione mobile posizionata alternativamente in ciascuno dei segmenti di rete sotto esame.

### Documentazione prodotta

I risultati dell’attività di Internal Security Auditing saranno riportati all’interno di un documento finale, con struttura e caratteristiche analoghe al caso precedente.

### Prodotti e strumenti utilizzati

Vedi Capitolo precedente.

### Internal Web Application Assessment

La disciplina di Internal Web Application Assessment riguarda la verifica di una applicazione web dall’interno, ossia avendo accesso ai sistemi/infrastruttura che ospitano l’applicativo. Si tratta funzionalmente dello stesso tipo di indagine svolto per un External Web Application Assessment, in cui però cambia il punto di osservazione - e conseguentemente la quantità di informazioni coinvolte, a causa della maggiore visibilità disponibile. L’applicativo web da analizzare può offrire servizi via protocollo http o https.



L'assessment di tipo interno non è sinonimo di code review (disciplina nota anche come *Code Walk Through*). Qualora sia disponibile l'accesso a codici sorgenti, l'attività include verifiche volte a determinare pratiche di programmazione insicure, attraverso l'esame - in forma semi automatica - del codice. Porzioni di codice associate a funzionalità critiche (ad es., procedure di autenticazione) possono essere oggetto di un code review manuale, mentre altre aree applicative possono essere analizzate con tool automatici alla ricerca di possibili insicurezze (quali, ad es., buffer overflow). Il dimensionamento di attività di ispezione manuale del codice sarà effettuato in base a considerazioni sul volume dell'applicativo web, sulle esposizioni al rischio associabili alle componenti applicative esistenti, e non ultimo su valutazioni economiche, data l'onerosità di tale tipo di analisi.

Gli obiettivi principali dell'assessment riguardano l'analisi delle seguenti security issues:

- information leakage, cioè l'analisi di dati sensibili che possono essere esposti dall'applicativo (informazioni visibili mediante esame di pagine HTML, script embedded, altri file, o di altro materiale cui si riesca ad ottenere accesso, incluso codice server side che normalmente non è visibile dall'utente; informazioni ottenibili da commenti, messaggi di errore, od eventuali meccanismi di debugging che fossero presenti);
- gestione appropriata delle interazioni con l'utente, allo scopo di individuare possibili debolezze associate a input malformato, buffer overflow, ecc.;
- procedure di autenticazione;
- gestione della sessione, dove appropriato (meccanismi di logout, timeout della sessione, possibilità di introduzione impropria in una sessione da punti di accesso - URL - non verificati, session hijacking, ecc.);
- validazione dei dati (vincoli di integrità);
- alterabilità dei dati;
- interazioni non corrette con database (ad es., possibilità di eseguire comandi non previsti mediante tecniche di SQL injection, includendo query e altri statement SQL nei confronti del database causando l'acquisizione, modifica, cancellazione o introduzione di dati in maniera non controllata né autorizzata; nonché la possibile esecuzione di codice non autorizzato);
- interazioni non corrette o non appropriate con il sistema operativo (ad es., "shell escapes");
- vulnerabilità di Cross-Site Scripting, che consentono l'esecuzione di codice non controllato nel contesto di sicurezza dell'utente dell'applicativo, potendo consentire l'acquisizione di informazioni sensibili e causare, ad es., session hijacking;
- sicurezza dei dati in transito.



Oltre a questi punti, che sono comuni a quelli indirizzati da un assessment esterno, sono indagabili anche i seguenti:

- aspetti di configurazione di web server, application server;
- configurazione di DBMS coinvolti ed interazioni applicative con i medesimi;
- esame del content servibile dai web server/application server volto a determinare informazioni sensibili che potrebbero risultare accessibili (file di log, file di configurazione/parametri/contenenti credenziali ecc.);
- aspetti legati alla soluzione architeturale utilizzata.

Come già detto, la rilevazione di vulnerabilità può avvenire sia dall'analisi dell'applicativo (da documentazione tecnica, codice, interviste, verifiche su componenti software) nonché mediante sollecitazioni all'applicativo stesso, condotte in analogia a quanto viene fatto in un assessment esterno.

L'attività di Internal Web Application Assessment utilizza gli stessi strumenti impiegati per effettuare un assessment esterno; inoltre possono essere utilizzati tool di analisi automatica del codice.

Similmente al caso dell'assessment esterno, anche l'Internal Web Application Assessment può beneficiare dei risultati di un'attività di Internal Vulnerability Assessment, che in generale è sempre consigliabile effettuare per elevare il grado di sicurezza dell'infrastruttura utilizzata nel suo complesso.

### Pre-requisiti, vincoli e limitazioni

Il Cliente dovrà fornire il dettaglio dei Target, in termini di:

- Topologia
- Reti, sottoreti, segmenti
- Nodi
- Domini
- Applicativo web (particolari rilevanti: infrastruttura e tecnologie utilizzate; disponibilità e dimensioni di codice sorgente), ed eventuali credenziali utente, nel caso di Web Application Assessment

Potranno essere utilizzate le Form già presenti in RIF2.

NOTA: Non viene eseguita l'Analisi approfondita delle Applicazioni visibili (tipicamente via Web). Applicazioni web possono essere analizzate richiedendo l'apposito servizio di Web Application Assessment.

### Deliverables

Come sottolineato nei Paragrafi precedenti, l'Attività comprende:

- Eventuale analisi dei target in gioco (topologia) con il Cliente
- Esecuzione Scan
- Produzione di Report



Il Report avrà la struttura descritta al Paragrafo 3.2, e comprenderà anche tutti i risultati di dettaglio in forma elettronica. Al crescere del numero di nodi, tuttavia, l'Attività assume una connotazione sempre più continuativa, dovuta anche al fatto che la Rete Target è interna. Anche la produzione di Report, quindi, avrà caratteristiche di *work-in-progress* da congelare in un rilascio finale.

Al crescere del numero dei nodi, inoltre, ci si avvicina sempre più ad un *elapsed-time* di 6 mesi, che è la stima per 2000 nodi. L'opzione "2 ripetizioni/anno" intende quindi coprire, se richiesta, un *elapsed-time* di 1 anno.

## Opzioni Servizi

#	Attività	Quotazione
A4i.1	Eventuali Attività di pre-Analisi	
A4i.1a10	Internal Security Auditing IP (10 nodi, 1 ripetizione)	
A4i.1a30	Internal Security Auditing IP (30 nodi, 1 ripetizione)	
A4i.1a50	Internal Security Auditing IP (50 nodi, 1 ripetizione)	
A4i.1a100	Internal Security Auditing (100 nodi, 1 ripetizione)	
A4i.1a250	Internal Security Auditing (250 nodi, 1 ripetizione)	
A4i.1a500	Internal Security Auditing (500 nodi, 1 ripetizione)	
A4i.1a1000	Internal Security Auditing (1000 nodi, 1 ripetizione)	
A4i.1a2000	Internal Security Auditing (2000 nodi, 1 ripetizione)	
A4i.2a10	Internal Security Auditing IP (10 nodi, 2 ripetizioni/anno)	
A4i.2a30	Internal Security Auditing IP (30 nodi, 2 ripetizioni/anno)	
A4i.2a50	Internal Security Auditing IP (50 nodi, 2 ripetizioni/anno)	
A4i.2a100	Internal Security Auditing (100 nodi, 2 ripetizioni/anno)	
A4i.2a250	Internal Security Auditing (250 nodi, 2 ripetizioni/anno)	
A4i.2a500	Internal Security Auditing (500 nodi, 2 ripetizioni/anno)	
A4i.2a1000	Internal Security Auditing (1000 nodi, 2 ripetizioni/anno)	
A4i.2a2000	Internal Security Auditing (2000 nodi, 2 ripetizioni/anno)	

### Note:

- Le Attività da A4i.2 a A4i.11 comprendono la licenza perpetua (con 1 anno di manutenzione) del prodotto "ISS Scanner Bundle" (per il numero di nodi indicati), che rimane comunque di proprietà del Cliente.

## System/DataBase Security Auditing

La terza tipologia di Auditing riguarda il monitoraggio delle vulnerabilità nella configurazione di ciascun singolo sistema della rete, o di un sottoinsieme significativo di sistemi critici. Le informazioni così ottenute mirano ad elevare il livello di sicurezza e di robustezza di ciascun singolo sistema nei confronti di un uso non autorizzato delle sue risorse da parte degli utenti che vi accedono.

L'ambito di intervento dell'attività riguarda per prima cosa la rilevazione di *bug* e/o di versioni non aggiornate nei vari *subsystem* del Sistema Operativo. Viene poi effettuata la rilevazione di configurazioni errate o ritenute pericolose nel Sistema Operativo, nei suoi *subsystem* e nelle applicazioni che forniscono servizi e/o accessi agli utenti, come ad esempio *ownership* o *permission* errate, password deboli, account dormienti, misconfigurazione di servizi di rete etc.

Vengono inoltre rilevate le tracce dell'eventuale presenza di intrusioni, e viene infine calcolato un *checksum* avanzato di tutti i file critici del sistema (il cui insieme è configurabile), al fine di poter eseguire, al test successivo, un controllo di integrità che rilevi un'eventuale manomissione.

### Documentazione prodotta

I risultati dell'attività di System Security Auditing saranno riportati all'interno di un documento finale, con struttura e caratteristiche analoghe al caso precedente. Sono disponibili esempi.

### Prodotti e strumenti utilizzati

Anche in questo caso verranno utilizzati strumenti propri (anche sviluppati all'uopo), strumenti Public Domain provenienti dalla rete e dall'*underground* e strumenti commerciali, e si pone una particolare attenzione al continuo aggiornamento delle informazioni e degli strumenti utilizzati nell'Attività di Auditing, tramite gli enti internazionali preposti (CERT, CIAC, FIRST, ICSA, CSI, ISS X-Force ecc.), le mailing list e i newsgroup dedicati e le risorse dell'*underground*. L'aggiornamento si estende ovviamente anche alle versioni dei prodotti utilizzati.

In particolare, viene utilizzato il prodotto System Security Scanner (S2) di ISS. Esso è disponibile per le piattaforme Windows e per tutti i dialetti di Unix. La versione Windows dispone di *template* predefiniti dedicati all'analisi di sistemi in configurazioni critiche, quale ad esempio un Sistema Proxy con Microsoft Proxy Server.

## Intrusion Detection

L'Attività di Intrusion Detection si differenzia dalle Attività di *Vulnerabilities Management* per il fatto che avviene in modalità continuativa ed in tempo reale. Essa si riconduce ai processi di *Threat Management* (cioè di Monitoraggio delle Minacce, vedi "Adaptive Security Management"), ed il suo obiettivo è quello di istituire un presidio in grado di rilevare automaticamente (e 24 ore su 24) l'eventuale presenza di attacchi in corso nei confronti delle risorse IT sotto osservazione.



I Sistemi di Intrusion Detection (IDS, Intrusion Detection Systems) cercano di rilevare gli schemi di un attacco IT (**Signature**), cioè specifici **Pattern** che individuano un comportamento sospetto o malintenzionato.

Quando un IDS cerca i suddetti Pattern nel Traffico di Rete, si parla di Network-Based IDS.

Quando un IDS cerca i suddetti Pattern nei Log di un Sistema, si parla di Host-Based IDS.

Un IDS veramente efficace deve prevedere **entrambe le tecnologie** in maniera **integrata**, cioè con le medesime modalità e interfacce di gestione. Oltre a ciò, deve essere in grado di eseguire *Protocol Analysis* oltre che *Pattern Matching*, al fine di individuare eventi sospetti anche ai vari livelli dei protocolli di rete (pacchetti malformati ecc.).



Quindi un IDS:

- È l'equivalente di un Sistema di Allarme
- Centralizza le informazioni, analizza pattern sospetti e/o comportamenti sospetti
- Impatta il problema degli Attacchi Interni
- Analizza l'Infrastruttura IT per rilevare *Attacchi* e *azioni malintenzionate*, ove:
  - Un *Attacco* è un tentativo di guadagnare un accesso non autorizzato o di compiere azioni non autorizzate nell'Infrastruttura IT sotto esame
  - Un'*azione malintenzionata* è costituita da occorrenze di *pattern* e/o eventi che violano Politiche di Sicurezza esistenti

È molto importante che un IDS analizzi sia la Rete che i Sistemi (Server e Desktop), perchè questa è l'unica maniera per avere un'immagine completa di quanto sta accadendo.

Lo strumento di *Network-based* Intrusion Detection (detto anche sonda, probe o sniffer), installato su un nodo dedicato, viene posizionato in uno o più punti chiave della Rete (con gestione centralizzata tramite una Management Console), come ad esempio immediatamente a monte e/o a valle del Firewall, e/o in una sottorete di importanza critica. Esso esegue la ricostruzione delle sessioni in corso dall'analisi del traffico sulla Rete, ed esegue un certo insieme di Azioni (allarme, Mail, chiamata, invio di *snmp\_trap* ecc.) a fronte del riconoscimento di un'Attività sospetta.

Tale riconoscimento avviene sulla base di un vastissimo Database interno di *signature* di attacchi noti, ovviamente modificabile e aggiornabile. Tutte le sessioni possono essere seguite mentre avvengono, o essere oggetto di *record* e *play-back*. A fronte del rilevamento di Attività sospetta, un Firewall CheckPoint e/o un Router CISCO possono essere automaticamente riprogrammati, al fine ad esempio di abbattere connessioni o creare nuove regole che impediscano successivi accessi.

Si noti che anche sonde esterne (posizionate ad esempio su Internet) possono essere gestite in maniera sicura. È infatti sufficiente equipaggiare la sonda con due schede di rete: quella interna è normalmente afferente ad un qualunque segmento delle Reti interne con raggiungibilità verso la Management Console, mentre quella esterna, non necessitando di alcuna configurazione IP, è assolutamente invisibile.

La seconda modalità (*Host-based* Intrusion Detection) vede la presenza di un Agent (e quindi di un demone attivo 24 ore su 24) a bordo del singolo sistema che si vuole tenere sotto controllo, che cerca di rilevare eventuali attacchi a quel sistema, come ad esempio uso malizioso di "su", cambi di SETUID ecc..

## Prodotti utilizzati

Viene utilizzato RealSecure di ISS, ed in particolare RealSecure Network Sensor (per Network-based Intrusion Detection) e



RealSecure Server/Host Sensor (per Host-based Intrusion Detection). Entrambi includono anche la Management Console, che è la medesima in entrambi i casi.

Il DataBase di Signature di Attacco di RealSecure (sempre aggiornabile e configurabile) comprende più di 600 Signature.

La tecnologia **X-Press Updates** permette di effettuare upgrade *on-line* in maniera sicura, e quindi consente di essere aggiornati in tempo reale a riguardo delle più recenti nuove Signature di Attacco.

### Pre-requisiti, vincoli e limitazioni

È altamente consigliato che la sonda (Network Sensor) e la Management Console risiedano su macchine separate. Qualsiasi piattaforma Intel recente è utilizzabile.

Qualora una sonda risieda su una Rete *untrusted* (come ad esempio Internet), si consiglia la configurazione con doppia interfaccia di rete sopra descritta. È sempre consigliato che le schede di rete siano modelli standard noti (e non quelle fornite dagli stessi costruttori della macchina come Compaq o HP), dato che per eseguire lo *sniffing* della rete esse vengono mandate da RealSecure in *Promiscuous Mode*.

### Deliverables

Il *Deliverable* standard comprende: installazione di 1 Network Sensor, 5 Server Sensor (se richiesti) e Management Console integrata. Configurazione in modalità "Attack Detector" per il Network Sensor, e "Maximum\_<S.O.>" per il Server Sensor, con max 5 azioni automatiche.

### Nota

La "Host-based Intrusion Detection" non va confusa con la tecnologia nota come "System Scan". Quest'ultima, infatti, agisce sempre a livello di singolo Sistema, ma con uno Scanner, cioè con uno strumento che non ha alcuna vita continuativa, ma che viene lanciato quando un intervento umano (o un intervento automatico schedato) ne decreta l'utilizzo. Né più né meno che uno Scan di rete, quindi, solo che avviene a livello di Sistema, ed invece di rilevare i dati tipici di uno Scanner di rete (macchine che rispondono sulla rete, loro servizi aperti, ecc.), esegue un'Analisi della configurazione del Sistema (proprio a livello Unix o NT), e ne evidenzia gli eventuali errori e/o vulnerabilità, oltre a farne un *checksum* per un successivo Check di Integrità. Ecco perché uno strumento di questo tipo viene associato all'*Hardening* di una macchina: perché fornisce un utilissimo elenco di cose da sistemare a livello del Sistema Operativo sotto esame. Nel caso di ISS, il prodotto in questione si chiama "System Scanner", o anche "S2". Una volta era detto "S3", da "System Security Scanner".



## Opzioni

#	Attività	Quotazione
A5.1	Installazione e configurazione 1 Network Engine come da Paragrafo 6.3	
A5.2	Installazione e configurazione 1 Network Engine e 5 Host Agent come da Paragrafo 6.3	
A5.3	Fine Tuning ed eventuali Integrazioni	

Note:

- L'Attività A5.1 comprende la licenza perpetua (con 1 anno di manutenzione) del prodotto "ISS RealSecure Network Engine", che rimane comunque di proprietà del Cliente.
- L'Attività A5.2 comprende la licenza perpetua (con 1 anno di manutenzione) del prodotto "ISS RealSecure 1 Network Engine" e del prodotto "ISS RealSecure 5 Server Sensor", che rimangono comunque di proprietà del Cliente.