

*La Sicurezza Informatica e delle Telecomunicazioni
(ICT Security)*

BASE MINIMA DI SICUREZZA

Allegato 2

GENNAIO 2002

Scopo del documento è di fornire (nell'ambito del contesto normativo attuale), alcune indicazioni per assistere i Ministeri nell'individuazione delle misure di protezione che debbono essere realizzate e gestite con assoluta priorità, al fine di supportare le Amministrazioni sia nell'applicazione degli adempimenti normativi di riferimento (es 675-318) sia nel contrastare eventuali potenziali minacce ...

Le prime soluzioni di sicurezza proposte in questo documento hanno sia la caratteristica di propedeuticità realizzativa rispetto a quelle che verranno inserite successivamente nel piano complessivo, sia la peculiarità di rappresentare uno strato di base per la protezione dei sistemi ICT.

Tale strato non rappresenta certamente una soluzione completa e definitiva della sicurezza ma costituisce comunque una significativa barriera di protezione sulla quale implementare successivamente altre contromisure.

Più in dettaglio si tratta, per le Amministrazioni, di definire, progettare e realizzare, nell'arco temporale orientativo di 12 mesi, le seguenti misure.

1. ORGANIZZAZIONE DELLA SICUREZZA

Per assicurare che le contromisure individuate (qualunque siano, dalle politiche a quelle tecnologiche) possano effettivamente essere rese operative, è indispensabile integrare la struttura organizzativa esistente con una rete di responsabilità specifiche sulla sicurezza e condividere una serie di principi e regole che devono guidare la corretta gestione della sicurezza

La politica generale dell'amministrazione è di considerare e trattare le informazioni ed i servizi come parte integrante del Patrimonio; è quindi intenzione dell'Amministrazione garantire, in analogia a quanto avviene per le altre attività, il corretto svolgimento delle azioni di prevenzione, protezione e contrasto tramite la definizione delle seguenti *logiche organizzative*:

Presidio Globale: Sicurezza, analisi del rischio, controllo delle informazioni/servizi critici sono concetti che stanno assumendo una importanza sempre maggiore.

Deve essere quindi assicurata una visione unitaria e strategica a livello di Amministrazione in grado di valutare sia il rischio operativo complessivo sia le necessarie misure di sicurezza predisponendo:

a- l'istituzione un apposito " Comitato per la sicurezza ICT "

b : la nomina di un “ Consigliere Tecnico” per la Sicurezza ICT in diretto affiancamento al Ministro per tale materia.

Corretta Responsabilizzazione: la valutazione del rischio e la realizzazione della sicurezza necessaria devono essere garantite dai ruoli dell’Amministrazione che hanno a disposizione le effettive leve di responsabilità e di autonomia/delega, nonché di conoscenza dell’operatività per prendere *decisioni chiave* quali: classificare e valorizzare il bene, riconoscere un certo grado di esposizione al rischio, definire un conseguente livello di protezione, monitorare la coerenza dei comportamenti con le politiche stabilite.

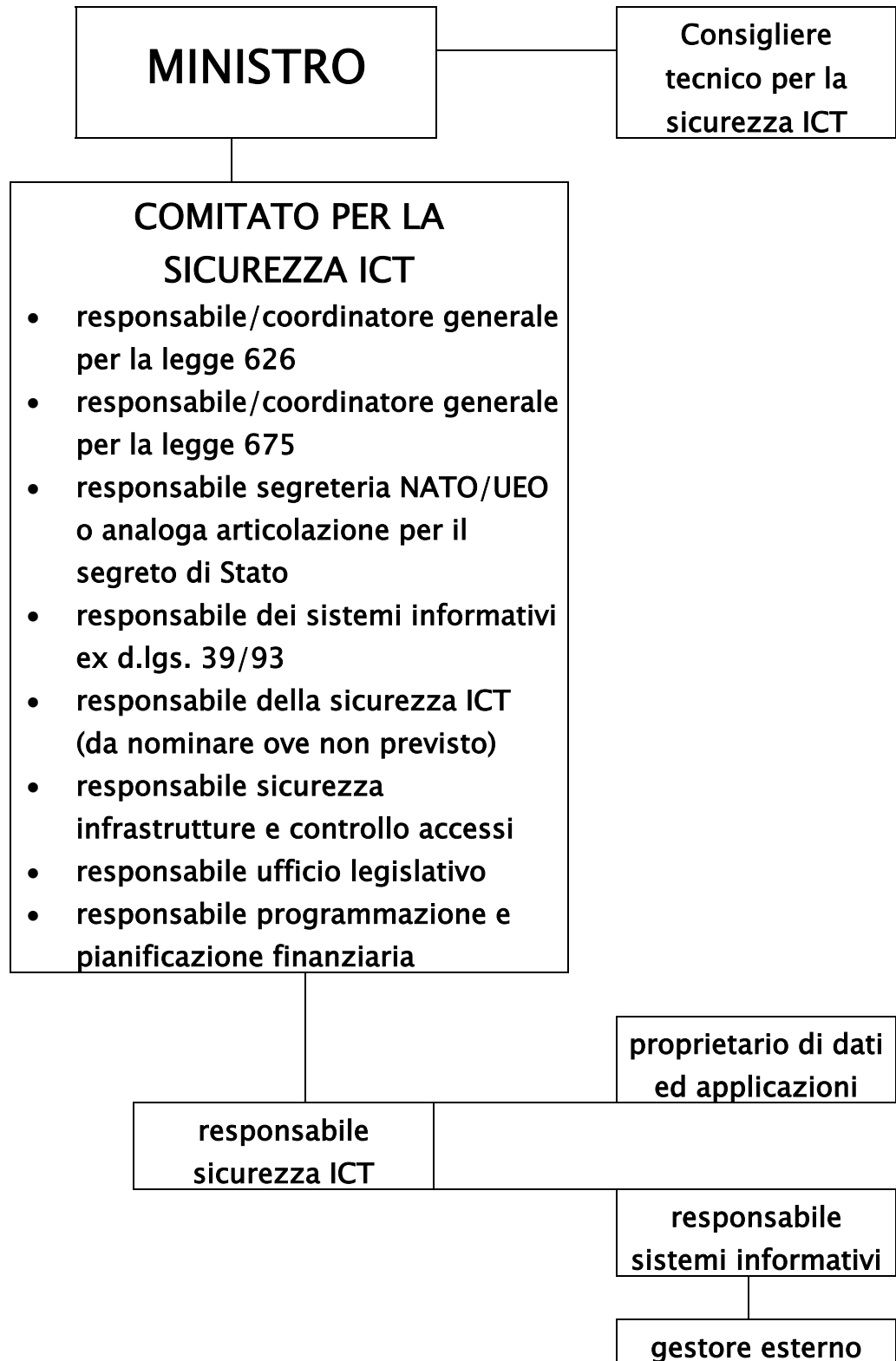
Bilanciamento Rischio/Sicurezza: essere in sicurezza significa operare avendo ottenuto una ragionevole riduzione delle probabilità di accadimento (vulnerabilità) di una determinata minaccia la cui presenza espone il bene ad un certo rischio. Qualsiasi investimento per la realizzazione di contromisure di sicurezza deve essere quindi rigorosamente collegabile al margine di riduzione del rischio ottenibile mettendo in campo quelle contromisure.

Separazione dei Compiti: vale per il processo della sicurezza il principio che “chi esegue non verifica”, distinguendo tra *monitoraggio e verifica* della sicurezza.

Per *monitoraggio* si intende l’attività di controllo continuo degli indicatori di performance, sicurezza e rischio, svolte dalla funzione/ruolo che realizza le misure di sicurezza, mentre per *verifica* si vuole significare l’attività di controllo saltuaria che si sviluppa attraverso un vero e proprio audit da parte di una funzione/ruolo (ICT Auditing) diversa da quella/o che ha realizzato la sicurezza.

Al fine di assicurare un corretto presidio organizzativo della sicurezza e consentire così sia una corretta gestione (security management system) sia una efficace diffusione e crescita della “cultura” della sicurezza, l’Amministrazione deve ancorare la Rete di Responsabilità ad un insieme di ruoli chiaramente identificati.

Segue uno schema di riferimento di Modello Organizzativo della sicurezza che soddisfa le logiche precisate.



Descrizione del modello

Ministro

Per le organizzazioni non ministeriali (es. Enti pubblici non economici) al vertice del funzionigramma deve essere collocato il Presidente o altro soggetto avente rappresentanza legale o altri poteri specificamente a lui conferiti

Consigliere Tecnico per la Sicurezza ICT

E' il consulente strategico del Ministro, l'interfaccia tra il Comitato ed il titolare del Dicastero

Comitato per la Sicurezza ICT

E' l'organo cui viene demandata la politica della sicurezza delle infrastrutture tecnologiche e del patrimonio informativo gestito prevalentemente con soluzioni automatizzate

Responsabile della sicurezza ICT

E' il soggetto cui compete la definizione delle soluzioni tattiche in attuazione alle direttive impartite dal Ministro direttamente o su indicazione del Comitato

Proprietario dei dati e delle applicazioni

E' ciascun direttore generale per la sfera di informazioni di diretta competenza o trattamento

Responsabile dei sistemi informativi automatizzati

E' il referente istituito dal decreto legislativo 39/93, cui compete la pianificazione degli interventi di automazione, l'adozione delle cautele e delle misure di sicurezza, la committenza delle attività da affidare all'esterno

Gestore esterno

E' il fornitore di servizi che opera sotto il controllo del responsabile dei sistemi informativi

Per facilitare ed accelerare lo sviluppo di una adeguata consapevolezza sui rischi e sull'esigenza di proteggere il patrimonio informativo in tutte le risorse umane dell'Amministrazione, requisito indispensabile per qualsiasi sistema di sicurezza, è inoltre necessario:

- Attuare un processo di sensibilizzazione sul valore delle informazioni, sul rischio al quale risultano esposte, sulle misure di sicurezza e sulla importanza di progettarle adeguatamente.
- Programmare una serie di comunicazioni (presentazioni, bollettini, avvisi, bacheche "virtuali", forum), finalizzate a promuovere la corresponsabilizzazione e la consapevolezza riguardo alle nuove logiche, modelli e comportamenti organizzativi della sicurezza.
- Pianificare la diffusione di informazioni "spot" relativamente agli argomenti chiave della gestione della sicurezza: analisi e gestione del rischio, pianificazione e monitoraggio delle contromisure, normativa e regolamentazione, audit e controllo.

Ciascuna Amministrazione progetterà e realizzerà la propria organizzazione della sicurezza e le sessioni formative in base alle proprie esigenze.

2. GESTIONE DELLA SICUREZZA

Per ottenere il funzionamento della sicurezza organizzativa occorre calare sulla struttura dell'Amministrazione un sistema di gestione (management system) della sicurezza composto da:

- Carta della Sicurezza, che definisce gli obiettivi e le finalità delle politiche di sicurezza, le strategie di sicurezza scelte dall'Amministrazione nonché il modello organizzativo ed i processi per attuarle.
- Politiche Generali di Sicurezza, che indicano, coerentemente con la Carta della Sicurezza, le direttive da seguire per lo sviluppo, la gestione, il controllo e la verifica delle misure di sicurezza da adottare; devono essere modificate al verificarsi di cambiamenti di scenario.
- Politiche Specifiche di Sicurezza (Norme), focalizzate sull'emissione di normative afferenti argomenti rilevanti per l'organizzazione, il Personale, i sistemi e aggiornate frequentemente sulla base dei cambiamenti organizzativi e tecnologici.

➤ Specifiche procedure, a supporto delle gestione operativa delle contromisure tecnologiche adottate. Tali procedure di base riguardano:

- La gestione della “System Security”
- La gestione della “Network Security”
- Il ciclo di vita del software
- La gestione operativa
- La continuità del servizio (Contingency Plan)
- La gestione degli incidenti
- Il controllo e il monitoraggio del sistema di sicurezza
- La sicurezza del Personale.

3. ANALISI E GESTIONE DEL RISCHIO

L’analisi del rischio è un processo fondamentale per la pianificazione, realizzazione e gestione di qualsiasi sistema di sicurezza ICT (ISMS- information security managemnt system) ...

Infatti, senza una costante valutazione del valore del patrimonio informativo, dell’intensità delle minacce attuali e potenziali, delle vulnerabilità del sistema e dei potenziali impatti tangibili e intangibili sull’attività e sul posizionamento dell’Amministrazione, risulta impossibile definire un sistema di sicurezza veramente equilibrato e bilanciato rispetto ai rischi ed ai danni/perdite che potrebbero verificarsi.

In un sistema di Governo delle P.A. sempre più aperto, cooperante, digitale ed interconnesso, anche a livello internazionale, i confini del rischio non hanno più barriere e le minacce diventano tutte possibili e, in qualche misura, sempre più probabili.

Ciascuna Amministrazione si deve pertanto dotare di un processo di analisi e gestione del rischio conforme agli standard internazionali di sicurezza, che preveda di massima i passi riportati nello schema seguente:

| Passi della Analisi del Rischio | Attività dell'Analisi del Rischio |
|---|--|
| Identificazione e Valutazione dei Beni | Elencare i beni dell'organizzazione, i processi e le informazioni valutate interne all'ambito dell'ISMS (information security management system) |
| Valutazione delle Minacce | Elencare le potenziali minacce associate alla lista dei beni utilizzando le checklist esistenti con le più conosciute e generiche vulnerabilità |
| Valutazione delle Vulnerabilità | Elencare le vulnerabilità associate alla lista dei beni utilizzando le checklist esistenti con le più conosciute e generiche vulnerabilità. |
| Identificazione dell'esistente e Pianificazione dei Controlli di Sicurezza | Identificare e documentare tutti i controlli di sicurezza esistenti/pianificati associati alla lista di beni in accordo con le precedenti revisioni della sicurezza. |
| Analisi del Rischio | Raccogliere insieme le informazioni relative ai beni , le minacce e vulnerabilità derivate dalle precedenti fasi di valutazione per fornire una semplice e pratica vista delle misure dei rischi. |
| Identificazione e Selezione dei Controlli di Sicurezza e Riduzione dei Rischi | Per ogni bene elencato identificare gli obiettivi di controllo rilevanti previsti(es dal BS 7799) ed utilizzare le minacce e le vulnerabilità correlate per selezionare quei controlli che garantiscono il raggiungimento degli obiettivi. |
| Accettazione del Rischio | Se necessario, considerare un'ulteriore riduzione dei rischi scegliendo controlli aggiuntivi in base alle reali esigenze. |

Il processo di Analisi del rischio è, tra l'altro, la "pietra angolare" che sostiene l'individuazione e la gestione delle misure minime di sicurezza per il trattamento dei dati personali richiesta dal DPR 318 della Legge 675 sulla Privacy.

4. CONTROLLO FISICO/LOGICO DEGLI ACCESSI

Il controllo degli accessi fa parte di diritto della Base Minima di sicurezza e deve essere implementata con priorità . Esso consiste nel

garantire che tutti gli accessi agli oggetti del sistema ICT avvengano esclusivamente secondo modalità prestabilite.

Seguono le indicazioni fondamentali per comprendere ed indirizzare la realizzazione di queste contromisure.

Controllo Fisico

Il controllo degli accessi fisici deve restringere i diritti di accesso del personale alle zone che ospitano risorse aziendali informatiche e non (magazzini tecnici, aree con dati e/o apparati ad alto rischio, uffici riservati, ecc.).

Gli accessi devono essere disciplinati da una procedura di carattere generale e da procedure specifiche per ogni singolo sito.

I controlli di accesso fisico alle aree devono servire a tutte le locazioni che contengono apparati di rete, LAN, impianti elettrici, impianti di condizionamento, telefoni e linee dati, supporti di backup e documenti e qualsiasi altro elemento richiesto per la gestione e manutenzione dei sistemi e non solo alla protezione dei locali contenenti sistemi hardware.

Si deve consentire l'accesso alle aree critiche compartimentate, secondo diversi livelli ed esigenze di sicurezza, alle persone preventivamente autorizzate.

Ciascun dipendente deve essere informato sulle aree di competenza in termini d'accesso fisico e d'orario.

Deve essere verificata l'efficacia dei controlli di accesso fisico alle aree sia durante il normale orario di lavoro che in altri orari .

Le procedure devono prevedere apposite regole di sicurezza in grado di disciplinare l'accesso disciplinando per singolo soggetto (es dipendente , consulente , personale di imprese varie ecc) la regola di accesso .

In particolare l'accesso ai Centri di produzione (Data Center, Call Center, ecc.) deve essere controllato tramite l'uso di badge magnetici/smart card strettamente personali rilasciati esclusivamente al personale conosciuto.

Devono essere privilegiate, evidenziando preventivamente le potenziali criticità che ne conseguono, le scelte a favore della tutela della protezione della persona , nel caso gli obiettivi del controllo degli accessi fisici siano in conflitto con quelli della Legge 626.

Controllo Logico

I controlli d'accesso logico devono fornire un modo tecnico per controllare l'accesso di un utente alle risorse di sistema ed alle informazioni al fine di garantire il controllo delle informazioni che gli utenti possono utilizzare, dei programmi che possono eseguire e delle modifiche che possono apportare.

Nella stesura delle procedure si deve tener conto che:

- L'accesso è la capacità da parte di un soggetto (utente o processo) di fare operazioni (lettura, aggiornamento, scrittura, comunicazione) che accedono e usano "oggetti" (applicazioni, programmi, dati).
- L'autorizzazione è il permesso per usare una risorsa del computer. L'autorizzazione è assegnata, direttamente o indirettamente, dal proprietario del sistema o dell'applicazione.
- L'autenticazione dimostra che gli utenti sono chi sostengono di essere.
- Il controllo d'accesso è strettamente legato all'autenticazione.

I controlli d'accesso logici devono contribuire a proteggere:

- I sistemi operativi e l'altro software di sistema dalla modifica o dalla manipolazione non autorizzata (e quindi contribuire ad accertare l'integrità e la disponibilità del sistema).
- L'integrità e la disponibilità delle informazioni limitando il numero di utenti e di processi con accesso.
- Le informazioni confidenziali dalla rilevazione agli individui non autorizzati.

Deve essere controllato il diritto d'accesso che si permette, ovvero quali sono i privilegi assegnati alle risorse in funzione del ruolo che ricoprono (per esempio la capacità per l'utente di eseguire, ma di non cambiare, i programmi di sistema, di leggere i files senza poterli riscrivere o cancellare, ecc).

Il servizio di identificazione ed autenticazione deve essere eseguito mediante tecniche basate su *password* e *userid* (identificativo utente); relativamente alla *userid* si fa riferimento alle norme previste dalla legge 675/96 e relativo DPR 318.

Tutti gli utenti interni e esterni che lavorano con continuità sui sistemi dell'Amministrazione, devono essere dotati di un proprio *userid* personale, mentre gli utenti esterni dovranno utilizzare, secondo i casi, un *userid* che identifica la persona, il ruolo o l'ente. In ogni caso è

obbligatoria l'autenticazione mediante password o altro sistema con caratteristiche di protezione più potenti.

Deve essere attivato un processo di sensibilizzazione dell'utenza per ottemperare ad una opportuna gestione delle password tramite controlli di qualità delle stesse.

La password deve essere considerata uno strumento di autenticazione poco efficace in presenza di dati particolarmente sensibili.

I dispositivi smart card devono essere privilegiati, rispetto ai badge magnetici, nei casi in cui sia necessaria una maggiore sicurezza; la smart card infatti, offre i seguenti vantaggi:

- Rende più semplici le operazioni di autenticazione in quanto l'utente deve semplicemente inserire la smart card nell'apposito alloggiamento e digitare il PIN (*Personal Identification Number*) per legittimare l'utilizzo del dispositivo; non è quindi necessario ricordare password complesse e modificarle periodicamente.
- Permette di utilizzare protocolli di autenticazione "potenti".
- Può essere impiegata per la firma elettronica dei documenti.

Ove possibile devono essere installati/attivati prodotti che offrono la funzione di "single signon " per rendere possibile un utilizzo corretto delle password e per non limitare l'usabilità delle funzioni; tale funzione infatti, richiede una sola volta l'autenticazione (la password) facendosi carico di autenticare l'utente verso gli altri sistemi, in modo automatico e trasparente per l'utente stesso.

5. PROTEZIONE ANTIVIRUS

Tutte le più recenti statistiche internazionali citano il virus informatico come la minaccia più ricorrente e più efficace. Esso può dar luogo a danni anche molto rilevanti per l'operatività e l'immagine dell'Amministrazione che, per contro, deve attivare una protezione sistematica ed adeguatamente presidiata. Relativamente a questo aspetto viene fornito un modello di procedura tipo per la gestione della contaminazione/anticontaminazione.

Il profilo del Virus

Dal punto di vista informatico il virus più comune si può definire come "una procedura automatica autoriproduttrice", quando detta procedura è eseguita, essa effettua più copie di se stessa; a loro volta le copie si moltiplicano con metodo analogo e così via. L'introduzione di applicazioni pericolose (virus) può essere causata da un'operazione

diretta o, come effetto collaterale e non individuabile, di una azione indiretta. Tra le azioni dirette vi sono il trasferimento di file, la lettura di una e-mail o di un attachment, l'installazione di una applicazione da un supporto esterno (floppy, nastro, zip) o attraverso Internet.

Tra le azioni indirette vi sono l'apertura di un file in formato Word o Excel (o tutti i formati che utilizzano un linguaggio eseguibile) contenente un macro virus o la visualizzazione di una pagina Web contenente un applet o un componente ActiveX.

In via generale, al lancio del programma eseguibile "infetto", il programma virus effettuerà le seguenti operazioni:

- Cercherà un programma eseguibile in cui riprodursi.
- Ne individuerà la prima istruzione.
- La sostituirà con una nuova istruzione che consenta di passare alla posizione di memoria successiva a quella dell'ultima istruzione del programma.
- Inserirà il codice del virus dopo l'ultima istruzione del programma.
- Inserirà dopo il codice del virus un'istruzione che emuli la prima istruzione del programma originale.
- Aggiungerà un'istruzione che passi alla seconda istruzione del programma originale.

Oltre a riprodursi, il virus informatico attuerà delle procedure dannose secondo intervalli casuali, a tempo determinato, o anche in base ad eventi di sistema.

La finalità di un virus informatico è perciò quella di nuocere al sistema usando varie metodologie orientate all'impedimento dell'accesso ai dati contenuti nel sistema stesso se non alla loro distruzione.

Un virus (trojan) può anche essere usato per violare l'integrità di un sistema di controllo accessi e consentire l'intrusione di estranei nei dati e nelle applicazioni aziendali.

Misure di prevenzione

Le applicazioni anti virus devono essere installate sui server e sui client; la frequenza di analisi del sistema deve essere quotidiana o residente in memoria. I sistemi commerciali anti virus devono essere aggiornati con frequenza settimanale, o in caso di apparizione di nuovi virus, tempestivamente.

Le workstation che possiedono applicazioni anti virus devono controllare tutti i dati che vengono immessi sul sistema.

I programmi non devono essere aperti senza essere prima sottoposti ad un'analisi. Tutti i file trasmessi attraverso la rete (comprese le e-mail) devono essere analizzati al momento della ricezione. L'analisi delle informazioni in transito tra interno ed esterno deve avvenire al perimetro della rete effettuando l'analisi attraverso i sistemi di accesso (firewall o server posta). Tale approccio permette il controllo e la gestione dei sistemi anti virus in modo centralizzato e rende più efficiente:

- L'uso delle risorse di elaborazione dei sistemi (l'analisi avviene una sola volta).
- L'amministrazione.
- L'aggiornamento dei sistemi anti virus.

Funzioni dei programmi antivirus

Un programma che si proponga di instaurare un livello sufficiente di sicurezza e protezione da virus informatici deve essere dotato di precise funzioni.

Il sistema di difesa dovrà avere:

- Il modo di funzionamento non intrusivo nei confronti del sistema, con impatto minimo e possibilità di ottimizzazione dell'occupazione di memoria.
- La presenza di funzioni di individuazione virus di bootstrap e di file.
- La possibilità di individuare i virus residenti in memoria è un requisito fondamentale del prodotto antivirus: in caso contrario, il prodotto stesso può divenire veicolo di propagazione.
- La possibilità di scoprire virus auto-mutanti (polimorfi).
- La possibilità di individuare infezioni relative al settore Master Boot Record.
- La possibilità di individuazione dei virus in file compressi. Il virus può essere localizzato all'interno del file compresso, o all'esterno del file ma compresso con esso.
- La possibilità di dirottare l'output su file o stampante: ciò risulta particolarmente utile in caso di numero elevato di file infettati, o rimozioni incomplete.
- La possibilità di notificare automaticamente al network manager l'esistenza del virus
- La possibilità di verificare il comportamento dell'anti virus in caso di file di rete aperti momentaneamente in lettura o scrittura

- La possibilità di controllo in tempo reale dei file in download da reti esterne, tenendo comunque presente che le indicazioni di sicurezza limitano la possibilità di collegamenti diretti verso l'esterno, possibili solo con la mediazione di server opportunamente protetti.
- La velocità di esecuzione molto alta: è un parametro importante in quanto l'operazione di controllo, se non effettuata sistematicamente, aumenta notevolmente la percentuale di rischio.
- La percentuale di falsi allarmi molto bassa: è un problema abbastanza diffuso fra gli antivirus e causa inconvenienti e costi non indifferenti agli utenti.
- La modalità di aggiornamento complete con funzioni per individuare efficientemente virus di tipo auto-criptato, tutti quei virus cioè, in grado di rendere la propria "firma" nel file contaminato illeggibile grazie a tecniche di crittografia variabili nel tempo;
- La garanzia di integrità del file di aggiornamento (controllato tramite checksum).
- La possibilità di specificare l'area di ricerca per velocizzare l'impiego, indicando l'area di ricerca, il tipo di file in cui cercare un virus o se quest'ultimo risiede in memoria, in un file su disco, sul settore di boot, o in altre zone specifiche tipiche dell'azione dei virus informatici.
- La disponibilità di opzioni di rimozione. Ad esempio, possibilità di rimozione del virus ricreando un file pulito senza modificare l'originale, opzioni di cancellazione definitiva o tentativo di preservazione tramite ridenominazione del file infetto.
- La possibilità di intercettare i virus "furtivi" (stealth) di nuova generazione che agiscono prendendo il controllo o perturbando le richieste d'interruzione (Interrupt) hardware e software interne al computer per evitare l'individuazione.
- La possibilità di intercettare un virus in presenza di più partizioni attive contemporaneamente.
- La possibilità di controlli sulla memoria RAM in tutti i suoi indirizzi.
- La possibilità di individuare e rimuovere virus in assenza di comandi utente, possibilità di esecuzione ad intervalli regolari.
- L'impossibilità per l'utente di cambiare la configurazione del programma a meno che non disponga dell'apposita password.
- La possibilità di fornire reporting su rete, aggiornare il file di log ad ogni esecuzione con l'indicazione dell'identificativo della workstation.

- La possibilità di produrre certificazioni esterne per integrità.
- La capacità di fornire chiare indicazioni sul proprio corretto funzionamento. Questa caratteristica è di fondamentale importanza, in quanto la consapevolezza del funzionamento di un anti virus, si ha solo al momento della scoperta del virus stesso.
- Il programma anti virus deve disporre di un metodo di auto validazione dopo l'installazione che fornisca l'assoluta certezza di funzionalità e non contaminazione.
- La possibilità di personalizzare i messaggi verso l'utente: la messaggistica all'utente riveste un ruolo di primaria importanza in quanto le operazioni da effettuare, una volta scoperto il virus, sono diverse. Come informativa minima, deve essere prodotto un rapporto sui rischi connessi al tipo di virus individuato, lo stato di avanzamento dell'infezione, le istruzioni per la rimozione e debbono essere date chiare indicazioni sulla necessità o meno di un immediato fermo macchina.

6. GESTIONE DEI SUPPORTI

L'Amministrazione deve assicurare che tutti i supporti informatici e cartacei vengano gestiti nel rispetto cosciente del bene aziendale (informazione) ivi contenuto e in ottemperanza ai dettati della legge sulla privacy e della gestione degli incidenti e delle emergenze.

Deve essere tenuto in considerazione dagli addetti, in sede di sviluppo delle applicazioni, il tema del "back-up" su supporto elettronico, predisponendo le applicazioni stesse in modo da essere trasportabili in caso di disastro o facilmente ripristinabili in fase d'emergenza.

Le copie dei programmi applicativi, dati, documentazione a supporto e software di sistema operativo usato in produzione richiedono una sicurezza fisica e logica; per quanto riguarda la sicurezza fisica devono essere depositate in un'ubicazione separata che agisca da Archivio di Sicurezza.

Relativamente ai dettati sulla gestione cartacea della legge 675/96 (tutela della privacy) e relativo DPR 318/99:

- Deve essere controllato che gli atti e i documenti contenenti i dati personali siano conservati in archivi ad accesso selezionato, e cioè organizzato in maniera tale che le pratiche conservate siano suddivise per argomenti, tipologie, caratteristiche omogenee, ecc.. Gli accessi dovranno perciò essere organizzati in maniera selettiva, con riferimento ai soli elementi necessari al tipo di consultazione.
- Deve essere controllato che gli atti e i documenti contenenti i dati personali che sono affidati agli incaricati del trattamento, vengano da questi ultimi conservati e restituiti al termine delle operazioni affidate.
- Deve essere controllato che gli atti e i documenti contenenti i dati personali che sono affidati agli incaricati del trattamento si riferiscono a dati inerenti agli articoli 22 e 24 della legge (sensibili e giudiziari). In tal caso:
 - Deve essere controllato che tali atti e documenti siano trattenuti dagli incaricati del trattamento, solo per il periodo necessario e sufficiente a svolgere la consultazione necessaria
 - Deve essere controllato che tali atti e documenti siano trattenuti e conservati, dagli incaricati del trattamento, in contenitori muniti di serratura.
- Deve essere controllato che gli archivi custodiscano dati inerenti agli articoli 22 e 24 della legge (sensibili e giudiziari). In tal caso, si deve predisporre una procedura per la verifica che l'accesso agli archivi sia controllato, prevedendo all'obbligo di identificare e registrare i soggetti che vi sono ammessi dopo l'orario di chiusura degli archivi stessi.
- Deve essere emanata una norma organizzativa scritta che imponga il controllo dei supporti magnetici prima della loro riutilizzazione. Nel caso i dati registrati non possano essere definitivamente cancellati, la norma deve prevedere la distruzione del supporto, vietandone tassativamente il riutilizzo. (Riguarda il caso di trattamento dei dati

di cui agli articoli 22 e 24 della legge 675/96 effettuato con gli strumenti di cui all'articolo 3).

- Deve essere controllato che i supporti non informatici contenenti la riproduzione di informazioni relative al trattamento di dati personali di cui agli articoli 22 e 24 della legge siano conservati e custoditi in archivi ad accesso selezionato e, se affidati agli incaricati del trattamento, che siano da questi ultimi conservati e restituiti al termine delle operazioni affidate; tali atti e documenti contenenti i dati devono essere conservati fino alla restituzione, in contenitori muniti di serratura.

In caso di incidente tutte le Aree devono fornire l'assistenza necessaria alla squadra di Pronto Intervento, attestando con apposito documento la validità delle prove condotte sui supporti informatici di back-up ed assicurando che i controlli amministrativi e di protezione sulle informazioni e sulle applicazioni continuino ad essere efficaci. La documentazione delle prove deve essere tenuta a disposizione per eventuali verifiche a posteriori.

Le informazioni riguardanti le attività vitali devono essere duplicate ed i relativi supporti conservati in un apposito archivio di sicurezza, la cui gestione è disciplinata da specifiche procedure.

Queste procedure devono prevedere che:

- I movimenti dei supporti ed il loro trasferimento avvenga in modo controllato.
- Si accerti, almeno una volta l'anno, l'effettiva giacenza fisica dei supporti.
- Siano stabilite le modalità ed i comportamenti da tenere in caso effettivo di emergenza/disastro.

Il materiale deve essere inventariato e, periodicamente, deve esserne verificata la disponibilità e la validità.

7. LA GESTIONE DEGLI INCIDENTI

Assume priorità la predisposizione di una procedura per la Gestione degli Incidenti e l'approntamento di uno specifico presidio organizzativo denominato CERT-AM: Computer Emergency Response Team dell'Amministrazione.

Un incidente è definito come un evento che può avere effetti negativi sulle operazioni del sistema e che si può configurare come frode, danno, abuso, compromissione dell'informazione, perdita di beni.

La gestione degli incidenti è strettamente legata alla pianificazione delle eventualità critiche.

La struttura di gestione degli incidenti deve essere considerata una componente della pianificazione, poiché garantisce la possibilità di rispondere rapidamente ed efficientemente all'evento negativo e di portare a termine le normali operazioni in seguito a danneggiamento.

Occorre prevedere:

- Contenimento e riparazione del danno derivante dagli incidenti.
- Prevenzione dei danni futuri.
- Benefici collaterali.

I membri del gruppo di gestione degli incidenti devono avere le opportune conoscenze e capacità, sia di tipo tecnico che non tecnico, che sono:

- Familiarità con la tecnologia cui si rivolge la struttura di gestione degli incidenti.
- Abitudine a lavorare in un gruppo.
- Abitudine a comunicare in maniera efficace con diversi tipi di utenti, che vanno dall'amministratore di sistema agli utenti inesperti ed ai dirigenti.
- Disponibilità ad intervenire ventiquattro ore su ventiquattro.
- Possibilità di spostamenti rapidi.

È estremamente importante imparare a rispondere in maniera efficace ad un incidente. Le ragioni principali sono:

- Evitare danni diretti alle persone.
- Evitare danni economici: se il personale che deve rispondere ad un incidente è stato adeguatamente istruito, il tempo richiesto a queste persone per gestire l'incidente è ragionevolmente limitato e possono essere utilizzate in altri ambiti.
- Proteggere informazione classificata, sensibile o proprietaria: uno dei danni maggiori di un incidente alla sicurezza è che l'informazione potrebbe rivelarsi irrecuperabile. Un'opportuna gestione degli incidenti minimizza questo pericolo.

- Limitare i danni all'immagine dell'organizzazione: le notizie sugli incidenti di sicurezza tendono a danneggiare il rapporto di fiducia tra un'organizzazione, le persone, le altre organizzazioni e l'opinione pubblica.

È importante stabilire con anticipo la priorità delle azioni da compiere durante un incidente. A volte un incidente può essere troppo complesso da fronteggiare in modo globale e simultaneo in tutte le sue implicazioni quindi è essenziale stabilire le priorità:

Priorità 1: proteggere la sicurezza delle persone

Priorità 2: proteggere i dati classificati o sensibili

Priorità 3: proteggere gli altri dati, inclusi i dati scientifici, proprietari e relativi alla gestione

Priorità 4: prevenire i danni al sistema

Priorità 5: minimizzare i danni alle risorse tecnologiche ed elaborative.

Chi deve essere avvertito

Il personale tecnico, gli Amministratori, i gruppi di risposta, le forze di polizia, i fornitori e distributori del software, altri fornitori di servizio. In casi specifici e preventivamente individuati, può essere anche necessario informare la stampa e/o la comunità degli utenti ed altre organizzazioni che potrebbero essere vittime dello stesso tipo di incidente.

Chi deve essere coinvolto

Per la gestione degli incidenti, deve essere creato un gruppo di risposta agli incidenti formato da Tecnici specialisti delle varie Aree Tecnologiche e da Esperti funzionali dell'Amministrazione.

Risposta all'incidente

La risposta ad un incidente si svolge attraverso le fasi di contenimento, di eliminazione, di ripristino e di azione successiva all'incidente.

Le procedure per trattare questo tipo di problema devono essere chiaramente formalizzate e comunicate. Occorre prevedere:

- Chi ha l'autorità di decidere quali azioni intraprendere
- In che momento e se devono essere coinvolte le forze di polizia

- Come e quando l'organizzazione deve cooperare con altre per cercare di risalire all'intruso
- Se l'intrusione deve essere fermata immediatamente dopo il rilevamento o l'intruso deve poter continuare la sua attività, per poterla registrare e utilizzare come prova

Come rilevare un incidente

Per stabilire se un determinato comportamento sospetto é indicativo di un incidente, bisogna analizzarlo alla luce delle seguenti considerazioni:

- discrepanze nell'uso degli account;
- modifica e sparizione di dati;
- cattive prestazioni del sistema (così come percepite dagli utenti);
- irregolarità nell'andamento del traffico;
- irregolarità nei tempi di utilizzo del sistema;
- quote particolarmente elevate di tentativi di connessione falliti.

Ovviamente, per rilevare anomalie bisogna avere un'idea precisa di che cosa possa essere considerato "normale". L'utilizzo di strumenti automatici per la rilevazione dell'andamento del traffico può senz'altro aiutare. Inoltre, invece di illudersi sulla possibilità di rilevare e bloccare tutte le intrusioni sul nascere, é preferibile concentrarsi su procedure che consentono di limitare l'impatto delle violazioni. Data l'enorme diversità degli attacchi, l'impiego di strumenti automatici é fondamentale. I sistemi di rilevamento automatico delle intrusioni si basano su di una combinazione di analisi statistiche e verifica della rispondenza alle regole.

Squadra di pronto intervento (CERT-AM)

Deve essere costituita una squadra di intervento per gli incidenti, in modo da poterli limitare e prevenire in maniera efficace ed economica.

La maggior parte dei programmi per la sicurezza informatica non sono efficaci quando si tratta di gestire nuove classi di minacce poco diffuse. Le risposte tradizionali, cioè l'analisi del rischio, la pianificazione delle emergenze e della revisione della sicurezza dei computer, non sono in genere sufficienti per controllare incidenti e per prevenire gravi danni relativamente a minacce poco probabili o poco note, quindi si devono attivare procedure organizzative reattive anziché misure tecnologiche protettive che potrebbero risultare troppo onerose.

La squadra di intervento deve essere preparata a rilevare ed a reagire agli incidenti garantendo:

- Risposta efficace e preparata
- Centralizzazione e non duplicazione degli sforzi
- Incremento della consapevolezza degli utenti rispetto le minacce.

Una squadra di risposta agli incidenti è costituita da alcune componenti fondamentali, tra cui un ufficio di *help desk*, una linea di comunicazione centralizzata e il personale con adeguate capacità tecniche.

Caratteristiche fondamentali di una squadra di intervento sono:

- La dimensione e l'area di impiego della squadra, che nella maggior parte dei casi è l'organizzazione stessa.
- La struttura, che può essere centralizzata, oppure distribuita.
- I meccanismi di comunicazione centralizzati per diminuire i costi operativi e il tempo di risposta.
- I meccanismi di allarme distribuiti nell'area che viene servita dalla squadra.
- Il personale con competenze tecniche e con capacità di comunicare e di tenere la situazione sotto controllo.