REGIONE EMILIA-ROMAGNA
Atti amministrativi

GIUNTA REGIONALE

Atto del Dirigente:	DETERMINAZIONE n° 7222 del 30/05/2012
Proposta:	DPG/2012/7342 del 16/05/2012
Struttura proponente:	SERVIZIO SISTEMA INFORMATIVO - INFORMATICO REGIONALE DIREZIONE GENERALE CENTRALE ORGANIZZAZIONE, PERSONALE, SISTEMI INFORMATIVI E TELEMATICA
Oggetto:	DISCIPLINARE TECNICO PER LA GESTIONE DEGLI INCIDENTI DI SICUREZZA INFORMATICA DELLA GIUNTA E DELL'ASSEMBLEA LEGISLATIVA DELLA REGIONE EMILIA ROMAGNA
Autorità emanante:	IL DIRETTORE - DIREZIONE GENERALE CENTRALE ORGANIZZAZIONE, PERSONALE, SISTEMI INFORMATIVI E TELEMATICA
Firmatario:	LORENZO BROCCOLI in qualità di Direttore generale
Luogo di adozione:	BOLOGNA data: 30/05/2012

DIREZIONE GENERALE CENTRALE ORGANIZZAZIONE, PERSONALE, SISTEMI INFORMATIVI E TELEMATICA
IL DIRETTORE

Visto il Decreto Legislativo 30 giugno 2003, n. 196 “Codice in materia di protezione di dati personali” (di seguito denominato Codice) con particolare riferimento agli articoli 31 ss. nonché il disciplinare tecnico in materia di misure minime di sicurezza di cui all’Allegato B del Codice;

Viste le deliberazioni della Giunta regionale:

- n. 2416/2008 del 29/12/2008 “Indirizzi in ordine alle relazioni organizzative e funzionali tra le strutture e sull'esercizio delle funzioni dirigenziali. Adempimenti conseguenti alla delibera 999/2008. adeguamento e aggiornamento della delibera 450/2007.” e in particolare l’Appendice 5 “Direttiva in materia di trattamento di dati personali con particolare riferimento alla ripartizione di competenze tra i soggetti che effettuano il trattamento”;
- n. 1264 del 01/08/2005 avente ad oggetto “Linee guida della Giunta della Regione Emilia-Romagna in materia di protezione dei dati personali”;
- n. 2199 del 19/12/2005 “Adozione del Codice di comportamento della Regione Emilia-Romagna, ai sensi dell'art. 25 della l.r. 26 novembre 2001, n. 43”;

Viste inoltre le proprie determinazioni:

- n. 6928/2009 “Disciplinare tecnico su modalità e procedure relative alle verifiche di sicurezza sul sistema informativo, ai controlli sull’utilizzo dei beni messi a disposizione dall’Ente (da ora in poi si intende Giunta ed Assemblea Legislativa) per l’attività lavorativa con particolare riferimento alle strumentazioni informatiche e telefoniche ed esemplificazioni di comportamenti per il corretto utilizzo di tali beni, da applicare nella Giunta e nell’Assemblea Legislativa della Regione Emilia-Romagna”;
- n. 1703/2009 “Disciplinare Tecnico per la gestione degli incidenti di sicurezza informatica della Giunta e dell'Assemblea Legislativa della Regione Emilia-Romagna” che definiva il carattere sperimentale delle prescrizioni in esso contenute;
- n. 130/2010 “Nomina dei componenti dell'Unita' di gestione degli incidenti di sicurezza informatica (UGISI) ai sensi della determinazione n. 1703/2009”;
- n. 2564/2010 “Proroga del periodo di sperimentazione previsto dalle determinazioni n. 1416/2009 (Disciplinare tecnico per amministratori di sistema della Giunta e dell’Assemblea Legislativa) e n. 1703/2009 (Disciplinare tecnico per la gestione degli incidenti di sicurezza informatica della Giunta e dell’Assemblea Legislativa della Regione Emilia-Romagna) con la quale si è provveduto a prorogare il periodo di sperimentazione fino al 31 marzo 2011;
- n. 597/2012 “Disciplinare tecnico per amministratori di sistema della Giunta e dell'Assemblea legislativa della Regione Emilia-Romagna”
- n. 4856/2008 “Disciplinare Tecnico in materia di videosorveglianza nella Giunta e nell'Assemblea legislativa della Regione Emilia-Romagna”;
- n. 2649/2007 “Disciplinare Tecnico relativo al controllo degli accessi ai locali della Giunta della Regione Emilia-Romagna”;
- n. 2651/2007 “Disciplinare Tecnico in materia di sicurezza delle applicazioni informatiche nella Giunta della Regione Emilia-Romagna”;
- n. 14852/2011 “Disciplinare Tecnico per utenti sull’utilizzo dei sistemi informativi della Giunta e dell’Assemblea Legislativa della Regione Emilia-Romagna”;
- n. 4213/2009 “Linee guida per la *governance* del sistema informatico regionale;

Viste le deliberazioni dell'Ufficio di Presidenza dell'Assemblea legislativa regionale:

- n. 197 del 18 ottobre 2006 "Direttiva e Linee guida dell'Assemblea legislativa della Regione Emilia-Romagna in materia di protezione dei dati personali, con particolare riferimento alla ripartizione di competenze tra i soggetti che effettuano il trattamento. - Modifica ed integrazione della deliberazione n. 45/2003 e n. 1/2005";
- n. 43 del 29 marzo 2011 "Modifiche ed integrazioni alla delibera n. 197/2006 concernente le direttive e linee guida dell'Assemblea legislativa in materia di protezione dei dati personali e alla delibera n. 10 del 2011, recante "Aggiornamento dei Responsabili ai sensi del D.Lgs. 30 giugno 2003, n. 196 in materia di trattamento dei dati personali - anno 2011";
- n. 173 del 24 luglio 2007 "Parziali modifiche e integrazioni agli indirizzi in ordine alle relazioni organizzative e funzionali tra le Strutture e sull'esercizio delle funzioni dirigenziali approvati con deliberazione n. 45/2003";
- n. 183/2005 di approvazione del Codice di comportamento;

Viste le determinazioni:

- n. 33 del 11/02/2008 "Disciplinare Tecnico relativo al controllo degli accessi ai locali della Assemblea legislativa della Regione Emilia-Romagna";
- n. 120 del 29/03/2011 "Parziali modifiche al "Disciplinare tecnico relativo al controllo degli accessi ai locali dell'Assemblea legislativa della Regione Emilia-Romagna" approvato con Determinazione n. 33 del 06/02/2008";
- n. 480 del 28/11/2007 "Disciplinare Tecnico in materia di sicurezza delle applicazioni informatiche nella Assemblea legislativa della Regione Emilia-Romagna";
- n. 195 del 05/05/2010 "Nomina dei componenti dell'Unità di gestione degli incidenti di sicurezza informatica (UGISI)";

Considerato che:

- i sopra richiamati articoli 31 e ss. del Codice impongono ai titolari di trattamenti di dati personali l'obbligo di adottare e predisporre tutte le misure di sicurezza preventive ritenute necessarie per ridurre al minimo i rischi di distruzione, perdita, accesso non autorizzato o trattamenti non consentiti relativamente ai suddetti trattamenti;
- la predisposizione di idonee procedure da seguire nel caso in cui si verifichino incidenti di sicurezza è quindi essa stessa una delle misure di sicurezza di cui al precedente alinea;

Valutato inoltre che, oltre che essere soggetta a precisi vincoli di legge imposti dal Codice:

- la tutela del patrimonio delle informazioni riveste importanza strategica per la Giunta e per l'Assemblea legislativa della Regione Emilia-Romagna,;
- il sistema informativo regionale è costituito da un'infrastruttura tecnologica molto articolata e complessa per cui si rende necessario assicurare maggiore organicità e coordinamento all'attività del personale informatico incaricato di gestire e amministrare i sistemi informatici e telematici anche a fronte di possibili incidenti di sicurezza;
- gli incaricati della gestione tecnica e amministrazione di sistemi, postazioni di lavoro, applicazioni informatiche, basi dati, apparati di rete svolgono compiti delicati che hanno un ruolo determinante per la sicurezza dell'intero patrimonio informativo dell'Ente e devono conoscere le azioni e i comportamenti che sono da intraprendere al verificarsi delle diverse tipologie di incidenti di sicurezza;

Ritenuto quindi per tutti i motivi sopraesposti di dover esplicitare e disciplinare le attività svolte dagli incaricati della gestione tecnica e amministrazione di sistemi, postazioni di lavoro, applicazioni informatiche, basi dati, apparati di rete a fronte di incidenti, al fine di assicurare organicità e coerenza nello svolgimento delle stesse promuovendo comportamenti coerenti ed omogenei di tutto il personale coinvolto;

Considerato che durante la fase di sperimentazione si sono rilevate alcune possibilità di semplificazione delle procedure precedentemente previste, con particolare riferimento ad una semplificazione del workflow relativo all'iter da effettuare qualora si verifichi un incidente di sicurezza, compreso l'utilizzo di uno strumento informatico a ciò predisposto, che comporta che una serie di operazioni vengano effettuate in modo automatizzato;

Considerato inoltre che, nel periodo di sperimentazione si è altresì rilevato che la maggior parte degli incidenti di sicurezza derivano da Malfunzionamento e che, in questo caso, è utile che sia proceduralizzata la gestione dei soli incidenti che presentano una gravità "alta";

Considerato peraltro che nel periodo di concreta applicazione è stata nominata l'UGISI, ma non è stato possibile sperimentare l'intero disciplinare di cui alla precedente determinazione n. 2653/2007, in quanto gli incidenti occorsi in questo periodo di tempo sono stati quasi esclusivamente provocati da Malfunzionamento;

Valutato pertanto di dover aggiornare il precedente disciplinare con le semplificazioni che si sono rivelate individuate come possibili;

Valutato infine di prorogare la fase di sperimentazione per poter testare le procedure in casi diversi dal Malfunzionamento e al contempo per sperimentare anche gli aggiornamenti effettuati e verificare che producano effettivamente una semplificazione delle procedure;

Acquisito il parere favorevole espresso dal Direttore Generale dell'Assemblea Legislativa, con nota prot. PG/2012/54678 del 01/03/2012;

Sentito il parere del Comitato di Direzione nella seduta del 13/02/2012;

Dato atto del parere allegato;

DETERMINA

1. di approvare l'allegato "Disciplinare tecnico per la gestione degli incidenti di sicurezza informatica della Giunta e dell'Assemblea Legislativa della Regione Emilia-Romagna";
2. di delegare il Responsabile della Sicurezza della Giunta ad effettuare il coordinamento e l'aggiornamento della designazione, qualora lo stesso si renda necessario, degli incaricati dell'unità di gestione degli incidenti di sicurezza informatica fornendo agli stessi le istruzioni di cui al suddetto Allegato con mezzi che attestino la certezza dell'avvenuta ricezione, a partire dalla data di adozione del presente atto;
3. di dare atto che il Direttore generale dell'Assemblea legislativa provvederà a delegare il Responsabile della sicurezza dell'Assemblea legislativa ad effettuare il coordinamento e l'aggiornamento della designazione, qualora lo stesso si renda necessario, degli incaricati dell'unità di gestione degli incidenti di sicurezza informatica fornendo agli stessi le istruzioni di cui al suddetto Allegato con mezzi che attestino la certezza dell'avvenuta ricezione, a partire dalla data di adozione del presente atto;
4. di disporre che il suddetto Allegato sia portato a conoscenza degli amministratori di sistema e dei componenti l'unità di gestione degli incidenti di sicurezza informatica con mezzi che attestino la certezza dell'avvenuta ricezione a partire dalla data di adozione del presente atto;
5. di applicare l'allegato "Disciplinare tecnico per la gestione degli incidenti di sicurezza informatica della Giunta e dell'Assemblea Legislativa della Regione Emilia-Romagna" dall'adozione del presente atto; da tale momento l'applicazione dell' Allegato sarà attuata in via sperimentale per la durata di un ulteriore anno, trascorso il quale l'Allegato sarà confermato o modificato sulla base degli esiti della sperimentazione.

Lorenzo Broccoli

Allegato

Disciplinare tecnico per la gestione degli incidenti di sicurezza informatica della Giunta e dell'Assemblea Legislativa della Regione Emilia-Romagna

INDICE

1 Premessa e finalità

La finalità del presente disciplinare è quella di individuare, il più puntualmente possibile, le azioni e i comportamenti da intraprendere al verificarsi delle diverse tipologie di incidenti di sicurezza informatica.

La decisione su quali soluzioni adottare è peraltro demandata all'unità di gestione degli incidenti di sicurezza informatica con l'eventuale ausilio degli amministratori di sistema e di tutti coloro che potenzialmente devono intervenire in caso di incidenti di sicurezza, tenendo conto della particolare situazione verificatasi nel caso concreto, in quanto la natura, complessità e variabilità dell'argomento trattato, non consentono di organizzare in uno schema rigido e strutturato una procedura di gestione incidenti che tenga conto di tutte le possibili situazioni.

Nel presente Disciplinare ogni qualvolta si fa riferimento a 'incidente' o 'incidente di sicurezza', ci si riferisce ad 'incidente di sicurezza delle informazioni trattate con l'ausilio di strumentazioni informatiche', salvo esplicita indicazione contraria.

Analogamente ogniqualvolta si fa riferimento a 'sistema', ci si riferisce a una postazione di lavoro, server, dispositivo di rete o di sicurezza, e in generale a qualunque dispositivo elettronico utilizzato per trattare informazioni.

2 Incidenti

2.1 Tipologie Incidenti

Di seguito si elencano le tipologie di incidenti che possono presentarsi:

Tabella 1: Tipologia Incidenti

Tipologia Incidente	Descrizione
Accesso Non Autorizzato	Accesso (sia logico che fisico) a reti, sistemi, applicazioni, dati o altre risorse tecnologiche di proprietà della Regione Emilia Romagna da parte di personale non autorizzato.
Denial of Service	Attacco informatico, intenzionale o non, alla disponibilità di una rete o sistema. Qualora abbia successo, comporta la difficoltà all'accesso o la totale indisponibilità di determinati sistemi e/o servizi.
Codice Malevolo	Un virus, worm, trojan, backdoor, spyware, o qualsiasi altro codice malevolo che infetti un sistema.
Malfunzionamento	Danneggiamento di un componente hardware (es.: hard-disk, RAM, scheda di rete) o software, oppure degrado delle performance per cause esterne o di servizio.
Uso Inappropriato	Violazione delle policy di sicurezza e delle relative normative.
Disastro	Qualsiasi evento distruttivo, non provocato direttamente da azione di operatori informatici

	(es.: corto circuito, incendio, allagamento, terremoto) che condiziona direttamente l'operatività dei sistemi informatici.
Multiplo	Incidente di sicurezza che comprende due o più di quelli sopra elencati.

Al fine di comprendere in quale categoria classificare un incidente di sicurezza, è possibile far riferimento al meccanismo di trasmissione utilizzato. Es.:

- un virus che crea una backdoor dovrebbe essere catalogato come tipologia *Codice Malevolo*, in quanto è presente un unico meccanismo di trasmissione;
- un virus che crea una backdoor che è utilizzata per ottenere un accesso logico non autorizzato, dovrebbe essere catalogato come tipologia *Multiplo*, in quanto sono presenti due meccanismi di trasmissione.

2.2 Eventi

Un evento è un qualsiasi elemento (es.: evidenza oggettiva, nuova vulnerabilità scoperta, crash di un sistema) che indichi il concreto verificarsi o la possibilità che si verifichi un incidente di sicurezza.

E' possibile classificare gli eventi in due macro categorie: quelli che evidenziano che l'incidente di sicurezza si è verificato o si sta verificando (eventi indicativi), e quelli che denotano che un incidente potrebbe verificarsi in futuro, dando quindi l'opportunità di prevenirlo (eventi preventivi).

Riportiamo alcuni esempi nella tabella sottostante:

Tabella 2: Eventi

Eventi Indicativi	Eventi Preventivi
Crash del Web Server; Presenza di un log che evidenzia molti tentativi di accesso ad una applicazione; Modifica del normale flusso di traffico interno della rete aziendale; Alert del software antivirus; Alert dei dispositivi di Intrusion Detection System; ecc.	Annuncio di un nuovo exploit relativo ad una vulnerabilità scoperta nel software utilizzato per la gestione della posta elettronica della organizzazione; Presenza di un log che evidenzia l'utilizzo di un Vulnerability Scanner; ecc.

Non tutti gli incidenti di sicurezza possono essere caratterizzati da eventi di tipo preventivo.

E' possibile inoltre classificare gli eventi in base alla categoria di sorgente che li genera, come di seguito riportato :

Tabella 3: Classificazione Eventi

Sorgente Evento	Evento
Computer Security Software Alerts	HIDS, NIDS, IPS; Anti-Virus, Anti-Spyware, Anti-Spam software; File Integrity Checking Software.
Logs	Application / OS / Service log; Log dei dispositivi di rete.

Informazioni Comunità Internazionale	Nuove vulnerabilità / exploit; Informazioni incidenti avvenuti in altre Organizzazioni.
Personale	Segnalazioni da Dipendenti dell'Organizzazione; Segnalazione da Personale esterno all'Organizzazione.

2.3 Gestione e Prevenzione Incidenti

Vi sono comportamenti, attività e regole che si devono necessariamente mettere in atto per cercare di prevenire gli incidenti di sicurezza e di gestire e risolvere in maniera più efficiente quelli eventualmente avvenuti. Tali contromisure possono avere natura sia tecnologica che organizzativa.

CONTROMISURE DI NATURA TECNOLOGICA

- Risk Analysis: attività periodiche di analisi del rischio per avere sempre aggiornato il grado di criticità dei sistemi e delle informazioni presenti nell'Organizzazione e le relative contromisure adottate per proteggerle.
- Autenticazione: l'autenticazione deve essere effettuata o prima di ulteriori interazioni operative tra il sistema e l'utente;
- Controllo accesso logico: deve essere monitorato l'utilizzo delle risorse da parte dei processi e dell'utenza attraverso la verifica e la gestione dei diritti di accesso.
- Patch Management[1]: utilizzo di sistemi automatici per identificare, ottenere, testare ed effettuare il deploy di patches e aggiornamenti.
- Host / Network Security: configurazione sicura delle postazioni di lavoro e del perimetro dell'architettura di rete regionale. In particolare:
  - configurare opportunamente eventuali accessi mediante reti wireless (es.: non basarsi soltanto sull'utilizzo di chiavi WEP)[2];
  - configurare opportunamente eventuali accessi da remoto da parte di personale / collaboratori regionali (es.: mediante meccanismi di autenticazione multi-factor)[3];
  - tenere aggiornati (e monitorati) sistemi di IDS/IPS[4];
  - utilizzare dispositivi di rete (es.: firewall, router) per proteggere zone critiche presenti nella rete interna regionale.
- Prevenzione della diffusione del codice malevolo: protezione dei sistemi a livello host (sistema operativo workstation / server), a livello server-application (email server, proxy, ecc.) e a livello client-application (email clients, instant messaging client, ecc.).
- Log-Audit: definizione di una soglia minima di audit (al di sopra della quale i log vengono memorizzati) per tutti i sistemi, abbassandola per quelli che si ritiene siano più critici.
- Log-Monitoring[5]: attività periodiche di monitoraggio dei log per disporre di informazioni sempre aggiornate (entro una certa soglia di confidenza dettata dall'intervallo temporale di monitoring):

[1] NIST SP 800-40v2, Creating a Patch and Vulnerability Management Program: http://csrc.nist.gov/publications/PubsSPs.html.
[2] NIST SP 800-48v1, Guide to Securing Legacy IEEE 802.11 Wireless Networks: http://csrc.nist.gov/publications/PubsSPs.html. NIST SP 800-97, Establishing Wireless Robust Security Networks: http://csrc.nist.gov/publications/PubsSPs.html.
[3] NIST SP 800-114, User's Guide to Securing External Devices for Telework and Remote Access: http://csrc.nist.gov/publications/PubsSPs.html.
[4] NIST SP 800-94, Guide to Intrusion Detection and Prevention Systems (IDPS): http://csrc.nist.gov/publications/PubsSPs.html.
[5] NIST SP 800-92, Guide to Computer Security Log Management: http://csrc.nist.gov/publications/PubsSPs.html.

- sul corretto funzionamento dei sistemi più critici per l'Ente;
- sull' effettiva disponibilità delle sorgenti di eventi nel caso si verifichi un incidente.

- Centralizzazione log e policy "log-retention": utilizzo di meccanismi per la memorizzazione centralizzata, in modalità protetta dei log (es. supporti WORM, Write Once, Read Many), diminuendo l'impatto di un'eventuale compromissione (o danneggiamento) di un particolare sistema sui log del sistema stesso.

  Implementazione di una policy di "log-retention" che ne specifichi la durata di conservazione.

- Correlazione di informazioni provenienti dalle diverse sorgenti di eventi mediante meccanismi di "Event-Correlation".
- Sincronizzazione: utilizzo di protocolli di sincronizzazione (es.: Network Time Protocol (NTP[6])) per la consistenza temporale delle informazioni.
- Backup: salvataggio delle informazioni dei sistemi ritenuti critici, con una periodicità da stabilire in base al grado di criticità delle informazioni stesse e dalla loro frequenza di aggiornamento
- Verifica periodica delle copie di backup e delle procedure di ripristino.
- Strumenti: utilizzo di strumenti software che siano di supporto nelle fasi della gestione di un incidente (es. un sistema di ticketing, opportuni strumenti diagnostici).
- Vulnerability Assessment: attività periodiche di verifica di presenza di vulnerabilità all'interno dei sistemi e della rete[7].
- Deny by Default: adozione del principio di bloccare/disabilitare tutte le connessioni/servizi, abilitando poi di volta in volta solo quelli strettamente necessari[8].
- Regole e modalità tecniche per il riutilizzo dei supporti di memoria in condizioni di sicurezza: si tratta di strumenti volti alla cancellazione o la reinizializzazione di supporti riutilizzabili (usb, hard disk,ecc.) al fine di consentirne un nuovo utilizzo senza criticità relative alla sicurezza.
- Ridondanza delle risorse elaborative: è necessario adottare processi e meccanismi che garantiscano la ridondanza delle risorse al fine di un loro ripristino in tempi brevi in caso di indisponibilità dei supporti (es. mirroring dei dischi, salvataggi periodici).
- Protezione del trasferimento dati: sono modalità tecniche che assicurano ai canali di trasmissione la riservatezza, l'integrità e la disponibilità dei contenuti che si intende trasferire.
- Utilizzo di motori di ricerca, archivi Web-based e mailing list[9] disponibili on-line.

CONTROMISURE DI NATURA ORGANIZZATIVA

- Formazione Personale: attività periodiche di formazione e sensibilizzazione del personale al corretto utilizzo delle risorse e al rispetto delle policy e procedure in tema di privacy e sicurezza delle informazioni.
- Elaborazione delle policy: devono essere fornite agli utenti le policy necessarie per un corretto utilizzo del sistema informatico.

[6] http://www.ntp.org/
[7] NIST SP 800-42, Guideline on Network Security Testing: http://csrc.nist.gov/publications/nistpubs/index.html.
[8] NIST SP800-41rev1, Guidelines on Firewalls and Firewall Policy (Draft): http://csrc.nist.gov/publications/nistpubs/index.html
[9] Bugtraq: http://www.securityfocus.com/archive/1
Focus on IDS : http://www.securityfocus.com/archive/96
Forensics: http://www.securityfocus.com/archive/104
Incidents: http://www.securityfocus.com/archive/75
LogAnalysis: http://www.loganalysis.org/pipermail/loganalysis/

- Knowledge Base: creazione di un repository di documentazione che sia a supporto in caso di verifica di un incidente di sicurezza, e che comprenda, ad esempio:
    - link a Organizzazioni / Enti di monitoraggio codici malevoli;
    - link a liste contenenti domini inseriti in blacklist per spam;
    - guide all'analisi e significato dei log dei dispositivi di rete, sistemi operativi e applicazioni utilizzate.
- Documentazione: garanzia che tutta la documentazione a supporto sia sempre disponibile, eventualmente prevedendo più copie in formato elettronico e cartaceo (riferimenti, procedure, manualistica).
- Assistenza: può risultare necessario ed utile, in particolari situazioni, il ricorso a risorse esterne per assistenza in diverse fasi della gestione di un incidente.
- Aggiornamento: processo di aggiornamento il più possibile costante sulle tematiche in oggetto (es.: vulnerabilità[10], metodologie di attacco).

Tracciamento e conservazione

E' importante che durante tutte le fasi di gestione di un incidente, dalla presa in carico alla chiusura dell'incidente, ogni azione eseguita sia documentata e catalogata temporalmente.

Questo può essere di aiuto:

- qualora emergano delle conseguenze legali (per eventuale difesa o per adire a vie legali);
- per la risoluzione di eventuali incidenti simili che dovessero presentarsi successivamente.

Qualora, a seguito di un incidente relativo alla sicurezza delle informazioni, risulti necessario intraprendere un'azione legale (civile o penale) contro una persona fisica o giuridica, le evidenze oggettive devono essere raccolte e conservate al fine di conformarsi ai requisiti di legge applicabili nelle sedi giurisdizionali competenti. [11]

È in ogni caso necessario utilizzare un sistema elettronico di trouble-ticketing per tracciare tutte le attività e per conservare i dati anche in formato elettronico.

E' comunque necessario conservare tutte i dati e le informazioni utilizzate e raccolte durante le fasi di gestione di un incidente, limitandone in modo opportuno l'accesso logico e fisico al personale non autorizzato.

3 Fasi procedurali e responsabilità nella gestione degli incidenti

La procedura di gestione di un incidente di sicurezza può essere suddivisa nelle seguenti fasi:

1. Rilevazione;
2. Identificazione e analisi;
3. Contenimento, Raccolta evidenze, Rimozione e ripristino
4. Chiusura incidente

Sono attive due Unità di Gestione degli Incidenti di Sicurezza Informatica (di seguito denominata UGISI), una per la Giunta e una per l'Assemblea legislativa. Tali unità sono coordinate rispettivamente dal Responsabile della Sicurezza della Giunta e dal Responsabile della Sicurezza dell'Assemblea Legislativa, ognuno per la parte di propria competenza. Le due UGISI dovranno coordinarsi tra loro nel caso in cui accada un incidente che coinvolga l'area di competenza di entrambe.

[10] 'SANS Top 20 Security Risks list' identifica alcune tra le più diffuse vulnerabilità: http://www.sans.org/top20/
CIAC (Computer Incident Advisory Capability): http://www.ciac.org/ciac/
NVD (National Vulnerability Database): http://nvd.nist.gov/home.cfm

[11] ISO 27001 Annex A, A.13.2.3

Tali unità costituiscono il nucleo permanente di riferimento per la gestione degli incidenti, da integrare di volta in volta con i diversi soggetti che devono intervenire a seconda del singolo concreto incidente.

Le UGISI hanno le seguenti competenze:

- rappresentano il punto di riferimento a cui rivolgersi per segnalare un incidente di sicurezza;
- gestiscono tutte le attività inerenti un incidente di sicurezza, ivi comprese quelle relative alla sua documentazione e notifica;
- garantiscono la disponibilità e rintracciabilità di liste di contatti (es.: personale dipendente, collaboratori, fornitori, manutentori), necessarie per la gestione di un incidente di sicurezza;
- garantiscono che la gestione incidenti risponda alle esigenze dell'Ente, provvedendo che sia sempre mantenuta aggiornata:
    - a valle di cambiamenti tecnologici, infrastrutturali e organizzativi;
    - a valle di incidenti di sicurezza che mettano in evidenza aspetti di miglioramento nella procedura stessa.

I riferimenti (nominativi, e-mail, telefono, ecc) degli incaricati assegnati all'UGISI devono essere reperibili attraverso i portali di comunicazione interna affinché gli utenti possano facilmente e tempestivamente effettuare le segnalazioni di incidenti, anche potenziali.
Per facilitare la gestione degli incidenti di sicurezza è operativo un workflow che automatizza le varie fasi di seguito elencate, in particolare il flusso delle comunicazioni fra i vari attori. Tale workflow ha anche lo scopo di facilitare la produzione del report di incidente e di tenere aggiornate le statistiche sugli incidenti di sicurezza gestiti dalle UGISI della Giunta e dell'Assemblea Legislativa.
Una rappresentazione grafica delle fasi di cui si compone la procedura di gestione degli incidenti di sicurezza è contenuta all'allegato A.

4 Rilevazione dell'incidente

4.1 Generalità

La fase di rilevazione degli incidenti inizia nel momento in cui si verifica un incidente di sicurezza anche potenziale, prosegue informandone l'UGISI competente e finisce quando tale unità lo prende in carico.

La rilevazione di un incidente può avvenire al verificarsi di almeno uno degli eventi elencati nel paragrafo 2.

4.2 Descrizione

Di seguito si riporta lo schema della procedura di rilevazione di un incidente:

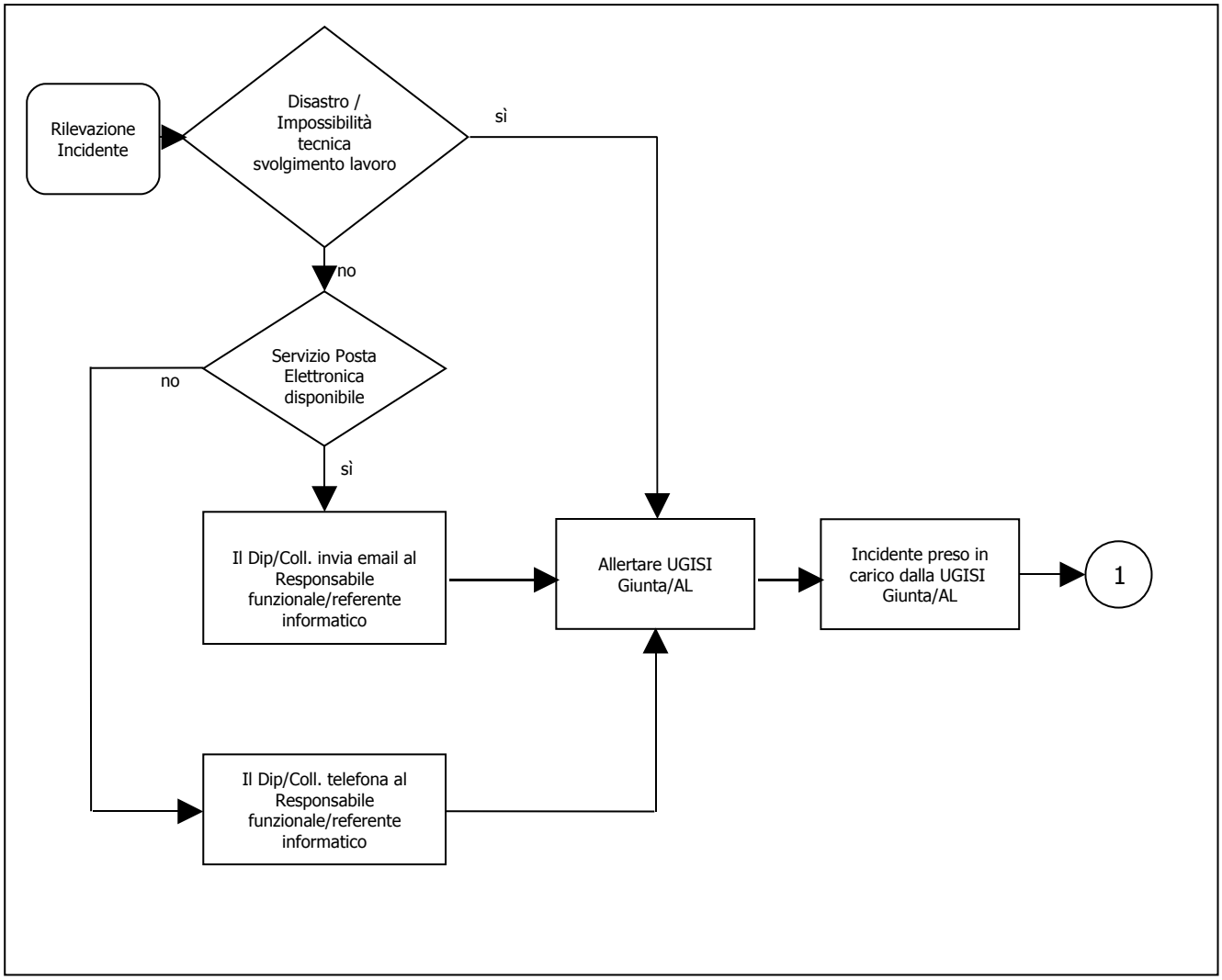


Figura 1: Rilevazione Incidente

In caso di rilevazione di incidente, il dipendente/collaboratore della Giunta o dell'Assemblea Legislativa invia una email al proprio responsabile funzionale[12] o, se questi non è presente, al proprio referente informatico; questi, quindi, a seconda che il dipendente/collaboratore appartenga alla Giunta o all'Assemblea Legislativa, provvederà ad inviare una email rispettivamente alla casella postale dell'UGISI della Giunta o dell'Assemblea Legislativa.

Se il servizio di posta elettronica non è disponibile, si procede in modo analogo, con l'unica differenza che il dipendente/collaboratore contatterà direttamente via telefono il proprio responsabile funzionale/ referente informatico.

[12] Con responsabile funzionale si intende in generale la persona direttamente responsabile del dipendente/collaboratore dell'Ente, a cui è possibile far riferimento per la segnalazione di eventuali problematiche o incidenti di sicurezza.

5 Identificazione e Analisi

5.1 Generalità

La fase di analisi dell'incidente ha inizio nel momento in cui l'UGISI lo prende in carico e prosegue fino a quando, una volta effettuata l'identificazione e l'analisi, è notificato (cfr. 5.2.6 Prima Notifica incidente) allegando la relativa documentazione.

5.2 Descrizione

Si riporta di seguito lo schema descrittivo, rimandando l'esposizione dettagliata ai paragrafi successivi:

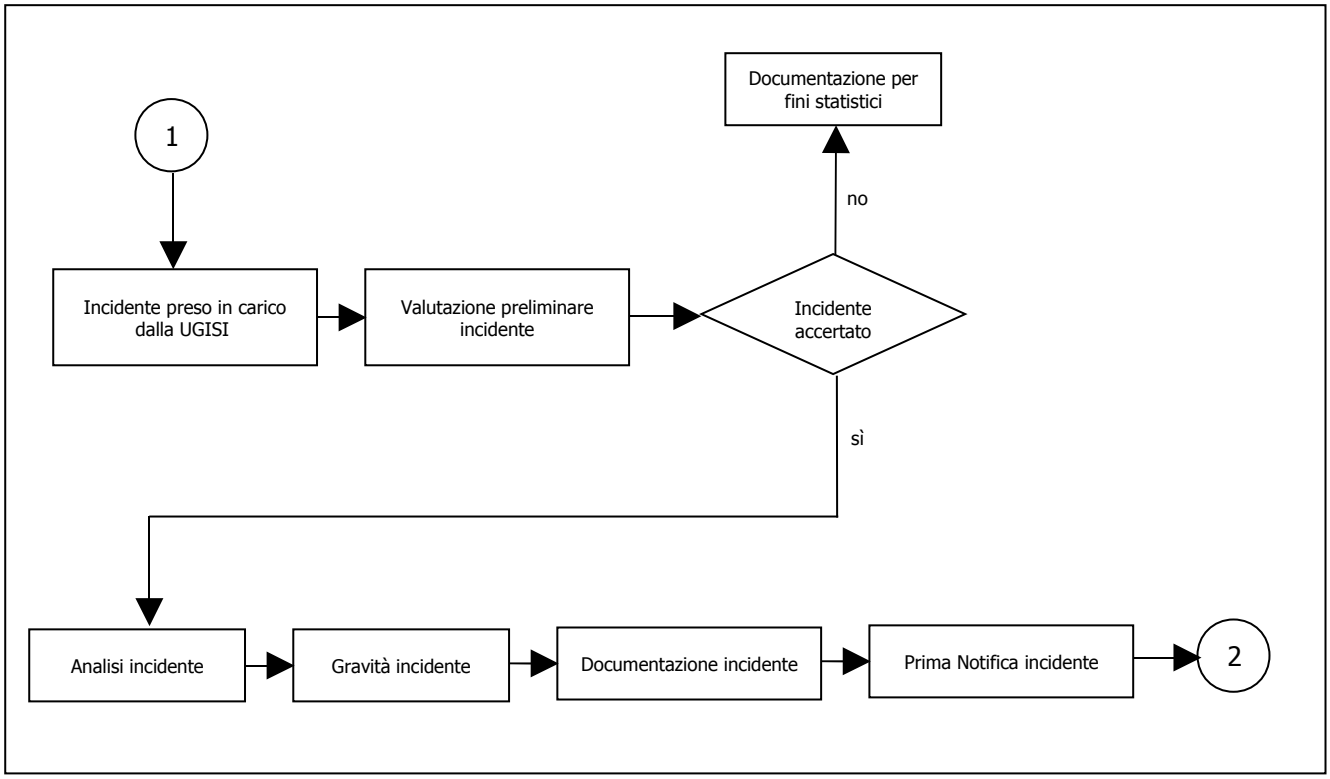


Figura 2: Identificazione e Analisi

5.2.1 Presa in carico incidente da parte dell'UGISI

A seguito della segnalazione del dipendente/collaboratore relativa ad un incidente di sicurezza anche potenziale, l'UGISI lo prende in carico.
L'UGISI deve poter reperire facilmente la seguente documentazione, che deve essere tempestivamente aggiornata:

- Riferimenti Lista Amministratori di sistema;
- Riferimenti Lista Responsabili Direzioni / Servizi RER;
- Riferimenti Lista Referenti Fornitori e Manutentori;
- Lista Sistemi ritenuti più critici.

Per facilitarne la reperibilità, la suddetta documentazione deve essere conservata, in formato cartaceo, in duplice copia di cui:

- una copia presso ciascuna UGISI;

- una copia presso la segreteria del Servizio Sistema Informativo - Informatico Regionale e del Servizio Sistemi Informativi – Informatici e Innovazione dell'Assemblea Legislativa.

5.2.2 Valutazione Preliminare

In questa fase l'UGISI effettua una valutazione preliminare dell'incidente, sulla base delle informazioni disponibili al momento.
Può essere opportuno farsi eventualmente coadiuvare dal dipendente/collaboratore che ha rilevato l'incidente,[13] e dal referente informatico di riferimento.

Lo scopo di questa fase è quello di comprendere se si tratta effettivamente di un incidente di sicurezza.

In caso positivo bisogna:

- catalogare l'incidente in una delle tipologie possibili al fine di procedere con le successive fasi di analisi.

In caso negativo bisogna:

- aggiornare il parametro "Numero complessivo di falsi positivi ricevuti" della Tabella 12: valutazione incidenti di sicurezza, descritta nel paragrafo 8 del presente Disciplinare.

5.2.3 Analisi

Durante questa fase occorre procedere con l' attività di analisi dell'incidente di sicurezza.

Nei prossimi paragrafi si descrivono, suddivisi per le singole tipologie di incidenti, gli eventi preventivi e indicativi che possono aiutare nell'analisi.

5.2.3.1 Accesso Non Autorizzato

L'incidente di sicurezza classificato come "Accesso Non Autorizzato" può essere associato a diverse tipologie di eventi.

Nella seguente tabella si elencano alcuni possibili eventi che possono precedere/scatenare un incidente e le corrispondenti azioni che occorre effettuare al fine di prevenire, se possibile, l'incidente di sicurezza:

Tabella 4: Eventi Preventivi "Accesso Non Autorizzato"

Eventi Preventivi	Azioni
• Attività di port scan, host scan, vulnerability scan, ping, traceroutes, DNS zone transfers, OS fingerprinting, banner grabbing.	• Analizzare se si verifica un cambiamento (a quella che può essere una normale attività di scanning), quale ad esempio un accanimento verso una particolare porta o un particolare host; se questo è legato a sfruttare una particolare vulnerability, provvedere ad eliminarla (patching, cambiamento regole firewall, disabilitazione servizi non utilizzati, ecc.).
• Un nuovo exploit che consente l'accesso non autorizzato, e che sfrutta una vulnerabilità (di un sowftare utilizzato dall'Ente) non ancora eliminata, è reso pubblico.	• Studiare l'exploit, e, dove possibile, adottare le opportune contromisure per limitarne un possibile impatto.
• Il personale regionale riporta tentativi di social engineering subiti.	• Emanare un bollettino (es.: email) che allerti il personale sui possibili rischi derivanti da attacchi di tipo social engineering. • Poiché l'attacco di tipo social engineering potrebbe essere soltanto una parte di una strategia di attacco più complessa, in base

[13] SANS Incident Identification Form : http://www.sans.org/score/incidentforms/IH_identification.pdf

	alle informazioni fornite dal personale sulla modalità di social engineering subito, cercare di capire le potenziali informazioni e risorse a cui il malintenzionato potrebbe essere interessato, al fine di analizzarne i relativi log.
• Il personale regionale riporta la presenza di tentativi (non riusciti) di accesso fisico a risorse / strutture da parte di personale non autorizzato.	• Informare il personale addetto alla vigilanza dell'episodio. • Verificare la criticità delle informazioni presenti nell'area dove si è verificato il tentativo di intrusione, ed eventualmente provvedere ad adottare opportune contromisure in termini di sicurezza fisica delle risorse presenti.

Nella tabella successiva si elencano alcuni possibili eventi indicativi (eventi "spia"), corrispondenti a possibili manifestazioni dell'incidente classificato come "Accesso Non Autorizzato".

Tabella 5: Eventi Indicativi Accesso Non Autorizzato

Eventi Indicativi	Manifestazione Accesso Non Autorizzato
• Esistenza di tool di sicurezza non autorizzati installati su un sistema. • Presenza di files e/o directory con nomi non usuali (contenenti caratteri binari, ecc.) all'interno del sistema. • Alert da parte di HIDS (es.: configurati da inviare segnalazione per ogni accesso root al sistema) installati sul sistema. • Utilizzo di Account utente non previsto, utilizzo contemporaneo su più sistemi di un unico account utente (previsto o non previsto), utilizzo di comandi non consoni alle funzionalità lavorative del personale a cui l'account è assegnato. • Modifica di file critici, librerie di sistema, file di configurazione presenti nel sistema. • Modifica della configurazione di sistema (policy di audit e di log, modalità scheda di rete, porte, servizi, ecc.) • Indisponibilità del sistema riportata dal personale.	• Accesso root non autorizzato ad un sistema.
• Utilizzo di Account utente non previsto, utilizzo contemporaneo su più sistemi di un unico account utente (previsto o non previsto), utilizzo di comandi non consoni alle funzionalità lavorative del personale a cui l'account è assegnato. • Tentativi di accesso a file contenenti informazioni critiche (es.: password-files) presenti nel sistema. • Web-Proxy logs che evidenziano tentativi di download, all'interno della rete RER. di tool di sicurezza non autorizzati.	• Accesso non-root (mediante utenza) non autorizzato ad un sistema.
• Tentativi di accesso a file contenenti informazioni critiche (es.: password-files) presenti nel sistema. • Alert da parte di HIDS (es.: configurati da inviare segnalazione per ogni accesso a dati e informazioni attraverso determinati protocolli (FTP; HTTP, ecc.)) installati sul sistema.	• Accesso non autorizzato a dati e informazioni (es.: password-file, databases, ecc.)*
• Rimozione dell' hardware (o di parte di esso) di un sistema.	• Accesso fisico

• Presenza di nuovo hardware non autorizzato (es.: modem, packet sniffing, ecc.). • Shutdown e Startup improvvisi di un sistema. • Indisponibilità di un sistema riferita dal personale.	

* In questa manifestazione di Accesso Non Autorizzato, il malintenzionato non ottiene accesso (root o con utenza non-root) ad un sistema, come nei primi due casi, bensì accede direttamente ad informazioni (es.: password-file, databases) da remoto attraverso protocolli FTP, HTTP, ecc.

Prevenzione

I seguenti accorgimenti possono in generale aiutare a prevenire incidenti di sicurezza classificati come "Accesso Non Autorizzato":

- configurare opportunamente tutte le modalità di accesso remoto alla rete interna, sia che queste vengano utilizzate da dipendenti/collaboratori, che da eventuali fornitori esterni;
- adottare soluzioni DMZ dove far risiedere tutti i sistemi contenenti i servizi che richiedano accesso diretto da Internet;
- utilizzare soltanto indirizzi IP privati per i sistemi della rete interna regionale;
- limitare i servizi erogati dai sistemi con accesso diretto da Internet ai soli strettamente necessari e ridondare quelli che si ritiene particolarmente critici;
- eseguire i servizi con privilegi più bassi possibili compatibilmente con le esigenze e caratteristiche del servizio stesso;
- utilizzare la funzionalità di screen saver automatico con password per tutti i sistemi;
- monitorare periodicamente i permessi di accesso alle risorse che si ritiene siano più critiche;
- monitorare periodicamente gli account utente, eliminando quelli che non sono più utilizzati;
- adottare una opportuna politica di scelta password;
- adottare opportune misure di controllo per l'accesso fisico alle risorse che si ritiene siano più critiche.

Considerazioni

L'Accesso Non Autorizzato è una metodologia di attacco che, a differenza degli altri, è caratterizzato da numerosi step necessari per essere portato a compimento.

Tipicamente ad una fase di "reconnaisance" iniziale (tramite attività di port/host/vulnerability scan, ping, traceroutes, ecc.), ne segue, da parte del malintenzionato, una successiva in cui si cerca di ottenere accesso ad uno o più sistemi, cercando di sfruttare, se presenti, vulnerabilità che ne consentano un accesso di tipo root e ripiegando eventualmente su quelle che consentono accesso con utenza di tipo non-root.

Si tratta pertanto di diversi step che possono richiedere un certo intervallo di tempo per essere eseguiti; è importante, quindi, rilevare e gestire l'incidente prima che giunga allo step finale (eventuale accesso di tipo root).

Durante un incidente di tipo "Accesso Non Autorizzato", può risultare difficile distinguere l'effettiva presenza dell'incidente da un'eventuale operazione di aggiornamento del sistema, che può determinare alcuni tra gli eventi indicativi sopra evidenziati (modifica di file critici, librerie di sistema, file di configurazione presenti nel sistema, modifica della configurazione di sistema (policy di audit e di log, modalità scheda di rete, porte, servizi, ecc.). A tal riguardo può essere utile definire e schedulare le attività di aggiornamento (upgrade sistema operativo, modifica hardware, ecc.).

5.2.3.2 Denial of Service[14]

L'incidente di sicurezza classificato come "Denial of Service (DoS)" è associato a diverse tipologie di eventi.

Nella seguente tabella si elencano alcuni possibili eventi che possono precedere/scatenare l'incidente e le corrispondenti azioni che occorre effettuare al fine di cercare di prevenire l'incidente di sicurezza:

Tabella 6: Eventi Preventivi Denial of Service

Eventi Preventivi	Azioni
• Un' attività di port scan, host scan, vulnerability scan, spesso precede un tentativo di DoS, per capire quale, fra le sue modalità, può essere maggiormente efficace.	• Monitorare l'evento preventivo, e in caso contattare il proprio ISP.
• Rilascio di nuove versioni di tool DoS.	• Analizzare, se possibile, il tool per valutare, a valle delle contromisure già presenti, il suo impatto su eventuali sistemi regionali maggiormente esposti.

Nella seguente tabella si elencano alcuni possibili eventi "spia" e corrispondenti possibili manifestazioni dell'incidente Denial of Service.

Tabella 7: Eventi Indicativi Denial of Service

Eventi Indicativi	Manifestazione Denial of Service
• Indisponibilità dell'applicazione riportata dal personale. • NIDS / HIDS alert. • Presenza di pacchetti IP con indirizzo sorgente non appartenente a domini conosciuti. • Presenza di log dell'applicazione non conformi ad un suo corretto funzionamento.	• DoS verso un'applicazione di un particolare host.
• Indisponibilità del sistema operativo e delle applicazioni presenti riportata dal personale. • NIDS / HIDS alert. • Presenza di pacchetti IP con indirizzo sorgente non appartenente a domini conosciuti. • Presenza di log a livello di sistema operativo non conformi ad un suo corretto funzionamento.	• DoS verso il sistema operativo di un particolare host.
• Traffico di rete fortemente sbilanciato (molto traffico in ingresso, poco in uscita alla rete). • Forte aumento utilizzo banda di rete. • Indisponibilità rete con perdita saltuaria della connettività • NIDS / HIDS alert. • Presenza di pacchetti IP con indirizzo sorgente non appartenente a domini conosciuti. • Presenza di log a livello di firewall e di dispositivi di rete non conformi ad un loro corretto funzionamento.	• Network-based DoS verso una rete.

[14] Distributed Denial of Service (DDoS) Attacks/tools: http://staff.washington.edu/dittrich/misc/ddos/
A Taxonomy of DDoS Attacks and DDoS Defense Mechanisms: http://lasr.cs.ucla.edu/ddos/ucla_tech_report_020018.pdf

Prevenzione

I seguenti accorgimenti possono in generale aiutare a prevenire incidenti di sicurezza DoS:

- implementare politiche di limitazione di banda per determinati protocolli (es.: ICMP), sia a livello di dispositivi di rete (es.: firewall, border-router) che a livello di ISP;
- in generale, la limitazione può essere applicata ai servizi che si ritiene siano maggiormente esposti;
- limitare i servizi erogati dai sistemi con accesso diretto da Internet soltanto a quelli strettamente necessari;
- ridondare i dispositivi di rete e i sistemi che si ritiene siano maggiormente critici;
- accertarsi che i dispositivi di rete ed i sistemi che si ritiene siano maggiormente critici non lavorino, in termini di risorse utilizzate, in prossimità della massima capacità;
- per ridurre la probabilità di IP spoofing, implementare le seguenti regole sia sui dispositivi di rete sia su quelli di filtraggio (firewall, border-router, ecc.) alla rete RER[15]:
    - pacchetti in ingresso alla rete regionale non devono avere un indirizzo IP sorgente appartenente al range di indirizzi assegnato a sistemi interni alla rete stessa;
    - pacchetti in ingresso alla rete regionale devono avere un indirizzo IP destinazione appartenente al range di indirizzi assegnato a sistemi interni alla rete stessa;
    - pacchetti in uscita dalla rete regionale devono avere un indirizzo IP sorgente appartenente al range di indirizzi assegnato a sistemi interni alla rete stessa;
    - pacchetti in uscita dalla rete regionale non devono avere un indirizzo IP destinazione appartenente al range di indirizzi assegnato a sistemi interni alla rete stessa;
    - pacchetti in ingresso o in uscita dalla rete regionale non devono avere un indirizzo IP sorgente o destinazione che appartenga alla lista “reserved space” riportata nella RFC1918;
- configurare i dispositivi di rete (firewall, border-router) in modo che prevengano DoS “reflector attack”[16].
- definire e attuare le politiche di limitazione all’utilizzo di software peer-to-peer e instant messaging, implementando nei dispositivi di rete (firewall, border-router) le opportune restrizioni.

Considerazioni

Spesso gli incidenti di tipo “Denial of Service” vengono causati utilizzando indirizzi IP di sistemi diversi da quelli utilizzati dal malintenzionato (IP spoofing), rendendo così complicato risalire all’origine dell’attacco. A tal riguardo può risultare utile l’eventuale presenza di informazioni (log, HIDS/IDS alert, ecc.) raccolte durante la preliminare fase di port / host / vulnerability scan, durante la quale è presumibile che il malintenzionato abbia utilizzato un indirizzo IP non modificato.

Una variante dell’incidente DoS, è il Distribuited DoS (DDoS), in cui il malintenzionato installa del software su sistemi “zombie”, i quali, ignari di tutto, vengono controllati da remoto per effettuare l’attacco al verificarsi di un comando.
Anche in questo caso risulta difficile risalire alla corretta identità del sistema sorgente.

[15] Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing: http://www.ietf.org/rfc/rfc2267.txt
[16] www.infosecwriters.com/text_resources/pdf/Cisco-DoS-DDoS.pdf

Una ulteriore variante dell'incidente DoS è quella in cui, sfruttando delle vulnerabilità, è possibile far riavviare un Web Server inviandogli pacchetti malformati; da notare come in questo caso, almeno in prima analisi, è possibile che il restart venga attribuito ad una instabilità del sistema operativo del sistema che ospita il Web Server, e non ad un avvenuto incidente DoS.

5.2.3.3 Codice Malevolo[17]

L'incidente di sicurezza classificabile come "Codice Malevolo" è associato a diverse tipologie di eventi.

Nella seguente tabella si elencano alcuni possibili eventi che precedono/scatenano l'incidente e le corrispondenti azioni che occorre effettuare al fine di cercare di prevenire l'incidente di sicurezza:

Tabella 8: Eventi Preventivi Codice Malevolo

Eventi Preventivi	Azioni
• Presenza di un nuovo codice malevolo che potrebbe avere come target del software utilizzato dall'Ente.	• Verificare, tramite i siti dei principali vendor di software antivirus, che il codice malevolo sia effettivamente presente (e non sia un cosiddetto hoax). In caso positivo, verificare che le signature del software antivirus siano aggiornate e contengano quella relativa al codice malevolo. Qualora la signature non sia ancora disponibile, diramare un bollettino (es. email) che allerti il personale sui possibili rischi derivanti dal nuovo codice malevolo.
• Un codice malevolo è stato correttamente intercettato (disinfettando o mettendo in quarantena il file infetto) dal software antimalware.	• Verificare, se possibile, a che livello di penetrazione sia giunto il codice malevolo (se sia stato intercettato dal software a livello rete, o da quello dei singoli sistemi interni alla rete) ed il numero di sistemi colpiti. Determinare la eventuale vulnerabilità che il codice malevolo avrebbe cercato di sfruttare. Se presente, provvedere ad eliminarla (patching, cambiamento regole firewall, disabilitando servizi non utilizzati, ecc.).

Nella seguente tabella si elencano alcuni possibili eventi "spia" e corrispondenti possibili manifestazioni dell'incidente Codice Malevolo:

Tabella 9: Eventi Indicativi Codice Malevolo

Eventi Indicativi	Manifestazione Codice Malevolo
• Antivirus software alert. • IPS alert. • Aumento del numero di email inviate/ricevute dal sistema. • File modificati/cancellati dal sistema. • Instabilità del sistema. • Lentezza del sistema nell'apertura di programmi e nella loro esecuzione. • Presenza di modifica dei template di Word, Excel, ecc. • Qualora il virus ottenga un accesso root al sistema, vedere gli eventi indicativi relativi alla manifestazione Accesso Non Autorizzato "Accesso root non autorizzato ad un sistema".	• Un virus che si propaga tramite il servizio di posta elettronica infetta un sistema.
• Antivirus software alert.	• Un worm che si propaga sfruttando la

[17] NIST SP 800-83, Guide to Malware and Incident Prevention and Handling: http://csrc.nist.gov/publications/PubsSPs.html
Vendor Website (Sophia): http://www.sophos.com/security/
Vendor Website (Symantec): http://www.symantec.com/business/security_response/threatexplorer/threats.jsp
Vendor Website (Trend Micro): http://www.trendmicro.com/vinfo/virusencyclo

• IPS alert • Instabilità del sistema. • Lentezza del sistema nell'apertura di programmi e nella loro esecuzione. • Incremento del traffico di rete. • Tentativi di accesso al servizio che presenta la vulnerabilità. • Qualora il worm ottenga un accesso root al sistema, vedere gli eventi indicativi relativi alla manifestazione Accesso Non Autorizzato "Accesso root non autorizzato ad un sistema".	vulnerabilità di un servizio infetta un sistema.
• Antivirus software alert. • IPS alert relativi alla presenza di comunicazioni client-server legati alla presenza di Trojan Horse. • Log dei dispositivi di rete (Firewall, router) relativi alla presenza di comunicazioni client-server legati alla presenza di Trojan Horse. • Presenza di connessioni di rete tra il sistema e sconosciuti host remoti. • Presenza di processi sconosciuti all'interno del sistema. • Presenza di porte aperte sconosciute all'interno del sistema. • Instabilità del sistema. • Lentezza del sistema nell'apertura di programmi e nella loro esecuzione. • Qualora il Trojan Horse ottenga un accesso root al sistema, vedere gli eventi indicativi relativi alla manifestazione Accesso Non Autorizzato "Accesso root non autorizzato ad un sistema".	• Un Trojan Horse è presente in un sistema.
• Vedere gli eventi indicativi relativi al particolare codice malevolo (virus, worm, trojan horse). • Presenza di dialog-box richiedenti l'autorizzazione ad effettuare determinate operazioni (scaricare software, collegarsi un sito Web, ecc.).	• Un codice malevolo presente in un sito Web, viene utilizzato per infettare un sistema.
• L'origine del messaggio non appartiene a noti computer security group (né sono presenti link a questi). • I toni presenti nel messaggio sono orientati a creare un senso di paura e panico. • Il messaggio esorta ad eliminare files e ad inoltrarlo ad altri utenti.	• Un dipendente / collaboratore segnala di aver ricevuto un hoax.

Prevenzione

I seguenti accorgimenti possono in generale aiutare a prevenire incidenti di sicurezza Codice Malevolo:

- Mantenere aggiornati i software antivirus, ed effettuare attività periodiche di scan dei sistemi.

  I software antivirus dovrebbero essere configurati in modo che, se non è possibile disinfettare un file infettato, questi venga messo in quarantena e non eliminato. Questo può aiutare durante la fase di analisi dell' incidente.

I software antivirus dovrebbero essere inoltre configurati in modo da far partire automaticamente lo scan degli allegati delle email prima che vengano aperti.

- Aggiornare i dipendenti / collaboratori sulle principali metodologie di propagazione dei codici malevoli, incluse le modalità di phishing[18].
- Al fine di prevenire la presenza di Spyware, configurare i Web Browser in modo da non consentire l'installazione di software sui sistemi da parte di siti web visitati.

  Utilizzare inoltre software antivirus che abbiano la funzionalità di rilevare anche la presenza di spyware.
- Configurare il servizio di posta elettronica in modo che sia il sistema server (email server) sia i client blocchino file con determinate estensioni (es.: .pif, .vbs, .txt.vbs, .htm.exe, ecc.).

  Nei casi in cui risulti effettivamente necessario inviare file di questo tipo, è possibile rinominarli, specificando nel testo della email la procedura per aprirli.
- Configurare inoltre i sistemi client di posta elettronica a non aprire (o eseguire) automaticamente gli allegati.
- Disabilitare la funzionalità di open SMTP Relay[19] (SMTP Relay senza autenticazione) nel sistema server di posta elettronica[20].
- Utilizzare software anti-spam, a livello di sistemi server e/o client di posta elettronica, o come appliance di rete.
- Attuare, se presenti, le politiche di limitazione all'utilizzo di software peer-to-peer e instant messaging, implementando nei dispositivi di rete (firewall, border-router) le opportune restrizioni.
- Effettuare attività periodiche di scan dei sistemi all'interno della rete, per verificare la eventuale presenza di cartelle condivise che presentino inadeguati livelli di accesso.
- Utilizzare HIDS e strumenti software di File Integrity Checkers[21] nei sistemi che si ritiene siano più critici.

Considerazioni

Gli eventi indicativi sopra illustrati possono essere determinati anche da cause diverse da quelle imputabili ad un incidente di tipo "Codice Malevolo"; per esempio, l'instabilità del sistema può essere dovuta a problemi legati al sistema operativo.

E' importante quindi una valutazione oculata da parte di personale che abbia ricevuto un opportuno training nella disamina di incidenti di questo tipo.

Nello stabilire la priorità di un incidente di tipo "Codice Malevolo", occorre prendere in considerazione i seguenti aspetti:

- tipologia di codice malevolo (virus, worm, trojan horse);
- sistemi infettati;
- modalità di trasmissione (virus tramite posta elettronica, trojan horse tramite ftp, ecc.);
- tipologia di tool, se presenti, installati dal codice malevolo nei sistemi infettati;
- modalità di propagazione temporale (es.: sistemi infettati per ora) qualora non ci sia attività di contenimento dell'incidente.

[18] Anti-Phishing Working Group: http://www.antiphishing.org/
"Phishing" Scam, Federal Trade Commission (FTC): http://www.ftc.gov/bcp/edu/pubs/consumer/alerts/alt127.shtm.
[19] http://www.mail-abuse.com/an_sec3rdparty.html
[20] NIST SP 800-45v2 Guidelines on Electronic Mail Security: http://csrc.nist.gov/publications/PubsSPs.html.
[21] http://sourceforge.net/projects/afick

5.2.3.4 Malfunzionamento

Al verificarsi del danneggiamento di un componente di un sistema, occorre fare riferimento a:

- lista dei contatti relativa ai referenti interni e/o fornitori per quanto riguarda i sistemi e apparati di produzione:
- struttura di help-desk nel caso di postazione di lavoro individuale.

Al verificarsi del danneggiamento di una struttura ospitante i sistemi (es.: rottura impianto di condizionamento / tubazione, incendio) occorre fare riferimento al responsabile della gestione della sala macchine e, in sua assenza, alla portineria dello stabile, dove è depositata la lista di contatti relativa al personale manutentore.

Prevenzione

I seguenti accorgimenti possono in generale aiutare a prevenire incidenti di sicurezza classificati come "Malfunzionamento":

- effettuare attività periodiche di maintenance sia software sia hardware dei sistemi, in particolar modo per quelli che si ritiene siano maggiormente critici, e delle strutture presso cui sono ubicati;
- prevedere, qualora possibile, per le risorse che si ritiene siano più critiche, dei sistemi di test su cui verificare il nuovo software e hardware installato.

Considerazioni

In caso di incidenti di particolare gravità (es.: allagamento dovuto a rottura di una tubazione ubicata sopra la sala server, incendio legato ad un corto circuito che coinvolge uno o più sistemi), può risultare necessario attivare un piano di Business Continuity o Disaster Recovery[22], che preveda l'attivazione di un sito alternativo in modo da garantire la continuità delle funzioni aziendali.

5.2.3.5 Uso Inappropriato

L'incidente di sicurezza classificato come "Uso Inappropriato" è associato a diverse tipologie di eventi, che, a differenza delle tipologie di incidenti individuate nei paragrafi precedenti, non sono di solito di tipo preventivo.

Nella seguente tabella si elencano alcuni possibili eventi indicativi e corrispondenti a possibili manifestazioni dell'incidente "Uso Inappropriato":

Tabella 10: Eventi Indicativi Uso Inappropriato

Eventi Indicativi	Manifestazione Uso Inappropriato
• segnalazioni da parte di soggetti terzi; • a seguito di quanto rilevato durante una verifica di sicurezza effettuata a causa di un'altra tipologia di incidente di sicurezza (secondo quanto specificato nel paragrafo 6 del DT verifiche e controlli) • Presenza di log (Web Proxy, FTP / Email server, ecc.) • Incremento utilizzo risorse di rete (banda, storage, ecc.) • Presenza di nuovi software installati sui sistemi. • Traffico anomalo da/verso determinati	• Uso inappropriato di servizi (es.: file/music sharing).

[22] http://www.cnipa.gov.it/site/_files/cnipa_quad_35_int.pdf

sistemi • Presenza di files e/o directory con nomi non usuali (contenenti caratteri binari, ecc.) all'interno del sistema.	
• IPS alert. • segnalazioni da parte di soggetti terzi • a seguito di quanto rilevato durante una verifica di sicurezza effettuata a causa di un'altra tipologia di incidente di sicurezza (secondo quanto specificato nel paragrafo 6 del DT verifiche e controlli) • Presenza di log (Web Proxy, FTP / Email server, ecc.) • Presenza di file inappropriati sui sistemi.	• Accesso a siti inappropriati (es. giochi di azzardo, violenza, ecc). • Invio spam.
• IPS alert. • Segnalazioni da parte di Enti/Agenzie/Organizzazioni esterne alla rete regionale.	• Attacco verso l'esterno condotto dall'interno della rete regionale

In caso di incidente di sicurezza di tipo "Uso inappropriato", l'amministratore di sistema deve attenersi a quanto definito nel Disciplinare tecnico in materia di verifiche di sicurezza e controllo sull'utilizzo delle strumentazioni.

Prevenzione

I seguenti accorgimenti possono in generale aiutare a prevenire incidenti di sicurezza di tipo "Uso Inappropriato":

- effettuare attività periodiche di formazione del personale, sensibilizzandolo sulle tematiche di privacy e sicurezza delle informazioni;
- condividere con tutto il personale le policy e le procedure di comportamento, rendendole accessibili e di facile fruizione;
- informare il personale sulle possibili conseguenze che un comportamento inappropriato, sia esso voluto che accidentale, potrebbe avere sia sulla RER e sia su chi ha determinato l'incidente.

5.2.3.6 Disastro

Per definizione un incidente classificato come "Disastro" è dovuto a cause di forza maggiore, per cui non è in generale possibile effettuare un'analisi sia a livello di eventi indicativi che preventivi.

Considerazioni

In caso di incidenti di particolare gravità (es.: allagamento dovuto a rottura di una tubazione ubicata sopra la sala server, incendio legato ad un corto circuito che coinvolge uno o più sistemi), è necessario attenersi a quanto previsto dai piani di Continuità Operativa e di Disaster Recovery dell'Ente che saranno predisposti.

5.2.3.7 Multiplo

L'incidente di sicurezza classificato come "Multiplo" risulta di più difficile analisi a causa dei seguenti motivi:

- è facile che accada di rilevare una sola tipologia di incidente, senza rendersi conto che si tratta solo di un anello di una catena di incidenti;

- può accadere di rilevare diverse tipologie di incidenti, ma non di rilevare che si tratta in realtà di un unico solo più strutturato;
- le differenti fasi di un incidente multiplo possono avvenire nel corso di un intervallo di tempo che può essere anche relativamente lungo (es.: settimane, mesi).

  Quindi è probabile che non siano più presenti evidenze relativamente alle prime fasi.

Da quanto sopra emerge quanto sia importante, per la rilevazione di incidenti di sicurezza Multiplo, la presenza di un adeguato sistema di logging, log-retention ed event-correlation.

5.2.4 Gravità Incidente

In questa fase viene stabilita la gravità dell'incidente di sicurezza sulla base della seguente matrice:

Tabella 11: Gravità incidenti

Gravità incidente di sicurezza	Descrizione
Alta	Il grado di compromissione di servizi e/o sistemi è elevato. Si rilevano danni consistenti sugli asset. Il ripristino è di medio o lungo periodo. L'incidente presenta una tra le seguenti condizioni: • danni a persone e rilevanti perdite di produttività • rischio di azioni legali • estesa infezione virale in grado di compromettere molteplici sistemi e di propagarsi nella rete • compromissione di sistemi o di reti in grado di permettere accessi incontrollati a informazioni confidenziali • siti web violati o utilizzati a fini di propagazione di materiale terroristico o pornografico • frode o attività criminale che coinvolga servizi forniti dall'Ente • impossibilità tecnica di fornire uno o più servizi critici a un elevato numero di utenti per un intervallo di tempo superiore ai 30 minuti nell'arco di una giornata • impossibilità tecnica di fornire uno o più servizi critici ad un elevato numero di utenti per intervalli di tempo inferiori ai 30 minuti di tempo ripetuti su più giornate • impossibilità tecnica di fornire uno o più servizi critici ad una piccola parte di utenti per un periodo di tempo superiore ai 30 minuti di tempo nell'arco di una o più giornate • impossibilità tecnica di fornire uno o più servizi di criticità media per un periodo di tempo superiore ai 2 giorni lavorativi • perdita di immagine e/o reputazione nei confronti degli utenti
Media	L'incidente non presenta nessuna condizione che porti alla catalogazione "gravità alta". Il grado di compromissione di servizi e/o sistemi è di una certa rilevanza e possono essere rilevati danni sugli asset di una certa consistenza. Il ripristino ha tempi che non compromettono la continuità del servizio

	L'incidente presenta una tra le seguenti condizioni: • compromissione di server • degrado di prestazioni relativo ai servizi offerti dall'Ente con conseguente perdita di produttività da parte degli utilizzatori • attacchi che provocano il funzionamento parziale o intermittente della rete • impossibilità tecnica di fornire uno o più servizi critici in casi che non rientrano nella gravità alta • basso impatto in termini di perdita di business • basso impatto in termini di perdita di immagine e/o reputazione nei confronti degli utenti
Bassa	L'incidente non presenta nessuna condizione che porti alla catalogazione "gravità alta o media". Non vengono compromessi asset o servizi. L'incidente presenta le seguenti condizioni: • Interruzione dell'attività lavorativa di un numero ristretto di dipendenti. • contaminazioni multiple da virus in un medesimo sito • molteplici sospetti di intrusione da parte di uno stesso attaccante

Per alcune manifestazioni di tipologie di incidenti può risultare necessario assegnare una gravità prima che l'analisi sia completa; in tal caso occorre valutarla sulla base dei riscontri e dell'analisi effettuata fino a quel momento, assumendo che la gravità aumenterà nel caso non si effettui alcuna operazione di contenimento. In ogni caso, è opportuno verificare ciclicamente, nel periodo in cui l'incidente è in corso, la gravità assegnata allo stesso in quanto essa può variare nel tempo.

Nel caso in cui l'incidente di sicurezza fosse di tipologia Malfunzionamento, la procedura di gestione descritta nel presente disciplinare si applicherà solo se la gravità, secondo i criteri contenuti nella Tabella 11, è Alta.
Diversamente l'incidente non verrà catalogato come incidente di sicurezza e verrà gestito con le procedure previste per gli incidenti informatici.

La definizione di "servizi critici" contenuta nella medesima Tabella 11 gravità Alta è esplicitata nel Piano di Continuità Operativa e di Disaster Recovery dell'Ente.

Al termine della fase di analisi, è necessario informare tempestivamente il Responsabile della Sicurezza competente.

5.2.5 Documentazione Incidente

Il "Rapporto di incidente di Sicurezza", da utilizzare è quello previsto in uno specifico Allegato del Disciplinare Tecnico in materia di verifiche di sicurezza e controlli sull'utilizzo delle strumentazioni dell'Amministrazione, e rappresenta il form da utilizzare ai fini della documentazione di un incidente di sicurezza.

5.2.6 Prima Notifica Incidente

L'UGISI, coinvolta tramite la segnalazione del responsabile funzionale o del referente informatico, dopo aver effettuato una prima valutazione ed analisi dell'incidente, deve inviare una prima notifica contenente le informazioni emerse nella fase di analisi alla casella di posta elettronica dell'UGISI stessa, in modo da informarne tutti i componenti compreso il coordinatore, vale a dire il Responsabile della sicurezza corrispondente.

La prima notifica può essere segnalata attenendosi al modello del Rapporto incidente di sicurezza (Allegato del Disciplinare Tecnico in materia di verifiche di sicurezza e controlli sull'utilizzo delle strumentazioni dell'Amministrazione) compilando soltanto le parti che in questa fase è possibile conoscere. Lo scopo principale di questa prima notifica è di informare il Responsabile della sicurezza coinvolto della presenza di un incidente.

Il Rapporto incidente di sicurezza sarà poi completato in tutte le sue parti in fase di chiusura dell'incidente.

Infine il Responsabile della Sicurezza coinvolto deve conservare per la durata di cinque anni il Rapporto, in formato elettronico, in una cartella soggetta a backup periodico e ad accesso opportunamente limitato.

6 Contenimento, Raccolta evidenze, Rimozione e Ripristino

6.1 Generalità

In questa fase si provvede, per quanto possibile, a:

- contenere gli effetti dannosi provocati dall'incidente di sicurezza, evitando che questi si propaghi coinvolgendo altri ambiti dell'Ente;
- raccogliere le "evidenze" dell'incidente, al fine di allegarle alla documentazione dell'incidente;
- rimuovere la causa del danno;
- riattivare, mediante procedure di ripristino, i sistemi coinvolti nell'incidente, permettendo agli utenti di tornare ad operare.

6.2 Descrizione

Si riporta di seguito lo schema descrittivo, rimandando l'esposizione dettagliata ai paragrafi successivi:

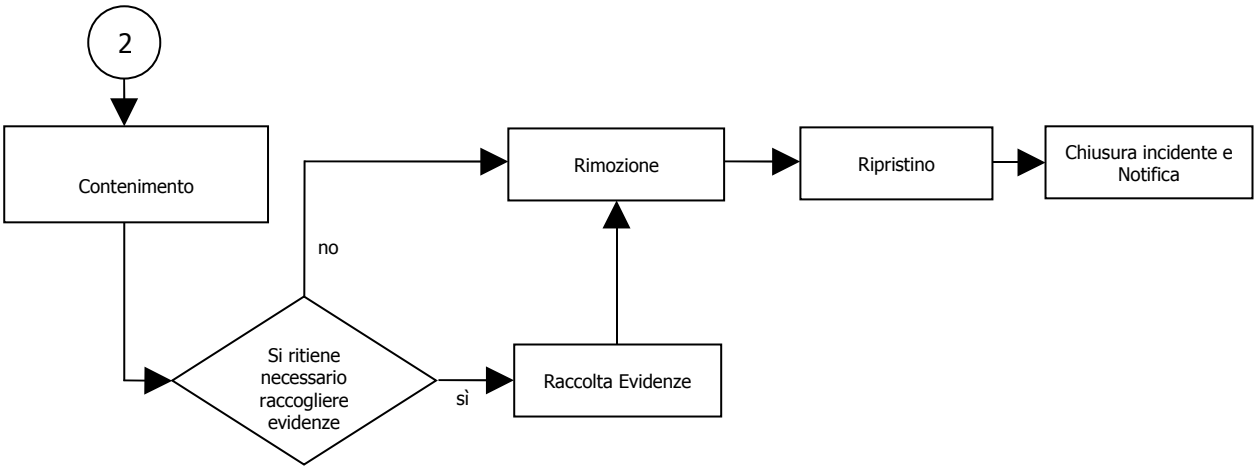


Figura 3: Contenimento, Raccolta evidenze, Rimozione, Ripristino e Chiusura

6.2.1 Contenimento

In generale, i seguenti aspetti possono essere considerati nella scelta della strategia più opportuna da adottare per il contenimento di un incidente di sicurezza:

- tempo e risorse necessarie per implementarla;
- efficacia (contenimento parziale o totale dell'incidente di sicurezza);
- durata (contenimento limitato ad un intervallo di tempo -4 ore, 2 giorni, o altro - o permanente dell'incidente di sicurezza);
- potenziale pericolo di furto di risorse;
- necessità di conservare le evidenze che verranno raccolte nella fase successiva;

- necessità di mantenere determinati servizi (es.: connettività di rete, servizi forniti a Enti, client).

Durante la fase di contenimento, qualora emergano le seguenti necessità:

- allocare delle risorse economiche per la fase di Analisi e/o le e successive fasi di gestione;
- isolare e/o poi arrestare eventuali servizi o sistemi critici di produzione coinvolti;
- valutare eventuali conseguenze legali;
- relazionarsi con altri Servizi/Direzioni dell'Ente;

occorre contattare il Responsabile della Sicurezza coinvolto per le eventuali azioni da intraprendere.

6.2.1.1 Accesso Non Autorizzato

La strategia di contenimento per l'incidente di sicurezza classificato come "Accesso Non Autorizzato" richiede tempi di reazione abbastanza rapidi.

Dovrebbe essere eseguita un appropriata combinazione delle seguenti azioni:

- Isolare (disconnettendoli dalla rete) i sistemi vittima dell'incidente: questa soluzione, che dovrebbe essere adottata dopo aver determinato l'impossibilità di utilizzarne altre, va presa valutando le possibili conseguenze che l'isolamento dei sistemi potrebbe determinare per l'Ente in termini di:
  - capacità di fornire uno o più servizi ad una larga clientela (Enti, utenti finali, ecc.);
  - alto impatto in termini di perdita di business;
  - alto impatto in termini di perdita di immagine e/o reputazione nei confronti della clientela (Enti, utenti finali, ecc.);
  - presenza di conseguenze legali per l'Ente.

  Considerare che non necessariamente isolando un sistema dalla rete, questi risulta al riparo da ulteriori danni; si consideri al riguardo, ad es., un tool installato sul sistema vittima da parte del malintenzionato che ne ha ottenuto l'accesso, che invii dei ping regolari verso un altro host. Se il tool è programmato in modo da cancellare dati sul sistema dove risiede nel momento in cui i ping non vanno a buon fine, può accadere che isolando il sistema si rischi di perdere dei dati in esso contenuti.
- Disabilitare i servizi utilizzati per ottenere l' accesso non autorizzato: questa soluzione si adotta qualora si riesca a determinare il particolare servizio (es.: FTP) del sistema che il malintenzionato ha utilizzato (sfruttandone una vulnerabilità) per ottenere l'accesso.

  Il servizio va disabilitato in maniera temporanea o permanente a seconda della sua effettiva necessità all'interno del sistema.
- Disabilitare l'accesso a porzioni di rete: qualora possibile, disabilitare (a livello di router / firewall) la possibilità di connessioni in ingresso a porzioni di rete regionale che si ritiene siano particolarmente critiche.
- Disabilitare l'account utente utilizzato: a seconda della modalità di accesso, l'account utilizzato può avere diversi gradi di privilegi e può essere utilizzabile su uno o più sistemi della rete regionale; disabilitarlo nel livello più alto possibile.
- Incrementare i livelli di sicurezza fisica: in caso di accesso fisico non autorizzato, valutare la possibilità di opportuni accorgimenti per aumentare i controlli in ingresso alle aree coinvolte.

6.2.1.2 Denial of Service

La strategia di contenimento per l'incidente di sicurezza classificato come "DoS" consiste generalmente nel cercare di terminare il DoS stesso.

La soluzione ideale per fare questo sarebbe quella di bloccare tutto il traffico che proviene dalla sorgente del DoS; tuttavia, come si è accennato nella fase di analisi, molto spesso si tratta di un grande numero di indirizzi IP (non corrispondenti a quello del malintenzionato) dispersi ovunque in Internet.

Inoltre, anche qualora si riesca ad individuare e bloccare un range dal quale vengono utilizzati numerosi indirizzi IP, è possibile che tale range venga poi cambiato di conseguenza.

Si riportano di seguito alcune azioni che potrebbero essere eseguite per cercare di mitigare l'incidente di sicurezza:

- implementare soluzioni di filtraggio: alterare il perimetro di sicurezza della rete filtrando i pacchetti che determinano il DoS.

  Questa soluzione non sempre è possibile, in quanto può determinare una mancanza di disponibilità di un servizio verso la clientela (es.: DoS condotto mediante la modalità SYN flood utilizzando la porta 80 del protocollo HTTP del web server; bloccando i pacchetti di tipo SYN verso quella porta si impedisce l'accesso al sito web a tutti gli utenti).
- limitazione di banda; limitare la banda del sistema (o del servizio) vittima, così che un massimo numero di pacchetti al secondo possa raggiungere il sistema (o sfruttare un servizio);
- provvedere all'aggiornamento del sistema: soluzione da adottare qualora un sistema presenti una vulnerabilità che lo renda suscettibile ad un attacco di tipo DoS (es.: crash del sistema operativo alla ricezione di pacchetti malformati);
- prendere accordi con il proprio ISP al fine di implementare opportuni meccanismi di filtraggio per bloccare un eventuale incidente in corso;
- rilocare il sistema: cambiare indirizzo IP del sistema vittima del DoS, o trasferire il particolare servizio (vittima del DoS) su un altro sistema.

6.2.1.3 Codice Malevolo

La strategia di contenimento per questo tipo di incidente, a differenza di quanto accade per l'accesso non autorizzato, prevede di valutare inizialmente la soluzione di isolare (disconnettendolo dalla rete) il sistema infettato dal codice malevolo. I termini su cui basarsi per prendere questa decisione sono gli stessi e cioè:

- capacità di fornire uno o più servizi ad un numero considerevole di utenti;
- alto impatto in termini di perdita di business;
- alto impatto in termini di perdita di immagine e/o reputazione nei confronti degli utenti;
- presenza di conseguenze legali per l'Ente.

Tali termini consentono di determinare se le conseguenze (danni) derivanti dalla disconnessione del sistema dalla rete sono maggiori dei rischi che si corrono lasciandolo connesso.

Di seguito si elencano alcune azioni che potrebbero essere eseguite per cercare di mitigare l'incidente di sicurezza:

- identificare ed (eventualmente) isolare altri sistemi infetti;

  poiché può accadere che il codice malevolo non venga rilevato dal software antivirus, utilizzare altre modalità di ricerca, quali ad esempio:

- Port scan per verificare la presenza di porte in ascolto utilizzate dal codice malevolo (alcune delle quali note in letteratura);
- Cleanup-tool sviluppati appositamente per rilevare e rimuovere determinati codici malevoli;
- controllare i log di sistemi (es.: Email server, firewall) dove presumibilmente il codice malevolo ha lasciato traccia;
- configurare HIDS/NIDS per rilevare signature associate alla presenza/ passaggio del codice malevolo;
- controllare i processi attivi sul sistema per avere conferma che siano tutti legittimi;

- configurare i sistemi (server e/o client) di posta elettronica: qualora la signature relativa al codice malevolo non sia ancora presente, provare a configurare la posta elettronica in modo da bloccare e-mail che presentino degli elementi in qualche modo riconducibili al codice malevolo (es.: nome soggetto/oggetto, nome/tipo file allegato);
- nei casi di infezione di un gran numero di sistemi infettati all'interno della rete che determini, a causa dell'elevato traffico, l'impossibilità di utilizzo del servizio di posta elettronica e/o una notevole riduzione della disponibilità di banda sia interna alla rete regionale sia verso Internet:
  - spegnere il sistema server di posta elettronica;
  - isolare la rete regionale da Internet.

  Anche in questo caso vanno applicate le stesse considerazioni che si utilizzano nella scelta di disconnettere dalla rete un sistema critico.
- spegnere il servizio utilizzato dal codice malevolo.

  Considerare la eventuale presenza di una gerarchia di dipendenze fra diversi servizi, al fine di evitare che lo spegnimento di uno di essi determini anche quello (non necessario) di altri.

Si deve considerare che eventuali sistemi spenti durante la fase di contaminazione del codice malevolo, potrebbero prendere l'infezione nel successivo momento di ri-accensione, anche a distanza di diversi giorni.

Bisogna considerare altresì che le metodologie di rilevazione automatica e centralizzata di codici malevoli possono risultare inadeguate in caso di sistemi che utilizzano sistemi operativi virtuali e/o meccanismi di dual-multi boot.

6.2.1.4 Malfunzionamento

La strategia di contenimento per l'incidente di sicurezza classificato come "Malfunzionamento" dipende dalla sua particolare manifestazione.

Al verificarsi del danneggiamento di un componente di un sistema, occorre fare riferimento a:

- lista dei contatti relativa ai referenti interni e/o fornitori per quanto riguarda i sistemi e apparati di produzione:
- struttura di help-desk nel caso di postazione di lavoro individuale.

Al verificarsi del danneggiamento di una struttura ospitante i sistemi (es.: rottura impianto di condizionamento / tubazione, incendio) occorre fare riferimento al responsabile della gestione della sala macchine e, in sua assenza, alla portineria dello stabile, dove è conservata una copia della lista di contatti relativa al personale manutentore.

In caso di incidenti di particolare gravità (es.: allagamento dovuto a rottura di una tubazione ubicata sopra la sala server, incendio legato ad un corto circuito che coinvolge uno o più sistemi), può risultare necessario attivare un piano di Business Continuity o Disaster Recovery, che preveda l'attivazione di un sito alternativo al fine di garantire la continuità delle funzioni aziendali.

6.2.1.5 Uso Inappropriato

Tipicamente, questo incidente di sicurezza non richiede alcuna strategia di contenimento.
Le uniche azioni possibili sono: rimuovere eventuali conseguenze legate a violazione di policy e procedure di sicurezza (es.: software non autorizzato) oppure fare prevenzione (es. implementare filtri di navigazione).

6.2.1.6 Disastro

In caso di incidenti di particolare gravità (es.: allagamento dovuto a rottura di una tubazione ubicata sopra la sala server, incendio legato ad un corto circuito che coinvolge uno o più sistemi), può risultare necessario attivare un piano di Business Continuity o Disaster Recovery, che preveda l'attivazione di un sito alternativo al fine di garantire la continuità delle funzioni aziendali.

6.2.1.7 Multiplo

In presenza di un incidente di questo tipo, la scelta della strategia di contenimento si può basare nel cercare di contenere la componente dell'incidente che è attualmente in corso (e che ne ha determinato la identificazione).

Ad esempio, se è presente un attacco DoS rivolto verso un sistema interno regionale, proveniente da altri sistemi interni infettati da un codice malevolo (non rilevato, o rilevato e rimosso parzialmente) un mese addietro, occorrerà cercare di concentrarsi su quello che in quel momento è in corso, ossia il DoS.

6.2.2 Raccolta Evidenze

Durante la fase di contenimento può emergere la necessità di procedere con la fase di raccolta delle evidenze[23].

La necessità di procedere con la raccolta delle evidenze può essere dovuta[24] a:

- Possibilità di conseguenze legali:
  - per accertare e registrare oggettivamente le responsabilità;
  - per definire la posizione dell'Ente rispetto a quanto accaduto;
- necessità di procedere con indagini più approfondite per determinare l'accaduto o per verificare la reale entità dei danni.

6.2.2.1 Conseguenze Legali

Qualora, a seguito di un incidente relativo alla sicurezza delle informazioni, risulti necessario per l'Ente intraprendere un'azione legale (civile o penale) contro una persona fisica o giuridica, oppure nel caso in cui ci siano le premesse affinché l'Ente possa essere oggetto di azione legale (civile o penale), le evidenze oggettive devono essere raccolte e conservate e presentate al fine di conformarsi ai requisiti di legge applicabili nelle sedi giurisdizionali competenti.

Qualora sia necessario procedere alla raccolta di evidenze affinché siano conservate e messe a disposizione delle autorità giudiziarie, occorre che un membro della UGISI si rechi sul luogo dove si è verificato l'incidente di sicurezza, e:

- identifichi lo scope: identifichi l'area che potrebbe essere di interesse per la raccolta di evidenze. Es.:

[23] RFC 3227: Guidelines for Evidence Collection and Archiving: http://www.ietf.org/rfc/rfc3227.txt
[24] www.aiea.it/pdf/sessioni%20di%20studio%20e%20di%20formazione/2007/Torino_8_febbraio_2007_massa.pdf

- se l'incidente ha coinvolto più sistemi all'interno di una stanza, lo scope è l'intera stanza;
- se l'incidente ha coinvolto più sistemi della rete regionale, lo scope potrà essere costituito da più stanze o edifici;

- protegga lo scope: una volta identificato, occorre proteggere lo scope, delimitando l'area (es.: tramite dei cordoni).

  Fino a prova contraria, almeno in questa fase, tutto ciò che è presente all'interno dello scope deve essere considerato come potenziale origine di evidenze.

  E' importante che in questa fase non venga fatto nulla che possa in qualche modo alterare le evidenze.

- preservi le evidenze volatili: accertarsi che tutte le evidenze di natura volatile siano opportunamente memorizzate, per evitare che possano essere perse. Es.:
  - fotografare le immagini presenti sul monitor di un sistema coinvolto, documentandolo eventualmente, per evitare che vengano perse a causa di perdita di alimentazione.

Nel caso in cui l'Ente abbia intrapreso un'azione legale con relativa denuncia alle Autorità competenti, è necessario congelare i sistemi coinvolti in attesa dell'arrivo delle Autorità stesse a cui saranno consegnate le evidenze oggettive raccolte.

Nel caso in cui esista la possibilità che l'Ente sia oggetto di azione legale da parte di terzi e quindi la raccolta delle evidenze viene fatta a scopo cautelativo, si può procedere in autonomia, avvalendosi anche della collaborazione di consulenti esterni specializzati.

Tutta la fase di raccolta delle evidenze deve essere fatta in modo che le evidenze siano utilizzabili in un processo giuridico. Il processo di raccolta e di conservazione delle evidenze deve essere controllabile e ripetibile.

6.2.2.2 Conseguenze Non Legali

La raccolta delle evidenze, come accennato in precedenza, può avvenire anche qualora si voglia semplicemente procedere con indagini più approfondite, non necessariamente legate ad un proseguo forense.

In tal caso, è comunque conveniente che un membro della UGISI si rechi sul luogo dove si è verificato l'incidente di sicurezza, effettui le azioni preliminari elencate al paragrafo precedente e contatti tempestivamente il Responsabile della Sicurezza coinvolto.

Si riportano di seguito alcuni possibili scenari in cui potrebbe essere di ausilio avviare la fase di raccolta evidenze.

Scenario 1: File crittografati

Un dipendente / collaboratore interrompe il suo contratto di lavoro / collaborazione con RER, lasciando nel proprio sistema delle importanti informazioni che risultano inaccessibili in quanto crittografate.

Scenario 2: Screen Saver

Diversi dipendenti / collaboratori lamentano l'impossibilità tecnica di poter lavorare a causa dell'attivazione di uno screen-saver sul proprio sistema, diverso da quello (eventualmente) impostato, che richiede una password per essere sbloccato.

Nel contempo, un'attività di alert è generata dall' HIDS installato sul Web Server.

Scenario 3: Virus

Un dipendente / collaboratore lamenta che nel corso delle due ultime settimane ha eliminato diverse volte lo stesso virus, nonostante il software antivirus risulti presente e aggiornato.

6.2.2.3 Fasi Raccolta Evidenze

Lo schema seguente riporta le quattro sottofasi in cui è possibile suddividere la fase di raccolta delle evidenze [25]

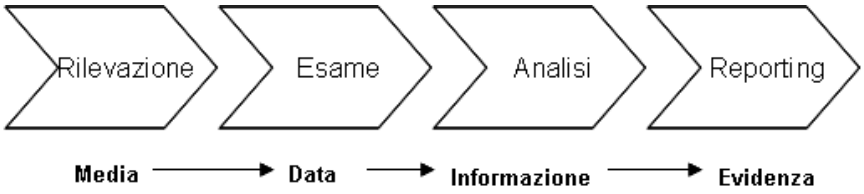


Figura 4: Fasi Raccolta Evidenze[26]

di seguito descritte:

- rilevazione: identificazione e raccolta dei dati, che vengono etichettati e tracciati;
- esame: utilizzo di appositi tool di tipo forense[27] al fine di estrarre le informazioni rilevanti dai dati raccolti;
- analisi: analisi delle informazioni estratte nella sottofase precedente, al fine di capire e trovare le risposte alle domande che hanno portato alla necessità della raccolta delle evidenze;
- reporting: documentazione dei risultati ottenuti dall'analisi, specificando le azioni intraprese, quelle da intraprendere, ed eventuali raccomandazioni (es.: modifiche a procedure, tools).

La raccolta delle evidenze è un processo complicato, in quanto ha lo scopo di trasformare i media (es.: supporti di memorie, sistemi, reti) in evidenze (da presentare eventualmente in sede legale). E' necessario che tutte le sottofasi vengano svolte con accuratezza per preservare l'integrità dei dati e delle informazioni, utilizzando opportuni strumenti di esame ed analisi, versioni originali delle utilità di sistema, recuperate da una copia di salvataggio anteriore alla compromissione del sistema[28], e supporti "legalmente sterili" per la memorizzazione di tutto ciò che viene raccolto ed estratto.

6.2.3 Rimozione

Durante l'attività di rimozione si cerca di eliminare le cause che hanno determinato il verificarsi dell'incidente.

Durante la fase di rimozione, qualora emergano le seguenti necessità:

- allocare delle risorse economiche per la fase di analisi e/o le successive fasi di gestione;
- isolare e poi arrestare eventuali servizi o sistemi di produzione coinvolti;
- valutare eventuali conseguenze legali;

[25] "Media" inteso come memoria RAM, connessioni, processi, supporti di memorizzazione, "Data" come processo di analisi offline dei dati raccolti, "Informazione" come correlazione delle informazioni durante il processo di analisi, "Evidenza" come prova dell'accaduto, in particolare in caso di conseguenze legali

[26] NIST SP 800-86 Guide to Integrating Forensic Techniques Into Incident Response: http://csrc.nist.gov/publications/PubsSPs.html

[27] Clearing House for Incident Handling Tools: http://chiht.dfn-cert.de/
PTK: http://ptk.dflabs.com/ita/index.html
SafeBack: http://www.forensics-intl.com/safeback.html
enCase: http://www.guidancesoftware.com/
ProDiscover: http://www.techpathways.com/DesktopDefault.aspx

[28] File integrity checking (samhain): http://www.la-samhna.de/samhain/
Controllo presenza rootkit (chkrootkit): http://www.chkrootkit.org/

- relazionarsi con altri Servizi/Direzioni dell'Ente;

bisogna contattare tempestivamente il Responsabile della Sicurezza coinvolto per le eventuali azioni da intraprendere.

6.2.3.1 Accesso Non Autorizzato

Qualora il malintenzionato abbia ottenuto un Accesso root non autorizzato ad un sistema, in generale la soluzione migliore consiste nel:

- reinstallare il sistema operativo (qualora si abbia a disposizione una precedente copia di backup testata dei dati e applicazioni che risiedono nel sistema);
- eliminare la/le (eventuali) vulnerabilità che hanno consentito l'accesso non autorizzato.

Qualora l'Accesso sia mediante utenza non-root e non sia possibile reinstallare il sistema operativo, è possibile:

- utilizzare strumenti di rilevazione e rimozione rootkit[29];
- eliminare la/le (eventuali) vulnerabilità che hanno consentito l'accesso non autorizzato.

In ogni caso è conveniente cambiare le password presenti nel sistema.

Qualora l'accesso sia avvenuto anche a causa di password non appropriate, bisogna eventualmente rivedere la policy che stabilisce i requisiti da rispettare per la creazione di password.

6.2.3.2 Denial of Service

In questo caso la fase di rimozione coincide con quella di contenimento e che consiste generalmente nel cercare di terminare il DoS stesso.

6.2.3.3 Codice Malevolo

In generale i software anti codice malevolo (es.: antivirus, antispam) rimuovono la causa dell'infezione[30].

Occorre sottolineare che nel caso in cui siano infettati un gran numero di sistemi, l'attività di rimozione può richiedere diversi giorni o settimane per essere portata a compimento.

Qualora non sia possibile eliminare la causa dell'infezione dal sistema, occorre provvedere a reinstallare il sistema operativo, ripristinando i dati a partire dalle ultime versioni di backup pulite e valide.

Di seguito si riportano i casi in cui, in generale, è necessario prendere in considerazione una tale eventualità:

- il codice malevolo (es.: backdoor) ha determinato un accesso root non autorizzato al sistema;
- il codice malevolo (es.: rootkit) ha replicato files di sistema e/o di boot;
- dopo la rimozione del codice malevolo, il sistema presenta un comportamento instabile.

6.2.3.4 Malfunzionamento

[29] Chkrootkit: http://www.chkrootkit.org/
[30] NIST SP 800-83, Guide to Malware Incident Prevention and Handling: http://csrc.nist.gov/publications/PubsSPs.html.

Fare riferimento a quanto riportato nella fase di contenimento.

6.2.3.5 Uso Inappropriato

Fare riferimento a quanto riportato nella fase di contenimento.

6.2.3.6 Multiplo

Fare riferimento a quanto riportato nella fase di contenimento.

6.2.4 Ripristino

Durante l'attività di ripristino, i sistemi coinvolti vengono riportati nelle condizioni in cui erano prima del verificarsi dell'incidente.

Per la fase di ripristino, qualora i sistemi coinvolti dall'incidente di sicurezza siano di produzione, attivare le stesse procedure di validazione applicate dopo l'installazione di nuove applicazioni o upgrade rilevanti; in particolare fare riferimento a quanto espresso nel Disciplinare Tecnico per amministratori di sistema della Giunta regionale dell'Assemblea legislativa, in particolare alle tabelle B, C, e D.

7 Chiusura Incidente e Notifica

Terminata la fase di ripristino, l'incidente di sicurezza si può ritenere chiuso.

L'UGISI è tenuto a informare dell'avvenuta chiusura dell'incidente, inviando in forma riservata il *Rapporto di incidente di sicurezza,* il Responsabile della Sicurezza coinvolto il quale ne effettua la revisione finale.

Poi, come previsto dal paragrafo 6.2 dell'Allegato A del Disciplinare Tecnico in materia di verifiche di sicurezza e controlli sull'utilizzo delle strumentazioni dell'Amministrazione, il Responsabile della Sicurezza competente deve *"inviare in forma riservata il Rapporto incidente di sicurezza ai Responsabili coinvolti (Responsabili del trattamento di dati personali, Responsabili della sicurezza o Responsabili dei Sistemi Informativi di altri enti, Responsabili da cui il soggetto che ha provocato l'incidente dipende funzionalmente) o ad altri titolari del trattamento di dati personali.*

Qualora l'incidente si sia verificato nel sistema informatico condiviso e interconnesso tra Giunta e Assemblea Legislativa, il Responsabile della sicurezza della Giunta deve inviare in forma riservata il Rapporto di incidente di sicurezza al Responsabile della sicurezza dell'Assemblea Legislativa."

Il Responsabile della Sicurezza coinvolto deve conservare il Rapporto in una cartella ad accesso limitato ai propri membri, per cinque anni o per tutto il tempo ritenuto necessario (ad esempio allo svolgimento di indagini, nel caso di conseguenze penali, o perlomeno alla definitiva rimozione delle cause scatenanti l'incidente).

8 Lezioni Apprese

In questa fase si cerca di comprendere l'accaduto per individuare eventuali migliorie ai sistemi, risorse e policy, e per impedire o ridurre le probabilità che un incidente di sicurezza simile possa verificarsi nuovamente, o comunque per garantire una risposta più efficace.

A valle di un incidente di sicurezza può risultare utile eseguire le seguenti attività:

- prevedere una piccola attività di reportistica in modo da riassumere alcuni parametri caratteristici del processo di gestione degli incidenti, così da consentire una sua più immediata valutazione in termini di efficacia ed efficienza.

  E' possibile utilizzare la seguente tabella:

  Tabella 12: valutazione incidenti di sicurezza

Parametro	Valore
Numero complessivo di rilevazioni incidente ricevute	
Numero complessivo di incidenti identificati come "Accesso Non Autorizzato"	
Numero complessivo di incidenti identificati come "Denial of Service"	
Numero complessivo di incidenti identificati come "Codice malevolo"	
Numero complessivo di incidenti identificati come "Malfunzionamento"	
Numero complessivo di incidenti identificati come "Uso Inappropriato"	
Numero complessivo di incidenti identificati come "Disastro"	
Numero complessivo di incidenti identificati come "Multiplo"	
Numero complessivo di rilevazioni incidenti rivelatisi Falsi Positivi	
Tempo medio gestione incidenti	

  da aggiornare a valle di ogni incidente (o presunto tale).

  .

- Verificare che il processo di gestione incidenti sia risultato adeguato a fronteggiare la situazione.

  In particolare porsi le seguenti domande:

  - La procedura di gestione incidenti è stata eseguita al verificarsi dell'incidente? E' risultata adeguata?
  - Sono stati presenti degli aspetti che hanno rallentato la risoluzione dell'incidente?
  - Sono presenti degli elementi che si ritiene siano da cambiare per rendere il processo di gestione degli incidenti più efficace ed efficiente?
  - E' necessario aggiornare l' analisi dei rischi a valle dell'incidente?
  - Sono necessarie della azioni correttive da intraprendere a valle (dell'analisi dei rischi e) dell'incidente così da evitare che possa riaccadere?
  - E' necessario modificare le policy aziendali (es.: aggiungere file con una determinata estensione - es.: .scr - tra quelli bloccati dal sistema antivirus)?

- E’ necessario aggiornare e/o migliorare gli interventi formativi al fine di istruire il personale aziendale sulle problematiche inerenti la sicurezza e la privacy dei dati?
- Sono necessarie addizionali risorse (es.: personale, tool, strumento hw) per rendere il processo di gestione degli incidenti più efficace ed efficiente?
- Sono necessarie modifiche e/o riconfigurazioni del software (es.: aumentare frequenza di aggiornamento delle signature dei software antivirus e/o IDS, modificare il livello di dettaglio della detection (falsi positivi / negativi) dei software IDS)?

Qualora emergano aree di miglioramento, bisogna contattare il Responsabile del Servizio Sistema Informativo - Informatico Regionale o il Responsabile del Servizio Gestione e Sviluppo Sistemi Informativi – Informatici e Innovazione dell’Assemblea legislativa, per le eventuali azioni da intraprendere.

Glossario

Nota: il presente glossario contiene solo definizioni di termini utilizzati più volte nel presente documento e comunque di carattere generale e ritenute poco soggette a significative variazioni nell'immediato futuro. Per eventuali ulteriori definizioni, si faccia riferimento ai numerosi dizionari online e siti tematici esistenti[31].

Backdoor: codice (non necessariamente) malevolo che consente l'accesso remoto ad un sistema bypass-ando i controlli di sicurezza.

La backdoor può essere anche un software (es.: VNC) utilizzato da un amministratore di rete effettuare connessioni da remoto.

Banner Grabbing: attività di (enumeration) hacking che consiste nell'ottenere informazioni riguardo applicativi installati in un sistema, tramite il banner iniziale che questi applicativi propongono (dove viene esplicitamente dichiarata l'applicazione, la versione e l'eventuale livello di patching), quando interrogati mediante opportuni protocolli (es.: telnet, nmap).

DNS Zone Transfer: operazione di copia, di solito eseguita all'interno di una "zona", di tutti i record presenti all'interno di un DNS master su un DNS slave; mediante opportuni attacchi è possibile "ingannare" il server DNS facendo in modo che l'intero database DNS venga trasferito su di un server utilizzato dall'attaccante.

Evidenza: nell'ambito dell'analisi forense, si intende una "traccia" di reato.
Affinché siano valide da un punto di vista legale, una evidenza deve essere[32]:

- Ammissibile, per poter essere utilizzabile in sede legale;
- Autentica, ovvero strettamente legata ai media digitali da cui è stata rilevata;
- Completa, correlando tutte le informazioni possibili;
- Affidabile, per non sollevare dubbi sulla sua autenticità;
- Ripetibile, permettendo a chiunque di ricostruire il processo che ha portato alla sua rilevazione ottenendo gli stessi risultati.

Falso Negativo: si verifica quando un software non segnala erroneamente la presenza di un codice malevolo e/o di una signature relativa ad un tentativo di azione malevolo in genere, quando questa è effettivamente presente.

Falso Positivo: si verifica quando un software segnala erroneamente la presenza di un codice malevolo e/o di una signature relativa ad un tentativo di azione malevolo in genere, quando questa non è presente.

Footprinting[33]: attività di hacking volta a identificare le risorse informatiche possedute dal bersaglio (es.: organizzazione), quali

- Internet: nomi di dominio, IP pubblici, ecc.
- Intranet: protocolli in uso (IP, IPX), IDS attivi, ecc.
- Accessi remoti: meccanismi di autenticazione, numeri telefonici, ecc.
- Extranet: VPN, ecc.

Logic Bomb: codice malevolo simile al virus, con la caratteristica di attivarsi al verificarsi di determinati eventi temporali e/o comportamentali (es.: raggiungimento di una data temporale, spegnimento del computer, acceso a una determinata cartella).

Di seguito riportiamo una tabella che riassume le principali differenze fra i codici malevoli sopra esposti:

	Capacità di legarsi ad un file	**Capacità di replicarsi in modo automatico**	**Capacità di replicarsi in modo automatico tra**

[31] http://www.sans.org/resources/glossary.php
[32] www.aiea.it/pdf/sessioni%20di%20studio%20e%20di%20formazione/2007/Torino_8_febbraio_2007_massa.pdf
[33] http://www.aiea.it/pdf/sessioni%20di%20studio%20e%20di%20formazione/2008/Torino%2017%20gennaio%202008%20Pensare%20come%20un%20hacker.pdf

		all'interno del sistema	sistemi collegati in rete
Virus	Si	Si	No
Worm	No	Si	Si
Trojan	Si	No	No
Logic Bomb	Si	Si	No

Phishing: frode che si manifesta nell'inviare messaggi di posta elettronica che, in apparenza, sembrano provenire da siti Web sicuri (es.: istituti bancari, società di emissione di carta di credito), ma che hanno il solo scopo di dirottare l'utente verso siti Web fake, al fine di richiedere informazioni riservate (es.: password, numeri carta di credito, dati inerenti al proprio conto).

Rootkit: codice malevolo che si caratterizza nella sua capacità di modificare le funzioni principali del sistema operativo, con lo scopo di aggiungere specifiche capacità al codice malevolo stesso (es.: nascondere la propria presenza ai software anti-codice malevolo).

Il rootkit viene spesso utilizzato in congiunzione con la backdoor.

Spyware: codice (non necessariamente) malevolo, caratterizzato dal manifestarsi tramite finestre di pop-up sul monitor dell'utente, con lo scopo di acquisire informazioni sul comportamento di interazione dell'utente col sistema; questo codice viene installato all'insaputa dell'utente, (es. keystroke logger) e di solito non viene rilevato se non con anti spyware

Lo spyware può anche essere legato ad un comportamento corretto di un programma che lo utilizza per determinati scopi (es.: reminder per aggiornamenti).

Traceroute: applicazione che consente di ricavare gli indirizzi IP delle reti attraversate per raggiungere il bersaglio a partire dal sistema che ospita l'applicazione stessa.

Trojan: codice malevolo caratterizzato dal fatto di legarsi ad un file (tipicamente un eseguibile di un programma noto e dall'apparenza innocuo (es.: gioco, movie)).

Il concetto di Trojan è in qualche modo legato a quello di social engineering, in quanto in entrambi i casi l'utente viene raggirato mediante una qualche forma di innocua apparenza.

A differenza di virus e worm, i Trojan non sono in generale capaci di replicarsi in modo automatico.

Virus: codice malevolo caratterizzato dal fatto di legarsi ad un host-file, e di replicarsi in modo automatico all'interno del sistema dove è presente.

A differenza del worm, il virus non si replica in modo automatico tra sistemi collegati in rete, ma necessita di una qualche forma di interazione da parte dell'utente.

Esistono diversi tipi di virus, a seconda della modalità con cui agiscono, delle porzioni di memoria che vanno ad intaccare, e così via.[34]

[34] http://www.zonapc.it/articoli/virus/virus_1.php

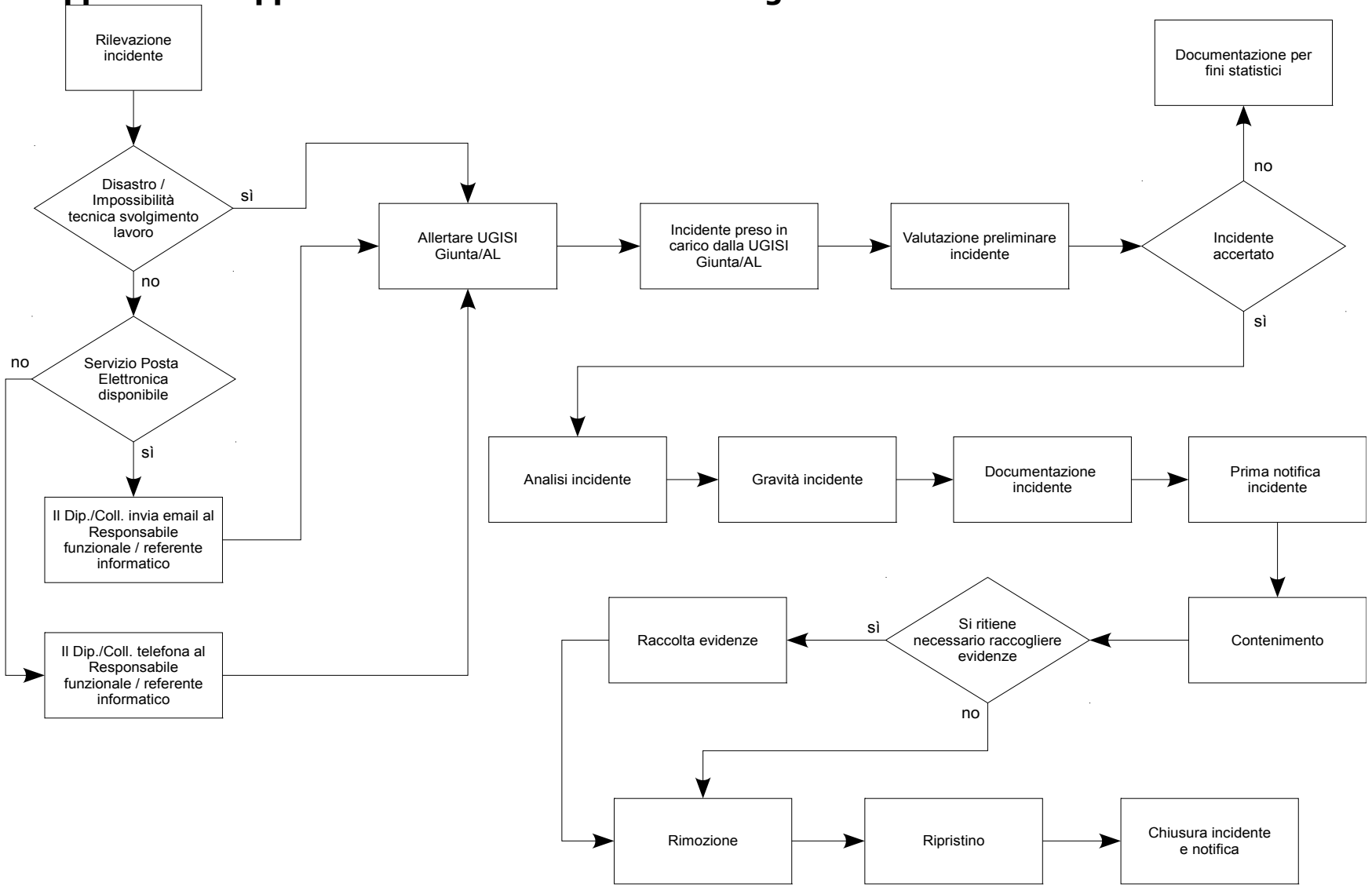
Worm: codice malevolo[35] simile al virus, con la differenza che non necessita di legarsi ad un host-file, e si replica in modo automatico sia all'interno del sistema dove è presente, e sia tra sistemi collegati in rete.

Zombie: (ignaro) sistema su cui è installato un programma comandato da remoto da un sistema master.

Tipicamente esso trova applicazione nei DDoS, dove più sistemi zombie vengono utilizzati per far partire un attacco verso un determinato target.

[35] http://it.wikipedia.org/wiki/Worm

Appendice: Rappresentazione della Procedura di gestioni incidenti



REGIONE EMILIA-ROMAGNA
Atti amministrativi

GIUNTA REGIONALE

Grazia Cesari, Responsabile del SERVIZIO SISTEMA INFORMATIVO - INFORMATICO REGIONALE, in qualità di Responsabile della Sicurezza della Giunta regionale, esprime, ai sensi della deliberazione della Giunta Regionale n. 2416/2008, parere di regolarità amministrativa in merito all'atto con numero di proposta DPG/2012/7342

data 17/05/2012

IN FEDE

Grazia Cesari