Note per l'implementazione delle “misure minime”

v 1.1
24 Maggio 2018

CONSIDERAZIONI GENERALI

Questo documento contiene le proposte del gruppo di lavoro della Commissione Calcolo e Reti istituito per fornire indicazioni pratiche per un'implementazione della Circolare del 18 aprile 2017, n. 2/2017 (in sostituzione della circolare n. 1/2017 del 17 marzo 2017): «Misure minime di sicurezza ICT per le pubbliche amministrazioni. (Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015)», pubblicata sulla GU del 5-5-2017, di seguito indicata come "misure minime" o MM. Facciamo notare che alcune delle misure erano già imposte dal *Disciplinare per l'uso delle risorse informatiche dell'INFN* (*Disciplinare* nel seguito), approvato dal Consiglio Direttivo dell'Ente il 31 marzo 2016.

I componenti del gruppo di lavoro sono:

- Silvia Arezzini,
- Alessandro Brunengo
- Luca Carbone
- Roberto Cecchini,
- Vincenzo Ciaschini,
- Michele Gulmini,
- Leandro Lanzi,
- Paolo Lo Re,
- Antonella Monducci,
- Sandra Parlati,
- Gianluca Peco.
- Massimo Pistoni,
- Stefano Zani.

La nostra impressione è che le misure minime siano state pensate senza tenere in conto le necessità e le particolarità di un ambiente come il nostro. Pur riconoscendo la loro importanza e ragionevolezza, riteniamo che alcune di esse non possano in alcun modo essere applicate ad apparecchiature destinate ad usi di ricerca e/o tecnologici. Tanto per fare un esempio, si pensi al caso, tutt'altro che raro, dell'impiego di software autoprodotto: come sarebbe possibile farlo rientrare nell'elenco di "software autorizzati" [2.1.1] senza ricadere in problemi gestionali difficilmente risolvibili?. E ancora, sembra molto difficile togliere l'accesso privilegiato dei ricercatori e docenti ai propri portatili: misura necessaria se si vogliono applicare centralmente una buona parte delle misure minime. Ci sembra quindi essenziale distinguere tra due tipologie di apparecchiature:

- **di prevalente uso tecnico - scientifico** (**TS**):
  - server dedicati al calcolo scientifico,
  - desktop, laptop e device mobili per attività istituzionali di ricerca, comprese quelle tecnologiche e per la gestione dei sistemi,
  - dispositivi di acquisizione dati,

- dispositivi per la gestione di impianti;

- **di uso gestionale - amministrativo** (**GA**):
  - macchine che trattano dati gestionali, riservati, personali, sensibili (p.e. contratti, accordi di collaborazione, convenzioni, trasferimento tecnologico e fondi esterni),
  - server in gestione al Servizio Calcolo.

Per la prima categoria di apparecchiature, che per forza di cose devono essere amministrate dagli stessi utilizzatori, alla luce anche di quanto indicato dalla stessa AgID[1], sono stati prodotti dei documenti tecnici (*Norme* nel seguito) contenenti le **misure obbligatorie** richieste dalle MM e suggerimenti di *best practice* . Questi documenti saranno consegnati agli amministratori delle macchine TS, che dovranno dichiarare di averne presa visione, alla stregua di quanto viene fatto per il Disciplinare, assumendosi la **completa responsabilità** della gestione delle stesse.

Per la seconda categoria, sia pure con un notevole impegno, siamo riusciti ad applicare una buona parte delle MM entro il 31 dicembre 2017, nonché ad individuare le soluzioni tecniche ed il relativo piano di attuazione per quelle che ancora non è stato possibile realizzare, come indicato nel documento di implementazione firmato dal Presidente il 30 Dicembre 2017.

Ci preme far notare che l'attuazione delle MM, oltre all'impegno straordinario iniziale per la loro adozione, che coinvolgerà pesantemente il personale informatico di tutte le strutture dell'INFN, cambierà anche le modalità con cui sono stati gestiti molti dei Personal Computer, desktop e laptop GA. Tutte le macchine di questa categoria, che attualmente siano amministrate dagli stessi utilizzatori, dovranno passare sotto la **completa gestione** dei Servizi di Calcolo, con un pesante aggravio di lavoro, anche per la gestione ordinaria.

Un altro caso da tenere presente è quello degli utenti *roaming*, che si autenticano via 802.1x usando le credenziali della propria *home institution* (p.e. tramite **eduroam**). Anche qui non vediamo come le MM possano essere applicate, e del resto la particolarità di questo tipo di accesso è riconosciuta anche nel *Disciplinare*. Riteniamo sufficiente imporre che questo tipo di connessione consenta solamente l'accesso **all'esterno della LAN**.

---

1 Alla domanda posta dal gruppo di lavoro CODAU sull'implementazione delle MM: "In mancanza del responsabile designato ai sensi dell'Art.17 del CAD e dell'incarico esplicito ad un dirigente, chi ha la responsabilità dell'attuazione delle misure minime?", AgID ha risposto:

> La responsabilità complessiva per l'Ateneo è in capo al rappresentante legale ovvero al Rettore. Tuttavia, stante l'articolazione organizzativa degli Atenei, in essi sono tipicamente presenti strutture dotate di ampia autonomia, che si estende anche alla definizione, implementazione ed erogazione di servizi. In considerazione di ciò, la responsabilità di applicazione delle misure minime va, per tali strutture, ascritta al Responsabile della struttura stessa, tipicamente il Direttore di Dipartimento. In taluni casi, legati all'utilizzo di dispositivi e postazioni sotto il totale controllo dei singoli utenti (es. docenti e ricercatori) la responsabilità diretta potrebbe essere ascritta ad essi.

1. INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI

La differenza tra [1.1.1] e [1.1.4] è che il primo è di **tutte** le risorse, mentre il secondo solo di quelle **autorizzate.**

Non riteniamo che l'inventario debba essere sempre disponibile in un db (o simili), ma che semplicemente si sia in grado di generarlo a richiesta.

La responsabilità è dei Servizi Calcolo o dei Responsabili Locali nel caso di reti gestite da altri (cfr. il *Disciplinare*).

[1.1.1] IMPLEMENTARE UN INVENTARIO DELLE RISORSE ATTIVE COLLEGATO A QUELLO DI ABSC 1.4

Nelle nostre Strutture non sono consentiti accessi non autorizzati, come anche indicato nel *Disciplinare*.

[1.3.1] AGGIORNARE L'INVENTARIO QUANDO NUOVI DISPOSITIVI APPROVATI VENGONO COLLEGATI IN RETE.

[1.4.1] GESTIRE L'INVENTARIO DELLE RISORSE DI TUTTI I SISTEMI COLLEGATI ALLA RETE E DEI DISPOSITIVI DI RETE STESSI, REGISTRANDO ALMENO L'INDIRIZZO IP.

Si conservano le assegnazioni di indirizzi IP ai MAC Address. In linea con le normative attuali i **dati verranno conservati per almeno 6 mesi**.

Le informazioni sono reperibili nei log e nei file di configurazione, a seconda del tipo di accesso che si utlizza: dhcp (“statico” o dinamico), radius, dns, NAT, ecc..

2. INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI

Tutte le misure di questo capitolo ci sembrano ragionevolmente applicabili solo alle apparecchiature di tipo GA.

Agli utenti non deve venire consentito l'accesso privilegiato, il che ovviamente causerà grossi problemi organizzativi, dato che il maggior controllo si tradurrà in un aumento del carico di lavoro richiesto ai singoli Servizi Calcolo. Lavoro sia per l'implementazione, sia per la gestione, dato che, togliendo l'accesso privilegiato agli utenti, quasi qualsiasi operazione non ordinaria dovrà essere eseguita dal Servizio Calcolo.

Nel caso di Windows, la soluzione migliore (nel caso di piccoli numeri potrebbe essere preferibile una gestione individuale) sembra il loro inserimento in un Dominio.

Nel caso MacOS, una delle soluzioni possibili per una gestione centralizzata è l'impiego di MacOS Server e dei servizi Open Directory e Profile Manager. Anche qui, nel caso di piccoli numeri potrebbe essere preferibile una gestione individuale, realizzata attraverso immagini e profili gestiti localmente.

[2.1.1] STILARE UN ELENCO DI SW AUTORIZZATI CON RELATIVE VERSIONI NECESSARI PER CIASCUN TIPO DI SISTEMA, COMPRESI SERVER, WORKSTATION E LAPTOP DI VARI TIPI E PER DIVERSI USI. NON CONSENTIRE L'INSTALLAZIONE DI SOFTWARE NON COMPRESO IN ELENCO

Vedi documenti specifici.

Per le apparecchiature TS un elenco di questo tipo non è definibile a priori.

[2.3.1] ESEGUIRE REGOLARI SCANSIONI ALLA RICERCA DI SOFTWARE NON AUTORIZZATO

Il nuovo antivirus risolverà questo problema, almeno per quanto riguarda Windows (seconda metà 2018). Nel caso di sistemi macOS, potrebbe essere necessario attivare un meccanismo di *whitelist* basato su Gatekeeper, che impedisce l'esecuzione di codice non firmato digitalmente. Si può procedere in due modi: creando una distribuzione di software autorizzato e firmato (utilizzando sistemi di installazione *on-demand* tipo Munki), o installando le applicazioni centralmente via macOS Server.

[2.3.2] MANTENERE UN INVENTARIO DEL SOFTWARE IN TUTTA L'ORGANIZZAZIONE CHE COPRA TUTTI I TIPI DI SISTEMI OPERATIVI IN USO, COMPRESI SERVER, WORKSTATION E LAPTOP

Vedi sopra.

3. PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER

Queste MM per le TS sono demandate all'utente, come indicato nelle *Norme.*

[3.1.1] UTILIZZARE CONFIGURAZIONI SICURE STANDARD PER LA PROTEZIONE DEI SISTEMI OPERATIVI

Per l'installazione e la configurazione dei sistemi si possono utilizzare metodi diversi a secondo della piattaforma operativa

Microsoft Windows

Nel caso di Windows può essere utilizzato il servizio **WDS** (*Windows Deployment Servers*). WDS è un servizio che permette, tramite la rete e con l'ausilio del protocollo PXE, di automatizzare l'installazione del sistema operativo e di tutti gli applicativi necessari sui personal computer (laptop, desktop, workstation, etc.), al fine di costruire una installazione tipo, già comprensiva delle applicazioni utili e dei necessari sistemi di sicurezza (quali Antivirus, Firewall, IPS, etc.). Inoltre, con l'ausilio del servizio **WSUS** (*Windows Server Update Services*) è possibile mantenere aggiornati i Sistemi Operativi alle più recenti versioni di update, patch e hotfix. Una volta terminato il *deployment* con WDS, rimane solo da effettuare la personalizzazione per l'utente specifico che utilizzerà il computer.

Apple MacOS

Nel caso di sistemi operativi macOS esistono varie soluzioni, sia opensource sia commerciali, che permettono la gestione centralizzata di installazioni e configurazioni di sistema. Attraverso il servizio **NetBoot/NetInstall** (derivazione Apple di PXE) è possibile realizzare installazioni e boot di immagini preconfezionate del sistema operativo e delle applicazioni via rete, compresi eventuali sistemi di sicurezza (Firewall, Antivirus, etc). Attraverso una gestione personalizzata di ProfileManager e del protocollo MDM (macOS successivo a 10.7 Lion) si realizza la gestione centralizzata dei sistemi (sullo stile delle Group-Policy Windows). Per realizzare entrambe le funzioni, lo strumento probabilmente più semplice e di facile implementazione è **macOS Server**.

Linux

In completa analogia con i sistemi Windows, esistono soluzioni per il *deployment* automatico anche della piattaforma opensource Linux. Il servizio **Foreman/Puppet,** opportunamente configurato, automatizza l'installazione del sistema operativo e di tutti gli applicativi necessari sui personal computer, costruendo un'installazione tipo, già comprensiva delle applicazioni utili e dei necessari sistemi di sicurezza.

Sistemi tecnico-scientifici

Eventuali procedure manuali per l'installazione, la configurazione e la personalizzazione dei sistemi di tipo TS, ad opera degli stessi utilizzatori, dovranno essere effettuate seguendo le indicazioni e i suggerimenti indicati nelle *Norme*.

[3.2.1] DEFINIRE ED IMPIEGARE UNA CONFIGURAZIONE STANDARD PER WORKSTATION, SERVER E ALTRI TIPI DI SISTEMI USATI DALL'ORGANIZZAZIONE

Si impiegano le stesse metodologie del [3.1.1].

[3.2.2] EVENTUALI SISTEMI IN ESERCIZIO CHE VENGANO COMPROMESSI DEVONO ESSERE RIPRISTINATI UTILIZZANDO LA CONFIGURAZIONE STANDARD

Si impiegano le stesse metodologie del [3.1.1].
In alternativa si può eseguire un ripristino da una copia immagine, effettuata come indicato in [3.3.1].

[3.3.1] LE IMMAGINI D'INSTALLAZIONE DEVONO ESSERE MEMORIZZATE OFFLINE

Una soluzione potrebbe essere un backup immagine del disco di sistema, fatto immediatamente dopo l'installazione e la personalizzazione (p.e. con **clonezilla**), utilizzabile anche per soddisfare la [3.2.2]. I supporti devono essere smontati subito dopo l'uso (in alternativa si può usare una *tape library*).

[3.4.1] ESEGUIRE TUTTE LE OPERAZIONI DI AMMINISTRAZIONE REMOTA DI SERVER, WORKSTATION, DISPOSITIVI DI RETE E ANALOGHE APPARECCHIATURE PER MEZZO DI CONNESSIONI PROTETTE (PROTOCOLLI INTRINSECAMENTE SICURI, OVVERO SU CANALI SICURI)

E' necessario usare sempre:
- **RemoteDesktop**, per la gestione remota di Windows,
- **SSH** o **Screen Sharing** per la gestione remota di macOS (dalle versioni macOS successive alla 10.8 Screen Sharing si basa su VNC fully encrypted),
- **SSH** per la gestione remota di Linux.

Per le TS è specificato nelle *Norme.*

4. VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITÀ

[4.1.1] AD OGNI MODIFICA SIGNIFICATIVA DELLA CONFIGURAZIONE ESEGUIRE LA RICERCA DELLE VULNERABILITÀ SU TUTTI I SISTEMI IN RETE CON STRUMENTI AUTOMATICI CHE FORNISCANO A CIASCUN AMMINISTRATORE DI SISTEMA REPORT CON INDICAZIONI DELLE VULNERABILITÀ PIÙ CRITICHE

Il gruppo Auditing

- esegue scansioni periodiche **dall'esterno** della LAN;
- mette a disposizione una versione di **kali** personalizzata (**INFNKALI**: **OpenVAS**, **nmap**, **ethereal**, **nikto**), mantenuta sempre aggiornata, che ogni Servizio Calcolo dovrà utilizzare per le scansioni **dall'interno** della propria rete locale (per un buon risultato sarà necessario definire su ogni nodo un utente non privilegiato). L'esecuzione di queste scansioni va eseguita anche sulle macchine TS.

[4.4.1] ASSICURARE CHE GLI STRUMENTI DI SCANSIONE DELLE VULNERABILITÀ UTILIZZATI SIANO REGOLARMENTE AGGIORNATI CON TUTTE LE PIÙ RILEVANTI VULNERABILITÀ DI SICUREZZA

La distribuzione **INFNKALI** viene mantenuta sempre aggiornata: gli utilizzatori devono scaricare l'ultima versione prima di ogni scansione.

[4.5.1] INSTALLARE AUTOMATICAMENTE LE PATCH E GLI AGGIORNAMENTI DEL SOFTWARE SIA PER IL SISTEMA OPERATIVO SIA PER LE APPLICAZIONI

Per le macchine TS questa è un'obbligo indicato nelle *Norme*. E comunque, come peraltro previsto dalle stesse MM, sono possibili eccezioni **documentate** (p.e. la versione di Java richiesta per le applicazioni del Sistema Informativo).

[4.5.2] ASSICURARE L'AGGIORNAMENTO DEI SISTEMI SEPARATI DALLA RETE, IN PARTICOLARE DI QUELLI AIR-GAPPED, ADOTTANDO MISURE ADEGUATE AL LORO LIVELLO DI CRITICITÀ

[4.7.1] VERIFICARE CHE LE VULNERABILITÀ EMERSE DALLE SCANSIONI SIANO STATE RISOLTE SIA PER MEZZO DI PATCH, O IMPLEMENTANDO OPPORTUNE CONTROMISURE OPPURE DOCUMENTANDO E ACCETTANDO UN RAGIONEVOLE RISCHIO

Vedi sopra.

[4.8.1] DEFINIRE UN PIANO DI GESTIONE DEI RISCHI CHE TENGA CONTO DEI LIVELLI DI GRAVITÀ DELLE VULNERABILITÀ, DEL POTENZIALE IMPATTO E DELLA TIPOLOGIA DEGLI APPARATI (E.G. SERVER ESPOSTI, SERVER INTERNI, PDL, PORTATILI, ETC.)

Vedere il documento specifico, che dovrà essere personalizzato da ogni Struttura

[4.8.2] ATTRIBUIRE ALLE AZIONI PER LA RISOLUZIONE DELLE VULNERABILITÀ UN LIVELLO DI PRIORITÀ IN BASE AL RISCHIO ASSOCIATO. IN PARTICOLARE APPLICARE LE PATCH PER LE VULNERABILITÀ A PARTIRE DA QUELLE PIÙ CRITICHE

Vedi sopra.

5. USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE

[5.1.1] LIMITARE I PRIVILEGI DI AMMINISTRAZIONE AI SOLI UTENTI CHE ABBIANO LE COMPETENZE ADEGUATE E LA NECESSITÀ OPERATIVA DI MODIFICARE LA CONFIGURAZIONE DEI SISTEMI

Le macchine GA verranno gestite dal Servizio Calcolo.

[5.1.2] UTILIZZARE LE UTENZE AMMINISTRATIVE SOLO PER EFFETTUARE OPERAZIONI CHE NE RICHIEDANO I PRIVILEGI, REGISTRANDO OGNI ACCESSO EFFETTUATO

[5.2.1] MANTENERE L'INVENTARIO DI TUTTE LE UTENZE AMMINISTRATIVE, GARANTENDO CHE CIASCUNA DI ESSE SIA DEBITAMENTE E FORMALMENTE AUTORIZZATA

Già previsto nel *Disciplinare*.

[5.3.1] PRIMA DI COLLEGARE ALLA RETE UN NUOVO DISPOSITIVO SOSTITUIRE LE CREDENZIALI DELL'AMMINISTRATORE PREDEFINITO CON VALORI COERENTI CON QUELLI DELLE UTENZE AMMINISTRATIVE IN USO

[5.7.1] QUANDO L'AUTENTICAZIONE A PIÙ FATTORI NON È SUPPORTATA, UTILIZZARE PER LE UTENZE AMMINISTRATIVE CREDENZIALI DI ELEVATA ROBUSTEZZA (E.G. ALMENO 14 CARATTERI).

[5.7.3] ASSICURARE CHE LE CREDENZIALI DELLE UTENZE AMMINISTRATIVE VENGANO SOSTITUITE CON SUFFICIENTE FREQUENZA (PASSWORD AGING).

[5.7.4] IMPEDIRE CHE CREDENZIALI GIÀ UTILIZZATE POSSANO ESSERE RIUTILIZZATE A BREVE DISTANZA DI TEMPO (PASSWORD HISTORY)

Qui la parola “amministrative” non c'è, ma sembra ovvio che si stia facendo sempre riferimento a queste.

[5.10.1] ASSICURARE LA COMPLETA DISTINZIONE TRA UTENZE PRIVILEGIATE E NON PRIVILEGIATE DEGLI AMMINISTRATORI, ALLE QUALI DEBBONO CORRISPONDERE CREDENZIALI DIVERSE

Se la macchina non ha utenze sono sufficienti gli account personali (non privilegiati) degli amministratori che però potranno anche essere utilizzati per la gestione (ad es. con il comando **`sudo`** per i sistemi Linux e macOS o con l'appartenenza al gruppo **`administrators`** per Windows). Negli altri casi gli amministratori dovranno avere due account (non privilegiati) dei quali solamente uno che consenta attività gestionali.

[5.10.2] TUTTE LE UTENZE, IN PARTICOLARE QUELLE AMMINISTRATIVE, DEBBONO ESSERE NOMINATIVE E RICONDUCIBILI AD UNA SOLA PERSONA

Già previsto nel *Disciplinare*.

[5.10.3] LE UTENZE AMMINISTRATIVE ANONIME, QUALI "ROOT" DI UNIX O "ADMINISTRATOR" DI WINDOWS, DEBBONO ESSERE UTILIZZATE SOLO PER LE SITUAZIONI DI EMERGENZA E LE RELATIVE CREDENZIALI DEBBONO ESSERE GESTITE IN MODO DA ASSICURARE L'IMPUTABILITÀ DI CHI NE FA USO

Vedi sopra: tutti i comandi privilegiati in Linux e macOS devono essere eseguiti da account personali con **`sudo`**. In Windows l'account locale `Administrator` è disabilitato (eventuali login di emergenza nel caso che il Dominio sia indisponibile vengono fatti via device esterno).

[5.11.1] CONSERVARE LE CREDENZIALI AMMINISTRATIVE IN MODO DA GARANTIRNE DISPONIBILITÀ E RISERVATEZZA

Le eventuali credenziali amministrative anonime (p.e. `Administrator`) o quelle personali dell'**unico** amministratore verranno conservate in modo sicuro e ne verrà registrato ogni accesso.

Se ci sono almeno due amministratori del sistema non c'è bisogno di norme particolari di conservazione delle loro credenziali, visto che un amministratore è sempre in grado di ottenerne delle nuove.

[5.11.2] SE PER L'AUTENTICAZIONE SI UTILIZZANO CERTIFICATI DIGITALI, GARANTIRE CHE LE CHIAVI PRIVATE SIANO ADEGUATAMENTE PROTETTE.

Le chiavi private devono essere leggibili dal solo proprietario, non devono essere conservate su supporti accessibili via rete e devono essere protette da una password di almeno 8 caratteri alfanumerici.

8. DIFESE CONTRO I MALWARE

Si applicano solo alle GA.

[8.1.1] INSTALLARE SU TUTTI I SISTEMI CONNESSI ALLA RETE LOCALE STRUMENTI ATTI A RILEVARE LA PRESENZA E BLOCCARE L'ESECUZIONE DI MALWARE (ANTIVIRUS LOCALI). TALI STRUMENTI SONO MANTENUTI AGGIORNATI IN MODO AUTOMATICO

Questo viene già fatto. Fanno eccezione i casi in cui questo non avrebbe senso: p.e. server linux senza utenza.

[8.1.2] INSTALLARE SU TUTTI I DISPOSITIVI FIREWALL ED IPS PERSONALI

Le versioni recenti di Windows hanno tutte un firewall attivo per default. I sistemi macOS devono essere configurati per abilitare il firewall di sistema (application Firewall)

Per quanto riguarda gli IPS (Intrusion Prevention System) è presente nella versione per Windows del nuovo antivirus, per quanto riguarda gli altri sistemi, al momento non abbiamo trovato soluzioni soddisfacenti.

[8.3.1] LIMITARE L'USO DI DISPOSITIVI ESTERNI A QUELLI NECESSARI PER LE ATTIVITÀ AZIENDALI

I dispositivi **personali** dovranno accedere alle risorse di rete solo tramite **eduroam**, o altra rete wifi che non consenta l'accesso alla rete interna.

Riteniamo che la categoria "dispositivi esterni" non comprenda, ad esempio, i device USB esterni, che nel seguito vengono indicati come "rimovibili".

[8.7.1] DISATTIVARE L'ESECUZIONE AUTOMATICA DEI CONTENUTI AL MOMENTO DELLA CONNESSIONE DEI DISPOSITIVI REMOVIBILI

Inserita nelle impostazioni di default delle immagini standard.

[8.7.2] DISATTIVARE L'ESECUZIONE AUTOMATICA DEI CONTENUTI DINAMICI (E.G. MACRO) PRESENTI NEI FILE

Default per le applicazioni Office

[8.7.3] DISATTIVARE L'APERTURA AUTOMATICA DEI MESSAGGI DI POSTA ELETTRONICA

Disattivata l'apertura automatiche dei link esterni e degli allegati.

[8.7.4] DISATTIVARE L'ANTEPRIMA AUTOMATICA DEI CONTENUTI DEI FILE

Inserita nelle impostazioni di default delle immagini standard.

[8.8.1] ESEGUIRE AUTOMATICAMENTE UNA SCANSIONE ANTI-MALWARE DEI SUPPORTI RIMOVIBILI AL MOMENTO DELLA LORO CONNESSIONE

[8.9.1] FILTRARE IL CONTENUTO DEI MESSAGGI DI POSTA PRIMA CHE QUESTI RAGGIUNGANO LA CASELLA DEL DESTINATARIO, PREVEDENDO ANCHE L'IMPIEGO DI STRUMENTI ANTISPAM

Diremmo usando **solo** strumenti antispam. Da associare al [8.9.3] di cui sembra un duplicato.

[8.9.2] FILTRARE IL CONTENUTO DEL TRAFFICO WEB

Analizzare il contenuto del traffico comporta l'uso di un firewall a livello applicativo, con costi non sostenibili in tutte le strutture. Strumenti di *network intrusion detection* (p.e. **snort**) possono essere utilizzati per la produzione di allarmi.

[8.9.3] BLOCCARE NELLA POSTA ELETTRONICA E NEL TRAFFICO WEB I FILE LA CUI TIPOLOGIA NON È STRETTAMENTE NECESSARIA PER L'ORGANIZZAZIONE ED È POTENZIALMENTE PERICOLOSA (E.G. .CAB)

Per quanto riguarda la posta elettronica questa funzione viene già svolta dagli antivirus (o filtri a livello MTA). Per quanto riguarda il "traffico web" sarebbe necessario l'impiego di un *firewall* a livello applicativo (cfr. [8.9.2]), non disponibili ovunque, a causa del loro costo elevato.

10. COPIE DI SICUREZZA

Queste attività sono già, almeno in gran parte, implementate.

È necessario spiegare agli utenti quali cartelle vengono salvate e richiedere che i dati di lavoro siano lì conservati.

[10.1.1] EFFETTUARE ALMENO SETTIMANALMENTE UNA COPIA DI SICUREZZA ALMENO DELLE INFORMAZIONI STRETTAMENTE NECESSARIE PER IL COMPLETO RIPRISTINO DEL SISTEMA

[10.3.1] ASSICURARE LA RISERVATEZZA DELLE INFORMAZIONI CONTENUTE NELLE COPIE DI SICUREZZA MEDIANTE ADEGUATA PROTEZIONE FISICA DEI SUPPORTI OVVERO MEDIANTE CIFRATURA. LA CODIFICA EFFETTUATA PRIMA DELLA TRASMISSIONE CONSENTE LA REMOTIZZAZIONE DEL BACKUP ANCHE NEL CLOUD

I backup remoti ("su cloud") devono essere cifrati.

[10.4.1] ASSICURARSI CHE I SUPPORTI CONTENENTI ALMENO UNA DELLE COPIE NON SIANO PERMANENTEMENTE ACCESSIBILI DAL SISTEMA ONDE EVITARE CHE ATTACCHI SU QUESTO POSSANO COINVOLGERE ANCHE TUTTE LE SUE COPIE DI SICUREZZA

Smontare i dispositivi di backup dopo il salvataggio (*tape library* OK).

13. PROTEZIONE DEI DATI

[13.1.1] EFFETTUARE UN'ANALISI DEI DATI PER INDIVIDUARE QUELLI CON PARTICOLARI REQUISITI DI RISERVATEZZA (DATI RILEVANTI) E SEGNATAMENTE QUELLI AI QUALI VA APPLICATA LA PROTEZIONE CRITTOGRAFICA

Per “dati rilevanti” si intendono anche quelli “riservati” e non solo i personali e sensibili. L’elenco dei dati riservati è contenuto nel PdGR.

Non risulta al momento evidente quali categorie di dati debbano essere sottoposte a protezione crittografica.

[13.8.1] BLOCCARE IL TRAFFICO DA E VERSO URL PRESENTI IN UNA BLACKLIST

Cfr. [8.9.2].

Si può ricorrere al blocco a livello DNS (Response Policy Zone, disponibile nelle ultime versioni di **bind**). Esistono liste di domini "pericolosi" scaricabili gratuitamente e aggiornate quotidianamente. È chiaro che una lista di questo tipo deve essere **molto conservativa** ed affidabile. Per questo motivo, se si decide di utilizzare il servizio, sembra più opportuno ricorrere ad un fornitore commerciale (ad es. **spamhaus**). Perché questo meccanismo funzioni è ovviamente necessario proibire l'uso di server DNS esterni.