Considerazioni sulle "Misure minime di sicurezza"

Gruppo Harmony

Workshop CCR
LNGS, 25 Maggio 2017

Considerazioni

- Le Norme Minime sono realizzabili (con uno sforzo non indifferente), ma **solo** limitatamente a macchine “amministrative”, cioè non utilizzate per ricerca o didattica.
- Le metodologie di accesso per utenti *roaming* (p.e. Eduroam) non possono rispettare le NM e vanno in qualche modo escluse (come lo sono, ad esempio, nel **Disciplinare**).

ABSC1: Inventario dei dispositivi

- Non sembra particolarmente critico, almeno per quanto riguarda le norme minime
  - [1-1-1 & 1-4-1] implementare un inventario delle risorse attive, che vengono identificate come tutti i sistemi collegati alla rete e i dispositivi di rete stessi, registrandone almeno l'indirizzo IP.
  - [1-3-1] aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete.
- Tutti registrano queste informazioni, anzi per le macchine “classiche” vengono registrati anche il proprietario e la funzione. Sono esclusi tablet e smartphone, ma l'identificazione è richiesta solo a un livello di sicurezza più alto [1-4-3]
- In alcune sedi esistono strumenti automatici di rilevazione, **non richiesti** al livello minimo.
- Per le macchine connesse tramite NAT: il Servizio Calcolo e Reti avrà la rilevazione del gateway, e il suo responsabile dovrà avere a disposizione il registro delle macchine abilitate in reti nascoste. Tutto già previsto nel **Disciplinare d'uso delle risorse informatiche.**

ABSC2: Inventario dei software

- Ci sembrano **inapplicabili alla generalità delle nostre macchine e reti.**
  - [2-1-1] Stilare un elenco di sw autorizzati con relative versioni. Non consentire installazione di sw non compreso in elenco
  - [2-3-1] Eseguire regolari scansioni alla ricerca di sw non autorizzato
  - [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
- La misura ci sembra applicabile se i PC sono connessi ad un dominio Windows. La criticità risiede nel fatto che nelle Amministrazioni potrebbero essere presenti sistemi di altro tipo.
- Non sembra praticabile togliere sempre al ricercatore l'accesso privilegiato (si pensi ad esempio ai laptop).

ABSC3: Proteggere le configurazioni hardware e software

- Non ci sembra critico per i sistemi "amministrativi" gestiti tramite un dominio windows discorso diverso per altri casi)-
  - [3-1-1] Utilizzare configurazioni sicure standard per la protezione dei sistemi operativi
  - [3-2-1] Definire ed impiegare una configurazione standard per workstation, server e altri tipi di sistemi usati dall'organizzazione.
  - [3-2-2] Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzando la configurazione standard.
  - [3-3-1] Le immagini d'installazione devono essere memorizzate offline.
  - [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).

ABSC4: Valutazione e correzione continua della vulnerabilità

- Alcune patch di sicurezza e la richiesta di installazione delle ultime versioni di sistemi operativi e di software potrebbero essere in conflitto con configurazioni "blindate" necessarie al funzionamento di software vitali (cfr sw Sistema Informativo).
- È necessario predisporre un piano di gestione dei rischi.
  - **[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.**
  - **[4-4-1] Assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano regolarmente aggiornati con tutte le più rilevanti vulnerabilità di sicurezza.**
  - **[4-5-1] Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni.**
  - [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.
  - **[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.).**
  - [4-8-2] Attribuire alle azioni per la risoluzione delle vulnerabilità un livello di priorità in base al rischio associato.

ABSC5: Uso appropriato dei privilegi di amministratore

- Non si rilevano particolari criticità. Alcune misure sono già previste nel Disciplinare.
  - [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.
  - [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.
  - [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).
  - [5-10-1] Assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse.
  - [5-10-2]Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona.
  - [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.
  - [5-11-1] Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza.
  - [5-11-2] Se per l'autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette.

ABSC8: Difese contro i malware

- Acuni aspetti sono chiari e certe misure già applicate, come l'antispam, altri necessitano chiarimenti.
- Filtrare il contenuto comporta l'uso di apparecchiature molto costose e solleva problemi di privacy.
  - [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.
  - **[8-1-2] Installare su tutti i dispositivi firewall ed IPS personali.**
  - **[8-3-1] Limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali**
    - Eliminazione BYOD ed esclusione da accesso alla rete dei device mobile esclusi quelli di servizio?.
  - [8-7-1] Disattivare l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili.
  - [8-7-2] Disattivare l'esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file.
  - [8-7-3] Disattivare l'apertura automatica dei messaggi di posta elettronica.
  - [8-7-4] Disattivare l'anteprima automatica dei contenuti dei file.
  - [8-8-1] Eseguire automaticamente una scansione anti-malware dei supporti rimuovibili 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.**
  - **[8-9-2] Filtrare il contenuto del traffico web.**
  - **[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).**

ABSC10: Copie di sicurezza

- Non abbiamo individuato aspetti particolarmente critici
  - [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.
  - [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.

ABSC13: Protezione dei dati

- Collegamenti anche con il regolamento sulla 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**
  - **[13-8-1] Bloccare il traffico da e verso url presenti in una blacklist.**