POLITICHE DI GESTIONE DELLE COMUNICAZIONI E LORO IMPLEMENTAZIONE

yvette@yvetteagostini.it

vodka@sikurezza.org

Consulente sicurezza delle informazioni

Security evangelist

Moderatrice della mailing list ml@sikurezza.org

DEFINIZIONE

POLITICA DI SICUREZZA:

- documento condiviso ed approvato dai piu' alti vertici dell'azienda
- che definisce quali sono i comportamenti accettabili
- relativamente a specifici ambiti di interesse della sicurezza delle informazioni

Le politiche non sono procedure ne' tanto meno manuali o guide utente

Comunicazioni elettroniche

- messaggi di posta elettronica
- trasferimento di documenti in formato elettronico (file tranfer)
- partecipazioni a newsgroup, forum, bacheche elettroniche,ecc.
- utilizzo di programmi di instant messaging
- fax
- utilizzo di dispositivi mobili, sia telefonici che per messaggistica

MOTIVAZIONI?

- evitare le conseguenze dell'utilizzo improprio degli strumenti aziendali
  - fuoriuscita indesiderata di informazioni rilevanti e/o dati sensibili
  - pubblicazione di dettagli utili ad eventuali attaccanti
  - diffusione di malware
  - violazione delle leggi
- mantenere un livello di sicurezza delle informazioni (asset intangibile) proporzionale al loro valore (e quindi sostenibile)
- Responsabilizzare il personale a ogni livello dell'azienda (diffusione della cultura della sicurezza delle informazioni

ESEMPI

- **Alcuni tipi di malware mandano in giro brani di file presi dagli hard disk dei computer infettati e tra essi vi possono essere anche informazioni riservate….**
- **….Inoltre utilizzano gli indirizzi contenuti nella rubrica**
- **Gli header dei messaggi di posta elettronica contengono informazioni utili sull'indirizzamento interno usato in azienda**
- **Gli utenti aziendali utilizzano programmi di instant messaging e scambiano informazioni con l'esterno in modo incontrollato**
- **Comunicazioni telefoniche di particolare rilievo avvengono su linee non protette**
- **I sistemi di videoconferenza non sono posti in sicurezza…..ecc…ecc…..**

Classificazione delle informazioni

- le informazioni sono parte del patrimonio dell'azienda, sebbene siano intangibili
- hanno un valore e sono soggette a minacce…..
- …..tanto più gravi quanto maggiore è il loro valore….
- ……perciò devono essere protette
- per fare ciò è necessario classificare le informazioni secondo il loro valore, la loro criticità per I processi di business
- esempio:
  - segrete
  - riservate
  - pubbliche

Accesso alle informazioni

- in un sistema che protegge le informazioni non tutti hanno accesso allo stesso set di informazioni

- principio del need to know/least privilege

- inutile essere troppo selettivi a livello di politica se poi non vi è un enforcement coerente e usabile

- inutile regolamentare strettamente l'accesso alle informazioni se il personale non è a conoscenza di:

    - principi di classificazione
    - sanzioni applicabili
    - metodi di enforcement

Ciclo di vita delle informazioni

- tutto il ciclo di vita delle informazioni deve essere preso in considerazione:
  - creazione
  - scambio
  - aggiornamento
  - termine di validità-distruzione

- ogni fase deve essere gestita in modo confacente al valore dell'informazione e ai rischi cui è soggetta

- Esempio: cosa succede agli hard disk dei pc che vengono sostituiti?
- Esempio: come viene gestito l'accesso al file server dove risiedono I file che devono essere aggiornati?

Applicazioni della politica (enforcement): email

- posta elettronica:

Antivirus centralizzato e locale

Aggiornamento pushato centralmente

Isolare nel più breve tempo possibile le postazioni infettate da virus

Controllo del contenuto degli header al fine di evitare diffusione di dettagli architetturali e sistemistici

Diffusione capillare delle regole di utilizzo della posta elettronica ai dipendenti

Applicazioni della politica (enforcement): scambio file

- controllo degli accessi e privilegi granulare
- verifica delle transazioni sui file critici (registro degli accessi)
- utenti non devono avere la possibilità di installare programmi di scambio file se non autorizzati espressamente
- watermarking dei documenti
- eventuale disabilitazione di dispositivi di copia file su cd, chiavi usb
- verifica periodica dei file server per evitare scambio di materiale che violi il copyright

Applicazioni della politica (enforcement): Dispositivi mobili

- implementazione del controllo accessi a livello infrastrutturale
- utilizzo delle vpn
- utilizzo di vpn con accesso condizionato al soddisfacimento di determinati requisiti da parte dei client:
  - cisco network admission control
  - Checkpoint webssl
- autenticazione reciproca bidirezionale (con verifica di certificati, ad esempio)

Comunicazioni telefoniche

- non tutti I telefoni possono chiamare gli stessi numeri
- esclusione di numerazioni speciali
- regole di verifica dell'identità del chiamante (per evitare il social engineering) diffuse a tutto il personale
- utilizzo di dispositivi telefonici cifranti (molto costosi) per le comunicazioni particolarmente sensibili
- VOIP: utilizzo di dispositivi che tengano conto dei rischi (hijacking delle chiamate, DoS)

Domande?