Misure Minime di Sicurezza per la PA

Esperienze del Comune di Vicenza e dei Comuni del GdA

Città di Vicenza

Contenuti

- Tipi di attività svolte
- Descrizione di ogni controllo
- Strumenti sw e problematiche dai comuni del Gruppo di Approfondimento (GdA) sulla Sicurezza Informatica Regione Veneto

Attività

- Configurazioni fatte sui sistemi già presenti
- Dotazioni di nuovi strumenti sw
- Definizione di nuovi processi organizzativi interni

ABSC1 INVENTARIO HW

- OCS Inventory NG per i PC in dominio
- NAGIOS per tutti gli apparati di rete, switch, UPS, MPSL, timbratori, firewall
- Foglio di calcolo con tutti i dispositivi IP, smartphone, telefoni VOIP, telecamere
- Inventario in php di tutto il materiale SIC compresi tablet e portatili (manuale)
- Problemi: frammentazione e mancanza di «ip discovery»: strumento automatico e completo

ABSC2 INVENTARIO SW

- Foglio di calcolo per elenco dei sw autorizzati
- Blocco di sw non presenti in «whitelist»:
  - pc da immagine del 3.2.1 con utenti non amministratori locali non possono installare sw combinato ad antivirus
  - Confronto manuale tra OCS INVENTORY inventario dei sw installati e whitelist
  - Sw commerciali per automatizzare il blocco

ABSC3 CONFIGURAZIONI SICURE HW E SW

- Implementate GPO Policy di dominio AD e policy locali di client Windows
- Creata immagine con configurazione standard con tutti i sw e impostazioni di sicurezza per pc e un template di virtual machine per i server

ABSC3 CONFIGURAZIONI DI SICUREZZA DEI PC

- Firewall windows abilitato pc
- Utente «administrator» locale disabilitato, creato utente amministratore con un nome diverso per ogni pc, utenti utilizzatori non sono amministratori di pc
- Disabilitato IPv6
- Disabilitate macro Office e Open Office
- Disabilitato SMBv1 (vedi raccomandazioni CERT-PA Wannacry)
- Personalizzazioni sui programmi (intranet, icone)
- Configurato il default profile di windows tramite file di risposte automatiche e il sysprep

ABSC4 VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA’

2 attività principali VA e patch management

- Vulnerability Assessment OPENVAS sw open source, usato per testare alcuni server
- VA in consip SPC CLOUD LOTTO 2 SICUREZZA

  www.spc-lotto2-sicurezza.it
- Usato TrendMicro Deep Security e TMVP: policy blocca le connessioni corrispondenti vulnerabilità rilevate e dovute a patch mancanti
- Demo SGBOX sw ad hoc, ha anche SYS LOG
- Aggiornamento dei sistemi e applicazioni: WSUS e sw di terze parti (es: KASEYA)

ABSC5 PRIVILEGI DI AMMINISTRATORE

- Limitazione dei privilegi di amministrazione (Verificati tutti i vari gruppi amministrativi di AD, tolti utenti non nominativi o non più in uso)
- Inventario delle utenze amministrative: ogni account riconducibile ad una sola persona fisica
- Abilitato audit delle modifiche di AD
- Si è definita una procedura interna con le regole per la gestione sicura delle credenziali degli amministratori (lunghezza 14 caratteri, scadenza password).

ABSC8 DIFESE DAI MALWARE

- Antivirus TrendMicro Officescan per tutti i client, TrendMicro Deep Security per alcuni server
- Firewall perimetrale HUAWEY filtraggio per bloccare traffico malevolo che transita in rete, blacklist
- Antispam per proteggere email (Zimbra AMAVIS open)
- Si è rivista la configurazione dei vari sw/servizi già presenti perché rispondesse ai controlli punto 8

ABSC10 COPIE DI SICUREZZA

- Backup e verifiche di restore: sw Arcserve, Vranger passeremo a Veam completo utile in caso di disastro
- Procedure organizzative
- Protezione dei supporti:
  1. Offline
  2. Diversi tipi: nastro e SAN

ABSC13 PROTEZIONE DATI

- Cifratura di quali dati? Stiamo ancora approfondendo il tema legato al GDPR, cifratura dei database
- Crittografia dei portatili: «Bitlocker» di Windows incluso nelle versioni più recenti
- controllo dispositivi esterni: ci sono sw commerciali per gestirli (permettere uso alcuni e non di altri, cifrarne contenuto, tracciarne i trasferimenti) un esempio: Endpoint Protector CoSoSys
- Controlli sulle connessioni internet: cfg sul firewall

Problematiche aperte dal Gda Sicurezza

- Mancanza di risorse economiche e di tempo
- Richiesta alla Regione che fornisca sul portale un servizio, ad esempio OCS Inventory, per tutti i piccoli comuni
- controllo 4 sul Vulnerability Assessment

SOLUZIONI DEI COMUNI DEL GDA SICUREZZA

- Molti fogli calcolo per inventario HD e SW
- Impiego di soluzioni open source
- OCS INVENTORY e NAGIOS x monitoraggio
- GLPI open x inventario con ZABBIX x monitoraggio
- SPICEWORKS x inventario e ticket
- Acronis per immagini pc
- NINITE open x patch e aggiornamenti

SOLUZIONI DEI COMUNI DEL GDA SICUREZZA

- WSUS per aggiornamenti sicurezza windows
- Kaspersky x antivirus e VA, SOPHOS e Symantec antivirus
- Miradore open per inventario e gestione dei mobile MDM
- Zeroshell open per gestire gli accessi al wifi

GRAZIE

elorenzoni@comune.vicenza.it