Caratteristiche del software per il Content Filtering

Il software per la realizzazione di Content Filtering e Web Security dovrà possedere tutte le specifiche caratteristiche che di seguito sono elencate. È fondamentale che tutte le funzionalità richieste siano gestite in modo centralizzato dallo stesso prodotto ed è inoltre necessario che la soluzione sia modulare e scalabile su di un'architettura complessa.

CARATTERISTICHE FUNZIONALI

- Protezione da spyware, mobile malicious code, keyloggers, phishing, pharming, proxy avoidance, siti di hacking, software potenzialmente pericoloso, minacce web realizzate su porte diverse dalla 80

- **Gestione dei protocolli di rete**, compresi quelli incapsulati nella porta http, di Instant Messanging, Peer-to-Peer, **Proxy Avoidance** con un database dinamico, **includendo la protezione dalle comunicazioni di reti Bot**

- **Gestione dei ptotocolli per lo scambio di allegati nei più comuni tool di Instant Messaging**

- **Gestione traffico Http veicolato su porte diverse dall'80;**

- Categorizzazione di siti che comportino perdità di produttività (pubblicità, aste on-line, instant messaging su web, download di file di vario tipo), abuso di banda (tv e radio via Internet, Streaming, peer-to-peer, siti per archivio dati) o responsabilità legale (materiale per adulti, sesso, cattivo gusto...)

- Gestione nel database proprietario di categorie e sottocategorie per un'ottimizzazione delle regole di navigazione (almeno **90 categorie**). Così come per le categorizzazioni relative ad abuso di banda, perdita di produttività o responsabilità legale, anche la categorizzazione relativa a sicurezza dovrà dividersi in sottocategrie

- **Categorie specifiche necessarie sono le sottocategorie dedicate a siti con codice malizioso, spyware, phishing e altre frodi, keyloggers, Bot Networks.**

- Gestione di siti malevoli anche sulla base della reputazione, tale sistema deve essere solo uno degli elementi considerati per la classificazione di un sito malevolo in quanto lo si ritiene di poca utilità in caso di compromissione di siti a good reputation.

- **Gestione back channel comunication attivata da codici maliziosi;**

- **Gestione comunicazione verso l'esterno da parte degli spyware, compresi quelli drive-bys;**

- **Gestione traffico verso l'esterno generato da email-based worm;**

- Sono richiesti aggiornamenti automatici quotidiani del database per url e protocolli

- **É richiesto un meccanismo automatico di download del nuovo delta di DB nel caso vengano riscontrati aggiornamenti critici per la sicurezza: tempo di reazione alla pubblicazione di nuovi aggiornamenti critici pari a 5 minuti**

- Console centralizzata basata su tecnologia Web per la gestione delle policy create in maniera combinata con categorie di siti e protocolli, accedibile su protocollo sicuro HTTPS

CARATTERISTICHE GESTIONALI

- Definizione di policy di sicurezza e categorie di siti customizzabile

- Gestione avanzata delle regole con pagine di avviso, quote di tempo o fasce orarie, capacità di bloccare download o parole chiavi sulla base di categorie ben definite.

- **Gestione multilivello degli amministratori per la stesura delle policy di filtro e l'utilizzo di reportistica: un super amministratore potrà delegare diversi utenti alla gestione delle politiche di filtraggio e/o all'utilizzo della reportistica su diversi gruppi di utenza.**

- **Tutti i log di navigazione potranno essere anonimizzati**, si avrà quindi la possinilità di eliminare dal log tutte quelle informazioni (IP, Username) che possano ricondurre al singolo utente.

- **Logging selettivo solo per categorie interessanti ai fini statistici**

- Alerting con mail, messaggi a schermo, trap snmp a seguito di eventi sistema relativi all'istallazione e/o all'occorrenza di navigazioni per determinate categorie o protocolli.

- Strumenti di reportistica di breve e lungo periodo con la possibilità di schedulare reports e spedirli via e-mail (esportazione report nei formati convenzionali excel, pdf, word...); dovranno essere disponibili strumenti web based per l'analisi real time della navigazione internet nella rete e per l'analisi drill down dei log consolidati.

- **Gestione della banda per soglie specifiche, per tipologia di sito o protocollo utilizzato**

- **Servizio di notifica automatica nel caso in cui il propio sito istituzionale sia infetto da Mobile Malicious Code o il brand sia utilizzato in Internet per attacchi di tipo phising (servizio di notifica Best Effort).**

- **Dovrà essere, possibile ancora con un servizio a notifica, testare le vulnerabilità del web server aziendale.**

- I linguaggi trattati dal database per la categorizzazione dei siti devono essere più di 50

- Interazione con il vendor, tramite un tool automatico, per integrazione del database con categorie di siti e/o protocolli specifici o nuovi. Interfaccia diretta con il vendor per risoluzione di casi specifici o ricategorizzazione di liste di URL.

- **Possibilitá d'aprire ticket di supporto direttamente al vendor**

CARATTERISTICHE ARCHITETTURALI

- Capacità di autoconfigurare le macchine attraverso pac file o WPAD

- Modularità e Scalabilità delle varie componenti software per architetture complesse (diverse migliaia di utenze gestite); **supporto ad implementazioni multi piattaforma con sistemi Linux o Windows.**

- Integrazione con server di autenticazione per ricavare l'autenticazione in modo trasparente da Windows-based directory service, server RADIUS o eDirectory server.

- Possibilità di configurare il software per funzionare in High Availabilty se gestito da un bilanciatore di carico esterno

- **Possibilità di distribuire più sonde per il monitoring del traffico di segmenti di rete distinti**