ANEXO A1

SOLUCIÓN PARA LA PROTECCIÓN AVANZADA DE CORREO.

I. SERVIDOR VIRTUAL FILTRO PARA CORREO ELECTRONICO(ANTISPAM)

A. Características Generales

1. Debe estar licenciado para 3000 buzones por un periodo de mil noventa y cinco (1095) días calendario.
2. Agregar múltiples reportes funcionalidades para poder acomodarlos. Las vistas se podrán personalizar en rangos de tiempo.
3. Debe permitir tener reportes y gráficas de estado de mensajes entrantes/salientes por dominio.
4. Debe proporcionar reportes/gráficas de cantidades de correo detectados según categoría de mensajes como Spam, Malware, mensajes maliciosos, recipientes inválidos, mensajes limpios, etc.
5. Reportes top de usuarios según cantidad de correos recibidos o enviados, detalles del flujo de sus correos y búsqueda por usuario.
6. Reportes de resultados de análisis de Antivirus, Anti-Malware Avanzado, Filtros de Outbreaks (contagios) incluyendo intentos de Phishing, entre otras amenazas.
7. Reportes de análisis de archivo por Anti-Malware Avanzado y búsqueda por SHA-256 y/o SHA-1. Tal reporte proveerá destinatarios que recibieron archivo (de ser el caso) y capacidad de drill-down para ver detalles del mensaje asociado al transporte del archivo de malware.
8. Reportes de filtrado de URLs y categorías Top en los correos entrantes, según tipo de correo.
9. Reportes de alto volumen de correo en base a diferentes parámetros como remitente, top subjects, top filtros de mensaje.
10. Reportes para verificar la capacidad y carga del sistema en diferentes rangos de tiempo, que describen cantidad de conexiones totales entrantes/salientes, promedio de tamaño de correo entrante/saliente, tamaño total de correos, utilización de recursos.
11. Reportes de los estados de las diferentes cuarentenas, con opciones para tomar acción sobre mensajes determinados.
12. Capacidad de calendarizar, enviar y archivar reportes.
13. Rastreo detallado de correos electrónicos: Capacidad de poder hacer búsqueda de un mensaje procesado y poder ver su característica/composición y su detalle cronológico del procesamiento recibido durante el flujo.
14. Todas las funcionalidades anteriores deben ejecutarse desde la consola de gestión centralizada que permitirá que la solución opere en modo activo-activo
15. Debe proveer un componente para enviar correos de prueba, simulando Phishing o ataques de ingeniería social. Se deberá detectar si el usuario abrió el correo electrónico y mostrar estadísticas al respecto. Esta funcionalidad puede ser brindada por la propia marca o marca de terceros siempre y cuando cumpla con todo lo solicitado.
16. La entidad brindará el entorno virtual incluyendo la licencia de virtualización, todo licenciamiento adicional necesario para la implementación como base de datos (no se aceptarán bases de datos tipo express) u otros necesarios para la implementación de la herramienta, deberá ser proporcionado como parte de la solución.

B. Gestión y monitoreo.

1. Capacidad de tener múltiples Gateways Virtuales, para definir diferentes interfaces IP con colas de correo únicas y listeners únicos.
2. Capacidad de Autenticación SMTP entrante y conexiones protegidas por TLS/SSL (con capacidad de elegir si es preferido o mandatorio)
3. Para facilitar la gestión en despliegue de múltiples appliances ya sean físicos y/o virtuales, capacidad para centralizar funciones como reportes, cuarentenas y bitácoras de rastreo de mensajes.
4. Capacidad de alertar vía e-mail, hacia diferentes destinatarios dependiendo de la categoría y severidad de la alerta.
5. Capacidad de generar bitácoras (logs) en varias categorías (Anti-Spam, Anti-Malware avanzado, Cuarentenas, etc.) y niveles de criticidad, y diferentes subscriptores dependiendo del tipo de log.
6. Capacidad de almacenar, rotar, extraer manualmente y empujar por mecanismos de FTP, SCP, Syslog y SIEM las bitácoras generadas. Se aceptará como mínimo dos mecanismos de los antes mencionados y que la capacidad de rotar sea opcional.
7. Capacidad de hacer cambios a la configuración y probarlos antes de que se apliquen (por medio de un "commit") en producción. Se aceptarán soluciones que permitan implementar ambientes de pre producción a fin de probar nuevas configuraciones siempre y cuando esto no genere costos adicionales a la entidad.
8. Capacidad de importar y exportar la configuración del sistema a través de archivo XML y/o un formato estructurado.

C. Manejo de Correo de Alto Volumen.

1. Capacidad de crear filtros de mensajes en base a múltiples parámetros, que permitan la detección de e-mail en alto volumen y aplicar acciones como cuarentena y descartado (drop).
2. Poder aplicar rate-limiting selectivo tanto en flujos entrantes como salientes.
3. Poder aplicar throttling de mensajes por remitente, destino o Gateway Virtual, en base a límites configurables.
4. Poder aplicar excepciones a este tipo de reglas. También se permitirá realizar excepción de control de retransmisión de correo entrante o conexiones por IP address o búsqueda de DNS reversa.
5. Poder manejar y aplicar uno o más perfiles de rebotado de correo (Bounce).

D. Prevención de Spoofing de dominio con DMARC

1. Las políticas de DMARC son publicadas a través de los servidores DNS como resource records (RR) de texto (TXT) y anuncian lo que un recipiente de email debe de hacer con el correo recibido que no está "alineado". "Alineación" se refiere a que si se ha pasado la verificación DomainKeys/DKIM o se a pasado la verificación SPF, entonces el mensaje está alineado y es pasado por DMARC.
2. Tener la capacidad de habilitar verificación de DMARC dentro de las políticas del flujo de e-mail.
3. Tener la capacidad de monitorear y generar reportes de verificación de DMARC.

E. Manejo general de correos electrónicos.

1. Tener que se pueden tener diferentes políticas para tratamiento de correo entrante.
2. Tener que se pueden tener diferentes políticas para tratamiento de correo saliente.
3. Tener que se puede encontrar rápidamente en qué política cae un mensaje, dependiendo del remitente o destinatario.
4. Tener criterios para selección de política - basado en remitente, destinatario, direcciones de e-mail o LDAP Group Queries.
5. Tener capacidad de conectividad con LDAP a través de SSL, y utilizarlo como sólo-lectura.
6. La efectividad de la solución para proteger de correo spam debe ser de al menos 99 %
7. Debe ofrecer una efectividad de protección del 80% del correo spam tan solo con la capa de reputación.

F. Servicios de Seguridad Generales

1. Soportar el escaneo de Antivirus por dos motores, o habilitar Multi-Scanning para escaneo de correos en paralelo. Solo se requiere la licencia de un motor antivirus.
2. Realizar el descartado, cuarentena y entrega de mensajes sospechosos de ser spam.
3. Permitir que los usuarios puedan reportar mensajes de spam a través de un plug-in en su cliente de correo (Outlook) y/o un disclaimer en mensaje de correo.
4. Determinar la acción de entrega, cuarentena, etiquetado, descartar o rebotar mensajes de mercadeo.
5. Debe cómo los mensajes que han caído en uno de los múltiples tipos de cuarentena, pueden recibir acciones predeterminadas, como retención y liberación manual o automática después de cierto intervalo de tiempo.

G. Outbreak Filters y Anti-Phishing

1. Debe tener protección de amenazas emergentes, Outbreak Filters que defiende ante nuevos outbreaks en horas de forma antes de las soluciones de antivirus tradicionales.
2. Tener cómo se puede crear un disclaimer o aviso de OVF en base a una platilla predefinida y variables de sustitución. Este disclaimer se desplegará sobre el cuerpo del correo. Tener también que se puede modificar el Subject del correo.
3. Tener cómo se puede proteger ante ataques mezclados "Blended Threats" por medio de reescribir URLs dentro de mensajes sospechosos. Cuando se da clic, los URL se redireccionan automáticamente a la solución de Web Security del mismo fabricante, el contenido se escanea, y se desplegará una pantalla de bloqueo si el sitio contiene malware.
4. Tener cómo selectivamente por medio de las políticas de e-mail, se puede habilitar el reescribir los URLs para todos los mensajes o bien de únicamente para mensajes no autenticados por DKIM.
5. Tener como ciertos dominios, direcciones IP, hostname (opcional) pueden ser omitidos de la modificación de URL, a través de listas blancas.
6. Tener que estas URLs reescritas siguen teniendo efecto y aun cuando el usuario hace forward del mensaje a alguien dentro de la organización.
7. Tener como los mensajes identificados como Phishing pueden ser enviados a una cuarentena específica.

8. Tener cómo los URLs dentro de los correos pueden ser sujetos a filtrado y categorización web en base a reputación y contenido del sitio. Sitios con URLS identificados como inapropiados según las categorías seleccionadas por el administrador (por ejemplo, Apuestas, Freeware, Hacking, Juegos, Adultos, etc.), pueden ser modificados o bloqueados. De esta manera, si el URL viola la política, el correo podrá ser puesto en cuarentena, descartado, o únicamente el URL modificado o bloqueado.

H. Funcionalidad de Protección contra Malware Avanzado (APTs)

1. Tener capacidad de análisis de archivos mediante Reputación de Archivo y Análisis dinámico (Sandbox) de Archivos.
2. Tener capacidad para presentar un reporte de comportamiento de Archivo dentro de Sandbox y veredicto basado en métricas del comportamiento del malware.
3. Tener capacidad para identificar archivos por medio de su hash SHA-256 y/o SHA-1, y capacidad de hacer búsqueda de la disposición de un archivo para ver estado de bloqueo.
4. Capacidad para seleccionar el tipo de archivos deben ser enviados a análisis dinámico (Sandbox).
5. La plataforma debe realizar las actualizaciones de sus motores de protección automáticamente cada 5 minutos.
6. Capacidad de Análisis Retrospectivo, indicando los cambios de disposición (veredicto) de un archivo, proporcionando seguridad aún y después que un archivo adjunto ha sido entregado.

I. Prevención de Pérdida de Datos (DLP).

1. Tener la capacidad de aplicar políticas de DLP de manera fácil y selectiva al correo saliente.
2. Tener políticas predefinidas tales como PCI, Protección de Privacidad, documentos confidenciales, etc.
3. Capacidad de personalización de políticas predefinidas de DLP.
4. Tener capacidad de crear políticas de DLP nuevas y crear clasificadores custom.
5. Capacidad de medir severidad del incidente de DLP en escala del 0 al 100 y/o 0 al 10 con rangos de "Crítico", "Alto", "Medio" y "Bajo", y tomar diversas acciones dependiendo del nivel de severidad.
6. Capacidad de aplicar diferentes acciones tales como Cuarentena, Entregar y Encriptar.
7. Capacidad de notificar/advertir al usuario que su mensaje es inconsistente con la política corporativa y direccionarlo a capacitación correspondiente. Esta notificación podrá ser personalizada en base una plantilla.
8. Tener en una Tabla los incidentes de DLP en base a su categoría/calificación y la acción tomada, y capacidad de hacer drill-down para verificar la bitácora de rastreo del mensaje y el contenido específico que disparó el incidente.

J. Cifrado/Descifrado de correo electrónico.

1. El objetivo principal es Tener capacidad de cifrado de correos electrónicos por métodos como PXE y S/MIME y/o componente de cifrado de correos al cuál se pueda acceder por usuario y password generado por el usuario destinatario. Se aceptarán características similares siempre y cuando cumpla con el objetivo de la funcionalidad solicitada.

2. Capacidad para enviar correos encriptados al exterior de la organización. El usuario remitente puede especificar qué correo debe de ser encriptado, utilizando alguna palabra clave en el Subject, tal como [CIFRAR].
3. Capacidad para encriptar el correo automáticamente en base al contenido del correo especificado por alguna regla de DLP, diccionario o regla de contenido.
4. El correo podrá ser visto por el destinatario después de introducir un usuario y contraseña válidos (que el podrá establecer registrándose en el Servicio de Cifrado, servicio también integrable con gateways SAML 2.0 o en su defecto permitan al destinatario leer los mensajes previo autoregistro en la misma plataforma ofertada.
5. El destinatario podrá visualizar este tipo de correos tanto en su PC como en un dispositivo móvil como Apple iPhone o bien Google Android, y hacer un reply, conservando el mensaje encriptado.
6. Capacidad de tener "Read Receipts" garantizados. También se aceptará un procedimiento o funcionalidad adicional que permita verificar que el correo cifrado fue accedido.(opcional)
7. Capacidad de hacer recall de mensajes encriptados y establecer expiración para revocar la apertura de tales mensajes, pudiéndose cubrir dicha funcionalidad con un componente adicional que forme parte de la solución ofertada.
8. S/MIME y/o PXE y/o componente de cifrado de correos al cuál se pueda acceder por usuario y password generado por el usuario destinatario.
9. Capacidad de cifrado, firmado y descifrado basados en S/MIME y Public Key Infrastructure (PKI). Esta funcionalidad provee el "harvesting" de certificados, generación de llave de proxy y otras capacidades de gestión de llaves.