CASO DE ÉXITO EN EL CONTEXTO DE SEGURIDAD DE ENDPOINTS Y CORREO ELECTRÓNICO

Alternativas en computación ha proporcionado desde 2010 servicios administrados de seguridad en endpoints y correo electrónico a una empresa pública con una base instalada de casi 60,000 equipos de cómputo de usuario final y un servicio de correo electrónico institucional con más de 85,000 cuentas de correo.
Al inicio del servicio, el cliente tenía presente una problemática recurrente de infecciones informáticas en su base instalada de equipos de cómputo de usuario final lo cual le originaba afectaciones serias sobre todo en su prestación de servicios públicos, también tenía serios problemas con la recepción de correo no deseado lo cual le consumía recursos de cómputo que bien podrían destinarse a sus tareas sustantivas.
Un problema adicional que enfrentaba el cliente era destinar recursos humanos suficientes para realizar tareas de seguridad informática que no son la razón de ser de la empresa.
La solución que se implementó con el cliente para atender la problemática descrita, fue:
La implementación de los SERVICIOS ADMINISTRADOS DE SEGURIDAD DE ENDPOINTS Y CORREO ELECTRÓNICO.

Dichos servicios con los siguientes alcances:

- **Proporcionar una infraestructura que incluye hardware, software, administración, operación, y monitoreo de una solución antivirus y antispyware para equipos de cómputo personal y servidores.**
- **Proporcionar una infraestructura que incluye hardware, software, administración, operación, y monitoreo de una solución antispam perimetral para el correo institucional o corporativo del cliente.**
- **Proporcionar el apoyo técnico necesario para instalar, configurar y aplicar políticas adecuadas que permitan al cliente contar con un servicio administrado de la solución institucional o corporativa propuesta, de manera jerárquica, integrada y con una administración centralizada para brindar protección contra virus, spyware y correo spam perimetral, para los equipos de cómputo personal y servidores.**

Arquitectura básica de la solución propuesta:

La arquitectura de la solución propuesta está integrada por

A) **el servicio de antivirus basado en Symantec Endpoint Protection y**
B) **el servicio de antispam basado en Symantec Messaging Gateway**

Los servicios de administración proporcionados son los siguientes:

- **Para el ambiente de producción los administradores asignados en sitio, certificados por el fabricante de la solución propuesta, en días hábiles con un horario de atención de lunes a viernes de 9:00 a 18:00 horas.**

Sus actividades:

  - **Monitoreo de la correcta operación de la solución, mediante los tableros de control de la consola.**
  - **Atención de eventos relacionados con la solución.**
  - **Implementación de modificaciones a la configuración de la consola y políticas.**
  - **Administración de equipos en la estructura del cliente en grupos.**
  - **Generación de reportes diarios relativos a la atención de incidentes, de monitoreos específicos y estado de funcionamiento de la consola central.**
  - **Generación de procedimientos específicos para erradicación y contención de virus, para instalaciones especiales, para actualizaciones de versiones.**

- **Soporte por Administración Remota vía un acceso seguro, el cual será vía VPN SSL otorgado por el cliente.**
- **Acceso a la base de datos del fabricante donde se pueda consultar en línea la solución a problemas relacionados con los productos.**
- **Soporte técnico del fabricante 7x24 vía telefónica y correo electrónico.**
- **Posibilidad de escalar problemas relacionados al funcionamiento del producto directamente con el fabricante.**
- **Atención de soporte personalizado 7x24 a través de un Gerente Técnico de Cuenta (TAM) con certificado directo del fabricante de la solución propuesta. El TAM se involucra con la implementación, instalación y operación necesarias para el rendimiento ideal de todos los productos utilizados para integrar el servicio, así como mantener el historial de soporte con el cliente. El TAM asiste a reuniones semanales con el cliente para la coordinación técnica de todos los servicios de la solución, así como la**

entrega de los reportes semanales del análisis estadístico de la actividad viral, spyware y antispam, así como los reportes donde se especifiquen las solicitudes de servicio, tiempo de solución y cierre de incidentes de soporte técnico, realiza la visitas semanalmente durante la vigencia del contrato, para proporcionar asesoría técnica especializada, coordinar actividades de instalación, configuración, arranque operacional y adecuación de los productos y servicios ofertados.
Además, el TAM proporciona soporte técnico en horario 7x24 cuando los ingenieros en sitio no tienen los elementos suficientes para dar una respuesta satisfactoria a la atención de peticiones e incidentes del cliente.

Los resultados obtenidos para el cliente, producto de los servicios administrados que le fueron proporcionados durante el periodo enero 2013 a junio de 2016 fueron los siguientes:

El índice de disponibilidad de la infraestructura contra código malicioso se mantuvo en 99.964% y la disponibilidad de la solución de antispam perimetral fue de 99.974%.

Se cubrieron 55,258 clientes de antivirus en promedio. Se realizaron 17´240,559 eventos de contención de incidentes de virus.

Se eliminó el 82.8% de virus de manera automática, 12.07% por escaneo calendarizado, 3.47% por escaneo manual y 1.63% detectados de manera proactiva por el antivirus.

El 87.35% de los incidentes de virus contenidos se debieron a virus conocidos y erradicados. El 56.97% fueron virus de muy bajo riesgo y el 33.62% fueron virus de bajo riesgo.

Se atendieron 4,023 tickets de soporte por mesa de servicio relacionados con los servicios administrados de seguridad de endpoints y correo electrónico.

Durante este periodo la solución de protección de antivirus y antispam en el perímetro de seguridad, reportó las siguientes cifras:

Se recibieron 223´194,747correos en la solución de antivirus y antispam de entrada, donde 122´774,690 (55%) fueron rechazados por mala conexión y reputación, 26´478,071 (11.86%) contenían spam y 22,010 (0.000098%) fueron detectados con virus, permitiendo la entrada de 68´519,977 (30.69%) correos limpios.

A la salida de correo se recibieron 152´234,440 correos, de los cuales 151´328,243 fueron limpios (99.40%), 903,025 fueron detenidos por reglas de contenido (0.59%) y 1,127 por virus (0.00074%).

CONCLUSIONES:

Para el cliente, los beneficios de la contratación de los servicios de seguridad para endpoints y correo electrónico se vieron reflejados sustancialmente en una reducción importante de las infecciones informáticas en su base instalada de equipos de cómputo de usuario final lo cual contribuyó a una mayor productividad de su personal, un mejor aprovechamiento de su infraestructura y una mejora sustancial en la prestación de servicios públicos a su cargo.
La filtración de correo electrónico no deseado, en los porcentajes tan altos mostrados en las estadísticas, le permitió destinar recursos de cómputo a sus tareas sustantivas y logró controlar un punto de ingreso de virus informáticos al analizar todo el correo antes de la entrega al destinatario final.
El cliente no tuvo necesidad de destinar recursos humanos suficientes para realizar tareas de seguridad informática y los utilizó para actividades propias definidas como la razón de ser de la empresa.
El cliente no tuvo la necesidad de adquirir infraestructura de cómputo (hardware y software) para incrementar la seguridad de sus endpoints y correo electrónico ya que con la contratación de los servicios administrados tales recursos se encuentran incluidos.
Como caso especial para ejemplificar los beneficios obtenidos por el cliente se puede mencionar que las soluciones de seguridad en endpoints y correo electrónico utilizadas para el servicio minimizaron el riesgo de pérdida de información a causa del código malicioso Ransomware la propagación de códigos maliciosos de éste tipo tiene como objetivo el cifrar los archivos de sus víctimas y pedir un rescate en bitcoins para recuperar la información. La campaña de propagación de este ataque comienza con un falso correo electrónico que llega a la bandeja de entrada de los usuarios. El asunto del correo simula ser un fax enviado al usuario con un adjunto. Los usuarios que ejecuten esta amenaza verán todos sus archivos cifrados ya que este malware descarga un ransomware y se les exigirá pagar un rescate en bitcoins para recuperar su información. Los ataques de éste tipo generan grandes pérdidas para las empresas en dos sentidos, la pérdida de información y la pérdida económica ya que los costos por recuperar la información cifrada pueden ser de varios miles de dólares.
Es importante señalar que México es el país más afectado en Latinoamérica por infecciones de ransomware.