NEUMANN BUSINESS SCHOOL

ESCUELA DE POSTGRADO

MAESTRÍA EN
GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN

“PROPUESTA DE MEJORA APLICANDO DIRECCIÓN DE PROYECTOS BAJO ENFOQUE PMI EN EL DESARROLLO DE ACTUALIZACIONES DE SEGURIDAD PARA LA RED ASISTENCIAL TACNA ESSALUD”

TRABAJO DE INVESTIGACIÓN
PARA OPTAR EL GRADO A NOMBRE DE LA NACIÓN DE:

MAESTRO EN
GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN

AUTOR:
LARRY EDWIN ANIBAL RIEGA RIEGA

DOCENTE GUÍA:
ERNESTO ALESSANDRO LEO ROSSI

TACNA – PERÚ
2020

Pág.

ÍNDICE

INDICE DE GRÁFICOS

INDICE DE TABLAS

INDICE DE ANEXOS

RESUMEN EJECUTIVO

La presente investigación, tiene como fin, plantear algunas alternativas de mejora automatizadas a muy bajo costo, sin el uso de Internet y de manera transparente para el usuario final, con el objetivo de contar con una estrategia para establecer, implementar, mantener y mejorar contínuamente la gestión de la seguridad de la información en la Red Asistencial Tacna EsSalud , estableciendo un procedimiento para el tratamiento adecuado de los riesgos de seguridad de la información, tratando de minimizar al máximo la afectación de los servicios de salud y establecer medidas de de prevención, respuesta, recuperación y rehabilitación que garanticen la continuidad de las operaciones en la mencionada Red Asistencial.

En suma, se trata de un estudio del tipo de investigación cuantitativa y de alcance explicativo. El diseño de la investigación es no experimental longitudinal de tendencia, la técnica fue la observación y la muestra fue 441 equipos de cómputo funcionando bajo plataforma Windows de la Red Asistencial Tacna EsSalud.

Los informes del control de parches de Sophos (Anexo C), indican que existen en todas las sedes de la Red Asistencial Tacna EsSalud, direcciones Ip con vulnerabilidades críticas, altas, medias y bajas en el sistema operativo, sin solucionar, producto de la falta del despliegue de actualizaciones y parches de seguridad en los equipos de cómputo hacia la mencionada red, desde el Data Center principal en Sede Central en Lima, ya que toda la infraestructura de TI en EsSalud a nivel nacional es gestionada de manera centralizada desde dicho departamento .

Entre los principales hallazgos, podemos mencionar que la Red Asistencial Tacna EsSalud, aún tiene equipos con plataforma Windows XP (17) , lo que constituye una grave fuente de vulnerabilidad dentro del parque informático de la Red Asistencial Tacna EsSalud.

Se obtienen como principales conclusiones, la necesidad de implementar un sistema automatizado multiplataforma de despliegue e instalación de actualizaciones y parches de seguridad sin costo para EsSalud, con una mínima intervención del personal de TI, sin el uso de Internet y evitando cualquier tipo de afectación a los servicios que la entidad brinda a los asegurados.

INTRODUCCIÓN

Las vulnerabilidades electrónicas son uno de los aspectos más críticos dentro de la seguridad de la información. En el periodo 1999-2003 crecieron en un 807% según el CERT, mientras los incidentes en el mismo periodo crecieron en un 1,295% según la misma fuente. Por otro lado, desde el 2001 al 2004, el tiempo de aparición de los mecanismos de explotación de las vulnerabilidades se ha reducido en un 50% año a año.

La primera aproximación hacia el control de las vulnerabilidades se basó en la detección de las mismas y en una priorización de su severidad. En la medida que la complejidad de la red crece, este modelo colapsa por su incapacidad de responder de manera rápida a preguntas tales como : ¿cuál es mi nivel de riesgo actual? ¿Qué mitigo primero? ¿cuánto tiempo tengo para mitigar? ¿cómo ha evolucionado mi riesgo? ¿Qué riesgo debo aceptar?.

Hoy la industria coincide en enfocarse en la Gestión de Vulnerabilidades, buscando responder a las preguntas anteriores con el fin de optimizar el uso de recursos, cumplir con requerimientos legales, normativos y cumplir con los objetivos de negocio.

Es necesario alinear las nuevas tecnologías de seguridad para soportar las necesidades corporativas, esto ayuda con el cumplimiento de los objetivos del negocio, es precisamente ello lo que no está sucediendo en la mayoría de las empresas, porque los mecanismos tradicionales de control reactivos actuales no soportan un crecimiento de negocio inesperado, tampoco hay un adecuado mantenimiento e integración de los sistemas obsoletos heredados. Actualmente, los controles gestionados con tablas de bases de datos, que no son dinámicos como la amenaza moderna, son insuficientes para hacerse cargo de esta realidad, sin capacidad de generar firmas para la velocidad de surgimiento de nuevas

variantes o para detectar su ingreso en código web, presentan lamentablemente una brecha significativa.

La seguridad de información tiene muchas facetas diferentes siendo la meta principal proteger la confidencialidad, integridad y disponibilidad de los activos de información de una organización, cualquier incidente que afecte a uno de estos componentes puede poner en riesgo rápidamente a toda una organización, exponiéndola a conflictos legales y daño en su imagen corporativa. La tendencia en estos momentos es usar Sandboxing, lo que permite aproximarse a controles más efectivos con la utilización de máquinas virtuales, el uso de seguridad positiva a nivel de los dispositivos y la detección de tráfico de servidores de comando y control.

En empresas con esquema de seguridad tradicional, es necesario cambiar la arquitectura centralizada de protección del perímetro, debido a que no pueden bloquear las amenazas de malware moderno-provenientes de la nube, para ello es necesario proceder de manera homogénea, coordinada y cooperativa. Es necesario implementar procedimientos complementarios a la estructura actual, que permitan delegar la administración de los dispositivos de seguridad de la gestión preventiva y reactiva de incidentes a un equipo de personas con experiencia en combatir el malware basado en comportamiento. Este tipo de actividades va a garantizar la respuesta de amenazas globales mediante su detección temprana en la red con una mitigación coordinada entre los motores de inteligencia global propietarios; la gestión de vulnerabilidades y el análisis de las reglas del firewall también vienen acompañados de este escenario granular.

La mayoría de las instituciones no está en la capacidad de prevenir, ni de responder adecuadamente a estas amenazas de malware moderno, porque no tiene una visión de conjunto de cómo estos abusos o amenazas potenciales puede dañar la identidad digital de la empresa al negocio, su impacto es transversal a toda la organización. No es posible anticiparse a riesgos de seguridad, debido a que no

cuentan con una solución predictiva e inteligente, que permita predecir de forma continua las amenazas de malware moderno y anticiparse a los riesgos empresariales, no existe una evaluación proactiva de seguridad con ataques del mundo real.

Se debe de simular las potenciales rutas de ataque, revelando exposiciones presentes en la arquitectura actual, es necesario cambiar el modelo y la forma de pensar para hacer frente a múltiples amenazas que no están basadas en firmas, con el modelo de red actual no se puede garantizar una cobertura del total del vector de amenazas de malware.

Es muy difícil investigar la naturaleza de un evento de malware, debido a la ausencia de herramientas para el análisis forense, lo que se realiza en la mayoría de las veces es restaurar al equipo a su estado original de fábrica, no hay una base de datos de conocimientos. Las Tecnologías de correlación (SIEM) y recolección de logs (Loggers) se encargan de este tipo de tareas y recopilan información sobre la amenaza, facilitando de este modo la actividad forense y un futuro requerimiento de auditoria.