



EL CONDADO DE WAUKESHA DEPENDE DE LA ADMINISTRACIÓN DE PARCHES PARA MINIMIZAR LAS AMENAZAS CIBERNÉTICAS

Por primera vez en la historia, el personal de primera respuesta y los despachadores en los condados de Waukesha y Milwaukee tienen la capacidad de comunicarse fácilmente entre condados, municipalidades y agencias utilizando el nuevo sistema de radios para seguridad pública OASIS (Organización de Subsistemas de RF Interoperables, Seguros y Afiliados). El sistema de radio facilita la interoperabilidad para el personal de primera respuesta en el campo, mejorando la forma en la que se comunican entre ellos y con los centros de 9-1-1.

LISTO PARA UN SISTEMA DE RADIOS NUEVO

Era momento para que el Condado de Waukesha, Wisconsin, tuviera un nuevo sistema de comunicación para la seguridad pública, ya que el sistema análogo del que habían dependido por años estaba al final de su ciclo de vida útil. Entonces, comenzó el debate entre los condados de Milwaukee y Waukesha para crear un sistema de comunicaciones vanguardista e interoperable que ambos pudieran compartir. Compraron un nuevo sistema de radio P25 basado en IP: el ASTRO 25 simulcast de 800 MHz de Motorola Solutions. El sistema llamado OASIS tiene un solo núcleo compartido con dos subsistemas y puntos de respuesta para seguridad pública (PSAPS) múltiples para 9-1-1.

Los objetivos del nuevo sistema son mejorar la cobertura de radio, proporcionar comunicaciones directas entre usuarios de diferentes agencias y mejorar la confiabilidad, seguridad y capacidad del sistema. La fecha de lanzamiento del sistema fue el 15 de marzo de 2017, cuando las llamadas al 9-1-1 comenzaron a despacharse.¹ “Cuando vimos la coordinación de seguridad pública, realmente nos enfocamos en la idea de que no hay límites”, dijo Gary Bell, director de preparación para emergencias. “El ambiente de IP permite que esto ocurra relativamente con efectividad para que podamos compartir la infraestructura y los activos, así como proporcionar resultados mejores para el personal de respuesta”.

CONDADO DE WAUKESHA, WISCONSIN

- Población: 390 000
- El tercer condado con más población en Wisconsin
- El área metropolitana de Milwaukee se encuentra dentro de sus límites
- Colinda al Este con el Condado de Milwaukee

COMUNICACIONES POR RADIO

Sistema Simulcast ASTRO® 25 de 800MHz

Sistema compartido con el Condado de Milwaukee

Un núcleo compartido y dos subsistemas

Además de proporcionar servicio al departamento de policía y de bomberos/SME, también lo hace para:

- 19 municipalidades
- 13 agencias de país
- 8 socios de ayuda mutua
- Doce centros de despacho de 9-1-1



MOTOROLA SOLUTIONS



SE LOGRÓ LA INTEROPERABILIDAD ENTRE CONDADOS

Anteriormente, existían sistemas de radio aislados que daban servicio a los diversos departamentos en todo el país. Esto ocasionaba problemas cuando diversas agencias y departamentos respondían a los incidentes. Chris Petterson, gerente de los servicios de radio del condado de Waukesha, exalta los beneficios del nuevo sistema de radio por IP: “Ahora todos en el Condado de Waukesha tenemos el 100 % de capacidad para comunicarnos con quien sea en todo el condado. Ahora tenemos una interoperabilidad entre dos condados. Y con la llegada de la ISSI (Interfaz entre RF y Subsistema), podemos interactuar con la Ciudad de Milwaukee, que está cerca, y con el estado de Wisconsin, de hecho. Así que ahora expandimos la interoperabilidad a todos en el condado, en ambos de ellos”.

EL PERSONAL DE PRIMERA RESPUESTA DEPENDE DE LAS RADIOS COMO SU LÍNEA DE VIDA

El propósito del nuevo sistema crítico de radio por IP es servir a las necesidades de los despachadores y el personal de primera respuesta en el campo. Además de garantizar la disponibilidad de la red, el especialista de servicios de radio del Condado de Waukesha, Steven Milner, habló sobre los beneficios de dar servicio a los radios portátiles y móviles para asegurarse de que están optimizados, brindando una línea de vida para el personal de primera respuesta. “Nos aseguramos de que nuestro equipo cumpla con todos los estándares más recientes, que todo el firmware esté actualizado para que no exista nada que pueda afectar a nuestros usuarios en el campo,

(tal como) alguien hackeando el sistema o accediendo a algún radio y reprogramándolo o clonándolo en el sistema. Realmente cuidamos mucho la forma en la que programamos los radios. Utilizamos autenticación de enlaces por capas. Utilizamos administración de radios. Y simplemente nos aseguramos de que todo esté actualizado. Tenemos mucho cuidado en cómo lo hacemos. Mantenemos el sistema muy seguro, tenemos un control fuerte sobre las contraseñas”.

RESILIENCIA - TANTO FÍSICA COMO CIBERNÉTICA

Ya que la fuerza policial y el personal de servicio de bomberos utilizan el sistema, cuando este se diseñó y creó, pensamos mucho en cómo asegurarnos de que fuera resiliente, minimizando los riesgos de seguridad físicos y cibernéticos. Se integró redundancia en el sistema y se tomaron precauciones para asegurarnos de que el equipo central y el sitio físico siempre estén disponibles. Se construyeron las torres de acuerdo con las especificaciones de clase 3 para la infraestructura crítica; cada sitio cuenta con generadores en espera y energía redundante e ininterrumpida. Contamos con medidas contra incendios, alarmas para intrusiones y vigilancia por video en cada sitio. La segunda parte de la resiliencia del sistema es la ciberseguridad, protegerlos contra las ciberamenazas tales como el malware, los botnets, la negación de servicios y cualquier amenaza potencial que pudiera existir en el futuro. Tal como explica Petterson: “Hemos tomado todas las precauciones posibles para protegernos contra los eventos considerablemente estáticos, como los fallos en el suministro energético y las tormentas; las cosas que son más o menos

predecibles. Los ciberataques son algo nuevo, estos evolucionan y son dinámicos. Es muy importante el hecho de que Motorola y los ingenieros que diseñaron este sistema evalúan todo activamente y ponen atención proactiva en las amenazas. El que hagan estos cambios sin nuestra intervención activa es realmente importante”.

LOS CIBERATAQUES SON CADA VEZ MÁS FRECUENTES

Ningún sistema basado en IP es inmune a los ataques externos, incluyendo los sistemas de comunicación críticos basados en IP. De acuerdo con una encuesta que realizó Ponemon en 2017, 98 % de las empresas encuestadas consideran que el malware es la amenaza principal y las irrupciones de ransomware van en aumento, de 13 % en 2016 a 27 % en 2017.² Bell explica las amenazas potenciales para las redes críticas: “Siempre que se levanta un sistema, casi inmediatamente que este ingresa a una red, comienzan los intentos de invasión. Los hackers de sombrero negro están intentando dañar o secuestrar tus datos para recibir Bitcoin o alguna otra divisa digital. Lo que intentamos es hacer más difícil que estas personas con sombreros negros ingresen en nuestro sistema para impactar su funcionalidad”.



85% DE TODOS LOS ATAQUES DIRIGIDOS PUEDEN PREVENIRSE SI SE APLICA UN PARCHES ³

LOS PARCHES SON DE EXTREMA IMPORTANCIA

De acuerdo con la Unidad de Ciberseguridad del Departamento de Seguridad Nacional de los EE. UU.3, puede evitarse hasta 85 % de todos los ataques dirigidos con la aplicación de parches de seguridad. El mantener un sistema parchado con tantos puntos de acceso y sitios de infraestructura como un sistema crítico de radio, multicondado e interoperable ha representado un verdadero reto. De hecho, 80 % de las filtraciones de datos se dan debido a una administración de parches deficiente.⁴

“La actualización y el parchado del software es de vital importancia para cualquier sistema basado en IP”, resalta Bell. Luego nos explica los riesgos potenciales al realizar el parchado internamente. “El sistema regional de radios, OASIS, cuenta con múltiples agencias con varios profesionales de TI que se responsabilizan de hacer dichas actualizaciones. Así que, solo es necesario que una persona tome vacaciones o que alguien no actualice el sistema para que todo quede expuesto a un evento de interrupción. Todo lo que no se toca o, en caso de que se cuente con personas dispares y diferentes que realicen este trabajo, representa realmente 75 % de los intentos en donde dichos vectores vienen a impactar los sistemas. Así que, el tener el servicio adecuado de actualización de software permite que un individuo maneje todas las entradas en nuestro sistema”.

PARCHES DE SEGURIDAD ADMINISTRADOS

Para tratar las amenazas potenciales de ciberseguridad y proporcionar un proceso profesional y consistente para actualizar los parches de seguridad, el Condado de Waukesha eligió utilizar un Servicio de Actualizaciones de Seguridad. Los expertos de Motorola Solutions monitorean las actualizaciones de seguridad para buscar parches de sistema operativo y antivirus conforme se descubren vulnerabilidades y amenazas nuevas. En sus laboratorios de pruebas dedicados, los equipos de expertos prueban y certifican que las actualizaciones son esenciales y críticas y no impactarán las operaciones de las comunicaciones de forma adversa. Cuando todo queda validado y es seguro para los sistemas, el software se actualiza automáticamente. Se proporciona entonces un reporte de estado, para mantener informado al equipo. Los beneficios que obtenemos son simples, explica el especialista de servicios de radio del Condado de Waukesha, Steven Milner. “Para nosotros, la aplicación de parches es transparente. Tenemos un servicio de suscripción en donde ellos (Motorola Solutions) ejecutan el parchado. Realmente no estamos conscientes de nada de lo que pasa en segundo plano. Esto no nos causa problema alguno. Y ellos nos notifican cuando llevarán a cabo el parchado o sobre cualquier cosa que pudiéramos ver; se aseguran de que estemos consciente de esto con antelación”.

Desde un punto de vista administrativo, Bell resaltó por qué eligieron aplicar los parches de seguridad a través de un servicio. “No es algo que deba atribuirle a mi personal para asegurarme de que sean expertos en el tema con respecto a los sistemas, ya que tenemos muchos sistemas. Tal como lo sabemos, una pequeña brecha o apertura de una actualización de los parches puede causar problemas significativos. Así que dependemos de nuestros socios de la industria, en este caso Motorola Solutions, para que sigan su protocolo y realicen estas actualizaciones remotamente en el sistema a través del cortafuegos”.

“La razón por la cual elegimos el SUS (Servicio de Actualizaciones de Seguridad) fue realmente para prevenir los ataques de ransomware. Lo que intentamos es hacer más difícil que estas personas con sombreros negros ingresen en nuestro sistema para afectar su funcionalidad”.

—Gary Bell, Director de Preparación contra Emergencias



EL TRABAJO EN EQUIPO AYUDA A MANEJAR LA COMPLEJIDAD

“El trabajo en equipo en la seguridad del sistema es nuestro enfoque en todas las relaciones con nuestros socios de la industria”. Bell comentó sobre el valor de esto en su organización al saber que todas las actualizaciones, ya sea los parches de Windows® o la protección de McAfee®, se evalúan antes de enviarse al mundo real. Los resultados son exactamente lo que quiere. “Ningún socio en el campo (usuario de radio) ni nadie detrás de unos auriculares y micrófono (operadores del 9-1-1) notan algún impacto”.

Bell continúa: “El tan solo saber que existen individuos ahí afuera que se dedican a vigilar el sistema, que tienen una línea base para lo que es el tráfico normal y que pueden prever cuándo ocurrirán los picos para tomar acción, definitivamente me permiten - como administrador del sistema - relajarme un poco y enfocarme en lo que necesito hacer”.

PAZ MENTAL

Hay algo que nos tranquiliza al saber que estamos haciendo todo lo que podemos para minimizar las vulnerabilidades, protegernos contra los ciberataques y proporcionar el mejor sistema de comunicación para la seguridad pública a los condados de Waukesha y Milwaukee. Como administrador, Bell asienta: “Quiero enfocarme en mi gente en vez de en la tecnología. Así que, el contar con individuos que brindan apoyo detrás de la escena, supervisando el sistema y asegurándose de que ellos (el personal de despacho y de campo) cuenten con las herramientas para realizar sus trabajos, es vital”.

Para obtener más información, visítenos en motorolasolutions.com

1. OASIS Annual Report <http://county.milwaukee.gov/ImageLibrary/Groups/cntyOEM/Gov-Board/2017OASISAnnualReportFINALsigned.pdf>

2. <https://www.motorolasolutions.com/content/dam/msi/docs/services/support-services/cyber-security-professional-services/cyber-resilience-whitepaper.pdf>

3. <https://www.us-cert.gov/ncas/alerts/TA15-119A>

4. <https://dzone.com/articles/80-of-breaches-still-result-of-poor-patch-manageme>



Motorola Solutions, Inc. 500 West Monroe Street, Chicago, IL 60661 U.S.A. 800-367-2346 motorolasolutions.com

MOTOROLA, MOTO, MOTOROLA SOLUTIONS y el logotipo de la M estilizada son marcas comerciales o marcas comerciales registradas de Motorola Trademark Holdings, LLC y son utilizadas bajo licencia. Todas las demás marcas comerciales pertenecen a sus respectivos propietarios. © 2018 Motorola Solutions, Inc. Todos los derechos reservados. 07-2018