SEGURIDAD CIBERNÉTICA MANEJANDO EL RETO Y LA COMPLEJIDAD

PROTEJA SU ACTIVO MÁS IMPORTANTE: LA INFORMACIÓN

Según McAfee®, cada año se desarrollan unos 60.000.000 de programas de malware (software malicioso) a medida que los delincuentes cibernéticos intentan superarse a sí mismos.1 Lo que es peor, el espionaje informático patrocinado por el sector corporativo y el gobierno es un problema que se agrava a nivel internacional, puesto que los hackers utilizan métodos cada vez más sofisticados para evadir las murallas de seguridad. La protección de sus datos es tan importante como la protección de su efectivo, y esto se debe a que cualquier situación que ponga en riesgo sus sistemas de información también implica una amenaza para su empresa.

Es preciso preguntarse qué sucedería si la información confidencial de sus clientes, miembros de organismos, documentos financieros y proyectos clasificados cayeran en las manos equivocadas. En el mejor de los casos, podría perder su ventaja competitiva. Y, en el escenario más pesimista, podría sufrir pérdidas significativas. El hecho que su empresa aparezca en la primera plana a causa de una falla de seguridad no solo dañaría su reputación y calificación crediticia, sino que lo expondría a demandas legales e, incluso, a la bancarrota.

LOS RIESGOS DE SEGURIDAD TIENEN UN COSTO MUY ELEVADO

Los ataques y las irrupciones a sus sistemas de información resultan costosos, ya sea por las pérdidas operacionales que se generan mientras usted se encarga de identificar y rectificar el problema, o por el tiempo y el dinero que debe invertir para recuperar su imagen. Si a eso le suma los estrictos requerimientos de cumplimiento normativo vigentes en prácticamente todas las industrias, que traen aparejadas fuertes multas y penalizaciones, notará que la gestión proactiva de los riesgos puede ahorrarle a su organización innumerables complicaciones y costos.

Con una implementación correcta, la seguridad cibernetica permite gestionar los riesgos de manera proactiva. Protege los activos de información críticos, garantiza la integridad de los datos y resguarda la confidencialidad de la información. Además, brinda a su organización la posibilidad de retener evidencia e iniciar acciones judiciales de manera efectiva.

LA SEGURIDAD CIBERNÉTICA PERMITE IMPLEMENTAR POLÍTICAS, PROCEDIMIENTOS Y MECANISMOS TÉCNICOS PARA PROTEGER, DETECTAR Y CORREGIR PROBLEMAS QUE AMENACEN LA SEGURIDAD DE SU RED.

¿ESTÁ PREPARADO?

¿SABÍA QUE...?

- Pasar de una red analógica antigua a una red digital basada en IP altamente eficiente aumenta la complejidad y presenta nuevos riesgos.
- El uso compartido de información y la interoperabilidad generan aún más vulnerabilidades.
- El cumplimiento normativo y las exigencias reglamentarias evolucionan y suelen estar vinculados con el otorgamiento de financiación.
- Las fallas de seguridad pueden acarrear publicidad negativa, pérdidas financieras e implicaciones políticas.
- Los presupuestos gubernamentales se reducen, mientras que los requerimientos para mejorar la seguridad aumentan.

REDES GUBERNAMENTALES: UN OBJETIVO FRECUENTE DE LOS HACKERS

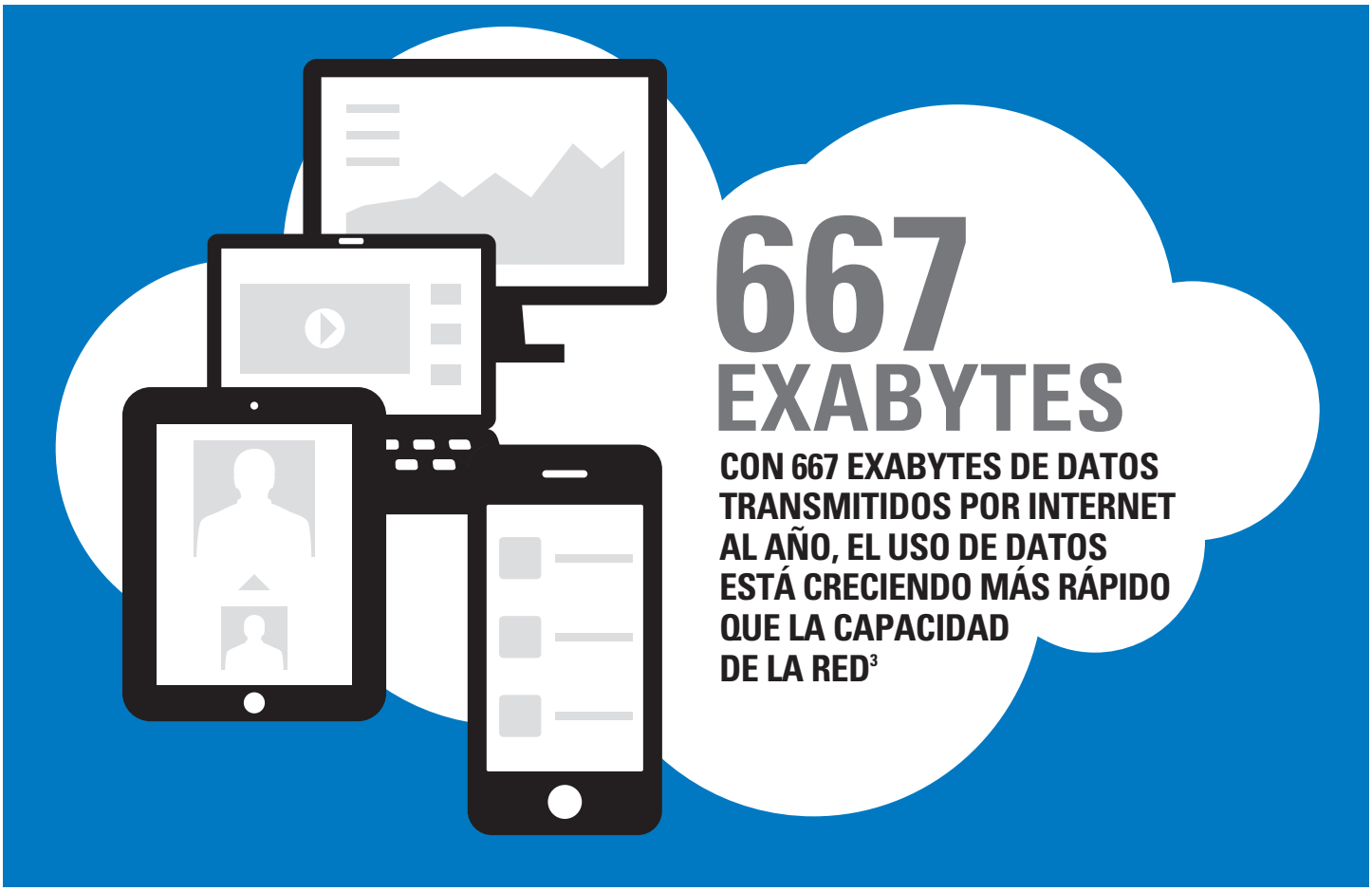
Los hackers apuntan a las redes gubernamentales, pues su objetivo es conseguir propiedad intelectual muy valiosa. Cada vez más, los ataques se originan en países extranjeros. Un gusano nformático altamente especializado, como el virus Stuxnet, es una herramienta sofisticada de ataque cibernético que bloqueó la red completa de una planta nuclear y que ahora se considera una supe rarma.[2]

LA MOVILIDAD IMPLICA UN CAMBIO RADICAL Y UN DESAFÍO PARA TODOS

La potencia informática avanzada y la conectividad en cualquier lugar están, literalmente, al alcance de la mano. Los dispositivos empresariales nos permiten estar conectados con smartphones, sistemas de radios digitales de dos vías y sistemas de administración de activos basados en la ubicación, y esto contribuye a que los trabajadores móviles puedan mantenerse en contacto con la oficina central. Con las cámaras digitales podemos subir imágenes a la nube, con los sistemas de juegos tenemos la posibilidad de competir con jugadores de todo el mundo y con los smartphones encendemos luces y electrodomésticos y aparatos eléctricos de manera remota.

La conectividad en cualquier lugar ha cambiado nuestras expectativas acerca del modo en que accedemos a la información en el trabajo. El trabajo a distancia se está generalizando. Los datos móviles son activos de misión crítica. Twitter y Pinterest están dejando de ser simplemente un medio social para convertirse en herramientas empresariales. El bloqueo centralizado de las redes se ha vuelto imposible. Y el volumen de datos cursados supera la capacidad de la red para administrarlos, con 667 exabytes transmitidos anualmente por Internet hasta el año 2013, según Cisco.[3]

Al mismo tiempo, los empleados llevan sus propios dispositivos al trabajo, una situación que expone las redes empresariales a un nuevo mundo de vulnerabilidades. Las personas han logrado un nivel de conocimiento tecnológico sin precedentes y cada vez dependen más de sus dispositivos móviles. Desafortunadamente, la mayoría desconoce la responsabilidad de proteger los dispositivos y los datos de los que depende su empresa, y esa situación representa un riesgo enorme



EL GASTO DE TI AUMENTA, PERO TAMBIÉN AUMENTAN LAS INTRUSIONES

La mayoría de las organizaciones concentran gran parte de su presupuesto de seguridad en soluciones técnicas. Adquieren el paquete completo (un firewall, un programa antivirus o una herramienta anti-malware), lo instalan en la red y dan por solucionado el problema. Dado que la atención de los gobiernos ahora se centra más en la seguridad de la información, la "adquisición del paquete completo" se ha convertido en la "revisión del paquete completo", a fin de garantizar que todos los sistemas cumplan con las últimas reglamentaciones en materia de seguridad de redes.

¿Cuán eficaz es este enfoque? Si bien el 37% de las organizaciones encuestadas incrementarán el gasto destinado al cumplimiento de la seguridad de la información y a la prevención de pérdida de datos y dispositivos móviles, la cantidad de casos de intrusión continúa en alza.[4] Según Privacy Rights Clearinghouse (Agencia sobre derechos de privacidad), el mayor nivel de filtraciones de datos se registró en 2011, con 535 casos informados que, en total, afectaron a 30,4 millones de registros confidenciales. Lo que es aún más inquietante, la mayoría de los casos fueron generados por personas que pertenecían a la organización.[5]

LA SEGURIDAD ES TAN SÓLIDA COMO SUS USUARIOS

Los malos hábitos de los usuarios pueden superar fácilmente el sistema de seguridad mejor planificado y más avanzado desde el punto de vista tecnológico. ¿Sus empleados comprenden que sincronizar un smartphone en una PC de la oficina o usar una unidad de almacenamiento Thumbdrive para trasladar trabajo del hogar a la oficina pueden exponer su red a los programas de malware? ¿Son conscientes de que la aplicación no autorizada que instalaron en su PC de escritorio o la red punto a punto utilizada para transferir archivos de gran tamaño podrían abrir un acceso indirecto para irrumpir en sus sistemas tan cuidadosamente protegidos? ¿Saben que si se pierde un dispositivo, o es objeto de un robo, esta situación podría poner en riesgo los datos más confidenciales?

Si bien las soluciones técnicas y los controles de cumplimiento normativo son fundamentales, nada se compara con un usuario informado y cuidadoso con los temas de seguridad. Es por eso que implementar procesos adecuados para que sus empleados aprendan las mejores prácticas de seguridad debe ser un tema prioritario. Es preciso que sepan que utilizar un dispositivo en una red sin protección puede dar lugar a una serie de problemas de seguridad.

40% DE AUMENTO
EN ATAQUES CIBERNÉTICOS CONTRA LAS REDES FEDERALES EN UN AÑO[6]

9 HORAS PARA CONFIRMAR UNA FILTRACIÓN[6]

20 HORAS PARA PARA INFORMAR UNA FILTRACIÓN[6]

MUCHAS VECES LA PEOR AMENAZA NO SON ELLOS, SINO NOSOTROS MISMOS

Todas las organizaciones se defienden de "ellos", es decir, de los hackers, los espías y otras entidades maliciosas que intentan flanquear las defensas. Hay un riesgo menos evidente que tiene que ver con los comportamientos riesgosos (abrir archivos adjuntos, hacer clic en enlaces, visitar sitios Web maliciosos) de los empleados pertenecientes a su organización, aunque lo hagan sin ninguna intención perjudicial. Incluso la mejor defensa puede ser evadida por estos empleados cuando no siguen las buenas prácticas de seguridad y, por descuido, dejan el sistema expuesto.

Todos "nosotros", al ser parte de una organización, debemos comprender qué activos de información se almacenan y por qué motivo el acceso a dichos activos debe ser limitado. Todos nosotros debemos confiar en que la información está protegida. Cuanto más crítica sea la misión, más importante será que nuestro territorio esté protegido satisfactoriamente contra todas las amenazas.

EL FUNCIONAMIENTO EN PILOTO AUTOMÁTICO NO ES SEGURO

Confiar en la "adquisición del paquete completo" o en la "revisión del paquete completo" sin la participación de los usuarios es como confiar en un sistema de piloto automático sin la presencia de un piloto real en el avión. La inteligencia artificial no sustituye el sentido común de un usuario experimentado. Si su empresa solo mide el éxito basándose en los resultados de la implementación de controles de cumplimiento normativo y pasa por alto los procedimientos operativos y las políticas gerenciales, está volando a ciegas.

Una solución de seguridad cibernetica exitosa fusiona todos estos aspectos con un cambio en las conductas, en cada nivel de la organización. Este enfoque, denominado Defensa en Profundidad por la Agencia de Seguridad Nacional (NSA), es una estrategia que incluye varios niveles de defensa en todo el ciclo de vida útil del sistema. Tiene en cuenta la tecnología en uso, las operaciones de la organización y el personal que participa en el proceso.

La empresa se beneficia cuando capacita a su personal. Al insistir constantemente con este tema y al brindar capacitación sobre las actuales vulnerabilidades y las mejores estrategias de mitigación de riesgos, usted logra que cada empleado se convierta en un defensor de la seguridad. De ese modo, los usuarios se transforman en una herramienta real para reducir el costo total de propiedad (TCO). Además, este es un primer paso fundamental para intensificar la seguridad.

LOS ATAQUES CIBERNÉTICOS APUNTAN A LOS ORGANISMOS GRANDES Y PEQUEÑOS. MÁS DE 70 ORGANISMOS ENCARGADOS DEL CUMPLIMIENTO DE LA LEY FUERON ATACADOS POR UN INFAME GRUPO INTERNACIONAL DE HACKERS, CONOCIDO COMO ANONYMOUS.[7]

COMPARTIR INFORMACIÓN ES UNA PRÁCTICA RUTINARIA

Muchos de sus empleados nunca han conocido un mundo sin computadoras ni acceso a Internet. Utilizan dispositivos móviles muy potentes y comparten datos a diario en cada ámbito de sus vidas, ya sea mediante álbumes de fotos en línea, blogs y tweets, cronologías en Facebook o aplicaciones GPS en tiempo real.

Cuando los empleados tienen acceso a su intranet o a sus bases de datos, el hecho de compartir información les resulta natural. Si consideran que la seguridad de su empresa es un obstáculo, suelen evadir esos procedimientos, ya sea involuntaria o intencionalmente. La mayoría de los usuarios no comprenden cabalmente los riesgos ni son capaces de anticiparse a las vulnerabilidades. Además, como la seguridad cibernetica a menudo se centra en los equipos de escritorio y en los servidores, pasa por alto la protección de las tecnologías móviles y portátiles, que son las más utilizadas por los empleados.

Los expertos en seguridad deben enfrentar el desafío de mantenerse al día con las crecientes amenazas a los datos digitales, puesto que los hackers explotan las vulnerabilidades de los nuevos productos no bien salen al mercado. El auge de la computación en la nube suma otro nivel de complejidad para las organizaciones, puesto que los usuarios comparten tecnología, confían en proveedores para la seguridad y abren la organización a los ataques maliciosos perpetrados por hackers capaces de recopilar datos confidenciales y de controlar los servicios de la nube.

CUANTO MENOS SABEN, MAYOR ES LA AMENAZA

Puede que sus empleados no tengan del todo claro el tema de la seguridad de la información. También es posible que su organización no haya definido e implementado políticas de manera adecuada, y que, en su lugar, confíe en las medidas de cumplimiento normativo, los mecanismos técnicos o en un equipo de TI encargado de la protección. O bien, puede que la causa sea la falta de comunicación. Muchos sistemas de seguridad no están documentados o son percibidos como mandatos sin fundamentos que los usuarios omiten fácilmente por obstaculizar la productividad o por considerarlos directivas territoriales del sector de TI.

Un marco informal sin procedimientos claramente documentados puede crear la percepción de que el cumplimiento de la seguridad es opcional. La ausencia de un firme respaldo gerencial también puede dar lugar a una actitud informal que favorece la productividad por sobre la protección de datos. Si los encargados de la toma de decisiones no priorizan la seguridad, los usuarios tampoco lo harán. En última instancia, cuanto menos participen los usuarios en las políticas de seguridad, menos responsables se sentirán de su cumplimiento y más riesgos asumirán de manera involuntaria.

LA SEGURIDAD CIBERNETICA ES CRÍTICA ANTE LA CONVERGENCIA DE REDES

Independientemente de que su organismo u organización utilice un sistema de radios de dos vías, el 9-1-1 de próxima generación, un sistema inalámbrico o una red LTE, existen distintos niveles de complejidad asociados con cada tecnología. Como cada nivel representa una oportunidad de que alguien fuerce un control de seguridad y dañe la red, usted necesita distintos niveles de protección para mantener protegida la información confidencial, desde historias clínicas de pacientes hasta datos de seguridad pública.

En un panorama que cambia vertiginosamente y que se caracteriza por una combinación de ataques, como virus, suplantación de identidad (phishing) y robo de identidad, es importante implementar anillos concéntricos de protección. Este enfoque holístico debe tener en cuenta todo el ciclo de vida de la protección de la seguridad: desde la evaluación de la seguridad, la integración y los servicios gestionados, como la supervisión del firewall y la protección contra intrusiones, hasta el desarrollo de políticas.

Un error común que se repite en muchas organizaciones es la falta de planificación. Simplemente no es suficiente implementar un control de seguridad y quedarse tranquilo. Es preciso realizar un mantenimiento y una revisión de los controles con regularidad, en especial porque las amenazas al entorno cambian continuamente. Además, analizar el proceso de seguridad con anticipación es fundamental para planificar su presupuesto.

PREGUNTAS CLAVE QUE DEBE FORMULAR PARA PROTEGER SU RED

- ¿Dispone de un programa de seguridad establecido, con personal y fondos asignados?
- ¿Su organización ha realizado o actualizado su perfil de riesgos de seguridad?
- ¿Cuenta con un programa de gestión de vulnerabilidades?
- ¿Cuenta con un procedimiento de escalamiento de incidentes?
- ¿Sus redes o datos están regulados por leyes estatales o federales?
- ¿Comparte información con otras entidades u organismos?

DEFINA SUS OBJETIVOS DE SEGURIDAD, Y SUS USUARIOS

En lo que concierne a la seguridad cibernetica, es fundamental definir sus objetivos y comunicar su plan claramente. Forme un equipo de usuarios y partes interesadas para explorar los objetivos, las realidades, las opciones y la voluntad de su organización.

En primer lugar, analice si el objetivo se puede medir, lograr y vincular con su misión. Luego averigüe quiénes son los expertos internos y los puntos débiles, y cuál es la mentalidad de los usuarios en cuanto a la seguridad. A continuación, piense en qué desafíos de seguridad se resuelven mejor con mecanismos técnicos, cambios operacionales y concientización de los usuarios, y determine en qué medida el presupuesto repercutirá en dichas alternativas. Por último, identifique actitudes y condiciones que deban cambiarse, recursos requeridos y el valor del soporte externo.

Una vez que su equipo haya definido los objetivos de seguridad cibernetica, documente sus decisiones y comprométase con un proceso continuo de gestión de cambios. Para la capacitación, prepare mensajes personalizados según los diferentes usuarios de la red.

Asegúrese de utilizar las redes sociales de su empresa para generar consenso y respaldo, incluida la gerencia. Aproveche la experiencia de sus especialistas en seguridad internos o recurra a otros especialistas que no pertenezcan a su organización.

PRESENTE SUS POLÍTICAS Y ANALICE LOS POSIBLES RIESGOS

Al reunir a los grupos de usuarios, ofrézcales políticas claras basadas en metas y objetivos bien definidos. Señale claramente los riesgos que cada procedimiento pretende mitigar. Sea franco y específico al describir las posibles consecuencias de no cumplir con las normas de seguridad.

Su personal debe comprender que los riesgos de seguridad provienen de fuentes internas y externas, y de ataques agresivos y vulnerabilidades pasivas. Esta es su oportunidad de inculcarle a su organización cuáles son las amenazas de ingeniería social, como la suplantación de identidad (phishing) y la falsificación. Todos deben retirarse con una clara idea de cómo la conectividad a Internet expone sus sistemas a amenazas, como cookies, código móvil, ataques de denegación de servicio y accesos indirectos para irrumpir en las redes punto a punto.

DEFINA, DOCUMENTE Y DECIDA

La capacitación orientada a la concientización debe ser un proceso continuo en su organización si se pretende lograr un cambio real en el comportamiento de los usuarios. En el caso de los empleados, la documentación es el libro de textos que respalda su aprendizaje y define los procesos técnicos y los procedimientos operacionales de la seguridad cibernetica.

COMO MÍNIMO, LA DOCUMENTACIÓN DEBE ABORDAR LAS SIGUIENTES PREGUNTAS PRINCIPALES

¿QUIÉN DEBE UTILIZAR LOS RECURSOS DE RED?

¿El acceso se extiende a otros organismos, entidades, proveedores externos o clientes? ¿Debería restringirse el acceso a ciertos grupos de personal interno?

¿CUÁL ES EL PROPÓSITO Y EN QUÉ CONSISTE EL PROCESO DE LA AUTENTICACIÓN DE USUARIOS?

¿Cómo se define la calidad de una contraseña y cómo se protege? ¿De qué modo su organización usa redes privadas virtuales (VPN) y otras herramientas de autorización remota?

¿QUÉ EQUIPOS SE PUEDEN CONECTAR A LA RED?

¿De qué modo su red está protegida contra los sistemas "infectados"?

¿CÓMO SE DEBE MANEJAR UNA POSIBLE FALLA DE SEGURIDAD?

¿A quién se le debe notificar el extravío de un smartphone o el robo de un dispositivo? ¿Cuál es el proceso para proteger el acceso a los datos cuando un empleado es despedido?

AL DESCRIBIR CLARAMENTE LOS ROLES Y LAS RESPONSABILIDADES DE SUS EMPLEADOS EN EL PROCESO DE SEGURIDAD DE LA INFORMACIÓN, UNA BUENA DOCUMENTACIÓN CONTRIBUYE A REDUCIR LA CONFUSIÓN Y MEJORAR LA PRODUCTIVIDAD. ASIMISMO, SIRVE COMO NOTIFICACIÓN DE QUE LA SEGURIDAD CIBERNETICA ES UNA PRIORIDAD PARA SU ORGANIZACIÓN, UN TEMA RESPALDADO POR EL ESCALÓN MÁS ALTO Y RESPETADO EN CADA NIVEL.

PREPARE A SUS EMPLEADOS PARA LA DEFENSA

La concientización de los usuarios es una importante arma defensiva en su arsenal de seguridad cibernetica. A medida que su personal logre una comprensión más cabal de los riesgos y el costo que implican las prácticas deficientes de seguridad, podrá reforzar su función en la protección de su organización. Los usuarios más informados pueden ser aliados en el tema de la seguridad, puesto que aceptarán los controles y los aplicarán con mayor uniformidad.
Al compartir la responsabilidad de proteger los activos de información críticos, sus empleados son más valiosos, ya que minimizan el riesgo, reducen el nivel de exposición y disminuyen los costos en toda la empresa.

MENTALIDAD LOCAL CON INICIATIVAS INTEGRALES

Los ataques de seguridad son cada vez más imperceptibles, y suelen estar dirigidos a un objetivo específico, motivados por temas financieros. En la actualidad, los ataques polimórficos, capaces de modificarse automáticamente con cada ejecución, están presentes en todos lados. Si bien a la mayoría de las organizaciones les gustaría creer que sus datos más confidenciales y su información de misión crítica están inmunizados, esto no es así. Las amenazas son cada vez más complejas y frecuentes, y el hecho de invertir en tecnología, respetar las normas de cumplimiento o instalar una defensa tradicional en el perímetro no es una solución que garantice la seguridad.

A medida que las redes convergen y las personas trabajan en colaboración y comparten datos en todo el mundo, las soluciones de seguridad cibernética deben cubrir todos los frentes relacionados con las personas, las políticas, los procesos y los aspectos tecnológicos de forma integral: desde evaluaciones de seguridad de defensa en profundidad hasta procedimientos para cumplir con los requerimientos normativos.

Sin duda alguna, la planificación adecuada es el componente clave de un enfoque holístico. Mediante la detección y el control de las amenazas desde un principio y la implementación de nuevos controles como consecuencia de lecciones aprendidas en ataques previos, su organización puede adoptar una estrategia productiva a largo plazo.

AÍSLE SU RED Y BENEFÍCIESE

Ya sea que usted comparte datos de seguridad pública o información clínica de pacientes, utiliza una red de radios de dos vías o la última red LTE, al diseñar una infraestructura segura y aislar sus redes con anillos concéntricos de protección, su empresa obtiene los siguientes beneficios:

- Aumenta la confiabilidad y mejora el cumplimiento normativo de la red.
- Elimina las vulnerabilidades y los costos de tiempo de inactividad.
- Mejora el desempeño de sus sistemas empresariales críticos.
- Garantiza la continuidad de sus operaciones y la conectividad con el mercado.
- Cumple su misión y, en última instancia, ayuda a su organización a prosperar.

LAS SOLUCIONES DE SEGURIDAD CIBERNÉTICA DEBEN CUBRIR TODOS LOS FRENTES RELACIONADOS CON LAS PERSONAS, LA TECNOLOGÍA, LAS POLÍTICAS Y LOS PROCESOS DE FORMA INTEGRAL

FUENTES

1. Informe de McAfee sobre amenazas: Primer trimestre de 2012
2. "Public safety can benefit when hackers go bad", Urgent Communications, 17 de agosto de 2011
3. "Data, data everywhere", The Economist, 25 de febrero de 2010
4. www.eweek.com/c/a/Security/Study-Most-Technology-Companies-Have-Data-Losses
5. www.privacyrights.org/top-data-breach-list-2011
6. www.nextgov.com/technology-news/2011/03
7. "Hacker switches sides to help public safety stave off hack attacks", The Fire Chief, 10 de agosto de 2011

Para saber cómo gestionar la complejidad, visite **motorolasolutions.com/services/government**

Motorola Solutions, Inc. 1301 E. Algonquin Road, Schaumburg, Illinois 60196 EE.UU. **motorolasolutions.com**

MOTOROLA