Defensa contra el ransomware en 5 pasos

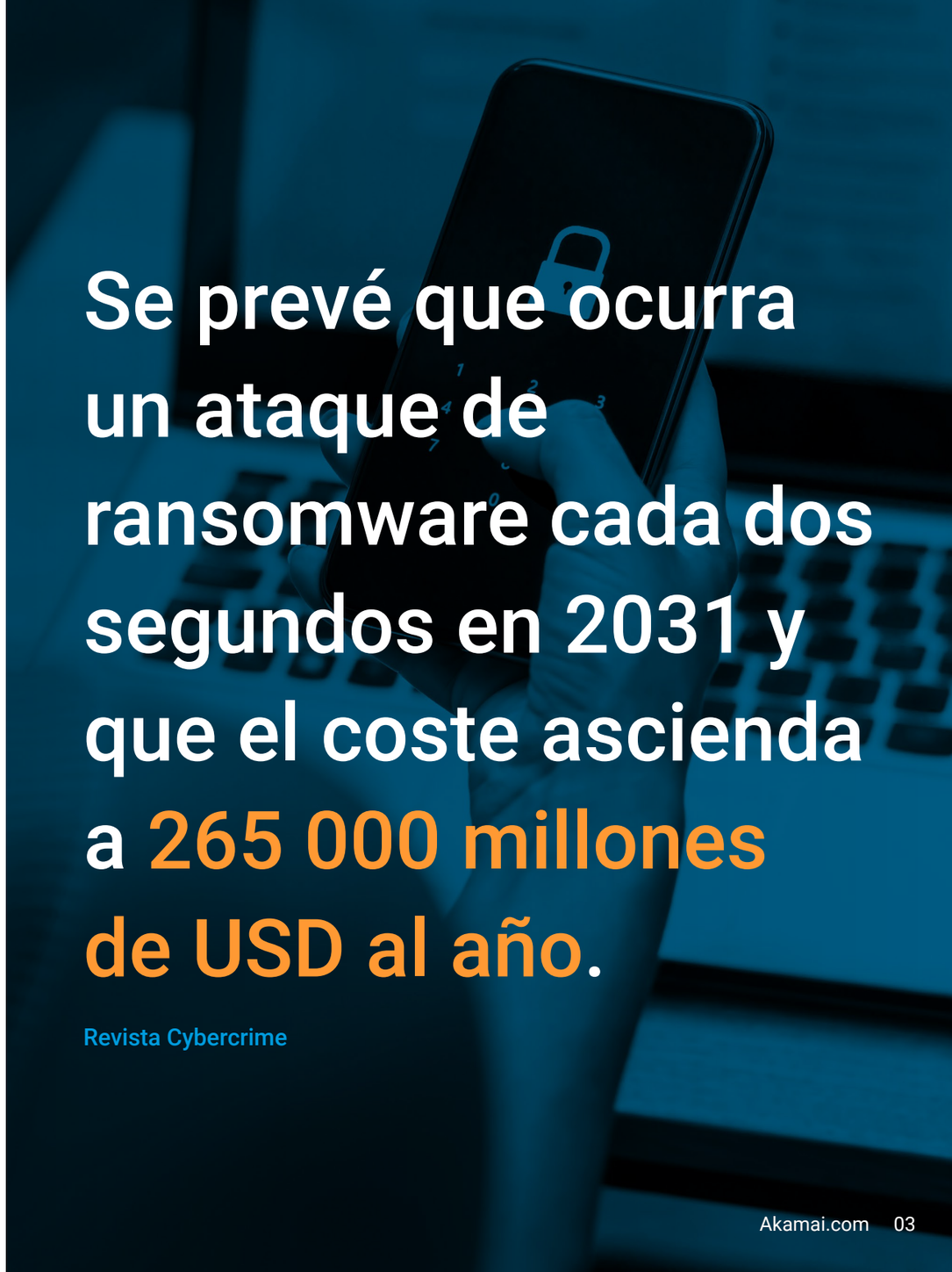
Cómo reforzar sus defensas más allá del perímetro

TABLA DE CONTENIDO

Introducción

El auge y la propagación del ransomware

El ransomware, que en su día simplemente era una molesta cepa de malware que utilizaban los agentes maliciosos para restringir el acceso a archivos y datos a través del cifrado, se ha convertido en un método de ataque de proporciones épicas. Aunque la amenaza de perder datos de forma permanente ya es de por sí estremecedora, los ciberdelincuentes y los hackers de estado se han vuelto lo suficientemente sofisticados como para utilizar el ransomware para introducirse en grandes empresas, administraciones estatales y locales, infraestructuras globales u organizaciones de salud pública y paralizarlas. Muchos de estos grupos incluso ofrecen sus servicios como ransomware como servicio (RaaS).



Se prevé que ocurra un ataque de ransomware cada dos segundos en 2031 y que el coste ascienda a 265 000 millones de USD al año.

Revista Cybercrime

El negocio del ransomware le saldrá caro

En 2022, un ataque de ransomware obligó a 7-Eleven a cerrar 175 tiendas, ya que no podían utilizar sus cajas registradoras ni aceptar pagos. A principios de ese mismo año, un ataque de ransomware con un malware llamado BlackCat contra una empresa petrolera alemana afectó a 233 gasolineras y Royal Dutch Shell tuvo que redirigir sus envíos a diferentes almacenes de suministro debido a esta incidencia. El ataque a Colonial Pipeline ocurrió en mayo de 2021, interrumpiendo el suministro de petróleo y gas a lo largo de toda la costa este de EE. UU. En 2020, el ataque de ransomware Snake paralizó las operaciones globales de Honda.

En la actualidad, la combinación de tecnología obsoleta, estrategias de defensa "suficientemente buenas" centradas solo en los perímetros y los terminales, la falta de formación (y los protocolos de seguridad deficientes) y la ausencia de una solución mágica e infalible pone en riesgo a organizaciones de todos los tamaños. Además, los ciberdelincuentes han visto una oportunidad de negocio en estos ataques y tratan de cifrar la mayor extensión de red corporativa posible para luego pedir rescates que pueden costar desde miles a millones de dólares.

Pero el aspecto económico no es lo único que está en juego. Las consecuencias de un ataque de ransomware pueden ser muy perjudiciales: el tiempo de inactividad puede detener las operaciones comerciales, interrumpir la productividad y poner en riesgo sus datos.

Una vez que los datos confidenciales de una empresa se filtran o están en peligro, es muy probable que la imagen de la marca sufra daños y que la fidelidad de los clientes se vea afectada. Según una encuesta de 2020, el 80 % de las filtraciones de datos afectaron a información de identificación personal (PII) de los clientes, el 32 % puso en peligro la propiedad intelectual y el 24 % comprometió datos anónimos de clientes. Además, los agentes maliciosos pueden utilizar estos datos confidenciales para perjudicar a su negocio o llevar a cabo otros actos delictivos, incluida la venta de tales datos.

Dada la amenaza que presenta la rápida propagación del ransomware a través de las redes, proteger exclusivamente el perímetro no es suficiente.

Akamai

¿Sabía que...?

El coste medio de un ataque de ransomware en 2022, sin incluir el coste del rescate en sí, fue de 4,54 millones de USD.

IBM Security

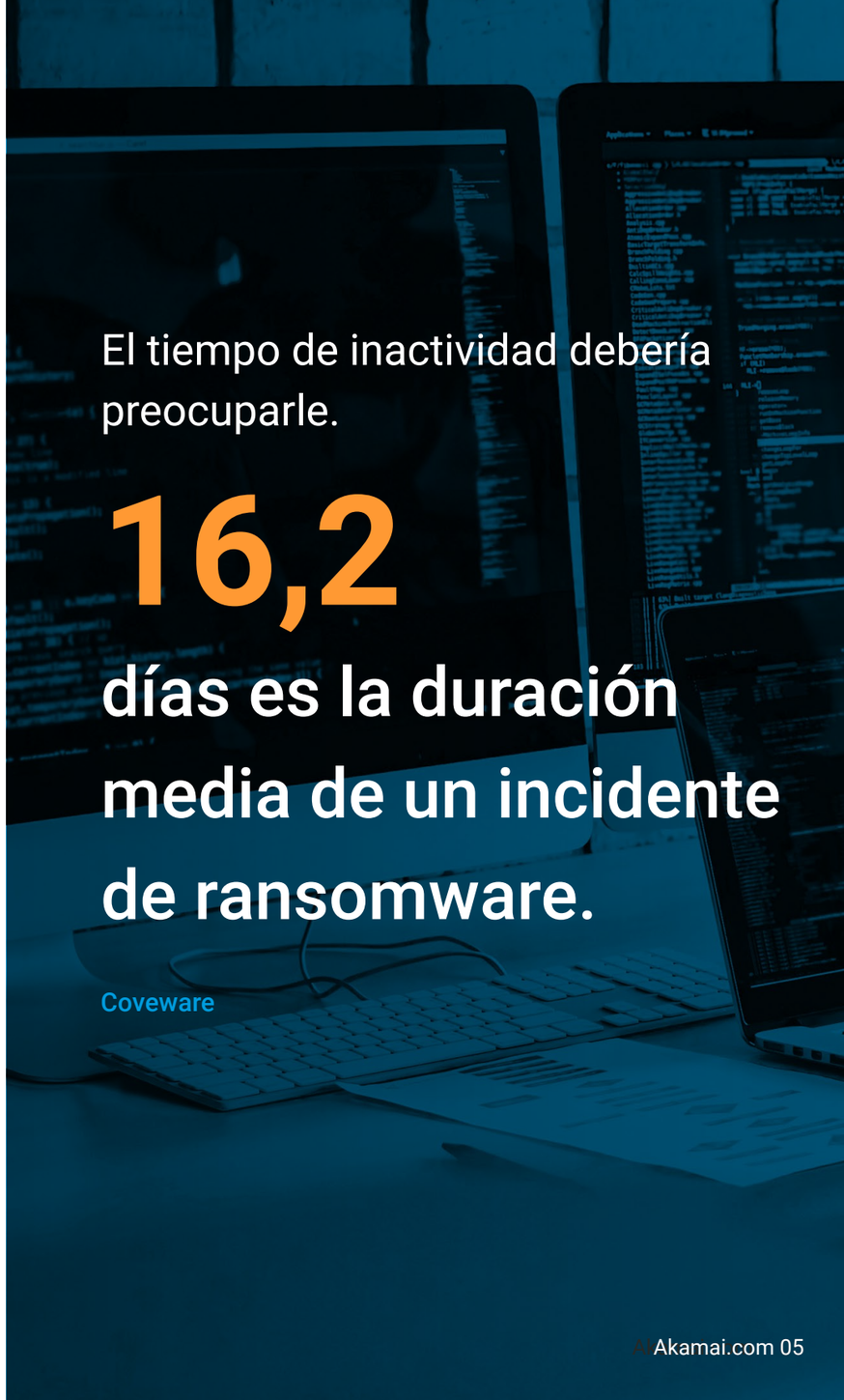
Detenga el movimiento lateral. Detenga la propagación del ransomware.

Un ataque de ransomware comienza con una filtración inicial. A menudo, esta se produce a través de un correo electrónico de phishing, una vulnerabilidad en el perímetro de la red o ataques de fuerza bruta que abren fisuras en las defensas y distraen de la intención real del atacante.

Una vez que el malware ha conseguido acceder a un dispositivo o aplicación, avanza mediante movimientos laterales a través de la red y por diferentes terminales para extender la infección y multiplicar los puntos de cifrado. Por lo general, los ciberdelincuentes se hacen con el control de un controlador de dominio, obtienen las credenciales y, a continuación, buscan y cifran la copia de seguridad para impedir que el operador pueda restaurar los servicios congelados.

El movimiento lateral es fundamental para el éxito de un ataque. Si el malware no se puede propagar más allá del punto de entrada inicial, no es útil. Por lo tanto, evitar el movimiento lateral es clave.

¿Hasta qué punto es completa su estrategia de mitigación de amenazas de ransomware?



Mitigación de riesgos

Creación de una estrategia de defensa blindada

La detección y prevención del movimiento lateral dentro de la red se reduce principalmente a dos áreas clave: en primer lugar, **reducir el vector del ataque inicial** y, en segundo lugar, **limitar las rutas de propagación**.

Para ello, puede tomar medidas como limitar la cantidad de servidores que están expuestos a Internet, estar al día con la gestión de parches para reducir la superficie de ataque, establecer delimitaciones para reducir las rutas de propagación entre aplicaciones y hacer una copia de seguridad de los datos para que pueda volver a conectarse rápidamente y evitar la pérdida generalizada de datos, en caso de que ocurra un ataque.

Cuatro maneras de dar prioridad a la planificación de seguridad

La seguridad debe formar parte del presupuesto, la planificación y la estrategia general de preparación de su empresa. Esto significa concienciar a los principales ejecutivos y a los miembros de la Junta Directiva sobre la importancia de permanecer alerta ante los posibles riesgos y las herramientas necesarias para mitigarlos.

1. Asegúrese de incluir la ciberseguridad en la función que gestiona la mitigación de riesgos a nivel general en su organización. Incluya perfiles con experiencia en seguridad en su equipo de dirección.
2. No olvide dedicar parte del presupuesto y conceder recursos a la generación de copias de seguridad y la segmentación de red.
3. Cree planes de respuesta antes de que se produzca un desastre o un evento adverso (como un ataque de ransomware). Estar organizado y preparado le permitirá reaccionar más rápido y de manera más eficiente.
4. Analice el impacto en la seguridad cada vez que integre, diseñe o desarrolle nuevos productos y servicios. Pregúntese: ¿estoy abriendo una nueva puerta para los atacantes?

Lista de verificación para la detección del ransomware

¿Qué sucede en su red?

Como ocurre en otras muchas organizaciones, la detección del ransomware puede ser un desafío. Por desgracia, esto significa que su red es vulnerable a ataques. Si no cuenta con capacidades de detección sólidas, cuando reciba una notificación de rescate, ya será demasiado tarde: la mayor parte de su red estará cifrada.

Cuando hablamos de detección, debe capturar al ransomware mientras este se propaga. Para conseguirlo, necesitará lo siguiente:

Buena visibilidad

Si no sabe lo que está sucediendo en su red, no podrá detectar el ransomware u otras ciberamenazas.

Políticas de segmentación

Una vez que se definen y se justifican todas las comunicaciones, cualquier elemento fuera de lo habitual se detecta rápidamente y le permite recibir alertas.

Sistemas de detección de intrusos (IDS) y herramientas de detección de malware

Detectarán los intentos de propagación de los operadores de ransomware. Para ello, utilizarán reglas y firmas predefinidas para vulnerabilidades o ataques conocidos o una detección de anomalías más general o automatizada.

Herramientas de engaño

Establecer trampas, señuelos o una plataforma de engaño distribuida capaz de identificar movimientos laterales no autorizados puede ser una manera eficaz de descubrir una filtración activa en curso con incidentes de alta fidelidad.

Creación de una estrategia de defensa contra el ransomware

A pesar de contar con las mejores defensas en el perímetro, las filtraciones son inevitables. Por este motivo, debe contar con una estrategia de defensa que minimice la eficacia de un ataque y detenga la propagación dentro de su red. Busque un proveedor que ofrezca una solución de seguridad integral que sea capaz de detectar amenazas en el tráfico este-oeste del centro de datos y bloquear el movimiento lateral.

Preparación

Busque una solución con la que pueda identificar todos los activos y las aplicaciones que se ejecutan en su entorno de TI. Este nivel de precisión en la visibilidad le permitirá asignar con rapidez activos esenciales, datos y copias de seguridad, e identificar vulnerabilidades y riesgos. Al contar con una visión completa de su entorno de red, podrá responder y activar reglas rápidamente durante una filtración.

Prevención

La solución que elija debería permitirle crear reglas para bloquear las técnicas comunes de propagación del ransomware. Mediante la segmentación definida por software, puede crear microperímetros Zero Trust en torno a aplicaciones esenciales, copias de seguridad, servidores de archivos y bases de datos. También puede crear políticas de segmentación que restrinjan el tráfico entre usuarios, aplicaciones y dispositivos y, en última instancia, bloquear los intentos de movimiento lateral.

Detección

Implemente una solución que le alerte sobre cualquier intento de obtener acceso a las aplicaciones segmentadas y las copias de seguridad. Los intentos de acceso bloqueados son indicadores de que hay movimiento lateral. Asimismo, le recomendamos incorporar la detección basada en la reputación, que alerta de la presencia de dominios y procesos maliciosos conocidos. Si detecta con rapidez los ataques que han logrado traspasar el perímetro, puede minimizar el tiempo de permanencia y atrapar a los atacantes antes de que se muevan del punto de entrada inicial.

Solución

La activación automática de medidas de cuarentena y contención de amenazas cuando se detecta un ataque es fundamental. Aplique reglas de aislamiento que permitan la desconexión rápida de las áreas afectadas de la red, al tiempo que las políticas de segmentación bloquean el acceso a las aplicaciones esenciales y a las copias de seguridad del sistema.

Recuperación

Por último, necesita capacidades de visualización que sean compatibles con estrategias de recuperación por fases en las que la conectividad se restaura gradualmente una vez que se ha comprobado que no hay ningún problema en las diferentes áreas de la red.

Conclusión

¿Confía en su estrategia de defensa actual?

El ransomware no va a desaparecer. De hecho, el ransomware afectó al 66 % de las organizaciones en 2021, lo que supone un aumento del 78 % con respecto a 2020, y la cifra no parece disminuir. Estos datos indican que el mundo seguirá experimentando con más frecuencia ataques más ambiciosos, con objetivos más valiosos y con un rescate más alto, que tendrán graves consecuencias para su negocio. Ahora más que nunca, necesita estrategias avanzadas de planificación y mitigación de riesgos cuyo enfoque vaya más allá del perímetro.