arcserve®

No seas parte de la estadística:

Anticípate A Los Atacantes Cibernéticos Con Una Estrategia Holística De Protección Contra El Ransomware

En los entornos empresariales de hoy, todo el día conectados y obsesionados por los datos, las amenazas cibernéticas son la prioridad de los equipos de seguridad de TI.

El ransomware, en particular, es la causa de muchas noches en vela. La frecuencia de los ataques está subiendo, y las últimas cepas y tácticas son cada vez más personalizadas, destructivas y difíciles de detectar con rapidez.

Por ejemplo, desde 2019, hubo al menos 440 ataques de ransomware dirigidos contra sectores de infraestructura crítica, como salud, servicios financieros, gobierno y educación. En 2020, el COVID-19 dio lugar a una tendencia de ataques de ransomware y fraudes por suplantación de identidad (phishing) relacionados con la pandemia, dirigidos a empleados distraídos que buscaban respuestas y garantías durante una época de grandes incertidumbres.

El ransomware continúa evolucionando con nuevas tácticas y tecnologías que surgen constantemente, por ejemplo:

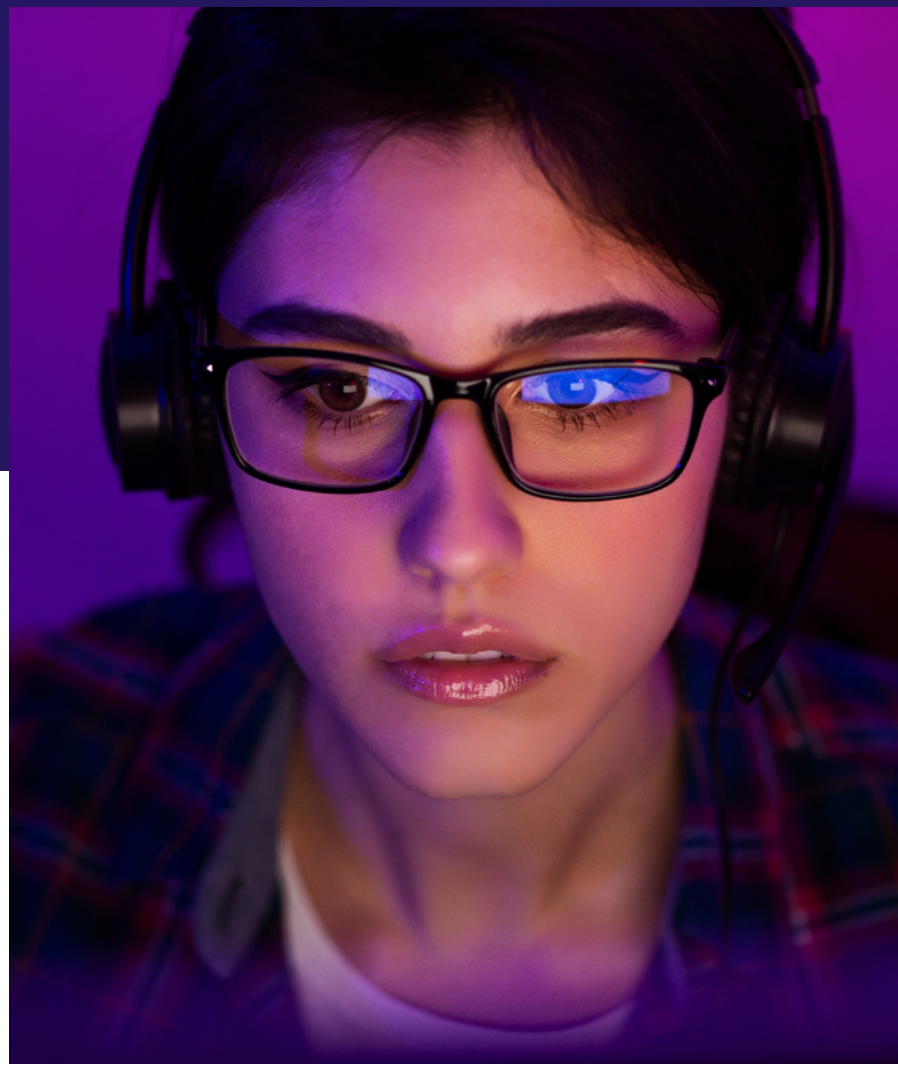
Doble extorsión
Los operadores de ransomware no solo cifran tus datos, sino que también los publican en Internet.

Cifrado diferido
El ransomware permanece inactivo durante un período de tiempo antes de cifrar los datos con el fin de actuar cuando estén listas las copias de seguridad.

Ataques sobre copias de seguridad
Algunas cepas de ransomware buscan archivos de respaldo y los encriptan, lo que hace que la recuperación de desastres se vuelva una pesadilla.

Cómo los entornos de TI actuales posibilitan los ataques de ransomware

La naturaleza y el diseño de los entornos modernos de TI crearon un ecosistema con muchas partes en movimiento y sistemas dispares.



Esta falta de conexión invariablemente amplía la superficie de ataque de una organización y hace que sea más difícil defenderse contra ataques de ransomware. Algunas de las vulnerabilidades más explotadas surgen de un grupo de fuentes comunes.

Altos niveles de complejidad

Las infraestructuras de TI de hoy son altamente complejas. Muchas organizaciones tienen problemas para respaldar y proteger su amplia gama de plataformas y aplicaciones. Es común que los equipos de TI tengan que hacer malabares para manejar una gran variedad de elementos de infraestructura, tales como::

- Infraestructuras locales y de nube pública, privada o híbrida
- Dispositivos y computación móvil
- Soluciones como software como servicio (SaaS), plataforma como servicio (PaaS), e infraestructura como servicio (IaaS)
- Y mucho más

Riesgo de proveedores externos

A la hora de asociarse con un tercero, es esencial confirmar que se toma la seguridad cibernética con la misma seriedad que tu empresa. Cualquier acceso, red y base de datos que compartan puede ser un punto débil que los operadores de ransomware pueden aprovechar. Por eso, es fundamental tener procesos sólidos de diligencia debida y evaluación de seguridad.

Equipos distribuidos

El COVID-19 convirtió a casi todos los equipos en equipos distribuidos. No obstante, el poco tiempo que tuvieron para prepararse para la transición hizo que las organizaciones se acomoden apresuradamente a una infraestructura de soporte y seguridad “lo suficientemente buena”. En muchos casos, “lo suficientemente buena” no era en verdad tan buena. Por eso, los trabajadores remotos se convirtieron en víctimas populares para los delincuentes cibernéticos.

Falta de parches y actualizaciones

Los parches y las actualizaciones de seguridad son tediosas y consumen mucho tiempo. También son dos de las mejores formas de evitar los ataques de ransomware. Los estudios muestran que una de cada tres violaciones de seguridad podría haberse evitado con parches actualizados. En realidad, se lanza al mercado un caudal infinito de parches, y muchos equipos de TI no llegan a dar abasto para seguirles el ritmo.

Sistemas heredados

Los sistemas y el software heredados son una invitación abierta para los operadores de ransomware. Los sistemas más antiguos no se integran adecuadamente con las soluciones más nuevas de seguridad cibernética, lo que significa que no cuentan con el nivel de seguridad suficiente.

El COVID-19 convirtió a casi todos los equipos en equipos distribuidos. No obstante, el poco tiempo que tuvieron para prepararse para la transición hizo que las organizaciones se acomoden apresuradamente a una infraestructura de soporte y seguridad “lo suficientemente buena”.

Suma de costos directos e indirectos del ransomware

El daño de un ataque exitoso de ransomware puede variar considerablemente según el tipo de organización, la industria, el nivel de riesgo y la gravedad del ataque. Sin embargo, todas las empresas necesitan tener presente una verdad universal: el daño del ransomware va mucho más allá del daño del ataque inicial.

Existen varios impactos de un ataque de ransomware que resultan más obvios e inmediatos, como:

- Tiempos de inactividad y pérdida de productividad por el cifrado de los datos
- Pérdida de ganancias como resultado de esta inactividad
- Pérdida potencial de datos si las copias de seguridad no están completas o seguras
- Costos directos de los esfuerzos de limpieza y los pagos de rescate (si decides tomar esa decisión, que nosotros no recomendamos)

Sin embargo, existen otros impactos a largo plazo mucho menos tangibles, pero igual de dañinos. Por ejemplo, es difícil cuantificar el daño a la reputación. Las violaciones de seguridad afectan la confianza de los clientes y de los accionistas de la empresa. Pueden generar una reducción en la cantidad de clientes nuevos y actuales que eligen otros proveedores de soluciones, o una pérdida de ventaja competitiva en el mercado.

Según el sector en el que se desarrolla tu empresa, y la gravedad del ataque, tu organización puede verse envuelta en problemas de cumplimiento y regulatorios, o afectada por un procedimiento legal por resarcimientos con posibles multas y penas considerables.

Las violaciones de seguridad afectan la confianza de los clientes y de los accionistas de la empresa. Pueden generar una reducción en la cantidad de clientes nuevos y actuales que eligen otros proveedores de soluciones, o una pérdida de ventaja competitiva en el mercado.

Estrategia holística de protección contra el ransomware

Ante los nuevos tipos de amenaza de ransomware, muchas organizaciones notan que sus antiguas estrategias de seguridad y mitigación ya no son adecuadas. A partir de esto, los equipos de seguridad de TI empezaron a adoptar soluciones holísticas y proactivas para prevenir los ataques de ransomware.

Una estrategia holística de protección contra el ransomware es como aplicar un campo de fuerza a tu organización. Incorpora una estrategia de seguridad integral que bloquea el acceso y minimiza el daño a tu infraestructura de TI con medidas tanto defensivas como ofensivas.

Una protección completa contra el ransomware incluye una combinación de:

- **Tecnologías y herramientas de seguridad cibernética**
- **Capacidades de recuperación orquestadas**
- **Planes viables para administrar empleados, políticas y procesos**

Tecnologías y herramientas de seguridad cibernética

La protección de datos críticos para el negocio y de infraestructuras de múltiples generaciones es un objetivo primario de los equipos de seguridad de TI. Como parte de una estrategia holística de protección contra el ransomware, la seguridad cibernética incluye todo, desde la protección de endpoints y firewalls, hasta la administración de identidades y accesos y la prevención de la pérdida de datos.

Para poder enfrentar los desafíos actuales de ransomware, tu solución de seguridad cibernética debe incluir tecnología de detección y prevención, como por ejemplo:

- Detección de malware basada en firmas y sin firmas
- Una red neuronal de deep learning
- Tecnología contra exploits, como Sophos Intercept X Advanced

Capacidades de recuperación orquestadas

En un mundo ideal, el 100% de los ataques de ransomware se evitarían el 100% de las veces. En realidad, existe una posibilidad bastante importante de que tu organización se vea afectada en algún momento. Una rápida recuperación luego de una crisis depende de tu nivel de preparación y orquestación. Ambos puntos deben ser incluidos en tu estrategia holística de protección.

Las organizaciones altamente resilientes tienen un plan de recuperación de desastres (DR) probado y listo para su implementación mucho antes de necesitarlo. Uno de los componentes principales de un plan sólido de DR es un proceso de backup seguro, completo y actualizado. Pero por sí solo no es suficiente.

Tu plan de recuperación debe incluir, sin falta, backup en la nube, pero también protección contra las nuevas cepas de ransomware que atacan los archivos de copias de seguridad. La estrategia tradicional de backup 3-2-1 ya no es suficiente. Para garantizar capacidades integrales de recuperación, ahora es necesario incluir copias de seguridad aisladas, es decir, un plan de backup 3-2-1-1.

Dado que cada vez más organizaciones están trabajando con empleados remotos que usan soluciones basadas en la nube como Microsoft Office 365, es fundamental contar con un plan implementado para proteger tus aplicaciones de SaaS ante posibles pérdidas de datos. Muchas soluciones de SaaS utilizan un modelo de responsabilidad compartida, es decir, si no realizas un backup de tus datos, es tu problema.

Acciones para empleados, políticas y procesos

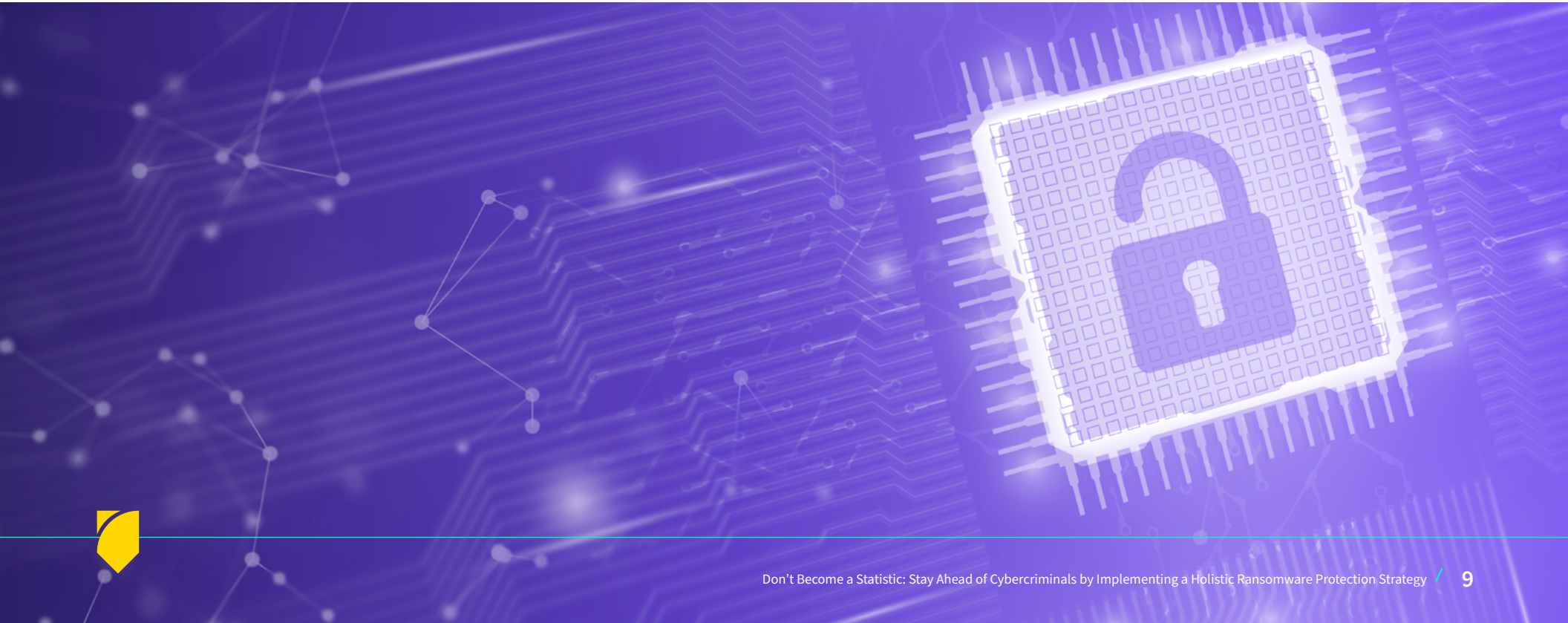
Las personas suelen ser el punto más débil en la cadena de protección contra el ransomware. ¿Qué pasaría si pudieras hacer que todos tus empleados sean una extensión del área de TI para así convertirse en tu primera línea de defensa?

La capacitación es el primer paso para mitigar el error humano. Algunas de las áreas clave en que concentrarse incluyen:

- Simulacros de recuperación de desastres con datos
- Capacitación sobre seguridad cibernética, para que los empleados sepan a qué amenazas estar atentos
- Capacitación sobre concientización de seguridad, que les enseñe qué hacer (o qué no hacer) para evitar violaciones de seguridad e infecciones con malware

Otra forma de minimizar el aspecto de error humano en las amenazas de ransomware es implementar políticas de acceso seguro, como la autenticación de factores múltiples, y de diligencia debida, como controles de antecedentes de empleados, evaluaciones de riesgos de terceros y una seguridad física tradicional bien implementada.

> **Las personas suelen ser el punto más débil en la cadena de protección contra el ransomware.**



Un futuro libre de ransomware con el socio adecuado

Una vez que tengas todo listo para implementar una estrategia holística de protección contra el ransomware, es importante asociarte con un proveedor de soluciones que tenga experiencia y conocimiento trabajando en la prevención de ransomware.

Además de la experiencia, necesitarás alguien que comparta los valores de tu empresa y entienda tu negocio.

Si tu socio y tu empresa hablan el mismo idioma y comparten metas, es mucho más fácil trabajar en equipo para alcanzar los mismos objetivos. Un proveedor de soluciones adecuado puede ayudarte a implementar una estratégia holística contra ransomware al establecer los componentes clave de un plan de seguridad de datos y sistemas completamente sólido.

Si tu socio y tu empresa hablan el mismo idioma y comparten metas, es mucho más fácil trabajar en equipo para alcanzar los mismos objetivos.

Integración y seguridad

La única forma de lograr una protección total contra el ransomware es mediante la integración de la protección de datos con la seguridad cibernética. Cuando tu estrategia de protección contra ransomware incluye las fuerzas combinadas de soluciones como Sophos Intercept X , y Nutanix HCI y Arcserve Unified Data Protection, puedes:

- Reducir la complejidad de la infraestructura
- Mejorar los acuerdos de nivel de servicio (SLA)
- Integrar perfectamente la seguridad cibernética y la protección de datos en todas las cargas de trabajo on-premise, de nube, de infraestructuras hiperconvergentes (HCI) y de SaaS

Backup y recuperación

Es imposible enfatizar demasiado sobre lo importante que es contar con un backup seguro, probado y actualizado para poder realizar una recuperación exitosa luego de un ataque de ransomware o de una interrupción no planificada. El socio correcto puede ayudar a tu organización a encontrar las soluciones de backup y recuperación adecuadas según tus necesidades actuales de protección y almacenamiento de datos (capaces de escalar, de ser necesario, para blindar tu estrategia de seguridad para el futuro).

Protección de datos por suscripción

Es importante encontrar un socio que tenga en cuenta los objetivos de tu organización como factor principal de cualquier transacción. Esto es particularmente cierto a la hora de realizar un presupuesto para una solución de protección contra el ransomware.

Cuando te asocias con un proveedor de soluciones que ofrece licencias universales, tienes la tranquilidad de que todos tus datos están protegidos y además sabes qué estás pagando exactamente. Sin costos ocultos, solo pagas por lo que necesitas, para escalar verticalmente según tus necesidades.

Defiéndete, evoluciona y adáptate

Tanto el ransomware como las otras amenazas cibernéticas llegaron para quedarse. Nuestra única opción es aprender a defender nuestros sistemas, aplicaciones y datos.

Estas amenazas están en constante evolución y adaptación, por lo que nuestras estrategias de seguridad también deben evolucionar y adaptarse constantemente.

Una seguridad completa de los datos comienza con un enfoque administrado para proteger las infraestructuras de TI y los datos de respaldo frente a los ataques cibernéticos, pero esto no es todo.

El camino hacia un futuro libre de ransomware debe incorporar tecnología de seguridad cibernética, procesos orquestados de backup y recuperación, y políticas, procesos y capacitaciones integrales que permitan cubrir el aspecto humano de la prevención contra el ransomware. Los equipos de seguridad de TI deben hacer frente a las amenazas de ransomware de manera proactiva y continua, a través de una estrategia holística de protección que evolucione a medida que lo hagan las amenazas.

El camino hacia un futuro libre de ransomware debe incorporar tecnología de seguridad cibernética, procesos orquestados de backup y recuperación, y políticas, procesos y capacitaciones integrales que permitan cubrir el aspecto humano de la prevención contra el ransomware.