EUROPEAN
RENTAL
ASSOCIATION

RESUMEN EJECUTIVO
Guía de ERA a las mejores prácticas en ciberseguridad para la industria de alquiler de equipos

Ciberseguridad: ¿estás preparado para el reto?

Una de las mayores amenazas para la industria del alquiler de equipos es la vulnerabilidad al impacto de la ciberseguridad en nuestros negocios. En 2021, no existe una hoja de ruta establecida en nuestro sector, en la que una empresa de alquiler de equipos pueda evaluar en qué punto se encuentra en relación con la ciberseguridad e identificar las prácticas líderes a las que puede aspirar. El propósito de esta Guía es definir el alcance de las intervenciones de ciberseguridad en toda la empresa, identificar los elementos centrales de una estrategia de éxito, incluso los factores especiales que pueden afectar a las empresas de alquiler, y repasar las prácticas líderes que adoptan hoy los líderes de nuestra industria. Esta Guía se ha elaborado con el apoyo y los aportes inestimables de las empresas miembros de ERA.

La amenaza de la ciberseguridad en la actualidad y el "llamamiento a la acción"

Esta Guía expone cómo el sector del alquiler de equipos en toda Europa se enfrenta a un reto sin precedentes en las amenazas que presentan las vulnerabilidades y las exposiciones de las tecnologías de la información en nuestro negocio y, en particular, cómo los clientes nos exigen cada vez más protección en materia de ciberseguridad. El sector se encuentra en un proceso de consolidación, con empresas más pequeñas que se fusionan con otras para crecer en escala y empresas más grandes que adquieren otras más pequeñas para entrar en nuevos mercados y para consolidar su participación en el mercado o aumentarla. El negocio del alquiler de equipos está adoptando la "digitalización". Más presencia en línea significa más amenazas de ciberseguridad. Los equipos de alquiler son cada vez más inteligentes y están cada vez más conectados a las redes, las cuales pueden ser el medio para el ataque. Las empresas de alquiler de equipos que han sufrido un incidente grave sienten que han expuesto a un alto riesgo su negocio, su reputación y, sobre todo, a sus clientes y partes interesadas. La legislación de la UE es cada vez más estricta y la Guía señala las últimas novedades de la Directiva de la UE sobre seguridad de las redes y las tecnologías de la información (NIS, por sus siglas en inglés). El sector necesita ahora una unión continua entre las empresas europeas para colaborar en las mejores prácticas de ciberseguridad, las amenazas comunes y los problemas a los que se enfrentan todas las organizaciones.

Necesidades de inversión y presupuesto en ciberseguridad

Esta Guía ilustra las inversiones y los costos de una buena ciberseguridad. Presenta una escala de inversión y "madurez" que indica la inversión inicial para conseguir lo básico. Una buena ciberseguridad requiere una gran inversión, la cual debe renovarse año tras año. La inversión directa en ciberseguridad en todos los sectores se calcula en torno al 5 % del gasto en TI, y es mayor al principio. Los líderes también indican que la mayor inversión está en los costos indirectos e intangibles para "diseñar", gestionar e integrar la seguridad en todas sus actividades, lo que, en última instancia, puede suponer más que los costos directos.

Hoja de ruta de las principales prácticas y "lista de control"

La intervención en materia de ciberseguridad suele centrarse en la tecnología y los sistemas, pero muchos riesgos tienen su origen en el comportamiento humano, la solidez de los procesos y la supervisión, la notificación y la respuesta dentro de la empresa. Según los líderes del alquiler de equipos en este campo, una organización debe considerar una estrategia para toda la empresa que garantice que se tengan en cuenta todas las áreas de vulnerabilidad. Cada organización tendrá diferentes riesgos, alcance de las operaciones y brechas; sin embargo, los

líderes consideran que se puede desarrollar una lista de control de alcance integral bajo cuatro elementos de capacidad que abarquen: el proceso, las personas, la tecnología y la infraestructura. Esta Guía analiza dichos elementos y presenta los requisitos de capacidad básicos en cada uno de los tres niveles de "Nivel de base", "Maduración" y "Líder". Se incluye una lista de control que vincula la evaluación de riesgos y vulnerabilidades esenciales con los niveles actuales de madurez de la empresa como ayuda para la planificación y la reducción de riesgos.

"Se obtiene lo que se mide....." Los líderes informan que es esencial garantizar que las áreas clave de rendimiento que impactan en el estado de la ciberseguridad se midan con indicadores clave de desempeño (KPI, por sus siglas en inglés). La hoja de ruta de la Guía continúa indicando las medidas típicas y los sistemas de medición del rendimiento que utilizan actualmente las empresas líderes para cada uno de los elementos.

Ilustración de las principales prácticas

Ahora la Guía muestra algunas de las principales prácticas que se utilizan hoy en día en relación con los cuatro elementos de capacidad. Los líderes hacen hincapié en que, aunque un plan de seguridad completo forma parte esencial de una estrategia global, un plan integral no tiene por qué ser el primer paso: un plan completo puede venir normalmente en etapas de madurez. Las características clave son:

- **Proceso:** Los líderes subrayan que es más importante en las primeras etapas tomar medidas para identificar todas las posibles áreas de alto riesgo en la empresa y priorizar las acciones para colocar *plugs* o parches en las vulnerabilidades. Un análisis exhaustivo de los riesgos en cada uno de los pilares de esta Guía puede ser un buen punto de partida. A medida que se abordan las áreas de alto riesgo, se pueden tratar las áreas de riesgo medio. Cabe destacar que la investigación indica que, a partir de un nivel básico, avanzar para cubrir todas las áreas de riesgo significativas puede ser un proceso que lleve de tres a cinco años, el cual requiere una inversión material y sostenida. Los líderes apuntan a un recorrido, que puede ser de tipo básico, bueno o mejor, para lograr una seguridad adecuada mediante el uso de acreditaciones formales como hitos o diseñado a medida pero siguiendo los mismos principios. Se señalan una serie de marcos internacionales en uso.

- **Personas:** *La ciberseguridad no es una "cosa tuya"...* Desempeña un papel importante la gestión de los recursos humanos (RR. HH.) en la defensa de la ciberseguridad. La intervención y el apoyo de RR. HH. en las empresas líderes tiene un amplio alcance, que abarca el diseño y el desarrollo de políticas y procedimientos (incluso el Reglamento General de Protección de Datos y los protocolos de protección de datos) y su comunicación con todo el personal, la adaptación de los términos y condiciones de los empleados y la descripción de sus funciones para incluir las responsabilidades en materia de datos y seguridad, la concienciación y la formación sobre los imperativos de la ciberseguridad y el análisis de las necesidades de formación para las funciones de primera línea y el personal específico de seguridad. Son esenciales los medios de comunicación, como los boletines informativos o los boletines en las redes sociales para difundir en toda la empresa las últimas tendencias o amenazas.

- **Tecnología:** Las herramientas de tecnología de la información se siguen desarrollando rápidamente y proporcionan un poderoso medio de ciberdefensa para la “alerta temprana” y la interceptación de amenazas. El control de las amenazas y del estado de salud es posible gracias a la tecnología con sistemas avanzados, como "Splunk" y "MS Azure Sentinel", cuyo uso se ilustra. Establecer un Centro de Operaciones de Seguridad (SOC, por sus siglas en inglés) es esencial para aprovechar al máximo la potencia de los sistemas automatizados. Los líderes pueden contar con un SOC interno, a menudo complementado por centros de terceros, que brinde asistencia las 24 horas del día los 7 días de la semana y servicios avanzados de supervisión y gestión.

- **Infraestructura:** *"Si ocurre lo peor, a pesar de haber implementado las mejores medidas de prevención, hay que estar preparado con un plan de gestión de incidentes".* Los ataques pueden presentarse de muchas formas, pero uno de los más graves puede ser un "ataque de ransomware". En una situación de negación de sistema, se necesita una respuesta de emergencia inmediata, pero antes se tiene que haber puesto en marcha un proceso para evaluar y clasificar la situación. Esta Guía ilustra cómo los líderes analizan y responden, y proporciona una plantilla de "las primeras 48", que puede ayudar a planificar el período de gestión de crisis inmediatamente después de un evento de negación de sistema u otra amenaza importante.

Prepararse para un futuro seguro

La lucha por una buena seguridad informática nunca terminará, pero para mantenerse a la vanguardia, los líderes destacan que las empresas de alquiler de equipos deben:

1. *Conocer sus activos, sus fortalezas y sus vulnerabilidades*
2. *Llevar a cabo una evaluación de riesgos*
3. *Planificar e invertir adecuadamente*
4. *Prepararse, por si ocurre lo peor*
5. *Actualizarse y mejorar continuamente*

La "Guía de ERA a las mejores prácticas en ciberseguridad" pretende ayudar a las empresas de alquiler de equipos de todo tipo y tamaño a planificar, desarrollar o mejorar continuamente su ciberseguridad.