Consejos de ciberseguridad para empresas en Costa Rica y Centroamérica

San José, Costa Rica. 11 de julio de 2024

En un entorno empresarial cada vez más digital, la ciberseguridad es una prioridad estratégica para las empresas costarricenses para resguardar sus datos y sus finanzas. Con millones de intentos de ciberataques registrados anualmente, es indispensable que las empresas adopten medidas proactivas y reactivas para protegerse contra estas amenazas tangibles e intangibles.

Según datos recientes de FortiGuard Labs, en el 2023, más de 800 millones de intentos de ciberataques estaban dirigidos a empresas y organizaciones establecidas en Costa Rica. Además, en el estudio "Estado de la ciberseguridad en Costa Rica" se evidencia que han sido tramitados ante el OIJ entre el 2013 y 2023, más de 18 mil delitos, entre los que destacan estafas, plantación de identidad, espionaje, suplantación de páginas electrónicas y otros.

Mario Vargas, Gerente General del Grupo EULEN Costa Rica, comenta: "La ciberseguridad es un desafío creciente en el país. Es crucial que las empresas estén informadas y preparadas para enfrentar estas amenazas mediante un plan de Ciberseguridad diseñado e implementado por expertos. Nuestro compromiso en Grupo EULEN es proporcionar soluciones y educación para fortalecer la protección digital en nuestro país aportando la experiencia internacional en la ejecución de estas estrategias, alerta temprana y soluciones específicas, según la razón de ser de la empresa".

En apoyo a estas iniciativas, el Grupo EULEN Costa Rica, proveedor de servicios de seguridad integral, comparte consejos para que las empresas puedan protegerse de estas nuevas modalidades de crimen.

Recomendaciones de Ciberseguridad para empresas:

1. **Evaluación de riesgos y vulnerabilidades**: Identificar los activos críticos, evaluar las posibles amenazas y determinar las debilidades en la infraestructura de seguridad es esencial. Las evaluaciones y pruebas de seguridad son herramientas clave para detectar brechas existentes.
2. **Capacitación y concienciación del personal:** La mayoría de las brechas de seguridad se originan en acciones involuntarias del personal. Invertir en programas de capacitación en ciberseguridad es fundamental para educar a todos los miembros de la empresa sobre las amenazas actuales y las mejores prácticas de seguridad.
3. **Adopción de tecnologías avanzadas de seguridad**: Implementar soluciones avanzadas como la inteligencia artificial y el aprendizaje automático permite detectar y mitigar ataques de manera proactiva. *Firewalls* avanzados y sistemas de detección de intrusiones son componentes esenciales de una defensa robusta.
4. **Actualización constante de sistemas y aplicaciones**: Las actualizaciones de *software* frecuentemente incluyen parches de seguridad que protegen contra vulnerabilidades conocidas. Un programa riguroso de actualizaciones y parches asegura que la infraestructura de TI esté protegida contra las amenazas más recientes.

5. **Protección de datos en la nube y respaldos regulares**: Con la adopción creciente de servicios en la nube, es vital implementar medidas de seguridad robustas. La encriptación de datos, el monitoreo continuo y la gestión de accesos son cruciales. Además, una estrategia sólida de respaldo de datos garantiza la disponibilidad y recuperación rápida en caso de un incidente.
6. **Monitoreo continuo y respuesta inmediata**: Detectar actividades sospechosas de forma temprana es crítico para limitar el impacto de un ataque. Los sistemas de monitoreo continuo permiten identificar patrones anómalos y responder de manera efectiva.
7. **Fomento de la colaboración y el intercambio de información sobre amenazas**: La colaboración y el intercambio de información entre organizaciones pueden prevenir ataques. Participar en comunidades de ciberseguridad y colaborar con organismos gubernamentales fortalece las defensas colectivas.
8. **Implementación de controles de acceso rigurosos**: Asegurar que solo el personal autorizado tenga acceso a información crítica y sistemas importantes es vital. La gestión adecuada de permisos y el uso de autenticación multifactor pueden prevenir accesos no autorizados.
9. **Desarrollo de un plan de respuesta a incidentes**: Contar con un plan bien definido para responder a incidentes de seguridad es esencial. Este plan debe incluir protocolos de comunicación, acciones inmediatas para contener el ataque y pasos para restaurar la normalidad operativa.

Han pasado ya dos años desde que varias instituciones públicas del país fueron víctimas de ataques informáticos, afectando en diferentes escalas los servicios. Esta situación elevó las alertas en todos los sectores de la sociedad, para adoptar medidas urgentes para evitar ser víctima de ciber amenazas e incluso en la presentación de la Estrategia Nacional de Ciberseguridad 2023-2027, para hacer de Costa Rica un país ciberseguro.

"Disponemos de distintos tipos de servicios, que abarcan desde soluciones básicas de ciberseguridad hasta medidas más sofisticadas que requieran alto grado de especialización tanto en el ámbito de las tecnologías de la información como en entornos industriales, para garantizar la continuidad de los servicios en todo su ciclo de vida", añadió Vargas.

En el primer semestre de 2024, GRUPO EULEN, presentó la expansión global de su línea de **servicios de ciberseguridad**, entendiendo la importancia de garantizar la seguridad de datos y sistemas de información y comunicación que utilizan las empresas e instituciones públicas para el desarrollo de todos sus procesos, sumando esfuerzos con la inteligencia de la seguridad.

Para más información:
Freddy Román Navarro
froman@themapcomm.com
Tfn. +506 6051-3971
The Map Communications http://www.themapcomm.com