

Consejos de ciberseguridad para empresas en Panamá

Ciudad de Panamá. 11 de julio de 2024.

En un entorno empresarial cada vez más digital, la ciberseguridad es una prioridad estratégica para las empresas panameñas para resguardar sus datos y 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, Panamá enfrentó más de 1.7 millones de intentos de ataques de *phishing* en 2023, convirtiéndose en una de las estafas cibernéticas más comunes en la región. Además, en el primer semestre de 2023, el país fue blanco de más de 1,500 millones de intentos de ciberataques, situándose entre los países más atacados de América Latina y el Caribe. El sector bancario y financiero ha sido el principal objetivo, con una organización promedio experimentando alrededor de 1,214 ataques cibernéticos en los últimos seis meses. Panamá también lidera la región en la cantidad de ataques de ransomware, con al menos 8,000 casos e intentos registrados en 2023.

Antonio Pérez, Gerente General del Grupo EULEN Panamá, comenta: "La ciberseguridad es un desafío creciente en Panamá. 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 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 Panamá, proveedor de servicios de seguridad integral para las empresas, 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 concientización 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.

A pesar de contar con un sólido marco de gobernanza digital, las instituciones de ciberseguridad en Panamá aún están en desarrollo. Iniciativas como el CSIRT Panamá y la campaña "Panamá Cibersegura" han sido implementadas para combatir los ciberataques.

Antonio Pérez añade: "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".

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.

El Grupo EULEN es líder en el diseño de servicios a empresas, con el objetivo de ofrecer a la sociedad servicios innovadores que aportan soluciones útiles, de calidad y más eficientes. Está especializado en las actividades de limpieza, seguridad, servicios auxiliares (de logística, generales y de telemarketing), FSM (Facility Services & Management), servicios sociosanitarios, mantenimiento integral, soluciones globales de recursos humanos y empleo y medio ambiente. Fundada en 1962 en Bilbao, la compañía está presente en 11 países y el volumen de ventas consolidadas supera los 1.600 millones de euros, con una plantilla global de más de 75 000 personas.

El Grupo EULEN está adherido al Pacto Mundial y firmemente comprometido con la sociedad a través del desarrollo de políticas socialmente responsables: integración laboral de colectivos desfavorecidos, conciliación de la vida familiar y profesional para su personal

Para más información:

Sheila Phillips
sphillips@themapcomm.com
<http://www.themapcomm.com>

Tfn. +507 6450-3923
The Map Communications