CENTRO
DE COMPETENCIAS
TECMILENIO

El futuro de la ciberseguridad en redes computacionales

El futuro de la ciberseguridad en redes computacionales

La amenaza de ciberataques no deja de aumentar día a día, por lo que la ciberseguridad se ha convertido en una cuestión crítica para cualquier empresa y los particulares. Debido a la gran cantidad de información sensible que se transmite y almacena en línea, es muy importante protegerse contra la ciberdelincuencia, por lo que el futuro de la ciberseguridad debe enfocarse en proteger la información, según Banafa (2023).

De acuerdo con un informe de la empresa de seguridad cibernética Symantec, se espera que la ciberseguridad se convierta en una parte integral de la planificación de la infraestructura de red en el futuro cercano. Además, se espera que las empresas y organizaciones inviertan más en tecnologías y soluciones de seguridad cibernética para protegerse contra las crecientes amenazas en línea.

El informe también señala que la formación y capacitación de los usuarios finales en cuestiones de seguridad cibernética será un área clave de enfoque en el futuro, ya que los usuarios son a menudo el punto débil en la seguridad cibernética.

También se espera que la inteligencia artificial y el aprendizaje automático sean cada vez más utilizados para identificar y mitigar amenazas de seguridad en tiempo real.

El informe señala que la tecnología blockchain será cada vez más utilizada para aumentar la seguridad en la gestión de datos y transacciones. Se espera que la combinación de estas tecnologías y soluciones de seguridad cibernética ayude a proteger mejor la información y los sistemas en línea en el futuro, según Haley (2019).

Los dispositivos de IoT (Internet de las Cosas) cada vez más comunes, tendrán un impacto en el futuro de la seguridad, debido a que son usados para controlar sistemas e infraestructuras. Aunque estos dispositivos IoT, en la actualidad tienen características de seguridad deficientes y por lo mismo pueden ser manipulados por los ciberdelincuentes, las empresas deberán implementar medidas de seguridad mediante la actualización del firmware y el software de los dispositivos IoT, utilizando otros con múltiples niveles de seguridad, tales como 2FA.

En la actualidad, los gobiernos invierten en investigación y desarrollo, para evitar ataques y proteger el acceso a información sensible. En el futuro puede que se desarrollen algoritmos de cifrado nuevos o la informática cuántica para descifrar códigos complejos, según Banafa (2023).

Los algoritmos cuánticos podrían predecir ataques cibernéticos en un futuro, en base a tendencias y datos históricos.

En el futuro, se espera que la ciberseguridad se convierta en una parte integral de la planificación de la infraestructura de red y que las empresas y organizaciones inviertan más en tecnologías y soluciones de seguridad cibernética. Esto incluirá la adopción de medidas preventivas, tales como la implementación de políticas de seguridad de la información, y la realización de pruebas de penetración para identificar y corregir vulnerabilidades en la red.

Además, se espera que haya un mayor enfoque en la formación y capacitación de los usuarios finales en cuestiones de seguridad cibernética, para que puedan reconocer y evitar los riesgos de seguridad cibernética y actuar de manera segura en línea.
En resumen, el futuro de la ciberseguridad en redes computacionales será cada vez más complejo y sofisticado, y requerirá una mayor colaboración entre empresas, organizaciones y proveedores de servicios de seguridad cibernética para asegurar la protección de la información y los sistemas en línea.

Referencias bibliográficas

- Banafa, A. (2023). *El futuro de la ciberseguridad. Previsiones y tendencias*. Recuperado de https://www.bbvaopenmind.com/tecnologia/-mundo-digital/futu-ro-ciberseguridad-previsiones-tendencias/

- Haley, K. (2019). *El Informe sobre amenazas de seguridad en la nube de Symantec CSTR 2019*. Recuperado de https://www.symantec.com/con-tent/dam/symantec/docs/reports/is-tr-24-2019-en.pdf.