La Importancia de la Inteligencia Artificial en la Seguridad Cibernética

Autor: Yamil Rosario Martinez
Asesor: Dr. Nelliud D. Torres
Departamento de Ingeniería y Ciencias de Computadoras

Resumen

El mundo se está digitalizando a un ritmo sin precedente. Los sistemas de información y la tecnología están cambiando o evolucionando muy rápido. Con los adelantos en la tecnología, la velocidad de los procesos y la cantidad de datos que se genera diariamente es casi imposible que los sistemas puedan ser protegidos y monitoreados por seres humanos sin la ayuda de aplicaciones o sistemas inteligentes que faciliten el trabajo. Debido a la gran cantidad de dispositivos electrónicos que hay conectados a la Internet los expertos en seguridad cibernética van a enfrentar muchos retos para poder proteger los sistemas adecuadamente. En el tiempo presente se necesita de todo el apoyo que se pueda conseguir para prevenir y mitigar los ataques cibernéticos y las violaciones de datos.

Introducción

Durante los pasados años se ha visto un aumento en la cantidad de ataques cibernéticos que las compañías están recibiendo. Cada vez estos ataques se vuelven más complejos, sofisticados y difíciles de detectar. Algunos de los factores para este aumento podría ser la gran cantidad de dispositivos que se conectan diariamente a la Internet, ya sean teléfonos inteligentes, computadoras portátiles, computadoras de escritorio, tableta, consolas de juegos o incluso cámaras de seguridad por solo mencionar algunos. Esto ha ocasionado que el tráfico de datos aumente considerablemente, así como la cantidad de vectores de ataque que se pueden identificar.

Muchos de los equipos que se utilizan hoy día para conectarse a la Internet no están protegidos correctamente ya sea porque están mal configurados, no cuentan con los últimos parchos de seguridad o simplemente cuando fueron diseñados la seguridad no era la prioridad del manufacturero. Los ataques cibernéticos generan millones de dólares en ganancias. De acuerdo con un estudio realizado por IBM y el Instituto Ponemon en el año 2019, el costo promedio total de las violaciones de datos ha aumentado un 12% en los últimos 5 añs. Las violaciones de datos durante el año 2019 tuvieron un costo total aproximado de $3.92 millones de dólares y el tiempo promedio que se tardaron las compañías en identificar y contener la falla fue de 280 días. Los costos de las violaciones de datos van a seguir aumentado, por eso es necesario establecer mejores medidas de seguridad. La introducción de la inteligencia artificial en los sistemas de seguridad puede ayudar a reducir las amenazas que cada vez van a ser mayores.

¿Qué es la Seguridad Cibernética?

La seguridad cibernética es la diciplina que se encarga de proteger la integridad y la privacidad de la información almacenada en los sistemas de información. Se diseñó basada en reglamentos, modelos y estándares para poder proteger las redes, los dispositivos electrónicos, los programas y los datos contra ataques, daños o acceso no autorizado. La seguridad cibernética es importante porque las compañías almacenan datos y generan miles de transacciones es sus sistemas. Una parte importante de esos datos y transacciones puede ser información confidencial, ya sea propiedad intelectual, datos financieros, información de sus empleados o clientes u otros tipos de datos para los cuales el acceso o la exposición no autorizada podría tener consecuencias negativas. El objetivo final de la seguridad cibernética es poder proteger la economía, la infraestructura crítica y el país de los daños que pudieran ser resultado del uso indebido, accidental o intencional de los sistemas de información.

¿Qué es una Violación de Datos?

Una violación de datos se define como un evento o incidente en el que la información de una persona ya sea su información privada, registro médico, información financiero o información de tarjeta de crédito fue accedida sin autorización.

Inteligencia Artifical

La inteligencia artificial es un término que lleva rondando en el campo de la tecnología desde la década de los 50 cuando Alan Turing propuso la pregunta ¿Puede pensar una maquina? La posibilidad de poder construir aplicaciones y sistemas más inteligentes que los seres humanos ha sido desde el principio el horizonte de la inteligencia artificial. La inteligencia artificial es la combinación de algoritmos con el propósito de crear máquinas que puedan simular la inteligencia humana. La inteligencia artificial tiene muchas aplicaciones posibles. Algunas de las que se utiliza hoy día son en biotecnología, salud, comercio, servicios financieros, redes sociales y seguridad cibernética.

Técnicas Utilizadas en la Inteligencia Artificial

Técnica	**Uso**
Agentes Inteligentes	Proactividad, Reactivo, Defensa contra DDoS
Red Neuronal	Sistemas de Detección y Prevención de Intrusos, Alta Velocidad de Operación, Investigaciones Forense, Detección de Calor
Sistemas Expertos	Apoyo a Decisión, Detección de Intruso en la Red, Base de Conocimientos, Motores de Inferencia
Aprendizaje Automático	Aprendizaje Supervisado y No Supervisado, Detección de Malware, Detección de Intrusos

¿Porque es necesaria la Inteligencia Artificial?

La inteligencia artificial está en todos los lugares. Se está utilizando en cosas tan sencillas como predicciones de compras, reconocimiento de imágenes, reconocimiento de voz hasta en áreas más complejas como lo son las redes sociales o los autos autónomos. Con la ayuda de la inteligencia artificial la recopilación de datos es mucho más fácil. Esto es debido a que las capacidades de almacenamiento y eficacia de los sistemas han aumentado y sus costos han bajado, los algoritmos matemáticos que se utilizan han mejorado y los procesos de computación son mucho más rápidos. La realidad es que en tiempo real las enormes cantidades de datos que se transmiten cada segundo son sumamente difíciles de manejar y analizar por seres humanos. Con la ayuda de la inteligencia artificial el análisis de estos datos podría reducirse a milisegundos. Con estos resultandos las empresas podrían fácilmente identificar, reaccionar y recuperarse de amenazas.

La inteligencia artificial va a producir la próxima revolución industrial de nuestro tiempo. Esto es debido a que el gasto mundial en inteligencia artificial para el año 2019 llego a $35.8 billones de dólares. Un aumento de 44% sobre la cantidad gastada en 2018. La industria va a empezar a reemplazar el cerebro humano por maquinas, maquinas que sean más inteligentes, maquinas que puedan hacer el trabajo mucho más rápido, que no se cansen, no se aburran, no necesiten descansar, dormir y no se rompan.

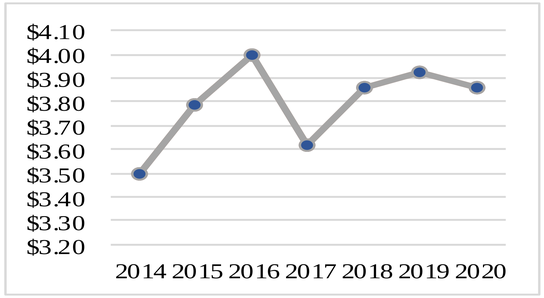
¿La Amenaza es Real?

Si bien las ventajas y beneficios en el tiempo que estamos viviendo son muchos, también esto trae consigo varios aspectos negativos. Una de las amenazas más significativas y destructivas que estamos enfrentado es que nuestra información privada y persona está en constante peligro. En los últimos años se han visto un aumento significativo en los ataques cibernéticos que hemos estado recibiendo, esto trae por consiguiente pérdida de dinero para los usuario o compañías que han sido afectadas. Las pérdidas financieras son un riesgo muy significativo para las empresas, además de que la reputación que estás compañías han creado se vería afectada. En los últimos años hemos visto como algunas de las compañías más importantes del mundo han sufrido ataques cibernéticos y la información de sus clientes o empleados ha sido comprometida. Los ataques cibernéticos no discriminan y afectan a los individuos, empresas privadas y organizaciones gubernamentales, por igual. Se está avanzando en una era en la que los criminales cibernéticos pueden estudiar y atacar a sus víctimas desde cualquier parte del mundo a cualquier hora. Cualquier organización independientemente de su tamaño o ubicación geográfica puede ser un objetivo potencial. La necesidad de integrar la inteligencia artificial en la seguridad cibernética nunca ha sido más critica que ahora.

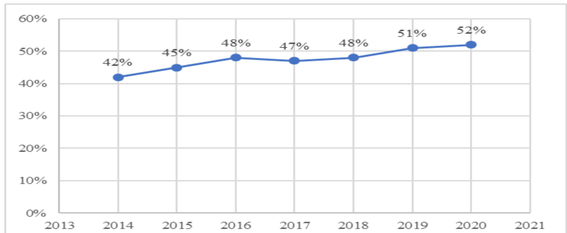
La tecnología está cambiando constantemente. Al igual que la tecnología cambia, también la forma que los criminales cibernéticos utilizan para distribuir sus virus o programas malignos. La realidad es que la detección de los programas malignos se ha vuelto mucho más difícil a cómo era en el pasado. No es raro que los criminales cibernéticos utilicen múltiples técnicas para disfrazar sus códigos, hacer que sus códigos malignos sean indetectables para los antivirus y utilicen la encriptación para evitar ser examinados. Esto hace que las posibilidades de que los criminales cibernéticos puedan comprometer un sistema sin ser detectados sean mayores.

Costo de las Violaciones de Datos

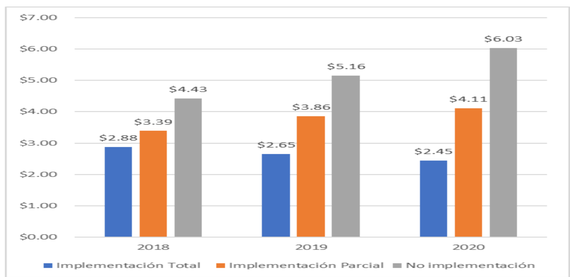
Costo Total Promedio de las Violaciones de Datos



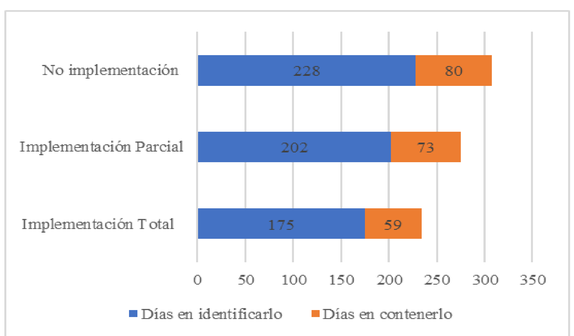
Tendencia en las Violaciones de Datos Causados por Ataques Malicioso



Costo Total Promedio de Violaciones de Datos del 2018-2020



Tiempo Promedio para Identificar y Contener una Violación de Datos



Uso de la Inteligencia Artificial en la Seguridad

Entre los muchos beneficios que la inteligencia artificial le puede brindar a la seguridad cibernéticas estos son solo algunos:

- La inteligencia artificial tiene la capacidad de analizar el comportamiento de los usuarios. Lo que esto significa es que los algoritmos que utilizan pueden aprender y crear patrones de comportamiento.
- Los sistemas de seguridad basados en inteligencia artificial y aprendizaje automático se pueden configurar para que estén proactivamente buscando posibles vulnerabilidades que puedan ser identificadas.
- Ayudan a compensar la escasez de personal diestro en el campo de la seguridad cibernética que están sufriendo las compañías y ayudan a reducir costos operacionales.
- Se pueden utilizar para eliminar datos no deseados, de esta forma ayudará a los expertos en seguridad cibernética a comprender mucho mejor el entorno cibernético con el fin de poder detectar las actividades anormales.
- Esta tecnología es capaz de analizar grandes cantidades de datos, esto permite que se puedan desarrollar sistemas y aplicaciones de manera apropiada con el fin de poder reducir los ataques cibernéticos.
- Pueden identificar de inmediato el tráfico inusual en las redes, esto ayuda a reducir lo que es la minería de Bitcoin, la ejecución de archivos remotos e incluso los inicios de sección de Fuerza Bruta.
- Pueden detectar patrones de comportamiento malicioso en el tráfico de la red, en los archivos y sitios web que se introducen en las redes. Esto es debido a que las redes basadas en inteligencia artificial pueden detectar ataques que no serían posible detectar por sistemas regulares de defensa.
- Detección y mitigación de ataques DDoS con éxito. Se ha demostrado que compañías con escasos recursos de defensa han tenido éxito contra ataques de gran escala de DDoS cuando utilizan inteligencia artificial.
- Los sistemas bancarios y comerciales están utilizando la inteligencia artificial para ayudar a prevenir los delitos financieros.

Conclusión

Cada día los ataques cibernéticos están creciendo tanto en complejidad como en frecuencia. Los métodos convencionales que estamos utilizando para identificar las amenazas y *malware* están fallando. Los atacantes están constantemente desarrollando nuevas formas de eludir los controles de acceso y *firewall* para poder comprometer las redes. Las compañías están haciendo todo lo posible para luchar contra los ataques cibernéticos, pero es sumamente difícil poder predecir que nuevo ataque surgirá y como funcionaran. Es aún más difícil poder identificar cual será la próxima gran amenaza. Por tal razón necesitamos soluciones modernas que sean impulsadas por la inteligencia artificial para poder hacer frente a los riesgos de seguridad actuales y futuros. Para impulsar la seguridad y poder combatir las amenazas cibernéticas, las compañías deben adoptar nuevas tecnologías. La inteligencia artificial no es 100% a prueba de amenazas, pero está claro que jugara un papel importante en las estrategias de defensa de las compañías, permitiéndole estar mas preparadas para las próximas amenazas cibernética.

Referencias

IBM Security, *Cost of Data Breach Report 2020*. Armonk, NY: IBM Corporation, 2020.

B. Fischer. (2020, Marzo 2). *What is the Average Cost of a Data Breach?* [Online]. Available: https://www.scasecurity.com/cost-of-a-data-breach/#:~:text=The%20average%20size%20of%20a,breach%20will%20exceed%20%24150%20million.

S. Bhutada and P. Bhutada, “Application of Artificial Intelligence in Cyber Security,” *International Journal of Engineering Research in Computer Science and Engineering (IJERCSE).* vol. 5, no. 4, p. 2014-2019, April 2018.

NortonLifeLock. (n.d.) *What is a data breach?* [Online]. Available: https://us.norton.com/internetsecurity-privacy-data-breaches-what-you-need-to-know.html

C. Czosseck, E. Tyugu and T. Wingfield. “Artificial Intelligence in Cyber Defense”. *3rd International Conference on Cyber Conflict*, Tallin, Estonia: Cooperative Cyber Defense Center of Excellence (CCD COE) and Estonia Academy of Science, 2011.
M. R. Gurrola–López y J. C. Macias-Torres. (n.d.) *Agentes Inteligentes* [Online]. Available: https://sitiointeligenciaa.wordpress.com/agentes/

O. Gan. (2018, marzo 21). *Artificial Intelligence: a Silver Bullet in Cyber Security? CPX360* [Online]. Available: https://www.youtube.com/watch?v=ggje-L0ViFM

D. Palmer. (2020, marzo 2). *AI is changing everything about cybersecurity, for better and for worse. Here’s what you need to know* [Online]. Available: https://www.zdnet.com/article/ai-is-changing-everything-about-cybersecurity-for-better-and-for-worse-heres-what-you-need-to-know/