TRENDS 2020

Para la **década** que se está iniciando, Microsoft ha identificado cuatro tendencias que darán ***forma*** a la industria de la seguridad de la información para que las empresas se **protejan**.

1. **Lo bueno y lo malo de la IA**

La capacidad de la **inteligencia artificial** para aprovechar el poder de los datos ha dado nuevas **capacidades** e **información** de valor para enfrentar el **crimen cibernético** de identificar más rápido y más a fondo ***patrones y anomalías***, para adoptar medidas defensivas en el campo de forma rápida.

2. **Colaboración para proteger las cadenas de suministro**

Con más de **75,000** millones de dispositivos móviles (incluido IoT "Internet of things") que se prevé estén e uso a nivel mundial en 2020, las brechas como el **software obsoleto**, los **dispositivos no seguros** y las cuentas de administrador **predeterminadas** pueden brindar un amplio rango de vectores para que los **atacantes** ingresen a los sistemas.

3. **La importancia de asegurar el cloud público**

Hasta que las empresas implementen **mejores prácticas en seguridad**, incluso los ataques más trillados, como el **phishing**, seguirán siendo efectivos. El riesgo es cada vez mayor con las empresas que tienen servicios en la nube.

4. **La caída de las contraseñas y el surgimiento de Zero Trust**

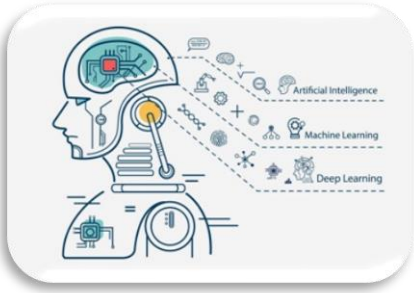
En 2019, más de **4,000 millones** de registros fueron expuestos debido a brechas de datos. Las **identidades** y **contraseñas** con una **pobre** seguridad se mantienen como el **eslabón más débil**, en especial frente a malware basado en IA. El **63%** de todas las brechas de datos confirmadas involucraron contraseñas **débiles**, por **defecto** o **robadas**.

TRENDS 2020

La ciberseguridad ha encontrado un **nuevo aliado** que puede poner las cosas más difíciles a los ciberdelicuentes: la inteligencia artificial (IA). La inteligencia artificial y el aprendizaje de máquinas aportan a la seguridad la capacidad de ***adaptarse***, y de reaccionar ante movimientos **sospechosos** que se salen de las reglas convencionales.

Mejoras en la IA de las herramientas

Las principales herramientas de seguridad, desde los antivirus hasta las redes virtuales privadas o la gestión de cuentas, se van a ver **reforzadas** por la inteligencia artificial.



Nuevas formas de autentificación remota

El nuevo estilo de **coworking** en las empresas, en donde crece el acceso remoto a los recursos internos, obligará a buscar **nuevas herramientas** de seguridad que permitan hacer cosas como decidir quién tiene acceso a qué.

Mayor control de los datos personales y la privacidad

Los últimos escándalos de privacidad, han **concienciado** a los usuarios, que piden nuevas herramientas que velen por su **privacidad**, o que permitan decidir quien puede ver sus datos, y por cuanto tiempo.

Hardware infectado

La IA y el aprendizaje de máquinas hacen más **peligrosas** las amenazas que provienen del hardware infectado**: desde memorias USB a cables USB** y cargadores que infectan el móvil cuando intentamos recargarlo (lo que se conoce como juice jacking).

Si tienes preguntas, o necesitas información adicional, puedes escribir al área de seguridad de la información: areaseguridad@visanet.com.gt

Los cibercriminales también usarán la IA

No solo los sistemas de seguridad aprovecharán la IA para protegernos. Los **hackers** también han comenzado a usar la inteligencia artificial para estudiar **comportamientos** y **flujos de datos** y **predecir** dónde están los **agujeros** de seguridad, estudiar los mecanismos de defensa que quieren romper **y simular patrones** de comportamiento para atacar las redes o **eludir** los controles de seguridad.