arsys

Inteligencia Artificial

¿cómo es el futuro inmediato de la ciberseguridad?

Los ciberataques son un enorme riesgo para empresas y particulares. Son cada vez más numerosos y más sofisticados, y las perspectivas para 2019 no son nada halagüeñas. La ciberseguridad tiene ante sí un reto enorme, y la inteligencia artificial cuenta con muchas papeletas para ser protagonista en la protección activa de las organizaciones, y no solo para respaldar la ciberseguridad.

A lo largo de esta guía veremos qué tipos de amenazas existen en 2019, cómo se ha de preparar una empresa ante los ciberataques y cómo nos pueden ayudar la inteligencia artificial y los algoritmos de machine learning a estar más preparados ante los ataques.

Amenazas y tendencias en ciberseguridad en 2019

La sofisticación de los ataques será cada vez mayor en 2019. Si el año anterior vimos casos de filtrado de datos sensibles en grandes compañías, ataques de ransomware cada vez más sofisticados y los asistentes personales por voz como objetivos interesantes para los delincuentes, en 2019 podemos esperar un mayor nivel en las amenazas.

Nuevas y más potentes variantes de malware

El malware es una de las principales fuentes de ingresos de los delincuentes. Hoy, el abanico de posibles objetivos de ataque es enorme, y seguirá creciendo. Además de los ordenadores y servidores, hemos de prestar atención a los dispositivos móviles —portátiles, tablets o smartphones— y también todos los nuevos dispositivos IoT.

Las posibilidades son enormes, y uno de los ejemplos más inquietantes es el ataque a dispositivos médicos conectados, ya que podría llevar a chantajes que no solo exijan dinero a cambio de los datos, sino que amenacen la vida de los usuarios. Es posible que suene un poco extremo, pero la posibilidad existe.

El informe Threat Landscape Report indica que «la innovación y las tendencias destructivas se mostraron entre las variantes de malware analizadas durante todo el año. Esto, combinado con la tendencia en auge del cryptojacking, apunta a la continua transformación del cibercrimen».

Los ataques dirigidos y las APT serán más sofisticados y avanzados

Las amenazas persistentes avanzadas —en inglés Advanced Persistent Threats, o APT— se centrarán en el ciberespionaje y sofisticarán sus técnicas, además de crecer en número. Serán más difíciles de detectar y de contrarrestar, y cualquier entidad que necesite conseguir información hará importantes inversiones en el desarrollo de estas herramientas maliciosas.

El sector industrial será un objetivo principal del cibercrimen

La transformación digital en el sector industrial tiene una contrapartida clara: un aumento de su vulnerabilidad ante los ciberataques. Las amenazas no dejan de aumentar en el sector, y podemos destacar los ataques dirigidos y de código malicioso, el robo de información sensible, la pérdida de disponibilidad de los sistemas o la alteración de los procesos.

Aumenta la amenaza de los ataques DDoS

Los ataques DDoS no han dejado de crecer y de innovar en su terreno. Son una gran amenaza al atacar directamente a la disponibilidad de los sistemas, y en 2019 se espera un auge de los TDoS —Telephony Denial of Service, o denegación de servicio de telefonía—. En este tipo de ataque se lanzan demasiadas solicitudes de acceso al sistema y, por tanto, se produce un colapso que afecta a los usuarios legítimos. También veremos cómo el PDoS —Permanent Denia of Service— aumenta en importancia, sobre todo dirigido a los centros de datos y dispositivos IoT.

El Cloud, un objetivo cada vez más interesante para el ciberdelincuente

La razón de que aumente el interés por los entornos Cloud es su uso cada vez más generalizado. Con cada vez más empresas migrando al Cloud, es lógico pensar que este entorno sea muy interesante para aquellas organizaciones criminales que hacen negocio con los datos sensibles. El mayor reto para frenar esta tendencia es el de evitar las fugas de información desde el interior.

Qué deben hacer las empresas para protegerse de los ataques y cómo ayuda la inteligencia artificial

Las medidas clásicas para hacer frente a los ciberataques son bien conocidas por todos:

- Mantener el software actualizado, especialmente atendiendo a las actualizaciones de seguridad.
- Evitar la apertura de emails y documentos de origen desconocido o no confiable.
- Alertar al equipo de seguridad de la empresa ante la menor duda o sospecha de estar siendo objeto de fraude o ataque —incluyendo la ingeniería social—.
- Formar a los empleados en seguridad para minimizar los posibles puntos de entrada de un ataque a la empresa.
- Mantener una política de backups lo suficientemente robusta y segura para evitar la pérdida irreparable de datos.

Sin embargo, estas medidas pueden ser insuficientes a corto plazo debido a la complejidad creciente de los ataques, a la sofisticación de las herramientas utilizadas por los delincuentes y al cada vez más amplio conjunto de posibles objetivos.

Por un lado, existe una carencia de profesionales IT cualificados en seguridad a nivel global, y la percepción es que las empresas son vulnerables ante este tipo de crimen. El informe «The Life and Times of Cybersecurity Professionals» destaca que un 91% de las empresas encuestadas perciben que son vulnerables —un 45% opina que son «de alguna manera vulnerables», mientras que un 46% afirma ser «extremadamente vulnerables» ante ciertos ataques graves—.

La automatización es una buena solución para mejorar en seguridad. Cada vez es más difícil que los profesionales de la seguridad puedan gestionar todos los frentes con soltura. Esto es cierto, sobre todo, en entornos con flujos de datos masivos —Big Data, IoT—. El machine learning permite crear una fuerza activa de seguridad que ejecute las tareas más repetitivas y tediosas y que, a su vez, proporcione nuevas herramientas de prevención y defensa.

Un ejemplo de la aplicación de sistemas de aprendizaje automático lo tenemos en la técnica «honey pot». Se trata de configurar una serie de servidores falsos, como reclamo, que contengan información aparentemente legítima, pero inventada, sin valor. De esta manera, los atacantes se centran en esos servidores y pueden revelar sus técnicas. El problema es la cantidad de tiempo y recursos necesarios para supervisar y monitorizar entramados complejos de servidores falsos.

Los algoritmos de aprendizaje automático son la respuesta para esta dificultad, pues pueden realizar estas tareas con mayor velocidad y precisión que los operadores humanos, y aprender con la experiencia, incorporando ese conocimiento al sistema de manera continuada.

Por tanto, entramos en una era en la que la inteligencia artificial será cada vez más protagonista en la ciberseguridad. Esto, lejos de suponer una amenaza para los trabajadores de seguridad IT, es una oportunidad para que centren sus esfuerzos y sus capacidades humanas en áreas más creativas.

arsys

www.arsys.es

www.facebook.com/arsys.es

twitter.com/arsys

www.linkedin.com/company/arsys-internet/