10 predicciones sobre riesgos y amenazas de ciberseguridad para 2020

sedian
Seguridad Digital de Andalucía

Junta de Andalucía

1 Noticias falsas

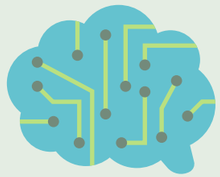
La producción de imágenes y vídeos utilizando tecnologías de Machine Learning para generar noticias falsas se incrementará.

2 Ransomware

Aumentarán los casos de malware y ransomware dirigidos contra empresas y organismos públicos. Ransomware como método de extorsión.

3 IA - ML

La Inteligencia Artificial y el Machine Learning se aplicarán en la detección de incidentes, pero también serán utilizados por los atacantes.



4 IoT

Se atacará a las infraestructuras más críticas, sobre todo donde se ha desplegado IoT sin tomar las medidas de seguridad adecuadas.

5 DevOps

El desconocimiento o baja capacitación de desarrolladores y técnicos de sistemas en la seguridad de los sistemas de integración continua, provocará la aparición de riesgos en los despliegues implementados por estos equipos de DevOps.

6 APIs

Las APIs (esenciales en el ecosistema de aplicaciones actual) quedarán expuestas como la parte más débil dentro de los entornos basados en la nube.

7 Ciberconflictos

Los ciberataques alentados por ciertos estados se usarán cada vez más como un instrumento al servicio de la geopolítica, con el objetivo de influir en la política y economía de ciertas regiones del planeta.

8 Digitalización

Como consecuencia de la transformación digital aumentará la movilidad de los empleados, ampliándose la superficie de exposición y consiguientemente el riesgo de ataques.

9 Banca abierta

Los sistemas bancarios estarán en el punto de mira con la banca abierta (PSD2), el malware para cajeros y dispositivos móviles.

10 5G

Se espera una gran cantidad de vulnerabilidades en torno a esta tecnología debido a los errores inevitables por su reciente desarrollo.

Fuente: Informe "Predicciones de amenazas para 2020" de AndalucíaCERT | Predicciones de las empresas: Check Point SOFTWARE TECHNOLOGIES LTD. · eset · FORTINET · kaspersky · McAfee · TREND MICRO