Resumen Ejecutivo

Endorsed by:

ICC UNITED KINGDOM
INTERNATIONAL CHAMBER OF COMMERCE
The world business organization

TREND MICRO™

Project 2030
Resumen Ejecutivo

Tendemos a centrarnos en el presente, sobre todo cuando vivimos grandes acontecimientos mundiales. Pero no podemos dejar que nuestro enfoque actual nos impida anticipar cómo la tecnología afectará a nuestro futuro. Solo calculando cuidadosamente los escenarios futuros, la comunidad de ciberseguridad puede prepararse para protegerlo.

Trend Micro ha adoptado una visión futurista de la tecnología, y de las ciberamenazas asociadas a ella, que podría influir y hacer evolucionar el mundo para el año 2030.

Esta nueva sociedad puede parecer una película de ciencia ficción desde nuestro punto de vista en 2021. Así nos sentimos en 2012 cuando publicamos el **informe Project 2020**. Ese futuro nos parecía inalcanzable, pero resultó ser una **predicción bastante** precisa del estado de la tecnología y los ciberriesgos en la actualidad.

Ahora repetimos esta práctica para mirar al futuro de la sociedad.

El mundo en 2030

¿Cómo viviremos y trabajaremos en 2030? El informe examina el mundo futuro desde el punto de vista de un individuo, una organización y un gobierno para dar una idea global del impacto de la evolución tecnológica.

Nuestra ciudadana, Resila, vive en un mundo totalmente conectado en el que las necesidades cotidianas, como hacer la compra, están totalmente gestionadas por dispositivos y sensores conectados. De hecho, casi todo está conectado con sensores para recoger datos. Los datos nutricionales, el uso del gimnasio y los patrones de sueño se comparten con su médico. Los medicamentos se imprimen en 3D y el hogar conectado ha alcanzado la madurez. Su hijo estudia digitalmente, con toda la información proporcionada a través de lentes digitales, aunque la educación se centra ahora en el procesamiento más que en la adquisición de conocimientos. Hoy pensamos que los datos son los reyes, pero su dominio del mundo solo crecerá.

Resila trabaja para Konsolidated Rubber and Logistics (KoRLo) Industries, una empresa de fabricación que ha evolucionado de forma experta para mantener su relevancia. Han sintetizado polímeros autorregenerativos que se utilizan en condiciones extremas, como en el fondo marino y en satélites de órbita terrestre baja. Los sensores de sus productos informan sobre el desgaste y las necesidades de mantenimiento, predicen fallos y proporcionan diagnósticos. La Industria 4.0 también ha alcanzado la madurez con el seguimiento de la cadena de suministro y las líneas de producción totalmente digitalizadas. Toda la TI de KoRLo está basada en la nube y los empleados humanos trabajan solo en la estrategia empresarial, respondiendo a las anomalías graves y verificando el trabajo automatizado.

Todo esto tiene lugar en la ciudad de New San Joban, un centro enfocado en la privacidad y el conocimiento tecnológico. Al igual que con la visión de las empresas y ciudadanos de 2030, el gobierno también está saturado de datos procedentes de los sensores de toda la ciudad. Qué hacer con todos los datos es una de las principales preocupaciones del ayuntamiento, así como garantizar su seguridad. El IoT Masivo (MIoT) y el 5G han conectado todo a través de una SIM, lo que ha provocado una mayor disparidad tecnológica entre los estados soberanos. La ciudad no tiene dinero en efectivo, ha prohibido los plásticos de un solo uso y el centro de la ciudad está libre de gasolina.

La conectividad y el mundo impulsado por los datos también han traído más atención a las protecciones de ciberseguridad y a las acciones judiciales de los comités internacionales. Sin embargo, todas estas normas y órganos de gobierno dependen de la participación, la implicación y el compromiso de cada país.

Ciberamenazas en 2030

Para 2030, la conectividad tendrá un impacto en todos los aspectos de la vida cotidiana, tanto a nivel físico como psicológico. Los actores de amenazas maliciosas también evolucionarán para usar y abusar de la innovación tecnológica, como siempre hacen.

Sobre la base de los escenarios descritos, las actividades delictivas pueden clasificarse en general como:

- Manipulación de datos
- Denegación de servicio/ interrupción
- Extorsión
- Operaciones de influencia
- Uso indebido de la capacidad de procesamiento
- Acceso no autorizado/intrusión
- Exposición de datos no autorizada
- Interceptación ilegal de comunicaciones/ transferencia de datos

A primera vista, estas categorías parecen muy similares a lo que nos enfrentamos hoy en día, y las amenazas básicas son bastante similares. Sin embargo, la automatización y la IA cambiarán la esencia de cómo funcionan este tipo de ataques.

El conocimiento y la comprensión están fuertemente dictados por algoritmos y resultados de búsqueda, lo que hace que la manipulación de datos y la desinformación sean vectores de ataque muy valiosos.

Los problemas de privacidad y vigilancia son un reto para gobiernos, empresas y particulares. Los beneficios de la conectividad y la disponibilidad de datos pueden verse eclipsados por su potencial de abuso.

Y el uso y abuso de la IA para automatizar ataques y envenenar conjuntos de datos puede afectar a todos los niveles de la sociedad.

Estos escenarios y sus amenazas asociadas requerirán cambios en el negocio y la regulación de la ciberseguridad. Todos, como profesionales de la ciberseguridad, debemos evolucionar nuestra tecnología y formación para prepararnos para un futuro en el que todo está conectado y en riesgo.

[SUM00_2030_Report_Executive_Summary_210527US]