La privacidad digital del futuro: previsiones de especialistas para la próxima década.

Cuando el tema es privacidad, el escenario nunca es el mismo. Amenazas y prioridades cambian constantemente. Entonces, ¿qué es lo que deben saber las empresas sobre lo que las espera en la próxima década?

AUTOR
Marco Preuss

Sea en celulares, smartwatches y hasta en otros gadgets. Hoy en día, nuestros datos personales están por toda parte. Recolectar informaciones personales hace que muchos servicios sean mejores y más prácticos para los usuarios pero, a lo largo de los años, hemos tenido múltiples casos de demuestran también los riesgos de este hábito que se ha hecho tan común.

Cuando el tema es privacidad de datos, es posible hacer una comparación con un río. Sí, un río. Porque uno nunca entra en el mismo río dos veces. El agua de un río está en constante movimiento. Así como las preocupaciones, amenazas y prioridades dentro del mundo de la seguridad digital. Pensando en eso, ¿cuáles serán las amenazas que nuestros datos enfrentarán en la próxima década?

Los especialistas de Kaspersky hicieron una lista con sus proyecciones y explican cómo las empresas pueden prepararse para enfrentar cada una de esas amenazas:

1. Gobiernos van a acceder a los datos de sus ciudadanos sin pedir permiso

Esto es algo que ya está pasando, pero que en los próximos años se va a hacer aún más común. Gobiernos alrededor del planeta tienden a crear leyes que los autoricen a acceder directamente a más y más datos e informaciones de sus ciudadanos. Y van a usar muchas excusas para eso, incluyendo cosas como terrorismo, inestabilidad de sistemas y hasta el hecho real de que esos datos ya son amplia y deliberadamente explotados por el sector privado.

2. La laguna entre reglamentación y realidad solo crecerá

Aunque las justificativas sean claras y entendibles, el aumento del acceso a datos privados de millones de personas conlleva muchos riesgos, como el uso no autorizado de esos datos y las fugas de datos.

Será un gran desafío para las autoridades regulatorias saber adaptar sus parámetros en la misma velocidad en la que avanzan las nuevas tecnologías. Las empresas también han sido lentas para cambiar el modo como tratan los datos de sus usuarios. El único cambio reciente significativo ha sido la práctica de pedirle al usuario su consentimiento sobre las cómo la empresa puede usar sus datos, un proceso que hoy en día ya se ha vuelto obligatorio en muchos países. Pero aún no es posible ver ninguna tendencia que direcciones hacia el aumento de la seguridad de datos sensibles de los usuarios.

O sea, cuando el tema es privacidad digital, ya existe una gran distancia entre las leyes y la realidad. Y esa laguna tiene todo para seguir creciendo, lo que hace que leyes y reglas parezcan cada vez menos eficaces.

3. Herramientas de contraataque crearán una guerra virtual por la privacidad.

Los probables escenarios citados anteriormente son un aliento para aquellos que desarrollan nuevas tecnologías de protección de privacidad. Esos especialistas van a adoptar nuevos métodos, pero nuevas amenazas serán creadas por los hackers para engañarles y así se dará inicio a una guerra virtual

Mientras tanto, los usuarios de tornarán más proactivos y curiosos acerca de su privacidad. Se creará una alta demanda por gerentes de contraseña, redes privadas (VPNs), y tokens (generadores automáticos de claves) para sistemas de identificación por dos factores (2FA).

Entretanto, ese tipo de mecanismo de protección solo se hace cargo de proteger la puerta del frente de una casa. Pero ataques y otros problemas también ocurren en los fondos, en el backend. Ese tipo de herramienta protege el ambiente local, pero no son un escudo eficiente contra ataques a sistemas como el almacenamiento en nube (cloud), por ejemplo. Y como las herramientas basadas en la nube están cada vez haciéndose más indispensables, los empleados de cada empresa también tendrán que entender donde están los riesgos. VPNs protegen contra algunos tipos de robo de datos, como la dirección IP y la geolocalización, por ejemplo, pero no te protegen contra usuarios que comparten datos con otros servicios, como Google y Facebook.

4. Seguiremos siendo engañados por diversión

“El crecimiento acelerado de videojuegos, tests y aplicaciones que hacen que el usuario comparta datos personales para poder divertirse es algo que no debería ser tan subestimado por las personas.”

Cibercriminales pueden usar ese tipo de estrategia para atacar empresas, robándole los datos personales a empleados que accedan a esos servicios y usando esos datos para acceder a sistemas e informaciones corporativas.

5. Veremos nuevos ataques a los procesos democráticos, pero también protección contra la desinformación.

Este tipo de ataque es algo que ya se ha hecho común en los últimos años y no existe un motivo evidente para que deje de ocurrir. Hoy en día ya existen tecnologías capaces de recrear la identidad visual y hasta la forma de hablar de una persona y, con las elecciones presidenciales de EEUU luego adelante, estos métodos deben robar la atención del público y ser explotados por los dos lados de la disputa.

"Pero donde hay una acción, también hay una reacción. Al mismo tiempo, podremos contar con nuevas herramientas para confrontar a los que tratan de manipular al público, sea con fake news, deep fakes o cualquier otra herramienta."

6. Proveedores del Internet de las Cosas (IoT) aumentarán sus inversiones en seguridad.

Los últimos años han sido turbulentos para la industria de la seguridad digital. Eso porque los ataques a objetos que utilizan el Internet de las Cosas, las filtraciones de datos y las campañas de desinformación y fake news se han vuelto cada vez más desafiadoras.

Esos fenómenos harán que los proveedores suban su nivel de colaboración entre empresas para el bien de la seguridad. Hace poco, Amazon, Apple, Google y Zigbee Alliance anunciaron la creación de un grupo de trabajo en conjunto para desarrollar y promover un sistema de conectividad gratis y libre de royalties. Eso hará con que los equipos que utilicen IoT sean más compatibles y tengan una base mucho más segura. Lo que se espera ahora es que otras empresas se sumen a esa corriente.

Con todo lo dicho arriba, es posible decir que estamos delante de una década muy interesante para la privacidad. Pero los desafíos son significativos y las empresas tendrán un rol fundamental para asegurar la privacidad de sus datos, no solo de sus empleados, pero también de sus consumidores.

La esperanza es que nuevas soluciones sean creadas rápidamente en respuesta a nuevas amenazas. Mientras tanto, todas las empresas pueden empezar haciendo su parte, al adoptar entrenamientos de seguridad y privacidad para sus empleados.