DICIEMBRE 2020 | N° 12-2020

HACKEOS, ROBOS DE CUENTAS Y EXTORSIONES: 6 PREDICCIONES DE CIBERSEGURIDAD PARA 2021

BOLETÍN INFORMATIVO LC/FT/FPADM

1. El ADN de la Ciberseguridad y el cuidado de la migración a la nube

Situación actual: la ciberseguridad se convirtió en el motor que acelera la migración a la llamada nube, por eso las compañías se preocupan por tener un acceso simple a este formato que prescinde de que la información se encuentre en una unidad de almacenamiento física. Predicción: la necesidad de contar con una plataforma convergente, digital y en la nube significa que veremos el surgimiento del "Zoom de la seguridad".¿Qué sería esto? Como descubrimos este año, Zoom "funciona" y eso es lo que se empezará a demandar en las compañías: que la seguridad esté tan arraigada en las aplicaciones y plataformas al punto que las personas ya no se den cuenta de que están siendo "protegidas". La nube se volverá parte del ADN de la ciberseguridad, de una forma en que hoy no lo es.

2. Machine learning: objetividad bajo la lupa

Situación actual: Las tendencias en el trabajo remoto significan que el monitoreo es más necesario que nunca y debe gestionarse con machine learning. Predicción: en 2021 el aprendizaje automatizado y la analítica estarán sometidos a un escrutinio aún mayor, ya que se cuestionará la confianza en su naturaleza imparcial y justa, así como sus límites éticos. Para crear sistemas cibernéticos que ayuden a identificar a los usuarios riesgosos y eviten acciones perjudiciales, los datos que se analizan provienen en su mayor parte de estudiar las actividades de los usuarios, su comportamiento. Al realizar este análisis hay que usar una combinación de algoritmos e inteligencia humana. Sin el aporte de la intuición, los conocimientos, el contexto y la comprensión de la psicología humana, se corre el riesgo de crear algoritmos sesgados o de tomar decisiones basadas en datos tendenciosos o con fallas. 2021 será un año en el se incrementarán los ataques. No estarán dirigidos solamente a industrias, como las financiera y el retail, apuntarán al usuario. Al robo de identidad a través de campañas de fake news y phising, modalidad que aumentó un 600% bajo pandemia, se escucharán mucho.

El año del coronavirus fue también, a fin de cuentas, el de los hackeos y los problemas de seguridad informática. Con casos emblemáticos como el de Migraciones en Argentina, Garmin en todo el mundo, Capcom en Japón, y hasta un ransomware que terminó con una víctima fatal en Alemania, el panorama no es el mejor para 2021. O al menos eso anticipan algunas consultoras.

3. La Seguridad, diseñada para el comportamiento humano

Situación actual: Los cambios generados por la pandemia actual revelaron debilidades en las herramientas y protocolos de seguridad para trabajadores remotos. Predicción: en la industria de la ciberseguridad, la observación y la comprensión de los comportamientos deben ir acompañados del contexto. "Queremos que las personas puedan hacer su trabajo dentro de las limitaciones de nuestra red y políticas corporativas, por lo que bloquearlas solo fomentaría la tendencia humana a encontrar una ruta más fácil (¡y menos segura!) para hacer su trabajo", explican desde Forcepoint. "Con un equipo de investigación interdisciplinario, que reúne a expertos de seguridad, contrainteligencia, TI y ciencias conductuales, la comprensión del comportamiento se puede integrar a los sistemas de ciberseguridad", agregan.

4. La desinformación y las fake news

Situación actual: las campañas de desinformación son fáciles y de bajo costo de implementar, mientras que el riesgo y las sanciones son casi inexistentes; y peor aún las personas continúan creyendo al pie de la letra lo que leen; sin ninguna investigación adicional. Predicción: para 2021, y en adelante, la desinformación seguirá aumentando en enfoque y alcance. Históricamente hablando, la innovación está impulsada en gran medida por la necesidad.Si bien la desinformación es una amenaza grande y creciente, es interesante pensar qué nueva tecnología podría surgir a partir de que los expertos plantean el tema a niveles gubernamentales, o cómo las redes sociales pueden evolucionar para enfrentar este desafío urgente.

5. Identidades sintéticas, una nueva amenaza

Situación actual: según la consultora McKinsey, el fraude mediante identidades sintéticas es el tipo de crimen financiero de mayor crecimiento en los Estados Unidos y se está ampliando a otras geografías. Los estafadores sintéticos utilizan credenciales reales y falsas para crear un perfil falso lo suficientemente creíble para solicitar créditos. Predicción: surgirán células organizadas de infiltrados de reclutamiento que faciliten el que ofrezcan personas con malas intenciones se conviertan en empleados confiables, con el objetivo de exfiltrar propiedad intelectual (IP) incalculable. El problema para detectar este tipo de fraude mediante aprendizaje automatizado radica en el definir el conjunto de datos con el cual se lo entrena. Esto significa que hay que ir más profundo y comprobar la identidad con fuentes de datos de terceros que demuestren un historial congruente. "Vemos muchos casos de robo de datos por parte de empleados que creen que no serán descubiertos y, por otro lado, una gran cantidad de fugas de datos causadas por el error humano o una mala administración de seguridad", aseguran desde Forcepoint. El ser humano es el nuevo perímetro de la ciberseguridad, es el eslabón más débil dentro de la cadena, por lo que es esencial educar para prevenir ataques, contemplando una constante capacitación al personal.

6. Monitoreo del usuario en tiempo real

Situación actual: Casi de la noche a la mañana, las organizaciones cambiaron de una fuerza laboral predominantemente basada en una oficina a trabajadores remotos. El antiguo perímetro de seguridad claramente desapareció, los datos debieron ser más accesibles que nunca. En 2021, saldrá a la luz la cantidad de propiedad intelectual robada por atacantes externos y/o personas internas malintencionadas -uno de los problemas más grandes- durante el trabajo remoto de 2020. Predicción: la visibilidad de los datos y la gestión de la protección de éstos será el imperativo de ciberseguridad más importante para las empresas en 2021, para trabajar de forma segura, independientemente de la ubicación. "Para detener la fuga de datos, necesitamos saber exactamente dónde están minuto a minuto. Lo que significa que se debe introducir el monitoreo de la actividad del usuario en tiempo real", explican. "La transparencia en la implementación de estas soluciones y la consideración cuidadosa de la privacidad del usuario deben ser el núcleo de cualquier solución de monitoreo de la actividad", cierran.