Ciberseguridad en 2021: El poder de la visibilidad y la reacción rápida

En este momento se están enviando en el mundo más de 152 mil millones de emails y el número no para de crecer. Y dentro de todos esos correos que van y vienen, hay algunos que tienen el potencial de **poner en riesgo los datos corporativos**: los de *phishing*. Todas las semanas y a veces en varios días consecutivos recibo emails de bancos en los que no tengo cuenta tratando de que ingrese mis datos personales o haga click en un link; si miro la dirección de correo del emisor fácilmente me doy cuenta de que ni siquiera fueron enviados por esas instituciones.

Pero en el mundo de las estrategias para captar usuarios vulnerables, la ingeniería social se vuelve cada vez más sofisticada. ¿Qué pasa si el email que recibes es de un banco en el que sí tienes cuenta? ¿De un servicio que sí utilizas? O incluso, ¿qué pasa si es de la misma empresa en la que trabajas? Y el panorama se pone más complejo aún si el *look and feel* de esos emails es prácticamente idéntico a los reales de esas organizaciones. En definitiva, cada vez es más probable que caigamos en una trampa. Y en el contexto actual somos **doblemente objetivo de hackers**: para acceder a nuestros datos personales, pero también para usarnos como medio para atacar a las organizaciones en las que trabajamos.

El teletrabajo amplió la superficie de ataque al diversificar exponencialmente los puntos de acceso a la información y las redes que utilizamos para conectarnos. Y si bien es importante que los colaboradores tengan conocimiento sobre **proteger los datos** y tengan conciencia situacional, el rol central en la protección de datos lo tiene la tecnología.

¿Escucharon alguna vez la frase “Ojos que no ven, corazón que no siente”? Bueno, en seguridad no aplica. Tengamos o no visibilidad de lo que sucede, se termina sufriendo igual. Por eso ganar visibilidad y poder de reacción tiene que ser el norte en la estrategia de cada departamento de TI. Las **arquitecturas basadas en confianza cero** *(ZeroTrust)* son parte de la solución; Zero Trust evalúa constantemente la confianza en cada punto de contacto verificando que el perímetro digital seguro se encuentre íntegro. Pero las soluciones basadas en *machine learning* también tienen mucho para aportar en este sentido.

Usando *machine learning* el primer paso es armar un perfil de cada usuario. Al aprender cómo trabajan usualmente, a qué hora se conectan, a qué tipo de documentos acceden, a qué hora terminan su jornada laboral, entre otros factores, será más fácil **identificar posibles amenazas**. Una vez que los perfiles de cada usuario están establecidos el sistema podrá monitorear e identificar comportamientos anómalos en tiempo real. Y poner en marcha medidas inmediatas para defender los datos, que van desde bloquear temporalmente cuentas de usuario, hacer que expiren links a documentos compartidos, grabar la sesión, notificar a los usuarios que su comportamiento ha generado inquietudes respecto a la seguridad y muchas más.

La tecnología permite recuperar la visibilidad que se cree perdida cuando los empleados ya no trabajan en el edificio corporativo. Brinda datos y permite monitorear la seguridad de forma proactiva con un enfoque “Always on”. Si pensamos que el trabajo remoto llegó para quedarse adaptar la infraestructura es clave no sólo para mejorar la experiencia de trabajo sino para

proteger los datos en un contexto de amenazas a la seguridad en constante evolución. Mientras tanto, se siguen enviando emails buscando captar usuarios desprevenidos.