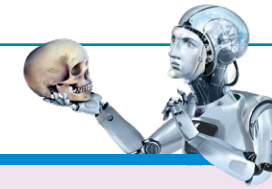
CAVILACIONES SEGURAS



Cómo sopla el lobo

Joseph Jacobs, allá por el siglo XIX, el historiador que popularizó el cuento de los tres cerditos, nos dejó una de las mejores lecciones sobre gestión de riesgos y resiliencia.

En el cuento, la amenaza es un lobo con una capacidad de soplido devastadora. En nuestro mundo, el de la ciberseguridad, había una vez tres CISOs que intentaban proteger sus activos frente a un lobo cada vez más astuto, al tanto de los últimos desarrollos tecnológicos, y con grandes contactos en el mundo de la ciberdelincuencia. Todo un as encontrando la mínima grieta para entrar en nuestras compañías.

El primer CISO, un romántico de la vieja escuela, construyó su estrategia con una seguridad perimetral básica. Era una infraestructura rápida de desplegar, fácilmente administrable y ya conocida desde los antiguos años noventa. Conseguía así una falsa sensación de seguridad.

"La moraleja es clara: en la era de los modelos frontera, sólo aquel CISO que utilice la IA como aliado para reforzar sus cimientos podrá dormir tranquilo cuando el lobo empiece a soplar. Porque el lobo, créanme, va a soplar. Bueno, ya está soplando".

Sin embargo, en el panorama actual, la ilusión de un perímetro seguro es tan frágil como la casita de paja del cerdito menos trabajador ante un atacante que sabe que el "dentro" y el "fuera" son conceptos ya superados.

El segundo CISO decidió que la casita de paja no era suficiente y optó por la madera. Su casa es más robusta: no solo tiene seguridad perimetral, sino que también ha implementado una buena gestión de identidades y una segmentación de red. Aprendió su lección con incidentes incunables como Wannacry, NotPetya y Solarwinds. Es una defensa sólida, pero la madera sigue siendo combustible ante las nuevas chispas tecnológicas.

Finalmente, llegamos al CISO más preparado, aquel que ha entendido que su función no es sólo construir muros, sino dotar a su arquitectura de resiliencia. Este CISO ha levantado su casa con ladrillo y, digamos, hormigón armado, integrando la Inteligencia Artificial de forma transversal en todos sus procesos de seguridad, desde el control de accesos hasta el ciclo de vida de desarrollo seguro (DevSecOps).

¿Por qué es tan crítico este último enfoque? Porque el "lobo" ha evolucionado. La llegada de los nuevos modelos frontera de IA, como Mythos de Anthropic o la versión 5.5 de ChatGPT de OpenAI, ha cambiado las reglas del juego. Estas herramientas poseen capacidades de detección de vulnerabilidades y de explotación automática que hacen que el soplido del lobo sea ahora letal.

Para que el lobo no pueda bajar por la chimenea de nuestra "casa de ladrillo", las organizaciones deben acometer cinco grandes esfuerzos: (**1**) En la red, hay que implementar ya arquitecturas de **confianza cero** (*zero trust)*, no basta con segmentar; debemos implementar una microsegmentación profunda donde la confianza nunca se asuma y siempre se verifique. (**2**) En los cambios, una **gestión de parches** casi perfecta: la IA del atacante encontrará el *exploit* en muy poco tiempo. Nuestra capacidad de respuesta en la actualización de software y aplicación de parches debe ser casi inmediata y eficiente. (**3**) En nuestra **monitorización**, hemos de alcanzar **observabilidad**: ya no nos sirve saber si un sistema está "vivo" y "funcionando". Necesitamos conocer el estado interno de nuestros sistemas a partir de los datos que generan y detectar anomalías antes de que se conviertan en incidentes. (**4**) En nuestro **software**, necesitamos saber que ha sido **desarrollado de modo seguro**. Para ello, seamos prácticos, vamos a tener que utilizar esos modelos de IA que usan los malos para atacarnos. (**5**) Finalmente, aceptémoslo, en algunas ocasiones, esperemos que pocas, el lobo logrará entrar por nuestra chimenea. Así qué, necesitamos una **gestión de crisis** a prueba de incidentes críticos: debemos sacar sobresaliente en resiliencia.

En esta nueva entrega de mis "cavilaciones", la moraleja es clara: en la era de los modelos frontera, sólo aquel CISO que utilice la IA como aliado para reforzar sus cimientos podrá dormir tranquilo cuando el lobo empiece a soplar. Porque el lobo, créanme, va a soplar. Bueno, ya está soplando.

Dr. Alberto Partida

linkedin.com/in/albertopartida