Deloitte.

Amenazas en el mundo de la seguridad de ATM

Por ***Marcelo Díaz***

Las amenazas dirigidas a los cajeros automáticos o ATM, por sus siglas en inglés, siguen al alza. Ciertamente, durante el período de pandemia, fue uno de los pocos sectores de la ciberseguridad que vio disminuido su impacto, pero hoy nuevamente vuelve a aumentar. En 2021, el número de dispositivos encontrados con malware para cajeros automáticos y terminales de punto de venta (POS) aumentó un 39%.

Asimismo, el skimming y el shimming de tarjetas de cajero automático siguen siendo una amenaza persistente, pues muchos cajeros automáticos aún no están protegidos de manera efectiva. Además, hay otros factores que inciden como el fraude transfronterizo, el que todavía existan tarjetas con bandas magnéticas y que las técnicas de robo continúan evolucionando, por mencionar algunos.

En ese escenario, para una red de cajeros automáticos a nivel nacional es vital no solo tener la mejor tecnología disponible en el mercado, sino también el conocimiento y la flexibilidad para atender cualquier contingencia, así como la mantención permanente.

A pesar de los avances en esta materia, lo cierto es que ésta es un área crítica, sobre todo en ciertos períodos del año como fiestas patrias, navidad y vacaciones. El año pasado, de hecho, se hizo un total de tres mil 354 denuncias ante la PDI por el delito de uso fraudulento de tarjetas de débito y crédito a nivel nacional.

En la actualidad, la tendencia es que los delincuentes no solo buscan deshabilitar los cajeros que tienen sistemas antiskimming para obligar a los usuarios a acudir a otro más cercano que esté intervenido para capturar la información de la tarjeta, también están atacando los sistemas integrados utilizados en los cajeros automáticos y terminales de punto de venta. De esa manera, además de robar dinero, también se adueñan de credenciales de tarjetas de crédito y datos personales, y consiguen por esa vía entrar a los sistemas y tomar el control de los dispositivos de una red.

Hoy con gran el impulso tecnológico de la Internet de las Cosas, IoT, además de los cajeros automáticos y los POS, también se debe poner atención en los controles de acceso, las cámaras de vigilancia, las bóvedas de seguridad, entre mucho más, para lo cual la tecnología de avanzada presenta un gran abanico de opciones, como la seguridad biométrica, por dar un ejemplo. **Lo importante es no desatender ninguna arista, pues los ciberdelincuentes buscan cualquier brecha. La ciberseguridad es un desafío permanente.**