Akamai alerta de ciberdelincuentes en este año

Para Josh Shaul, vicepresidente de Productos de Seguridad Web de Akamai, l**os datos de los consumidores en internet, es el principal botín que buscarán los delincuentes informáticos desde la primera semana de este nuevo año.**

Asegura que los **piratas informáticos suelen robar nombres de usuario y contraseñas**. "El propósito final es ganar dinero, la mayoría de las veces mediante la **compra fraudulenta de bienes que pueden venderse en el mercado negro**. Y el fraude potencial no se limita a la empresa violada, sino que se extiende a otras empresas en línea".

Pero, ¿qué tipos de organizaciones son los objetivos probables de los ataques de robo de datos de clientes?

"En primer lugar, **ninguna empresa u organización es inmune al ataque cibernético**, por lo que todos los que hacen negocios en línea y almacenan datos de clientes son vulnerables. A los ciberdelincuentes les gustaría ir donde haya muchos datos potencialmente valiosos. Eso significa que las otras agencias de crédito, las principales compañías de tarjetas de crédito, y ahora compañías como LifeLock, la compañía de protección contra el robo de identidad que ha estado publicitando mucho y agregando clientes a raíz de las recientes infracciones. Por ejemplo, **Equifax fue violado, pero uno esperaría que estas organizaciones tengan una seguridad militar, y no es así**", explica Shaul.

Los ciberdelincuentes, dice, como el proverbial ladrón de bancos, también querrían ir donde está el dinero, pero las principales instituciones de servicios financieros invierten mucho para mantener esa seguridad de grado militar. "Están protegiendo sus activos, operaciones y clientes corporativos e individuales de alto valor. Los clientes minoristas regulares se benefician del nivel de seguridad existente".

Alertas

Para el especialista en ciberseguridad de Akamai, **las más vulnerables son las empresas como los grandes minoristas que tienen gran cantidad de datos de consumidores**, pero no los márgenes de beneficio y la financiación, o quizás no la motivación, para aplicar la protección que podrían tener.

"Existe una **discrepancia entre el valor de los datos a proteger y la seguridad que pueden pagar**. Estas organizaciones deberían reevaluar sus posturas y estrategias de seguridad a la luz de la violación de Equifax y la cantidad de datos sobre sus clientes que ya están comprometidos.

"En el lado del gobierno, **el IRS es probablemente el objetivo más grande**. Tienen la información de todos y tienen casi toda la información que un estafador podría pedir. Por supuesto, tienen una seguridad muy sólida, tanto para proteger los datos como para detectar el robo de identidad. Pero

no han sido perfectos. Las agencias que dispersan los beneficios, como Medicare, parecen ser mejores en la protección de datos que en prevenir el fraude, pero su desafío se complica por el hecho de que las reclamaciones fraudulentas toman muchas formas", explica.

Una industria en una posición difícil es la salud. Las organizaciones de proveedores y los intercambios tienen una enorme cantidad de información personal de las personas además de la información clínica en sus registros de salud electrónicos.

"Están bajo una gran presión para proteger los datos personales de los pacientes. Pero también tienen una tensión fundamental entre los gastos clínicos y otros. Los médicos y las organizaciones de proveedores se centran en los resultados de los pacientes, es la forma en que están conectados. Así que **prefieren gastar en tecnología clínica en lugar de información o tecnología de seguridad**", agrega.

Reitera que **los hackers son pescadores submarinos que buscan peces grandes**. "Pero también están trabajando constantemente en segundo plano, lanzando una amplia red y esperando pacientemente a que los peces salgan a la superficie, incluidas las vulnerabilidades antiguas parcheadas de forma incompleta".