Autor:

Jon Maier

Fecha: 22/04/2022
Tema: Alfa conversacional

Alfa conversacional: Ciberseguridad de Niza a una tecnología esencial

En el mundo digital actual, los datos son oro y más actores maliciosos están intentando conseguir el premio. Recientemente, dos empresas de tecnología pesada proporcionaron datos de clientes a *hackers* que se hicieron pasar por agentes de la ley que demuestran que sus defensas cibernéticas no son tan sólidas como deberían[1]. Esto planteó preocupaciones, que se vieron exacerbadas por el componente de guerra cibernética del ataque de Putin a Ucrania, generando tensión en la periferia en individuos, empresas y gobiernos que se preguntan quién puede estar acechando dentro de sus redes. En respuesta, la administración de Biden advirtió a las empresas de niveles potencialmente más altos de cibercrimen relacionados con sanciones impuestas por el Oeste y tensas relaciones geopolíticas[2]. En este entorno, nadie puede escapar de los ciberataques, pero pueden trabajar para prevenirlos. Como resultado, esperamos que el gasto en ciberseguridad siga aumentando y que las empresas de ciberseguridad atraigan el interés de los inversores debido a su modelo de ingresos recurrentes. En nuestra opinión, estos factores, junto con la capacidad del tema de ciberseguridad para ayudar a gestionar el riesgo geopolítico en una cartera, hacen que esta exposición sea esencial.

Aspectos clave

- Esperamos que los planes de acción públicos y privados que ayudan a prevenir el cibercrimen aumenten en su alcance y den lugar a un mayor gasto sostenido en ciberseguridad. Una empresa de investigación líder predice que el gasto global en ciberseguridad superará los 1,75 billones de USD, de forma acumulativa, entre 2021 y 2025[3].
- La Administración de Biden ha aumentado su mensaje de urgencia a las empresas estadounidenses con respecto a la necesidad de protegerse contra los ciberataques que tienen un impacto en los gobiernos, contratistas gubernamentales y empresas privadas por igual. Es probable que la implicación posterior sea un mayor gasto en ciberseguridad.
- La exposición al tema de la ciberseguridad trae consigo la actitud defensiva de los ingresos recurrentes constantes y el potencial de crecimiento asociado con las respuestas del sector público y privado a comportamientos cibercriminales cada vez más sofisticados.

El truco de SolarWinds fue una llamada a la acción

El jaqueo de SolarWinds descubierto en diciembre de 2020 fue un momento clave para la ciberseguridad. Se cree que este jaqueo es obra del servicio de inteligencia exterior de Rusia. Como antecedentes, unas 100 empresas y una docena de agencias gubernamentales se vieron comprometidas, incluidos los departamentos de Tesorería, Justicia y Energía de los EE. UU., así como el Pentágono[4]. El ataque fue una llamada de atención sobre lo invasiva y generalizada que pueden ser las implicaciones, especialmente cuando los atacantes ponen en peligro el software más utilizado. La administración de Biden comprende la necesidad de modernizar las defensas de ciberseguridad y actualizar los requisitos de seguridad para las organizaciones que contratan con el Gobierno de EE. UU.[5] A la luz de la agresión rusa a Ucrania, la administración de Biden aumentó su mensaje de urgencia a las empresas estadounidenses con respecto a la necesidad de protegerse contra los ciberataques. Las implicaciones posteriores probablemente serán un mayor gasto en ciberseguridad.

Y luego hubo una guerra y más gastos en ciberseguridad

Las recientes amenazas de ciberseguridad dirigidas a bancos y departamentos gubernamentales ucranianos llevan el tema de la ciberseguridad a la primera línea de la guerra. Para ayudar a defender a Ucrania de los ciberataques, la Unión Europea proporcionó un equipo de respuesta cibernética rápida compuesto por expertos de Lituania, Croacia, Polonia, Estonia, Rumanía y los Países Bajos. El sector privado también está colaborando. Justo antes de la invasión de Putin, el Centro de Inteligencia sobre Amenazas de Microsoft identificó actividad inusual dirigida a los departamentos gubernamentales e instituciones financieras de Ucrania y rápidamente se involucró en su divulgación[6]. Alphabet también ha sido clave para prevenir los ciberataques en Ucrania[7].

Estas respuestas se asemejan a los planes de acción públicos y privados iniciados por la Administración de Biden para proteger los sectores de electricidad, gasoductos y agua en los Estados Unidos, y para utilizar la autoridad

gubernamental para exigir nuevas medidas de ciberseguridad y defensa de red[8]. El objetivo de la administración de modernizar las defensas cibernéticas también incluye la cooperación continua con numerosos aliados y socios internacionales para frustrar las huelgas de *ransomware* y atribuir públicamente la actividad cibercriminal[9].

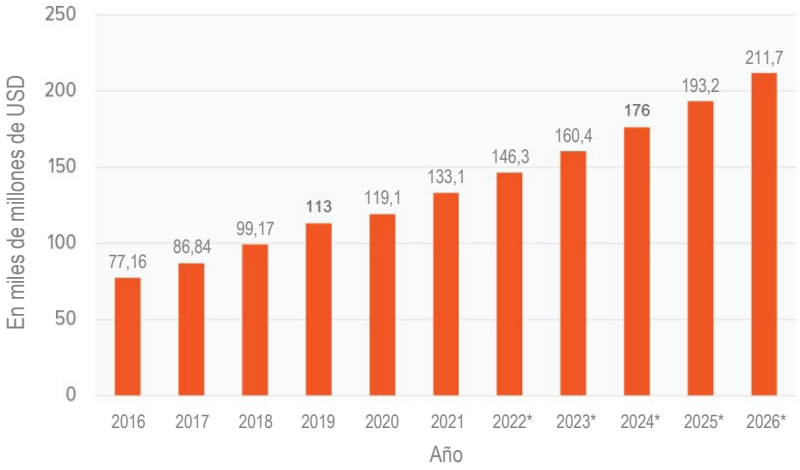
La estrecha coordinación del sector tecnológico con el gobierno de Ucrania, la UE y la Organización del Tratado del Atlántico Norte (OTAN) no tiene precedentes en cuanto a su alcance y ritmo. La respuesta habla del avance de la tecnología cibernética y el papel fundamental que desempeña en la economía global. Esperamos que los esfuerzos como estos continúen y probablemente aumenten el gasto en ciberseguridad, ya que el cibercrimen es un riesgo que persiste.

La ciberseguridad podría ser una oportunidad de alto crecimiento

La guerra en Ucrania y las máquinas geopolíticas asociadas llaman la atención sobre la importancia de una fuerte defensa cibernética. Los pedidos ejecutivos y la nueva estrategia de ciberseguridad de la Casa Blanca probablemente aumentarán la adopción, especialmente cuando hay planes de supervisión gubernamental y normas que exigen estándares mínimos[10]. Creemos que es probable que el cambio de la ciberseguridad de una inversión voluntaria a una inversión regulada necesaria para hacer negocios aumente la rápida adopción en EE. UU., Europa, y en otros lugares[11]. La protección absoluta de los datos es ambiciosa dada la compensación directa entre la seguridad de los datos y la accesibilidad, pero el gasto en ciberseguridad, que probablemente continúe creciendo puede mitigar los riesgos, y este tema debería considerarse para una cartera más amplia.

INGRESOS GLOBALES DE CIBERSEGURIDAD

Fuente: Datos de Statista a marzo de 2022



Año	Tasa de crecimiento
2017	12,55 %
2018	14,20 %
2019	13,95 %
2020	5,40%
2021	11,75%
2022*	9,92%
2023*	9,64%
2024*	9,73%
2025*	9,77%
2026*	9,58%

* Datos previstos

Nota: Los datos mostrados aún no reflejan los impactos en el mercado de la guerra entre Rusia y Ucrania.

Un ETF de ciberseguridad puede añadir resiliencia a una cartera

Las tecnologías de ciberseguridad trabajan para proteger proactivamente contra posibles ataques mientras mitigan y reparan los daños de los incidentes que ya han ocurrido. El aumento de la incidencia y la gravedad de los ciberataques demuestran la necesidad permanente de gasto en ciberseguridad. Para las empresas de ciberseguridad, esta necesidad cada vez más imperiosa crea un modelo de negocio que genera ingresos recurrentes sólidos. Como resultado, al invertir en el nivel más amplio de este tema, los inversores pueden diversificar su exposición entre empresas porque es poco probable que los factores que impulsan la adopción disminuyan pronto.

Siempre es difícil elegir al ganador en cualquier sector o tema. Si bien se requiere información detallada para elegir de manera efectiva una empresa individual que podría superar al mercado, invertir en un tema podría llevar a los inversores hacia un ETF, donde se puede diversificar su riesgo. Dado que las acciones de ciberseguridad pueden aumentar el rendimiento de los precios tras el anuncio de piratería a gran escala, o bajar si un desarrollador de aplicaciones es víctima de una gran violación, un ETF podría ser una buena solución diversificada.

Notas al pie:

[1] FICHA TÉCNICA de la Casa Blanca: Actúe ahora para protegerse contra posibles ciberataques, 21/03/2022

[2] FICHA TÉCNICA de la Casa Blanca: Actúe ahora para protegerse contra posibles ciberataques, 21/03/2022

[3] Empresas de ciberseguridad, Gasto en ciberseguridad global para superar los 1,75 billones de USD entre 2021 y 2025, 10/9/2021

[4] NPR, un ciberataque “peor pesadilla”: La historia incontable del SolarWinds Hack, 16/04/21

[5] NPR, un ciberataque “peor pesadilla”: La historia incontable del SolarWinds Hack, 16/04/21

[6] Agencia de ciberseguridad y seguridad de infraestructuras, organizaciones objetivo de malware destructivo en Ucrania, 01/03/2022

[7] Chamber Business News, a medida que crecen las amenazas, los expertos evalúan la preparación del gobierno y del sector privado para los ciberataques, 24 de marzo de 2022

[8] NYT, a medida que los tanques avanzaban hacia Ucrania, también lo hizo el malware. A continuación, Microsoft entró en la guerra el 28/02/2022

[9] CSIS, una responsabilidad compartida: Cooperación público-privada para la ciberseguridad, 22/03/2022

[10] Revisión tecnológica del MIT, dentro del plan para solucionar los interminables fallos de ciberseguridad de Estados Unidos, 18 de marzo de 2022

[11] Reuters, UE propone reglas de ciberseguridad para los organismos de la UE en medio de las preocupaciones de ciberseguridad, 22 de marzo de 2022