NOTA DE FUTURO 1/2019

18 de marzo de 2019

José González Portero, Sergio Galache Gómez,
Loreto Machés Blázquez y Pilar Rogi Minguell[*]

Tendencias Cibernéticas y Geopolíticas 2019

Tendencias Cibernéticas y Geopolíticas 2019

Siete aspectos geopolíticos importantes para 2019

2019 annual forecast geopolitics intelligence global risk

1. La competencia entre las grandes potencias se intensificará en 2019

Estados Unidos aumentará su ofensiva estratégica contra China mediante aranceles y sanciones en tecnologías emergentes, un mayor apoyo a Taiwán y una postura más firme en el mar del sur de China. Así mismo, el fracaso de acuerdos sobre el control de armas acelerará la guerra armamentística entre Estados Unidos, Rusia y China. El actual panorama geopolítico proporcionará oportunidades estratégicas a potencias fronterizas más débiles como Polonia o Taiwán, no obstante, también causará un quebradero de cabeza a potencias intermedias que intenten encontrar un punto medio como Turquía, India y Vietnam.

2. Aumentará el riesgo geopolítico para el comercio

Alegando amenazas a la seguridad nacional, Estados Unidos se apoyará en Europa, Japón, Australia, Canadá, Corea del Sur y Taiwán para dificultar las inversiones chinas. Esto afectará a la investigación y el comercio en áreas estratégicas, desde la inteligencia artificial hasta el despliegue del 5G que comenzará en 2019. El imperativo de China de ponerse al día en ámbitos fundamentales como el área aeroespacial y el desarrollo de semiconductores de alta calidad solo aumentará las amenazas cibernéticas a empresas y obligará al desarrollo de una política estadounidense en ciberseguridad mucho más ofensiva.

* Alumnos en prácticas de la Universidad Pontificia de Comillas

3. Volatilidad comercial en la era de la economía global

Un posible enfrentamiento entre Estados Unidos y la Organización Mundial del Comercio podría paralizar el proceso de resolución de disputas de la institución y forzar a los países a resolver sus diferencias comerciales mediante una vía bilateral mucho menos predecible.

Canadá, México, Japón y Corea del Sur tienen una mejor oportunidad de negociar cuotas para reducir las amenazas de los aranceles de Estados Unidos. No obstante, las conversaciones comerciales entre la Unión Europea y Estados Unidos están condenadas a fracasar. Alemania será el país que más perderá en una posible batalla comercial automovilística con Estados Unidos. No obstante, este último no será capaz de forzar a la UE a realizar concesiones en la agricultura para satisfacer a la Casa Blanca. A su vez, a pesar de que los aranceles que Estados Unidos ha impuesto a China aumentarán la incertidumbre del comercio, el efecto global que podrá tener la política comercial de la Casa Blanca en 2019 en la economía global será silenciado.

4. Italia y el brexit

El desafiante gobierno populista de Italia representará la mayor amenaza para la zona euro en 2019 a medida que crece la preocupación sobre el aumento de los niveles de deuda del país y su frágil sistema bancario. Así mismo, Bruselas trabajará simultáneamente con el Reino Unido para conseguir un acuerdo del *brexit*, pero el veto parlamentario británico es el principal obstáculo para la salida del país de la Unión Europea.

5. Los próximos pasos en la campaña anti-Irán

Mediante unas segundas sanciones ambiciosas, Estados Unidos procurará aislar de forma regional a Irán y debilitar al país desde dentro. Esto creará tensión entre Washington y Teherán y reducirá la ya de por si débil posibilidad de alcanzar una negociación constructiva. Una agenda en común para debilitar a Irán ayudará a trazar lazos estratégicos y de alto nivel entre Estados Unidos y Arabia Saudí, a pesar de los sucesos en la familia real y el descontento de gobiernos extranjeros con el reinado del príncipe Mahammed bin Salaman. Así mismo, el caso Khashoggi estará presente en la Casa Blanca en 2019.

6. El aumento de la oferta en el mercado energético global

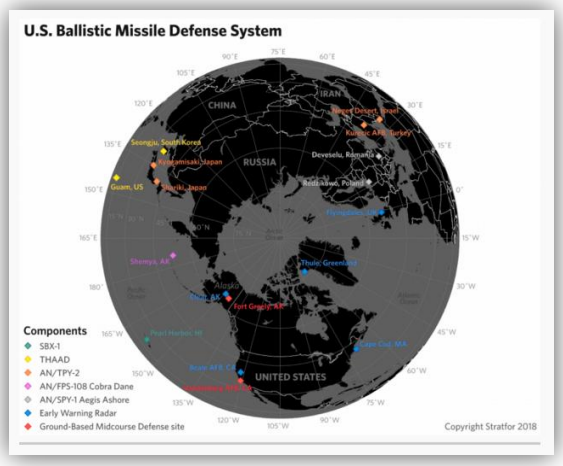
Será muy improbable que se produzca un colapso en el mercado del petróleo en la primera mitad de 2019, ya que la exportación de petróleo de Irán está limitada por sanciones y las restricciones de los

oleoductos limitan el aumento de producción de Estados Unidos. Sin embargo, la gráfica de la oferta se desplazará por completo en la segunda mitad del año cuando la capacidad de los oleoductos de Estados Unidos aumente.

Arabia Saudí y Rusia controlarán la oferta del petróleo para impedir un descenso del precio al vigilar los efectos de las exportaciones residuales de Irán en el mercado. El mercado global de gas natural licuado experimentará un cambio cuando Estados Unidos asuma su puesto entre los top tres exportadores GNL del mundo en 2019.

7. Etiopía está cambiando el Cuerno de África

La ambiciosa agenda de Etiopía está generando interés económico y está atrayendo a potencias extranjeras al Cuerno de África. No obstante, las amenazas internas al actual gobierno y conflictos étnicos amenazan con reducir el impulso de Addis Ababa.



CIODIVE

https://www.ciodive.com/news/2019-trends-security-limited-to-the-perimeter-offers-minimal-safety/544554/?sf205754590=1

Cinco aspectos de seguridad que las empresas no podrán perder de vista en 2019

1. Los cibercriminales están uniendo sus fuerzas

Las empresas tendrán que asumir que los cibercriminales debatirán sobre posibles alianzas y colaboraciones entre ellos en la *dark web*. Las comunidades delictivas más grandes atraen el interés de aquellas con una capacidad menor, hecho que supondrá la extinción de las familias más pequeñas. Las comunidades grandes son conscientes de este hecho y anuncian sus servicios con el fin de no tener que llevar a cabo ellos mismo el ataque, sino aquellos aliados que se les unen.

2. Modelo de seguridad: Zero Trust

Las empresas que emplean el modelo de seguridad Zero Trust (confianza cero en español) asumen que no se pueden fiar de todo lo que está en su red. Una serie de medidas que contribuyen al

desarrollo de una efectiva política de seguridad Zero Trust son: la aplicación de controles de acceso, garantizar la accesibilidad en función de los empleados y mejorar las soluciones de autenticación.

3. Las campañas de desinformación correrán como la pólvora

Las campañas que llevan a cabo actores maliciosos ponen en riesgo a los empleados y suponen un problema para los equipos de TI. Las empresas tienen que estar preparadas para posibles consecuencias relacionadas con campañas de desinformación. Sobre todo aquellas empresas que tienen una presencia en las redes sociales deben estar alerta con lo que respecta a la seguridad de sus cuentas.

4. Automatización o desaparición

Con la llegada de la automatización al campo de la ciberseguridad, las empresas tendrán una menor carga con las ciberamenazas, ya que los sistemas de inteligencia podrán adaptarse de una forma más efectiva a los ataques a medida que aprenden del comportamiento de los usuarios. A su vez, son cada vez más proveedores de seguridad, en sectores de gestión de identidad o seguridad en la nube, los que están optando por incorporar inteligencia artificial y aprendizaje automático en sus servicios.

5. Destapar las amenazas en la cadena logística

La cadena logística expone a las empresas en su punto más débil en ciberseguridad. Actores maliciosos no discriminan en función del tamaño de una empresa y saben que muchas de ellas no invierten el tiempo suficiente en la seguridad de terceros. Debido a esto, las empresas deben estudiar y entender la fiabilidad de sus terceros actores.

DarkReading

https://www.darkreading.com/vulnerabilities---threats/advanced-phishing-scenarios-you-will-most-likely-encounter-this-year/a/d-id/1333632

Los escenarios avanzados de phishing que encontrará en 2019

El delito ciber por correo electrónico, como el BEC (*business email compromise*), el *spear phishing* y el *ransomware* no desaparecerán en el año 2019.

El 2018 ha sido otro año récord en ciberataques y las empresas deberán esperar muchos más en 2019. Los estafadores, que continúan priorizando los correos electrónicos como su vector de ataque,

están aumentando el uso de técnicas *de phishing* mucho más sofisticadas con el fin de eludir las medidas de seguridad de los correos tradicionales. Debido a esto, se puede estimar que en el próximo año aumenten las amenazas avanzadas de *phishing*, como (BEC), *spearphishing*, *ransomware* y la suplantación de marca.

El panorama de amenazas en 2019

Los delincuentes han incrementado sus ataques tanto a empresas como entidades de gobierno, siendo el beneficio económico el principal propulsor. De acuerdo con IndustryWeek, el *ransomware* y la suplantación crecieron un 350% y 250% respectivamente en 2018. La Comisión de Bolsa y Valores (SEC) estima que el coste medio de un ataque cibernético alcanzó los 7.5 millones de dólares en 2018 con respecto a los 4.9 millones de dólares en 2017. Estas cifras son alarmantes, sin embargo, es todavía más preocupante el número de municipios, grandes empresas y pequeños negocios que se han visto afectados por ciberataques en 2018.

Los delincuentes ya no discriminan a sus objetivos con tanta frecuencia como en el pasado. En la actualidad, lanzar una campaña de phishing automatizada requiere poco trabajo para un posible retorno de la inversión alto. Estas son algunas de las tendencias que podemos esperar:

1. Ataques más complejos realizados por personas menos preparadas

Delincuentes con distintos niveles de destrezas pueden acceder a una amplia variedad de herramientas del mercado negro, incluyendo guías de explicación, que permiten a cualquier persona desarrollar ataques complejos.

2. Continuarán los ataques a nivel nacional

Se estima que los ataques a nivel nacional continúen y aumenten en 2019. Como las entidades gubernamentales están aumentando su seguridad, los atacantes también podrán desviar sus fuerzas en atacar a empresas y entidades privadas. De acuerdo con numerosas empresas de ciberseguridad, 2019 será un año plagado de ciberguerras.

3. Los ataques serán más “inteligentes” y más automatizados

Así como la inteligencia artificial y el aprendizaje automático ayudarán a la detección y prevención de ataques *phishing*, la misma tecnología ayudará a los cibercriminales. Estos ya utilizan esta tecnología para buscar debilidades con el fin de crear tipos de *malware* que puedan eludir con mayor facilidad los sistemas de detección.

4. La historia se repetirá

La historia se repetirá, ya que los atacantes están desarrollando nuevas estrategias y, de esta forma, traerán de nuevo a la luz antiguas técnicas.

5. Intentos continuos de eliminar la autentificación de dos factores

Durante los últimos años, los *hackers* han intentado sortear los dos factores de autentificación. De acuerdo con el informe de McAfee del año 2019 sobre amenazas en ciberseguridad no hay indicios de que estos intentos disminuyan en el futuro y los cibercriminales continuarán desarrollando un sistema más preciso para recopilar la información necesaria en la autentificación, como usuarios, contraseñas y *cookies*.