Eleven Paths

Informe de tendencias en ciberseguridad para 2020

El presente informe pretende enfocar las posibles amenazas que podrían surgir en el entorno digital en el año 2020, dibujando un panorama de un posible futuro impulsado por la evolución de las amenazas y los avances tecnológicos.

Telefónica CYBER SECURITY UNIT

elevenpaths.com

Índice

Resumen ejecutivo

El presente informe pretende enfocar las posibles amenazas que podrían surgir en el entorno digital en el año 2020, dibujando un panorama de un posible futuro impulsado por la evolución de las amenazas y los avances tecnológicos.

El futuro podría parecer complejo, sobre expuesto y mal configurado, pero si hay anticipación, es defendible.

1. Introducción

El año 2020 es el testigo de la **transición a una nueva década**, y también lo hará la **ciberseguridad**. Las empresas cuentan con una amplia variedad de aplicaciones, servicios y plataformas que **requerirán de protección ante los posibles ataques.** Contaremos con ataques conocidos, tales como **extorsión, ofuscación y *phishing***, no obstante, **surgirán nuevos riesgos.**

Hay que destacar que, los ciber delincuentes no se desanimarán ante la posibilidad de comprometer los sistemas, cambiarán y se adaptarán en su elección de tácticas y vectores de ataque, lo que hará completamente necesario que **los usuarios y las empresas se intenten anticipar, y sobre todo estén bien protegidos.**

Es bastante probable que los atacantes superen los parches incompletos, y, en consecuencia, **los administradores de sistemas deberán asegurar la puntualidad como la calidad de los parches.**

Los investigadores de **Karspersky** [1] señalan, además, que los ataques dirigidos sufrirán cambios durante el 2020. La tendencia mostraría que las amenazas crecerán en sofisticación, y serán más selectivas, diversificándose bajo la influencia de factores externos, como el desarrollo de tecnologías como el Machine Learning para el desarrollo de Deep fakes.

1.1. Alcance

El alcance de este documento es la recopilación de información en base a diferentes firmas y proveedores de seguridad tales como Check Point, Trend Micro, CyberArk, Shophos Lab y Kaspersky entre otras y expertos en seguridad, que realizan un análisis de futuros escenarios que podrían ocurrir en 2020 relacionados con posibles ataques a infraestructuras, clientes, y usuarios.

[1] https://www.computing.es/seguridad/noticias/1115428002501/2020-amenazas-creceran-sofisticacion-y-seran-mas-selectivas.1.html

1.2. Objetivos

El objetivo de este documento es enfocar las posibles amenazas a las que se enfrentaría el mundo de la ciberseguridad en el año 2020.

Las amenazas del mundo digital están en constante evolución, y en consecuencia es imprescindible adaptarse a los posibles escenarios de ataque, puesto que la transformación digital ya es una realidad en la actualidad.

Las amenazas evolucionan, y en consecuencia el entorno de seguridad debe avanzar e incluso intentar anticiparse a dichos ataques, asegurando a las personas, empresas y a los sistemas de información de los que dependen.

2. Prospectiva de tendencias 2020

2.1. Ataques de *ransomware*

El panorama de las amenazas continúa evolucionando, la velocidad y el alcance de dicha evolución es tan acelerada como impredecible.

El año 2019, se ha visto definido por numerosos ataques *ransomware* que han afectado incluso a la actividad de las empresas que fueron objeto de ataque.

Según **SophosLabs**, los atacantes de *ransomware* continuarán apostando por realizar ataque activos y automatizados que pondrán las herramientas de administración de las organizaciones en su contra, evadiendo los controles de seguridad, y desactivando las copias de seguridad con el objetivo de causar el máximo impacto en el menor tiempo posible.

El *ransomware* **apuntará a la nube,** según **WatchGuard Threat Lab** [2]**,** se pronostica que los ataques de *ransomware* apuntarán a la nube, incluidos los almacenes de archivos, *buckets* S3 (servicios de almacenamiento a través de una interfaz de servicio web) y entornos digitales.

Check Point [3], predice el aumento de **ataques *ransomware* dirigidos**, enfocados a empresas, gobiernos locales, y organizaciones de atención sanitaria concretas. Los atacantes, optaran por dedicar tiempo a la preparación del ataque, reuniendo información sobre sus víctimas para asegurarse de poder infligir el máximo daño, por lo que el número de secuestros aumentaría. Además, puntualiza Check Point, que las empresas podrán necesitar evaluar opciones para protegerse, y como consecuencia, podrán aumentar las organizaciones que contratan pólizas de seguro contra el ransomware, lo que derivará en las **demandas de rescates por parte de los atacantes.**

[2] https://cuadernosdeseguridad.com/2019/12/watchguard-prediciones-2020

[3] https://cuadernosdeseguridad.com/2019/12/tendencias-2020-ciberseguridad-check-point/

CyberArk [4] pone énfasis en el efecto mariposa del *ransomware*, ya que seguirá aumentando el próximo año. Como el objetivo de estos ataques estaría focalizado en la interrupción y la desestabilización de los sistemas, las ciudades deberán **enfocarse en la resistencia cibernética.**

Kaspersky, define la evolución del ***ransomware***, al ***ransomware* selectivo**, los ciberdelincuentes se habrían vuelto más selectivos y en consecuencia ha disminuido el ataque multiuso generalizado.

Ahora, se centrarían en intentos agresivos de pagos de extorsión por dinero. Un giro potencial podría ser que, en lugar de hacer que los archivos sean irrecuperables, los actores amenacen con publicar los datos robados.

2.2. Cloud Computing

Los entornos de computación en la nube serán un objetivo ideal para los ciber atacantes.

Los ataques de **inyección de código**, ya sea directamente al código o a través de una biblioteca de terceros, se utilizarán de forma prominente contra las **plataformas de nube**. Estos ataques - **desde *cross-site scripting* e inyección de SQL** - se llevarán a cabo para **espiar, tomar el control e incluso modificar archivos y datos sensibles almacenados en la nube.**

Los atacantes inyectarán alternativamente **código malicioso** a las bibliotecas de terceros que los usuarios descargarán y ejecutarán sin percatarse.

Además, las vulnerabilidades en los componentes de los contenedores [5] serán las principales preocupaciones de seguridad para los equipos de DevOps (DevOps corresponde a una práctica de ingeniería de *software* que tiene como objetivo unificar el desarrollo de software y la operación del *software*).

Las plataformas sin servidores ofrecen "funcionar como un servicio", permitiendo a **los desarrolladores ejecutar códigos sin que la organización tenga que pagar por servidores o contenedores completos**. Las bibliotecas obsoletas, las malas configuraciones y las vulnerabilidades conocidas y desconocidas serán los puntos de entrada de los atacantes a las aplicaciones sin servidores.

Los ataques de inyección de código a las plataformas Cloud, **se realizarán a través de bibliotecas de terceros.**
Por lo tanto, será prioritario tener seguridad en los entornos de nube en **Azure, AWS, y Google Cloud Platform.**

Para ello, el experto en seguridad, Kevin Beaver 6, recomienda utilizar tecnologías tales como firewalls de red, Active Directory y capacidades de registro y alerta de punto final.

[4] https://www.interempresas.net/Ciberseguridad/Articulos/259701-CyberArk-desvela-las-principales-tendencias-en-ciberseguridad-para-2020.html

[5] https://www.trendmicro.com/vinfo/us/security/research-and-analysis/predictions/2020

[6] https://searchdatacenter.techtarget.com/es/cronica/Principales-tendencias-amenazas-y-estrategias-de-seguridad-de-red-para-2020

2.3.Machine Learning

El **Machine Learning**, está diseñado para eliminar *malware* que se encuentra bajo ataque, el año 2019, destacó el potencial de los ataques contra los sistemas de seguridad de aprendizaje automático.

Según Shophos lab, el Machine Learning, podría tener una connotación negativa, puesto que, modelos de detección de ML podrían ser engañados, y, en consecuencia, el aprendizaje automático podría aplicarse a la actividad ofensiva para generar contenido falso, que resultaría convincente para la ingeniería social.

Según **Ponemon Institute**, expertos en Inteligencia Artificial anticipan que la Inteligencia Artificial y el Machine Learning, derivarán en constantes mejoras en la gestión de bienes de las empresas y en la seguridad TI en particular, gracias a la mejora de la resiliencia del **endpoint,** entre otras cosas.

Además, las herramientas continuarán mejorando gracias a diferentes conjuntos de datos lo que dará como resultado una imagen más amplia de las amenazas globales.

Además, cabe destacar, que podría aumentar el **abuso de información personal** con la **Inteligencia Artificial**, esta tecnología ya está en uso actualmente, y sería tan solo cuestión de tiempo que **algunos atacantes la aprovechen.**

Por lo tanto, el aprendizaje automático (ML) y la Inteligencia Artificial (IA) podrán serán abusados para escuchar en dispositivos conectados como televisores y altavoces inteligentes para adentrarse en las conversaciones personales y de negocios, **que luego podrían proporcionar material para la extorsión o el espionaje corporativo.**

2.4.Ataques de *phishing*

Check Point coloca el *phishing* como amenaza que podrá marcar el panorama de las amenazas de 2020, junto al *ransomware*.

Los ataques de *phishing* irán más allá del email, mientras que el correo electrónico se mantiene como el vector de ataque más utilizado, los ciberdelincuentes cada vez emplean una mayor variedad de fórmulas a la hora de engañar a las potenciales víctimas para que faciliten información personal, credenciales, o envíos de dinero. De esta manera, se prevé que los ataques de *phishing* se utilizarán contra los **teléfonos móviles a través de mensajes SMS, así como a través de redes sociales y plataformas de *gaming*.**

2.5.Open Banking y *malware* móvil

Este tipo de ataque pretende robar **datos de pago, credenciales y fondos de las cuentas de las víctimas**, por lo que cualquiera que esté dispuesto a pagar a los desarrolladores de *malware*, podría distribuir *malware* de manera generalizada, además se prevé que los ataques de *phishing* también serán más sofisticados y efectivos, atrayendo así a los usuarios móviles a hacer clic en enlaces web maliciosos.

Relacionado con el *malware*, cabe destacar, la existencia de los ataques dirigidos contra el Open Banking, **los sistemas bancarios estarán más vulnerables, a medida que prosperen los pagos móviles online.**

El *malware* móvil dirigido a los sistemas de banca y pago en línea será más activo, ya que los pagos móviles en línea en Europa prosperan gracias a la Directiva de Servicios de Pago Revisada (PSD2) de la Unión Europea (UE).

De esta directiva, podrán derivar fallos en las interfaces de programación de las aplicaciones (API), y hasta nuevos esquemas de *phishing*.

Los sistemas bancarios estarán por lo tanto en la mira de Open Banking y *malware* de cajeros automáticos. Se prevé que la venta clandestina de programas maliciosos en los cajeros automáticos seguirá ganando terreno.

A raíz de esto, aumentará el **espionaje y la extorsión**, se utilizará el Machine Learning y la Inteligencia Artificial, con el **fin de espiar conversaciones personales y de negocios.**

2.6.5G

La revolución tecnológica del 2020 estará de la mano de la **implantación de la quinta generación de las tecnologías y estándares de comunicación inalámbrica.**

Según la Comisión Europea, esta innovación ofrecerá una mayor velocidad de conexión a Internet de todos los dispositivos móviles, y podría ser objeto de ataque, **podría ser utilizada por hacktivistas, grupos criminales con intereses financieros o incluso por países con el objetivo de atacar a otras naciones**. Entre los principales objetivos podrían encontrarse los sistemas de servicios esenciales como el suministro eléctrico, pero también contra el propio sistema financiero.

Relacionado con estos presuntos ataques que podrían venir derivados de hacktivistas, se relaciona con el concepto de potencial "**ciberguerra fría**" [7], que pronostica Check Point.

A medida que la sociedad depende de una conectividad continua e ininterrumpida, delincuentes y creadores de amenazas a Estados y naciones tienen más posibilidades de influir en resultados de acontecimientos políticos, causar interrupciones, e incluso daños masivos que pongan en peligro miles de vidas.

Cabe destacar, por ejemplo, el enfrentamiento entre Estados Unidos y China, donde el primero ha creado una lista negra de productos chinos donde considera que son peligrosos para el país, como ha sucedido con Huawei, ya que no puede utilizar los productos tecnológicos estadounidenses para sus productos.

Desde Check Point, indican que habrá una tendencia al alza, de ciberataques contra **infraestructuras críticas y servicios públicos.**

[7] https://www.europapress.es/portaltic/ciberseguridad/noticia-check-point-alerta-llegada-ciberguerra-fria-2020-20191028143414.html

3. Conclusiones

El mundo de las amenazas está en constante evolución, por lo tanto, el mundo de la ciberseguridad debe intentar anticiparse y establecer una mejora continua de sus soluciones.

Realizando una búsqueda activa de amenazas, enfoque integral y holístico para monitorizar e identificar de manera proactiva actividades sospechosas o potencialmente maliciosas, y de este modo, tomar medidas o minimizar, si no evitar, el impacto del daño.

Las infraestructuras críticas se verán afectadas por más ataques y paradas de producción, a la par que las empresas, siendo seguramente el *ransomware* el arma favorita.

En general, la prospectiva de ataques indica que se centraran en aumentar la actividad en ***ransomware***, incrementar el sigilo en aplicaciones maliciosas de, aprovechando la configuración incorrecta de la nube, e incluso llegando a engañar al Machine Learning.

Por lo tanto, es esencial, priorizar la **anticipación,** ya que siempre será la mejor defensa ante los posibles potenciales ataques. En 2020, las amenazas crecerán en **sofisticación y serán más selectivas**. En consecuencia, la **prevención** de las amenazas debe ser prioritaria, y para ello habrá que focalizar, la monitorización, detección y respuesta, y por supuesto, la seguridad de principio a final de todas las capas de seguridad.

Ya no basta solo con defenderse con modelos de seguridad tradicionales basados únicamente en la detección, cuando se detecta la amenaza, hay veces que el daño ya está hecho, por lo tanto, se crea una necesidad de bloquear automáticamente los ataques avanzados, evitando que afecten a los sistemas, habría que combinar **la prevención de amenazas en tiempo real, inteligencia compartida y protecciones avanzadas en todas las redes, nubes e implementaciones.**

Sobre ElevenPaths

En ElevenPaths, la unidad global de ciberseguridad del Grupo Telefónica, creemos que es posible un mundo digital más seguro. Apoyamos a nuestros clientes en su transformación digital, creando innovación disruptiva, aportando la privacidad y la confianza necesaria en nuestra vida digital diaria.

Combinamos la frescura y energía de una start-up con la potencia, conocimiento y robustez de Telefónica, contribuyendo con soluciones que posibilitan la prevención, detección y respuesta ante amenazas diarias en nuestro mundo digital.

Generamos alianzas estratégicas que permiten ampliar la seguridad de nuestros clientes y además, colaboramos con organismos y entidades como la Comisión Europea, CyberThreat Alliance, ECSO, EuroPol, Incibe, y la la Organización de los Estados Americanos (OEA).

Más información

elevenpaths.com

@ElevenPaths

blog.elevenpaths.com