Eleven Paths

WHITEPAPER

Informe de tendencias en ciberseguridad 2019

11.04.2019

Telefónica CYBER SECURITY UNIT

elevenpaths.com

Índice

1. Resumen ejecutivo

Cada año que comienza nos brinda una nueva oportunidad de revisar todo lo que ha ocurrido el año anterior y también anticipar algunos de los asuntos que nos ocuparán durante el siguiente año. En 2019, desde ElevenPaths, la Unidad de Ciberseguridad de Telefónica, queremos aprovechar este momento para analizar la evolución de las amenazas en el mundo digital, los nuevos retos que se nos presentan y el modo en que los distintos actores de la industria nos estamos adaptando a estos cambios, así como destacar las áreas que consideramos deben recibir mayor atención en los próximos meses.

Los riesgos derivados de la expansión de la transformación digital de las empresas y de la vida diaria de las personas siguen alcanzando gran relevancia. Así, se pone de manifiesto la necesidad de adaptar la seguridad a las nuevas formas de despliegue, administración y operación que surgen con la adopción de la nube y el concepto de *DevSecOps* va cobrando mayor protagonismo. También aumenta el riesgo asociado al correo electrónico, con ataques más sofisticados, y a los cada vez más ubicuos dispositivos IoT, cuya protección reclama el desarrollo de soluciones de seguridad adaptadas o incluso específicamente diseñadas para este tipo de dispositivos. Aun así, la concienciación y educación de los usuarios siguen siendo un elemento clave en la protección de los individuos y de las empresas.

Por otro lado, el aumento de los ataques a empresas basándose en debilidades de sus *partners* obliga a ampliar el ámbito de gestión del riesgo y a adoptar nuevas herramientas orientadas a analizar y automatizar los procesos que permiten conocer y gestionar estos riesgos crecientes.

Ante este escenario, los modelos de seguridad tradicionales basados en perímetro quedan en entredicho, obligando a adoptar estrategias de confianza cero y detección post-brechas. Adicionalmente, se va tomando conciencia de la inevitabilidad de sufrir un ataque, y el sector de los seguros está respondiendo con ofertas adaptadas para los distintos tipos de empresas.

En el horizonte de los CISOs, se mantiene la necesidad de soluciones que proporcionen una visión holística del riesgo, entendido y gestionado en términos de negocio. Pero, además, sofisticados ataques que antes se reducían al ámbito de estados e infraestructuras críticas se amplían a otras organizaciones, y el fraude online salta la barrera del entorno financiero para extenderse a otros sectores; todo ello lleva a reforzar la protección de la información privada, aspecto este que continúa siendo un reto, especialmente en entornos internacionales. Por otro lado, la falta de profesionales cualificados sigue siendo una constante destacada, que dificulta a las empresas su adaptación a un entorno en el que las amenazas crecen en número y complejidad y los presupuestos no siguen el mismo ritmo.

La industria trata de responder a todos estos factores, y ofrece nuevas soluciones, como los servicios gestionados de *Managed Detection and Response* (MDR) que permiten a cualquier compañía contar con una ciberseguridad avanzada, o las soluciones *Digital Risk Protection* (DRP), que protegen a las empresas en su exposición al mundo digital y cuya adopción se está extendiendo. Aparecen también las Plataformas de Aplicación de Inteligencia de Amenazas como un paso más en el uso de la inteligencia, para mejorar el rendimiento de cualquier SOC.

Finalmente, se sigue trabajando en la utilización del *machine learning* como técnica para ayudar a construir una mejor inteligencia de protección frente a amenazas, pero es necesario profundizar en sus criterios y modos de aplicación. Y ampliar el ámbito del uso de la inteligencia artificial, no sólo a la prevención y detección, sino también a la reacción.

2. La digitalización

Los procesos de digitalización de nuestro día a día son imparables. La transformación profunda que estamos viviendo en nuestras vidas y en las empresas como consecuencia de la digitalización continúan, modificando nuestras conductas y añadiéndose, muchas veces de forma casi imperceptible, a nuestras costumbres y modos de hacer. Pero, sobre todo,

son cambios necesarios e irreversibles. Muchas de las tendencias que veremos en este año, tienen que ver con esos cambios, que abren nuevas amenazas y modos de ataque.

2.1.Adopción de la Cloud

La adopción de la nube es importante, e incluso crítica[1], para empujar la competitividad y el posicionamiento de la empresa y por tanto es un elemento clave en el proceso de Transformación Digital emprendido por la mayoría de las empresas[2]. En este nuevo contexto de gestión de infraestructura y datos, la seguridad emerge como el principal reto a abarcar, ya que los procesos de despliegue, administración y operaciones de infraestructura y aplicaciones de negocio en entornos híbridos, multi-cloud y SaaS requieren de nuevos controles y *skill sets* para ser eficientes.

En este contexto, las unidades de negocio pueden desplegar nueva infraestructura, como, por ejemplo, código mediante procesos ágiles, de forma que los desarrolladores suben nuevas versiones de aplicaciones de negocio críticas para la empresa cada día, semana o mes en máquinas virtuales y contenedores mediante procesos de DevOps. Para esto, se utilizan esquemas de *Continuous Integration/Continuous Deployment*, CI/CD, que requieren incorporar nuevos controles de seguridad a los *workloads* para proteger la continuidad del negocio sin afectar la productividad.

2.2.La seguridad del correo electrónico

El correo continuará siendo el principal vector de ciberamenazas para las empresas. Más de un 80 % del *malware* que llega a las empresas lo hace por esta vía que, lejos de haber pasado de moda, es reinventada y explotada por los ciberdelincuentes usando nuevas técnicas y métodos más sofisticados para comprometer a sus víctimas. Aparte del habitual *malware*, como, por ejemplo, el *ransomware* que se puso de moda en los últimos años, nos encontramos con el *Business Enterprise Compromise* (BEC), una forma de *phishing* dirigido –conocido como "el timo del CEO"— que está creciendo de forma relevante y comienza a generar mayores pérdidas a las empresas que el propio *ransomware*[3].

La protección frente a este tipo de amenazas que utilizan el correo y que producen pérdidas económicas, de productividad o reputacionales requiere combinar la concienciación de los empleados sobre los riesgos y conductas apropiadas en el uso del correo que minimicen los riesgos de que la empresa sea afectada, junto con una solución de seguridad para el correo que ayude a detectar y proteger a la empresa y a los usuarios de estas amenazas.

2.3.Las personas son el eslabón más débil de la cadena

A pesar del nivel de inversión que en los últimos años se ha ido realizando en soluciones de seguridad, aún sigue habiendo un gran número de ataques que tienen éxito explotando la falta de cuidado, de conocimiento o de higiene de ciberseguridad de los individuos. Los esfuerzos para educar y mantener un alto nivel de concienciación y alerta en todo el personal deberían ser una de las prioridades de las organizaciones.

2.4.Internet de las Cosas

El Internet de las Cosas, IoT – *Internet of Things* - es otra de las tendencias asociadas a la digitalización. Como las demás, influye tanto en las personas como en las empresas.

[1] (1) 13% de las organizaciones que han implantado, o planean implantar una estrategia de transformación digital dicen que para ello la nube es crítico y un adicional 80% manifiestan que es importante

[2] 72% de las organizaciones prevén poner en marcha estrategias de transformación digital en los próximos 2 años.

[3] https://www.muycanal.com/2018/08/03/empresas-timo-del-ceo-bec

2.4.1. B2C Hogar Digital

El aumento de la presencia de dispositivos IoT en el hogar empezará a convertir a estos dispositivos en un vector de ataque relevante para el usuario residencial. Este nuevo foco de riesgo vendrá a unirse al continuo crecimiento del *malware* y *phishing* desde aplicaciones móviles. También se observará una tendencia a añadir una capa de seguridad y control parental en el propio hogar, a través de dispositivos específicos, o de la propia red del operador, que permiten proporcionar estas funcionalidades a todo dispositivo conectado a la WiFi del hogar sin necesidad de descarga de aplicaciones específicas de protección.

2.4.2. Simplificar la identificación y autenticación de dispositivos.

A medida que los consumidores y las empresas están adoptando más dispositivos IoT, la incorporación a la red, al ecosistema IoT y su protección se han convertido en una tarea ardua. En 2019 se hará más evidente la necesidad de proveer soluciones que simplifiquen el proceso de "*onboarding*", facilitando la identificación y autenticación de dispositivos IoT de manera sencilla y escalable.

2.4.3. Incremento de incidentes que afectan o involucran dispositivos IoT

Cada vez de manera más evidente, el IoT es una realidad en el ámbito empresarial que está contribuyendo a difuminar el concepto de perímetro de seguridad en las empresas, haciendo que los sistemas habituales de seguridad perimetral sean menos efectivos. Debido a esto, la detección de intrusiones/amenazas se vuelve necesaria y requiere el desarrollo de soluciones específicas para dichos entornos. En este sentido, se hace imprescindible generar ciberinteligencia específica sobre dispositivos IoT, por lo que se prevé la aparición de sistemas que puedan contribuir a ello, como los *honeypots* de dispositivos IoT. Estos sistemas recogen ataques dirigidos a este tipo de dispositivos y ayudan a extraer este tipo de inteligencia específica, que se puede usar para alimentar múltiples soluciones de seguridad.

3. Evolución de las amenazas por cambios en el entorno

No solo vemos ataques que tienen que ver con los procesos de digitalización, sino que las amenazas también evolucionan por cambios en el entorno.

3.1. Gestión de ciber-riesgos asociados a terceros

En 2018, hemos observado varios ataques basados en aprovechar las vulnerabilidades de terceras partes que colaboraban con la empresa objetivo del ataque. Para un atacante, desde el punto de vista de negocio, tiene todo el sentido: en un mundo altamente interconectado, la seguridad de cualquier organización es tan buena como la de su *partner* más débil.

Dentro del proceso de madurez de las empresas, en lo que se refiere a su propia seguridad, estas se enfrentan al nuevo desafío de gestionar los riesgos derivados de sus relaciones con terceras partes. Las técnicas tradicionales basadas en cuestionarios, auditorías e instrumentos legales siguen siendo válidas en algunos casos, pero no escalan ni proporcionan toda la información necesaria para gestionar ese tipo de riesgos.

Están apareciendo nuevas herramientas basadas en análisis y evaluaciones automatizadas de ciberseguridad, como una forma muy eficaz de conocer y gestionar los riesgos asociados a terceras partes en todas las etapas del proceso, desde selección a *onboarding* y monitorización continua durante toda la duración del contrato.

3.2. Los ciberseguros como una red de protección e impulsor de una mejor ciberseguridad

Hasta ahora, la Ciberseguridad como disciplina de riesgo se ha centrado en la prevención, detección y respuesta, planteamientos válidos y necesarios, pero, cada vez más claramente, insuficientes. Las brechas y los daños van a suceder inevitablemente en cualquier organización.

En una era en la que todos los negocios se están digitalizando, contar con la cobertura de un seguro es una necesidad de negocio. En el mercado de los ciberseguros están apareciendo multitud de servicios y productos con cobertura a grandes compañías, pequeñas y medianas empresas e individuos. En el futuro, los ciberseguros jugarán un importante papel al ofrecer una red de seguridad para muchos negocios y los incentivos adecuados para que todos los sectores mejoren sus posiciones.

3.3. Confianza cero y detección post-brechas como la siguiente frontera en la seguridad

La práctica en seguridad está reconociendo la imposibilidad de crear defensas 100% efectivas basadas en la premisa de perímetros seguros con sistemas y usuarios confiables. Al aceptar el hecho de que tales perímetros seguros no pueden existir, está surgiendo un nuevo paradigma en ciberseguridad, basado en privilegios mínimos, cifrado y ofuscación, visibilidad avanzada, analítica y respuesta a incidentes.

4. El entorno de gobierno de la Ciberseguridad

A lo largo de los últimos años, ciertas tendencias regulatorias y de entorno van, poco a poco, modificando nuestras obligaciones y la forma en la que entendemos las necesidades de seguridad. Algunas de estas tendencias continuarán siendo destacables durante este año.

4.1. La relevancia de la gestión de la privacidad y de los datos de carácter personal

Esto no solo aplica al ámbito europeo, sino también al de otros países y regiones que están actualizando sus modelos de cumplimiento y protección de datos, incluyendo algunas cuestiones que ya se recogen en el RGPD y que, por tanto, complican el cumplimiento regulatorio en entornos internacionales.

4.2. Visión unificada del modo en que la seguridad impacta en el negocio

Cada vez se hace más necesario que los programas de seguridad prioricen e informen al negocio de la situación en la que se encuentra y eso implica hablar en términos de riesgo y disponer de esta información, en la medida de lo posible, en tiempo real aplicada a cada uno de los procesos de negocio. Este será uno de los aspectos claves en el gobierno de la ciberseguridad.

4.3. Las capacidades de los atacantes alcanzan niveles previamente reservados a los estados.

Durante el pasado año, hemos visto un incremento en la actividad de ciertos actores patrocinados por estados dirigida al robo de propiedad intelectual, secretos comerciales u otro tipo de información confidencial de organizaciones comerciales y privadas. En paralelo, se ha ido sofisticando el nivel de las herramientas y servicios inspirados en técnicas antes disponibles solo para los estados y ahora de fácil acceso en foros y mercados en la *dark web*. Por ello, los CISOs tienen que preocuparse ahora de ataques que antes sólo veían los gobiernos y las infraestructuras críticas.

4.4.El fraude *on-line* deja de ser una preocupación únicamente de los bancos

Tradicionalmente, el fraude online era considerado un problema de banca e instituciones financieras. Pero con la aceleración de la transformación digital de las empresas y la migración de los canales de negocio e interacción con sus clientes a entornos online, el fraude empieza a ser una gran preocupación también en otros sectores como el comercio electrónico, comercio móvil, agencias de viaje, etc. Incluso los individuos deberán comenzar a tomarse el robo de identidad en serio, monitorizando sus cuentas y la publicación de su información privada ante la posible revelación de información y fugas de terceros.

5. Gestionando la escasez de talento

El mercado de la ciberseguridad sigue en continua expansión y su crecimiento supera el de la economía mundial. En este entorno, la materia prima escasa es el talento. Sólo en la Unión Europea, UE, se estima que pueda requerirse 825.000 profesionales hasta 2025. A nivel mundial, (ISC)[2] pronostica 1,8 millones en 2022.

Este crecimiento genera dos situaciones contrapuestas que continuarán conformando la dinámica del mercado en este año:

1. Un mercado laboral altamente competitivo
2. Un aumento en la inversión tecnológica que compense la falta de personal cualificado.

La competitividad del mercado laboral se traduce en un crecimiento de salarios año contra año de hasta un 11% con mayor exigencia no sólo en salario sino en el global del paquete de compensación y beneficios, como el acceso al teletrabajo, la flexibilidad de la jornada o los seguros médicos. Algunas cifras reveladoras incluyen la duplicación de las solicitudes de perfiles o el aumento en la duración de los procesos de *recruiting* ante el reto de encontrar los profesionales idóneos.

- Los perfiles de mayor demanda incluyen los CISOs con conocimientos de gobierno y técnicos que, en su mayoría tendrán estudios de post-grado en ciberseguridad o similar,
- Arquitectos de seguridad con profundos conocimientos en el diseño de arquitecturas de red, tecnologías de los principales fabricantes y experiencia en seguridad de red.
- *Pentesters* y/o hacking ético senior con más de cinco años de experiencia y conocimientos demostrados por las principales certificaciones como OSCP, CEH y experiencia multidisciplinar añadiendo análisis forense, de código o *reversing* de *malware*.
- Y, en la medida en que el proceso de madurez del RGPD continua, sigue aumentando la demanda de consultores de privacidad y *Data Protection Officers*, DPOs

En este sentido, muchas organizaciones están dirigiéndose a sus prestadores de servicio de confianza y piden CISOaaS o DPOaaS, externalizando la gestión de la ciberseguridad y la protección de datos para así superar el reto de la falta de talento.

6. Evolución de las soluciones de protección

Afortunadamente, también en el ámbito de la protección y de las soluciones, hemos apreciado durante los últimos años progresos interesantes, que veremos madurar en este año y unirse a las herramientas en que se apoyan los responsables de seguridad.

6.1.Las soluciones de Digital Risk Protection se generalizan

"Los profesionales de la seguridad cada vez más buscan soluciones de *Digital Risk Protection*, DRP, para vigilar la exposición a la que se enfrentan las organizaciones en sus infraestructuras digitales, activos y cuentas online."[4]

Se trata de una nueva categoría de soluciones que permite a las empresas proteger su exposición en el mundo digital, ya sea a través de activos fuera de su perímetro, identidades digitales usadas en redes sociales u otros canales digitales, u otra información que, expuesta en internet, puede ser aprovechada por actores maliciosos en sus campañas de ataque. Esto incluye desde la protección de la marca y la de la identidad de los principales ejecutivos de la empresa a la investigación en la *dark web*.

Estas soluciones permiten descubrir y monitorizar estos activos digitales, proveer capacidades de remediación rápida ante los ataques y proteger la reputación y la marca en los canales de comunicación.

Según Forrester, un 77 % de los clientes consideran DRP como una nueva solución que viene a unirse al conjunto de herramientas que proveen información esclarecedora dentro de sus arsenales de inteligencia de riesgo[4].

6.2.Capacidades de SOC avanzadas para todos

La industria de la ciberseguridad se enfrenta a dos realidades opuestas: por un lado, es necesario que todas las organizaciones incrementen el nivel de sofisticación de sus defensas para poder protegerse ante amenazas cada vez más avanzadas; por otro, hay una gran escasez de profesionales expertos y los presupuestos, aunque crecientes, siguen siendo limitados. Por ello, construir una ciber-defensa avanzada está lejos de las capacidades de la mayoría de las empresas.

La industria responde a esta necesidad con una nueva generación de servicios de seguridad gestionada llamados *Managed Detection and Response* (MDR) o Detección y Respuesta Gestionada. Los servicios de MDR proporcionan una visibilidad total de los dispositivos y la red, mecanismos avanzados post-brecha basados en detectar comportamientos anómalos o maliciosos, e inteligencia de amenazas, y ofrecen una respuesta a incidentes ágil y experimentada como parte del paquete. MDR es una alternativa rentable que permite a cualquier compañía protegerse en el ciberespacio.

6.3.De la recogida de Inteligencia de Amenazas a la aplicación de Inteligencia de Amenazas.

"Inteligencia de Amenazas" ha sido uno de los términos de moda en el sector durante los últimos años. Sin embargo, numerosas empresas que se inician en este tema ya se han dado cuenta de que no es suficiente con recopilar un gran volumen de inteligencia de amenazas, ya que esta puede ser muy compleja, volátil y difícilmente aplicable fuera del contexto de investigaciones profundas y especificas realizadas por analistas expertos.

Por ello, están apareciendo nuevas herramientas y técnicas que pueden ayudar a cualquier SOC a mejorar su eficiencia y su eficacia: utilizando una Plataforma de Inteligencia de Amenazas, un SOC puede combinar y priorizar toda la inteligencia de amenazas táctica y operacional que recibe e integrarla en el ciclo de vida de todos los eventos del SOC, desde la detección y clasificación al *hunting* y respuesta a incidentes.

[4] The Forrester New Wave™: Digital Risk Protection, Q3 2018 (Traducción propia)

7. Innovación al servicio de la seguridad

7.1.En 2019 no se hablará de si aplicar *machine learning* o no, sino de cómo hacerlo

Machine learning es una técnica antigua, pero relativamente reciente en el mundo de la ciberseguridad. Como toda herramienta, bien aplicada puede suponer un gran beneficio; pero puede no ser siempre la más adecuada para solucionar un problema concreto o no aplicarse adecuadamente. Creemos que precisamente esa correcta aplicación de sistemas de inteligencia es uno de los retos aún pendientes para que realmente suponga una ventaja eficaz y no un mero reclamo publicitario.

Por ejemplo, en los sistemas de detección de *malware* a través de *machine learning*, es imprescindible resolver varias cuestiones para poder disponer de un sistema suficientemente maduro que alivie la carga de los sistemas de detección tradicionales basados en firmas y heurística. Parte del trabajo necesario requiere trazar una línea entre lo normal y anormal.

Si nos ceñimos al método no supervisado para detectar anomalías en red o *malware*, resulta complejo saber qué es anómalo y se necesitarán muchas iteraciones para una comprobación posterior, con la consiguiente inversión de tiempo y participación humana o refuerzo puramente "tradicional" del análisis. Veremos tendencias en las que sabremos si finalmente debemos o no prescindir por completo del humano, según los modelos.

En el caso del método supervisado, para construir un clasificador las muestras de *malware* o ataques de red ya vienen etiquetadas en tipos de tráfico que pasan mezclados por una caja de *machine learning*. Parte de la clave del éxito de un sistema basado en *machine learning* radica en conocer los criterios considerados para tomar y clasificar las muestras con las que se alimenta ese sistema. Y aunque en muchos campos ya se ha dado con una fórmula exitosa, para otros tantos no se dispone aún de la respuesta exacta.

7.2.Del *machine learning* a la IA

El *machine learning* puede llegar a permitir la construcción de una inteligencia que proteja de forma eficaz contra las amenazas. Pero hoy ya no se discute tanto sobre cómo proteger un equipo para que no sea atacado, sino sobre cómo responder de forma adecuada cuando se vea comprometido.

Así, aunque cada vez se trabaja más en el campo de la contingencia en el *endpoint*, donde normalmente se acumulan (o comienzan) los problemas de seguridad, ésta no puede apoyarse solo en las firmas y la detección heurística/dinámica tradicional. Y es ahí donde la inteligencia artificial puede realizar un importante papel: como apoyo fundamental, no solo a la detección preventiva en sistemas sensibles, sino también a la reacción cuando se produzca el ataque.

7.3.A vueltas con la identidad y autenticación

La identidad y la autenticación siguen siendo retos en la red, con grandes visos de mejora. El hecho de que los atacantes hayan puesto sus ojos en los segundos factores de autenticación, significa que están siendo más usados que nunca, pero también ha evidenciado sus deficiencias. Se requieren capas de autorización y mejoras en general a la hora de gestionar la identidad, tanto para los para los usuarios, como para las máquinas que, en número creciente, se conectarán a la red y tendrán su “identidad” en ella dentro del enjambre de dispositivos IoT.

El modelo racional de autoridad certificadora del sistema tradicional está siendo cuestionado: aunque es un sistema fiable, resulta imperfecto para los tiempos actuales. Ahora más que nunca emerge un potencial negocio aplicable, no solo al SSL/TLS, sino también a otras áreas relacionadas con la confianza en la identidad de un tercero, ya sea máquina o humano. Es un mercado que tiene que desarrollarse y estandarizarse.

Pero no se puede tratar sobre la identidad y la autenticación sin perder de vista la privacidad. Se debe conseguir un equilibrio entre la seguridad y la privacidad, con soluciones de protección a los usuarios que no impliquen la compartición de información valiosa con terceros, poniendo así en peligro su privacidad.

7.4.La miniaturización de la seguridad

La seguridad debe volverse ágil, asequible e invisible para que sea eficiente. El reto está de nuevo en introducir las soluciones de seguridad actuales en aparatos de menor capacidad técnica y computacional que los sistemas tradicionales de escritorio o los *smartphones*, como son las cámaras o *routers,* dispositivos que, además, por definición, no aspiran a ser mucho más potentes en el futuro. Pensamos que habrá demanda de este tipo de soluciones que ayuden a mantener seguros, con la tecnología actual, este tipo de aparatos, considerando sus limitaciones.

Acerca de ElevenPaths

En ElevenPaths, la Unidad de Ciberseguridad de Telefónica, creemos en la idea de desafiar el estado actual de la seguridad, característica que debe estar siempre presente en la tecnología. Nos replanteamos continuamente la relación entre la seguridad y las personas con el objetivo de crear productos innovadores capaces de transformar el concepto de seguridad y de esta manera, ir un paso por delante de nuestros atacantes, cada vez más presentes en nuestra vida digital.

Más información

www.elevenpaths.com
@ElevenPaths
blog.elevenpaths.com