Thought Leadership White Paper

Título: El papel de la Seguridad Cognitiva en el combate de los ciberataques avanzados

Sin duda, la ciberseguridad ha avanzado desde los últimos 30 años. Sin embargo, según un informe reciente de Frost & Sullivan patrocinado por Ricoh[1], el 90% de las empresas a nivel mundial han sido vulneradas por algún tipo de ataque en estos últimos 10 años, a pesar de contar con una protección perimetral y en algunos otros casos con la protección de antivirus a nivel dispositivo. Estas tecnologías han evolucionado, sin embargo, no han sido lo suficientemente eficaces para detener los ciberataques más sofisticados.

La realidad es que las tecnologías de seguridad más sofisticadas y mejor desarrolladas demandan un gran nivel de inversión a las empresas y aun así, pueden llegar a tardar hasta un día o poco más en detectar las amenazas de los hackers. Este corto lapso de tiempo es suficiente para que estas amenazas puedan denegar el servicio de un gran corporativo por horas o días, obtener la base de datos de clientes de un banco, robar la información de desarrollo de una planta, una farmacéutica, o exponer información sensible para ser vendida en el mercado de la *Deep Web* o finalmente denegándole el acceso a la misma mediante el cifrado o exigiendo una cantidad de dinero considerable para la recuperación de la misma.

Entonces la pregunta es, ¿la evolución tecnológica de los sistemas de protección y seguridad ha perdido la guerra contra los miles de hackers que desarrollan ataques nuevos todos los días?, ¿debemos resignarnos como empresas o corporativos a aceptar intrusiones, robos y ataques informáticos todo el tiempo a pesar de contar con una estrategia de seguridad de la informática sólida?, ¿existe alguna nueva vertiente tecnológica de ciberseguridad en el mercado que ofrezca un cambio radical en la forma de protección que reduzca consistentemente la incidencia en brechas de seguridad?. La respuesta es sí, se llama 'Seguridad Cognitiva',

¿Qué ofrece esta nueva tecnología?

La 'Seguridad Cognitiva' involucra varios conceptos tecnológicos tan antiguos como son las redes neuronales, inteligencia artificial y big data. Es la asociación de todas estas tecnologías integradas a las soluciones de seguridad convencionales que existen hoy en día. La razón por la cual se están implementando las tres tecnologías juntas se debe a la

[1] Estudio: Tecnologías y Modelos de Negocios Innovadores que Transformarán Mercados e Industrias: *Una mirada sobre el impacto de la disrupción digital en los sectores de Retail, Finanzas e Industria*

capacidad de procesamiento que tenemos versus el costo de adquirirla, hecho que no era completamente accesible hace algunos años.

Una de las razones por la cual ciertos ataques cibernéticos han sido tan efectivos y que han sido capaces de burlar al sector empresarial, se debe a la naturaleza cambiante y evasiva de los mismos. Estos ataques, solamente pueden detectarse con tecnologías basadas en patrones de reconocimiento y en base a *sandboxing*), pero aún están sujetas a ser burladas si el código del malware cuenta con mecanismos de evasión, permitiendo la activación del malware tiempo después de su llegada a la red, asegurando que se encuentra ya dentro de alguna computadora, servidor o algún otro dispositivo. El malware de nueva generación cuenta con la inteligencia para burlar diversos sistemas de *sandbox,* ya que cuenta con algoritmos de evasión que detectan que está siendo analizado por un ambiente virtual y no por un dispositivo de un usuario real.

Por otra parte, los ataques dirigidos o del tipo APT (Advanced Persistent Threat), -a diferencia del malware antecesor que buscaba de manera estadística y general lanzar ataques de forma masiva para ver cuántas víctimas eran infectadas-, los ataques APT, buscan primero identificar las vulnerabilidades en el navegador o en el software del usuario por medio de un "Exploit Kit" para lanzar un ataque dirigido con base a esta vulnerabilidad. De forma similar, los ataques APT pueden encontrar las vulnerabilidades en un servidor corriendo importantes aplicaciones como un CRM u otra aplicación.

¿La Seguridad Cognitiva sustituirá a la Seguridad Convencional?

La seguridad Cognitiva promete revolucionar las soluciones de seguridad actuales, pero no sustituirlas. La seguridad cognitiva brinda capacidades tecnológicas tan revolucionarias que cualquier fabricante de seguridad que no integre algoritmos cognitivos dentro de sus roadmaps o en sus soluciones tecnologías en el corto o mediano plazo está condenado a ser devorado por la voraz competencia de quienes sí lo hagan.

La seguridad cognitiva no es una solución que, por sí misma, vaya a reemplazar a algún dispositivo de seguridad en las arquitecturas establecidas, pero sí promete ser un complemento de cada una de estas. Será una tendencia en el corto plazo ver como los principales fabricantes de soluciones tecnológicas de seguridad empiezan a integrar en cada uno de sus soluciones los algoritmos cognitivos de detección de amenazas.

De la misma forma que los firewalls de antaño evolucionaron en los firewalls de nueva generación y estos a su vez lo hicieron en sistemas de detección de brechas, estos últimos evolucionarán en sistemas de detección de brechas cognitivas. Los componentes principales de un sistema de protección perimetral son el Antimalware o Antivirus, el IPS/IDS y el Sandbox y son precisamente estos componentes los que serán beneficiados en mayor forma por la seguridad cognitiva.

Como ejemplos del potencial de la seguridad cognitiva se pueden mencionar varios casos. Por ejemplo, los módulos de antivirus o antimalware en los firewalls operan en conjunto

con funciones de sandbox para la detección de amenazas. El sandbox proporciona una capa adicional de seguridad para detectar amenazas invisibles a un antivirus porque realiza inspección y verificación de la información emulando a un usuario. Esto pareciera ser un mecanismo infalible de inspección, sin embargo, no lo es, ya que los desarrolladores de malware fabrican técnicas de evasión para sandboxing: técnicas de evasión para ambientes virtuales, de ambiente operativo, y basadas en la interacción humana[2]. Cualquiera de estas técnicas están enfocadas en mantener un comportamiento normal que no desenmascare la actividad maliciosa de malware contenido en la información recibida, de tal forma que se logre la penetración del componente malicioso dentro de la organización.

De la misma forma, el IPS está diseñado para apoyar y trabajar en conjunto con el antivirus o antimalware. Su trabajo es detectar patrones anómalos de comportamiento en el tráfico de una red que ha sobrepasado la capacidad de detección de un antimalware. Un caso específico de esto son los ataques de "Día Cero", los cuales explotan una vulnerabilidad no detectada aun por el fabricante del hardware o software y que en consecuencia no pueden ser detectadas mediante algún mecanismo estático como el del antivirus. Más aún, los desarrolladores de malware más hábiles han desarrollado técnicas de evasión para IPS mediante la manipulación de cabezales o en el mismo cuerpo de las tramas de paquetes. Otras técnicas de evasión pueden incluir ofuscación, cifrado de paquetes, fragmentación y mecanismos de violación de protocolo[3].

Un último caso a ejemplificar son las tecnologías dedicadas al procesamiento y correlacion de *logs* como los analizadores de logs y los SIEMS. Estas tecnologías permiten hoy en día de una forma muy manual poder detectar diversos tipos de eventos de seguridad. Actualmente, este análisis de logs se hace por medio de personal altamente calificado que ha pasado por varios años dolorosos de experiencia que le han dado la habilidad y capacidad de llevar a cabo el análisis y la correlación de eventos. Este personal es normalmente escaso y difícil de contratar, lo cual normalmente redunda en contratación de personal medianamente calificado que no puede explotar la capacidad completa de estos sistemas lo que a su vez conlleva en la detección tardía de las amenazas de seguridad. Según en un estudio[4] publicado por Cisco en su Reporte Anual de CyberSeguridad 2017, hasta un 54% de las alertas de seguridad no son mitigadas o remediadas.

Los tres ejemplos anteriormente presentados, representan la generalidad de la problemática más común en los sistemas de seguridad que los corporativos y las empresas experimentan día a día. Llevar a cabo una estrategia de contención eficiente, conlleva a un crecimiento proporcional en la cantidad de personal, lo cual no es factible, pues en

[2] https://www.sans.org/reading-room/whitepapers/forensics/detecting-malware-sandbox-evasion-techniques-36667
[3] https://www.sans.org/reading-room/whitepapers/intrusion/beating-ips-34137
[4] http://b2me.cisco.com/en-us-annual-cybersecurity-report-2017

realidad, las tendencias a corto plazo, indican que la cantidad de ataques siempre será mayor que la cantidad de gente que pueda atender estos eventos.

Es por esta razón que la Seguridad Cognitiva se ha convertido en un parteaguas, ya que promete ser un complemento de los mecanismos de seguridad mencionados. Por instancia, la seguridad cognitiva puede volver más inteligentes a los algoritmos y mecanismos de detección basados en antivirus y sandboxing, implementando técnicas de *machine learning* e inteligencia artificial para permitir mayor capacidad de detección de amenazas que utilizan técnicas de evasión regular y avanzada.

Por otro lado, los sistemas de detección y protección IPS/IDS pueden convertirse en mecanismos de detección menos vulnerables capaces de detectar nuevos patrones de tráfico maliciosos que mediante análisis cognitivos requieran menor entrenamiento, administración y seguimiento por parte de los administradores de seguridad.

Finalmente, la mayor pesadilla de todo personal en los SOCs o del personal dedicado a la administración de la seguridad es el proceso de mitigación, el cual como se menciona, en muchos casos, la sofisticación del ataque requiere de múltiples conocimientos y experiencia previa y, en algunos casos, la interacción de varias personas al mismo tiempo que lleven a cabo varias tareas de mitigación para reducir el costo y el impacto del ataque en curso. En estos casos la seguridad cognitiva ayuda en múltiples tareas. Por un lado, la correlación y la creación de reglas para la generación de alarmas se reduce considerablemente ya que los algoritmos de autoaprendizaje y el análisis cognitivo se encargarán de convertir a los SIEMS y a los analizadores de logs en dispositivos más avanzados que puedan crear y actualizar nuevas reglas de detección y alarmas de forma automática mediante autoaprendizaje.

Adicionalmente, la seguridad cognitiva permitirá que los logs que se almacenan indefinidamente dejen de convertirse en terabytes de basura de información no estructurada que no puede ser explotada. Las nuevas capacidades de análisis de "Big Data" en los sistemas cognitivos permiten emular a la mente humana en la capacidad de razonamiento y correlación, pero a una velocidad millones de veces superior. Esta cantidad de información contenida en los logs se analizará de forma automática para detectar patrones de trafico anómalos, eventos maliciosos que hoy pudieran pasar desapercibidos aun con un esfuerzo masivo de análisis manual realizado por varios expertos en un SOC. Lo más importante es que cuando uno de estos eventos se repita en el futuro estos serán detectados de forma automática evitando que estos nuevos ataques repetitivos tengan que ser tratados como un ataque nuevo que no ha sido reconocido.

La seguridad cognitiva promete sólidamente convertirse en una tecnología disruptiva en el campo de la seguridad, pues ésta a diferencia de muchas otras propuestas tecnológicas. Cuenta con bases sólidas que permitan a las organizaciones evolucionar de una labor intensiva y masiva para la resolución de los eventos de seguridad a un proceso automatizado por algoritmos de auto aprendizaje (Machine Learning) que detecten variaciones en patrones de trafico hoy difícilmente identificables y que tomen decisiones

basadas en variaciones de eventos históricos contenidos en información estructurada y no estructurada que seguramente la mente más aguda y analítica de un grupo de expertos de seguridad no puede detectar hoy en día.

¿Cuál es la propuesta de valor de Ricoh referente a la ciberseguridad?

Ricoh IT Services cuenta con un amplio portafolio integral de soluciones que conjuntan a las tecnologías de seguridad cognitiva mejor posicionadas por los analistas. Nuestras soluciones están enfocadas en reducir considerablemente el número de incidentes de seguridad y el número de eventos con falsos positivos lo cual mantiene en un alto nivel de estrés al personal de IT. Nuestra oferta de soluciones está basada en arquitecturas integrales que se comunican entre si y no en componentes aislados que ayudaran a su empresa a reducir los costos de soporte y mantenimiento y costos operativos con un mejor resultado en su seguridad.

RICOH IT Services tiene presencia a nivel global y en el continente americano contamos con más de 700 especialistas en diversas tecnologías. Nuestros especialistas en seguridad analizaran los requerimientos en particular de cada uno de nuestros clientes evitando que usted invierta en tecnologías obsoletas que fallen en su capacidad de protección y en su lugar invierta en tecnologías que implementan los últimos avances en "Machine Learning", Análisis de "Big Data" e Inteligencia Artificial aplicados a la seguridad. Nuestro portafolio de soluciones de seguridad es uno de los más amplios y cuentan con la madurez de décadas de desarrollo integrando las tecnologías cognitivas más avanzadas y mejor posicionadas en el mercado que van desde aquellas dirigidas a la protección del usuario final, pasando por aquellas para la protección perimetral, el data center y la nube, todas estas soportadas por una estrategia defensiva actualizada y una inteligencia en seguridad a nivel mundial que monitorea todas las redes en el mundo en más de 130 países.