Seguridad cognitiva

Un paradigma emergente frente a la inseguridad de la información.

Jeimy J. Cano M., Ph.D, Ed.D(c), CFE

Introducción

La ilusión del control basada en barreras, un dentro seguro y un afuera amenazante, es una lectura tradicional de la seguridad y el control que se ha afianzado en el imaginario de los especialistas en protección de la información (Leuprecht, Skillicorn y Tait, 2016). La creencia de que mientras más fuertes y más altas sean las murallas, mayor será el esfuerzo de los atacantes para sortearlas, ha comenzado a ceder, para darle paso a nuevas visiones del aseguramiento de la información e infraestructuras tecnológicas, basadas en analítica de datos y monitoreo permanente.

La generación de datos e información desde los sistemas de información y las instalaciones propias de la infraestructura de seguridad tecnológica, establecen el nuevo reto de la gestión de la seguridad de la información como quiera que, en una lectura analítica de estos datos es posible identificar y correlacionar eventos, que de acuerdo con las reglas de negocio establecidas, pueden ser catalogados como amenazas potenciales, tráfico inusual o patrones normales de operación.

Lo anterior demanda de las áreas de operación de seguridad de la información, aumentar su capacidad de análisis y pronóstico de tal forma que, todos los datos generados desde las plataformas tecnológicas de seguridad, se conviertan en insumos para la inteligencia de las aplicaciones analíticas, con el fin de asegurar, no sólo un moni-

toreo activo de lo que ocurre en el entorno o dentro de la organización, sino que comiencen a tener un ejercicio de identificación de amenazas tempranas con acciones disuasivas y preventivas para aumentar la capacidad de acción de la empresa, ante la inevitabilidad de la falla.

En este contexto, los avances tecnológicos aplicados a la seguridad de la información, advierten una frontera de nuevas prácticas, que demandan no sólo un ejercicio formal de generación datos de calidad, una correlación eficiente de la información y una detección de patrones de amenazas, sino posibilitar una reducción en el tiempo de respuesta y resolución de un incidente, conocer y enfrentar la complejidad y sofisticación de los ataques, además de aprender rápidamente de su entorno e incidentes, para afinar su capacidad orientada a discriminar entre eventos y amenazas potenciales (Kelley, 2016).

Así las cosas, la industria de la seguridad de la información se encuentra en una transición acelerada que implica otras capacidades y competencias analíticas, y sobre todo, un nuevo paradigma de protección que privilegia el monitoreo activo, la inteligencia analítica y una vista prospectiva para entregar a la organización un pronóstico basado en hechos y datos cumplidos, sobre su práctica y no solamente una mirada de retrovisor.

En consecuencia, este documento busca esbozar una aproximación a la evolución de las prácticas de seguridad y control sobre la gestión de la infraestructura tecnológica basado en el monitoreo continuo y la correlación de eventos, hacia una visión más cognitiva y de aprendizaje continuo, que empareje con los retos de velocidad, precisión e inteligencia que impone un entorno asimétrico, incierto y ambiguo, donde la inseguridad de la información es la norma.

Monitoreo continuo y correlación de eventos. Lecciones aprendidas

Sin pretender hacer una retrospectiva sobre la práctica de monitoreo y correlación de eventos en seguridad de la información, la cual necesariamente demanda un importante número de referencias y productos que han ayudado a construir lo que se tiene hoy, se tomarán algunos elementos básicos de análisis para ilustrar el legado de la práctica vigente, con el propósito de recorrer los principales avances y logros que dan cuenta de la efectividad de estas técnicas frente a entornos que, en su momento, eran menos volátiles que los actuales.

Una primera reflexión se plantea en torno a los sistemas de detección de intrusos (IDS en inglés), tecnología que se desarrolla a partir de la configuración de reglas y librerías de patrones de ataques, que permiten alertar a los operadores de las infraestructuras sobre eventos anormales registrados en el tráfico de red, con el fin de realizar las acciones de contención necesarias o bloquear dicho flujo con otro control, dentro del perímetro de seguridad informática definido.

Particularmente, los sistemas de detección de intrusos, basados en análisis estadísticos y perfiles de comportamiento, establecen los umbrales de desviación permitidos, para poder indicar si se encuentra en curso una posible intrusión, los cuales no necesa-

riamente corresponden con la realidad, habida cuenta de situaciones de excepción que se pueden presentar y confundir las configuraciones iniciales, generando posibles falsos positivos, que demandan una caracterización más detallada del tráfico de la red que se monitorea (Rediris, 2008).

La evolución tecnológica de los detectores de intrusos, se complementa con los SIEM (*Security Information and Event Management*), como componente clave para revelar patrones emergentes, fruto de la correlación de la información registrada y analizada en el IDS, en contexto con otros registros de seguridad y control producidos por diferentes dispositivos de seguridad tecnológicos. Esta propuesta de correlación aumenta la capacidad de los analistas de seguridad para comprender tendencias del tráfico de red, antes inexploradas y menos visibles, dado el volumen y la limitada capacidad de relacionamiento disponibles (Swift, 2010).

Necesariamente, al aumentar los puntos de monitoreo y control, se aumenta la generación de registros de eventos, lo que demanda de las soluciones de correlación una nueva evolución, para aumentar su capacidad de procesamiento, mejorar la calidad de sus análisis y sobre todo, para cerrar las brechas alrededor de los posibles falsos positivos. Frente a estos desafíos, la potencia y capacidad de las infraestructuras en la nube, abre la posibilidad de una mayor eficiencia de la correlación de eventos, como quiera que ahora es posible cruzar información no sólo propia, sino con terceros para obtener una visión enriquecida de las amenazas en un entorno más abierto y de mayor exposición al riesgo.

En la actualidad, los sistemas de detección de intrusos, así como los SIEM, son estándares de facto de los perímetros de seguridad informática, con funciones y capacidades de análisis más eficientes, alrededor de un ejercicio de prevención y correlación para brindar información clave a los analistas de seguridad de la información, con el fin de afinar sus acciones de protección y de reporte, con mayor sensibilidad frente a los cambios del entorno y mayor integración con múltiples fuentes de datos, ahora incluyendo protocolos propios de sistemas de control industrial, que implican una comprensión diferente de los riesgos y amenazas, dadas las particularidades de este tipo de sistemas en entornos industriales.

La práctica de la puesta en operación de sistemas de detección de intrusos y de correlación de eventos revelan lecciones aprendidas claves en las empresas, como la lucha contra los falsos positivos, la capacidad de procesamiento y la precisión de las alertas, las cuales exigen una evolución del campo de los algoritmos estadísticos al aprendizaje continuo y a la computación cognitiva.

Las nuevas fronteras para la práctica de la seguridad de la información

Es claro que las infraestructuras de monitoreo y control de nueva generación de las empresas, combinadas con servicios contratados de correlación de eventos y vigilancia de la reputación, establecen el marco general de protección actual de las organizaciones, frente al entorno agreste y de atacantes con capacidades de acción inciertas.

Este contexto reta los mejores ejercicios de pronóstico que el ejecutivo de seguridad pueda realizar, pues de alguna forma debe dar respuesta preguntas incómodas, insistentes y necesarias de la junta directiva, tales como:

- ¿Qué tan protegidos estamos?
- ¿Qué tan seguros somos en comparación con empresas semejantes del sector?
- ¿Qué tan preparados estamos para asumir un incidente?

Transformar la vista actual de la protección de las infraestructuras tecnológicas de las empresas implica aumentar la capacidad de visión prospectiva de la práctica de seguridad, así como la inteligencia necesaria para aprender rápidamente de su entorno y ajustar (casi) en tiempo real, las reglas y variables de monitoreo, contención y respuesta para asumir con mayor eficiencia y precisión los posibles incidentes que puedan comprometer la base de procesamiento, almacenamiento y telecomunicaciones de una empresa.

Si en el pasado los atacantes buscaban alterar un programa, manipular los datos, lograr un acceso no autorizado y procurar una acción deliberada que afectara los datos, los equipos o las instalaciones (Roufaiel, 1990), hoy, los nuevos delincuentes digitales no sólo se recrean con acciones como las anteriormente mencionadas, sino que avanzan hacia el secuestro de datos, el *malware* a la medida, las campañas de desinformación y ataques masivos sobre infraestructuras claves de las empresas o naciones, para aprovechar la incertidumbre del entorno y las posturas estáticas de seguridad y control vigente en algunas empresas.

Frente a esta realidad, se plantea el uso de sistemas cognitivos, como aquellos sistemas de aprendizaje autodirigido que usan técnicas de minería de datos, máquinas de aprendizaje (machine learning), procesamiento de lenguaje natural, interacción humana y computacional, con el fin de imitar la forma como trabaja el cerebro humano. Lo anterior, supone capacidades superiores a las prácticas actuales de monitoreo y control que expanden la capacidad del analista frente a su correlación de eventos (Zadelhoff, 2016).

Este nuevo tipo de sistemas son alimentados por cuerpos de conocimientos representados en datos estructurados y no estructurados, los cuales son “curados” o afinados por expertos especializados en una materia en particular, para entrenarlos en su lógica de análisis, con el fin de habilitarlos para comprender, razonar y aprender con celeridad, precisión y alto nivel de confianza sobre aquellos eventos que puedan ser positivos o negativos en una infraestructura de tecnología de una organización (ídem).

De esta forma se funda una nueva frontera en la práctica de seguridad y control, que pasa de una revisión pasiva de los “commodities” de protección de las empresas como son los *firewalls*, los sistemas de detección de intrusos, vpn (virtual private network), el cifrado entre otras, a una vista activa y anticipatoria, orientada por los comportamientos de las personas, la inteligencia de amenazas, el planteamiento de escenarios compartidos (McClimans, Fersht, Snowdon, Phelps y La-

salle, 2016), de tal forma que el ejercicio de pronóstico se base en el instinto y la experiencia desarrollado por los sistemas cognitivos, semejantes a los de los analistas de seguridad actuales, en una escala superior y de dimensiones que desbordan las capacidades humanas.

Retos de la seguridad cognitiva, un futuro por descubrir

De acuerdo con Kelley (2016), de una solución de seguridad cognitiva se espera desarrollar al menos tres características claves:

- Inteligencia: Aumento de la capacidad de detección y una mejor toma de decisiones frente a la respuesta a incidentes.

- Velocidad: Mejora significativa de la respuesta a incidentes.

- Precisión: Proveer mayor confianza para distinguir entre eventos y verdaderas amenazas.

Características que sugieren un nivel de preparación, aseguramiento y evolución superior en las prácticas de seguridad de la información, donde el éxito de la gestión de la protección de la información ya no es sortear con éxito una auditoría, o priorizar las potenciales amenazas identificadas, sino la habilidad para analizar y aprender de conjuntos de datos estructurados y no estructurados, para comprender patrones de comportamientos y sus significados (IBM, 2016).

Esta nueva frontera de la seguridad de la información, asistida por técnicas de inteligencia artificial y entrenada por conocimiento experto de practicantes y académicos, es capaz de conectar puntos en el espacio de las posibilidades identificadas, plantear hipótesis de posibles amenazas y riesgos siguiendo el razonamiento basado en evidencia, así como la interpretación de las variaciones identificadas en el análisis de los datos tanto estructurados como no estructurados (ídem).

Considerar la propuesta de seguridad cognitiva, debe potenciar las fortalezas de las capacidades y habilidades de los nuevos analistas de seguridad de información y su debida aplicación, además de establecer medidas para salvaguardar la privacidad, el control de acceso y el "ADN digital" de las personas y las organizaciones (Sputnik, 2017), como quiera que la identidad, la reputación y la visibilidad se encuentran en medio de un "tsunami" de información que fluye y cambia, y que es necesario entender para asegurar un uso digitalmente responsable de los datos, de acuerdo con la regulación nacional e internacional.

Finalmente, para motivar cambios en las prácticas actuales de seguridad, de cara a la puesta en operación de la seguridad cognitiva, es preciso entender que el "fecundo, evolutivo y ventajoso" estado de inseguridad cognitiva (Karageorgieva y Ivanov, 2010), configura una realidad de posibilidades en el intelecto del hombre, en el que la inteligencia artificial aún tiene espacios para continuar aprendiendo y desaprendiendo, con el fin de combinar patrones contradictorios o inusuales, con ataques conocidos, para crear lógicas inesperadas que logren en algún momento modelar y anticipar actividades contrarias, que puedan ser potencialmente negativas para una empresas o persona.

Referencias

[1] IBM (2016) Cognitive security. Evolve your defenses with security that understands, reasons and learns. Recuperado de: http://cognitivesecuritywhitepaper.mybluemix.net/?cm_mc_uid=&cm_mc_sid_50200000=1477492209

[2] Karageorgieva, A. y Ivanov, D. (2010) On cognitive insecurity. En Petrov, V. (2010) *The philosophy of security in an insecure world. Proceedings of XXV Varna International Philosophical School*. 178-184. ISBN: 978-954-92549-2-1.

[3] Kelley, D. (2016) Cybesecurity in the cognitive era. Priming your digital inmune system. *IBM Institute for Business Value*. Recuperado de: https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03111USEN

[4] Leuprecht, C., Skillicorn, D. y Tait, V. (2016) Beyond the Castle Model of cyber-risk and cyber-security. *Government Information Quarterly*. Recuperado de: http://post.queensu.ca/~leuprech/docs/articles/Skillcorn_Leuprecht_Tait_2016_Beyond%20the%20Castle%20Model%20of%20Cybersecurity_Government%20Information%20Quaterly.pdf

[5] McClimans, F., Fersht, P., Snowdon, J. Phelps, B. y Lasalle, R. (2016) The State of Cybersecurity and Digital Trust 2016. Identifying Cybersecurity Gaps to Rethink State of the Art. *Accenture – HFS Research*. Recuperado de: https://www.accenture.com/t20160704T014005__w__/us-en/_acnmedia/PDF-23/Accenture-State-Cybersecurity-and-Digital-Trust-2016-Report-June.pdf

[6] Rediris (2008) Sistemas de detección de intrusos. Recuperado de: https://www.rediris.es/cert/doc/unixsec/node26.html

[7] Roufaiel, N. (1990) Computer related Crimes: An Educational and Professional Challenge. *Managerial Auditing Journal*. 5, 4. 18-25.

[8] Sputnik (2017) ¿Qué es el 'ADN digital' y qué amenazas ocultas para la seguridad cibernética? Recuperado de: https://mundo.sputniknews.com/increible/201702031066686665-adn-amenazas-seguridad-red/

[8] Swift, D. (2010) Successful SIEM and Log Management Strategies for Audit and Compliance. SANS. Recuperado de: https://www.sans.org/reading-room/whitepapers/auditing/successful-siem-log-management-strategies-audit-compliance-33528

[9] Zadelhoff, M. (2016) Cognitive Security = Security that understands, reasons and learns. Recuperado de: http://www.forbes.com/sites/ibm/2016/05/10/cognitive-security-security-that-understands-reasons-and-learns/

Jeimy J. Cano M., Ph.D, Ed.D(c), CFE. *Ingeniero y Magíster en Sistemas y Computación de la Universidad de los Andes. Ph.D in Business Administration de Newport University; Especialista en Derecho Disciplinario de la Universidad Externado de Colombia y candidato a Doctor en Educación en la Universidad Santo Tomás. Cuenta con un certificado ejecutivo en gerencia y liderazgo del MIT Sloan School of Management, MA, USA. Profesional certificado como Certified Fraud Examiner (CFE) por la Association of Certified Fraud Examiners y Cobit5 Foundation Certificate de ISACA. Director de la revista "Sistemas", de la Asociación Colombiana de Ingenieros de Sistemas –ACIS-.*