La Necesidad de un Nuevo Avance en Ciberseguridad

Por: Ricardo Villadiego

Tabla de Contenido

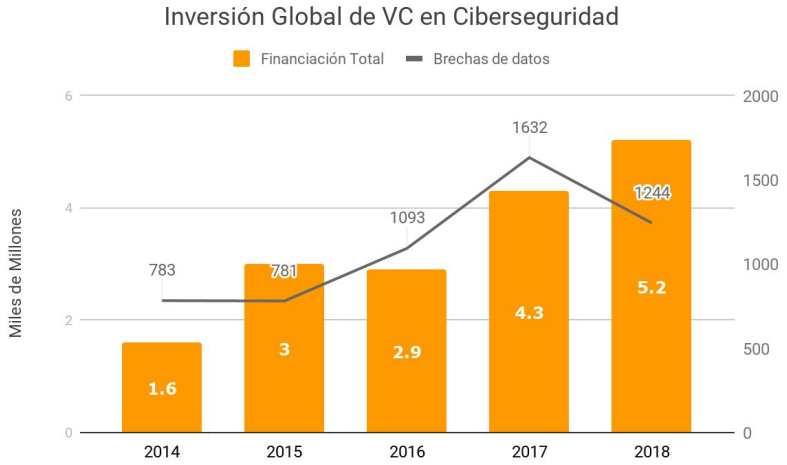
Resumen Ejecutivo

Este documento compara el nivel de inversión de fondos de capital privado (VC, por su sigla en inglés) en la industria de ciberseguridad con las brechas reportadas en Estados Unidos. La conclusión de esta comparación promueve en los profesionales de seguridad la necesidad de explorar las causas de por qué la industria de la ciberseguridad ha tenido resultados por debajo de lo esperado desde el punto de vista de protección sin importar el nivel de inversión. Este documento también evalúa la naturaleza reactiva de la industria, la complejidad del proceso de toma de decisiones y las resultantes consecuencias para las organizaciones. Además, se examina la falta de un ciclo de retroalimentación en las actuales arquitecturas de ciberseguridad. Por último, se discute el descubrimiento de un concepto de ciberseguridad denominado Continuous Compromise Assessment™ , la cual implementa un ciclo de retroalimentación en las arquitecturas de seguridad de las empresas.

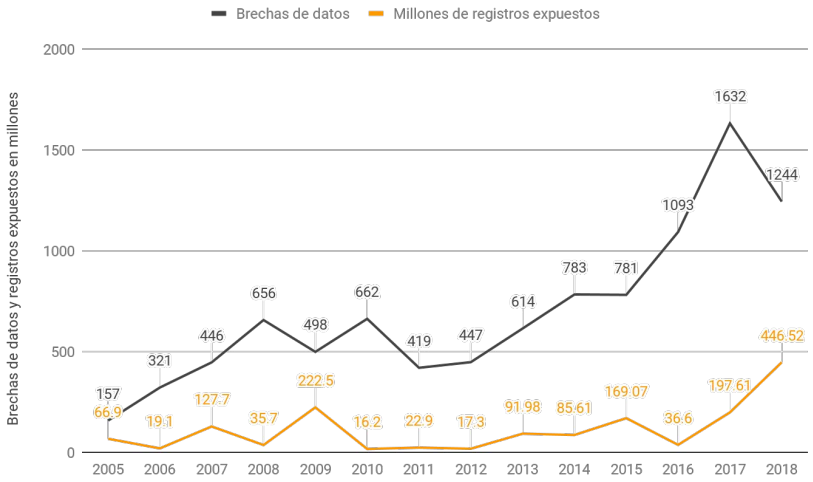
El Estado de la Ciberseguridad

La industria de la ciberseguridad está en furor. Para comenzar, las VC siguen inyectando capital de forma nunca antes vista para permitir el crecimiento de los actuales proveedores y financiar nuevas compañías. Entre 2014 y 2018, la industria de VC invirtió la sorprendente suma de $17.100 millones según Strategic Cyber Ventures.[1]

Entre 2014 y 2018, la industria de VC invirtió la sorprendente suma de $17.100 millones



Sin embargo, durante el mismo periodo, el número de brechas de seguridad creció exponencialmente y la cantidad de datos expuestos resultó en una crisis de escala global. De acuerdo con el Identity Theft Resource Center de EE.UU.[2] , el número de brechas creció de 783 en 2014, ya una terrible cifra de por sí, a un pico de 1632 casos en 2017.



[1] 2018 Cybersecurity Venture Capital Investment: https://scvgroup.net/2018-cybersecurity-venture-capital-investment/
[2] 2018 Identity Theft Resource Center 2018 Data Breach Report

El mismo estudio refleja que el problema está presente en todas las industrias.

Número de brechas de datos en EE.UU.

Año	Banca/Crédito/ Finanzas	Negocios	Educación	Gobierno/ Ejército	Medicina/ Salud	Total
2013	35	194	54	60	271	614
2014	38	263	57	91	332	781
2015	71	312	58	63	275	779
2016	51	497	97	72	373	1090
2017	134	907	128	79	384	1632
2018	135	572	77	100	367	1251

Inversión no necesariamente significa protección

No es cierto que las organizaciones que cumplen al pie de la letra con las regulaciones más exigentes, como es el caso del sector bancario, tienen mejores resultados que aquellos sectores menos regulados, ni que las industrias que hacen mayores inversiones en ciberseguridad tienen menos brechas. Probablemente es hora de que aceptemos que inversión no necesariamente significa protección.

Por años, hemos sido condicionados a definir el éxito en términos de inversión de tiempo y dinero. En cuanto a ciberseguridad, esta fórmula no está produciendo los resultados esperados para una industria con tan alto nivel de inversión.

Tal fórmula universal (Éxito = Tiempo + Dinero) ha funcionado en muchos aspectos de la vida, desde deportes hasta llevar un hombre a la luna. Esta fórmula ha producido impresionantes resultados en el campo de la salud; por ejemplo, en agosto de 2019, la OMS y el Instituto Nacional de Alergias y Enfermedades Infecciosas anunció una cura para el ébola y un progreso significativo en cuanto a una vacuna contra el VIH, una enfermedad que significaba la muerte hace casi 20 años.

Sin embargo, en el frente de la ciberseguridad, la ciber-guerra puede estar perdida. Otro indicio de esto es una marca icónica como Capital One anunciando ser víctima de una enorme brecha. La forma en que llegamos a este punto merece ser explorado.

¿Cómo Llegamos Hasta Aquí?

Existen cuatro aspectos que llevaron a la industria a su estado actual de compromiso e incertidumbre:

a. **Las amenazas en constante evolución** generan una cantidad infinita de vulnerabilidades las cuales deben ser defendidas por las empresas. Las tecnologías de ciberseguridad siguen siendo reactivas, lo cual conlleva a un "ciber-ciclo" de atacantes escaneando redes, desarrollando explotaciones o atacando sistemas con defensas que detectan ataques, analizan explotaciones y luego crean parches para tales sistemas.

b. La inyección de **capital ilimitado** a la industria está promoviendo que los proveedores de soluciones de defensa sigan el enfoque de "detectar para mitigar". Como resultado aparecen tecnologías que no están listas, son inestables por naturaleza y se vuelven obsoletas tan pronto son desplegadas sin siquiera llegar a probar su nivel de efectividad.

c. Producto de a.) y b.), las arquitecturas de ciber-defensa han **aumentado su complejidad,** acumulando una enorme cantidad de proveedores que pasan por alto las capacidades de administración y monitoreo, añadiendo así poca protección al sistema. La complejidad y los costos sus asociados crean una falsa sensación de seguridad, especialmente en los niveles más altos de la organización.

d. La sociedad actual está psicológicamente ligada a encontrar gratificación instantánea. Esta noción es utilizada en la resolución de problemas como la búsqueda de **una solución mágica.** Este comportamiento y la inhabilidad de aceptar la idea de tener una brecha ocasionó que quienes toman las decisiones en una compañía aceptaran el actual marco de innovación en ciberseguridad: detectar para mitigar.

La complejidad y su costo asociado crean una falsa sensación de seguridad

Para empeorar más las cosas, muchas de las actuales soluciones y arquitecturas de ciberseguridad funcionan como un sistema de bucle abierto en su núcleo. Es decir, no tienen en cuenta los aspectos positivos de los sistemas de bucle cerrado, en los cuales el resultado ideal (en este caso, no estar comprometido) es medido continuamente para asegurarse que los cambios realizados se aplican al sistema (la arquitectura de ciberseguridad).

Es imposible obtener diferentes resultados haciendo siempre lo mismo. Para romper el ciber-ciclo, la ciberseguridad necesita cambiar paradigmas para aplicar teorías de control y así medir de forma continua los valores de referencia. Para cualquier organización, este debe ser "no estar comprometido". Cualquier desviación del valor de referencia debería ser identificado y mitigado oportunamente al ajustar la arquitectura de ciber-defensa.

Tomando las Decisiones Correctas

Las organizaciones deben decidir sobre la estrategia de defensa adecuada para su modelo de negocio, industria y partes interesadas. Esto representa mantener un enfoque eficiente, efectivo y proactivo a la vez que se mantiene en orden la reducción de las tasas de errores de conmutación. Sin embargo, debido al significativo aumento en el número de brechas durante la última década, ¿estamos tomando las decisiones correctas?

Un estudio reciente[3] indica que los retos de crear capacidades de ciberseguridad en organizaciones se basan en ideas erradas sobre dos aspectos de complejidad que han recibido poca atención:

- **La incertidumbre alrededor de los ciber-incidentes:** Los profesionales de seguridad y riesgos no encuentran nada fácil aplicar teorías convencionales sobre toma de decisiones a las inversiones de ciberseguridad debido a la dificultad de medir el impacto de un ciber-incidente hipotético. En consecuencia, a menudo toman decisiones y hacen juicios basándose en su experiencia y en sus mejores conocimientos con respecto a la posibilidad de que se presenten ciertos eventos.

  La naturaleza severa e incierta de los ciberataques, en conjunto con los frecuentes cambios en la adquisición de tecnología y la presencia de nuevas vulnerabilidades, hace aún más difícil la tarea de quienes toman decisiones para que puedan dirigir eficientemente recursos de inversión en capacidades de ciberseguridad. La creciente presencia de ciberamenazas ha creado un ambiente que se enfoca en las defensas técnicas, pero pasa por alto la economía de una inversión de ciberseguridad. Si una compañía no experimenta ningún ciberataque, o más precisamente, si no detecta ninguno, no existe mucha motivación para invertir en ciberseguridad. Por esta razón, muchos profesionales de la industria no suelen prever los ciber-riesgos de la mejor manera. No sorprende observar diferencias significativas entre las percepciones y el estado real de la ciberseguridad de sus organizaciones. Como resultado, pueden subestimar la frecuencia en la que ocurren los incidentes y el tiempo que les toma a las soluciones de ciberseguridad comenzar a trabajar, prevenir, detectar y responder ante uno.

- **Retrasos en crear capacidades de ciberseguridad:** La ciberseguridad ha crecido en términos de complejidad y es muy probable que lo siga haciendo. Como cualquier otro modelo complejo, los sistemas de ciberseguridad incluyen potenciales retrasos. En una organización reactiva en la que los administradores comienzan a invertir en el desarrollo de capacidades de ciberseguridad solamente después de detectar un ataque, los sistemas de información computacionales de la organizaciones no se recuperarán adecuadamente a tiempo y seguirán siendo vulnerables. Como dijo el Rey Enrique VIII de Inglaterra: “De todas las pérdidas, la del tiempo es la única irreparable pues jamás podremos recuperarlo”. Si las organizaciones pudieran evitar este enfoque reactivo, combatir la urgencia de resolver todo a corto plazo y actuar de forma decisiva para implementar las capacidades de ciberseguridad que requieren, podrían estar en una mejor posición.

Si una compañia no experimenta ningún ciberataque, o más precisamente, si no detecta ninguno, no existe mucha motivación para invertir en ciberseguridad

[3] Decision-making and biases in cybersecurity capability development: Evidence from a simulation game experiment.

El Avance de Ciberseguridad

La crisis global de ciberseguridad es un problema que debe ser rápidamente resuelto o mejorado significativamente. Las VC continúan invirtiendo capital en la industria y con un entorno de amenazas que puede evolucionar infinitamente (y lo hará), abordar el problema es cada vez más crítico.

Las organizaciones tienen que asumir que los cibercriminales ya están dentro

El foco debe centrarse en crear capacidades de ciberseguridad que alteren fundamentalmente el estado actual de ciberseguridad. Necesitamos replantear nuestro paradigma de seguridad para que salga del enfoque tradicional que intenta mantener a los adversarios fuera de nuestras redes. Este cambio se conoce como "Presunción de Brecha". Deborah Hayden de la Dirección para el Aseguramiento de la Información de la NSA ha hablado bastante del tema desde diciembre de 2010.[4]

La industria no cuenta con un proceso objetivo que brinde certeza sobre los ciber-incidentes, el cual es uno de los dos motores para tomar las decisiones correctas en ciberseguridad. En Lumu, llamamos a este proceso **evaluación continua del compromiso** o Continuous Compromise Assessment ™.

Para comprender mejor este concepto, es necesario revisar primero el modelo Cyber Kill Chain[5], el cual sirve para identificar y prevenir actividades de ciber-intrusión. El modelo identifica lo que los adversarios deben realizar para alcanzar su objetivo. La siguiente gráfica simplifica el proceso.

Al ver más de cerca las diferentes etapas entre las múltiples variaciones de Cyber Kill Chain, se puede evidenciar el común denominador que determina las nefastas intenciones de los adversarios: **acceso a redes.** El tráfico de redes es el epicentro para iluminar las amenazas. Casi todas las amenazas deben ser descargadas primero y luego comunicarse de vuelta con su comando y control para brindarle información a los atacantes.

La habilidad de reunir tráfico de redes para iluminar amenazas puede ser el **ciclo de retroalimentación** que muchos investigadores académicos y de ciberseguridad han visualizado por más de una década

La habilidad de reunir tráfico de redes para iluminar amenazas puede ser el **ciclo de retroalimentación** que muchos investigadores académicos y de ciberseguridad han visualizado por más de una década. Incluso con los avances en ancho de banda y almacenamiento, reunir tráfico de redes para una organización grande puede tener limitaciones de costos. El problema ahora evoluciona en cómo reunir señales de tráfico de redes en una forma que represente con precisión el resumen de las "conversaciones" dentro de la red de una organización.

[4] Assumption of Breach: The New Security Paradigm by Jeffrey Carr
[5] Developed by Lockheed Martin
https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

En su libro *Secretos y Mentiras*, Bruce Schneier fórmula que "con frecuencia los patrones de comunicaciones son tan importantes como el contenido del comunicado". Por ejemplo, el simple hecho de que Alicia llame por teléfono a un terrorista reconocido cada semana es más importante que los detalles de su conversación. Al juntar esto con los pasos asociados con Cyber Kill Chain, podemos descubrir rápidamente que el proceso de comprometer un dispositivo y una red hará que tal dispositivo y tal red se comporten de forma diferente. Estos son algunos pasos para ilustrar el proceso:

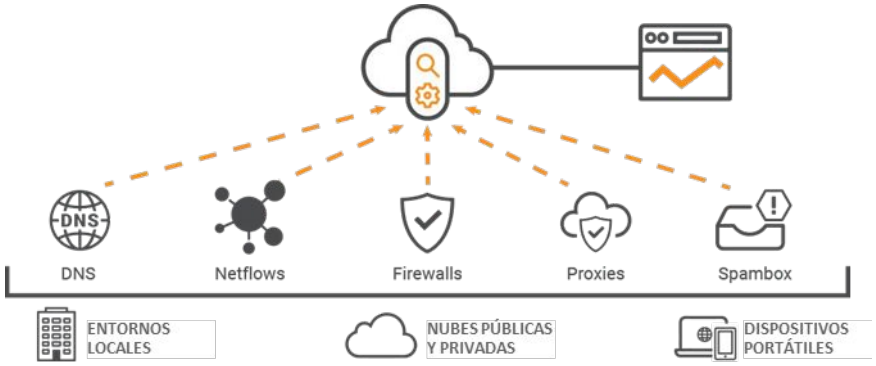
- El dispositivo del usuario final a quien el adversario planea atacar se dirigirá a un nuevo **host.**
- Si el ataque es exitoso, el dispositivo intentará conectarse con la infraestructura del adversario **(comando y control)** buscando instrucciones y/o exfiltrando información.
- En ataques más sofisticados, el adversario necesitará escalar privilegios y, para lograrlo, el dispositivo comprometido intentará comunicarse con dispositivos adyacentes y/o blancos de alto valor dentro de la organización comprometida. Esta es una clara señal de **movimiento lateral.**
- A medida que el adversario consigue nuevas víctimas, más dispositivos intentarán conectarse con su infraestructura.

Un mayor análisis de los pasos descritos entre otros facilitó determinar los elementos clave de metadatos: desde el tráfico requerido por las redes hasta una representación precisa del resumen de las conversaciones dentro de una organización, como se describe en la siguiente tabla:

Metadatos de red	Por qué son importantes
Consultas de DNS	Recolectar consultas de DNS brinda contexto sobre el intento de conexión desde los dispositivos de la organización hacia la infraestructura del adversario.
Flujos de red	Entre otro comportamiento malicioso, los flujos de red proporcionan perspectivas dentro de los dispositivos de una organización que son controlados por los adversario e intentan moverse lateralmente.
Registros de acceso de proxies de perímetro o firewalls	En casos en los que los ataques evitan la resolución de dominios, los rastros de contacto con el adversario residirán en el registro de acceso de los firewall o proxies, dependiendo de la configuración de red de la organización.
Spambox	El email es el método preferido por los atacantes para distribuir explotaciones a los usuarios finales de una organización. El análisis del correo no deseado de una organización permite ver el tipo de ataques que reciben, pero aún más importante, si los usuarios finales están accediendo a tales ataques y si la organización está en un alto riesgo de compromiso.

[6] Verizon 2019 Data Breach Report.

Señalar el tráfico de esta forma en lugar de hacer una captura completa es un proceso óptimo dado que representa solo una pequeña fracción del tráfico total de la red. Sin embargo, aún es posible identificar el nivel de compromiso de una organización.



Se han desarrollado técnicas específicas para facilitar el proceso de recolección de datos a la vez que se minimiza la fricción en los múltiples entornos que definen una red actualmente.

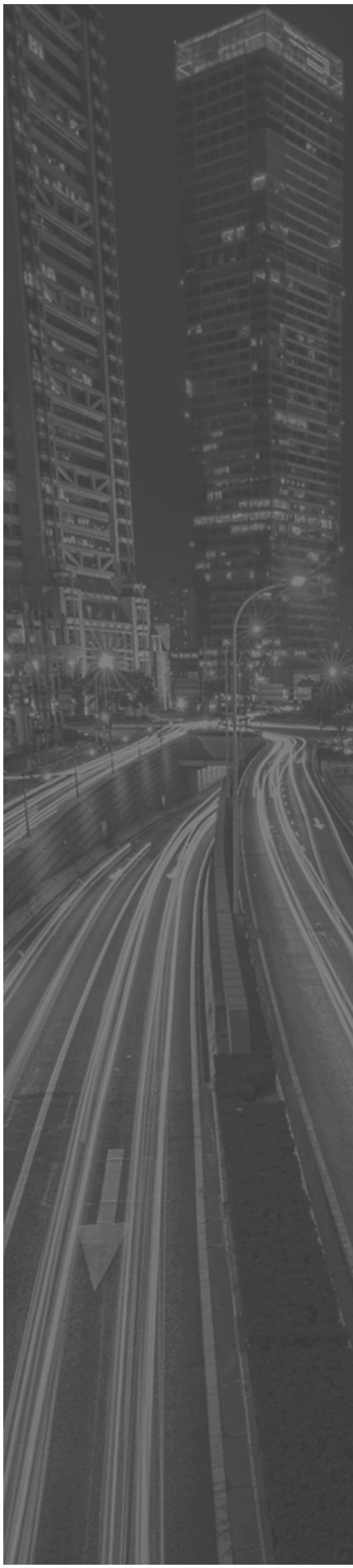
El problema que queda por resolver es cómo hacer de este un proceso continuo. Es posible realizar el proceso de recolectar y procesar estas señales en un lapso específico, pero representa un gran reto. Las organizaciones pueden desencantarse rápidamente debido al nivel de complejidad presente en recolectar y procesar datos, incluso con la ayuda de herramientas que prometen abordar al menos algunas de estas señales claves, como colectores de flujo de redes.

Para resolver esto último, se requiere un proceso confiable, preciso y continuo desde la recolección hasta la iluminación como se muestra en la siguiente imagen.

Solo cuando el proceso continuo es implementado podemos afirmar que el ciclo de retroalimentación ha sido creado y este puede considerarse el avance de ciberseguridad de la modernidad. Un continuo proceso de evaluación de compromiso no solo simplificará el proceso de toma de decisiones para los administradores, sino que también cambiará por completo la dinámica del ecosistema de ciberseguridad y el ciber-ciclo de atacantes versus defensores.

Conclusión

La ciberseguridad es compleja. El éxito en escenarios complejos yace en la habilidad del sistema para regularse después de una alteración. En la práctica, esto se hace a través de sistemas de bucle cerrado o “sistemas de error controlado”, entendiendo error como el estado de compromiso para un incidente particular de ciberseguridad. Entre más rápido se mueva la industria hacia el desarrollo de las capacidades de ciberseguridad necesarias que ayuden a una organización a evaluar su continuo estado de compromiso, más rápidamente se alcanzará esa ciber-resistencia. Con cambios pequeños pero intencionales en la arquitectura de ciberseguridad, la diferencia entre el ciber-incidente y la detección de la brecha puede acortarse dramáticamente.



Illuminating threats and adversaries

www.lumu.io

Lumu Technologies Inc. | 8350 NW 52nd Terrace Suite 301, Miami, FL 33166 | info@lumu.io | +1 (877) 909-5868