El desequilibrio: ante la disparidad de incentivos la ciberseguridad sale perdiendo

Ya hace tiempo que los ciberdelincuentes llevan ventaja. Ellos encuentran continuamente nuevas formas de robar datos, interrumpir servicios y obstaculizar el flujo legítimo de la información; y no porque sean mejores, sino porque sus incentivos no tienen nada que ver con los alicientes para los defensores. Para entender mejor esta disparidad en los incentivos de ambos grupos, hemos encuestado a 800 profesionales de la ciberseguridad procedentes de cinco sectores industriales clave. El informe ha identificado tres diferencias de incentivos principales: entre las estructuras corporativas de las empresas de seguridad y el libre flujo de las empresas de los delincuentes, entre estrategia e implementación, y entre los altos directivos y los encargados de la puesta en práctica u operadores.

Tres niveles de diferencias de incentivos ponen a los defensores en desventaja

Agresores frente a defensores	Los incentivos de los agresores se basan en un mercado fluido y descentralizado, lo que contribuye a que sean ágiles y se adapten rápidamente, mientras que los defensores se enfrentan continuamente a la burocracia y las decisiones de sus superiores.
Estrategia frente a implementación	Si bien es cierto que más del 90 % de las empresas disponen de una estrategia de ciberseguridad, menos de la mitad tienen dicha estrategia completamente implementada.
Directivos frente a operadores	Los directivos que diseñan las ciberestrategias miden el éxito de manera diferente a los encargados de ponerlas en práctica, lo cual limita su efectividad.

Estructura corporativa frente a empresa delictiva

Aunque el objetivo de la mayoría de los ciberataques es algún tipo de organización con una cierta jerarquía y organización burocrática, los ciberdelincuentes actúan en un mundo de freelances, clandestino pero abierto, y con incentivos claros. El mercado de la ciberdelincuencia responde a las señales de precios con innovación y con la oferta de nuevos productos y servicios a diario. Cuando se agotan las funciones obsoletas, se sustituyen rápidamente online. Esto facilita una competencia dinámica y una rápida innovación entre los distintos componentes del mercado de la ciberdelincuencia; desde los delincuentes más sofisticados y con más recursos, y los respaldados por un estado nación, hasta los hacktivistas y los consumidores de ciberdelincuencia como servicio. Para este estudio entrevistamos a expertos técnicos en ciberseguridad y a agentes de las fuerzas de seguridad para profundizar en el conocimiento de estos mercados.

Los mercados de la ciberdelincuencia están muy especializados, por lo que ofrecen a los profesionales de élite la oportunidad de convertirse en expertos de su sector. Las especialidades más habituales son los programadores de malware, los diseñadores de sitios web maliciosos, los expertos en infraestructuras, los hackers especializados en exploits y vulnerabilidades, y los artistas de la estafa dedicados a idear planes basados en la ingeniería social. Las ganancias se distribuyen entre los especialistas según su contribución. La competencia dinámica y la información disponible sobre reputación desplazan continuamente a los menos capacitados y encumbran a los mejores.

Uno de los principales efectos de esta competencia directa y del modelo de compensación es lo rápidamente que se utilizan las nuevas vulnerabilidades o exploits. Los delincuentes aprovechan hasta un 42 % de las vulnerabilidades solo 30 días después de haberse divulgado. Por ejemplo, cuando los desarrolladores del destacado kit de exploits Angler (que supuso en su momento hasta el 82 % de la actividad de los kits de exploits, según una estimación) fueron arrestados, bastaron unas semanas para que los delincuentes que lo utilizaban lo sustituyeran por el kit de exploits Neutrino para distribuir sus cargas útiles. La mayoría de los delincuentes investigan poco o nada; en cambio sí aprovechan el trabajo de los delincuentes más experimentados, que suele distribuirse rápidamente gracias a los mercados web clandestinos, así como al enorme número de sistemas existente, que llevaría demasiado tiempo corregir con parches. Esto presenta, además, la ventaja de mantener los costos bajos.

Si observamos los sucesos ocurridos en relación con la ciberdelincuencia parecería que muchos delincuentes proceden de Rusia y Europa del Este. Algo de cierto hay en esta suposición, sobre todo debido a los avanzados programas de matemáticas e informática disponibles y a la escasez de ofertas de empleo legítimas en dichas zonas. Incluso los empleados de empresas de TI y telecomunicaciones legales en estas regiones están con frecuencia pluriempleados como delincuentes, y a veces publican abiertamente sus identidades de la Internet profunda en sus perfiles de Facebook. Los equipos de ciberseguridad de las empresas tienen mucho que aprender de estos mercados clandestinos. Unos incentivos claros y mejoras de la reputación pueden tener un efecto positivo considerable en la actitud y la eficacia.

Desconexión entre estrategia e implementación

En la actualidad la ciberseguridad es el riesgo número uno para las organizaciones, según la mayoría de los encuestados. Más del 70 % de los directores reciben información sobre los riesgos de seguridad en las juntas directivas, especialmente en lo relativo a retos que ni siquiera se consideraban entre los 10 principales hace solo seis años. Casi todos (93 %) manifestaron que su organización tiene una estrategia de ciberseguridad destinada a bloquear tanto las amenazas nuevas como las existentes.

Y aquí empiezan a observarse las primeras diferencias. Muchos directivos creen que su estrategia está plenamente implementada en toda la organización, mientras que solo el 30 % de los operadores aceptan esta suposición. En ambos grupos, el principal parámetro para medir la eficacia de la ciberseguridad es el número de ataques, sin embargo, a partir de ahí comienzan las divergencias. Los altos directivos confían más en los parámetros de rendimiento, como el costo de recuperación tras un ataque o la rentabilidad del gasto en ciberseguridad. Los operadores se inclinan por los parámetros técnicos, como los análisis de vulnerabilidades y las pruebas de penetración. Más de la mitad (54 %) de los directivos encuestados están más preocupados por el impacto en la reputación de la empresa que por los efectos reales de un incidente de seguridad. Es bastante preocupante el hecho de que entre estos profesionales únicamente menos de un tercio (32 %) cree que un incidente de ciberseguridad provoca la pérdida de ingresos o ganancias, lo que les puede dar una falsa sensación de seguridad.

Otra evidencia de la falta de conexión entre la estrategia y la implementación son los métodos empleados para garantizar que las medidas de ciberdefensa no abran nuevos riesgos para la organización. Aunque la mayoría (71 %) afirmó que mantienen una plataforma de seguridad que se integra con las tecnologías nuevas y existentes, el 64 % dijo que también están adquiriendo tecnologías de seguridad que se solapan. Esta estrategia puede parecer sólida, sin embargo las tecnologías que se solapan y no se integran de forma adecuada pueden generar brechas en la seguridad, ya que el empleo de distintas configuraciones y sistemas de control complica la creación e implementación de directivas de seguridad coherentes.

Incentivos diferentes para los directivos y los operadores

Los ciberdelincuentes tienen un incentivo directo en forma de compensación monetaria, publicidad o el daño en la reputación de su víctima. Nuestra encuesta pone de manifiesto que entre los profesionales de la ciberseguridad no solo hay una falta de incentivos, sino que además, los directivos confían más en los efectos de los incentivos actuales que el personal al que intentan motivar.

Casi la mitad de los operadores encuestados afirmaron que no existían incentivos en su empresa, lo que equivale a más de cinco veces el número de directivos que manifestaron lo mismo. Es posible que los empleados en los niveles más bajos de la estructura organizativa desconozcan los incentivos por rendimiento o que no consideren que las ofertas son efectivas. Afortunadamente, el 65 % de los profesionales encuestados manifestaron que se sentían motivados personalmente para reforzar las medidas de ciberseguridad de su empresa.

Los directivos que informaron sobre los incentivos existentes para los profesionales de ciberseguridad identificaron en primer lugar la compensación económica (60 %) o el reconocimiento (58 %). Sin embargo entre los profesionales no directivos, hablaron de estos mismos incentivos de un 15 a un 25 % menos. Cuando se les preguntó qué incentivos les gustaría recibir, los operadores otorgaban casi el mismo peso a la compensación económica (63 %) y al reconocimiento o los premios (62 %). Este resultado coincide con otros estudios que muestran que las oportunidades de promoción profesional son tanto o más valoradas que las bonificaciones.

Lecciones de la ciberdelincuencia

Las empresas pueden aprender de la comunidad de hackers para ayudar a corregir estas diferencias. La seguridad como servicio puede ofrecer la flexibilidad necesaria para luchar contra las operaciones de ciberdelincuencia como servicio. Los consultores especializados pueden sumar al equipo de personal interno experiencia y recursos específicos cuando sea necesario. Los incentivos por rendimiento y el reconocimiento pueden promover la mejora de las defensas y la agilización de los ciclos de aplicación de parches. Es necesario experimentar para determinar la combinación perfecta de parámetros e incentivos para cada empresa, pero está en su mano aumentar la velocidad y la especialización de las defensas, así como mejorar los resultados de la seguridad.

Resumen ejecutivo

Lecciones del mercado de la ciber-delincuencia	Los delincuentes	Los defensores
Aprovechamiento de las fuerzas del mercado	**La delincuencia como servicio** El mercado de la ciberdelincuencia que es abierto y descentralizado aprovecha la competencia y los precios de mercado para minimizar las barreras de acceso, impulsar la innovación y ayudar a las iniciativas empresariales que prosperan a ganar escala rápidamente.	**La seguridad como servicio** Un mayor uso de la externalización y los contratos abiertos puede reducir los costos, incrementar la competitividad y facilitar la adopción generalizada de tecnologías y prácticas de seguridad eficaces.
Uso de divulgación pública	**Dirigir los ataques a vulnerabilidades conocidas** El aprovechamiento de las vulnerabilidades que se han hecho públicas evita costosas investigaciones y el desarrollo de exploits, e incorpora rápidamente las nuevas vulnerabilidades a los ataques para maximizar su efectividad antes de que se apliquen los parches de los sistemas de defensa.	**Mejora de las prácticas de aplicación de parches** Responder con más celeridad a la divulgación de vulnerabilidades mediante una mejor aplicación de parches y una sustitución más rápida de los sistemas obsoletos contribuye a incrementar la seguridad y eleva los costos para los agresores.
Incremento de la transparencia	**Foros abiertos y publicidad online** Los foros abiertos y la publicidad facilitan la proliferación de nuevos ataques eficaces y modelos de negocio delictivos, así como la adopción generalizada de las mejores prácticas.	**Intercambio de información y colaboración** Ampliar el intercambio de información recorta costos para los defensores, gracias a una disminución de la duplicación, y ayuda a difundir noticias sobre nuevas tecnologías y prácticas que aportan mejoras significativas para la seguridad.
Reducción de las barreras de acceso	**"Cualquiera con conocimientos de informática"** El ecosistema de la ciberdelincuencia, que carece de requisitos en cuanto a cualificaciones formales o limitaciones geográficas, puede atraer a profesionales que no han sido valorados en la economía legal y aprovechar al máximo su potencial.	**Aprovechamiento de la reserva de talento global** Contar con una reserva de expertos más amplia, con jóvenes y especialistas en TIC extranjeros que con frecuencia acaban involucrándose en la ciberdelincuencia, ayuda a las empresas a llenar los vacíos en la plantilla de ciberprofesionales y aprovecha el talento existente en el mercado de la ciberdelincuencia.
Equiparación de los incentivos	**Los mercados freelance recompensan el rendimiento** En el mercado de ciberdelincuencia freelance, los operadores de todos los niveles y áreas funcionales de la cadena de ataque son recompensados por el mercado por su excelencia o bien penalizados si los resultados no son los esperados.	**Incentivos por rendimiento** Para equiparar los incentivos de los directivos con los de los operadores, se deben ofrecer premios y bonificaciones a los empleados y administradores que consiguen buenos resultados en seguridad.

Para obtener más detalles sobre la diferencia de incentivos en la ciberseguridad, con un desglose por país y sector vertical, descargue el informe completo, El desequilibrio: ante la disparidad de incentivos la ciberseguridad sale perdiendo, Centro de Estudios Estratégicos e Internacionales (CSIS), marzo de 2017.

McAfee. Part of Intel Security.
6205 Blue Lagoon Drive
Suite 600
Miami, Florida 33126
U.S.A.
www.intelsecurity.com

 2480_0217_exe-misaligned-tilting-playing-field
March 2017