Por qué los ciberdelincuentes superan a los defensores: disparidad de incentivos en el sector de servicios financieros

Ya hace tiempo que los ciberdelincuentes llevan ventaja; encuentran continuamente nuevas formas de robar datos, interrumpir servicios y obstaculizar el flujo legítimo de información. Y no es porque sean mejores, sino debido a la enorme diferencia entre sus incentivos y los de los defensores. Con objeto de intentar comprender mejor esta disparidad de incentivos, hemos realizado una encuesta entre 200 profesionales de TI en el sector de los servicios financieros, y hemos comparado sus respuestas con las de 600 profesionales de TI de otros sectores en todo el mundo. En el **informe** se identifican tres diferencias de incentivos principales: entre las estructuras corporativas de las empresas de seguridad frente al 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 global.

Estructura corporativa frente a empresa delictiva

Ya hace tiempo que en el sector de los servicios financieros se conocen las ventajas de contar con incentivos claros y directos. Los ciberdelincuentes actúan en un entorno clandestino formado por freelancers con motivaciones claras, en el que priman la competición dinámica y la rapidez en la innovación. Esto estimula un alto grado de especialización, lo que permite a la élite de la ciberdelincuencia convertirse en verdaderos expertos en su campo, y genera una amplia red de proveedores y clientes. La información se comparte a través de una amplia variedad de canales y las nuevas vulnerabilidades se aprovechan rápidamente. La existencia de mercados activos facilita la búsqueda de clientes interesados y pone precio a la información y al código nuevos.

Según este estudio, las empresas de servicios financieros son las que están más cerca de conseguir un mercado de información abierto para la ciberdefensa. Son las más propensas a compartir información con otras empresas, incluidos partners (63 % frente al 52 % de encuestados de sectores no financieros), consultores externos (49 % frente al 39 %) e incluso competidores (26 % frente al 19 %). Solo el 7 % de los entrevistados afirmaron no compartir ningún tipo de información sobre ciberamenazas, frente al 14 % en otros sectores.

Esta disposición a compartir influye en las fuentes que utilizan las empresas de servicios financieros para tomar decisiones sobre ciberseguridad. Es un poco más probable que utilicen información que se ha compartido desde fuentes externas que en el caso de otros sectores. Esto incluye la inteligencia de proveedores de seguridad (63 % frente al 57 %), consultores externos (51 % frente al 46 %), y grupos industriales (26 % frente al 22 %). Es posible que esta información sea analizada y resumida por los operadores, ya que los profesionales de los servicios financieros son más propensos a utilizar informes internos que los de otras empresas (70 % frente al 61 %).

El apoyo a mercados abiertos para la ciberseguridad en el sector de los servicios financieros se extiende más allá de la información y llega a servicios y consultores. Las empresas de este sector son más propensas a invertir una parte importante de su presupuesto de ciberseguridad en consultores (49 % frente al 40 % de las empresas no pertenecientes al sector financiero), y un poco más propensas a invertir dinero en servicios profesionales para la supervisión y respuesta a incidentes (38 % frente al 34 %). Se ha demostrado que esta apertura a información de terceros y a especialistas externos tiene un impacto positivo en la eficacia de la seguridad.

Desconexión entre estrategia e implementación

En la actualidad la ciberseguridad es el principal riesgo para las empresas, según la mayoría de los encuestados de todos los sectores. Casi el 80 % de las empresas de servicios financieros informan a su consejo de administración sobre los riesgos para la ciberseguridad en la mayoría o en todas las reuniones, frente al 70 % de las empresas de otros sectores. Mientras que casi todos los entrevistados (95 %) del sector financiero afirmaron que su empresa cuenta con una estrategia de ciberseguridad destinada a hacer frente tanto a las amenazas nuevas como a las existentes, las dificultades surgen principalmente en la implementación. Solo algo más de la mitad (51 %) de las empresas afirmaron que tienen completamente implementada su estrategia de ciberseguridad, y el 8 % no ha implementado ni una parte.

Parte de la discrepancia entre la existencia de estrategias de seguridad y su implementación puede deberse a una preocupación errónea de la naturaleza de los riesgos para las empresas. Los cuadros directivos de estas empresas de servicios financieros parecían, de media, más preocupados por el daño a la reputación de la empresa (67 %) que por la pérdida de ingresos o beneficios (50 %). Si tenemos en cuenta el aumento reciente de los robos directos en el sector financiero, frente a las pérdidas por fraude como consecuencia del robo de números de tarjetas de crédito, esta actitud puede dar una falsa sensación de seguridad.

Las empresas que ponen en práctica su estrategia de seguridad muestran un nivel de **madurez en seguridad** por encima de la media. En orden de prioridades, estos equipos de seguridad daban más importancia a la defensa proactiva, seguida de la investigación sobre nuevas estrategias y soluciones y, por último, la defensa reactiva. Y lo que posiblemente sea más importante, dedican la menor cantidad de tiempo a tareas no relacionadas con la ciberseguridad, un 8 % frente al 14 % de los equipos de otros sectores.

Al tratarse de un sector castigado desde hace mucho tiempo por los ciberataques, no sorprende que el 73 % de los profesionales de los servicios financieros consideraran adecuado su presupuesto para implementar su estrategia, frente a solo el 58 % de otros sectores industriales. Solamente un pequeño número de empresas del sector financiero tenían la percepción de que su presupuesto (4 %) o su personal (9 %) era insuficiente, y que esto afectaría negativamente a la implementación de su estrategia.

Otra disparidad entre estrategia e implementación se refiere a los métodos utilizados para garantizar que las medidas de ciberdefensa no expongan a la empresa a nuevos riesgos. Aunque la mayoría de las empresas financieras (73 %) afirmaron mantener una plataforma de seguridad que integra tecnologías nuevas y existentes, un número similar (70 %) reconoció 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 a la reputación de su víctima. Es más probable que los equipos de ciberseguridad de los servicios financieros disfruten de incentivos, como el reconocimiento (55 % frente al 48 % de los de otros sectores) y las bonificaciones (53 % frente al 43 %). Solamente el 9 % de los encuestados afirmaron no tener actualmente ningún incentivo, frente el 21 % de otros sectores. El principal elemento disuasorio para evitar comportamientos arriesgados relacionados con la ciberseguridad por parte de los empleados es la amenaza de acciones legales (69 % frente al 59 %). Además, el 56 % de los profesionales de TI del sector financiero afirman que la implementación de la estrategia se incorpora a sus evaluaciones de rendimiento individuales, frente a solo el 46 % de los pertenecientes a otros sectores.

Para determinar si la estrategia está cumpliendo los objetivos se necesita un conjunto de parámetros suficientemente detallado. Solo el 1 % de los encuestados del sector de los servicios financieros afirmaron ser incapaces de determinar si estaban cumpliendo objetivos, frente al 7 % de los de otros sectores. Si bien no es una mayoría significativa, un número mayor de encuestados de equipos de ciberseguridad del sector financiero afirmaron disponer de métodos apropiados para la evaluación de la estrategia que otros sectores, como actividades de gestión de riesgos (66 % frente al 57 %), y tiempo de resolución medio (52 % frente al 45 %).

Lecciones de la ciberdelincuencia

Parece que las empresas de servicios financieros, con una larga trayectoria en distintos mercados, son las que muestran menos diferencias en cuanto a los incentivos para la ciberseguridad. Ya son los mayores usuarios de servicios de consultaría y seguridad externos, pero probablemente podrían darle más importancia a la inteligencia sobre amenazas y a la información de seguridad externa que a sus informes internos. Parece que los procesos de seguridad de estos equipos maduran bien, y deberían seguir centrándose en soluciones integradas en lugar de utilizar productos de seguridad que se solapan. Puede que también necesiten prestar más atención a las nuevas amenazas y al riesgo de pérdidas financieras reales en lugar de centrarse en los daños a su reputación, ya que el objetivo de los agresores es cada vez más apropiarse de fondos directamente (se pueden citar a modo de ejemplo el aumento de los troyanos bancarios para dispositivos móviles, el robo a través del sistema interbancario SWIFT en Bangladesh o el ataque a las cuentas de Tesco Bank).

Lecciones del mercado de la ciberdelincuencia	Los delincuentes	Los defensores
Aprovechamiento de las fuerzas del mercado	**La delincuencia como servicio**	**Seguridad como servicio (SaaS)**
	El mercado de la ciberdelincuencia, que es abierto y descentralizado, aprovecha la competencia y los precios para minimizar las barreras de acceso, impulsar la innovación y ayudar a las iniciativas empresariales que prosperan a ganar escala rápidamente.	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.
Divulgación pública	**Dirigir los ataques a vulnerabilidades conocidas**	**Mejora de las prácticas de aplicación de parches**
	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.	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**	**Intercambio de información y colaboración**
	Los foros abiertos y la publicidad facilitan la proliferación de nuevos ataques y modelos de negocio delictivos, así como la adopción generalizada de las mejores prácticas.	Ampliar el intercambio de información recorta costos para los defensores gracias a una reducción de la duplicación. Además, 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"**	**Aprovechamiento de la reserva de talento global**
	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.	Contar con una reserva de expertos más amplia, multinacional y demográficamente diversa 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**	**Incentivos por 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.	Para equiparar los incentivos de los directivos con los de los operadores, se deben ofrecer compensaciones y bonificaciones a los empleados y administradores que consiguen buenos resultados en seguridad.

Para obtener más detalles sobre la disparidad de incentivos en la ciberseguridad, con un desglose por país y sector vertical, descargue el informe completo, **Why Offense Beats Defense: Misaligned Incentives** (Por qué los ciberdelincuentes superan a los defensores: disparidad de incentivos).

McAfee LLC
2821 Mission College Blvd,
Santa Clara, CA – 95054, USA
www.mcafee.com/mx

MARZO DE 2017