Kaspersky®
Threat Intelligence

Casos estratégicos para usar la inteligencia de amenazas

Nuestras vidas dependen de Internet en gran medida, pues el bajo coste y la alta velocidad de las comunicaciones que proporciona lo convierten en un componente fundamental y crítico para que los gobiernos y empresas alcancen el éxito. Los entornos dinámicos e interconectados proporcionan varias funciones importantes con la posibilidad de mejorar las comunicaciones, proteger información personal, confidencial y de otro tipo; y proporcionar la supervisión y el control de los sistemas críticos y los procesos empresariales, a la vez que se fomenta la competencia. No obstante, la siempre creciente interconectividad expande la superficie de ataque y los adversarios se preparan para aprovecharse de cualquier vulnerabilidad posible en cada nivel.

A lo largo de los dos últimos años, hemos observado la pérdida de límites entre los diferentes tipos de amenazas y actores de amenazas. Un ejemplo de ello es el vertido de código que realizó el grupo Shadow Brokers y que puso una serie de exploits avanzados (desarrollados deliberadamente por la NSA) al alcance de grupos criminales que, de otro modo, no habrían tenido acceso a aquel tipo de código tan sofisticado. Otro ejemplo es la aparición de campañas de amenazas persistentes avanzadas (APT por sus siglas en inglés) centradas no solo en el ciberespionaje, sino en el robo de dinero para financiar otras actividades a las que se dedica el grupo APT.

Los motivos de los actores de amenazas varían bastante, desde robo de dinero a socavar a la competencia, robar identidades y cometer fraude. Además, cada industria y organización tiene su información única que proteger, un conjunto único de aplicaciones, tecnologías que emplean, etc. Todo ello supone un alto nivel de variabilidad en el modo en que se ejecutan los ataques, y cada día aparecen nuevos tipos.

En el rápidamente cambiante panorama de las amenazas, dirigir el crecimiento de un negocio mediante la transformación digital puede ser todo un reto y los líderes de las empresas deben adoptar una estrategia sopesando constantemente los riesgos con los objetivos y prioridades de la empresa.

Comprender los riesgos permite tomar decisiones informadas, por ejemplo: cuando se lanza una nueva iniciativa, se abre una nueva oficina regional o se planea una inversión tecnológica. También ayuda a desarrollar estrategias proactivas de mitigación y a justificar el presupuesto asignado, así como las necesidades de personal.

La inteligencia de amenazas estratégica proporciona una visión sobre las tendencias en amenazas, las técnicas y métodos que emplean los atacantes, así como sus motivos y atribuciones, lo que ayuda a responder una serie de preguntas específicas:

- ¿Quiénes son sus adversarios? ¿Qué quieren?
- ¿Qué grupos de amenazas están activos en su sector o región?
- ¿Qué vectores de ataque se emplean?
- ¿Cuál es el mejor modo de organizar un ataque contra su organización?
- ¿De qué rutas e información dispone un atacante que vaya tras usted ?
- ¿Se ha llevado a cabo ya un ataque? ¿Se encuentra en un peligro inminente?
- ¿Qué acciones se deben llevar a cabo para reducir su perfil de riesgo?

Comprender estas preguntas y esquematizar las preguntas de sus activos, sistemas y procesos empresariales críticos le permite desarrollar un análisis de riesgos exhaustivo y comunicar claros escenarios de riesgos relevantes a su equipo directivo y, así, justificar las inversiones en programas, tecnologías y personal. Con esta información, una empresa puede centrar su estrategia de protección de la información en las áreas principales en las que se centran los cibercriminales y actuar con rapidez y precisión para repeler a los intrusos y minimizar el riesgo de que un ataque tenga éxito.

Kaspersky Lab ofrece:

Tipo de informe	Inteligencia proporcionada	Caso de uso
APT Intelligence Reporting	• Descripciones de tácticas y métodos usados por los atacantes en campañas de ciberespionaje con objetivos intersectoriales • Los perfiles de los actores de amenazas con las TTP (Tácticas, Técnicas y Procedimientos) que usan • Cotejar los TTP asociados con MITRE ATT&CK, una base de conocimiento de TTP adversarios basada en experiencias del mundo real	• Comprender los actores de amenazas que acechan a su industria o región y los TTP que usan • Identificar qué información y sistemas están en riesgo, el impacto potencial al verse comprometidos y cómo dar prioridad • Ajustar las estrategias de la seguridad de la información, planear y justificar las inversiones en tecnología, personal y programas que cubran posibles vectores de ataque
Financial Threat Intelligence Reporting	• Descripciones de tácticas y métodos usados por los que atacan el sector financiero • Información sobre ataques en infraestructuras específicas, como cajeros o terminales TPV • Información sobre herramientas adaptadas para atacar redes financieras que usan, desarrollan y venden los cibercriminales en comunidades y foros de la Darknet de diferentes lugares	• Identificar a los adversarios que vayan tras instituciones financieras y los TTP que usan • Identificar la información y sistemas en riesgo, el impacto potencial de verse comprometido y cómo dar prioridad • Ajustar las estrategias de seguridad de la información, planear y justificar inversiones en tecnología, personal y programas que cubran posibles vectores de ataque
Customer-specific Threat Intelligence Reporting	• Identificación pasiva del perímetro de red, servicios disponibles y vulnerabilidades existentes • Análisis personalizado y análisis de exploits • Identificación, monitoreo y análisis de cualquier muestra de malware activa o no que vaya tras su organización • Filtrado de información y datos • Amenazas phishing que van tras las marcas de los clientes • Evidencia de amenazas y actividad botnet que amenacen a los clientes, socios y proveedores de la empresa • Análisis específico de la industria que incluye los TTP relevantes	• Garantizar la disponibilidad y correcta asignación de recursos para mitigar los errores de seguridad identificados • Informar de auditorías de compra de terceros para contrarrestar los ataques en la cadena de suministro • Ajustar las políticas y controles para mitigar posibles amenazas internas • Aumentar el conocimiento en seguridad del personal interno desarrollando un programa específico basado en hechos (p. ej. Credenciales corporativas comprometidas por servicios de terceros) • Mitigar los posibles daños de reputación monitoreando el uso no autorizado de las marcas de la empresa con fines phishing • Planificar y justificar las inversiones tecnológicas, de personal y en programas que cubran los vectores de ataque relevantes

Kaspersky Lab
Ciberseguridad empresarial: **www.kaspersky.com/enterprise**
Noticias sobre ciberamenazas: **www.securelist.lat**
Noticias sobre seguridad de TI : **business.kaspersky.com/**

#truecybersecurity
#HuMachine

latam.kaspersky.com