

ENTHEC[®]

El Riesgo Digital y su relación con el Riesgo Corporativo

La importancia de la Ciberseguridad para las compañías aseguradoras en el análisis de riesgo global y cómo se puede utilizar para reducirlo.

kartos[®]
XTI watch**bots**

La ciberseguridad es un problema de Gobierno y Riesgo corporativo

Aunque es cierto que la concienciación sobre el Riesgo Digital y la necesidad de potentes sistemas de Ciberseguridad es cada vez mayor en los Comités de Dirección de las organizaciones, en general existe la sensación de que es algo que compete exclusivamente al departamento de IT. En lo que se refiere a los aspectos técnicos, esto es verdad. Pero en el impacto de un posible ataque a la organización, las posibles repercusiones pueden afectar a todos y cada uno de los departamentos de la organización y causar a esta importantes daños operacionales, reputacionales, legales, de propiedad intelectual y económicos.

En este documento vamos a analizar cuáles son los riesgos para una organización de seguir una estrategia de Ciberseguridad defectuosa y cómo prevenirlos con el Servicio de Análisis de Ciberriesgo de las empresas aseguradores y analistas de riesgos.

La ciberseguridad en las organizaciones

Es un hecho que la inversión en Ciberseguridad de las organizaciones no ha dejado de crecer en los últimos años y ninguna previsión indica que esta tendencia vaya a cambiar. Frente a este dato, es también un hecho que, a pesar de ello, el número de ciberataques con éxito realizados a empresas tampoco deja de crecer, a pesar de la mejora en los sistemas de detección y defensa.

¿Cuál es la razón para que se den simultáneamente dos hechos aparentemente contradictorios?

Es imposible proteger una organización si no se dispone de toda la información.

Actualmente los sistemas de Ciberseguridad se basan en la información que recopilan de lo que se conoce como perímetro IT. Es decir, la infraestructura tecnológica que puede ser monitorizada y protegida con los recursos y los límites legales de una organización. De vez en cuando, se realizan ataques de intrusión y tests de vulnerabilidades para detectar fallos en los sistemas que puedan ser utilizados por los Ciberdelincuentes. Y con esta información, se intenta blindar la compañía.

El enfoque de blindaje sobre información del perímetro interno tiene al menos cinco puntos débiles:



FALTA DE INFORMACIÓN

Las organizaciones no llegan a toda la información corporativa sensible que está en la red a disposición de los cibercriminales y que les puede proporcionar una vía de entrada.



FACTOR COSTE

Si el nivel de protección de la organización se basa en el blindaje de cada elemento este deberá aumentar cada vez que se añada uno nuevo, haciéndolo ineficiente e inabordable.



FACTOR HUMANO

Por muy alto que sea el blindaje del perímetro interno IT, el factor humano es la primera causa desencadenante de un ciberataque a través de la ingeniería social, y es un factor que no puede ser blindado.



PERÍMETRO IT

Los límites de Ciberseguridad van más allá del perímetro IT, ya que se extienden hasta todos los proveedores, colaboradores o terceros con los que se comparte información y que acceden a sus sistemas.



FACTOR TIEMPO

Un factor crítico es la cantidad de tiempo que una vulnerabilidad está abierta o que una información está disponible, ya que multiplica la posibilidad de que se utilice.

El impacto del Riesgo IT en el Riesgo Corporativo

Un evento de ciberseguridad en el negocio de la organización que permita a los cibercriminales simplemente disponer de información de uso restringido o el acceso a la organización, a sus empleados o a los terceros con los que se relaciona, puede provocar:

- 1 Interrupción del servicio TI y de la operativa de la organización.
- 2 Fraude, pérdidas económicas estafas, robo, chantajes.
- 3 Fallos en el sistema de atención y relación a clientes.
- 4 Robo, publicación y venta de propiedad intelectual o industrial.
- 5 Robo de información relacionada con la competitividad, pérdida de posicionamiento.
- 6 Ataques orientados a causar daño legal aprovechando fallos en cumplimiento.
- 7 Disminución en la satisfacción de los clientes por atención o incumplimiento.
- 8 Daños reputacionales. Pérdida en el valor de marca y disminución de la confianza.
- 9 Publicación de datos personales de empleados, clientes y terceros.
- 10 Suplantación de identidad de la empresa o personas relacionadas con ella.

Factores de riesgo para cada CXO

Por la propia naturaleza de su trabajo, dentro de los departamentos de una organización se desarrollan tareas que pueden poner a la compañía en riesgo de un ciberataque. Por ello, todos son responsables de tomar las medidas protectoras dentro de su área de responsabilidad.

En las estrategias evolucionadas de ciberprotección, la Ciberseguridad y el Riesgo IT han dejado de considerarse responsabilidad exclusiva de CI para confirmarse como una responsabilidad conjunta del Board. Un problema de Riesgo Corporativo.



CEO

Vela por la integridad de la organización, por su reputación, su propiedad intelectual y por garantizar la continuidad de negocio y la protección de sus empleados.



CISO

Es el responsable último del Riesgo, la protección de la información corporativa y la estrategia de Ciberseguridad de la organización.



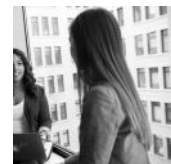
CMO

Vela por la reputación de la marca y por que la relación con los clientes esté basada en la confianza plena respecto a la protección de sus datos.



CFO

Es el responsable de evaluar el riesgo de proveedores y partners, en el que debe considerar el Riesgo IT en los casos de terceras partes.



LEGAL / COMPLIANCE

Vela por el cumplimiento de la legislación específica sobre tratamiento y protección de la información y los datos sensibles que maneje la organización.

Cibervigilancia

XTI

Cibervigilancia XTI: EASM + DRPS + SRS

Ofrece a tus clientes un Servicio de Valoración del Riesgo TI de su organización o de terceros que puedan comprometer su seguridad, a través de una plataforma de cibervigilancia XTI que además te permite evaluar el riesgo de cualquier Ciberpóliza y controlar el riesgo TI de tu propia Compañía Aseguradora.

1

EXTERNAL ATTACK SURFACE MANAGEMENT:

Detección de activos corporativos e información sobre sistemas, servicios en la nube y aplicaciones que están disponibles y visibles en el dominio público para cualquier ciberdelincuente.

2

DIGITAL RISK PROTECTION SERVICES:

Detección de información contextual sobre posibles agentes de ataques, sus tácticas y procesos para llevar a cabo actividades maliciosas. Eliminación de actividades maliciosas en nombre de la organización.

3

SECURITY RATING SERVICES:

Evaluación independiente de riesgos propios y de terceros, para una visualización amplia de la madurez en ciberseguridad de cualquier organización utilizando un enfoque externo. Ampliación y ponderación de la información proporcionada por los métodos tradicionales de evaluación de riesgos por terceros.

Servicios de Análisis de Riesgo Corporativo TI

Hacemos posible que las compañías aseguradoras puedan ofrecer a sus clientes un servicio de evaluación de riesgo corporativo por causas relacionadas con TI de una manera entendible por personas no formadas en Ciberseguridad, y además, valorar con exactitud el nivel de riesgo para cualquier Ciberpóliza



¿Cuál es el nivel de Riesgo TI que podré analizar?

Se proporcionan una indicación global de TI basado en el conocimiento que los cibercriminales tienen sobre las vulnerabilidades y los puntos débiles de la organización, y que por tanto reflejan de la manera más fiel posible cómo puede ser atacada la compañía y con qué impacto. Por eso es tan fiable.



¿Qué tipo de Riesgos podré controlar?

La información se estructura en nueve categorías diferentes entre las que se incluyen el análisis exhaustivo de documentos filtrados y de lo que se habla en redes sociales sobre la organización. Por tanto, además de los riesgos relacionados con la infraestructura tecnológica de la organización, se detectan riesgos relacionados con la protección de datos, el robo de información confidencial o de propiedad industrial, o riesgos de ataques reputacionales, que son indetectables por los sistemas de Ciberseguridad de las organizaciones.

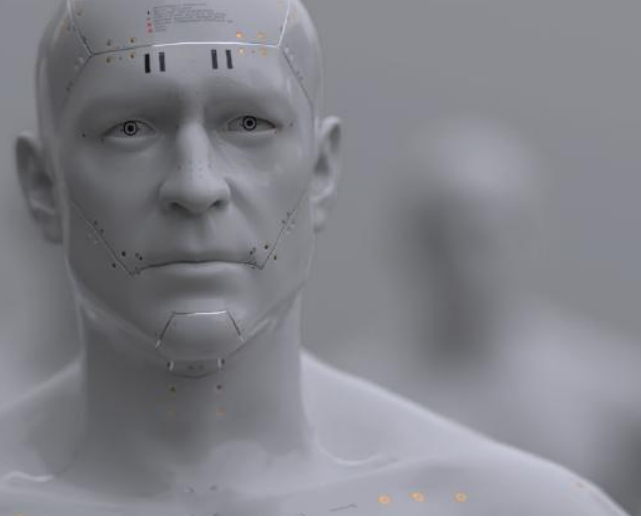


¿Para quién será de utilidad esta información?

- i. La información está diseñada para que los analistas de riesgos corporativos puedan ofrecer a sus clientes información de valor sobre los riesgos TI y el impacto que pueden tener en la situación de riesgo de la compañía en un lenguaje que puedan entender. Esto puede aplicarse a la propia organización o a organizaciones de terceros de los que se necesite hacer una valoración de la situación de riesgo.
- ii. Igualmente esta información puede utilizarse para el cálculo en tiempo real del nivel de riesgo de las compañías en la evaluación de Ciberpólizas.
- iii. Finalmente, puede compartirse con el CISO o responsable de Ciberseguridad para proporcionarle una visión del nivel de riesgo en el perímetro externo de la compañía que complemente la que le proporcionan sus sistemas.

kartos[®]

XTI watchbots



Kartos es la plataforma de cibervigilancia desarrollada por Enthec Solutions para extender el perímetro de seguridad controlado por las organizaciones e instituciones. Concebida desde un enfoque de estrategia hacker, Kartos está en permanente proceso de I+D para incorporar categorías y capacidades adelantadas a la evolución de los ciberataques.

Kartos XTI Watchbots: EASM + DRPS + SRS en una sola plataforma

A través de la monitorización y el análisis continuo de sus XTI Watchbots por la superficie externa, sin necesidad de implementación dentro del sistema IT corporativo ni de complicadas configuraciones **Kartos** facilita a las organizaciones el control y la neutralización de la información corporativa filtrada y expuesta, a la vez que permite la evaluación de riesgo corporativo por causas relacionadas con TI y terceros, de una manera asequible incluso para personas sin formación específica en Ciberseguridad.



Capa de IA que permite el funcionamiento 100% automatizado sin intervención humana en ninguna parte del proceso.



Funcionamiento continuo 365x24x7, lo que permite detectar filtraciones de nueva información prácticamente en tiempo real



Herramienta estrictamente no intrusiva. La investigación se realiza en Internet, la Deep Web y la DarkWeb y no se ataca el perímetro IT de las compañías, por lo que su funcionamiento y la información obtenida cumplen estrictamente con los límites impuestos por la legislación.



Máxima sencillez de uso. No requiere ninguna configuración compleja. Basta con introducir el dominio en la plataforma y funciona de manera autónoma, sin necesidad de configurar parámetros de búsqueda ni de cualquier otro criterio de localización de información.



Única plataforma que analiza las **conversaciones en redes sociales desde la perspectiva de detección de amenazas** y ataques, más allá de la relativa a reputación y branding.



Monitorización automatizada, objetiva y continúa de los riesgos causados por las terceras partes que pertenecen a la Superficie de Ataque Externa de la empresa.

Funcionalidades

Análisis de 9 categorías de amenazas

- Red
- Salud de DNS / Phishing
- Gestión de Parches
- Reputación IP
- Seguridad Web
- Seguridad e-mail
- Filtración de Documentos
- Filtración de Credenciales
- Redes Sociales

Configuración personalizable

- Personalización de contenidos y permisos de seguridad por departamentos corporativos y usuarios.
- Personalización de alarmas en tiempo real por vulnerabilidades.

Ciberseguridad en redes sociales

- Enfoque único en el mercado que consiste en el análisis de las principales redes sociales para detectar conversaciones que puedan hacer sospechar de un ataque en preparación.
- Detección de conversaciones en redes relacionadas con hacktivismo, fraude, phishing o campañas de fake news, entre otras.

Sencillez en la interpretación y el uso

- Información dividida en tres niveles y presentada de forma gráfica para que pueda mostrarse a personas sin conocimientos específicos de Ciberseguridad o a los expertos que deben solucionar problemas.

Modelo flexible de licencias

- Estructura de licencias anuales adecuada en coste y funcionalidades a las necesidades de cada organización, de acuerdo a los diferentes casos de uso en los que esté interesada.

Casos de uso

Servicio de Análisis de Riesgo TI a clientes

Uso de Kartos como base de la oferta del Servicio de Análisis de Riesgo TI a clientes, con detección de la información filtrada y expuesta en la red, así como de las brechas de seguridad que provocan dichas filtraciones, tanto propias como de terceros relacionados con el cliente.

Valoración del Riesgo TI de Ciberpólizas

Uso de Kartos como herramienta para evaluar el nivel de madurez de la estrategia de Ciberseguridad de una organización y sus partners o proveedores, que complemente el resto de medidas de valoración del Riesgo TI de una Ciberpóliza.

Detección de amenazas propias

Uso de Kartos para la detección de toda la información corporativa propia filtrada y expuesta en la red y riesgos de terceros, así como de las brechas de seguridad que provocan dichas filtraciones para tomar las acciones de remediación, protección y defensa necesarias.



Enthec es una Deep Tech de desarrollo y fabricación de software de Ciberseguridad con enfoque hacker, para extender el alcance de las estrategias de ciberprotección de las organizaciones.

Fundada como startup en 2019 por María Rojo, Enthec ha crecido a través de rondas de financiación y del éxito de su plataforma Kartos hasta consolidarse como una de las Deep Tech con soluciones más innovadoras y eficaces en el campo de la Ciberseguridad.

Para conocer más sobre nosotros, puedes entrar en nuestra web:

www.enthec.com

Si quieres probar de forma gratuita nuestra plataforma Kartos XTI Watchbots y conocer de qué forma puede ayudarte a ampliar tu oferta de Servicios de Análisis de Riesgo TI y a evaluar el Riesgo TI de cualquier Ciberpóliza, puedes ponerte en contacto con nosotros a través de esta dirección de correo:

hello@enthec.com



kartos®
XTI watch**bots**

¡Gracias!

© 2023 Enthec Solutions S.L.
Todos los derechos reservados.

Queda prohibida la reproducción total o parcial de este documento por cualquier medio sin la debida autorización.