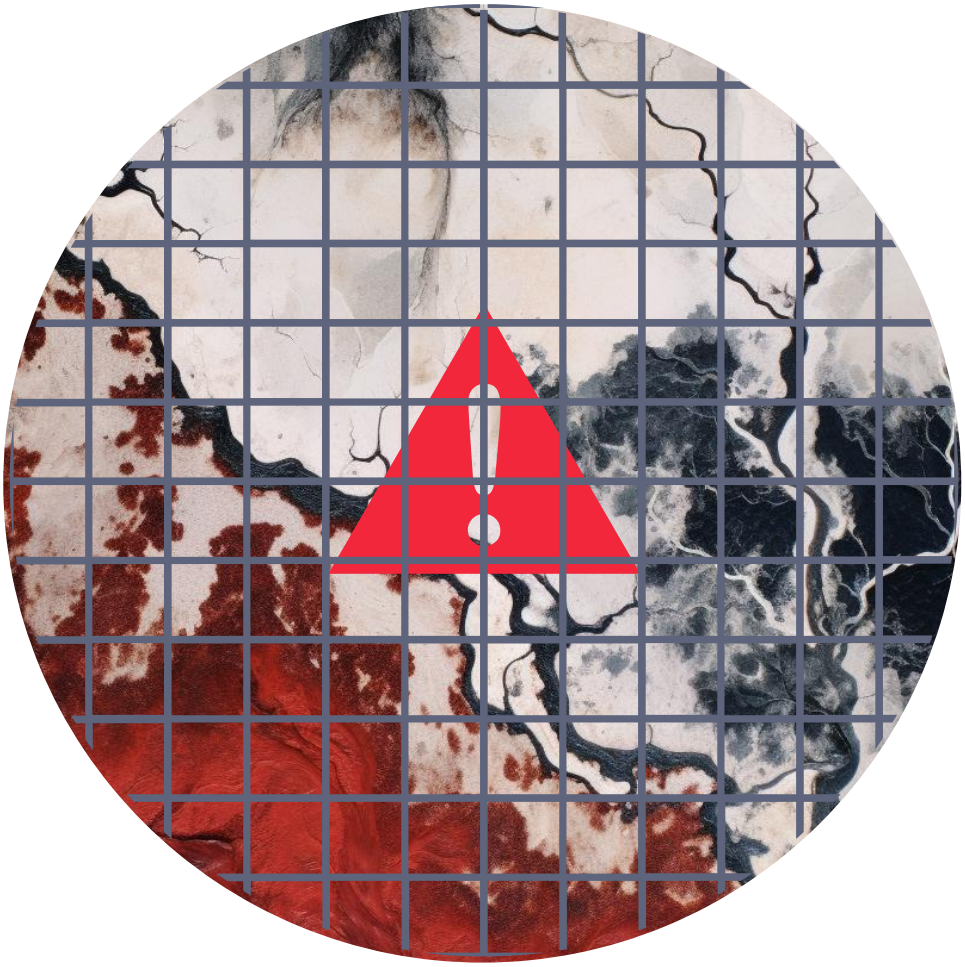
ENTHEC

WHITEPAPER

TOP 10 VULNERABILIDADES EN RED

Identificar y prevenir



ÍNDICE

Introducción 02

Top 10 vulnerabilidades más frecuentes en la Red 03

1. Leak de credenciales
2. Subdominios
3. Registro en portales de dudosa confianza
4. CMS desactualizados
5. Bases expuestas
6. Documentación protegida por el RGPD
7. Información sensible o crítica de la organización
8. Código fuente
9. Gestión de proyectos
10. Servicios expuestos

Kartos XTI Watchbots 20

INTRODUCCIÓN

Las organizaciones utilizan una gran cantidad de recursos para proteger su perímetro de seguridad y evitar la entrada de ataques y la fuga de información. Su objetivo es tener bajo control lo que ocurre dentro de la organización para detectar situaciones irregulares, neutralizarlas y minimizar sus efectos. En los últimos años, los sistemas y los equipos de ciberprotección corporativa se han ido perfeccionando y modernizando, utilizando nuevas tecnologías como la inteligencia artificial o el machine learning para proteger ese perímetro de seguridad.

Sin embargo, en este mismo tiempo, los ciberataques de éxito no solo no han disminuido, sino que han aumentado de forma alarmante.

El éxito de esos ataques radica en la cantidad de información sobre la organización atacada que los ciberdelincuentes manejan y que les facilita la preparación de un ataque muy difícil de neutralizar.

•¿Qué está fallando en la protección del perímetro de seguridad de las organizaciones?
•¿De qué forma y dónde consiguen los ciberatacantes acceso a toda esa información corporativa?

En el siguiente documento vamos a analizar las diez vulnerabilidades de seguridad corporativa más habituales que se pueden encontrar en la red y que son explotadas por la ciberdelincuencia para planificar su ataque de éxito. Y también descubriremos por qué asegurar el perímetro de las organizaciones pero no controlar lo que hay fuera de ellas compromete la seguridad de todos sus sistemas.

TOP 10 VULNERABILIDADES

1. LEAK DE CREDENCIALES

Pese a que la protección de las credenciales es prioridad en cualquier organización, la fuga de las mismas sigue siendo una de las vulnerabilidades más habituales que podemos encontrar en la red, sobre todo en los últimos tiempos

Las credenciales son la llave de entrada a los sistemas. Con acceso a la credencial corporativa de una sola cuenta, los ciberdelincuentes pueden tomar su control, moverse sin ser descubiertos dentro del sistema de la organización y obtener acceso a información confidencial y sensible, propiedad intelectual o a fondos.

Pese a que la protección de las credenciales es prioridad en cualquier organización, la fuga de las mismas sigue siendo una de las vulnerabilidades más habituales que podemos encontrar en la red, sobre todo en los últimos tiempos en los que el trabajo híbrido, y en muchos casos implementado con urgencia, ha provocado un aumento alarmante de este tipo de fugas. Normalmente, las organizaciones utilizan protocolos que obligan a cambiar las contraseñas cada poco tiempo para evitar que una fuga de credenciales no detectada pueda tener consecuencias graves, ya que, gracias a estas actuaciones, las listas de credenciales filtradas dejan de tener validez en muy corto plazo. Esto puede dificultar, en cierta forma, el primer objetivo de un robo de credenciales: tomar el control de una cuenta de un perfil muy concreto de la organización, como el CEO, el CISO, CFO o directivos del board principal.

Según el informe de Artic Wolf, en 2022 una organización tenía de media unas 17 listas de credenciales corporativas disponibles en la Dark Web, esperando a ser utilizadas por cualquier ciberdelincuente interesado.

TOP 10 VULNERABILIDADES

1. LEAK DE CREDENCIALES

La actualización constante y rutinaria de contraseñas suele provocar en los usuarios la adquisición de patrones que les permitan recordar cada nueva credencial sin esfuerzo, para evitar tener que dejar constancia de ella en lugares en los que podría quedar al descubierto. Esas contraseñas no utilizan siempre una misma palabra, porque los sistemas de autenticación no la darían como válida y por eso lo que se suele repetir es el patrón para elegir las palabras, cifras y símbolos de cada nueva contraseña. Una fuga de contraseñas puede darle a un ciberdelincuente las claves del patrón utilizado por un determinado usuario, de forma que pueda deducir en qué van a consistir las siguientes actualizaciones de algunas de las contraseñas corporativas y tener llave de entrada a la largo plazo al sistema de la organización sin necesitar nada más.

También, la fuga de credenciales faculta al ciberdelincuente para estudiar durante el tiempo en el que esa contraseña sea válida, las costumbres, aficiones y rutinas del usuario, de forma que luego, cuando diseñe el ciberataque, le será más fácil lograr que ejecute algún tipo de acción, como la descarga de un archivo del que no pueda sospechar, para introducir ransomware en el sistema corporativo.

Por lo tanto, la filtración de credenciales no solo supone un riesgo en cuanto al control de las cuentas corporativas más relevantes, sino también por la cantidad de opciones de ataque que ofrece al ciberdelincuente.

Acciones a realizar

Monitorizar qué credenciales corporativas están disponibles para cualquiera que quiera encontrarlas en la Web, Deep Web y Dark Web para tomar medidas de protección proactiva que neutralicen la utilización fraudulenta de las mismas para realizar un ataque contra la organización.

Establecer protocolos de actualizaciones períodicas

Sensibilizar y formar en seguridad a los usuarios con el fin de hacerlos conscientes de sus propios patrones de actualización y la necesidad de evitarlos

TOP 10 VULNERABILIDADES

2. SUBDOMINIOS

Un subdominio abandonado es una puerta de entrada a un ciberataque y, también, una fuente de valiosa información para un ciberdelincuente.

A lo largo de su desarrollo, una organización crea una gran cantidad de subdominios para productos paralelos, productos temporales, campañas publicitarias, campañas de marketing... Cualquier actividad habitual en una empresa conlleva crear un subdominio con una página web detrás del mismo, que es publica durante el tiempo que la organización lo necesite.

Muchos de esos subdominios están activos mientras dura la operación para la que fueron creados y después, simplemente, se abandonan. El primer problema derivado de este abandono es el paso del tiempo: las personas que trabajan hoy en una organización no tienen capacidad para conocer qué subdominios se utilizaron y luego fueron abandonados en etapas anteriores. Además, en las organizaciones pequeñas y medianas, suele ocurrir que no hay una figura profesional dedicada a la gestión centralizada de estos subdominios, de forma que cada uno es gestionado por el departamento que lo activó. En las organizaciones más grandes, la existencia de sedes en diferentes países dificulta dicha gestión centralizada de subdominios.

Todos estos factores influyen en que dentro de la cultura de seguridad corporativa, los subdominios abandonados no sean percibidos en la mayoría de los casos como una vulnerabilidad, y que una cantidad considerable de organizaciones ni siquiera sea consciente de su existencia.

TOP 10 VULNERABILIDADES

2. SUBDOMINIOS

Brechas de seguridad

- **Falta de actualización:** La primera brecha de seguridad de un subdominio abandonado está provocada porque, al dejar de utilizarse, también deja de actualizarse y, por lo tanto, de implementar las soluciones de protección que van desarrollándose para neutralizar las nuevas formas de ciberataque que van surgiendo. Un subdominio abandonado que deja de ser actualizado es una puerta abierta de entrada al sistema de la organización.
- **Integración abandonada:** El proceso más frecuente de abandono de los subdominios corporativos que apuntan a un servicio con integraciones de terceros es la inactivación del servicio, pero no del subdominio, que queda a merced de ser encontrado por un ciberdelincuente y reactivado como una integración fraudulenta desde la que activar un ciberataque.
- **Datos no borrados:** Un subdominio abandonado es un contenedor de información sensible de la organización, que pueden ser utilizados tanto para el diseño de un ciberataque contra ella, como para usurpar su identidad para ciberestafas a terceros.

Acciones a realizar

Establecer estrictos protocolos de inhabilitación de los subdominios que hayan cumplido su función y no vayan a ser utilizados en el futuro, incluido el borrado de todos los datos incluidos en ellos.

Centralizar la gestión de los subdominios corporativos.

Detectar los subdominios corporativos abandonados en la Web, Deep Web y Dark Web y crear un listado para su control periódico.

Controlar las brechas de seguridad de los subdominios corporativos abandonados para protegerse frente a ellas.

Inhabilitar los subdominios corporativos abandonados detectados

TOP 10 VULNERABILIDADES

3. REGISTRO EN PORTALES DE DUDOSA CONFIANZA

Los registros en portales de confianza dudosa no solo ponen en peligro la seguridad de la organización al ser susceptibles de convertirse en un vector de entrada de ciberataques. La asociación de activos corporativos a algunos de esos portales pueden suponer un peligro para la reputación de la organización o convertirse en información con la que negociar a cambio de su no difusión.

Todas las organizaciones tienen establecidas prohibiciones expresas de utilización del correo electrónico corporativo para fines y actividades que no estén relacionadas con la actividad y el negocio empresariales, muchas de ellas, con sanciones por incumplimiento de las mismas.
Puede parecer que el registro de direcciones de correo corporativo en páginas de dudosa reputación y seguridad es una vulnerabilidad del pasado superada por la concienciación de las personas que trabajan en las organizaciones. Sin embargo, la realidad es diferente.

La ley ampara el uso privado de los dispositivos tecnológicos corporativos por parte de los empleados y establece criterios de adecuación y comunicación fehaciente para las inclusiones, prohibiciones y exclusiones de actividades dentro del mismo.

El trabajo híbrido y los dispositivos tecnológicos corporativos móviles propician que la frontera entre el uso laboral y el uso privado se difumine y que se utilicen para los registros y las visitas a portales de dudosa confianza. El uso privado de estos dispositivos está protegido, además, por el derecho a la intimidad del trabajador, de forma que no siempre y en todos los casos, las organizaciones pueden controlar el historial de actividad de dichos dispositivos.

Junto a ello, las estadísticas de portales de contenido para adultos muestran que, entre semana, después de la franja nocturna, la siguiente franja en la que más visitas se realizan está dentro del horario laboral.

TOP 10 VULNERABILIDADES

3. REGISTRO EN PORTALES DE DUDOSA CONFIANZA

Acciones a realizar

Utilizar de forma continua los medios que la ley permite a las organizaciones para controlar la actividad en la red de los dispositivos corporativos, sin menoscabar en ningún caso el derecho a la intimidad de los trabajadores que operan con ellos.

Formar y concienciar periódicamente a los trabajadores de la organización sobre ciberseguridad y medidas de protección y actuación.

Detectar los registros con dominios corporativos que existen en los portales de dudosa reputación para su control y anulación

TOP 10 VULNERABILIDADES

4. CMS DESACTUALIZADOS

Para un ciberdelincuente, dar con alguna vulnerabilidad en el código de los CMS supone encontrar el vector de entrada a una gran cantidad de sitios y por eso siempre están en su punto de mira. Un CMS desactualizado es una puerta de entrada a un servidor y a la infraestructura de una organización.

Cerca del 90% de los sitios que han sufrido ciberataques pertenecen a desarrollos creados a través de CMS y una gran cantidad de páginas web son hackeadas al día en el mundo. Enviar campañas de spam a través del servidor corporativo o robar datos de los usuarios de la web de la organización son algunas de las consecuencias que puede tener un CMS que no esté siendo debidamente mantenido. Conscientes de ser un objetivo permanente de la ciberdelincuencia, las compañías proveedoras de CMS parchean su seguridad de forma constante. Por ello, la automatización de las actualizaciones de los CMS es el primer paso a la hora de abordar el mantenimiento de los CMS corporativos.

Asociados a los CMS, están los *plugins*, propios o de terceros, que permiten ampliar las características de los CMS y los temas, orientados al diseño. Una organización puede tener automatizada la actualización del CMS y, sin embargo, no la de algunos *plugins* e, incluso, puede ocurrir que *plugins* que quedan desfasados y dejan de ser utilizados por la organización queden abandonados y desactualizados.

Según los datos aportados por la firma W3Techs, en 2020 WordPress se convirtió en el sistema de gestión de contenidos de código abierto que sustenta el 40% de los sitios web de la red. Si a esta cifra se unen las de el resto de CMS más populares, se puede entender su influencia en la ciberseguridad de las organizaciones.

TOP 10 VULNERABILIDADES

4. CMS DESACTUALIZADOS

Acciones a realizar

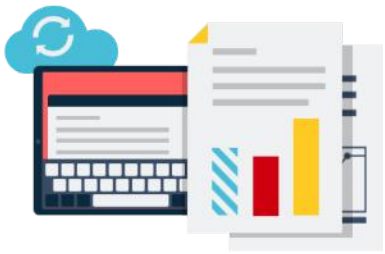
Al instalar *plugins* de terceros valorar la trayectoria del autor, el grado de compatibilidad del *plugin* con el CMS, la madurez del código y su reputación.

Auditar el CMS, controlar su estado de mantenimiento y el de los *plugins* instalados.

Mantener siempre automatizada la actualización del CMS y de los *plugins* instalados.

TOP 10 VULNERABILIDADES

5. BASES DE DATOS EXPUESTAS



Muchas de las bases de datos expuestas son descubiertas por investigadores de la red y las organizaciones afectadas no llegan a ser conscientes de los defectos de configuración de sus bases hasta que reciben la notificación.

La base de datos es uno de los activos más valiosos de cualquier organización. Su protección es una prioridad de los sistemas de seguridad de cualquier empresa. Sin embargo, tanto las organizaciones más pequeñas hasta las más grandes sufren regularmente brechas de seguridad que dejan expuestas sus bases de datos desde que se producen hasta el momento en el que son detectadas, que, por lo general, no es inmediato.

Los resultados de la búsqueda «bases de datos expuestas» o ejemplos de organizaciones con datos sensibles, como Medicall, dedicada a la atención médica —con una base de datos expuesta que contenía 2,7 millones de grabaciones privadas de pacientes suecos* — o tan populares como Adobe — una base de datos sin autenticación expuesta y detectada en 2019 por la empresa Comparitech**—, demuestran que la exposición de las bases de datos es un problema frecuente y recurrente que afecta a todo tipo de organizaciones.

Una base de datos corporativa puede quedar expuesta tras un ciberataque, pero también por una mala configuración o la falta de mantenimiento y actualizaciones de la propia base.

Inicialmente, las bases de datos se alojaban en soluciones on premise, pero desde el desarrollo del cloud computing y la utilización generalizada de nubes híbridas o de terceros, la protección de las bases de datos corporativas se ha vuelto más compleja, ya que la seguridad, en muchos casos, deja de estar por completo en manos de la propia organización.

Es igual de frecuente que la exposición de las bases de datos sea fruto de un delito como fruto de una negligencia por parte de la organización o de las personas que trabajan en ella.

TOP 10 VULNERABILIDADES

5. BASES DE DATOS EXPUESTAS

Brechas de seguridad

Una base de datos expuesta supone un riesgo múltiple para una organización:

- La organización incumple el deber de protección de datos con información sensible de terceros.
- Los datos corporativos quedan a disposición del que los encuentre, para ser utilizados con cualquier fin.
- Los datos corporativos pueden ser borrados por cualquiera que los encuentre y con ellos desaparecer la información corporativa sobre la que no exista copia de seguridad.
- La organización se enfrenta a una crisis de reputación.

Acciones a realizar

TOP 10 VULNERABILIDADES

6. DOCUMENTACIÓN PROTEGIDA POR EL RGPD

Cualquier documento de la organización, por pequeño que sea, que contenga datos de terceros recabados por la misma y que se filtre o quede expuesto puede ser causa de demanda por parte del tercero perjudicado y de sanción administrativa.

Esta vulnerabilidad comparte características con la anterior de la exposición de las bases de datos; incluso, a veces, es consecuencia de ella, aunque no siempre.

La cantidad de datos personales y sensibles de terceros, clientes, partners, proveedores, que recaban a diario las organizaciones han convertido su protección, fundamentada en el derecho a la intimidad, en una prioridad de los Estados y legisladores.

Todas las organizaciones, sea cual sea su tamaño, que recaben datos de terceros están obligados a protegerlos en la forma y medida que establece el Reglamento General de Protección de Datos (RGPD 2016/679), que incluye las sanciones correspondientes por el incumplimiento doloso o culposo de dicha protección.

La obligación de protección y vigilancia de los datos de terceros es, pues, una labor de todas y cada una de las personas que trabajan en la organización y manejan datos de este tipo en cualquiera de las herramientas corporativas: un simple correo electrónico que traslade datos confidenciales de un tercero amparados por el RGPD puede constituir una infracción contra el mismo.

A partir de la entrada en vigor de la Directiva NIS 2 de la Unión Europea, los directivos de las organizaciones obligadas en su articulado son responsables personalmente en el caso de que se demuestre que la organización no ha tomado medidas suficientes y diligentes para proteger los datos de terceros amparados por el RGPD.

TOP 10 VULNERABILIDADES

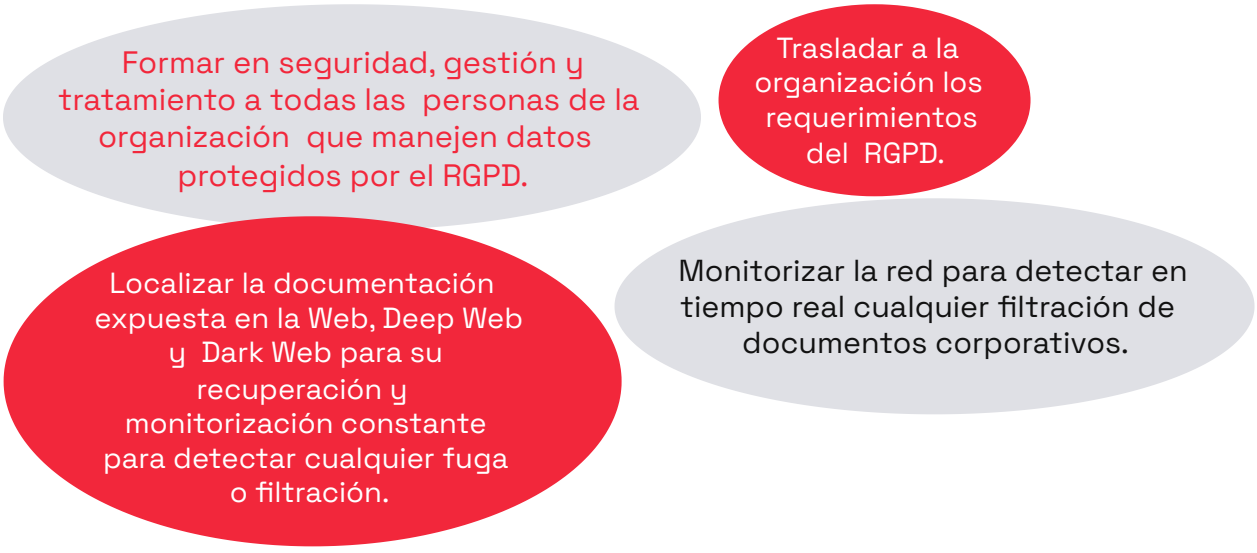
6. DOCUMENTACIÓN PROTEGIDA POR EL RGPD

Brechas de seguridad

Igual que ocurre con la exposición de las bases de datos, la exposición de documentación vulnerando el RGPD es una vulnerabilidad que tiene consecuencias múltiples para la organización:

- Sanciones administrativas e indemnizaciones a los terceros afectados.
- Crisis de reputación corporativa.
- Responsabilidad de la organización en el empleo fraudulento de los datos protegidos por parte de terceros.

Acciones a realizar



TOP 10 VULNERABILIDADES

7. INFORMACIÓN SENSIBLE O CRÍTICA

La gravedad de la exposición de esta documentación depende de su contenido, pero, en cualquier caso, la reputación de la organización que no tiene bien controlada la privacidad de su documentación interna siempre está en juego.

Además de la exposición de las bases de datos o de la documentación con datos protegidos por el RGPD, la de la documentación con información sensible o crítica, actual o pasada, de la organización es otra vulnerabilidad frecuente en la red y que también puede ocasionar un riesgo múltiple al ser detectada por ciberdelincuentes.

Contratos, negociaciones, estrategias, estudios de mercado, estudios de la competencia... la cantidad de documentación expuesta de las organizaciones en la Web, Deep Web y Dark Web es inmensa.

Los ciberdelincuentes utilizan la información que aporta este tipo de documentos de diferentes formas, dependiendo de la relevancia de la información que contengan: pueden pedir un rescate por ella o un pago por no divulgarla, pueden vendérsela a competencia interesada, les puede servir para recabar información para planificar un ataque o todo ello junto. Pocas organizaciones son conscientes de los riesgos que pueden formarse en cadena a partir de un solo documento corporativo filtrado en manos de quien sepa utilizarlo.

Acciones a realizar

Localizar los documentos internos expuestos en la Web, Deep Web y Dark Web para recuperarlos y neutralizar las posibles consecuencias de su utilización ilegal.

Monitorizar la red para detectar en tiempo real cualquier filtración de información corporativa.

Establecer una cultura corporativa de elaboración, manipulación, gestión y almacenamientos seguros de toda la documentación interna

TOP 10 VULNERABILIDADES

8. CÓDIGO FUENTE

El código fuente puede filtrarse de muchas formas, intencionadas o no, tanto a través de la actividad de las personas de la organización, de terceros de servicios externos que colaboren en el desarrollo de software o como consecuencia de algún ciberataque.

El código fuente es parte de la propiedad intelectual de una organización, un valioso activo que no siempre recibe una protección adecuada a su importancia.

En la teoría, un código fuente corporativo debería manipularse, tratarse y compartirse con los máximos estándares de seguridad ya que la información que contiene es una propiedad intelectual crítica y vital para la situación competitiva de la organización. En la práctica, la velocidad con la que se necesita la creación de código fuente para las organizaciones hace que los programadores no siempre puedan ser estrictos a la hora del tratamiento del código fuente.

Las herramientas de DevOps han sido desarrolladas con el objetivo de racionalizar esos tiempos, lo cual contribuye a la seguridad del código fuente. Sin embargo, para implementarlas, una organización debe primero migrar todos sus sistemas y su *legacy* a un entorno *cloud* totalmente cauterizado, lo que complica el proceso y retrasa la adopción.

Cuando el código fuente de una empresa está expuesto y es detectado por un Ciberdelincuente, puede terminar en manos de la competencia, que tendrá una guía para copiar la solución corporativa, puede utilizarse para clonar la solución y estafar en nombre de la organización o puede servir para estafar directamente a la propia organización.

Con el código fuente el ciberdelincuente sabrá cuáles son las prácticas de programación de la organización, si existen análisis estáticos, los niveles de seguridad, la optimización de código, y podrá averiguar rápidamente la calidad de trabajo y el nivel de protección de esa organización.

La publicidad del código fuente lo deja expuesto a ser transformado por cualquiera que tenga interés en ello. La asociación de malware al formato PDF se debe a que durante mucho tiempo el código fuente de Adobe estuvo expuesto en la red sin control alguno.

TOP 10 VULNERABILIDADES

8. CÓDIGO FUENTE

Acciones a realizar

Aplicar al código fuente las herramientas de *Data Lost Prevention* (DLP) para asimilaír su nivel de protección al de los datos.

Localizar todo el código fuente filtrado a la Web, Deep Web y Dark Web para neutralizar su posible utilización fraudulenta

Monitorizar en tiempo real la Web, Deep Web y Dark Web para detectar cualquier fuga de código fuente

Formar en seguridad a las personas de la organización que desarrollen código fuente.

TOP 10 VULNERABILIDADES

9. GESTIÓN DE PROYECTOS

Las filtraciones de la información contenida en las herramientas de gestión de proyectos significan que todo el trabajo de cualquier departamento de la organización queda a disposición del que lo encuentre en un rastreo por la Web, la Deep Web o la Dark Web.

Las organizaciones utilizan en todos los departamentos herramientas de gestión de proyectos para que los equipos puedan organizar y compartir el trabajo de forma inmediata y efectiva. Algunas de estas herramientas de gestión de proyectos se instalan dentro del sistema de la organización, por lo que pueden suponer una puerta de entrada al mismo si no están protegidas.

Cuando se produce una filtración de la información contenida en las herramientas de gestión de proyectos el riesgo es múltiple, porque esa información no solo puede ser utilizada para planificar un ciberataque o para pedir rescates, sino que también puede ser vendida a la competencia o utilizada para provocar una crisis de reputación a la organización. A todo esto se suma la imposibilidad de garantizar la integridad del proyecto, ya que cualquiera que tenga acceso a él a través de la herramienta de gestión puede modificar maliciosamente sus términos en cualquier momento.

En los casos de proyectos realizados en colaboración de terceros, tan importante como que la organización garantice su protección y confidencialidad es que tenga la seguridad de que los colaboradores hacen lo mismo en los mismos términos.

Acciones a realizar

Localizar los documentos internos expuestos en la Web, Deep Web y Dark Web para recuperarlos y neutralizar las posibles consecuencias de su utilización ilegal.

Monitorizar la red para detectar en tiempo real cualquier filtración de información corporativa.

Establecer una cultura corporativa de elaboración, manipulación, gestión y almacenamientos seguros de toda la documentación interna

TOP 10 VULNERABILIDADES

10. SERVICIOS EXPUESTOS

Un servicio abierto y expuesto constituye un riesgo alto para las organizaciones, ya que toda la información que pasa por ellos se transmite sin encriptación.

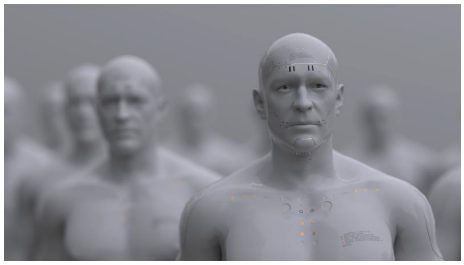
No es difícil para un ciberdelincuente encontrar en la red servicios para compartir archivos o servicios de conexión cuyos puertos están abiertos.

La seguridad de un puerto depende, sobre todo, de su gestión y del uso que se le da. El servicio que genera o consume el tráfico que pasa por un determinado puerto ha de estar actualizado para incorporar los parches a las brechas de seguridad que vayan apareciendo, bien por errores de configuración, bien por la adaptación a las nuevas tecnologías que van apareciendo.

Un puerto FTP sin actualizar es un riesgo para la seguridad corporativa, que puede ser aprovechado por la ciberdelincuencia para validar autenticaciones anónimas o como entrada para malware. Un servicio no cifrado puede llegar a habilitar a un atacante no autenticado para ejecutar procesos en remoto. Los puertos y protocolos no seguros pueden mostrar a los atacantes mucha información sobre su infraestructura, los servidores y las organizaciones que los están utilizando, como los recursos compartidos de red.

Acciones a realizar

kartos©
XTI watchbots



Los sistemas de ciberseguridad de una organización conocen lo que ocurre dentro de su perímetro IT, pero no controlan lo que ocurre fuera ni saben qué información puede encontrar un ciberdelincuente en la red.

Basta con que una persona de la organización se olvide o pierda su teléfono móvil sin proteger para que su correo y el acceso a los discos duros corporativos queden expuestos. O que un troyano en un PC hackee un USB, para que toda la información se filtre de manera inmediata.

Por eso la protección perimetral de una organización no es suficiente.
Por eso es necesario extenderla fuera de ese contorno.

Controlar la fuga de activos corporativos, la exposición de la información en la red, -Web, Deep Web y Dark Web- y las brechas que las originaron es imprescindible para garantizar la seguridad de la organización, minimizar la posibilidad de ciberataques y crisis de reputación y neutralizar los que se materialicen.

La plataforma **Kartos XTI Watchbots de Enthec Solutions** ha sido desarrollada para cubrir esta necesidad de controlar la información expuesta en la red de las organizaciones. Kartos utiliza la Inteligencia Artificial para buscar información como lo hacen los ciberdelincuentes y accede a datos de fuentes públicamente accesibles con información disponible para cualquiera que sepa buscarla.

Kartos no necesita despliegue ni instalaciones ni acceso a los sistemas corporativos: sus robots buscan de manera autónoma en la red de forma continua y, utilizando la IA, analiza y presenta los resultados de su rastreo en un dashboard con nueve vectores diseñado para facilitar el proceso de remediación.

A las ventajas de la detección de las vulnerabilidades de la organización, se suman las ventajas de la monitorización del riesgo de terceros.

Kartos XTI Watchbots posibilita que la organización controle las vulnerabilidades más frecuentes existentes en la red, la información corporativa que está expuesta, dónde se encuentra, el riesgo de terceros y el riesgo de sufrir un ataque.

WHITEPAPER

kartos©
XTI watchbots

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

Kartos XTI Watchbots es la plataforma de cibervigilancia desarrollada por Enthec para extender el perímetro de seguridad controlado por las organizaciones.
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.

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.

Digital Risk Protection Services

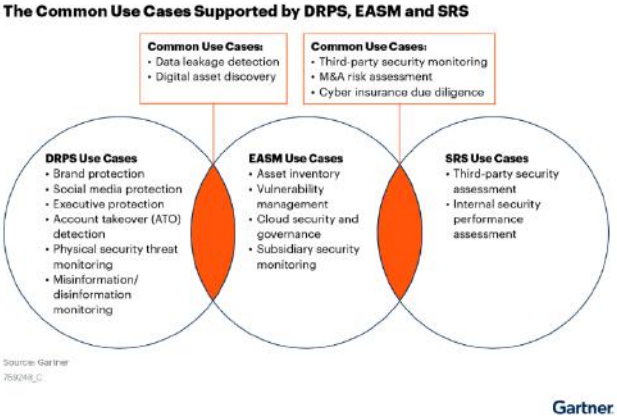
Detección de información contextual sobre posibles agentes de ataques, sus tácticas y procesos para llevar a cabo actividades maliciosas. Eliminación de actividades maliciosas en nombre de la organización.

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.

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



WHITEPAPER

kartos©

XTI watchbots

- **Capa de IA** que permite el funcionamiento 100% automatizado sin intervención humana en ninguna parte del proceso.
- **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 organizaciones, por lo que su funcionamiento y la información obtenida cumplen estrictamente con los límites impuestos por la legislación.
- 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.
- **Funcionamiento continuo 365x24x7**, lo que permite detectar filtraciones de nueva información prácticamente en tiempo real.
- **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.
- **Monitorización automatizada, objetiva y continúa de los riesgos causados por las terceras partes** que pertenecen a la Superficie de Ataque Externa de la organización.

Conoce más sobre nuestras licencias
Prueba de forma gratuita la Cibervigilancia XTI → hello@enthec.com
Empieza a usar Kartos

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