Conoce este conjunto de herramientas de seguridad online que podrían resultar imprescindibles para mejorar una planificación presupuestaria en 2021.

En septiembre, Gartner publicó una lista de las *«9 tendencias principales de seguridad y riesgo para 2020»*, poniendo un énfasis en la creciente complejidad y tamaño del panorama de amenazas moderno.

La visibilidad incompleta de las superficies de ataque externas condujo a un aumento dramático de infracciones desastrosas y fugas de datos durante 2020, comprometiendo la PII y otros datos confidenciales de millones de víctimas.

Estos incidentes se debieron a intrusiones sofisticadas por parte de actores malintencionados del estado-nación y grupos de piratería de APT, errores humanos y configuraciones erróneas generalizadas que exponen el almacenamiento en la nube sin protección o bases de datos con información confidencial a Internet.

Los analistas de seguridad de Gartner recomiendan automatizar laboriosos procesos y tareas de seguridad, en medio de la escasez constante de habilidades en ciberseguridad, y abordar rápidamente los riesgos emergentes de seguridad en la nube y los contenedores.

Gartner también recomienda prestar especial atención a los requisitos normativos y de privacidad para evitar multas severas y otras sanciones y comenzar la implementación de un modelo de confianza cero dentro de su organización, independientemente de su tamaño.

Aunque la creciente pandemia ha tenido un impacto devastador en muchas organizaciones y empresas de todo el mundo, la mayoría de las compañías intentaron trasladar sus procesos comerciales al espacio digital no afectado. Sin embargo, la mayoría de los presupuestos de ciberseguridad también fueron maltratados como efecto colateral de la recesión económica general.

Se proyecta que el gasto en ciberseguridad se recuperará y aumentará nuevamente en 2021, brindando alivio a los CISO hastiados y a sus equipos de seguridad de TI agotados. Mientras

tanto, es recomendable familiarizarse con un impresionante conjunto de herramientas de seguridad cibernética gratuitas, que podrían marcar una diferencia notable para el programa de ciberseguridad y planificación presupuestaria de 2021 para cualquier usuario u organización.

La semana pasada, la compañía de seguridad de aplicaciones ImmuniWeb, anunció una importante actualización de su Community Edition, disponible de forma gratuita. Proporciona 4 pruebas de seguridad gratuitas que cubren ampliamente muchas prioridades de seguridad y privacidad mencionadas por Gartner, y también brindan algunas capacidades sólidas para monitorear incidentes de seguridad y amenazas cibernéticas externas dirigidas a las empresas.

Prueba de cumplimiento y seguridad del sitio web

Para algunos casos de uso específicos, la prueba de seguridad de sitios web puede reemplazar un escáner de vulnerabilidades web comercial. De forma sorprendente, la prueba gratuita no es intrusiva y es segura para la producción, pues no bloqueará de forma accidental el antiguo servidor web o aplicación web heredada mientras envía una carga útil de explotación de desbordamiento de búfer o RCE.

ImmuniWeb afirma que su módulo de Análisis de composición de software (SCA) tiene una extensa base de datos de software web diversificado, que abarca desde WordPress y Drupal de código abierto, hasta productos web patentados y comerciales de Microsoft y Oracle.

Según los informes, el módulo SCA incluye más de 300 CMS y marcos web, 160,000 de sus complementos y extensiones y 8900 bibliotecas de JavaScript. Además, su base de datos de vulnerabilidades integrada cubre más de 12,000 vulnerabilidades CVE.

Además de las vulnerabilidades de las aplicaciones web y las actualizaciones de software que

faltan, la prueba gratuita verifica además si la configuración de su sitio web cumple con los requisitos específicos de GDPR y PCI DSS.

En una prueba, obtiene de forma simultánea una imagen inclusiva sobre cómo fortalecer la seguridad del sitio web, mejorar la resistencia del servidor web y mejorar los requisitos de cumplimiento y privacidad aplicables.

Prueba de detección de phishing y exposición a la Dark Web

Es una herramienta que podría ser muy importante para los analistas de amenazas y los equipos acules que buscan aumentar la visibilidad de los incidentes de seguridad en curso, incluidas las discusiones en la Dark Web y las ofertas de ventas de datos robados que implican a su organización o sus proveedores clave.

Por razones legales y de privacidad, la prueba gratuita no revelará todos los detalles de incidentes, como contraseñas robadas en texto plano o copias completas de las bases de datos comprometidas. Pero una descripción general suficientemente detallada y medible está disponible para respaldar y mejorar el proceso de toma de decisiones antes de invertir en soluciones de monitoreo de la Dark Web.

Además de la captura completo de la Dark Web, se obtiene una descripción general amplia sobre las filtraciones de Pastebin, las campañas de phishing en curso, la ocupación de dominios (cyber- y typo-squatting) e incluso, cuentas falsas en redes sociales que usurpan la identidad.

Es recomendable el uso de la herramienta gratuita para el programa de gestión de riesgos de terceros (TPRM), con el fin de calificar a los proveedores externos y proveedores que tienen acceso privilegiado a los datos confidenciales.

Prueba de privacidad y seguridad de aplicaciones móviles

Esta prueba de seguridad móvil gratuita permite la descarga de aplicaciones móviles directamente desde distintas tiendas de aplicaciones públicas en la parte superior de Google Play, e incluso Cydia, por lo que los usuarios con jailbreak de dispositivos iOS también pueden probar sus aplicaciones móviles por cuestiones de privacidad y seguridad.

La prueba móvil realiza escaneos de aplicaciones móviles tanto dinámicos (DAST) como estáticos (SAST), arrojando información sobre un amplio espectro de vulnerabilidades y debilidades móviles. El escaneo cubre los 10 principales riesgos de OWASP Mobile y también algunos problemas de seguridad específicos mencionados en el proyecto OWASP Mobile Security Testing Guide (MSTG).

Se puede observar una lista inclusiva de permisos solicitados por la aplicación probada y los servidores web externos a los que la aplicación móvil envía sus datos. Su módulo de análisis de composición de software (SCA) integrado ilumina las bibliotecas nativas y de terceros que se utilizan en la aplicación móvil.

Cabe señalar que debido a su naturaleza no intrusiva, el escáner móvil gratuito no cubre las pruebas terminales móviles como API o servicios web, que siempre deben incluirse en su programa de pruebas de seguridad móvil.

Prueba de cumplimiento y seguridad SSL

A diferencia de muchos servicios de la competencia, la prueba de seguridad SSL gratuita permite probar no solo el HTTPS omnipresente, sino también cualquier implementación de cifrado TLS, incluidos los servidores de correo electrónico y la VPN SSL.

Para los servidores de correo electrónico, la prueba también verifica si SPF, DMARC y DKIM están configurados correctamente, que son parte de las mejores prácticas más comunes para la seguridad del correo electrónico actualmente.

Además, la prueba realizará de forma automática un descubrimiento rápido de subdominios oportunamente, recordando a todos que no solo el sitio web principal «www» requiere atención.

La prueba pasa meticulosamente por todas las vulnerabilidades criptográficas o de implementación SSL/TLS conocidas actualmente, incluidas Heartbleed, ROBOT, BEAST, POODLE y una docena de otras fallas que pueden permitir la interceptación o descifrado de sus datos en tránsito.

Otro beneficio significativo es mapear la configuración de TLS a los requisitos específicos de PCI DSS, NIST y HIPAA, para que se pueda verificar si el nivel de cifrado cumple adecuadamente con los requisitos reglamentarios para evitar sanciones por incumplimiento.

Todas las pruebas se pueden actualizar, y al crear una cuenta gratuita, se pueden descargar como un documento PDF para que se pueda compartir internamente o con los clientes.

HTTPS debidamente reforzado y un sitio web seguro son una ventaja competitiva persuasiva para el negocio del comercio electrónico, especialmente después de historias de piratería sobre campañas masivas del Viernes Negro, que vacían las billeteras de compradores en línea desprevenidos.

Es posible acceder a las pruebas gratuitas de ImmuniWeb Community Edition mediante API o en su interfaz web.

Para las organizaciones que buscan ejecutar una gran cantidad de pruebas por día o para los proveedores de seguridad cibernética que buscan aprovechar las capacidades técnicas de ImmuniWeb Community Edition con fines comerciales, también hay una API premium disponible para la compra en línea.