Enero *2022*

Modelo Integral de Seguridad

Nuestras plataformas y procesos de seguridad están fundamentados en múltiples niveles de seguridad - que consta de sistemas y equipos de seguridad[1] combinado con procedimientos y prácticas de seguridad[2] junto con procesos de auditoría[3]. Todo esto para garantizar una seguridad sin precedentes para todos los servicios que ofrecemos. Nuestra plataforma y personal asegura la seguridad de nuestros servidores en 7 niveles diferentes:

Nivel-1 Seguridad del Centro de Datos(Hostname y Localhost de equipos de usuarios de Cristalino)

Las redes de centros de datos globales que usamos, han sido elegidas después de aprobar un proceso de auditoría integral. Y la seguridad y estabilidad son las variables más importantes en nuestro proceso de auditoría integral. Todos los centros de datos están equipados con cámaras de vigilancia, cerraduras biométricas, directivas de acceso solo para personal autorizado, acceso limitado al centros de datos, personal de seguridad y equipos de seguridad estándar en as instalaciones de Hostname.

Nivel-2 Seguridad de la Red de Servidores

Las instalaciones de nuestra infraestructura global incorpora mitigadores DDOS, sistemas de detección de intrusos y cortafuegos (firewalls), tanto en el nivel edge como en el nivel de rack. Nuestros despliegues han resistido intentos de hacking y de DDOS frecuentes (a veces hasta 3 en un solo día) sin ningún tipo de caída de nuestros servidor de Cortes y Riquelme Ltda. Ubicado en Hostname.

Firewall Proteccion - Nuestro sistema de protección de 24 horas al día con cortafuegos (firewalls) asegura el perímetro y ofrece la mejor primera línea de defensa. Utiliza tecnología de inspección altamente adaptable y avanzada para proteger sus datos, aplicaciones web, correo electrónico e Internet mediante el bloqueo de acceso a la red sin autorización. Se garantiza la conectividad controlada entre los servidores que almacenan sus datos e Internet a través de la aplicación de las políticas de seguridad diseñadas por expertos en la materia.

Sistema de detección de intrusiones de red - Nuestro sistema de detección de intrusos en la red y sistema de prevención y gestión de vulnerabilidades proporciona una protección rápida, precisa y completa contra los ataques dirigidos, anomalías de tráfico, spyware / adware, virus de red, aplicaciones falsas y otros exploits del tipo bomba de tiempo ubicados en el datacenter y en los equipos utilizados por los trabajadores de Cortes y Riquelme Ltda. Utiliza procesadores ultramodernos de alto rendimiento para networks que llevan a cabo miles de verificaciones simultáneas a cada flujo de paquetes sin aumento perceptible en la latencia. Cuando los paquetes de datos pasan a través de nuestros sistemas, estos son completamente analizados para determinar si son legítimos o

perjudiciales. Este método de protección instantánea es el mecanismo más eficaz de garantizar que los ataques dañinos no alcanzan sus objetivos.

Protección contra ataques distribuidos de denegación de servicio (DDoS) - La denegación de servicio (DDoS) es actualmente la principal fuente de pérdida financiera debido al crimen cibernetico. El objetivo de un ataque de denegación de servicio es interrumpir sus actividades comerciales al detener el funcionamiento de su sitio web, correo electrónico o aplicaciones web. Esto se consigue atacando los servidores o la red que alojan estos servicios y la sobrecarga de los recursos clave, tales como ancho de banda, CPU y la memoria. Los motivos típicos detrás de este tipo de ataques son la extorsión, los derechos de fanfarronear, declaraciones políticas, dañar a la competencia etc. Prácticamente cualquier organización que se conecta a Internet es vulnerable a estos ataques. El impacto de los ataques sostenidos DoS sin solucionar en los negocios seria colosal, ya que daría lugar a la pérdida de ventas y ganancias, la insatisfacción del cliente, la pérdida de productividad, etc., por razones de no disponibilidad o deterioro del servicio web. Un ataque DoS en la mayoría de los casos incluso provocaría una factura muy grande por usar demasiado ancho de banda que usted nunca planeo. Nuestro sistema de protección contra ataques distribuidos de denegación de servicio ofrece una protección inigualable contra ataques DoS y DDoS contra sus activos en el Internet, es decir, ataques a sus sitios web, correo electrónico y aplicaciones web para el trabajo diario, utilizando tecnología avanzada y sofisticada que se activa automáticamente tan pronto como se inicia un ataque. El sistema de filtro del mitigador DDoS bloquea casi todo el tráfico fraudulento y asegura que el tráfico legítimo pase en la medida de lo posible.

Nivel-3 Seguridad del Servidor

Sistemas detectores de intrusión en los servidores locales - Con el advenimiento de las herramientas que son capaces de saltarse los sistemas de de defensa de bloqueo de puertos tales como cortafuegos (firewalls), ahora es esencial para las empresas implementar sistemas de detección de intrusión en servidores locales (HIDS) pensando en la actualización de sistemas que ya estan en producción por parte de trabajadores de Cortes y Riquelme Ltda. que se centra en el monitoreo y análisis de las máquinas de un sistema de computación. Nuestro sistemas de detección de intrusión en servidor local detecta e identificar los cambios en el sistema y los archivos de configuración - ya sea por accidente, daño por intrusión externa - mediante escáneres heurísticos, información de ingreso al servidor local, y mediante el monitoreo de la actividad del sistema. El descubrimiento rápido de los cambios disminuye el riesgo de daño potencial, y también reduce la resolución de problemas y los tiempos de recuperación, disminuyendo así el impacto global, mejorando así la seguridad y funcionamiento de nuestros servidores.

Normalización de hardware- Hemos estandarizado las marcas de hardware con las que trabajamos y elegimos las que tienen un historial de altos estándares de

seguridad y apoyo de calidad. La mayor parte de nuestra infraestructura y socios para nuestros centros de datos utilizan equipos de Cisco, Juniper, HP, Dell, entre otros.

Level-4 Seguridad de Nuestro Software

Nuestras aplicaciones se ejecutan en sistemas múltiples con gran variedad de software de servidor. Los sistemas operativos incluyen varios sabores de Linux, BSD, Windows. El software de servidor incluye versiones y sabores de Apache, IIS, Resin, Tomcat, PostgreSQL, MySQL, MSSQL, Qmail, Sendmail,Mailjet. Nosotros garantizamos la seguridad, a pesar de la diversa cartera de productos de software que utilizamos, siguiendo un enfoque orientado a los procesos.

Aplicación oportuna de actualizaciones, correcciones de errores y parches de seguridad - Todos los servidores están registrados para recibir actualizaciones automáticas para asegurar que siempre tengan el último parche de seguridad instalada y que cualquier vulnerabilidad nueva se elimine lo antes posible. El mayor número de intrusiones resultan de la explotación de vulnerabilidades conocidas, errores de configuración o ataques de virus en lugares en donde ya hay contramedidas disponibles. De acuerdo con Cpanel, los sistemas y redes se ven afectados por estos eventos, ya que no han implementado consistentemente los parches de seguridad publicados.

Somos plenamente conscientes de la necesidad de tener procesos eficientes para la administracion de actualizaciones y parches de seguridad. Como los sistemas operativos y software de servidor se vuelven cada vez más complejos, cada versión más reciente está llena de agujeros de seguridad. Informaciónes y actualizaciones para nuevas amenazas de seguridad son publicadas casi diariamente. Hemos construido procesos consistentes y replicables, que estan dentro de un marco confiable de auditorias y reportes, que aseguran que nuestros sistemas estan siempre actualizados.

Análisis periódicos de la seguridad del servidor - Controles frecuentes son ejecutados con software de seguridad de nivel empresarial para determinar si algun servidor tiene vulnerabilidades conocidas. Los servidores son escaneados contra las bases de datos más completas y actualizadas hasta la fecha de vulnerabilidades conocidas. Esto nos permite proteger los servidores de forma proactiva de los ataques, y garantizar la continuidad de los negocios de nuestros clientes, mediante la identificación de agujeros de seguridad o vulnerabilidades antes de que se produzca un ataque.

Procesos de pruebas previas a la actualización - Las actualizaciones de software se publican con frecuencia por parte de diversos proveedores de software. A pesar que cada proveedor sigue sus propios procedimientos de prueba antes de la publicación de cualquier actualización, ellos no pueden probar los problemas de interoperabilidad entre los distintos softwares informáticos que se emplean al mismo tiempo. Por ejemplo, una nueva versión de una base de datos puede ser probada por el proveedor de base de datos. Sin embargo, el

impacto de la implementación de esta versión en un sistema operativo que ejecuta varios otros softwares de FTP, correo, y servidores web, no se puede determinar directamente. Nuestro equipo de administración del sistema documenta el análisis del impacto de varias actualizaciones de software y si alguno de ellos se percibe que tienen un alto riesgo, primeramnte son probados en beta en nuestros laboratorios antes de su despliegue en vivo.

Level-5 Seguridad de las Aplicaciones

Todo el software de las aplicaciónes que se utiliza en la plataforma esta construida por nosotros. Nosotros no tercerisamos el desarrollo de aplicaciones. Todo producto o componente de terceros pasa por procedimientos de instruccion en su manejo y por pruebas exhaustivas, donde todos los elementos de esos productos se dividen en sus partes mas elementales y el conocimiento de su arquitectura e implementación se transfiere a nuestro equipo. Esto nos permite controlar por completo todas las variables que intervienen en cualquier producto en particular. Todas las aplicaciones se han diseñado utilizando nuestro sistema privado de ingeniería de productos que sigue un enfoque proactivo hacia la seguridad. Cada aplicación se divide en varios componentes, tales como la interfaz de usuario, Core API, base de datos del sistema de administracion, etc. Cada capa de abstracción tiene sus propios controles de seguridad, a pesar del control de seguridad realizado por una capa de abstracción superior. Todos los datos sensibles se almacena en un formato encriptado. Nuestras prácticas de ingeniería y de desarrollo aseguran el más alto nivel de seguridad en lo que respecta a todo el software de las aplicaciónes.

Nivel-6 Seguridad del Personal

El eslabón mas debil de la cadena de seguridad es siempre la gente de su confianza. Personal general, el equipo de gente de desarrollo, los proveedores, y esencialmente tosas las personas que tienen acceso privilegiado a su sistema. Nuestro enfoque holístico de seguridad intenta minimizar los riesgos de seguridad provocados por el "factor humano". La información es compartida en cada caso solamente "si es necesario para tal caso". La autorización expira en el momento de la expiración de cada caso. El personal está entrenado específicamente en las medidas de seguridad y en la importancia critica de seguir esas medidas. Todo empleado que tenga privilegios de administrador y acceso a cualquiera de nuestros servidores, pasa por una verificación de antecedentes completa. Las empresas que no cumplen con esa medida, están poniendo en riesgo todos los datos sensibles e importantes de sus clientes, ya que no importa cuánto dinero se invierta en soluciones de seguridad de gama alta, si se contrata a una persona mala que tiene los accesos necesarios, puede causar un daño mayor que cualquier ataque externo.