La Seguridad Es Importante

La Seguridad En Hostdime Es Importante

En la industria de alojamiento web, la satisfacción del cliente es la prioridad número uno. Esto se extiende no sólo a la compra inicial, sino también a la protección de nuestros clientes y sus servidores, aplicaciones e información. HostDime formó un equipo de élite para manejar estos desafíos. El departamento de Seguridad y Abuso de la compañía es la primera línea de defensa en cuanto a la protección de los clientes de malware y usuarios malintencionados.
Contar con un departamento especializado para esos casos, puede ser algo fundamental para tener un equipo de la defensa – sobre todo cuando se trata de un proveedor de alojamiento web en la actualidad figura entre el servidor web los 50 mejores empresas de alojamiento en el mundo.
Somos responsables de muchas cosas, Cuando un cliente contacta con nosotros sobre un sitio potencialmente en peligro, nuestra tarea es llevar a cabo el qué, dónde y cómo del incidente. Después de eso, vamos a trabajar con el cliente para evitar que el problema ocurra de nuevo. Otras partes incluyen responder a las solicitudes y el desarrollo de software y políticas para mantener en funcionamiento HostDime sin problemas.
Por desgracia, en la época actual, los clientes tendrán que hacer frente a usuarios malintencionados que quieren estropear sus sitios web, Trabajamos de manera proactiva para ayudar a proteger a nuestros clientes de estos usuarios malintencionados. También trabajamos de manera reactiva para ayudar a los clientes que no reciben visualicen sus sitios web desconfigurados.
Con todo lo que ofrece HostDime, desde alojamiento básico

compartido hasta en los servidores dedicados que tienen un equipo se hace una Constante revision. Así que, ¿cuáles son algunas de las medidas reactivas que un equipo tiene cuando algo ha ido mal con un servidor?

Cuando se ponen en contacto, un miembro de nuestro equipo revisará la información proporcionada por el cliente y comenzar su investigación, En los casos en que las secuencias de comandos y el código son explotados, nos va a aislar del medio ambiente mediante la identificación de la vulnerabilidad y tomar medidas para reducir el tiempo de inactividad para el sitio del cliente. Cada tema debe ser abordado con el cuidado adecuado.

Una de las cosas el equipo de abuso y de Seguridad se ocupa es el de trata de malware, que es la abreviatura de software malicioso. Puede aparecer en forma de secuencia de comandos y el código e incluye, pero no se limita a, los virus informáticos, programas espía, troyanos y adware. Esto, por supuesto, es algo que el equipo de abuso Seguridad trabaja para eliminar.

En los casos en que el spam se intercambian, y se vulnera la información del cliente enviando mails masivos en los que el cliente no tiene acceso se debe pone en contacto con las listas de bloqueo en tiempo real sobre la reputación de IP, y localizar las secuencias de comandos de correo masivo para mantener limpia la cola de correo de mensajes no deseados Hay muchos pasos a asegurar un entorno de alojamiento. Con cada nuevo servidor desplegado, llevamos a cabo una auditoría de seguridad completa para asegurarse de que el cliente está recibiendo un sistema bloqueado para acoger con confianza su aplicación web o medios de comunicación. Mantener el sistema operativo y sus componentes parcheados, la modificación de Apache y PHP con conjuntos de reglas estrictas, y la utilización de afinado firewalls son sólo algunos ejemplos de los pasos que tomamos para ofrecer un buen pedazo de la mente.

Mantenemos una estrecha vigilancia sobre los boletines de seguridad y hacer los ajustes en nuestros servidores basados en los, Si nos encontramos con que el sitio de un cliente se

ha comprometido entonces, trabajamos duro para asegurarnos de que la forma en que la cuenta fue comprometida ya no sea accesible. Trabajamos con el cliente para restaurar el sitio.
Como una máquina bien engrasada, cada departamento es esencial para la operación diaria de HostDime, El abuso y proporcionar las políticas internas de seguridad para nuestros empleados con capacitación y documentación. También proporcionamos las bases para la protección de los servidores mediante la adopción de las medidas necesarias para asegurar a nuestros entornos de alojamiento y redes. Cuando un posible problema puede surgir, de abuso y de seguridad se puede confiar para manejar cualquier situación fuera de los límites de otros departamentos con confianza.