El Departamento de Seguridad y Abuso te Mantienen a Salvo

En la industria de alojamiento web, la satisfacción del cliente es la prioridad número uno. Esta se extiende no sólo a la compra inicial, sino también a la protección de los clientes y sus servidores, las aplicaciones y la información. HostDime.com, Inc. formó un equipo de élite para manejar estos desafíos. Abuso de la compañía y la división de Seguridad es la primera línea de defensa cuando la protección de los clientes de malware vicioso y usuarios malintencionados.

Como miembro de esa división particular, Jonathan S., analista de respuesta de abuso, dijo que puede ser algo fundamental para contar con un equipo de defensa – sobre todo cuando se trata de un proveedor de alojamiento web que actualmente clasificado entre los 50 mejores del servidor web de alojamiento de negocios en el mundo.

«Somos responsables de muchas cosas», dijo Jonathan, quien ha estado trabajando con HostDime por tres años. «Cuando un cliente contacta con nosotros acerca de un sitio potencialmente comprometido, es nuestra tarea para realizar el qué, el dónde y el cómo de los hechos. Después de eso, vamos a trabajar con el cliente para evitar que el problema se repita. Otras partes incluyen responder a las solicitudes DMCA y el desarrollo de software y políticas para mantener operativo HostDime sin problemas. »

No solamente los sitios están comprometidos con los requisitos DMCA (Digital Millennium Copyright Act) que el equipo tiene que vigilar si no también desafortunadamente se tiene que vigilar hackers, estafadores y spammers. Jason J., quien se unió a HostDime hace ocho meses, dijo que él se ocupa de este problema específico de vez en cuando.

«Desafortunadamente, en la época actual, los clientes tendrán que hacer frente a los delincuentes que quieren desfigurar sus sitios web«, dijo Jason, quien trabaja con la respuesta de los abusos. «Trabajamos activamente para ayudar a proteger a nuestros clientes de estos usuarios malintencionados. También trabajamos reactivamente para ayudar a los clientes que obtienen sus sitios web desfigurado".

Con todo lo que ofrece HostDime desde básico de hosting compartido hasta servidores dedicados que tienen un equipo, es realmente un pan comido. 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», explicó Jonathan. «En los casos en que los scripts y códigos son explotados, vamos 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 cuidado apropiado. »

Una de las cosas que Jonathan y el equipo de abuso y de Seguridad también se ocupan es del malware, que es la abreviatura de software malicioso. Puede aparecer en las formas de escritura y código e incluye, pero no está limitado a, los virus informáticos, spyware, troyanos y adware. Esto, por supuesto, es algo que el abuso y el equipo de seguridad trabaja para eliminar.

Sin embargo, no es lo único que los mantiene en estado de alerta.

«En los casos en que el spam se intercambian, se nos puede exigir a listas de contactos de bloqueo en tiempo real acerca de la reputación de IP, y trazar guiones de correo masivo para mantener limpia la cola de correo de mensajes no deseados»,

dijo Jonathan. «Hay muchos pasos para asegurar un entorno de alojamiento. Con cada nuevo servidor desplegado, llevamos a cabo una auditoría de seguridad exhaustiva para asegurar que el cliente recibe 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 las medidas que tomamos para proporcionar un buen pedazo de la mente. »

Esto es algo de lo que Jason se siente orgulloso. Un buen pedazo de algo que él cree que cada cliente de HostDime debe tener. Debido a esto, se toma su trabajo muy en serio.

«Mantenemos una estrecha vigilancia sobre los boletines de seguridad y hacer ajustes en nuestros servidores basados en ellas», dijo. «Si encontramos 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 es accesible. Trabajamos con el cliente para restaurar el sitio. »

«Nosotros trabajamos en el problema de seguridad crítico ocasional, en la que alguien puede ser despertado en mitad de la noche», añade Jonathan. «Hace varios años, el kernel de Linux sufría de una vulnerabilidad de elevación de privilegios muy peligrosa en la que un usuario puede ejecutar procesos de nivel raíz. Nos lo previsto el despliegue y el parcheo de los servidores para reducir el tiempo de inactividad del cliente. Incluso me quedé despierto toda la noche para asegurarme de que todos los servidores ejecutaran el nuevo kernel. Nos tomamos la seguridad muy en serio en HostDime y haremos los pasos que sean necesarios para proporcionar una experiencia segura de alojamiento para nuestros clientes. »

A pesar del nivel de seriedad que requiere el trabajo, el equipo se asegura de reír de vez en cuando. Jonathan dijo que

sí disfrutan bromeando acerca de código y scripts que son capaces de cortar-. También dijo que consiguen un retroceso, verdadero reto de habilidades de cada uno de exploits para hackear un guión y para ver quién puede completar lo más rápido. Sin embargo, al final del día, Jonathan sabe lo que ha empleado para hacer, y él ve su división como vital para la empresa.

«Como una máquina bien engrasada, cada departamento es esencial para el funcionamiento diario de HostDime», dijo. «Abuso y Seguridad provee las políticas internas de nuestros empleados con formación y documentación. También proporcionamos las bases para el servidor de endurecimiento tomando las medidas necesarias para asegurar nuestros entornos de alojamiento y redes. Cuando un posible problema puede surgir, de abuso y de Seguridad puede confiar para manejar cualquier situación fuera de los límites de otros departamentos con confianza”.