Respuesta a incidentes: cinco claves para los CISO

A medida que los ataques se vuelven más sofisticados y frecuentes, el 86% de los CISO están de acuerdo en que los ciberincidentes dentro de sus empresas son inevitables.

Por lo tanto, no es de extrañar que la mayoría (76%) crea que la rapidez y la calidad de la respuesta ante incidentes son los factores más importantes a la hora de medir su rendimiento. Esto significa que los responsables de los departamentos de seguridad de TI han de centrarse no sólo en la prevención de ataques, sino en la identificación de problemas a tiempo para minimizar los daños.

Que la respuesta a incidentes sea un proceso es una necesidad; sin embargo, los CISO todavía se enfrentan al dilema sobre cómo organizarlo. Hay cinco factores que los responsables de seguridad TI deben tener en cuenta al elegir cómo organizar la respuesta a incidentes en su organización:

1. Profesionales calificados

A menudo se malinterpreta la respuesta a incidentes como un salto a la fase de remediación cuando ocurre un incidente. Sin embargo, este proceso comienza incluso antes de que se haya producido un ataque y no termina cuando se detiene. En general, la respuesta a incidentes consta de cuatro etapas. La primera es la preparación para asegurar que todos los empleados responsables sepan cómo actuar en caso de ataque. La segunda fase consiste en la detección de incidentes. A continuación, un equipo de respuesta a incidentes debe eliminar el ataque y recuperar los sistemas afectados. Una vez resuelto el problema, se debe revisar la estrategia teniendo en cuenta esta experiencia, para mitigar casos similares que se repitan.

Estas actividades diversificadas requieren profesionales diferentes. Desafortunadamente, estos especialistas son escasos. Según un estudio, el 43% de los CISO tiene dificultades para encontrar analistas de malware, el 20% para encontrar especialistas que puedan responder a los ataques y el 13% no puede encontrar threat hunters.

2. Elegir un equipo externo

La elección de un equipo subcontratado tampoco es una tarea trivial. Para ser eficaz, un equipo subcontratado debe cubrir todas las competencias importantes de la respuesta a incidentes, a saber, la investigación de amenazas, el análisis de malware y la investigación forense digital. Es importante que el equipo externo disponga de certificados independientes que demuestren su base de habilidades. Pregunte también sobre su experiencia real. Cuanto más hayan trabajado para múltiples clientes en una variedad de industrias, más posibilidades hay de que se encuentren con incidentes típicos y puedan encontrar similitudes en casos aparentemente diferentes.

Para aquellas compañías en industrias reguladas, puede haber restricciones adicionales al seleccionar a los equipos externos. Por lo tanto, sólo se les permitirá

elegir entre los equipos de respuesta a incidentes que cumplan con los requisitos específicos de cumplimiento.

3. Costo de la respuesta a incidentes
Establecer un proceso interno de respuesta a incidentes es costoso. La organización necesita pagar un salario a tiempo completo a empleados con habilidades raras y costosas. También necesitan adquirir soluciones y servicios (como la inteligencia de amenazas) necesarios para la búsqueda de amenazas, el análisis de datos y la remediación de ataques.

Sin embargo, el costo medio de experimentar una violación de datos en todo el mundo también está aumentando: en la actualidad, el coste de una brecha asciende a una media de 1,23 millones de dólares para las empresas (un 24% más que los 992.000 dólares en 2017). Con el aumento del costo de los incidentes de TI, las empresas se están dando cuenta de que tienen que dar prioridad al gasto en ciberseguridad.

Algunas organizaciones consideran que un modelo de subcontratación flexible es más eficaz en costes, ya que les permite pagar sólo por el servicio recibido. Sin embargo, para las empresas que tienen que hacer frente a numerosos incidentes, es imprescindible contar con un servicio interno de este tipo. No obstante, todavía pueden encontrar un modelo más rentable cuando emplean personal de respuesta de primer nivel. Este equipo interno debe ser capaz de analizar el incidente primero para manejarlo de acuerdo con los procedimientos o enviarlo a expertos externos.

4. Sinergias con el equipo de TI
Cuando se produce un incidente, el equipo de TI puede decidir apagar los equipos infectados para reducir el impacto. Sin embargo, para los que tienen que trabajar sobre el incidente, es importante recoger primero las pruebas, lo que significa que la "escena del crimen" debe permanecer intacta por un tiempo después de un incidente. Recoger los registros y almacenarlos durante sólo tres meses, y desconectar los equipos infectados dificultan la tarea de los equipos de respuesta a incidentes.

Para evitar estas discrepancias, el equipo interno de respuesta a incidentes debe preparar una guía a medida para sus colegas de TI o introducir una formación especial para cualquier especialista en TI que necesite algo más que un simple conocimiento de la higiene de la ciberseguridad, pero que no requiera conocimientos profundos en materia de seguridad. Esta iniciativa garantizará que tanto el equipo interno como el externo trabajen coordinados.

5. Retrasos en dar una respuesta
Las organizaciones que subcontratan equipos de respuesta a incidentes pueden establecer los procesos más rápidamente, ya que un equipo externo siempre está disponible para intervenir y resolver un incidente cuando sea necesario. Sin embargo, esto trae consigo posibles problemas. Por ello, entre la empresa y el tercero se deben firmar contratos y acuerdos antes de que se lleve a cabo cualquier trabajo. Esto puede provocar un retraso en la respuesta al incidente.

Según nuestra experiencia, a menudo un equipo vuelve a trabajar un lunes y descubre que se ha producido una brecha de datos en la empresa durante el fin de semana. Durante varios días tratan de manejar el asunto por su cuenta. Al comprobar que no pueden hacer frente a la situación, deciden recurrir a expertos externos. Pero ya es viernes. Por ello, la compañía intenta aprobar todos los acuerdos rápido antes del próximo fin de semana para que el equipo de respuesta a incidentes se ponga manos a la obra. Si una organización tiene un equipo interno, puede evaluar mejor cada caso y delegar responsabilidades rápidamente.

Para la mayoría de las grandes organizaciones, la opción más efectiva es un enfoque híbrido de respuesta a incidentes que combine equipos de respuesta de terceros como segunda línea de respuesta y a un equipo interno como primera. Este modelo aporta beneficios y elimina las debilidades de

ambos enfoques. En definitiva, la externalización de la respuesta a incidentes no significa que la empresa pueda simplemente entregar las riendas a expertos externos y exonerarse de responsabilidad. Tener un plan sigue siendo la clave. Para reaccionar a tiempo, una empresa ha de estar preparada y tener una primera línea de respuesta. Debe haber instrucciones sobre cuándo pedir ayuda externa y de qué se ocupará esta. Alguien dentro de la empresa también debería tener la tarea de priorizar las acciones y coordinar la cooperación entre los departamentos internos y el equipo externo subcontratado. Es imprescindible establecer una figura que desempeñe esta tarea.

Fuente de información:

https://www.itdigitalsecurity