10 pasos a seguir después de sufrir un ciberataque

Todos los profesionales en el negocios de la ciberseguridad reconocemos que un incidente cibernético es inevitable; si bien la inversión en herramientas de seguridad refuerza la infraestructura interna y defiende proactivamente ante la gran mayoría de los ataques, es necesario contar con un plan integral de respuesta a incidentes.

La preparación para resolver emergencias es donde las organizaciones que buscan reducir los daños financieros y reputacionales logran resolver contingencias ante una brecha de seguridad.

Entonces, ¿qué recomienda Metabase Q a las organizaciones para prepararse para un incidente? Antes de tener los pasos a seguir, hay que tomar en cuenta el siguiente plan de 10 puntos como base a la respuesta a incidentes:

Plan de respuesta a incidentes

- Elabore un plan antes de que ocurra una brecha
- Comprenda su negocio y lo que es crítico, importante y significativo
- Priorice internamente la capacitación en concientización sobre seguridad
- Cree políticas, procedimientos y pautas para manejar incidentes de seguridad de la información.
- Asegúrese de tener visibilidad de la actividad y el comportamiento crítico de su entorno.
- Aprenda y practique a lidiar con los ataques más comunes
- Desarrolle y comprenda su capacidad de respuesta.
- Haga de la detección y análisis de incidentes una competencia central para su programa de seguridad
- Aproveche el asesoramiento y la orientación de expertos.
- Mantenga siempre abiertos canales de comunicación interna sobre la preparación de su programa, los planes de mejora y su capacidad de respuesta.

Metabase Q 10 pasos a seguir después de sufrir un ciberataque

Una vez efectuado un plan de respuesta a incidentes, es necesario conocer los pasos a seguir una vez ocurra un ciberataque, ya que si su equipo esta agotado, o estresado será más complicado tomar las decisiones correctas y seguir el plan de incidentes.

Metabase Q presenta los siguientes lineamientos a seguir:

10 pasos a seguir después de sufrir un ciberataque

1. Mantengan el orden: es importante sean Calmados, Analíticos, Lógicos y Metódicos.
2. No tome ninguna medida sin evaluar el factor de riesgo del incidente, incluido el riesgo de escalada y el riesgo para su negocio. Si hay una demanda de rescate, aconsejamos no ceder a la demanda de ciber criminales, ya que esto no garantiza que sus sistemas serán restaurados.
3. No comunique ninguna información sin intención específica. Sin embargo, su gerencia ejecutiva debe ser notificada del incidente inmediatamente.
4. Reúna sus equipos de gestión y de respuesta técnica contra incidentes y use su experiencia compartida para determinar cómo proceder.
5. Cree documentación con un cronograma del incidente, respondiendo preguntas como: ¿Qué se sabe? Qué necesita ser conocido? ¿Cuáles son las aprobaciones requeridas para cualquier acción futura que deba tomarse?
6. Evaluar la gravedad y el impacto del incidente, con la opinión y orientación del negocio. Asegúrate de que eres constantemente revisando este paso en cada oportunidad.
7. Cree planes para los pasos de alcance, contención y corrección, y luego ejecútelos. Incluso si es urgente se requiere respuesta, tómese el tiempo para considerar completamente sus opciones. Si su organización tiene un incidente libro de jugadas de respuesta, sígalo en consecuencia.
8. Suspenda todos los cambios programados en todos los sistemas afectados hasta que se resuelva el incidente.
9. ¡Resguardar la evidencia! Esto puede incluir el estado del sistema, registros de red, registros de aplicaciones, registros de firewall, copias de VM, etc. Todo lo que se pueda resguardar, debe ser.
10. Tome nota de todos los mensajes de error u otros síntomas en sus tecnologías y busque en Internet para ganar más visibilidad en la naturaleza del incidente. Si es un ataque de ransomware o un exploit conocido que afecta cierto software que usa, puede haber parches de seguridad conocidos disponibles.

Por último, obtenga ayuda profesional, contacte a Metabase Q. Use especialistas en respuesta a incidentes si no tiene el derecho capacidades capacitadas y listas para responder de inmediato.

Metabase Q 10 pasos a seguir después de sufrir un ciberataque

Acerca de Metabase Q

ACCEDE A LA CIBERSEGURIDAD INTELIGENTE Y DE NUEVA GENERACIÓN

Metabase Q (MQ) es líder en la provisión de servicios administrados de seguridad cuya misión es proteger a las empresas de todo el mundo contra ciberatacantes ágiles y bien financiados.

MQ brinda a las empresas y organizaciones gubernamentales más grandes del mundo el poder único para asegurar, controlar y administrar millones de puntos finales en toda la empresa en cuestión de segundos.

Con la velocidad, escala y simplicidad sin precedentes de MQ, los equipos de seguridad y operaciones de TI ahora tienen información completa y precisa sobre el estado de los puntos finales en todo momento para proteger de manera más efectiva contra las amenazas modernas y lograr nuevos niveles de eficiencia de costos en las operaciones de TI.