Gestión de crisis: ¿Cómo reaccionar en las horas posteriores a un ataque de Ransomware?

Los ataques de ransomware van en aumento. El nuevo malware, disponible llave en mano en la red oscura, combina la facilidad de implementación y el cifrado de alto nivel para un efecto cada vez más devastador. Ninguna organización se salva: establecimientos públicos, empresas, fábricas, etc.

¿Cómo sucede?

El escenario de un ataque de ransomware, desde la perspectiva de la víctima, siempre comienza de la misma manera. El sistema de información (SI) se congela repentinamente y aparece una demanda de rescate en las pantallas.

¿Cómo, a partir de este momento crucial, reaccionar y asegurarse de que la amenaza esté bien eliminada una vez finalizada la fase de restauración de datos? Bajo ninguna circunstancia debe entrar en pánico y actuar sin antes haber establecido un plan de acción.

¿Qué hacer?

Idealmente, este plan de acción debería definirse antes, pero si este no es el caso, es imperativo que se dé tiempo para la reflexión y la consulta, incluso con expertos. Durante esta fase de evaluación, cinco buenas prácticas pueden ayudarlo a abordar mejor la crisis.

No apague los sistemas afectados

Muy a menudo, el ransomware no está presente en el sistema de almacenamiento de la computadora, sino solo en la RAM. Al cortar el suministro de energía al equipo, se borra el malware … así como las posibilidades de identificarlo y atacarlo. Ser capaz de recuperar el código de malware a veces hace posible encontrar la clave de cifrado mediante ingeniería inversa y así recuperar sus datos. Por tanto, no es necesario apagar los sistemas afectados, sino desconectarlos de la red, para ralentizar la propagación del ataque.

No pague el rescate

Algunas organizaciones sufren más los efectos del ransomware

que otras. Detener la producción en una fábrica, por ejemplo, tiene un alto precio, lo que puede empujar a la gerencia a pagar rápidamente el rescate. Esto es un error, porque confirma la relevancia de su plan de negocios a los ojos de los delincuentes. Al demostrar que está dispuesta a pagar, la empresa corre el riesgo de convertirse en el objetivo ideal de futuros ataques, incluidos otros grupos de hackers.

Dominar la comunicación, interna y externa

Aunque la empresa tiene la obligación legal de comunicar públicamente el incidente, especialmente en el caso de una violación de datos, no es aconsejable hacerlo sin tener información completa, especialmente sobre la naturaleza exacta de los datos que podrían filtrarse hacia el exterior.

Es recomendable analizar antes de comunicar y evitar fugas internas para mantener el control de su comunicación.

No inicie sesión en sistemas infectados con cuentas privilegiadas

Tienen demasiado poder, que los piratas informáticos podrían explotar, y el ransomware a veces no es el único malware que circula en el sistema. Es preferible utilizar cuentas de un solo uso dedicadas a la respuesta a incidentes. Entonces será posible tomar nota de las acciones que realizarán estas cuentas, y así identificar la posible intervención de un hacker.

No confíe en herramientas no auditadas de Internet

Ante un ataque, resulta tentador buscar soluciones en Internet. No se recomienda instalar herramientas sin consejo previo: algunas pueden ser simplemente malware. Otros, mal

diseñados, pueden destruir sus posibilidades de rastrear y eliminar el ransomware que lo afecta. Las herramientas deben haber sido probadas y validadas imperativamente por expertos antes de cualquier uso en una máquina infectada.

Vuelva sobre la cadena de la muerte y recupera el control

El ransomware suele ser el último eslabón de una cadena de eliminación mucho más larga. El pirata informático primero ingresó a la infraestructura por varios métodos (phishing, kit de exploits, vulnerabilidad de día cero, etc.). Posteriormente, intentó obtener acceso a cuentas privilegiadas y luego se expandió a la red. Finalmente, realizó un reconocimiento y un mapeo del SI, luego extrajo datos.

Último paso, el lanzamiento de un ataque de ransomware en toda la infraestructura de TI. Desear reiniciar el IS lo más rápido posible a través de sus copias de seguridad es un paso arriesgado, porque el entorno restaurado también puede verse comprometido.

Restablecer las contraseñas de las cuentas privilegiadas tampoco es una panacea, especialmente si el atacante ha tomado el control de la infraestructura crítica, como el Active Directory de la empresa.

En resumen, es imperativo saber qué sucedió y buscar compromisos que afecten al SI, algunos de los cuales pueden tener varios años. Las herramientas EDR (detección y respuesta de endpoints) permiten ganar visibilidad sobre la infraestructura y sus terminales (computadoras, servidores, etc.). Una vez que las copias de seguridad hayan sido verificadas y restauradas, será necesario asegurarse de que todos los puntos de entrada descubiertos a través de este trabajo de investigación estén cerrados: eliminar cuentas comprometidas, recuperar el control de activos estratégicos

pirateados, completar brechas de seguridad, etc.

Aprenda del incidente

La ayuda de expertos es una ventaja para recuperar su SI. Pero también para tener información sobre el curso exacto del ataque y cómo protegerse contra el próximo. En todos los casos, habrá que revisar los procesos y poner en marcha procedimientos para fortalecer las defensas de la empresa. Es imposible pretender prevenir incidentes de seguridad, pero puede pretender retrasar su ocurrencia y minimizar sus efectos tanto como sea posible.

Leer también: La IA, inteligencia artificial también está al servicio del malware y los hackers ; ¿Cómo afecta el ransomware a mi negocio? ; 10 formas de prevenir, detectar y recuperar amenazas de ransomware y zeroday