Ransomware, ¿qué estrategias pueden establecerse para frenar estas máquinas de hacer dinero?

El ransomware se ha convertido en la pesadilla de los departamentos de informática y de las empresas en general. Sin embargo, ¿son una fatalidad? Preguntamos a Sébastien Viou, director de Ciberseguridad de Producto y Consultor de Stormshield, cuáles son las medidas que deben tomarse para afrontarlo.

STORMSHIELD

01 PROTEGERSE ANTES DEL ATAQUE

HACER UNA COPIA DE SEGURIDAD DE LOS DATOS... Y PROTEGER LAS COPIAS DE SEGURIDAD

«Esta precaución por sí sola no es suficiente, porque es lo primero que el ransomware intentará destruir, incluso antes del cifrado. Hay que hacer copias de seguridad sin conexión y trabajar cuidadosamente la frecuencia de estas copias de seguridad. También es necesario probar las restauraciones para asegurarse de que las copias de seguridad se puedan utilizar».

MANTENER EL SOFTWARE Y LOS SISTEMAS ACTUALIZADOS

«Las actualizaciones deben realizarse continuamente e incluir los PC Windows, así como los sistemas Linux y Mac, que también pueden ser puntos de entrada. Esto abarca toda la ofimática, desde Microsoft Exchange hasta Active Directory, incluidos todos los servidores expuestos, aunque sean pequeños».

COMPARTIMENTAR EL SISTEMA DE INFORMACIÓN

«Se recomienda para ello aplicar reglas estrictas de flujos autorizados entre diferentes zonas según su criticidad».

LIMITAR LOS DERECHOS DE LOS USUARIOS Y LOS PERMISOS DE LAS APLICACIONES

«En este sentido, la gestión a lo largo del tiempo es decisiva: para poder mantener la seguridad, se deben planificar revisiones periódicas».

LLEVAR A CABO LA SUPERVISIÓN DE LOS REGISTROS

«La recopilación de logs es obligatoria. En los casos en que se requiera un nivel de seguridad muy alto, es posible agregar un componente de detección de intrusos a través de un SOC».

SENSIBILIZAR A LOS EMPLEADOS

«Con la ingeniería social, el principal punto de entrada al sistema de información de una empresa siguen siendo sus empleados. Por lo tanto, es importante abordar los temas de ciberseguridad, aunque la sensibilización tenga sus límites».

PENSAR EN LA ESTRATEGIA DE COMUNICACIÓN DE CRISIS CIBERNÉTICA

«Aquí, nuevamente, es útil haber trabajado en los mensajes y contactos con anterioridad para comunicarse adecuadamente con las diferentes audiencias. Las comunicaciones deben servir para advertir de una interrupción inesperada de la producción, por ejemplo, o incluso de fugas de datos personales, tal y como establece el RGPD ».

ESTABLECER UN PLAN DE RESPUESTA A CIBERATAQUES

«Este plan es crucial, porque permite reaccionar rápidamente contactando lo antes posible, por ejemplo, con las empresas CERT identificadas de antemano. Obviamente incluye un componente técnico mediante la implantación de soluciones de protección como Stormshield Endpoint Security Evolution y Stormshield Network Security».

EVALUAR EL INTERÉS DE SUSCRIBIR UN CIBERSEGURO

«Algunos ciberseguros incluyen cláusulas de despliegue de soluciones de ciberseguridad; son interesantes en este sentido, porque imponen cierta protección. Sin embargo, el ciberseguro no debe considerarse como una medida de supervivencia suficiente por sí sola, y menos como una medida de protección. En otras palabras, el seguro contra el ransomware nunca constituye una estrategia de ciberseguridad».

02
LIMITAR LOS DAÑOS DURANTE UN ATAQUE

ADOPTAR LOS REFLEJOS ADECUADOS

«Hay que ser capaz de detectar rápidamente que algo va mal y no dudar en desconectarlo todo para mitigar el riesgo y contener la propagación al máximo. A nivel individual también hay que aprender a reaccionar, a decir «he hecho clic donde no debía» porque cada minuto cuenta».

LIDERAR LA GESTIÓN DE LA CIBERCRISIS DESDE EL COMITÉ EJECUTIVO

COMUNICARSE AL NIVEL ADECUADO

DENUNCIAR

03
RECUPERARSE DESPUÉS DE UN ATAQUE

RESTAURAR LOS SISTEMAS DESDE FUENTES LIMPIAS

INVESTIGAR LA RUTA DE ATAQUE SEGUIDA

«Para comprender cómo se ha desarrollado el ataque y las debilidades de su propio sistema, hay que analizar lo sucedido. De esta manera, tendremos todas las posibilidades de evitar que vuelva a suceder».

ELABORAR UN PLAN DE CORRECCIÓN

«Dependiendo del caso, ¿puede ser necesario configurar la autenticación multifactorial o mejorar las soluciones de seguridad presentes en los puestos de trabajo?».

ESTABLECER UN PLAN DE PRODUCCIÓN PARA PONERSE AL DÍA TRAS EL RETRASO ACUMULADO

EMPRENDER ACCIONES LEGALES SI AÚN NO SE HA HECHO

GESTIONAR EL IMPACTO PSICOLÓGICO PARA LOS EMPLEADOS

«Paro técnico, culpabilidad, sobrecarga de los equipos de informática... el ransomware también tiene consecuencias en los recursos humanos y hay que tenerlas en cuenta».

APLICAR EL PLAN DE COMUNICACIÓN ENTRE LOS CLIENTES AFECTADOS, LOS INVERSORES, ETC.

COMUNICAR EL SINIESTRO AL SEGURO