El enfoque de 360º de Beazley para la protección frente al ransomware

Un incidente de ransomware es uno de los ataques más perjudiciales y costosos que puede sufrir su empresa. El ransomware está en alza y su crecimiento no muestra indicios de ralentizarse. Los equipos de servicios de respuesta a reclamaciones y brechas de Beazley están en primera línea y tienen los conocimientos y la experiencia necesarios para ayudarle a proteger su empresa de estos ataques. Junto con nuestros proveedores de servicios de análisis forense (KPMG), hemos desarrollado una guía de buenas prácticas contra el ransomware para ayudarle a evitar que se produzcan estos incidentes.

Escenario de ransomware

1

Exposición inicial de su entorno

- Un grupo de ciberdelincuentes ataca a su empresa mediante una campaña de phishing.
- El malware consigue llegar a uno de sus usuarios desprevenidos en forma de archivo adjunto malicioso o un enlace de Internet en un correo electrónico.

2

Instalación del malware

- El usuario abre el archivo adjunto y el malware se instala en su ordenador.
- Aunque el usuario y sus equipos de seguridad y TI no lo saben, los atacantes ya han conseguido acceder a su entorno.
- Valiéndose de este acceso, los ciberdelincuentes analizan su red (sin ser detectados todavía) en busca de sistemas vulnerables y datos confidenciales. Esto incluye los ordenadores de otros usuarios, así como los servidores que de las aplicaciones críticas y los almacenes de archivos.

3

Propagación del ransomware

- Los ciberdelincuentes han logrado el acceso que necesitan y están listo para activar su trampa.
- Propagan una variante de ransomware que se extiende por toda la red cifrando los datos de forma indiscriminada.
- Los atacantes han encriptado una parte importante de sus activos y áreas enteras de la empresa están totalmente fuera de servicio, mientras que otras sufren alteraciones parciales.

4

Extorsión

- Los atacantes exigen una determinada cantidad de dinero a cambio de la clave para descodificar los archivos.
- El ataque también se hace público, lo cual provoca daños en la reputación de la empresa.
- Además, las autoridades reguladoras quieren saber si se ha producido un tratamiento inadecuado de los datos personales de los clientes, con el consiguiente riesgo de sufrir una importante sanción.

Cómo proteger a su empresa del ransomware

Controles mínimos, sin los que será vulnerable

- **Instalación y mantenimiento de una solución de protección de punto final (EPP) correctamente configurada y gestionada de forma centralizada:** una solución de EPP/antivirus fiable es un componente básico de cualquier sistema de seguridad.
- **Etiquetado de correos electrónicos:** Etiquetar los correos electrónicos de los remitentes externos permite alertar a los empleados de los mensajes que proceden de fuera de la organización.
- **Contenido y entrega de los correos electrónicos:** La aplicación estricta de los controles del Marco de Directivas de Remitente (SPF) en todos los mensajes de correo electrónico entrantes ayuda a verificar la legitimidad de los remitentes. Todos los mensajes entrantes deben filtrarse en busca de contenido malicioso, incluidos archivos ejecutables, documentos con macros y enlaces a sitios dañinos.
- **Complementos y configuración de Office 365:** habilitación de la autenticación de dos factores (2FA) en Office 365 y uso de la protección contra amenazas avanzada.
- **Macros:** Deshabilitación de la ejecución automática de las macros. Es aconsejable deshabilitarlas por completo si su empresa no las necesita.
- **Instalación de parches de seguridad:** es necesario realizar periódicamente análisis de vulnerabilidades e instalar rápidamente los parches de las vulnerabilidades críticas en los puntos finales y servidores, sobre todo en los sistemas expuestos al exterior.
- **Acceso remoto:** no hay que exponer el protocolo de escritorio remoto (RDP) directamente en Internet. En lugar de eso, se debe usar una puerta de enlace de escritorio remoto (RDG) o un RDP seguro situado detrás de una conexión VPN con autenticación de múltiples factores.
- **Controles del uso de soportes:** Se requiere establecer controles sobre la inserción y el uso de soportes que no cuenten con elementos adecuados de identificación o autenticación.
- **Proceso de respuesta frente a incidentes bien definido y probado:** Permite mitigar las pérdidas y restablecer rápidamente la actividad de la empresa tras un ataque de ransomware.
- **Copias de seguridad de sistemas y bases de datos esenciales:** asegúrese de realizar copias de seguridad periódicas, que deben ser verificadas y guardarse en una ubicación segura sin acceso a Internet.
- **Formación de los usuarios:** La mayoría de los ataques se aprovechan de los errores que cometen los usuarios. Impártales formación para que aprendan a identificar los correos electrónicos de phishing o con enlaces y archivos adjuntos maliciosos. Los simulacros de phishing periódicos son una excelente forma de prepararles.
- **Cortafuegos:** implemente el uso de cortafuegos de red y de servidor con conjuntos de reglas debidamente definidas, como por ejemplo no permitir las conexiones entrantes de forma predeterminada.

Medidas elementales para una mayor protección

- **Establecimiento de una configuración básica segura: e**l malware se basa en la búsqueda de lagunas de seguridad que pueda aprovechar. Una configuración básica de los servidores, puntos finales y dispositivos de red que se ajuste a estándares técnicos, como los del Centro de Seguridad en Internet (CIS), permite eliminar esas lagunas.
- **Filtrado del tráfico de la navegación en Internet:** las soluciones de filtrado del tráfico web evitan que los usuarios accedan a páginas maliciosas.
- **Uso de DNS protectoras:** impide el acceso a los dominios maliciosos conocidos en Internet.
- **Gestión de accesos efectiva:** es posible evitar que el ransomware se extienda como un virus por la empresa. Eso requiere establecer medidas apropiadas de control de acceso para los usuarios y los sistemas de toda la compañía. Por un lado, hay que implementar privilegios de acceso a los activos críticos (como servidores, puntos finales, aplicaciones, bases de datos, etc.); y por el otro lado, se debe aplicar la autenticación de múltiples factores (AMF) cuando sea necesario (como por ejemplo en el acceso remoto o vía VPN, las aplicaciones expuestas al exterior, etc.)
- **Pruebas regulares de las copias de seguridad:** la práctica reduce el tiempo de inactividad y la pérdida de datos al restaurar las copias de seguridad después de un ataque de ransomware.
- **Aislamiento de las copias de seguridad de la red corporativa:** evita que el ransomware pueda acceder a las copias de seguridad y cifrarlas en caso de que se produzca un ataque a la red principal de su empresa.
- **Creación de contraseñas de restauración únicas y guardadas por separado:** impide que los ciberdelincuentes puedan acceder a las copias de seguridad de los datos y cifrarlas.

Prácticas que proporcionan la máxima protección.

- **Herramientas de detección y respuesta de punto final (EDR):** las soluciones de EDR supervisan los servidores, los ordenadores portátiles y de sobremesa, así como los dispositivos móviles gestionados, para detectar señales de actividades maliciosas o inusuales. Estas herramientas también permiten una respuesta casi inmediata por parte de expertos en seguridad cualificados. Con un despliegue y una supervisión eficaces, las herramientas de EDR son una de las mejores defensas contra el ransomware y otros ataques de malware.
- **Evaluación inteligente del correo electrónico:** es recomendable ejecutar y evaluar automáticamente los archivos adjuntos de los mensajes entrantes en un entorno de sandbox para determinar si son maliciosos antes de su entrega a los usuarios.
- **Monitorización centralizada de los registros:** la recogida y supervisión centralizados de los registros, preferentemente mediante un Sistema de Gestión de Información y Eventos de Seguridad (SIEM), permite identificar las amenazas que traspasan las defensas internas.
- **Suscripción a servicios externos de inteligencia de amenazas:** ofrecen acceso a servicios externos que proporcionan detalles sobre el desarrollo de las tácticas, técnicas y procedimientos de los atacantes. También permiten consultar bases de datos de sitios web peligrosos conocidos, archivos adjuntos de correo, etc.
- **Cifrado de las copias de seguridad:** Evita que los atacantes puedan acceder a las copias de respaldo.
- **Segregación de la red:** permite controlar el acceso y el tráfico en el entorno de red. Un conjunto de reglas de cortafuegos correctamente configuradas asegurará que solo el tráfico necesario pueda pasar de un segmento a otro. Además, es prioritaria la segregación de los sistemas y el software que están llegando al final de su vida útil.
- **Aislamiento web:** el uso de una tecnología de aislamiento y contención de la web permite ofrecer a los usuarios una experiencia de navegación segura en Internet.
- **Permisos de aplicaciones:** los dispositivos solo deben poder ejecutar aplicaciones de confianza autorizadas por su empresa.

KPMG

KPMG ofrece una amplia gama de servicios que ayudan a las empresas a defenderse y responder a los ataques de ransomware. Para saber cómo podemos ayudarle, póngase en contacto con:

Matthew Martindale – Socio de ciberseguridad
cyber@kpmg.co.uk

beazley

BZCER034_ES_03/21