¿Cómo protegerme contra el Ransomware?

Mantener copias de seguridad periódicas de todos los datos importantes. Es necesario mantener dichas copias aisladas y sin conectividad con otros sistemas, evitando así el acceso desde equipos infectados. [ISO/IEC 27001:2022 8.13 Information backup; Nch-ISO 27002: 12.3.1 Respaldo de información]

Mantener el sistema actualizado con los últimos parches de seguridad, tanto para el sistema operativo como para el software que hubiere instalado. [ISO/IEC 27001:2022 8.8 Management of technical vulnerabilities; Nch-ISO27002: 12.6.1 Administración de vulnerabilidades técnicas]

Establecer separación de redes internas con elementos de control como por ejemplo un firewall interno distinto del firewall perimetral, con el objetivo de limitar las oportunidades de movimiento lateral del malware. [ISO/IEC 27001:2022 8.22 Segregation of networks; Nch-ISO 27002: 13.1.3 Segregación en las redes]

Mantener una línea de defensa con las últimas firmas de antivirus/antimalware (en lo posible incorporando tecnologías en base a análisis de comportamientos), además de disponer de una correcta configuración de los firewall a nivel de aplicación (basado en el criterio fundamental de que todo está prohibido salvo aquello que está explícitamente permitido). [ISO/IEC 27001:2022 8.7 Protection against malware; Nch-ISO 27002: 12.2.1 Controles contra el malware]

No permitir que los usuarios puedan instalar aplicativos, es decir, no tienen permisos de administrador [ISO/IEC 27001:2022 8.19 Installation of software on operational systems; Nch-ISO 27002: 12.6.2 Restricciones en la instalación de software y 12.5.1 Instalación de software en sistemas operacionales]

Contraseñas seguras, y en lo posible que incorporen la estrategia de un segundo factor de autenticación para reducir el impacto de una contraseña comprometida. [ISO/IEC 27001:2022 5.17 Authentication information; Nch-ISO 27002:2022 9.2.4 Administración de la información de autenticación secreta de los usuarios]

No exponer servicios de escritorio remoto a internet ni otros puertos de Windows (tcp/445 por ejemplo). Utilizar el concepto de extranet sobre VPN para acceder a recursos internos desde zonas externas. [ISO/IEC 27001:2022 5.15 Access control; Nch-ISO 27002: 9.1.2 Acceso a redes y servicios de red]

Políticas BYOD (Bring Your Own Device). Cada vez es más habitual que las empresas adopten este tipo de política, que permite al trabajador usar sus dispositivos electrónicos como medio de trabajo dentro de la organización. Estos aparatos son un potencial vector de infección y es por ello por lo que es imprescindible definir unas reglas de seguridad. [ISO/IEC 27001:2022 8.1 User endpoint devices; Nch-ISO 27002: 13.2.3 Mensajería electrónica]

Disponer de sistemas antispam y antimalware a nivel de correo electrónico y establecer un nivel de filtrado alto, de esta manera se reduce las posibilidades de infección a través de campañas masivas de ransomware por correo electrónico. [ISO/IEC 27001:2022 5.14 Information transfer; 8.7 Protection against malware; 8.23 Web filtering; Nch-ISO 27002: 13.2.3 Mensajería electrónica]

Establecer políticas seguras en el sistema para impedir la ejecución de archivos desde directorio comúnmente utilizados por el ransomware (App Data, Local App Data, etc.) Herramientas como AppLocker, Cryptoprevent o CryptoLocker Prevention Kit permiten crear fácilmente dichas políticas.

Es esencial que formemos y concienticemos a los colaboradores de una institución, enseñándoles a reconocer estas situaciones y cómo actuar en consecuencia. Los usuarios han de conocer las políticas en materia de ciberseguridad, como por ejemplo, las relativas de uso permitido en aplicaciones y dispositivos, el uso de WiFi públicas, la seguridad en el puesto de trabajo y en movilidad o la política de contraseñas.

Bloquear el tráfico relacionado con dominios y servidores C2 mediante un IDS/IPS, evitando así la comunicación entre el código dañino y el servidor de mando y control.

Mantener actualizadas listas blancas de aplicativos que están soportados y permitidos al interior de la institución.

Se recomienda el empleo de bloqueadores de Javascript para el navegador, que impide la ejecución de todos aquellos scripts que puedan suponer un daño para nuestro equipo. De este modo se reducen las opciones de infección desde la web (Web Exploit Kits).

Mostrar extensiones para tipos de archivo conocidos, con el fin de identificar posibles archivos ejecutables que pudieren hacerse pasar por otro tipo de archivo.

Cifra la información más sensible de tu institución para que, en caso de robo de tus ficheros, los ciberdelincuentes no puedan hacer pública la información. No olvides que no debes guardar la clave de cifrado en el mismo dispositivo, y si empleas un certificado para descifrarla, guárdalo en una memoria USB y mantenla desconectada de tus equipos.

Es recomendable realizar periódicamente una auditoria a nuestros sistemas, tanto para poner a prueba nuestros mecanismos de seguridad como para comprobar nuestra capacidad de defensa ante los ataques.

datto kaspersky SOPHOS radware VEEAM CISCO

eset Check Point SOFTWARE TECHNOLOGIES LTD SentinelOne Barracuda FORTINET