Asesoría Empresarial Integral
Av. Conde Oliveto 5 2ª izda
31003 Pamplona

T: 948 243 750
F: 948 236 747
www.pyramide.es
asesoria@pyramide.es

CONSEJOS BÁSICOS PARA LA PREVENCIÓN DEL RANSOMWARE:

1.- Primero y principal, asegúrese de disponer de copias de seguridad actualizadas.

El objetivo de la copia de seguridad es asegurar la continuidad del negocio en caso de un fallo que obligue a interrumpir la dinámica habitual de la empresa. Es esto lo que se debe valorar para saber cuántos recursos destinar a la copia de seguridad. Una buena práctica a la hora de realizar copias de seguridad es adoptar la estrategia 3-2-1 que se basa en diversificar las copias de seguridad para garantizar que siempre haya alguna recuperable.

Sus claves de actuación son las siguientes:

3: Mantener tres copias de cualquier fichero importante: el archivo original y 2 backups.

2: Almacenar las copias en dos soportes distintos de almacenamiento para protegerlas ante distintos riesgos. Si tuviéramos las dos copias en el mismo tipo de soporte, ambos pueden verse afectados por el mismo fallo de funcionamiento y por tanto poner en peligro las dos copias al mismo tiempo.

1: Almacenar una copia de seguridad fuera de la empresa, lo que también se conoce como backup offsite. La copia de seguridad en la nube es una clara opción de este tipo de copia.

2.- Parchee y mantenga actualizados su sistema operativo, antivirus, navegadores, *Adobe Flash Player*, *Java* y demás software.
Este hábito puede impedir ser comprometido mediante kits de explotación y asegura el correcto funcionamiento de los sistemas.

3.- Elimine de su parque informático aquellos equipos que cuentan con sistemas operativos obsoletos y de los que el fabricante no mantiene soporte activo.
Se demuestran como puertas de entrada o facilitadores de estos y otros tipos de ataques.

4.- Personalice sus ajustes de anti-spam de la forma correcta.
La mayoría de las variantes de ransomware son conocidas por difundirse mediante correos que atrapan visualmente y que contienen adjuntos contagiosos. Una gran idea es configurar su servidor de correo para bloquear adjuntos dudosos con extensiones como *.exe, .vbs, .scr*. [*NT: también, .vbe, .js, .jse, .bat, .cmd, .dll*]. La última oleada detectada se realiza con un documento .doc.
Otra solución es contratar un sistema de filtrado de correo perimetral, eliminando la mayor parte del correo spam, marcando el dudoso y evitando que lleguen al usuario final.

5.- No abra adjuntos que parezcan sospechosos.
Esto se aplica no solo a los mensajes de remitentes desconocidos sino de aquellos que usted cree que son de confianza. Los correos *phishing* pueden disfrazarse de notificaciones de servicios de transporte, algún comercio en línea, agencias oficiales o instituciones bancarias. Ante cualquier duda no abrir los documentos adjuntos.

6.- Piense dos veces antes de hacer clic.
Puede recibir hipervínculos peligrosos por medio de redes sociales o mensajería instantánea, y probablemente enviados por gente de su confianza, incluyendo amigos o colegas. Para llevar a cabo estos ataques, los cibercriminales comprometen sus cuentas y envían los enlaces maliciosos a tanta gente como sea posible.

Asesoría Empresarial Integral
Av. Conde Oliveto 5 2ª izda
31003 Pamplona
T: 948 243 750
F: 948 236 747
www.pyramide.es
asesoria@pyramide.es

7.- La "Opción Mostrar las Extensiones de Archivos" también puede ayudar.
Esta es una función nativa de Windows que le permite ver qué tipo de archivo se está abriendo, de modo se pueda distinguir claramente los tipos de archivos potencialmente peligrosos. Los estafadores pueden utilizar también una técnica que confunde donde a un solo archivo se le asignan varias extensiones. Por ejemplo, un archivo ejecutable puede parecer ser una imagen y tener la extensión *.gif*. Los archivos también pueden parecer tener dos extensiones, por ej. *cute-dog.avi.exe* o *table.xlsx.scr* – de modo que se debe estar atento a este tipo de trucos. Otro vector autónomo es mediante documentos MS Word maliciosos con macros habilitadas.

8.- En el caso que detecte un proceso sospechoso en su ordenador, apague de inmediato su conexión a Internet y el ordenador lo antes posible.
Esto es particularmente eficiente en una etapa temprana porque el ransomware no tendrá oportunidad de establecer una conexión con su servidor de Comando y Control (C&C) y por lo tanto no podrá completa la rutina de cifrado. Si ya ha empezado a cifrar el contenido, el apagado del ordenador impedirá que este continúe.

9.- Mantenga siempre activo, y correctamente configurado, el *Windows Firewall*.

10.- Ajuste su software de seguridad para escanear archivos comprimidos o archivados, si esta opción está disponible.

11.- Mejore la seguridad de sus componentes *Microsoft Office* (*Word, Excel, PowerPoint, Access*, etc)
En particular desactive las *macros* y *ActiveX*. Además, bloquear el contenido externo es una técnica confiable para evitar que se ejecute código malicioso en el PC.

12.- Usar contraseñas fuertes que no puedan ser halladas por los criminales remotamente usando fuerza bruta.
Use contraseñas fuertes únicas para distintas cuentas para reducir riesgos potenciales. Configure las directivas de su empresa (si se usa Active Directory) para automatizar la seguridad de las contraseñas de seguridad y tener el control de estas.

13.- Instale soluciones específicas para protegerse contra este tipo de ataques.
Se recomienda tener un antivirus de nueva generación que combine nuevas soluciones y servicios que proporcionen una visibilidad detallada de toda la actividad en todos los endpoints, un control absoluto de los procesos en ejecución, y la reducción de la superficie de ataque.
Por ejemplo, Adaptive Defense 360 de Panda Security.