Proteja su empresa frente a ataques de ransomware

Según el informe sobre ciberdelincuencia anual oficial de 2019, una empresa es víctima de un ataque con ransomware cada 14 segundos. Ahora que los empleados teletrabajan y lo hacen sin el cortafuegos corporativo, el riesgo crece.

¿En qué consiste?

El ransomware es un software malicioso que bloquea el acceso del usuario al sistema o dispositivo informático hasta que se paga una suma de dinero. Este malware descubre y cifra datos valiosos impidiendo que los usuarios puedan acceder a sus sistemas operativos para después pedir un pago, normalmente en forma de Bitcoin u otra criptomoneda, a fin de revelar la clave de descifrado.

No existe ninguna garantía de que, tras el pago del rescate, las víctimas recuperen el acceso a sus dispositivos y datos.

Copias de seguridad y actualización

Utilice varias soluciones de seguridad y asegúrese de que al menos una de ellas funciona sin conexión en un momento dado. Recuerde: los servicios de sincronización en la nube, como Dropbox o Google Drive, pueden sincronizarse después de que los datos ya se hayan cifrado, lo que hace que las copias de seguridad no sirvan de nada.

Actualice el software antivirus de la empresa periódicamente y opte por un proveedor que ofrezca complementos que detecten el cifrado de archivos y realicen copias automáticas de los archivos en peligro.

Elija una contraseña segura y cámbiela con regularidad. Recuerde que los ataques directos suponen el 31 % de todos los ataques.

El factor humano

Forme a los empleados para que sean capaces de reconocer los correos electrónicos sospechosos y notificar su existencia, ya que el ransomware se puede propagar fácilmente desde el spam y los correos electrónicos de suplantación.

Utilice la exploración de contenidos y filtros de correo electrónico para añadir otra capa más de protección. Estas herramientas pueden detectar enlaces maliciosos y eliminar correos electrónicos peligrosos antes de que lleguen al personal.

Asegúrese de contar con un protocolo de seguridad estandarizado en toda la empresa que abarque desde empleados hasta puestos de nivel ejecutivo.

Desarrolle un plan de recuperación de emergencia que incluya una respuesta a un posible ataque. Incluya directrices técnicas, pero también estrategias para mitigar las consecuencias legales y relativas a la imagen.

Compruebe con sus proveedores de seguros si su póliza cubre los costes relacionados con un ataque de ransomware.

Cree una estrategia de relaciones públicas para explicar la situación a los clientes, inversores y medios de comunicación en caso de que se produzca un ataque.

Para obtener más consejos expertos sobre la ciberseguridad en su fábrica inteligente, visite el www.euautomation.com