5 consejos de ciberseguridad para PyMEs

Tengo el placer de liderar el equipo de Avast Red, una unidad especializada dedicada a proteger nuestras aplicaciones empresariales, productos e infraestructuras de red. Se podría decir que mi equipo es todo negocio, literalmente. Mantenemos seguros los datos de nuestros clientes mediante el uso de técnicas ofensivas con fines defensivos. Específicamente, realizamos continuamente pruebas de penetración y evaluaciones de seguridad de los sistemas y aplicaciones de Avast en los que almacenamos información del cliente para minimizar el riesgo de acceso no autorizado y violación de datos. Pero una seguridad fuerte y efectiva necesita algo más que tecnología avanzada. También requiere que el personal esté capacitado en medidas y procedimientos de seguridad.

La cara del mundo de los negocios ha cambiado en el último año y medio, pero el esquema básico para la seguridad inteligente no lo ha hecho. Aquí está nuestro mejor consejo para ayudar a las PyMEs a mantener su infraestructura intacta, sus sistemas protegidos y sus datos seguros. Lo resumimos todo en cinco sencillos consejos de seguridad.

Los cinco mejores consejos de seguridad para PyMEs:

1. **Implementa un marco de política de seguridad**

Este es el primer paso crítico para tomar en serio la seguridad de tu empresa. Comienza un régimen de copias de seguridad, asegúrate de que las actualizaciones de seguridad se realicen de manera oportuna y utiliza la autenticación multifactor con tus empleados.

2. **Protege tus endpoints con software antivirus**

Utiliza software antivirus y antimalware de nivel empresarial, y asegúrate de que todos los endpoints estén cubiertos: PC, servidores, dispositivos IoT, etc. Si estás conectado a Internet, es un punto de entrada potencial y debe defenderse.

3. **Trae a los expertos**

Contratar a una organización especializada para el monitoreo de seguridad durante todo el día te quitará mucho estrés. Los ciberdelincuentes están en modo de ataque todo el día. Sus algoritmos nunca duermen, por lo que tus defensas tampoco deberían. Tener un equipo dedicado a la seguridad de tu empresa también te permite centrarte en las otras cosas importantes.

4. **Capacita a tus empleados**

Una de las mayores estafas que amenazan a las PyMEs en estos días es el ataque de compromiso de correo electrónico comercial (BEC, por sus siglas en inglés). Esta artimaña furtiva se basa en la ingeniería social para convencer a un empleado de instalar malware o hacer clic en un enlace malicioso. Por lo general, el atacante se hará pasar por un supervisor, un compañero de trabajo o alguien más relacionado con el negocio y afirmará tener información bastante urgente en forma de un enlace o archivo adjunto. La tecnología de seguridad avanzada solo te apoyará hasta cierto punto: debes capacitar a tus empleados sobre cómo reconocer las estafas BEC y otras tácticas comunes utilizadas por los atacantes.

5. **Únete a un círculo de información de riesgos**

Ser parte de un círculo local de información de riesgos es una excelente manera de mantenerte informado sobre lo que está sucediendo en tu sector. Te da acceso a la última inteligencia de riesgos de seguridad y te permite preparar defensas para diferentes tipos de ataques cibernéticos. Menos cosas te tomarán desprevenido si te mantienes en sintonía con otros en tu comunidad.

Actúa ahora para poner en práctica estos procedimientos de seguridad. La clave aquí no es elegir solo uno de estos, sino aplicarlos todos de una forma u otra. La ciberseguridad es importante para proteger nuestros hogares y cuentas personales, pero es absolutamente crítica para proteger nuestros negocios.