Home Office:
¿Cómo proteger la información de tu empresa?

safetica®

ASEGURE LA INFORMACIÓN DE SU EMPRESA EN POCAS HORAS

Qué acciones en el lado de TI pueden ser tomadas inmediatamente o dentro de unas pocas horas, localmente o remotamente cuando sea posible:

☑ Un tip efectivo para una situación inesperada

0. Toda la situación puede abordarse de manera muy efectiva, aunque de manera un poco radical. Simplemente puede "Desactivar todo" y permitir el acceso y los permisos a usuarios individuales cuando sea necesario.

☑ Proteja sus accesos

1. Configuración adecuada de roles de usuario y acceso a sistemas y ubicaciones. Se puede resolver fácil y eficientemente utilizando Active Directory (AD).
2. Habilitar una protección de acceso adicional; La validación se puede garantizar en este caso mediante el uso de la autenticación multi factor (generalmente de doble factor), que ahora es compatible con todos los sistemas de TI modernos. Esto ayuda a autenticar a los usuarios mediante SMS o códigos numéricos generados en la aplicación móvil

☑ Conexión remota a su red

3. Idealmente, se debe implementar una red privada virtual (VPN). De esta manera, conectar las computadoras a su red y a sistemas sensibles, datos y almacenamientos siempre se facilitan mediante VPN.

☑ Protegiendo sus estaciones de trabajo

4. Los dispositivos, en los que se pueden almacenar los datos de su empresa, deben tener discos duros cifrados.
5. Entre sus equipos de trabajo, las computadoras portátiles son una categoría bastante común que conlleva riesgos especialmente altos.
    a. Cifre los discos duros antes de enviarlos al usuario para proteger la estación de trabajo contra la fuga de datos en caso de pérdida o robo del dispositivo.
    b. Separe los perfiles de trabajo de los usuarios, como los usuarios domésticos, para evitar el acceso no deseado de usuarios no autorizados; los perfiles se pueden separar tanto a nivel del sistema operativo como en los navegadores web.
    c. Los medios de almacenamiento externos domésticos o de terceros también suelen estar conectados a los portátiles, lo que aumenta el riesgo de transmitir malware y también abre las puertas al robo de datos confidenciales: esto se puede controlar con las llamadas soluciones de control de dispositivos.

ASEGURANDO SUS ACTIVOS EN POCOS DÍAS

Ahora, algunas acciones más exigentes, que conducen, sin embargo, a una seguridad más adecuada del entorno de su empresa, incluso en el caso de la oficina en casa.

☑ Dispositivos portables

6. Los medios de almacenamiento portátiles como dispositivos USB, discos duros externos o dispositivos móviles también son una fuente frecuente de pérdida de información confidencial, conocimientos de la empresa, etc. Se recomienda cifrar discos duros y discos duros externos, ya sea por un método físico o virtual.

☑ Perímetro seguro

7. Implementar un perímetro de trabajo seguro reduce significativamente el riesgo de fugas de información confidencial. También restringir los servicios disponibles ayuda en gran medida a proteger los datos y las transferencias de datos:

    a. El uso de correos gratuitos públicos y servicios de correo electrónico basados en la web (como yahoo.com o gmail.com) conlleva riesgos considerables cuando se comunica desde una estación de trabajo.

    b. Lo mismo se aplica al uso de almacenamiento de archivos públicos bien conocidos o servicios en la nube disponibles gratuitamente (como, por ejemplo, Dropbox, WeTransfer, etc.).

    c. En general, restrinja el uso de dispositivos externos y su conexión a la estación de trabajo.

☑ Educación rápida para el usuario

8. Explicar la situación actual a los usuarios, actualizar las políticas de seguridad, compartir algunos consejos de seguridad altamente efectivos: estos son todos los pasos que ayudarán a proteger a los usuarios que trabajan desde casa. La emisión de recomendaciones se enfoca en trabajar con datos confidenciales y en trabajar con herramientas de TI y sistemas.

9. Mantenga su rutina de trabajo, horas de trabajo y calendario. Trabajar desde casa no significa trabajar independientemente, y la ética laboral junto con los contactos frecuentes también son un elemento importante para mantener un comportamiento razonable y seguro.

☑ Acceso Remoto

10. Los altos riesgos en términos de seguridad de los datos también están asociados con el llamado acceso remoto, que permite al usuario conectarse desde su computadora a la que funciona, y así acceder a sistemas internos y datos confidenciales. Desde el punto de vista del administrador de TI, este es un gran desafío, y las soluciones DLP pueden ayudar con su mitigación.

11. Los administradores de TI deben tener herramientas disponibles para monitorear los factores de riesgo y los incidentes de seguridad, idealmente con la opción de enviar alertas de seguridad instantáneas y / o informes regulares sobre sus datos más importantes.

PROTECCIÓN A LARGO PLAZO DE LOS DATOS Y EQUIPOS DE SU EMPRESA

También hay proyectos a largo plazo que llevan algún tiempo, pero que conducen a una protección ideal de su entorno de TI interno. Prevenga una situación similar en el futuro, esté preparado.

☑ Implementar protección de datos activa

12. En base a nuestras largas experiencias, recomendamos a los administradores de TI que diferencien entre las horas de trabajo oficiales y las horas no laborales de sus usuarios, y que supervisen de cerca las actividades e incidentes de seguridad fuera de las horas de trabajo, que implican intentos intencionados de filtrar datos confidenciales o acceso no autorizado a sistemas internos.

13. Mejore la seguridad de sus datos y la experiencia del usuario con las soluciones DLP (prevención de pérdida de datos) como Safetica.

☑ Entrenamiento detallado del usuario

14. La red de su empresa solo puede ser tan segura como la red de usuarios que se conectan a ella; eduque a sus usuarios sobre las mejores prácticas para configurar sus computadoras, dispositivos y redes personales:

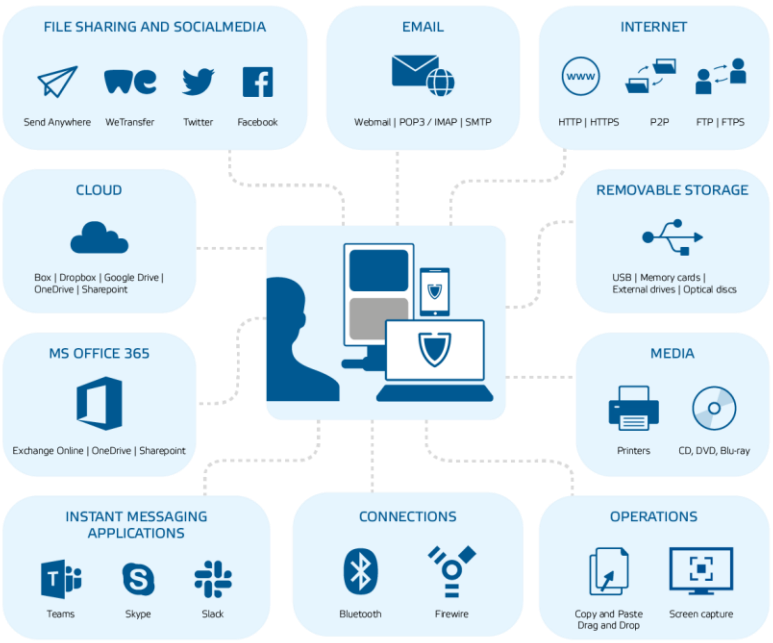
    a. Software de antivirus y sus configuraciones

    b. Actualización de aplicaciones, sistema operativo y componentes de la red.

    c. Usar aplicaciones de terceros y descargar aplicaciones de tiendas.

    d. Configuración de WPA2 con una protección de contraseña para conectarse a la red Wi-Fi doméstica.

DECIDA LO QUE AGREGA A LA "ZONA SEGURA"



CÓMO PUEDE AYUDARTE SAFETICA

Safetica mantiene sus datos protegidos en múltiples canales y plataformas, y garantiza que sus datos estén protegidos donde sea que se encuentre.

☑ Protección de datos: proteja los datos cruciales de su empresa y obtenga control sobre quién accede a ellos.

☑ Análisis del comportamiento de los usuarios: descubra cómo se utiliza el tiempo de trabajo, la impresión o el software costoso.

☑ Control de dispositivos conectados: determine qué dispositivos portátiles se pueden usar y evite que se conecten medios no autorizados.

SAFETICA

Safetica es una compañía de software Checa que protege a las compañías de todo el mundo de la filtración de datos confidenciales y amenazas internas. Estamos ofreciendo una solución de protección de datos disponible para pequeñas y medianas empresas. En Safetica creemos que todas las empresas merecen mantener seguros sus datos confidenciales.

La solución Safetica es otorgada por Gartner, Forrester y Radicati. Es el ganador de la competencia Red Herring TOP 100 Europe, el Premio Europeo de Seguridad de los Usuarios de Computer Weekly, y recibió
Calificaciones de 5 estrellas SNET y SC Magazine. Safetica también es signatario del Acuerdo de tecnología de ciberseguridad.

@Safetica @Safetica Safetica | www.safetica.com

03_2003