INFOPAPER:
CÓMO ADMINISTRAR LA CIBERSEGURIDAD DURANTE EL TELETRABAJO

Contenido

Introducción

El despertador suena más tarde, puedes comer en casa y el cuidado de los niños es más fácil de organizar. Teletrabajar puede tener muchas ventajas. Sin embargo, ciertos puntos no deben pasarse por alto para garantizar la seguridad de TI cuando se trabaja fuera de la empresa. Hornetsecurity tiene algunas recomendaciones para ayudarte con esto.

Teletrabajo ¡pero no olvides las precauciones de seguridad!

El avance de la digitalización y el desarrollo de nuevas tecnologías ya **han provocado muchos cambios para la economía mundial:** la computación en la nube, el big data, la robótica y la inteligencia artificial ofrecen ventajas a empresas de todos los sectores e industrias, como: la optimización de procesos, el ahorro de recursos y la rapidez en el intercambio de datos e información.

La creación de nuevas empresas y empleos son la consecuencia de estos desarrollos. Además, la tendencia ha llevado a **cambios en el lugar de trabajo:** muchos empleados pueden realizar sus tareas independientemente de la ubicación y seguir comunicándose con sus compañeros y responsables. **Las empresas permiten el teletrabajo.**

Microsoft 365 se considera un importante impulsor del trabajo colaborativo a través de la nube, lo que permite almacenar y compartir archivos importantes en tiempo real desde cualquier lugar. Esto simplifica aún más el teletrabajo. En tiempos de crisis, como la pandemia del coronavirus, el teletrabajo es a menudo la única forma en que las empresas pueden garantizar la seguridad de sus empleados; mientras mantienen las operaciones comerciales.

Sin embargo, tanto los empleadores como los empleados están constantemente **planteando preguntas sobre la seguridad de TI:**

- ¿Cómo puede garantizarse la protección de TI de toda la empresa durante el teletrabajo?
- ¿Tienen que tomar algunas medida las empresas y empleados?
- ¿Los mecanismos de protección como los filtros de spam y virus también están activos durante el teletrabajo?

En la siguiente sección, explicamos los riesgos de seguridad durante el teletrabajo y las posibles precauciones que garantizarán **la protección de datos internos de la empresa y las comunicaciones remotas.**

La formación de tus empleados sobre los potenciales riesgos es crucial

Primero, se debe informar a los empleados sobre **posibles riesgos de seguridad y medidas de protección a tomar** antes de comenzar a teletrabajar.

Hay que proporcionar información clara e inequívoca sobre la **normativa vinculante sobre ciberseguridad** y protección de datos de la empresa. Y es mejor que sea por escrito para que el procedimiento sea transparente y comprensible para todos.

Es particularmente importante sensibilizar a las personas de **peligros potenciales** como los ataques de phishing, que obviamente siguen siendo una amenaza durante el teletrabajo.

Además, asegúrate de informar a quiénes pueden recurrir los empleados si surgen problemas relacionados con la seguridad, con el fin de actuar rápidamente.

Asegura los datos de tu empresa y usa VPN

La WLAN en casa, en una cafetería o en el tren puede presentar riesgos de seguridad. Si los empleados acceden a **información sensible** o inician sesión en cuentas comerciales a través de una red insegura, la empresa corre el riesgo de que los ciberdelincuentes se aprovechen de la información en caso de un ciberataque. Por lo tanto, las empresas deben establecer medidas de seguridad como **red privada virtual (VPN)** soluciones para usar en conjunto con WLAN.

El servicio VPN también se puede complementar con la autenticación de 2 factores y cuando se trabaja a través de VPN, el empleador debe tener cuidado de limitar los derechos de acceso para que cada persona solo pueda acceder a la información relevante para ella. También existe el riesgo de pérdida de datos si un empleado almacena información confidencial en un ordenador portátil, que podría ser robado. Lo ideal es que los datos confidenciales solo se almacenen en **servidores seguros de la empresa o en entornos en la nube,** donde solo se puede acceder a través de VPN. Sin embargo, si los datos se almacenan en discos duros externos, es importante cifrar esta información o el acceso.

Evita acceso y visualización no autorizados

Para aprovechar al máximo el tiempo durante tus viajes, **mucho trabajo se realiza de camino**, por ejemplo: en el aeropuerto o en el tren. El problema de ello es que las personas que se sientan a tu lado, tienen la oportunidad de leer información interna de la compañía. **Deben usarse filtros de privacidad** siempre que se acceda a datos confidenciales de la empresa fuera de la oficina. Además, **siempre que el empleado abandone el ordenador debe bloquear la pantalla.** Esto también se debe hacer durante el teletrabajo. Por supuesto, el acceso al ordenador debe requerir una **contraseña al inicio**.

Usa hardware propio de tu empresa

El dispositivo final del usuario representa una brecha de seguridad importante. Si bien es relativamente fácil para la TI de la empresa, hacer cumplir y garantizar ciertos requisitos mínimos de seguridad en los dispositivos de la compañía. Esto es difícil para los dispositivos privados de los empleados.

La protección de estos dispositivos solo es parcialmente posible. Especialmente las memorias USB y los discos duros externos se consideran **la puerta de entrada del malware.** Sin embargo, existen varios enfoques para controlar los riesgos. Estos incluyen **políticas específicas del dispositivo** que aseguran que al menos los componentes de seguridad más importantes estén instalados, y activados en los clientes por ejemplo: bloqueo automático, desbloqueo solo con contraseña o escáneres de malware y firewalls.

Tambien ayudan, mecanismos como medidas de **control de acceso a la red (NAC).** Por ello, solo los dispositivos autorizados tienen acceso a la red de la compañía, y se puede garantizar que los componentes relevantes estén activos. **Sin embargo, la forma más segura es utilizar el hardware propio de la empresa.**

Instalar el último software de seguridad

Todos los dispositivos corporativos, incluidos los smartphones y los ordenadores portátiles, deben estar protegidos por un **software de seguridad actualizado.** En el mejor de los casos, esto incluye **características para la eliminación de datos de dispositivos** reportados como perdidos o robados, separación de datos personales y profesionales, y restricción de opciones de instalación de aplicaciones.

Pero el software de seguridad no sirve solo para proteger dispositivos; los cibercriminales también están atacando **aplicaciones y servicios**. Uno de los objetivos de ataque más populares es **Microsoft 365**, que actualmente tiene alrededor de 180 millones de clientes corporativos a nivel internacional.

Microsoft 365 - basado en la nube - es ideal para el teletrabajo. Sin embargo, identificar a un usuario de Microsoft 365 es muy fácil para un atacante, porque los registros MX y las entradas de detección automática son de acceso público. **Funciones de seguridad integrales** están diseñadas para evitar posibles ataques a las cuentas de Microsft 365, pero debemos recordar que al estar los datos en la nube se puede acceder desde cualquier lugar. Incluso en el caso de acceso no autorizado. Al usar Microsoft 365, las empresas eliminan un aspecto de seguridad importante: el firewall.

Si un atacante logra obtener acceso no autorizado a una cuenta de Microsoft 365, todos los datos están disponibles para él sin restricciones. Por lo tanto, los expertos en ciberseguridad recomiendan no depender únicamente de los mecanismos de protección de Microsoft, sino también asegurar las cuentas de Office 365 con **soluciones adicionales de terceros.**

Por ejemplo, los proveedores especializados ocultan los registros DNS y MX de Microsoft, haciendo **a los usuarios de Microsoft 365 difíciles de identificar para los atacantes y, por tanto, disminuyendo la probabilidad de que sean atacados.**

Protégete de los fallos de comunicación por correo electrónico

Los contratos, la información importante y los datos de contacto se intercambian por correo electrónico. Sin embargo, si el propio servidor de correo electrónico de la compañía fallara durante un período de tiempo más largo, esto sería catastrófico, especialmente para los empleados que teletrabajan, donde el soporte no está disponible tan rápido como de costumbre.

Las operaciones comerciales vitales se vuelven mucho más complejas a largo plazo **con posibles pérdidas de comunicación** Por lo tanto, es particularmente importante que haya soluciones alternativas disponibles para ayudar en una emergencia, de modo que no se pierdan los correos electrónicos y se puedan enviar y recibir mensajes. El **servicio de continuidad (Continuity Service) sería aquí la solución.** Un sistema de monitoreo autónomo detecta cuando el servidor de correo del cliente ha fallado, y **Continuity Service se activa de forma automática e inmediata.**

La entrega de los correos electrónicos se realiza sin interrupción por medios alternativos (buzón POP3 / IMAP o acceso a correo web).

El acceso a correos electrónicos seguros se mantiene incluso si hay una interrupción, por ejemplo, directamente desde Outlook.

Checklist

Con el siguiente "Checklist" de Hornetsecurity tendrás una visión general de los puntos más importantes a tener en cuenta para mantener medidas de **ciberseguridad durante el teletrabajo:**

- ☑ **La formación de los empleados ayuda a crear conciencia sobre los riesgos potenciales.**
- ☑ **Los clientes VPN garantizan un acceso seguro a datos confidenciales en la red corporativa**
- ☑ **Se debe evitar el acceso no autorizado al equipo.**
- ☑ **Usar hardware propio minimiza los riesgos de seguridad.**
- ☑ **El último software de seguridad y soluciones de terceros adicionales para los servicios en la nube de Microsoft 365 evitan los ciberataques.**
- ☑ **Los servicios de continuidad evitan la falla de la comunicación por correo electrónico en una emergencia.**