Con el teletrabajo, la ciberseguridad comienza con la protección de terminales

El tema a desarrollar en estos días es: Con el teletrabajo, la ciberseguridad comienza con la protección de terminales. El repentino cambio al teletrabajo ha cambiado nuestros hábitos y los ciberdelincuentes han aprovechado esta nueva oportunidad.

Como muchas empresas se ven obligadas a adoptar el trabajo remoto muy rápidamente, la seguridad ha pasado a un segundo plano. Por un lado, porque pensaban que solo iba a ser un episodio aislado, por otro lado, porque la mayoría planeaba centrarse en la seguridad una vez que todo estuviera en funcionamiento.

Desde el inicio de esta crisis de salud, se ha observado un número significativo de campañas de malware, spam y estafa directa. Incluso hoy en día, los ciberdelincuentes continúan aprovechándose de la falta de seguridad informática, vinculada al trabajo remoto, para lanzar nuevo malware y experimentar con nuevas técnicas.

1. La seguridad comienza con los puntos finales

Concretamente, todos los dispositivos conectados a una red son puntos finales: escritorio, portátil, servidor, entorno virtual o dispositivo IoT (impresora, Smart TV, dispositivo de fitness conectado o incluso una tostadora). Pero la digitalización generalizada dificulta considerablemente la protección de los puntos finales porque ahora todos los

dispositivos pueden conectarse a una red. Estos dispositivos conectados son cada vez más susceptibles a los ataques, ya sea para terminar la actividad comercial o para robar datos o dinero.

2. Comprenda qué hay en su red

La protección de los terminales es esencial, pero la pregunta correcta es ¿Cuántos dispositivos están realmente conectados a la red corporativa? Es sorprendente, pero más allá de los terminales tradicionales (computadoras de escritorio, portátiles y servidores) bien identificados, la mayoría de las empresas navegan de vista.

¡Esto puede y debe cambiar! Es imposible proteger lo que no se ve, por lo que es imperativo que las organizaciones identifiquen todos los dispositivos que acceden a la red y su punto de acceso para entender qué está conectado y, sobre todo, qué no está protegido. Una plataforma de protección de terminales impulsada por inteligencia artificial puede ayudar a las empresas a identificar fácilmente y obtener información sobre todos los dispositivos conectados a la red.

3. Proteja los dispositivos de la empresa

Si los empleados no están trabajando actualmente en sus negocios, eso no significa que siempre estarán trabajando desde casa. También pueden conectarse y trabajar en un parque (respetando las distancias sociales), un hotel o en su segunda casa. Al elegir trabajar en cualquier lugar y desde cualquier red pública, los empleados se arriesgan potencialmente a exponer los datos de la empresa en sus computadoras portátiles.

A continuación, se ofrecen algunos consejos para ayudar a las organizaciones a proteger distintos puntos finales:

- Asegúrese de que todos los dispositivos de la empresa utilicen cifrado de disco completo, de modo que si una computadora portátil se pierde o es robada, los datos que contiene no sean accesibles para los ladrones.
- Utilice la administración de contraseñas para que todas las cuentas de dispositivos requieran credenciales de inicio de sesión únicas.
- Recuerde a los empleados que cierren la sesión cuando el sistema no esté en uso, incluso en casa.

4. Sea inteligente al conectarse a redes corporativas

El acceso remoto a la propia red corporativa siempre aumenta el riesgo de que los datos de la organización caigan en las manos equivocadas. Esto sucede a menudo cuando los empleados están menos atentos y adoptan comportamientos que no tendrían en la oficina, como usar su computadora para uso personal, por ejemplo.

Para proteger mejor los datos de una empresa y conectar a los empleados remotos a sus redes y servidores, es recomendable utilizar una solución de seguridad de «confianza cero», que proporciona un modelo de seguridad de red basado en un estricto proceso de control de identidad, con el mismo requisito de seguridad que si el dispositivo estaba conectado a la red local de la organización. Y no dude en recordar que una computadora portátil de la empresa utilizada en casa sigue siendo propiedad de la empresa.

Se tolera el uso personal de estas herramientas informáticas si sigue siendo razonable y no afecta la seguridad o productividad de la red. También le corresponde al empleador establecer los contornos de esta tolerancia e informar a sus

empleados.

5. Tenga cuidado con las campañas de phishing y el malware

Con el aumento en la cantidad de correos electrónicos y otros servicios de mensajería instantánea que le permiten mantenerse conectado mientras trabaja de forma remota, puede ser difícil para los empleados diferenciar los correos electrónicos y comunicaciones legítimos de los que no lo están. A medida que las campañas de phishing y malware continúan aumentando, es imperativo inspeccionar los enlaces antes de hacer clic y pasar el cursor sobre ellos para ver la URL real.

Otra forma sencilla de ayudar a los empleados a protegerse contra este tipo de campañas es utilizar una solución de seguridad de respuesta y detección de terminales automatizada para bloquear el contenido malicioso ejecutado por el usuario. Con la gran mayoría de los empleados cambiando sus formas, proteger los activos comerciales, de comunicaciones y digitales nunca ha sido más esencial.

A medida que se adoptan nuevas formas de trabajo, las empresas deben proteger las computadoras que se utilizan en el hogar y asegurarse de que todos los dispositivos de IoT circundantes no puedan comunicarse con los activos corporativos. Esto requiere en particular la adopción de herramientas y estrategias apropiadas que protejan cada endpoint, en un estado hipermóvil, contra cualquier tipo de ataque, en cada etapa del ciclo de vida de la amenaza.

Leer también: Gestión de riesgos de seguridad cibernética del trabajo remoto en tiempos de epidemias y pandemias; Trabajo remoto, limitando las horas de trabajo y las de uso personal ; Qué es el trabajo remoto, beneficios y ventajas.