TELETRABAJO

Seguridad Endpoint para la continuidad del negocio

2020

TELETRABAJO

Seguridad Endpoint para la continuidad del negocio

Teletrabajar supone tener que cambiar el entorno al que estamos acostumbrados en las oficinas de la organización por un entorno al que, generalmente, le hemos otorgado otros usos como el ocio y el descanso. Sin embargo, nuestra carga de trabajo, así como horarios y procedimientos no se ve alterada, por tanto, para conseguir las misma eficiencia y seguridad que en nuestro puesto laboral habitual, debemos adoptar una serie de medidas con el único objetivo de proteger los activos de nuestra organización. Donde nosotros vemos una situación desconcertante, los cibercriminales ven una oportunidad de negocio a causa de la inseguridad que puede generar el teletrabajo.

Desde **Grupo Oesía** queremos que el teletrabajo se realice de forma segura y por ello ofrecemos una solución de seguridad complementaria para proteger los endpoints o puestos finales de trabajo y que todos los miembros de la organización puedan continuar con sus labores diarias.

Para ello, nos apoyamos en tecnología de nuestro partner **Check Point Software Technologies**, considerada una de las empresas líderes en el mercado.

Retos a los que nos enfrentamos al teletrabajar con Endpoint:

Al igual que exigimos cumplir la normativa y políticas de seguridad cuando trabajamos en las oficinas de la organización, debemos asegurar que el conjunto de profesionales de la compañía continúe aplicando estas medidas en remoto, a

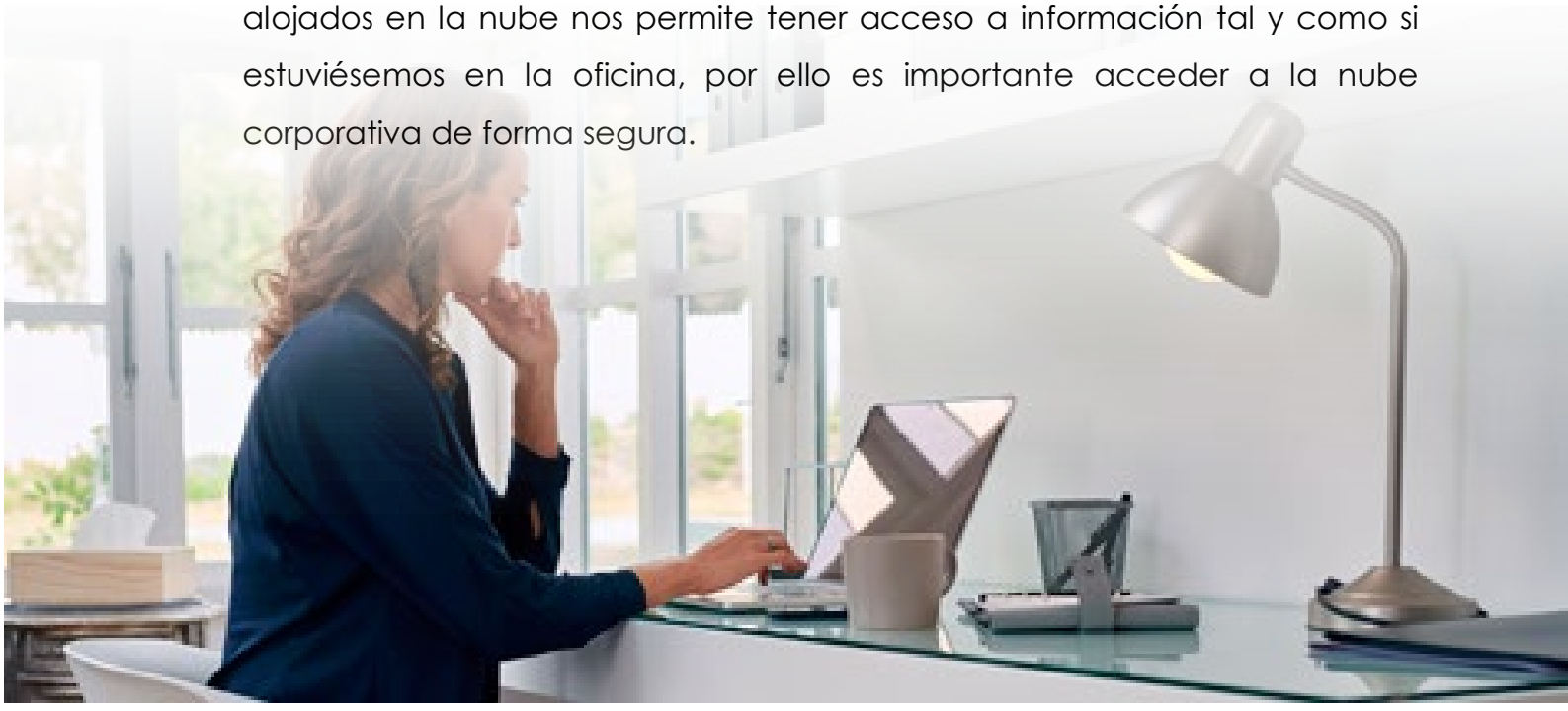
pesar de no disponer de los mismos recursos. El acceso a internet y a las herramientas corporativas es algo que está prácticamente asegurado en nuestros hogares, pero al igual que en las oficinas de la organización, tenemos que aplicar una serie de medidas para realizarlo de forma segura.

Este escenario nos exige la revisión de la normativa y políticas de seguridad en relación al acceso remoto de dichas herramientas corporativas y la información que manejamos. Surge la necesidad de actualizar nuestras medidas y anticiparnos a la actividad de los cibercriminales.

Algunos de los retos que enfrenta el teletrabajo son los siguientes:

- **Evitar la suplantación de identidad (Phishing):** hemos de tener cuidado con la comunicación electrónica que recibimos. Hemos de verificar el remitente, enlaces incluidos en el mensaje, contenido adjunto que podamos encontrar y el propio contenido del mensaje. Tenemos que ser críticos y dudar de los dominios sospechosos, puesto que los ciberdelincuentes usan la ingeniería social lograr sus objetivos.
- **Segregación de funciones en los dispositivos**: es lógico, sobre todo al principio, no diversificar funciones con nuestros dispositivos al teletrabajar en el mismo espacio físico en el que estamos acostumbrados a descansar o realizar actividades de ocio. Este hecho es vital para proteger nuestros dispositivos de trabajo y a la propia organización. Cada dispositivo tiene una función específica y tenemos que diferenciar bien lo que podemos y lo que no podemos hacer con cada dispositivo, puesto que el endpoint únicamente se usa para trabajar. Nunca debemos combinar nuestros diferentes dispositivos con las distintas utilidades que puedan ofrecernos.
- **Actualización de dispositivos y antivirus**: mantener los dispositivos y antivirus actualizados tal y como nos advierten los fabricantes de software o sistema operativo es esencial para aumentar la seguridad en el puesto de trabajo. Esta pequeña acción corrige las vulnerabilidades conocidas y mantiene seguro el endpoint y a la organización.

- **Verificar:** no supongamos nada, verifiquemos. Hemos de comprobar la información, quién tiene acceso a la misma, quién puede dar dichos accesos y asegurarla mediante la autenticación multifactor.
- **Proteger los datos:** debemos asegurarnos de que la información que manejamos con las herramientas corporativas está protegida en todo momento y no supone un riesgo para nuestra organización, de lo contrario, estaremos exponiendo el duro trabajo realizado a delincuentes que aprovechan estas situaciones de confusión para perpetrar sus objetivos.
- **Conexión segura**: trabajemos siempre de forma segura, utilizando las redes VPN (Red Privada Virtual) proporcionadas por la organización para acceder a los recursos necesarios a la hora de desempeñar el trabajo.
- **Proteger nuestro equipo**: el hecho de teletrabajar supone que ganemos confianza en relación a lo que nos rodea, es decir, el perímetro de seguridad alrededor de nuestros dispositivos, y por ende que perdamos seguridad en cierta medida. Es importante actuar con nuestro endpoint de la misma forma que actuamos en la oficina, es un activo de gran valor.
- **Cifrar los dispositivos:** El valor de la información que contienen nuestros dispositivos de trabajo es incalculable y también esencial tanto para la realización de nuestras laborales como para la continuidad del negocio. Es importante cifrar todos nuestros dispositivos, incluyendo los de almacenamiento extraíble.
- **Utilizar la nube de forma segura**: la gestión de los recursos de la organización alojados en la nube nos permite tener acceso a información tal y como si estuviésemos en la oficina, por ello es importante acceder a la nube corporativa de forma segura.



Paquete de Seguridad Endpoint desde 10,5 € al año.

Desde **Grupo Oesía** consideramos fundamental proteger a nuestros clientes y sus activos más esenciales. Por ello creemos que proteger el teletrabajo, hoy más que nunca, está justificado, contribuyendo de esta forma a la Continuidad de Negocio de nuestros clientes.

Características	Básico	Avanzado	Completo
Instalación			
Agente	✓	✓	✓
Extensión de navegador	✓	✓	✓
Reducción de la Superficie de Ataque			
Endpoint Firewall	✓	✓	✓
Control de aplicaciones	✓	✓	✓
Cumplimiento Endpoint	✓	✓	✓
Protección de puertos (Control periférico)	✓	✓	✓
Acceso remoto VPN	✓	✓	✓
Protección de datos: Cifrado de disco completo y almacenamiento extraíble			✓
Previene ataques antes de su ejecución			
Antivirus Endpoint: firmas conocidas, heurística.	✓	✓	✓
Análisis estático: Prevención basada en Machine Learning.	✓	✓	✓
Anti-Exploit	✓	✓	✓

Zero-Phishing: Anti-phishing, prevención de reutilización de credenciales	✓	✓	✓
Simulación de Amenazas (SandBox)		✓	✓
Extracción de Amenazas (Desinfección de documentos)		✓	✓
Detección y Protección en ejecución			
Anti-Ransomware Vigilancia de comportamiento: Mutaciones en malware conocido y malware desconocido	✓ ✓	✓ ✓	✓ ✓
Vigilancia de comportamiento: Ataque sin archivo	✓	✓	✓
Anti-Bot: Detección de tráfico de comando y control (C&C) malicioso	✓	✓	✓
Anti-Evasion: Detección de técnicas de evasión	✓	✓	✓
Contención y Resolución			
Bloqueo de tráfico a servidores de comando y control (C&C)	✓	✓	✓
Prevención de movimientos laterales y aislamiento de máquinas infectadas	✓	✓	✓
Finalización de proceso y cuarentena de archivos	✓	✓	✓
Restauración de archivos encriptados	✓	✓	✓
Esterilización completa de la cadena de ataque	✓	✓	✓

Investigación del Ataque y Respuesta (EDR)			
Colección forense	✓	✓	✓
Informe de análisis forense de eventos automatizado	✓	✓	✓
Caza de amenazas	✓	✓	✓
Inmunización contra ataques en múltiples superficies (IoC & IaA Sharing)	✓	✓	✓
Gestión, Despliegue, Monitorización 24X7 y Gestión de Incidentes en la nube	✓	✓	✓

Contacte con nosotros
si quiere asegurar sus Endpoints:

cert@oesia.com

La seguridad de la información empieza por ti.

Ciberseguridad | oesia

ciberseguridad.oesia.com