Mantenga la seguridad de su negocio cuando trabaje a distancia

Sebastien Roche, responsable principal de la seguridad de la información de Alcatel-Lucent Enterprise, comparte ideas sobre el enfoque de ALE acerca de la continuidad y la seguridad de la actividad empresarial.

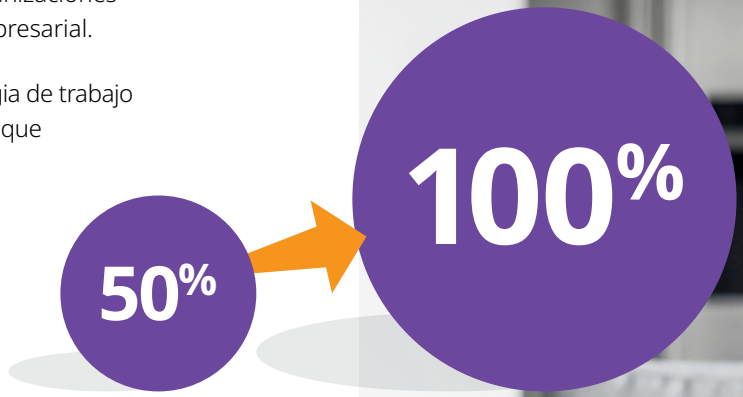
Folleto

Alcatel·Lucent
Enterprise

La nueva realidad #WFH

Desde 2020, las empresas que antes no ofrecían la opción de trabajar desde casa (#WFH) se enfrentan al reto de transformar sus organizaciones para garantizar la continuidad y la seguridad de la actividad empresarial.

Hace más de 15 años, Alcatel-Lucent Enterprise inició una estrategia de trabajo desde casa que fue adoptada por más del 50 % de los empleados que trabajan en las 50 oficinas de todo el mundo. Con más de la mitad de los empleados de ALE trabajando desde casa, ya teníamos la red y la arquitectura informática necesarias para posibilitar el trabajo a distancia. El verdadero desafío fue encontrar la forma de pasar del 50% de trabajadores en línea al 100%.



Listos para la acción

Desde hace casi 10 años, ALE se ha embarcado en una amplia transformación de TI. Se adoptó una arquitectura de red que proporcionaba seguridad en la nube para bloquear de forma proactiva las amenazas, identificar posibles ataques y garantizar el acceso seguro de los empleados.

La transformación incluía lo siguiente:

- Seguridad en la nube con puntos de acceso virtuales
- Rastreo en tiempo real
- Identificación de patrones de comportamiento atípicos para detectar amenazas

Folleto
Mantenga la seguridad de su negocio cuando trabaje a distancia

Preparación = Respuesta rápida en situaciones de crisis

Cuando golpeó la crisis, la decisión de empezar a trabajar a distancia a partir del lunes se tomó el viernes anterior por la tarde. Se indicó a los empleados que se llevaran sus portátiles y monitores a casa. El lunes por la mañana se empezó a trabajar como de costumbre, sin interrupciones, con los empleados comenzando el día desde sus oficinas a distancia. La transformación de la red que se había realizado aseguraba una conectividad remota segura, independientemente de la ubicación de los empleados.

El desafío del acceso

Los perfiles de usuario supusieron un reto importante para nuestro plan #WFH. En concreto, los equipos de I+D y de asistencia técnica necesitan acceder a determinados servidores y plataformas de desarrollo, lo que no permitía nuestra solución de acceso remoto.

Cuando comenzaron las labores de transición de todos los empleados al #WFH, adaptamos nuestra infraestructura para aumentar el ancho de banda y poder soportar el aumento del número de conexiones remotas para los empleados que trabajaban desde casa.

La seguridad es fundamental

La seguridad y la protección de los datos de las empresas son factores de suma importancia en tiempos de incertidumbre y afectan a muchas organizaciones que manejan información confidencial, como las organizaciones del sector público, los ministerios, los ayuntamientos y otros organismos municipales.

Antes de que empezáramos a contemplar el #WFH en ALE, implantamos y distribuimos una infraestructura segura, así como una solución de conexión privada totalmente basada en la nube para todos los empleados, a fin de garantizar el acceso remoto seguro a la red. Mantuvimos la solución VPN existente para un pequeño número de equipos que tenían necesidades específicas, como la conexión de teléfonos IP en sus oficinas a distancia. También proporcionamos a los empleados ordenadores profesionales capaces de gestionar descargas y actualizaciones de software automáticas.

Cierre la puerta a las vulneraciones de seguridad

Como era de esperar, durante este prolongado período de trabajo a distancia, se ha producido un aumento de las llamadas y los correos electrónicos relativos a correos electrónicos sospechosos y solicitudes de actualización de contraseñas. También hemos observado un repunte de los ataques de phishing, así como de ataques dirigidos a software vulnerable.

Si bien el uso de proxies protege a ALE de los principales problemas de ciberseguridad, todavía vemos nuevas vulneraciones cada día, en correos electrónicos, descargas o versiones de software/sistema operativo no actualizadas.

Mantener las comunicaciones

En ALE, mantenemos un vínculo virtual continuo con los equipos de ALE. Nos comunicamos frecuentemente, compartimos consejos y buenas prácticas y nos aseguramos de que nuestro equipo esté disponible para prestar asistencia a todos los empleados.

Lista de comprobación de ALE para el trabajo remoto seguro:

- No permita ni fomente el uso de dispositivos personales (PC) para la comunicación y el intercambio de datos profesionales
- Habilite un acceso privado y seguro para los empleados
- Automatice las actualizaciones de software en toda la red de la empresa
- Preste atención a las solicitudes de correo electrónico sospechosas
- Utilice software certificado. Las auditorías y certificaciones proporcionan una autenticación de seguridad del software.
- Simplifique los procesos de toma de decisiones. En situaciones de emergencia, un director de seguridad de la información o un responsable de TI debe tomar decisiones de manera rápida para abordar los problemas con el fin de garantizar la continuidad de los servicios.

Seis recomendaciones de ALE para una conectividad remota segura

1. Automatizar los recordatorios de cambio de contraseña

Ayude a los empleados a cambiar las contraseñas de la empresa antes de que caduquen. Antes de su vencimiento, los empleados recibirán un correo electrónico diario con instrucciones para que modifiquen la contraseña.

2. Habilitar la copia de seguridad de los datos en la nube

Permita y anime a los empleados a que guarden sus datos periódicamente para evitar cualquier pérdida en caso de que sus ordenadores portátiles tengan un problema. Ponga a disposición espacios de almacenamiento para las copias de seguridad de datos y ofrezca asistencia remota a través de un centro de servicios de TI o especialistas en TI.

3. Recordar a los empleados las mejores prácticas en materia de protección de dispositivos

Mantenga su ordenador portátil en perfectas condiciones:

- Apague el ordenador portátil al final del día (evite el modo de suspensión/bloqueo)
- Mantenga el ordenador portátil alejado de las fuentes de calor (como el sol o los radiadores)
- Evite comer o beber cerca del ordenador portátil
- Mantenga los cables lejos de los niños y las mascotas

4. La seguridad es lo primero

Preste formación a los equipos en materia de riesgos y mejores prácticas de seguridad:

- Anime a los empleados a pensarlo dos veces antes de hacer clic en los enlaces de los correos electrónicos, incluso cuando parece que el emisor es alguien conocido
- Ofrezca seguimiento informático en caso de duda
- Proporcione herramientas para la notificación de correos electrónicos sospechosos
- Utilice la ludificación para crear una cultura que priorice la seguridad: en ALE, utilizamos la ludificación para animar a los empleados a detectar y notificar correos electrónicos sospechosos

5. Comunicación

El aislamiento hace que la gente sea vulnerable a los ciberataques. Encuentre formas de mantener a sus equipos conectados:

- Organice actualizaciones periódicas, reuniones virtuales, eventos, espacios de colaboración, momentos «happy hour»
- Anime a los empleados a conectarse a menudo con sus equipos
- Envíe correos electrónicos regularmente para que los empleados sepan que el equipo de TI está disponible para ayudarlos y recordarles las mejores prácticas de seguridad

6. Fomentar hábitos de conectividad saludables

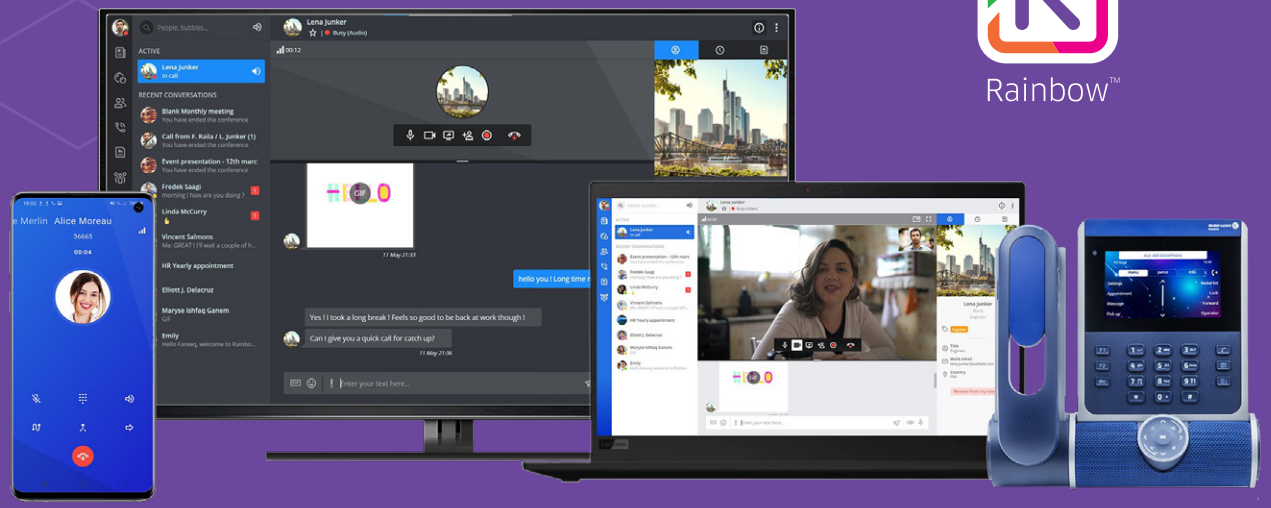
Las jornadas laborales de 12 horas con conexión continua o las reuniones consecutivas pueden ser algunos riesgos del trabajo a distancia. Anime a los empleados a que encuentren momentos de desconexión y en que no utilicen dispositivos electrónicos, y a que pasen tiempo con la familia o al aire libre.

Rainbow™ de Alcatel-Lucent Enterprise para la colaboración conectada

Rainbow: una plataforma de colaboración en equipo en la nube que ofrece chat, llamadas de vídeo y audio, así como la posibilidad de compartir pantallas y documentos, proporciona a los empleados de ALE los servicios que necesitan para estar conectados. La plataforma la utilizan ampliamente todos los empleados para colaborar con compañeros, clientes y Business Partners, y está conectada al sistema telefónico para las llamadas externas.

Además, nuestros Partners y clientes también han escogido Rainbow como su solución de colaboración. Rainbow cumple los requisitos de seguridad del sector público, de la defensa, la sanidad y otros sectores específicos, y se ajusta a estrictas normas de seguridad, como el RGPD y la HDS, entre otras. Rainbow cuenta con las certificaciones ISO 27001 y CSPN de la ANSSI.

Rainbow™



Folleto
Mantenga la seguridad de su negocio cuando trabaje a distancia

Trabajar a distancia con total seguridad

Mientras las organizaciones permiten a más empleados trabajar a distancia, los analistas confirman el aumento de los riesgos de ciberataques.

En ALE, utilizamos las aplicaciones y servicios de comunicación y colaboración que implantamos para nuestros clientes. Estas soluciones se desarrollan pensando en la ciberseguridad, sean cuales sean las condiciones de uso: en la oficina, a distancia o en desplazamientos. La mejor garantía que podemos dar a nuestros clientes, aparte de que estas soluciones están certificadas por agencias de seguridad internacionales y cumplen la normativa vigente, es que las utilizamos a diario con total confianza para miles de empleados de ALE en todo el mundo.

Visite nuestro sitio web para obtener más información.

Alcatel·Lucent Enterprise