Protección de las soluciones de comunicaciones unificadas y colaboración

Lo que se necesita en el mundo cambiante de hoy

Documento técnico

Alcatel·Lucent Enterprise

Índice

- Mayor atención a la ciberseguridad
- Seis áreas clave para la ciberseguridad de extremo a extremo
- Alcanzar los objetivos empresariales con menos riesgos
- Ciberseguridad: integrada en la mentalidad de los proveedores tecnológicos

Mayor atención a la ciberseguridad

En el transcurso de los últimos años, casi todas las empresas y organizaciones gubernamentales han cambiado la forma en que sus empleados se comunican, colaboran y comparten información. Aunque el rápido cambio para apoyar a los empleados que trabajaban desde casa fue crucial para mantener la continuidad de la empresa durante la pandemia, tuvo un precio: el perímetro de la red se extiende ahora mucho más allá de los límites tradicionales de la oficina, aumentando significativamente la superficie de ataque de la organización.

Los riesgos asociados a los perímetros de red ampliados no van a desaparecer pronto. Según Gartner, el 39 % de los trabajadores del conocimiento de todo el mundo trabajarán en modelos híbridos remotos y presenciales a finales de 2023. En Estados Unidos, esa cifra asciende al 51 %[1].

Las perturbaciones geopolíticas han aumentado aún más los riesgos para la ciberseguridad. La Agencia de Ciberseguridad de la Unión Europea ha calificado la invasión rusa de Ucrania de "cambio de juego" para el ciberespacio mundial.[2] Según la Asociación de Empresas Ucranianas de Subcontratación de TI, una de cada cinco empresas de Fortune 500 confiaron en desarrolladores de software del país en 2022.[3]

Al mismo tiempo, el impacto social de los ciberataques es cada vez mayor. En 2022, asistimos a importantes ciberataques contra infraestructuras civiles críticas, que provocaron una emergencia nacional en Costa Rica,[4] y continuaron los ataques contra organizaciones sanitarias.[5]

Las organizaciones no pueden permitirse retrasar las mejoras de ciberseguridad

Se calcula que la ciberdelincuenciaha costado a la economía mundial 5,5 billones de euros en 2021, y se espera que los daños superen los 10 billones de euros en 2025.[6] El problema es tan grave que la Unión Europea está creando una Ley de Ciberresiliencia y ha publicado una versión 2 significativamente mejorada de su Directiva sobre Seguridad de las Redes y Sistemas de Información (SRI) para proteger a los consumidores y a las empresas que compran o utilizan productos o software con un componente digital.[7] Estados Unidos también está aplicando medidas para reforzar la ciberseguridad, entre ellas la Orden Ejecutiva 14028, que anima a los organismos a adoptar principios de ciberseguridad de confianza cero y ajustar las arquitecturas de red en consecuencia.[8]

A medida que las empresas y los gobiernos buscan la transformación digital y un apoyo más permanente a los modelos de trabajo flexibles, no tienen más remedio que reforzar la ciberseguridad. Las soluciones que sus equipos utilizan para comunicarse, colaborar y compartir información deben incorporar las mejores prácticas de ciberseguridaden todos los niveles y en todos los aspectos de la funcionalidad.

1 Gartner Forecasts 39% of Global Knowledge Workers Will Work Hybrid by the End of 2023. Gartner, marzo de 2023.
2 La volátil geopolítica sacude las tendencias del panorama de las amenazas a la ciberseguridad en 2022. Agencia de Ciberseguridad de la Unión Europea. Noviembre de 2022.
3 Una de cada cinco empresas de la lista Fortune 500 confiará en Ucrania para sus necesidades de desarrollo de software en 2022. Ukrainian Hi-Tech Initiative, Octubre de 2022.
4 Los 13 ciberataques más costosos de 2022: una mirada retrospectiva. Security Intelligence, diciembre de 2022.
5 Resumen de 2022: Un año lleno de acontecimientos en materia de ciberseguridad. Forbes, diciembre de 2022.
6 New European Union cybersecurity proposal takes aim at cybercrime. Foro Económico Mundial, septiembre de 2022.
7 Ley de Ciberresiliencia de la UE. Comisión Europea, septiembre de 2022.
8 Orden ejecutiva sobre la mejora de la ciberseguridad de la nación. Agencia de Ciberseguridad y Seguridad de la Infraestructura.

Seis áreas clave para la ciberseguridad integral

Las soluciones de comunicaciones unificadas y colaboración deben implementar la ciberseguridad de extremo a extremo porque es la única forma de garantizar que la seguridad se aplica de forma exhaustiva. Un enfoque integral de la ciberseguridad ayuda a empresas y gobiernos a:

- **Prevenir los ciberataques** implementando la ciberseguridad en cada aspecto del diseño del producto para reducir la superficie de ataque.
- **Protegerse contra los ciberataques** aplicando las últimas normas de seguridad y las mejores prácticas en todos los componentes de la solución para aumentar la resistencia.
- **Reaccionar ante los ciberataques** tomando medidas rápidas y adecuadas para limitar el impacto y mejorar la resistencia, en caso de que se produzca un ataque.

Para determinar si las soluciones de colaboración y comunicaciones unificadas implementan la ciberseguridad de extremo a extremo, deben realizarse evaluaciones de las soluciones en las áreas descritas a continuación. Centrarse en estas áreas puede ayudar a garantizar que las evaluaciones de las solucionessean exhaustivas y se centren en las principales vulnerabilidades del panorama de las ciberamenazas.

1 Seguridad en diseño

Históricamente, los diseños de soluciones principalmente se guiaban por la necesidad de nuevas funciones, y la seguridad era una consideración importante, pero secundaria. Con el panorama cambiante, las prioridades tradicionales de diseño se han invertido y ahora los diseños de soluciones deben guiarse por los requisitos de ciberseguridad.

Las soluciones de hardware y software seguras por diseño tienen en cuenta la seguridad en cada paso de la definición, el desarrollo y la entrega del producto. Todo el hardware y los sistemas operativos están reforzados, la protección contra la denegación de servicio (DoS) está integrada y las soluciones aplican las mejores prácticas de ciberseguridad más importantes para el sector. Por ejemplo, una solución de comunicaciones unificadas y colaboración para organizaciones de seguridad nacional cumplirá las muy altos normas de resistencia y confidencialidad que exigen estas organizaciones.

2 Seguridad con acceso a la red de confianza cero

Las estrategias de seguridad que ofrecen confianza en función de la ubicación del usuario dentro del cortafuegos de la empresa, las credenciales que introduce o la aplicación o el dispositivo que utiliza ya no son adecuadas, ni siquiera cuando se combinan varios mecanismos de seguridad. En la actualidad, ningún usuario, dispositivo o aplicación debe tener confianza implícita

Las soluciones de colaboración y comunicaciones unificadas que aplican un modelo de seguridad con acceso a la red de confianza cero (ZTNA) ayudan a las organizaciones a contrarrestar eficazmente las amenazas en constante evolución. ZTNA no proporciona confianza a ningún usuario, dispositivo o aplicación, independientemente de dónde se encuentre. Se basa en cinco afirmaciones clave:

- La red es hostil
- Las amenazas externas e internas están siempre presentes
- La ubicación no basta para determinar la confianza
- Todos los dispositivos, usuarios y flujos de red deben estar autenticados y autorizados
- Las políticas de seguridad y red deben ser dinámicas y utilizar tantas fuentes de datos como sea posible

3 Macro y microsegmentación

La macrosegmentación y la microsegmentación permiten un enfoque granular y altamente controlado de la ciberseguridad para todos los diferentes usuarios, dispositivos y aplicaciones que acceden a la red.

La macrosegmentación segrega a los usuarios, dispositivos y aplicaciones según su dominio funcional para que no puedan comunicarse con los elementos de otros macrosegmentos. Por ejemplo, las aplicaciones de comunicaciones unificadas y colaboración de un macrosegmento no pueden comunicarse con las tecnologías de seguridad, como cámaras de CCTV y sistemas de cierre de puertas, de otro macrosegmento, ni con los sensores y controles de iluminación, calefacción y aire acondicionado de un tercer macrosegmento.

La microsegmentación define el modo en que los usuarios, dispositivos y aplicaciones de un macrosegmento pueden interactuar entre sí, y suele regirse por políticas de seguridad muy específicas. Por ejemplo, no debe permitirse que una cámara de vigilancia interactúe con una cerradura de puerta, a pesar de que se encuentren en el mismo macrosegmento relacionado con la seguridad.

4 Cifrado de extremo a extremo nativo

En las organizaciones modernas, los empleados, clientes, socios y proveedores pueden encontrarse en cualquier parte del mundo. Y las soluciones que utilizan para comunicarse y colaborar pueden estar instaladas en el edificio desde el que trabajan, al otro lado de la ciudad, o en un centro de datos al otro lado del mundo. En todos los casos, las personas deben poder intercambiar información de forma segura y confidencial mediante voz, vídeo y texto.

Para garantizar que solo los participantes en la conversación puedan acceder a la información que se intercambia, cada conversación debe estar totalmente cifrada de origen a destino. Eso significa que todos los elementos de hardware y software que intervienen en las comunicaciones de extremo a extremo deben llevar incorporados de forma nativa mecanismos de cifrado aprobados por los organismos de seguridad.

5 Certificaciones y acreditaciones de seguridad y privacidad

Hace apenas unos años, las certificaciones y acreditaciones de seguridad más estrictas sólo se exigían para productos de seguridad, como cortafuegos, o en sectores concretos, como defensa. Hoy en día, las normas específicas de seguridad deben aplicarse a todos los productos tecnológicos, en todos los sectores.

Es extremadamente importante verificar que las afirmaciones sobre ciberseguridad están respaldadas por certificaciones y acreditaciones reconocidas. He aquí algunos ejemplos del cumplimiento que debe buscarse:

- **Normas mundiales de seguridad y privacidad**, como ISO 27001 para la seguridad de la información, ISO 27017 para entornos más seguros basados en la nube, ISO 27018 para la protección de la información de identificación personal en entornos basados en la nube, y Common Criteria Evaluation Assurance Level (EAL) 2 y superiores para la seguridad de los sistemas informáticos.
- **Normas de seguridad y privacidad específicas del sector**, como la ley Health Insurance Portability and Accountability Act (HIPAA) en EE. UU. y Hébergeurs de Données de Santé (HDS) para el alojamiento de datos sanitarios en Francia.
- **Normas regionales de seguridad y privacidad**, como el Reglamento General de Protección de Datos (RGPD) de la Unión Europea.

6 Pruebas de seguridad continuas y especializadas

Al igual que las normas de seguridad, los procesos especializados de pruebas de seguridad que antes se reservaban a los productos de seguridad son ahora obligatorios en las soluciones de comunicaciones unificadas y colaboración.

Las pruebas de penetración son un buen ejemplo. Estas pruebas simulan ciberataques para revelar vulnerabilidades de seguridad, de modo que puedan abordarse de forma proactiva antes de que surjan problemas. Para anticiparse a las ciberamenazas en un panorama en constante evolución, deben realizarse de forma continua pruebas de penetración basadas únicamente en los requisitos de ciberseguridad.

Los proveedores de tecnología que se dedican a ayudar a sus clientes a mantener la máxima ciberseguridad deben proporcionar los recursos, herramientas y conocimientos necesarios para realizar pruebas de penetración continuas.

Alcanzar los objetivos empresariales con menor riesgo

Las soluciones de comunicaciones unificadasy colaboración que implementan la gama completa de medidas de ciberseguridad descritas en la sección anterior ofrecen a las empresas y organizaciones gubernamentales la libertad y flexibilidad necesarias para impulsar sus actividades al tiempo que minimizan los riesgos y garantizan el cumplimiento de la normativa. Pueden:

- **Permitir a los empleados** colaborar y compartir información de forma segura y confidencial utilizando cualquier medio y dispositivo, desde cualquier lugar.
- **Mejorar la experiencia del cliente** con comunicaciones enriquecidas, informativas y atractivas, una toma de decisiones más rápida, procesos empresariales automatizados y la capacidad de detectar proactivamente los problemas antes de que afecten al cliente.
- **Aumentar la excelencia operativa y la agilidad** utilizando una infraestructura digital que se despliega donde tiene más sentido para su organización –en las instalaciones o en una nube híbrida, privada o pública– al tiempo que se adhiere a estrictas políticas de privacidad de datos y garantiza el cumplimiento de la normativa sobre privacidad de datos.

Los ejemplos que figuran a continuación son solo algunas de las posibilidades que se abren y pueden adaptarse fácilmente a otras necesidades y sectores.

Crear un lugar de trabajo flexible y digital para capacitar a los empleados

Con la combinación adecuada de comunicaciones seguras y soluciones de colaboración, los empleados pueden trabajar de forma más rápida y flexible, manteniendo al mismo tiempo el pleno cumplimiento de la normativa del sector.

- En el sector sanitario, **un personal con gran movilidad puede colaborar y compartir información mientras** sigue cumpliendo plenamente las normas de seguridad de los datos. El personal puede intercambiar fácilmente actualizaciones y obtener rápidamente la asistencia que necesita. El personal médico puede utilizar comunicaciones seguras y en tiempo real para mejorar los resultados de los pacientes y la eficacia del flujo de trabajo. El personal no médico puede acelerar los procesos y las respuestas a los problemas de mantenimiento que podrían afectar a la seguridad de los pacientes y el personal.
- **En educación**, los profesores pueden ofrecer experiencias de aprendizaje a distancia más ricas y atractivas, con más oportunidades para que los alumnos participen en actividades, colaboren en proyectos e interactúen utilizando su medio preferido. El control de acceso exhaustivo y las políticas automatizadas mantienen la integridad de los datos, y los análisis priorizan las comunicaciones críticas y los recursos de red.
- **En las organizaciones gubernamentales**, el personal puede intercambiar información de forma segura a través de equipos dispersos. Pueden compartir pantallas, controlar a distancia el escritorio de otra persona e intercambiar archivos de gran tamaño para mejorar la colaboración. Y pueden interactuar de forma segura con los ciudadanos a través de aplicaciones web o móviles mediante voz, vídeo, chat o mensajería instantánea.
- **En el transporte**, el lugar de trabajo digital permite a los empleados utilizar sus propios dispositivos mientras trabajan, introducir procesos más eficientes y ofrecer a los pasajeros servicios mejorados, como la posibilidad de trabajar mientras viajan. Los protocolos de comunicación seguros, las instalaciones reforzadas y el código diversificado protegen los datos en cualquier punto de la red.

Conectar todo para mejorar la experiencia del cliente

Conectar de forma segura personas, objetos y aplicaciones con comunicaciones en tiempo real permite a las empresas y organizaciones gubernamentales:

- Proporcionar a los empleados los dispositivos, las tecnologías y los datos que necesitan para atender mejor a los clientes, minimizando al mismo tiempo el riesgo de que un error humano o la falta de concienciación pongan en peligro la seguridad.
- Utilizar dispositivos integrados y seguros para comunicarse y colaborar con los clientes mientras se desplazan, con pleno acceso a las soluciones de gestión de las relaciones con los clientes (CRM).
- Aumentar la protección, el control y la visibilidad de una gama diversa y en rápido crecimiento de dispositivos del internet de las cosas (IoT).
- Mantener actualizados los sistemas de comunicación y colaboración para evitar el riesgo de que las aplicaciones obsoletas aumenten la superficie de ataque y expongan vulnerabilidades.
- Implantar controles de acceso eficaces y cifrado de extremo a extremo en todas las plataformas.

La gestión unificada de redes permite gestionar de forma holística todas las plataformas de comunicaciones, aplicaciones y dispositivos IoT. La gestión de red unificada:

- Simplifica las tareas de gestión en redes por cable e inalámbricas y dispositivos IoT para reducir los costes de gestión de red, optimizar el rendimiento de la red y aumentar la eficiencia operativa.
- Acelera la resolución de problemas en entornos tecnológicos cada vez más diversos para reducir el riesgo de interrupciones del servicio y el tiempo de inactividad.

La gestión unificada de redes en todos los sectores ofrece toda una serie de ventajas. Por ejemplo:

En la sanidad, las soluciones IoT pueden rastrear la ubicación de equipos críticos como tanques de oxígeno, carros de paradas, monitores de pacientes, postes de suero y sillas de ruedas para mejorar la seguridad y la eficiencia. Las conexiones entre personas, objetos y aplicaciones también pueden utilizarse para activar alarmas que avisen al personal médico de las necesidades de los pacientes o del mal funcionamiento de los equipos, y pueden alertar a todo el personal de las instalaciones sobre situaciones inseguras.

En educación, hay un nuevo potencial para conectar los dispositivos y aplicaciones del campus inteligente con múltiples capas de seguridad para proteger los activos de la institución de los dispositivos poco seguros que acceden a la red. Las instituciones educativas también pueden utilizar la huella digital de dispositivos IoT para identificar características de los dispositivos como el tipo, el fabricante, el modelo y el sistema operativo para simplificar y acelerar la configuración de la red de IoT y la incorporación de dispositivos.

Aumentar la excelencia y agilidad operativa

Con la flexibilidad para implementar de forma segura soluciones de comunicaciones unificadas y colaboración en las instalaciones o en una nube híbrida, privada o pública, las empresas y las organizaciones gubernamentales pueden beneficiarse de las tecnologías digitales de la forma que mejor se adapte a sus objetivos y mandato. Cada organización puede alcanzar nuevos niveles de excelencia operativa al tiempo que cumple los requisitos específicos del sector mediante la adopción de modelos de nube para mejoras operativas y de agilidad como en:

- **Sanidad**, donde las historias clínicas digitales pueden utilizarse para mejorar la atención al paciente y aumentar la eficiencia con plena confianza en que la información personal se almacena en un centro de datos seguro y certificado en la nube.
- **Educación**, donde el profesorado, el personal y los estudiantes disponen de un acceso seguro y respetuoso con la privacidad a aplicaciones y servicios basados en la nube desde cualquier lugar. Y los departamentos de TI pueden reducir el tiempo y los costes asociados a la implantación, el soporte y la actualización de la amplia variedad de aplicaciones.
- **Gobierno**, donde las comunicaciones confidenciales se pueden ofrecer con alta disponibilidad y protegidas con mecanismos DoS incorporados y hardware y sistemas operativos de seguridad reforzada.
- **Transporte**, donde la alteración de las capacidades de comunicación puede crear situaciones peligrosas, lo que hace esenciales las soluciones soberanas de datos resilientes.

Ciberseguridad: integrada en la mentalidad de los proveedores tecnológicos

Aunque muchos proveedores de tecnología hacen hincapié en la ciberseguridad, no todos cuentan con los conocimientos exhaustivos necesarios para implantar la seguridad de extremo a extremo.

Alcatel-Lucent Enterprise va más allá que otros proveedores a la hora de implantar todas las mejores prácticas necesarias para la ciberseguridad de extremo a extremo. Nosotros:

- Seguimos las mejores prácticas y recomendaciones del Instituto Nacional de Ciencia y Tecnología (NIST) a la hora de realizar evaluaciones de riesgos sobre nuevas funciones y de implantar funciones de ciberseguridad, como el cifrado nativo, en nuestras soluciones.
- Contamos con el Certificado Common Criteria EAL2
- Aplicamos las normas ISO 27001 a todas nuestras soluciones basadas en la nube
- Admitimos ZTNA, segmentación granular de la red y políticas de seguridad muy específicas para reducir el riesgo de actividades no autorizadas.
- Ejecutamos pruebas específicas de seguridad altamente especializadas, como pruebas de penetración, en todos nuestros productos.
- Garantizamos que nuestros productos obtienen las certificaciones clave del sector, como HDS, HIPAA y la Ley de Derechos Educativos y Privacidad Familia (FERPA) como Rainbow by Alcatel-Lucent Enterprise.

Como expertos reconocidos en ciberseguridad, contribuimos a las propuestas de directivas sobre ciberseguridad de la Unión Europea. También aprovechamos nuestra experiencia para ayudar a nuestros clientes a elegir e implantar la combinación adecuada de soluciones de colaboración y comunicaciones unificadas seguras para sus necesidades y formar a sus empleados en las mejores prácticas de ciberseguridad.

Alcatel-Lucent Enterprise goza de confianza en todo el mundo

Las principales organizaciones de todos los sectores confían en nuestras soluciones de comunicaciones seguras para la era digital para alcanzar sus objetivos, entre ellos:

- Metrópolis y ciudad de Perpiñán en Francia, donde los funcionarios del gobierno están implementando un plan estratégico de transición digital que incluye videoconferencias y comunicaciones de voz para los empleados, soporte para aplicaciones IoT y nuevos contenidos y servicios para los residentes, turistas y empleados municipales de Perpiñán.
- Newman University en EE. UU., una universidad católica de artes liberales que ha dotado al personal de funciones de telefonía móvil que no requieren números de teléfono directos y al equipo informático de una plataforma única, intuitiva y basada en la nube para gestionar, aprovisionar y supervisar toda la infraestructura de red.
- Kingsway Hospitals en la India, que ha implantado soluciones de infraestructura de comunicaciones en tiempo real que mantienen conectados al personal clínico y administrativo para que puedan optimizar la prestación de cuidados y mejorar la experiencia del paciente.
- Grupo J. Malucelli en Brasil, que ha modernizado su red con una solución convergente de voz y datos que incluye telefonía en la nube, así como redes LAN y Wi-Fi con gestión en la nube para simplificar y reducir el coste de las comunicaciones de varias de las empresas del grupo.

Más información

Si desea saber cómo podemos ayudar a su organización a sacar el máximo partido de las soluciones de comunicaciones seguras de la era digital, visite nuestro sitio web o póngase en contacto con nosotros hoy mismo .

© 2024 ALE International, ALE USA Inc. Todos los derechos reservados en todos los países. El nombre y el logotipo Alcatel-Lucent son marcas registradas de Nokia que se usan bajo licencia por ALE. Para saber de otras marcas con titularidad exclusiva de ALE, visite www.al-enterprise.com/es-es/legal/marcas-comerciales-copyright. DID23042401ES (Agosto 2024)

Alcatel·Lucent Enterprise