Ciberseguridad integral en el campus

En esta era de la confianza cero, se necesita una estrategia de ciberseguridad integral para impedir que usuarios, dispositivos y aplicaciones no autorizados accedan a la red.

Cinco pasos para proteger su campus

Las estrategias de seguridad tradicionales ya no bastan para ahuyentar a los actores maliciosos. A continuación se describen cinco pasos para implementar una estrategia de **acceso a la red de confianza cero (ZTNA)** que ofrezca la cobertura de "desconfianza" que necesita.

1. **Supervisar.** Cree un inventario de todos los dispositivos y aplicaciones —autorizados y no autorizados— que solicitan o proporcionan información en la red, así como los protocolos que utilizan.
2. **Evaluar y validar el inventario.** Evalúe los dispositivos y aplicaciones por tipo y función. Esto detecta los dispositivos de TI en la sombra que pueden eliminarse para reducir inmediatamente la superficie de ataque.
3. **Planificar el enfoque de la autenticación, la auditoría de autorizaciones y la administración.** Elabore un plan multidimensional que incluya la macrosegmentación y la microsegmentación.
4. **Simular.** Pruebe y valide el enfoque desarrollado en el paso 3. Utilice los conocimientos obtenidos para ajustar las políticas de seguridad.
5. **Hacer cumplir** El cumplimiento de las políticas de seguridad se puede garantizar en el perímetro de la red, donde los usuarios, dispositivos y aplicaciones intentan acceder a esta.

Riesgos, normas y recompensas

Al embarcarse en su viaje ZTNA es importante tener en cuenta los **riesgos**, **normas** y **recompensas**.

Riesgos:

- Los dispositivos no autorizados y no gestionados por TI pueden causar estragos
- Las políticas de seguridad incoherentes producen debilidad.
- Las redes con segmentación de seguridad estática y confianza implícita permiten que usuarios, dispositivos y aplicaciones previamente fiables queden sin control

Normas:

- La normativa estadounidense incluye la Ley de Derechos Educativos y Privacidad Familiar (FERPA) y la Ley de Portabilidad y Responsabilidad de Seguros de Salud (HIPAA)
- El Reglamento General de Protección de Datos de la UE (RGPD) se aplica a todas las instituciones con matriculaciones de estudiantes de la UE, independientemente de la ubicación de la institución

Recompensas:

- **Amplia protección:** autentique cada conexión y asigne permisos a cada usuario y dispositivo con listas de control de acceso a la red y acceso basado en funciones
- **Reducción del riesgo de propagación de ataques:** proporcione un control granular microsegmentando el tráfico de usuarios dentro de un macrosegmento
- **Mejora de la reputación:** las buenas prácticas con procesos diligentes pueden potenciar la marca y la imagen pública de las instituciones
- **Mejores resultados académicos:** las tecnologías digitales innovadoras mejoran las oportunidades de aprendizaje y el éxito académico
- **Mayor eficacia de las TI:** garantice el uso adecuado de los recursos de red y tome decisiones fundamentadas acerca de nuevas estrategias tecnológicas
- **Beneficios económicos:** reduce el riesgo de que se requieran costosas medidas de mitigación en respuesta a los ciberataques

Su partner en ciberseguridad

Un partner con experiencia puede aportar conocimientos y soluciones de ciberseguridad de eficacia probada. Trabajamos con usted para ofrecerle soluciones de red seguras adaptadas a su estrategia.

Seguridad certificada:

Las soluciones de red de ALE cumplen las principales normas de seguridad, como las siguientes:

- Directrices y especificaciones internacionales de criterios comunes para la seguridad de TI
- Pruebas de conformidad del Joint Interoperability Test Command (JITC) de EE. UU.
- Federal Information Processing Standard (FIPS) 140-2 de EE. UU.

Las soluciones de ALE amplían las inversiones de nuestros clientes al integrarse con cortafuegos de Palo Alto Networks y Fortinet.

Experiencia certificada:

Somos un partner de confianza en ciberseguridad de instituciones de todo el mundo, entre las que se incluyen:

- California State University en los EE. UU., nuestras soluciones ponen en marcha una **red fiable y flexible** con mayor seguridad, Wi-Fi en todas partes y servicios en la nube abiertos y compartidos
- Centro Paula Souza en Brasil, nuestras soluciones proporcionan la **seguridad, alta velocidad y rendimiento** que los usuarios necesitan
- Linköping University de Suecia, nuestras soluciones ofrecen un acceso **resistente** y **seguro a la red** para estudiantes, profesores, invitados, partners externos, inquilinos de edificios universitarios y proveedores de servicios

Descubra cómo podemos ayudar para que su institución académica se centre exclusivamente en la enseñanza y el aprendizaje mientras nosotros nos centramos en proteger su red.

www.al-enterprise.com/es-es El nombre y el logotipo Alcatel-Lucent son marcas registradas de Nokia que se usan bajo licencia por Alcatel-Lucent Enterprise. Para obtener información sobre las marcas de Nokia, consulte la lista de marcas registradas de Nokia en nokia.com/terms-conditions/en. Todas las demás marcas comerciales son propiedad de sus respectivos propietarios. La información técnica de puede modificar sin previo aviso. ALE Holding no asume ninguna responsabilidad por los posibles inexactitudes del contenido. © 2023 ALE International. Todos los derechos reservados. DED20230502[01] (junio de 2023).