Ciberseguridad para enseñanza y aprendizaje de categoría mundial

Documento técnico

Alcatel·Lucent Enterprise

Índice

Un sector asediado

En los últimos años, el número y la complejidad de los ciberataques a instituciones académicas de todo el mundo han aumentado a un ritmo alarmante. Algunos informes han revelado que el sector educativo se encuentra en medio de una crisis cibernética, señalando que el reciente cambio al aprendizaje virtual basado en la nube ha dado a los piratas informáticos nuevas oportunidades que explotar.[1]

Por desgracia, este tipo de afirmaciones atrevidas se basan en estadísticas del mundo real. Entre agosto y septiembre de 2021, las organizaciones educativas fueron objeto de más de 5,8 millones de ataques de malware en todo el mundo, esto es, el 63 % de todos los ataques de este tipo.[2] Los datos publicados en 2022 confirman que la educación y la investigación siguen siendo los sectores más atacados. El informe identifica a Australia/Nueva Zelanda como la región más atacada, seguida de Asia y Europa, siendo Latinoamérica la que experimenta el mayor aumento de ciberataques semanales.[3]

Los ciberataques a instituciones académicas se han vuelto tan frecuentes que varias agencias estadounidenses, entre ellas el FBI y la Agencia de Ciberseguridad y Seguridad de Infraestructuras (CISA), unieron sus fuerzas en 2022 para emitir un aviso, advirtiendo a las instituciones educativas de que están siendo blanco desproporcionado de ataques de ransomware.[4]

El aumento del alcance y la escala de los ciberataques y, especialmente de los ataques de ransomware, están teniendo graves repercusiones en las instituciones de todo el mundo. Los estudiantes y el profesorado pierden tiempo de clase e información valiosos, lo que pone en peligro los objetivos educativos.

Tenga en cuenta lo siguiente:

- En septiembre de 2022, un ataque de ransomware al Distrito Escolar Unificado de Los Ángeles (LAUSD) provocó un cierre sin precedentes de los sistemas informáticos que se tradujo en continuas interrupciones del correo electrónico, los sistemas informáticos y las aplicaciones.[5]
- En 2021, un ciberataque en el Reino Unido interrumpió las comunicaciones por correo electrónico, teléfono y página web en 15 centros educativos, paralizando el aprendizaje en línea.[6]
- También en 2021, un ciberataque a gran escala contra la Universidad El Bosque de Bogotá (Colombia) afectó a plataformas institucionales, académicas y financieras durante tres días.[7]

Los ciberataques también dañan la reputación y la confianza de las instituciones, lo que puede derivar en una disminución de las matriculaciones y una pérdida de ingresos. En mayo de 2022, el Lincoln College de Illinois, con 157 años de antigüedad, cerró permanentemente después de que un ataque de ransomware creara un debilitante desafío financiero.[8]

1 America's Schools Face Mounting Threats from Cyberattacks. RealClear Education, mayo de 2022.
2 America's Schools Face Mounting Threats from Cyberattacks. RealClear Education, mayo de 2022.
3 Education sector seeing highest volumes of cyber attacks. SecurityBrief New Zealand, agosto de 2022.
4 Alert AA22-249A: #StopRansomware: Vice Society. CISA, septiembre de 2022.
5 Los Angeles school district warns of disruption as it battles ongoing ransomware attack. TechCrunch+, septiembre de 2022.
6 Cyberattack shuts down online learning at 15 UK schools. zdnet.com, marzo de 2021.
7 The Universidad El Bosque has regained control of its digital platforms. NewsBeezer.com, julio de 2021.
8 Ransomware attack shutters 157-year-old Lincoln College. CBS News, mayo de 2022.

Pensar con originalidad

Lamentablemente, los ciberataques a instituciones académicas se producen incluso cuando se aplican enfoques tradicionales de ciberseguridad. En 2019, el Centro Nacional de Ciberseguridad del Reino Unido descubrió que el 83 % de los 432 centros educativos analizados había sufrido al menos un ataque de ciberseguridad, a pesar de que el 98 % contaba con soluciones antivirus y el 99 % con un cortafuegos.

Para prevenir con mayor eficacia los ciberataques, las instituciones académicas deben alejarse de los enfoques tradicionales de la ciberseguridad. Mientras que enfoques tales como el castillo y el foso y la seguridad de defensa en profundidad eran eficaces en tiempos más sencillos, ya no proporcionan una protección adecuada. En una era en la que predominan Internet y los dispositivos portátiles, el perímetro de la red y la posibilidad de que se produzcan accesos no autorizados a la red puede extenderse ahora mucho más allá del perímetro físico del campus.

Ningún usuario, dispositivo o aplicación debe tener confianza implícita

Actualmente, la única estrategia de ciberseguridad de la red que puede contrarrestar eficazmente las amenazas es una que no proporciona confianza a ningún usuario, dispositivo o aplicación, independientemente de dónde se encuentre: en el campus, en la nube o fuera del campus. Esta estrategia se conoce como acceso a la red de confianza cero (ZTNA), y 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 deben ser dinámicas y utilizar tantas fuentes de datos como sea posible

Con el enfoque adecuado para implantar la seguridad de ZTNA, las instituciones pueden centrarse principalmente en la enseñanza y el aprendizaje, en lugar de en las tecnologías y las amenazas.

De aquí a la confianza cero

A medida que las instituciones desarrollan su estrategia de ciberseguridad de ZTNA, es importante recordar que evolucionar hacia la confianza cero es un proceso. No ocurre de la noche a la mañana. No existe una solución de confianza cero o un conjunto de soluciones que puedan adquirirse e implantarse sin más. Lleva tiempo implantar un entorno completo de confianza cero en todas las tecnologías.

También es importante que las instituciones académicas desarrollen y mantengan un enfoque equilibrado de la ciberseguridad. Si los mecanismos de seguridad implantados son demasiado rígidos o limitados, la gente buscará formas de eludir los mismos procedimientos que pretenden proteger sus dispositivos, datos y aplicaciones. Tendrán la tentación de añadir sus propios puntos de acceso, dispositivos y aplicaciones no autorizados para evitar las largas comprobaciones de ciberseguridad y las actualizaciones de software, y así poder realizar sus tareas más rápidamente. Es una táctica conocida como "TI en la sombra" y conlleva numerosos riesgos de ciberseguridad.

Además, cada institución tendrá que identificar y revisar las normas de privacidad que deben cumplirse para los datos que viajan por la red, así como las listas de control de acceso (ACL) y las políticas de cortafuegos para los datos que se almacenan en la nube.

Al revisar los requisitos normativos, es importante tener en cuenta las normativas nacionales e internacionales sobre privacidad. Por ejemplo, en EE. UU., las instituciones académicas deben cumplir la Ley de Derechos Educativos y Privacidad Familiar (FERPA) y la Ley de Portabilidad y Responsabilidad de Seguros de Salud (HIPAA). Pero también deben recordar que el Reglamento General de Protección de Datos (RGPD) de la Unión Europea (UE) se aplica a todas las instituciones cuya matriculación incluya estudiantes de la UE, independientemente de su ubicación.

Familiarícese con sus ciberriesgos y requisitos normativos

Antes de empezar a desarrollar una estrategia de ZTNA, debe evaluar a fondo los riesgos a los que se enfrenta la institución en la actualidad y valorar su gravedad. A la hora de preparar la evaluación de riesgos, tenga en cuenta los siguientes errores comunes:

- Dispositivos IoT no gestionados por TI. Estos dispositivos "fraudulentos" a menudo no cumplen las políticas de seguridad, ejecutan firmware obsoleto y carecen de protección antivirus, lo que aumenta sus posibilidades de ser utilizados por un malhechor como punto de entrada para un ataque.
- Equipos y dispositivos personales no autorizados que acceden a la red. Estos dispositivos informáticos en la sombra podrían ejecutar cualquier software y estar ya infectados con virus y malware listos para atacar la red.
- Políticas de seguridad incoherentes. Estas incoherencias introducen puntos débiles en la protección de redes que pueden ser objetivo de partes que no sean de confianza.
- Redes con segmentación de seguridad estática y confianza implícita. Estos enfoques tradicionales de la ciberseguridad permiten a los usuarios, dispositivos y aplicaciones, que inicialmente eran de confianza, atacar la red sin más comprobaciones para verificar que siguen siendo de confianza. También asumen que los ciberataques no pueden originarse desde dentro, lo que es incorrecto.

Una metodología en cinco pasos para la ciberseguridad de ZTNA

Los cinco pasos siguientes son fundamentales a la hora de desarrollar una estrategia de ciberseguridad de ZTNA. Estos pasos ayudan a garantizar que la red dispone de un conjunto completo de mecanismos de protección para impedir que usuarios, dispositivos y aplicaciones no autorizados accedan a la red.

- **Paso 1: supervisar.** Supervisar la red activa para crear un inventario de todos los dispositivos y aplicaciones, autorizados y no autorizados, que solicitan o entregan información en la red y los protocolos que utilizan para ello. Hay muchas herramientas disponibles que pueden recopilar esta información de la red y crear un informe de inventario que clasifica los dispositivos por tipo, fabricante, modelo, sistema operativo y otros factores. También existen herramientas de supervisión de flujos que identifican los distintos flujos de tráfico de aplicaciones en la red.
- **Paso 2: evaluar y validar su inventario.** Empiece por evaluar los dispositivos y aplicaciones por su tipo y función. Por ejemplo, ¿el dispositivo/aplicación se utiliza con fines educativos o de IoT? ¿Está relacionado con objetivos empresariales, sociales, académicos o de investigación? ¿Contribuye a mejorar la eficacia, la seguridad o la privacidad? ¿Es necesario para cumplir la normativa? Este proceso ayuda a identificar los dispositivos de TI en la sombra que pueden eliminarse para reducir inmediatamente la superficie de ataque.
- **Paso 3: planificar su enfoque de la autenticación, la auditoría de autorizaciones y la administración.** Para obtener los mejores resultados, elabore un plan multidimensional que incluya la macrosegmentación y la microsegmentación. La macrosegmentación utiliza LAN virtuales (VLAN), enrutamiento virtual y reenvío (VRF), redes privadas virtuales (VPN), así como otros enfoques para segregar usuarios, dispositivos y aplicaciones en la red. La microsegmentación define cómo se asignan esos usuarios, dispositivos y aplicaciones a su segmento de red y a las políticas de seguridad.
- **Paso 4: simular.** Pruebe y valide el enfoque desarrollado en el paso 3 y, a continuación, utilice los conocimientos obtenidos para ajustar las políticas de seguridad y asegurarse de que cubren todos los escenarios. Durante esta fase es importante probar todos los aspectos del enfoque. Por ejemplo, asegúrese de que las simulaciones incluyen la emisión de certificados, la configuración de políticas, la configuración de escenarios de cuarentena, la simulación de flujos de registro y las pruebas de integración de cortafuegos.
- **Paso 5: aplicar.** Una vez se han completado y ajustado las políticas de seguridad, pueden aplicarse en el perímetro de la red, donde los usuarios, dispositivos y aplicaciones intentan acceder a ella. Cuando se aplican políticas de seguridad probadas y validadas, se bloquea el acceso a la red de dispositivos no autorizados y se interrumpen los flujos inesperados. Además, los dispositivos pueden ponerse en cuarentena y se puede alertar de la situación a los equipos de TI. Estos mecanismos funcionan como una serie de puntos de control que impiden a los conductores peligrosos acceder a una autopista.

Aunque seguir este proceso de cinco pasos ayuda a las instituciones a evolucionar hacia la ciberseguridad de ZTNA, no es suficiente por sí solo. Para tener éxito, toda estrategia de ciberseguridad de ZTNA debe ir acompañada de un enfoque exhaustivo de la formación, la gestión de parches y una enérgica gestión de TI en la sombra.

Más que la suma de sus partes

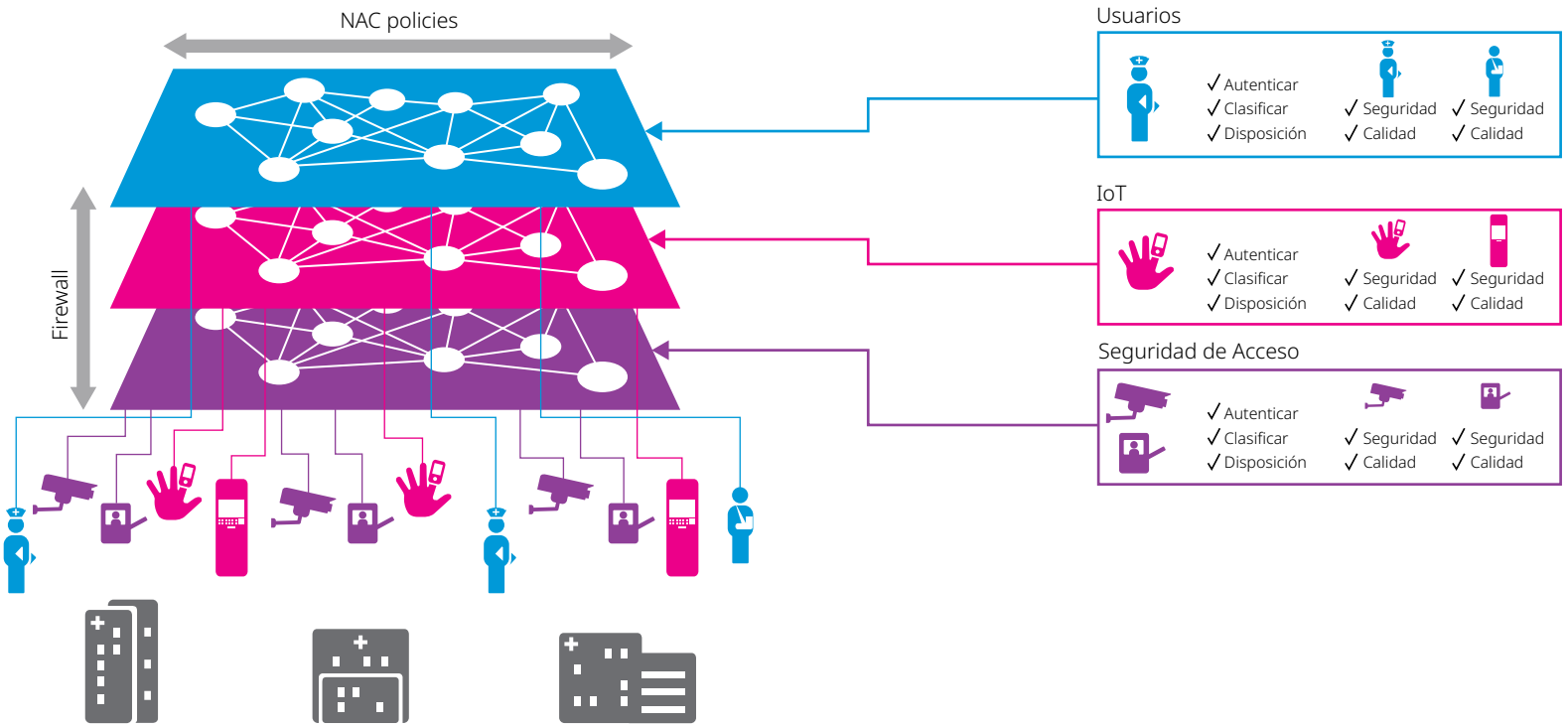
Seguir el enfoque paso a paso de la ciberseguridad de ZTNA permite a las instituciones académicas obtener importantes beneficios en todos los aspectos de sus operaciones. Aunque las ventajas más evidentes están relacionadas con la prevención y detección de accesos no autorizados a la red, también existen numerosas ventajas educativas y empresariales.

Protección expansiva

Desde el punto de vista tecnológico, las listas completas de control de acceso a la red y el control de acceso basado en funciones permiten autenticar todas las conexiones y asignar permisos a cada usuario y dispositivo que accede a la red. Como resultado, las instituciones obtienen un nivel granular de protección que hace mucho más difícil que los usuarios y dispositivos fraudulentos accedan a los recursos y datos de la red.

La capacidad de utilizar la microsegmentación para segmentar aún más el tráfico de usuarios dentro de un macrosegmento también permite un control más granular del acceso de usuarios y dispositivos para, así, reducir el riesgo de prorrogación de ataques dentro de la red. Con la microsegmentación, el tráfico de usuarios dentro de un macrosegmento, como una VLAN, puede separarse en función de factores como la hora del día, la ubicación del acceso, si el usuario es estudiante, profesor o personal administrativo, y otros controles de acceso (figura 1). La misma política de seguridad sigue a la persona esté donde esté, lo que permite a la institución aplicar un enfoque más unificado de la ciberseguridad.

Figura 1. La combinación de macrosegmentación y microsegmentación refuerza los controles de acceso a la red



Cosechar los frutos

Las instituciones académicas que se dan a conocer por su dedicación y diligencia a la hora de proteger escrupulosamente la seguridad y privacidad de la información de sus redes pueden mejorar su reputación, marca educativa e imagen pública. Su capacidad para protegerse de los ciberataques y evitar la publicidad negativa que inevitablemente acompaña a estos sucesos ayuda a atraer y retener a los estudiantes para reforzar el éxito a largo plazo. También permite que las instituciones académicas sean consideradas ejemplos de buenas prácticas en materia de ciberseguridad que otras instituciones pueden emular, contribuyendo así a reforzar las defensas contra los ciberataques dirigidos a las redes educativas de todo el mundo.

Una estrategia de ciberseguridad de ZTNA también contribuye a mejorar los resultados académicos. Con una red más segura, el profesorado y los estudiantes pueden aprovechar con confianza las innovadoras tecnologías digitales que mejoran las oportunidades de aprendizaje y el éxito de los estudiantes. Por ejemplo:

- El profesorado puede desarrollar e impartir lecciones más creativas, atractivas e interactivas que inspiren a los estudiantes, los expongan a innovaciones de vanguardia y los animen a participar activamente en los debates y actividades de clase, ya sea en el aula o a distancia.
- Los estudiantes pueden experimentar con las nuevas tecnologías, colaborar abiertamente entre sí y con el profesorado desde cualquier lugar, e incorporar las últimas innovaciones digitales a sus tareas para demostrar su potencial.

La base de la red de confianza garantiza que cada institución se centre en la enseñanza y el aprendizaje.

Los equipos de TI del sector educativo también se benefician de una estrategia de ciberseguridad de ZTNA. Al contar con un conocimiento más profundo del estado de la ciberseguridad de la institución académica, los equipos de TI pueden tomar decisiones más informadas sobre nuevas estrategias tecnológicas, como la adopción de un enfoque orientado a la nube o la compatibilidad con BYOD. Al mismo tiempo, pueden proteger y controlar mejor la infraestructura digital del campus y garantizar el uso adecuado de los valiosos recursos y el ancho de banda de la red.

Por último, pero no por ello menos importante, limitar la superficie de ataque de la institución tiene beneficios financieros potenciales, pues reduce el riesgo de que se requieran costosas medidas de mitigación en respuesta a los ciberataques.

Un Partner experto para una seguridad experta

Las instituciones académicas que implanten una estrategia de ciberseguridad de ZTNA necesitarán trabajar con un Partner experimentado que pueda proporcionar una visión y orientación expertas, así como soluciones de red de ZTNA de eficacia probada.

Alcatel-Lucent Enterprise cuenta con una amplia experiencia ayudando a instituciones académicas a avanzar globalmente hacia la ciberseguridad de ZTNA. Entendemos los pasos que deben dar estas instituciones para implantar una estrategia de ZTNA, y trabajamos con usted para proporcionar las soluciones de red seguras que se ajusten a su estrategia. A continuación, su institución puede aplicar un enfoque por capas a la seguridad de la red, para aprovechar mejor los mecanismos clave de ciberseguridad, como la microsegmentación y el control de acceso basado en funciones.

Seguridad integral

Las soluciones de red de ALE están certificadas para cumplir las principales normas de seguridad, incluyendo:

- 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.

La estrecha integración entre los cortafuegos y la infraestructura de red ayuda a las instituciones a localizar con precisión el origen de las actividades no autorizadas y maliciosas, y a poner en cuarentena los dispositivos infractores. Nuestras soluciones amplían las inversiones de nuestros clientes al integrarse con cortafuegos de Palo Alto Networks y Fortinet.

Amplia experiencia

Somos el Partner de confianza de instituciones académicas de todo el mundo que trabajan para mejorar su situación de ciberseguridad:

- En Universidad Estatal de California de EE. UU., nuestras soluciones de redes y de gestión de redes han creado una red fiable y flexible que proporciona una mayor seguridad, Wi-Fi en todas partes y servicios en la nube abiertos y compartidos para mejorar la experiencia global en el campus. La red, altamente fiable, proporciona soporte seguro a más de 500 000 usuarios en los más de 20 campus de la universidad y ha contribuido a ahorrar más de 100 millones de dólares en costes de infraestructura.
- En el Centro Paula Souza de Brasil, nuestras soluciones de red inteligentes y seguras proporcionan las altas velocidades y el rendimiento que los usuarios necesitan para trabajar mejor y más rápido. La autenticación unificada proporciona una experiencia de seguridad fácil de usar para empleados y visitantes. La tecnología de contención IoT permite que los dispositivos se conecten a la red de forma segura y controlada. Además, el personal de TI tiene visibilidad total de las operaciones de red y de las políticas unificadas de uso de la red.
- En la Linköping University de Suecia, nuestras soluciones de red ofrecen un acceso resistente y seguro a la red para estudiantes y profesores, así como para invitados, Partners externos, inquilinos de edificios universitarios y proveedores de servicios. Dado que las arquitecturas de red física y lógica están completamente separadas, los estudiantes y el profesorado pueden conectarse de forma automática y segura a su segmento de red asignado desde cualquier lugar y con cualquier dispositivo.

Más información

Para saber cómo podemos ayudar a su institución académica a evolucionar hacia una estrategia de ciberseguridad de acceso a la red de confianza cero, consulte nuestro sitio web o bien póngase en contacto con nosotros hoy mismo para hablar de sus necesidades específicas.

Alcatel·Lucent
Enterprise