Erstklassige Bildung dank Cybersicherheit

Whitepaper

Alcatel·Lucent Enterprise

Inhalt

Ein Sektor unter Beschuss

In den letzten Jahren haben die Zahl und die Raffinesse von Cyberangriffen auf akademische Einrichtungen rund um den Globus in alarmierendem Maße zugenommen. Einigen Berichten zufolge befindet sich der Bildungssektor mitten in einer Cyberkrise, da die jüngste Umstellung auf cloudbasierten virtuellen Unterricht Hackern neue Möglichkeiten eröffnet.[1]

Leider beruhen solche markigen Aussagen auf realen Statistiken. Zwischen August und September 2021 waren Bildungseinrichtungen das Ziel von mehr als 5,8 Millionen Malware-Angriffen weltweit, das entspricht 63 Prozent aller derartigen Angriffe.[2] Die im Jahr 2022 veröffentlichten Daten bestätigen, dass Bildung und Forschung nach wie vor die am stärksten angegriffenen Bereiche sind. Dem Bericht zufolge finden die meisten Angriffe in Australien/Neuseeland statt, gefolgt von Asien und Europa. Lateinamerika hat allerdings den größten Anstieg der wöchentlichen Cyberangriffe zu verzeichnen.[3]

Cyberangriffe auf akademische Einrichtungen sind so häufig geworden, dass sich mehrere US-Behörden, darunter das FBI und die Cybersecurity and Infrastructure Security Agency (CISA), im Jahr 2022 zusammengeschlossen haben, um eine entsprechende Empfehlung herauszugeben. Darin warnen sie Bildungseinrichtungen davor, dass sie unverhältnismäßig häufig Ziel von Ransomware-Angriffen sind.[4]

Die zunehmende Reichweite und das Ausmaß von Cyberangriffen, insbesondere von Ransomware-Angriffen, haben schwerwiegende Auswirkungen auf Institute weltweit. Schüler, Studenten und Lehrkräfte verlieren wertvolle Unterrichtszeit und Informationen, wodurch ihre Lernziele gefährdet sind.

Nachfolgend einige Beispiele aus der Vergangenheit:

- Ein Ransomware-Angriff auf den Los Angeles Unified School District (LAUSD) im September 2022 führte zu einer beispiellosen Abschaltung von Computersystemen. Dadurch kam es zu anhaltenden Unterbrechungen von E-Mails, Computersystemen und Anwendungen.[5]
- Ein Cyberangriff im Vereinigten Königreich im Jahr 2021 legte die E-Mail-, Telefon- und Website-Kommunikation an 15 Schulen lahm und brachte den Online-Unterricht zum Erliegen.[6]
- Ein groß angelegter Cyberangriff auf die Universidad El Bosque in Bogotá, Kolumbien, im Jahr 2021 gefährdete drei Tage lang institutionelle, akademische und finanzielle Plattformen.[7]

Cyberangriffe schädigen zudem den Ruf und die Vertrauenswürdigkeit der Einrichtungen. Dies kann geringere Anmeldezahlen und Einnahmeverluste zur Folge haben. Im Mai 2022 schloss das 157 Jahre alte Lincoln College in Illinois endgültig seine Tore, nachdem ein Ransomware-Angriff zu großen finanziellen Problemen geführt hatte.[8]

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

Blick über den Tellerrand hinaus

Leider finden Cyberangriffe auf akademische Einrichtungen auch dann statt, wenn traditionelle Konzepte für Cybersicherheit vorhanden sind. Im Jahr 2019 stellte das National Cyber Security Centre im Vereinigten Königreich fest, dass 83 Prozent der 432 untersuchten Schulen von mindestens einem Cybersecurity-Ereignis betroffen waren, obwohl 98 Prozent über Virenschutzlösungen und 99 Prozent über eine Firewall verfügten.

Um Cyberangriffe wirksamer zu verhindern, müssen sich akademische Einrichtungen von traditionellen Ansätzen der Cybersicherheit lösen. Strategien wie das „Burg- und Burggraben"-Modell und „Defense-in-Depth"-Sicherheit mögen in alten Zeiten ausgereicht haben. Heutzutage bieten sie jedoch keinen ausreichenden Schutz mehr. In einer Zeit, in der das Internet und Handheld-Geräte dominieren, kann sich der Netzwerkrand – und die Gefahr eines unbefugten Netzwerkzugriffs – nun weit über die physische Campusgrenze hinaus erstrecken.

Kein Nutzer, kein Gerät und keine Anwendung sollte automatisch Vertrauen genießen

Die einzige Strategie für die Cybersicherheit in Netzwerken, die heute wirksam gegen Bedrohungen vorgehen kann, ist eine, die keinem Nutzer, keinem Gerät und keiner Anwendung Vertrauen entgegenbringt. Dabei darf es keine Rolle spielen, wo diese sich befinden: Diese Strategie wird als Zero Trust Network Access (ZTNA) bezeichnet und basiert auf fünf Kernthesen:

- Das Netzwerk ist feindlich
- Externe und interne Bedrohungen lauern überall
- Der Standort alleine ist nicht genug, um Vertrauen zu schaffen
- Ausnahmslos alle Geräte, Nutzer und Netzwerkflüsse müssen authentifiziert und autorisiert werden
- Richtlinien müssen dynamisch sein und so viele Datenquellen wie möglich nutzen

Mit der richtigen Herangehensweise an die Implementierung der ZTNA-Sicherheit können sich die Institute weiterhin voll und ganz auf ihren Bildungsauftrag konzentrieren und müssen sich nicht mit Technologien und Bedrohungen herumschlagen.

Der Weg zu Zero Trust

Bei der Ausarbeitung einer ZTNA-Cybersicherheitsstrategie müssen die Institute sich vor Augen halten, dass die Entwicklung hin zu Zero Trust eine längere Reise ist. Das geschieht nicht über Nacht. Es gibt keine „Zero Trust"-Lösungen oder -Lösungspakete, die einfach gekauft und implementiert werden können. Es braucht Zeit, um eine lückenlose Zero-Trust-Umgebung für alle Technologien zu schaffen.

Für akademische Einrichtungen ist es außerdem wichtig, einen ausgewogenen Ansatz für die Cybersicherheit zu entwickeln und zu pflegen. Wenn die implementierten Sicherheitsmechanismen zu starr oder einschränkend sind, werden die Menschen nach Möglichkeiten suchen, genau die Verfahren zu umgehen, die ihre Geräte, Daten und Anwendungen eigentlich schützen sollen. Sie werden versucht sein, ihre eigenen, nicht autorisierten Access Points, Geräte und Anwendungen hinzuzufügen, um langwierige Cybersicherheitsprüfungen und Software-Updates zu vermeiden und so Aufgaben schneller erledigen zu können. Diese Taktik ist als „Schatten-IT" bekannt und birgt zahlreiche Risiken für die Cybersicherheit.

Darüber hinaus muss jede Einrichtung die Datenschutzbestimmungen für Daten, die über das Netzwerk übertragen werden, sowie die Zugriffskontrolllisten (ACLs) und Firewall-Richtlinien für Daten, die in der Cloud gespeichert sind, ermitteln und überprüfen.

Bei der Prüfung der gesetzlichen Anforderungen ist es wichtig, sowohl nationale als auch internationale Datenschutzbestimmungen im Blick zu haben. In den USA müssen akademische Einrichtungen beispielsweise den Family Educational Rights and Privacy Act (FERPA) und den Health Insurance Portability and Accountability Act (HIPAA) einhalten. Sie müssen aber auch im Hinterkopf behalten, dass die Datenschutz-Grundverordnung (DSGVO) der Europäischen Union (EU) für alle Einrichtungen gilt, in denen Studierende aus der EU eingeschrieben sind, egal wo sie sich befinden.

Informieren Sie sich über Ihre Cyberrisiken und gesetzlichen Anforderungen

Bevor Sie mit der Entwicklung einer ZTNA-Strategie beginnen, sollten Sie die Risiken, denen die Einrichtung derzeit ausgesetzt ist, gründlich analysieren und deren Schweregrad einschätzen. Achten Sie bei der Erstellung der Risikobewertung auf die folgenden häufigen Fallstricke:

- IoT-Geräte, die nicht von der IT-Abteilung verwaltet werden. Diese „unbekannten" Geräte halten sich oft nicht an Sicherheitsrichtlinien, verwenden veraltete Firmware und haben keinen Virenschutz. Dadurch erhöht sich die Wahrscheinlichkeit, dass sie von einem bösartigen Akteur als Einstiegspunkt für einen Angriff genutzt werden.
- Unbefugte Geräte und Privatgeräte, die auf das Netz zugreifen. Auf diesen Schatten-IT-Geräten könnte jede beliebige Software laufen und sie könnten bereits mit Viren und Malware infiziert sein, die nur darauf warten, das Netzwerk anzugreifen.
- Inkonsistente Sicherheitsrichtlinien. Diese Unstimmigkeiten führen zu Schwachstellen im Netzwerkschutz, die ein Einfallstor für nicht vertrauenswürdige Parteien sein können.
- Netzwerke mit statischer Sicherheitssegmentierung und automatischem Vertrauen. Diese traditionellen Ansätze der Cybersicherheit erlauben es Nutzern, Geräten und Anwendungen, die ursprünglich als vertrauenswürdig galten, das Netzwerk anzugreifen, ohne dass weitere Überprüfungen stattfinden, um sicherzustellen, dass sie weiterhin vertrauenswürdig sind. Zudem gehen diese herkömmlichen Strategien davon aus, dass Cyberangriffe nicht von innen kommen können. Das ist aber nicht der Fall.

Eine fünfstufige Methodik für ZTNA-Cybersicherheit

Die folgenden fünf Schritte sind für die Entwicklung einer ZTNA-Cybersicherheitsstrategie entscheidend. Mit diesen Schritten stellen Sie sicher, dass das Netzwerk über umfassende Schutzmechanismen verfügt, um unbefugte Nutzer, Geräte und Anwendungen am Zugriff auf das Netzwerk zu hindern.

- **Schritt 1: Überwachen.** Überwachen Sie das Live-Netzwerk, um eine Bestandsliste aller Geräte und Anwendungen – autorisierte und nicht autorisierte – zu erstellen, die Informationen über das Netzwerk anfordern oder übermitteln. So gewinnen Sie auch einen Überblick über die Protokolle, die sie dafür verwenden. Es gibt viele Tools, die diese Informationen aus dem Netzwerk sammeln und einen Bestandsbericht erstellen können, der Geräte nach Typ, Hersteller, Modell, Betriebssystem und anderen Faktoren kategorisiert. Es gibt auch Tools zur Überwachung des Datenflusses, die die verschiedenen Anwendungsdatenströme im Netzwerk aufdecken.
- **Schritt 2: Bewerten und validieren Sie Ihr Inventar.** Beginnen Sie mit der Bewertung von Geräten und Anwendungen nach Art und Funktion. Werden die Geräte oder Anwendungen zum Beispiel für Bildungs- oder IoT-Zwecke verwendet? Stehen sie im Zusammenhang mit geschäftlichen, gesellschaftlichen, akademischen oder Forschungszielen? Tragen sie zur Verbesserung der Effizienz, der Sicherheit und des Datenschutzes bei? Sind sie erforderlich, um gesetzliche Auflagen zu erfüllen? Dieser Prozess hilft dabei, Schatten-IT-Geräte aufzuspüren, die entfernt werden können. Auf diese Weise lässt sich die Angriffsfläche sofort verringern.
- **Schritt 3: Planen Sie Ihr Konzept für die Authentifizierung, Berechtigungsprüfung und Verwaltung.** Um die besten Ergebnisse zu erzielen, sollten Sie einen mehrdimensionalen Plan entwickeln, der eine Makro- und eine Mikrosegmentierung umfasst. Bei der Makrosegmentierung werden virtuelle LANs (VLANs), Virtual Routing and Forwarding (VRF), virtuelle private Netzwerke (VPNs) und andere Ansätze zur Trennung von Nutzern, Geräten und Anwendungen im Netzwerk verwendet. Die Mikrosegmentierung definiert, wie diese Nutzer, Geräte und Anwendungen ihrem Netzwerksegment und ihren Sicherheitsrichtlinien zugeordnet werden.
- **Schritt 4: Simulieren.** Testen und validieren Sie das in Schritt 3 entwickelte Konzept und nutzen Sie die daraus gewonnenen Erkenntnisse zur Feinabstimmung der Sicherheitsrichtlinien. So können Sie dafür sorgen, dass die Richtlinien alle Szenarien abdecken. In dieser Phase ist es wichtig, alle Aspekte des Konzepts zu testen. Stellen Sie beispielsweise sicher, dass die Simulationen die Ausstellung von Zertifikaten, die Konfiguration von Richtlinien, die Konfiguration von Quarantäne-Szenarien, die Simulation von Protokollflüssen und das Testen von Firewall-Integrationen umfassen.
- **Schritt 5: Durchsetzen.** Sobald die Sicherheitsrichtlinien vollständig und präzise abgestimmt sind, können sie am Rand des Netzwerks durchgesetzt werden, wo Nutzer, Geräte und Anwendungen versuchen, auf das Netzwerk zuzugreifen. Wenn getestete und validierte Sicherheitsrichtlinien durchgesetzt werden, wird unbefugten Geräten der Zugriff auf das Netzwerk verwehrt und unerwartete Datenströme werden unterbunden. Darüber hinaus können Geräte unter Quarantäne gestellt und IT-Teams auf die Situation aufmerksam gemacht werden. Diese Mechanismen funktionieren wie eine Reihe von Kontrollpunkten, die verhindern, dass gefährliche Fahrer auf eine Autobahn gelangen.

Die Befolgung dieses fünfstufigen Prozesses ist ein wichtiger Schritt für die Einrichtungen auf ihrem Weg zu ZTNA-Cybersicherheit, reicht aber allein nicht aus. Um erfolgreich zu sein, muss jede ZTNA-Cybersicherheitsstrategie von einem umfassenden Konzept für Schulungen, Patch-Management und ein energisches Vorgehen im Bereich der Schatten-IT begleitet werden.

Mehr als die bloße Summe der einzelnen Aspekte

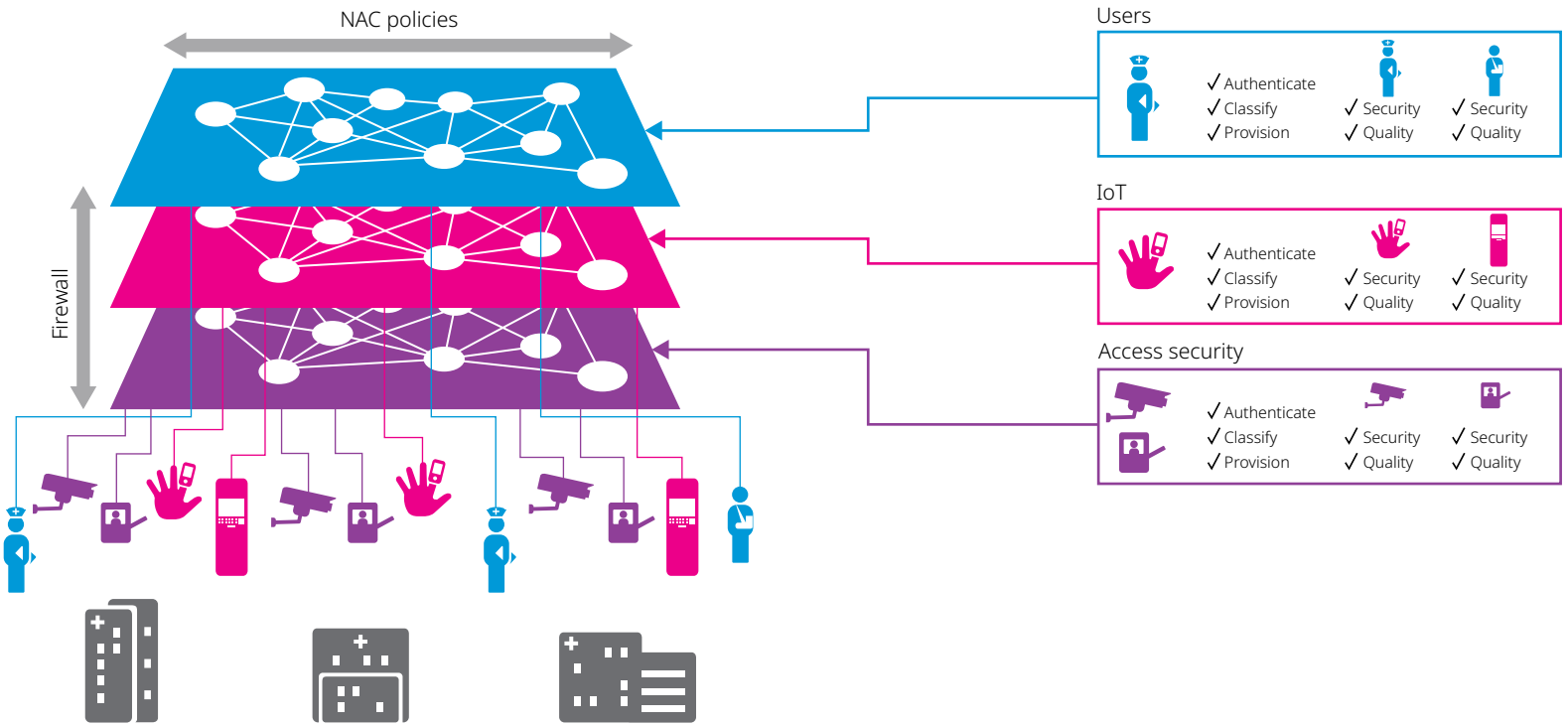
Durch die schrittweise Umsetzung des ZTNA-Cybersicherheitskonzepts können akademische Einrichtungen in allen Bereichen ihres Betriebs erhebliche Vorteile erzielen. Die offensichtlichsten Vorteile liegen in der Verhinderung und Erkennung von unbefugtem Netzwerkzugriff, aber es gibt auch zahlreiche Vorteile für Bildung und Geschäftstätigkeit.

Weitreichender Schutz

Aus technologischer Sicht bieten umfassende Netzwerkzugriffskontrolllisten und regelbasierte Zugriffskontrolle die Möglichkeit, jede Verbindung zu authentifizieren und allen Nutzern und Geräten, die auf das Netzwerk zugreifen, Berechtigungen zuzuweisen. Dadurch erhalten Institute ein fein abgestuftes Maß an Schutz, das den Zugriff auf Netzwerkressourcen und -daten für böswillige Nutzer und Geräte erheblich erschwert.

Die Möglichkeit, den Nutzerverkehr innerhalb eines Makrosegments mithilfe der Mikrosegmentierung weiter zu segmentieren, ermöglicht auch eine genauere Kontrolle des Nutzer- und Gerätezugriffs, um das Risiko einer Angriffsverschleppung innerhalb des Netzwerks zu verringern. Bei der Mikrosegmentierung kann der Nutzerverkehr innerhalb eines Makrosegments, z. B. eines VLANs, auf der Grundlage von Faktoren wie Tageszeit, Zugriffsort, Zugehörigkeit des Nutzers zu der Gruppe von Studenten, Lehrkräften oder Verwaltungsmitarbeitern und anderen Zugangskontrollen getrennt werden (Abbildung 1). Dieselbe Sicherheitsrichtlinie folgt der Person, egal wo sie sich befindet, und ermöglicht es dem Institut, einen einheitlicheren Ansatz für die Cybersicherheit umzusetzen.

Abbildung 1. Die Kombination von Makro- und Mikrosegmentierung stärkt die Zugangskontrolle im Netzwerk



Lohnende Vorteile für alle

Akademische Einrichtungen, die für ihr Engagement und ihre Sorgfalt beim Schutz der Sicherheit und der Privatsphäre der Informationen in ihren Netzwerken bekannt sind, können ihren Ruf, ihre Bildungsmarke und ihr öffentliches Image verbessern. Ihre Fähigkeit, sich vor Cyberangriffen zu schützen und die negative Publicity zu vermeiden, die mit solchen Ereignissen unweigerlich einhergeht, trägt dazu bei, Studierende für sich zu gewinnen und zu halten. So ist der langfristige Erfolg gesichert. Darüber hinaus können akademische Einrichtungen als Vorbild für bewährte Praktiken im Bereich der Cybersicherheit dienen, denen andere Einrichtungen nacheifern können. Dadurch lässt sich die Abwehr von Cyberangriffen auf Bildungsnetzwerke weltweit verbessern.

Eine ZTNA-Cybersicherheitsstrategie trägt auch zu besseren akademischen Ergebnissen bei. Mit einem sichereren Netzwerk können Lehrkräfte und Studierende die Vorteile innovativer digitaler Technologien nutzen, die die Lernmöglichkeiten und den Lernerfolg verbessern. Dies zeigt sich an folgenden Beispielen:

- Die Lehrkräfte können kreativere, ansprechendere und interaktivere Unterrichtsstunden bzw. Vorlesungen entwickeln und durchführen, die die Studierenden und Schüler inspirieren. Sie können sie mit den neuesten Innovationen vertraut machen und sie ermutigen, sich aktiv an den Diskussionen und Aktivitäten in der Klasse und im Kurs zu beteiligen, unabhängig davon, ob sie sich im Klassenzimmer bzw. Hörsaal befinden oder nicht.
- Die Studierenden und Schüler können mit neuen Technologien experimentieren, offen und ortsunabhängig miteinander und mit den Lehrkräften zusammenarbeiten und die neuesten digitalen Innovationen in ihre Aufgaben einbeziehen, um ihr Potenzial zu zeigen.

Die Grundlage des vertrauenswürdigen Netzwerks stellt sicher, dass der Schwerpunkt in jeder Einrichtung weiterhin auf der Lehre und Bildung liegt.

IT-Teams im Bildungswesen profitieren ebenfalls von einer ZTNA-Cybersicherheitsstrategie. Mit einem tieferen Einblick in den Cybersicherheitsstatus der akademischen Einrichtung können IT-Teams fundiertere Entscheidungen über neue Technologiestrategien treffen, wie z. B. die Einführung eines Cloud-first-Ansatzes oder die Unterstützung von BYOD. Gleichzeitig können sie die digitale Infrastruktur des Campus besser schützen und kontrollieren und die sinnvolle Nutzung wertvoller Netzwerkressourcen und -bandbreite sicherstellen.

Und nicht zuletzt hat die Begrenzung der Angriffsfläche des Instituts potenzielle finanzielle Vorteile: Sie verringert das Risiko, dass kostspielige Abhilfemaßnahmen als Reaktion auf Cyberangriffe erforderlich werden.

Ein kompetenter Partner für kompetente Sicherheit

Akademische Einrichtungen, die eine ZTNA-Cybersicherheitsstrategie implementieren, müssen mit einem erfahrenen Partner zusammenarbeiten, der sowohl fachkundige Einblicke und Anleitungen als auch bewährte ZTNA-Netzwerklösungen bieten kann.

Alcatel-Lucent Enterprise kann auf umfassende Erfahrungen bei der Unterstützung akademischer Einrichtungen in aller Welt zurückgreifen, wenn es um ZTNA-Cybersicherheit geht. Wir wissen, welche Schritte diese Institute unternehmen müssen, um eine ZTNA-Strategie zu implementieren. Wir arbeiten mit Ihnen zusammen, um sichere Netzwerklösungen anzubieten, die genau auf Ihre Strategie abgestimmt sind. Ihr Institut kann dann ein mehrschichtiges Konzept für die Netzwerksicherheit implementieren, um die wichtigsten Cybersicherheitsmechanismen, wie z. B. Mikrosegmentierung und regelbasierte Zugriffskontrolle, optimal zu nutzen.

Umfassende Sicherheit

Die Netzwerklösungen von ALE sind entsprechend den wichtigsten Sicherheitsstandards zertifiziert, darunter folgende:

- Internationale Common Criteria-Leitlinien und -Spezifikationen für IT-Sicherheit
- Compliance-Tests gemäß U.S. Joint Interoperability Test Command (JITC)
- U.S. Federal Information Processing Standard (FIPS) 140-2

Die enge Integration von Firewalls und Netzwerkinfrastruktur hilft Instituten, die Quelle unbefugter und bösartiger Aktivitäten genau zu lokalisieren und die angreifenden Geräte unter Quarantäne zu stellen. Unsere Lösungen erweitern die Investitionen unserer Kunden, da sie sich in Firewalls von Palo Alto Networks und Fortinet integrieren lassen.

Langjährige Erfahrung

Wir sind ein verlässlicher Partner für akademische Einrichtungen auf der ganzen Welt, die an der Verbesserung ihrer Cybersicherheit arbeiten:

- An der California State University in den USA haben unsere Netzwerk- und Managementlösungen ein zuverlässiges und flexibles Netzwerk geschaffen, das verbesserte Sicherheit, flächendeckendes Wi-Fi und offene, gemeinsam genutzte Cloud-Dienste bietet. Dadurch konnte das Angebot auf dem gesamten Campus verbessert werden. Das äußerst zuverlässige Netzwerk unterstützt mehr als 500.000 Nutzer an den über 20 Fakultäten der Universität und hat dazu beigetragen, mehr als 100 Millionen US-Dollar an Infrastrukturkosten einzusparen.
- Im Centro Paula Souza in Brasilien sorgen unsere intelligenten und sicheren Netzwerklösungen für hohe Geschwindigkeiten und Leistung, die Nutzer benötigen, um besser und schneller arbeiten zu können. Die einheitliche Authentifizierung bietet Mitarbeitern und Besuchern benutzerfreundliche Sicherheitsvorkehrungen. Die IoT-Eingrenzungstechnologie ermöglicht eine sichere und kontrollierte Verbindung von Geräten mit dem Netz. Zudem haben die IT-Mitarbeiter uneingeschränkten Einblick in den Netzwerkbetrieb und profitieren von einheitlichen Richtlinien für die Netzwerknutzung.
- An der Linköping University in Schweden sorgen unsere Netzwerklösungen für einen stabilen und sicheren Netzwerkzugang für Studenten und Dozenten, aber auch für Gäste, externe Partner, Mieter in Universitätsgebäuden und Service-Provider. Da die physische und die logische Netzwerkarchitektur völlig getrennt sind, können sich Studenten und Dozenten automatisch und sicher an jedem Ort und mit jedem Gerät mit dem Netzwerksegment verbinden, das ihnen zugewiesen ist.

Weitere Informationen

Wenn Sie erfahren möchten, wie wir auch Ihre akademische Einrichtung bei der Entwicklung einer Zero-Trust-Network-Access-Cybersicherheitsstrategie unterstützen können, besuchen Sie unsere Website oder nehmen Sie noch heute Kontakt mit uns auf, um Ihre spezifischen Anforderungen zu besprechen.

Alcatel·Lucent
Enterprise