Das Internet der Dinge in der Bildung

Verbesserung der Lern- und Unterrichtserfahrungen durch Nutzung von IoT auf einer sicheren Basis

Whitepaper
IoT im Bildungswesen

Alcatel·Lucent
Enterprise

IoT verändert das Gleichgewicht im Bildungswesen grundlegend

Das Internet der Dinge (IoT) hat das Potenzial, die Bildung dadurch zu transformieren, in dem sie durch die intelligente Verbindung von Schnittstellen und Prozessen, die Art und Weise grundlegend verändert, wie Schulen und Universitäten Daten und Informationen sammeln. IoT bezieht sich dabei auf die Vernetzung von physischen Objekten wie eingebettete Sensoren, Aktoren und anderen Geräten, die in der Lage sind, Informationen über Aktivitäten auf dem Campus in Echtzeit zu sammeln und zu übertragen. Wenn IoT mit Technologien wie z.B. Nutzermobilität und Datenanalyse kombiniert wird, führt dies zu einem neuen Paradigma in der Bildung. IoT ermöglicht den Institutionen somit:

- Neue Lernmethoden für Schüler und Studenten umzusetzen dank der Unterstützung von personalisierteren und dynamischeren Lernmaterial wie z.B. digitale Lehrbücher und Spiele-basiertes Lernen.
- Die Art und Weise zu ändern, wie Lehrkräfte ihren Unterricht und ihre Prüfungen durchführen dank intelligenten audio-visuellen Geräten, digitalen Videorekordern für die Erfassung des Unterrichts sowie mit Online-Tests.
- Abläufe in der Schulverwaltung zu vereinfachen durch proaktive Überwachung der kritischen Infrastruktur und eine effizientere und kostengünstigere Lösung für Heizungs-, Lüftungs- und Klimaanlagen, sowie Beleuchtung und Landschaftspflege zu schaffen
- das Angebot einer sichereren Umgebung für Schüler und Lehrerdurch digitale Überwachungskameras, intelligente Türschlösser sowie vernetzte Schulbusse.

IoT-Szenarien im Bildungswesen

IoT-Lösungen versprechen, Schulen und Universitäten intelligenter und erfolgreicher zu machen. Das IoT hat das Potenzial, die Art und Weise, wie Schüler und Studenten mit Lehrern und Professoren sowie der Verwaltung zusammenarbeiten und sich mit der Technologie und den Geräten im Klassenzimmer verbinden, neu zu definieren. Das trägt dazu bei, sowohl das Lernerlebnis als auch die Ergebnisse zu verbessern und die Kosten zu senken. Beispiele für IoT-Lösungen in der Bildung umfassen:

- Intelligente Tafeln (Smart Whiteboards) und andere interaktive digitale Medien, die Daten für den Einsatz im Klassenzimmer - oder zu jeder Zeit an jedem beliebigen Ort - sammeln und analysieren können. Dadurch werden sowohl der Unterricht als auch die Lernergebnisse optimiert.
- Lösungen wie intelligente Temperatursensoren und intelligente Heizungs-, Lüftungs- und Klimaanlagen, die den Energieverbrauch reduzieren und den Betrieb automatisieren.
- Intelligente Studentenausweise, Geräte zur Anwesenheitserfassung, Systeme zur Verfolgung der Schulbusse sowie Parksensoren, die den physischen Aufenthaltsort der Schüler und Studenten ermitteln können.
- Drahtlose Türschlösser, vernetzte Überwachungskameras und Gesichtserkennungssysteme, die Lehrkräften, Schülern, Studenten und Mitarbeitern Sicherheit bieten.
- Forschungsprogramme, die um intelligentere Systeme erweitert wurden in wichtigen Studienbereichen, beispielsweise Medizin, Landwirtschaft und Technik.

Herausforderungen beim Einsatz von IoT

Das IoT bringt eine noch nie dagewesene Datenmenge mit sich, welche die Netzwerkinfrastruktur vor große Herausforderungen bei der Leistung, dem Betrieb und dem Management stellt, verbunden mit erhöhten Sicherheitsrisiken von allen Endpunkten. Zur Lösung dieser Probleme müssen die Netzwerkadministratoren in Bildungseinrichtungen die herkömmlichen Netzwerkdesigns anpassen, um die neuesten Standards an Netzwerkintelligenz, Automatisierung und Sicherheit zu gewährleisten.

Schulen und Universitäten brauchen eine kosteneffektive Netzwerkinfrastruktur, die sicher mit riesigen Datenmengen umgeht, dabei jedoch auch einfach zu handhaben und zu betreiben ist. Die Infrastruktur muss daher:

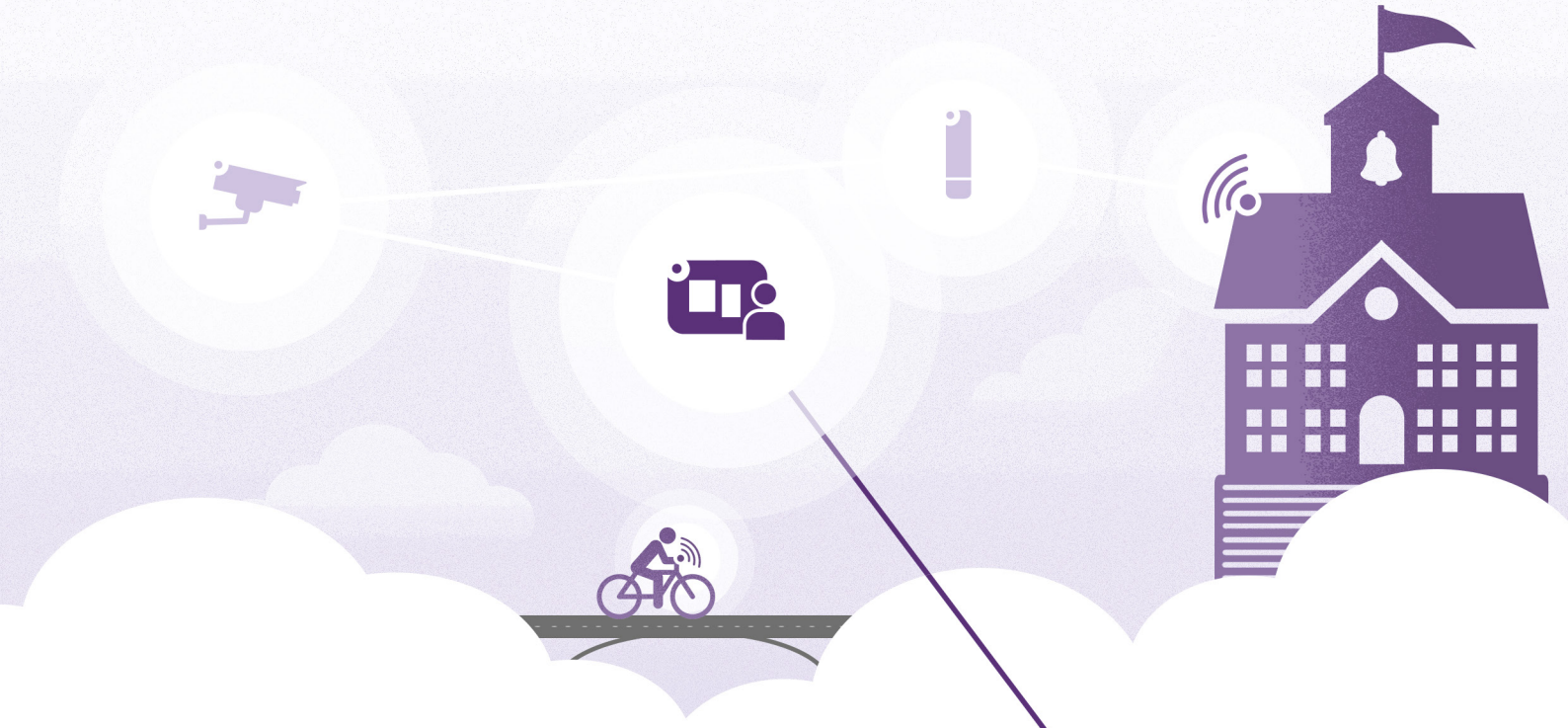
- **Einen einfachen, automatisierten Prozess für das Hinzufügen von IoT-Geräten bereitstellen.** Große IoT-Systeme können Tausende von Geräten oder Sensoren enthalten, und die manuelle Bereitstellung und Verwaltung all dieser Endpunkte ist kompliziert und fehleranfällig. Ein automatisiertes Hinzufügen ermöglicht es der Netzwerkinfrastruktur, Geräte dynamisch zu erkennen und sie dem entsprechend gesicherten Netzwerk zuzuordnen.
- **Die richtigen Netzwerkressourcen bieten, mit denen das IoT-System richtig und effizient läuft.** Viele Geräte im IoT- System liefern einsatzkritische Informationen, die ein bestimmtes QoS-Niveau erfordern. Zum Beispiel benötigen einige Anwendungsfälle ausreichend Bandbreite auf einer Hochleistungs-Netzwerkinfrastruktur, um Servicebereitschaft und Zuverlässigkeit zu gewährleisten.
- **Für eine sichere Umgebung gegen Cyber-Angriffe und Datenverlust sorgen.** Weil die vielen vernetzten Geräte und Sensoren im IoT zu einer entsprechenden Fülle von potentiellen Angriffsvektoren führen, ist zur Minimierung des Risikos von Cyberkriminalität Sicherheit von entscheidender Bedeutung. Diese Sicherheit ist auf mehreren Ebenen notwendig, darunter dem Containment der IoT-Netzwerke selbst.

IT-Fachleute planen noch mehr IoT

IT-Fachleute aus allen Branchen planen bereits in naher Zukunft den verstärkten Einsatz von IoT-Lösungen. Im Rahmen einer Umfrage von 451 Research zu den Trends 2017 im Internet der Dinge sagten 67 Prozent der antwortenden IT-Fachleuten, dass ihre Unternehmen entweder bereits eine IoT-Lösung implementiert oder ein IoT-System im Pilotbetrieb hatten. 21 Prozent der Befragten gaben an, dass ihr Unternehmen den Einsatz von IoT-Lösungen innerhalb von 12 Monaten planen, während 11 Prozent behaupten, dass die Pläne ihres Unternehmens IoT einzusetzen noch mehr als ein Jahr entfernt seien.

Durch IoT nimmt die Gefahr der Cyberkriminalität für Schulen und Universitäten deutlich zu.

Das Wachstum des IoT im Bildungswesen bringt auch einen rasanten Anstieg der Bedrohung der Cybersicherheit mit sich, da die Verbreitung von Sensoren und vernetzten Geräten die Angriffsoberfläche im Netzwerk stark vergrößert. Dazu ist IoT besonders anfällig, da viele IoT-Geräte ohne besonderen Fokus auf Sicherheit hergestellt oder von Unternehmen gebaut werden, welche die aktuellen Sicherheitsanforderungen nicht wirklich verstehen. Die IoT-Systeme sind somit zunehmend das schwache Glied für die Netzwerksicherheit in Bildungseinrichtungen.



- Das Netzwerk einer unbenannten Universität wurde dem 2017 Data Breach Digest von Verizon zufolge, von ihrem eigenen System mit 5.000 IoT-Geräten, einschließlich angeschlossener Verkaufsautomaten und intelligenter Glühbirnen, angegriffen. Die gehackten Geräte führten alle 15 Minuten Hunderte von DNS-Abfragen durch, was zur Folge hatte, dass die Netzwerkverbindungt der Universität unerträglich langsam oder gar unzugänglich wurde.[1]
- Weiße Rassisten hackten im Jahr 2017 vernetzte Drucker und Faxgeräte an verschiedenen Universitäten, einschließlich der Universität von Kalifornien, Berkeley, wodurch die Maschinen rassistische Propaganda ausdruckten.[2]
- Das Mirai-Botnet, das den Internetservice an der gesamten US-Ostküste sowie einem großen Teil von Westeuropa durch die Remote-Übernahme von Millionen von IoT-Geräte lahmgelegt hat, begann im Jahr 2016 als Angriff auf das Computernetzwerk der Rutgers University. Die Mirai-Software wurde entwickelt, um schlecht gesicherte Router, Sicherheitskameras und Baby-Monitore zu hacken.[3]

Ein Highschool-Student aus Michigan wurde im Jahr 2015 gefasst, als er einen DDoS-Angriff durchführte, der so ausgelegt war, dass das Schulnetzwerk zeitweise heruntergefahren wurde. Das Botnet, das den Cyberangriff verursacht hatte, zielte auf vernetzte IoT-Geräte wie Überwachungskameras und Router.[4]

Aufbau einer sicheren IoT-Netzwerkinfrastruktur

Der Schutz von IoT-Datenverkehr und Geräten in Schul- und Universitätsnetzwerken ist eine Herausforderung, die nicht durch eine einzelne Sicherheitstechnologie gelöst wird. Sie erfordert einen strategischen Ansatz, der die Vorteile von mehreren Sicherheitsvorkehrungen nutzt.

Um Bildungseinrichtungen dabei zu unterstützen, die Vorteile des IoT zu nutzen und die Risiken zu mindern, bietet Alcatel-Lucent Enterprise eine mehrstufige Sicherheitsstrategie. Die Strategie von ALE bietet Schutz auf jeder Schicht der Infrastruktur, vom einzelnen Nutzer und Gerät bis hin zum Netzwerk-Layer selbst. Sie umfasst auch eine IoT-Containment-Strategie, um das Einbinden von Geräten zu vereinfachen und zu sichern sowie, um die richtigen Netzwerkressourcen zur Verfügung zu stellen und um das System ordnungsgemäß und effizient zu betreiben. Und das alles in einer sicheren Umgebung, um Organisationen vor Cyberangriffen zu schützen.

IoT-Containment

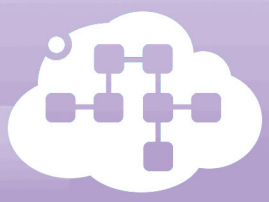
Um IoT-Containment zu ermöglichen, wird allen Benutzern, Geräten und Anwendungen innerhalb des ALE-Netzwerks ein Profil zugeordnet. Diese Profile, die Rollen, Zugriffsberechtigungen, QoS-Pegel und andere Richtlinieninformationen definieren, werden an alle Switches und Zugriffspunkte im Netzwerk weitergeleitet.

- Geräte werden mithilfe von Netzwerk-Virtualisierungstechniken in «virtuellen Containern» platziert, die es mehreren Geräten und Netzwerken ermöglichen, dieselbe physische Infrastruktur zu nutzen, dabei jedoch vom Rest des Netzwerks isoliert zu bleiben.
- In diesen virtuellen Containern werden QoS- und Sicherheitsregeln angewandt.
- Durch die Aufteilung des Netzwerks auf virtuelle Container hat eine Sicherheitslücke, die in einem Teil des virtuellen Netzwerks auftritt, keine Auswirkungen auf andere Geräte oder Anwendungen in anderen virtuellen Netzwerken.
- Wird ein neues IoT-Gerät angeschlossen, erkennt das Netzwerk automatisch dessen Profil und ordnet ihm die entsprechende virtuelle Umgebung zu.
- Die Kommunikation ist auf die Geräte beschränkt, die sich in dieser virtuellen Umgebung befinden sowie auf die Anwendung im Rechenzentrum, das diese Geräte steuert.
- Weil alle Benutzer ebenfalls Profile innerhalb des ALE haben, kann der Zugriff auf die virtuellen IoT-Container auf berechtigte Einzelpersonen und Gruppen beschränkt werden.

Umfassende Sicherheit

Zusätzlich zum IoT-Containment bieten ALE Netzwerktechnologien mehrschichtige Sicherheit über mehrere Ebenen des Netzwerks hinweg an.

- Auf der Benutzerebene stellen Profile sicher, dass die Benutzer authentifiziert werden und mit den passenden Zugriffsrechten autorisiert sind.
- Auf Geräteebene gewährleistet das Netzwerk, dass Geräte authentifiziert sind und mit den etablierten Sicherheitsregeln konform sind.
- Auf der Anwendungsebene kann das Netzwerk Regeln aufstellen, die sich auf jede Anwendung oder Gruppe von Anwendungen beziehen, einschließlich Blockierung, Begrenzung der Bandbreite sowie Steuerung, wer auf welche Anwendung zugreifen darf.
- Auf der Netzwerkebene profitieren ALE Switches von sicherer, diversifizierter Code. Es schützt Netzwerke vor intrinsischen Schwachstellen, Code-Ausnutzungen, eingebetteter Malware und potentiellen Hintertüren (Backdoors), die eine Gefährdung für Switches, Router und andere systemrelevante Hardware darstellen können.
- ALE Smart Analytics nutzt Deep Packet Inspection (DPI) und andere Technologien, um die Art der Daten und Anwendungen zu erkennen, die sich durch das Netzwerk bewegen, so dass die Identifizierung ungewöhnlicher Netzwerkverkehrsmuster und unbefugter Aktivitäten möglich ist.



IoT-Geräte bergen Risiken für jeden Bestandteil im gesamten Netzwerk. Durch die Einrichtung von Containern über virtuelle Netzwerksegmentierung werden IoT-Geräte und die Anwendungen, die sie steuern, isoliert, wodurch Bedrohungen reduziert werden, ohne dass Kosten und Aufwand für getrennte Netze entstehen.

Durchgehendes Betriebs- und Netzwerkmanagement

ALE Netzwerklösungen bieten für den Bildungsbereich zudem erhebliche operative und strategische Vorteile.

- Mithilfe von ALE können mehrere getrennte virtuelle Netzwerke an einer einzigen Infrastruktur betrieben werden, was die Investition in mehrere physische Netzwerke erspart.
- Die Unified Access-Lösung von ALE ermöglicht die Zusammenarbeit drahtgebundener und drahtloser Technologien in einem einzigen, robusten Netzwerk, gemeinsam mit bestimmten Netzwerkdiensten, Rahmenbedingungen, einem passenden Authentifizierungsschema und einer einzigen Authentifizierungs-Datenbank.
- ALE-Netzwerklösungen verfügen darüber hinaus über ein einziges Managementsystem für alle Elemente der Infrastruktur, einschließlich einheitlichem Management sowohl von drahtgebundenen LAN- als auch von drahtlosen WLAN-Netzwerken. Die OmniVista® 2500 Management Suite von Alcatel-Lucent bietet eine einzige zentrale Konsole zur Verwaltung von virtuellen Umgebungen, Switches, Zugangspunkten und alle anderen Komponenten des Netzwerks.

Ein hochleistungsfähiges Netzwerk-Portfolio

Switches, Access Points und Controller von ALE unterstützen die neueste Generation an hoher Bandbreite und geringer Latenzzeiten und können eine große Anzahl von Geräten in komplexen Umgebungen verwalten. ALE Netzwerkprodukte und -lösungen sind in der Lage, die Netzwerkanforderungen von Bildungseinrichtungen jeglicher Größe zu lösen. Außerdem bietet ALE eine Auswahl an robusten Switches, Access Points und Routern für Netzwerkeinsätze im Freien oder in rauer Umgebung.

Sichere IoT-Netzwerke und Strategien stehen bereits heute für die Bildung zur Verfügung

ALE Produkte und Lösungen bilden eine sichere Netzwerkgrundlage, die Schulen und Universitäten beim Einsatz von IoT-Systemen dabei unterstützt, neue Lernmöglichkeiten für die Studierenden zu schaffen und die Unterrichts- und Prüfungsmethoden von Lehrkräften zu verbessern. Sichere IoT-Lösungen tragen auch dazu bei, die Betriebsabläufe der Verwaltung zu einfachen und so eine sicherere Umgebung zu schaffen. ALE´s IoT-Containment und mehrstufige Sicherheitsstrategien reduzieren die Risiken und vereinfachen den Aufbau von IoT-Netzwerken durch einfacheres Einbinden von Geräten, die Bereitstellung effizienterer Prozesse sowie eine signifikante Erhöhung der Sicherheit. ALE unterstützt Institutionen bei der Digitalisierung durch die Bereitstellung von verbesserter Netzwerkintelligenz, Automatisierung und Sicherheit.

Möchten Sie mehr erfahren?

Für weitere Informationen über die IoT-Lösungen von Alcatel-Lucent Enterprise gehen Sie bitte auf ALE IoT-Sicherheit.

Vernetzte Bildung

Wo Bildung mit Technologie verbunden ist, die funktioniert. In Ihrer Schule, Hochschule oder Universität. Mit globaler Reichweite und lokaler Präsenz, liefern wir eigens entwickelte Netzwerke und Kommunikationen für die Bildungsumgebung, die eine sichere und zuverlässige Zusammenarbeit zwischen Ihrer Einrichtung und den Schülern sowie Studenten ermöglichen.

1 Universität durch ihr eigenes IoT-System angegriffen
2 Rassistische Propaganda an Universitäten durch Hacker gedruckt
3 Attacke durch das Mirai Botnetz
4 Schüler in Michigan vor Gericht wegen DDoS Attacke

00030918DE (April 2021)