WALLIX
CYBERSECURITY SIMPLIFIED

Stärkung der Identitäts- und Zugriffs-Cybersicherheit

im Bildungswesen

Stärkung der Identitäts- und Zugriffs-Cybersicherheit

im Bildungswesen

Cyber-Attacken, Ransomware, Phishing-Kampagnen, Cyber-Attacken gegen den Bildungssektor nehmen zu.

Die Daten von Studenten, Professoren, aber auch von Forschungslaboren und Akademien sind zunehmend begehrt. Cyber-Angriffe auf Server sind auf dem Vormarsch, aber der Bildungssektor ist nicht immer gut vorbereitet.

Wenn in Universitäten Postmappen, Ausleihformulare und Karteikarten wieder aktiviert werden müssen, ist im voll durchdigitalisierten Hochschulbetrieb etwas Gravierendes vorgefallen. Glück im Unglück hatte im Dezember 2019 die Universität Gießen. Ein Mitarbeiter des Universitäts-Rechenzentrums hatte intuitiv auf ungewöhnliche Fehlermeldungen reagiert und auf einen möglichen Cyberangriff geschlossen. Sämtliche IT-Système wurden daraufhin vollständig heruntergefahren. Die zweitgrößte hessische Hochschule mit rund 28.000 Studenten war für mehrere Wochen offline. Der Präsident der Universität sprach von einer "digitalen Naturkatastrophe". Die schnelle Reaktion im Rechenzentrum verhinderte massive Schäden in Form von großen Datenverlusten. Doch war auch kein Normalbetrieb mehr möglich : keine Mails, kein W-Lan, keine Noteneinträge, keine digitale Literatur, kein Zugriff auf Forschungsdaten, keine digitalen Neubewerbungen für Studienplätze, keine digitalisierten Verwaltungsabläufe. Nach und nach konnte das IT-System nach umfänglichen Sicherheitsüberprüfungen wieder neu aufgesetzt werden – rund 38.000 neue Passwörter mussten neu Verfügung gestellt werden, die persönlich abzuholen waren. Experten zufolge wurde versucht, die Universität Gießen mithilfe der Schadsoftware Emotet zu infizieren, die sich begann, über einen falsch geöffneten Email-Anhang zu verbreiten. Es hätte schlimmer kommen können. Und doch zeigt der Fall der Uni Gießen, dass der Bildungssektor vermehrt in das Fadenkreuz von Hackern geraten ist. Er wird von Hackern als leichtes Ziel angesehen, da er in Bezug auf die Cyber-Reife manchmal zurückliegt. Und die rasante digitale Transformation während der COVID-Pandemie hat diesen Trend nur noch beschleunigt.

Cyber-Attacken, Ransomware, Phishing-Kampagnen, Cyber-Attacken gegen den Bildungssektor nehmen zu.

DIE NEUEN HERAUSFORDERUNGEN IM BILDUNGSWESEN

Bildung ist nicht mehr auf ein Klassenzimmer oder einen Universitätshörsaal, eine Tafel, einen Lehrer oder einen Dozenten beschränkt. Schüler und Studenten werden heute zunehmend – und die Corona-Pandemie hat diesen Trend verstärkt, im digitalen Distanzunterricht im Rahmen einer E-Education ausgebildet.

Ob es um die Kommunikation mit Studenten am anderen Ende der Welt durch Austauschprogramme geht oder um die Teilnahme an Kursen an internationalen Universitäten, die Ausbildungs- und Lernzentren öffnen sich immer mehr nach außen, was gleichzeitig die Bildungsnetzwerke komplexer und anspruchsvoller macht.

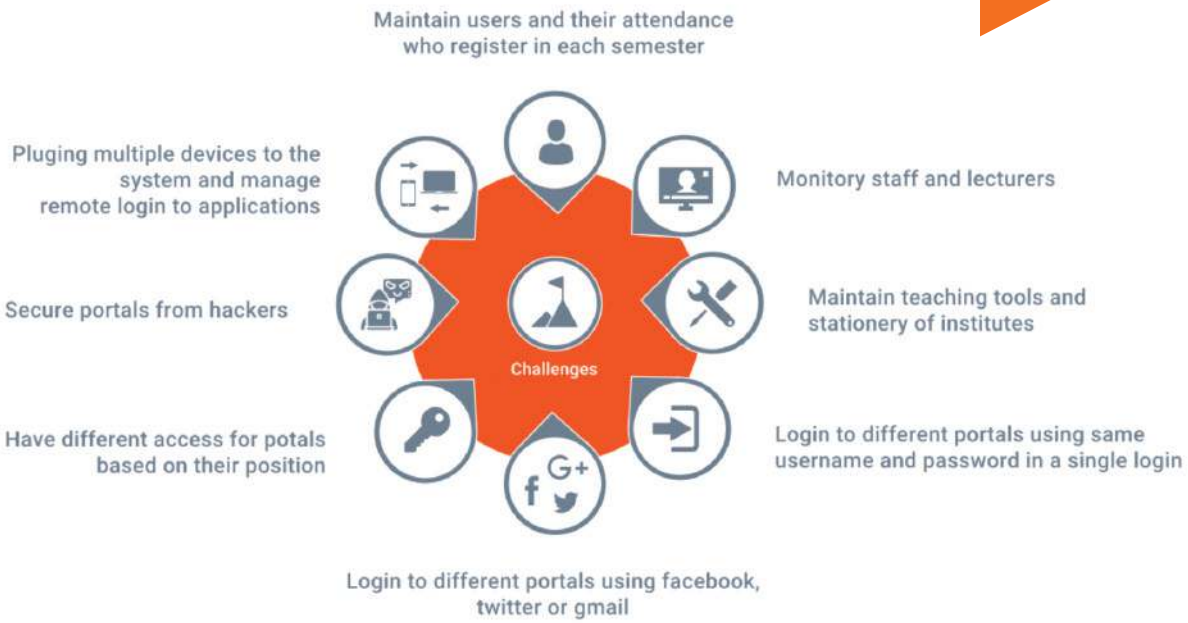
Digitale Inhalte, Tools für die Zusammenarbeit und Lösungen für die Online-Dateiverwaltung sowie -freigabe sowie digitale Eltern-Lehrer-Räume sind heute in vielen Bildungseinrichtungen alltäglich. Die Schul- und Universitätsverwaltung muss nicht nur den Zugriff von Schülern auf ihren digitalen Raum, Eltern, die auf Notenräume zugreifen wollen, Unternehmen, die Praktika anbieten, sondern auch externe Anbieter von IT-Lösungen oder Drittanwendungen verwalten.

Darüber hinaus erhöhen der Trend zur Vergrößerung von Akademien, die Gruppierung von Campus-Orten auf regionaler Ebene und der Wunsch, Ressourcen und Rechenzentren zu bündeln, den Zugang von Anwendern und IT-Teams zu geografisch verteilten Standorten mit der gemeinsamen Nutzung von Infrastrukturen, die Komplexität von Anbindungssystemen. Sie basieren auf großstädtischen oder regionale Breitbandnetzen, universitären Intranetportalen oder der nomadischen Nutzung digitaler Arbeitsumgebungen.

Schließlich hat die Corona-Krise der letzten Monate den Bildungssektor dazu gezwungen, sich neu zu erfinden. Das Bildungswesen ist einer der am stärksten von der Pandemie betroffenen Bereiche. Die Schulen und Universitäten, die gezwungen waren, ihre Türen zu schließen, mussten in kurzer Zeit ihre Kapazitäten und die Möglichkeiten zum Studieren und Arbeiten in der Ferne erweitern. In dieser Situation waren das Fernstudium und der Online-Austausch eine echte Hilfe, definierte Lernziele umzusetzen. Aber diese Zunahme von Remote-Verbindungen, insbesondere über Videokonferenzen, hat genauso die Gefährdung durch Cyber-Risiken erhöht: Kriminelle haben Schwachstellen in diesen Diensten schnell ausgenutzt, um Namen, Passwörter und E-Mail-Adressen zu erbeuten und sie im Dark Web zu verkaufen.

All diese Entwicklungen haben neue Herausforderungen für das Identitäts- und Zugriffsmanagement geschaffen, denen sich der Bildungssektor stellen muss.

Neben diesen neuen Einsatzmöglichkeiten ist die Aktualisierung der Identitäten und des Zugangs zu Netzwerken und Anwendungen eine der größten und teuersten Herausforderungen im Bildungssektor.



Eine wachsende Anzahl von Identitäten zu verwalten

Neben diesen neuen Einsatzmöglichkeiten ist die Aktualisierung der Identitäten und des Zugangs zu Netzwerken und Anwendungen eine der größten und teuersten Herausforderungen im Bildungssektor. Jedes Jahr oder jedes Semester müssen IT-Abteilungen an Schulen und Hochschulen Tausende von neuen Benutzern verwalten, die gleichzeitig an Bord genommen und/oder entfernt werden müssen. All diese Nutzer sind oft sehr heterogen: minderjährige Schüler, volljährige Schüler und Studenten, Lehrer, Eltern, Verwaltungspersonal, Lieferanten und Partner, lokale Behörden.

Dies ist ein zyklischer Prozess, den jede Universitäts-IT-Abteilung und Akademie durchführen muss und die die begrenzten internen IT-Einrichtungen zur Speicherung und Pflege der Daten jedes Schülers oder Studenten, ihrer Zeugnisse und anderer wichtiger und vertraulicher Informationen - Sozialversicherungsnummern, Stipendien, Behinderungen, finanzielle Situation der Familie usw., in eine hohe Verantwortung nimmt. In ähnlicher Weise müssen auch Informationen über den Lehrkörper und andere universitätsnahe Organisationen sowie Forschungsergebnisse sicher aufbewahrt werden.

Während des Onboarding-Prozesses müssen Studenten, Familien und Dozenten auf verschiedene Systeme und Anwendungen

zugreifen, z. B. auf das Studentenportal, die Online-Bibliothek, Assessment-Center, Daten des Forschungszentrums, etc. Diese Systeme müssen konsistent, konvergent, sicher und einfach zu bedienen sein sowie Provisioning-Funktionen in den IT-Infrastrukturen bieten.

Verstärkter Einsatz von Technologie in den Klassenzimmern

Auch die Klassenzimmer haben sich von einer traditionellen zu einer digitalen Umgebung entwickelt. Online-Portale bieten digitale Inhalte an und Aufgaben werden manchmal online eingereicht. Die Schüler müssen Dateien austauschen und in ihrer Arbeit stärker kollaborieren, was den Bedarf an digitalen Werkzeugen erhöht. Erschwerend kommt hinzu, dass sich immer mehr Professoren oder Studenten mittels ihrer persönlichen Geräten (BYOD) mit dem Netzwerk verbinden, was wiederum die Angriffsfläche der Bildungseinrichtungen vergrößert. Die Institutionen müssen jedoch vom ersten Tag an einen einfachen und sicheren Zugang zu kollaborativen Online-Ressourcen bieten.

Einhaltung gesetzlicher Vorschriften

Der Datenschutz und die Einhaltung gesetzlicher Vorschriften betreffen den Bildungssektor genauso wie andere Branchen. Standards und Vorschriften wie ISO 27001 oder GRPD, aber auch die Einhaltung der staatlichen Sicherheitspolitik für Informationssysteme schreiben Identitäts- und Zugriffssicherheit vor, während die Labels CyberEdu und SecNumedu auch eine Referenz für die Ausbildung im Bereich der digitalen Sicherheit darstellen.

Schließlich bleibt eine strenge, aber granulare Kontrolle des privilegierten Zugriffs ein Schlüsselelement der meisten Maßnahmen zur Einhaltung gesetzlicher Vorschriften, ebenso wie die Gewährleistung der Nachvollziehbarkeit von Aktionen für IT-Teams im Falle eines Audits.

Multiple Community Management und Datensicherheit

Sicherheitsvorfälle in Informationssystemen unterliegen oftmals Versuchen, unberechtigt Wissen zu erlangen, sensible Informationen zu verändern oder zu zerstören. Ihre Auswirkungen können von einem

mehrstündigen oder gar längeren Systemausfall, über den Diebstahl persönlicher Daten, die Schädigung der Reputation einer Institution und das Vertrauens in ihre IT-Dienste, der Kompromittierung von Personen, insbesondere Minderjährige, bis hin zur Unmöglichkeit, bestimmte wesentliche Aufgaben der öffentlichen Dienste zu gewährleisten, reichen.

Datenschutzverletzungen und andere Sicherheitsbedrohungen, wie etwa immer komplexere Cyberangriffe, zwingen die IT-Abteilungen von Universitäten und Bildungseinrichtungen dazu, robustere Authentifizierungsmethoden zu implementieren.

Neben den Mitgliedern der Kerngemeinschaft (z. B. Dozenten, Studenten und Mitarbeiter) gibt es auch externe Mitglieder: Studenten, die über E-Learning-Plattformen Online-Kurse ohne Leistungsnachweis belegen und sich vielleicht auf einem anderen Kontinent befinden sowie Drittparteien wie IT-Anbieter und Anwendungsanbieter. Alle benötigen von Zeit zu Zeit Zugang zu Universitätssystemen. Die Hochschule oder Schule muss daher wissen, in welcher Beziehung eine Person zu der betreffenden Organisation steht, und die Berechtigungen entsprechend und mit feiner Granularität vergeben.

Um diese Herausforderungen zu meistern, ist die Implementierung eines Identitäts- und Zugriffsmanagements notwendig, einschließlich der Feinabstimmung privilegierter Konten, die gleichzeitig nicht zu Lasten des Benutzerkomforts und der Produktivität gehen darf.

Wie Identitäts- und Zugriffsmanagement diese Herausforderungen angeht

Identitäts- und Zugriffsmanagement ist der Prozess der sicheren Kontrolle des Zugriffs auf Ressourcen, insbesondere auf sensible Ressourcen. Eine bessere Lösung für das Identitäts- und Zugriffsmanagement kann fast alle der oben beschriebenen Herausforderungen lösen.

Sicherer und einfacher Zugriff auf Anwendungen und Systeme durch eine starke und adaptive Authentifizierung

Eine typische Identitäts- und Zugriffsmanagementlösung muss einen

Benutzer mit seinem Namen und Passwort authentifizieren und seine persönlichen Informationen sowie Privilegien sicher verwalten. In Bildungseinrichtungen verwaltet es Studenten- und Mitarbeiterinformationen an einem zentralen Ort und bietet ein reibungsloses Anmeldeverfahren.

Externe Communities können auch an einer Stelle verwaltet werden, indem separate Rollen und Berechtigungen zugewiesen werden. Diese Lösungen bieten personalisierte und einfach zu handhabende Benutzerverfahren durch vernetzte Identitäten mit Single Sign-On und Logins für Studenten und Dozenten, Eltern und alle internen oder externen Anbieter, die erweiterte Berechtigungen benötigen, um automatisierte Prozesse zu implementieren und Netzwerke, Dienste und Anwendungen zu verwalten - und das alles bei gleichzeitiger Beseitigung von Zugangssilos zwischen allen angebotenen Diensten.

Der Zugriff auf Anwendungen wird vereinfacht, da sich der Benutzer nicht für jede Anwendung neu authentifizieren muss. Die Lösungen helfen auch dabei, Daten vor Ausspähung zu schützen. Alle Daten werden erst nach der Authentifizierung beim Identitätsprovider von einer zentralisierten Architektur aus freigegeben. Ein doppelter Authentifizierungsfaktor ist ebenfalls sehr empfehlenswert. In ähnlicher Weise schützt die Sicherung privilegierter Konten den Zugang zu kritischen IT-Infrastrukturen.

Absicherung des Fernzugriffs

Traditionelle VPN-Lösungen, die Remote-Verbindungen ermöglichen, sind aus Gründen der Kosten, der Komplexität und der Heterogenität der IT-Assets im Bildungssektor immer weniger relevant. Remote-Sitzungen benötigen jedoch das gleiche Maß an Kontrolle, Genehmigung, Verfolgung und Überwachung wie bei Inhouse-Sitzungen.

Die eingesetzten Lösungen müssen es den IT-Verantwortlichen daher ermöglichen, ihre Remote-Benutzer so zu überwachen, zu auditieren und zu kontrollieren, als ob sie sich auf dem Schulgelände oder Universitätscampus befinden.

Schützen Sie anfällige Endpunkte

Ransomware, Malware und Kryptoviren

müssen ebenfalls daran gehindert werden, in das Netzwerk einzudringen, selbst wenn Benutzer über erhöhte Rechte verfügen. Umso wichtiger ist es, Lösungen einzusetzen, die Privilegien auf Anwendungs- und Prozessebene kontrollieren und Verschlüsselungsvorgänge mit Endpunktschutztechnologien unterbinden. Durch den Entzug von Benutzerrechten auf Endpunkten und die Überwachung und Blockierung der kritischsten Prozesse auf den Rechnern können Schulen, Hochschulen und Universitäten die Verbreitung von Malware verhindern, die versucht, von einem mit dem Netzwerk verbundenen Endpunkt aus zu starten.

Entwicklung von Just-in-Time (JIT) & Zero Standing Privileges Prinzipien

Just-in-Time (JIT) und Zero Standing Privileges-Prinzipien sind die besten Methoden, um die IT-Ressourcen von Schulen und Universitäten zu schützen und sicherzustellen, dass die richtigen Benutzer - Verwaltungsmitarbeiter, Lehrkräfte, IT-Spezialisten - zur richtigen Zeit und für den richtigen Zweck Zugriff auf die richtigen Ressourcen haben.

Privilegien werden nur gewährt, wenn dies notwendig ist, um die Angriffsfläche zu reduzieren, die interne Bedrohung zu minimieren und eine starke Sicherheitsrichtlinie zum Schutz sensibler IT-Ressourcen zu implementieren.

Auch die Risiken, die mit der Vergabe von Administratorrechten verbunden sind, werden reduziert, ohne das IT-Personal zu überfordern. Privilegierter Zugriff auf Systeme wird nur bei Bedarf gewährt, basierend auf dem Prinzip des geringsten Privilegs, nicht mehr und nicht weniger. Und die Berechtigungssteuerung erfolgt transparent und granular auf der Anwendungsebene, während die Benutzer effizient arbeiten können

Sichere Passwörter

Die Fluktuation von Dozenten, sorglosen Studenten und Fremdadministratoren trägt immer noch dazu bei, dass weiterhin zu oft Passwörter auf Post-it-Notizen geschrieben oder in ungesicherten Excel-Dateien gespeichert werden, oder schlimmer noch, im Klartext aufgezeichnet werden und für jeden in einem Raum zugänglich sind.

Die sichere Aufbewahrung von Zugangsdaten in einem kontrollierten Tresor und der Schutz von Passwörtern vor Diebstahl und Weitergabe durch eine ausgefeilte Verschlüsselung ist daher in diesen erweiterten Umgebungen von größter Bedeutung. Hohe Passwortsicherheitskontrollen sowie eine Anwendung-zu-Anwendung-Passwortverwaltung für eine strenge Kontrolle von privilegierten Zugangsdaten sind ebenfalls wichtige Sicherheitsüberlegungen für IT-Abteilungen im Bildungswesen.

Verwalten und Einhalten von Vorschriften

Wie bereits erwähnt, kann eine ordnungsgemäß verwaltete und eingesetzte Privilegienmanagement-Lösung den unbefugten Zugriff auf sensible Serversysteme verhindern, durch den sich Hacker Zugang zu Netzwerken verschaffen und Daten gefährden.

Im Falle eines Angriffs ist es außerdem wichtig, dass die Sicherheitsverantwortlichen von Universitäten und Hochschulen genau feststellen können, was, wann und von wem begangen wurde. Diese Lösungen helfen bei der cyberforensischen Aufzeichnung und Bereitstellung von Informationen sowie zur Einhaltung der entsprechenden Vorschriften, um zu erfahren, wie Angriffe durchgeführt wurden.

Aber während die Sicherstellung der Nachvollziehbarkeit des Zugriffs auf Daten und die IT-Infrastruktur zu einem wichtigen Thema geworden ist, geht es nicht nur um die Installation von Software.

Die Aufrechterhaltung der Systemsicherheit und Compliance ist ein fortlaufender Prozess. Für die Akteure des Bildungssektors ist es wichtig, sich einer regelmäßigen Optimierung der implementierten Lösungen zu versichern und so den Nutzen ihrer Anfangsinvestition zu maximieren. Wenn Sie sich mit Experten für Identitäts- und Berechtigungsmanagement umgeben, können Sie auch bei der Reaktion auf Änderungen der gesetzlichen Compliance-Anforderungen, der Sicherung von Endpunkten, der Bereitstellung von Fat Clients oder der Erstellung von Plugins unterstützt werden.

Fazit

Schulen und Universitäten müssen sich proaktiv mit Bedrohungen auseinandersetzen und für die Prävention von Cyberangriffen planen, mit Erkennungsfunktionen sowie Reaktions- und Analysefunktionen im Falle eines Cyberangriffs.

Unter all den Herausforderungen, die im Bildungsbereich zu bewältigen sind, wird das Identitätsmanagement, der sichere Zugang dank robuster Sicherheitstechnologien, wie Single- oder sogar Multi-Faktor-Authentifizierung, Privileged Access Management und Endpoint Privilege Management, die Welt der Bildung in die Lage versetzen, ihre digitale Transformation sicher fortzusetzen.

Die Lösungen sind da – für eine sichere Ausbildung im digitalen Zeitalter.

Über WALLIX

Die WALLIX-Lösungen schützen verlässlich vor Cyberbedrohungen, Datendiebstahl und Datenmanipulation, hauptsächlich verursacht durch gestohlene Identitäten oder veruntreute Zugriffskonten. Die Lösungen werden weltweit über ein Netzwerk von mehr als 180 Systemintegratoren und Fachhändlern vertrieben. Als Euronext-notiertes Unternehmen begleitet WALLIX mehr als 1000 Unternehmen auf ihrem Weg in eine sichere digitale Zukunft.

WWW.WALLIX.COM

WALLIX
CYBERSECURITY SIMPLIFIED