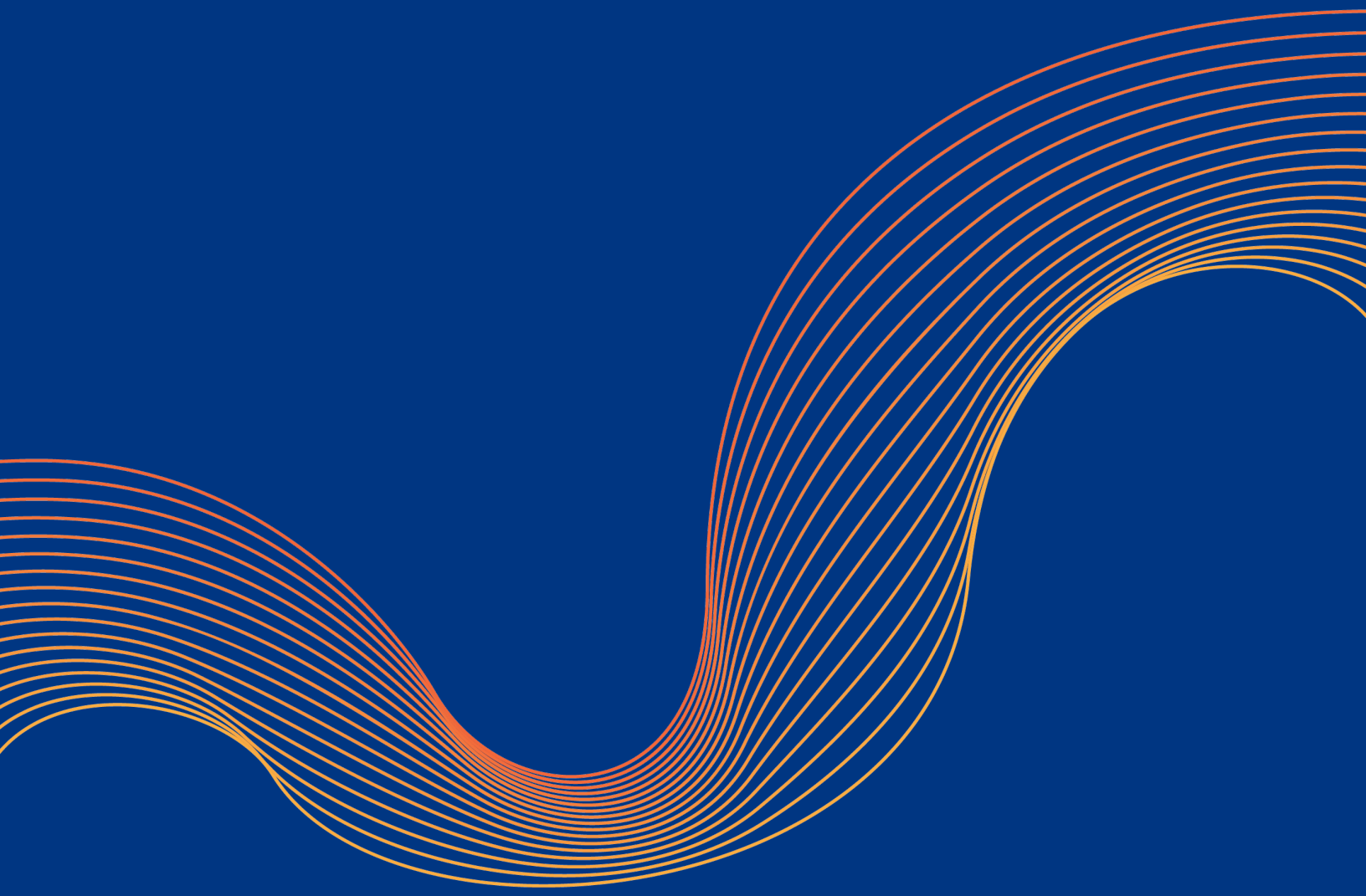
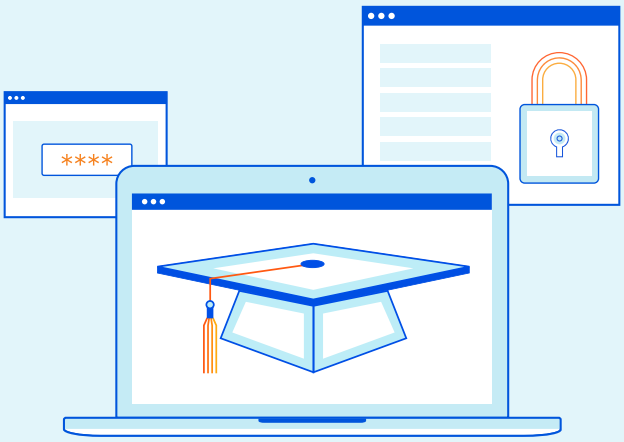
WHITEPAPER

CLOUDFLARE

Merkmale einer sicheren und skalierbaren Infrastruktur für den Fernunterricht



+49 89 2555 2276 | enterprise@cloudflare.com | www.cloudflare.com/de-de/



Einleitung

Die Vermittlung von Wissensinhalten per Fernunterricht ist ein Modell, das sich seit einigen Jahren steigender Beliebtheit erfreut. Zusätzlichen Auftrieb erhielt es durch die Covid-19-Pandemie: Die Notwendigkeit, Schüler und Studierende ebenso wie Lehrer und Dozenten vor dem Virus zu schützen, beschleunigte den Übergang zu Lösungen, die sich ganz oder zumindest teilweise auf Distance Learning stützen.

Die Anforderungen dieses Modells unterscheiden sich allerdings deutlich vom Präsenzunterricht: Das Lehrpersonal muss die Möglichkeit haben, auf eine breite Palette von Lernstilen einzugehen und unterschiedliche Formate zu kombinieren: Vorlesungen, Videos, interaktive Inhalte und mehr. Außerdem müssen die Lernenden schnell und gleichzeitig auf die ihnen zur Verfügung gestellten Ressourcen zugreifen können.

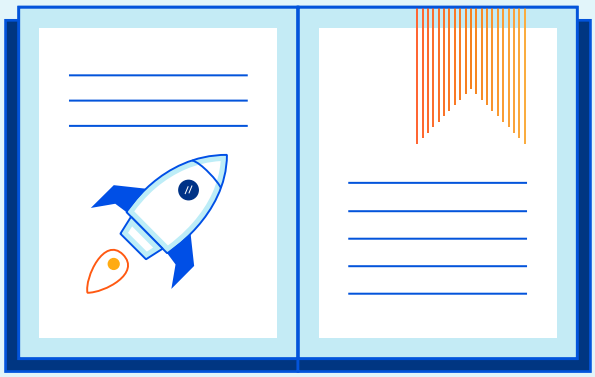
Bildungseinrichtungen müssen deshalb auch die technischen Voraussetzungen zur Unterstützung dieser großen Bandbreite an Inhaltstypen schaffen und gewährleisten, dass ihre Systeme funktionieren, wann immer die Schüler und Studierenden sie benötigen. Dafür müssen sie unter anderem folgende Herausforderungen meistern:

- Skalierbarkeit der Inhaltsbereitstellung
- Schutz vor DDoS-Angriffen
- Vermeidung von Kontoübernahmen
- Schutz vor bösartigen Inhalten und Malware

Skalierbarkeit der Inhaltsbereitstellung

Ob es einer Bildungseinrichtung gelingt, einen funktionierenden Lehrbetrieb per Fernunterricht sicherzustellen, hängt ganz entscheidend von ihrer IT-Infrastruktur ab. Das Lehrpersonal muss die Möglichkeit haben, seine Inhalte vielen Lernenden gleichzeitig zur Verfügung zu stellen, ohne dass es bei der Übertragung zu übermäßiger Latenz kommt.

Darüber hinaus muss gewährleistet sein, dass der Lehrstoff in verschiedenen Formaten bereitgestellt werden kann, also nicht nur als statische Webseiten, sondern auch in Form von dynamischen Inhalten, zum Beispiel als interaktive Online-Lerntools oder als gestreamte Videos. All das funktioniert nur, wenn die IT-Infrastruktur der betreffenden Einrichtung in der Lage ist, die Inhalte mit der nötigen Effizienz und Skalierbarkeit anzubieten.



Statische Inhalte

Zum Teil geht es im Lehrbetrieb um statische Inhalte, also insbesondere um Webseiten mit Informationen, die sich nicht ändern und nur selten aktualisiert werden müssen.

Was die technischen Voraussetzungen betrifft, bilden dabei die Skalierbarkeit und die Vermeidung von Latenz die größten Herausforderungen: Verkraftet es der Webserver, wenn mehrere Schüler oder Studierende versuchen, gleichzeitig auf dieselben Ressourcen zuzugreifen? Auch der Serverstandort kann in diesem Zusammenhang eine wichtige Rolle spielen, denn je weiter der Lernende vom Server entfernt ist, desto höher fällt die Latenz bei der Inhaltsbereitstellung aus.

Diese Schwierigkeiten mit statischen Inhalten lassen sich durch lokale Zwischenspeicherung im Cache verringern: Ruft ein Lernender eine bestimmte Seite häufig auf, liegt diese möglicherweise schon vor Ort als Kopie vor und kann entsprechend schnell bereitgestellt werden.

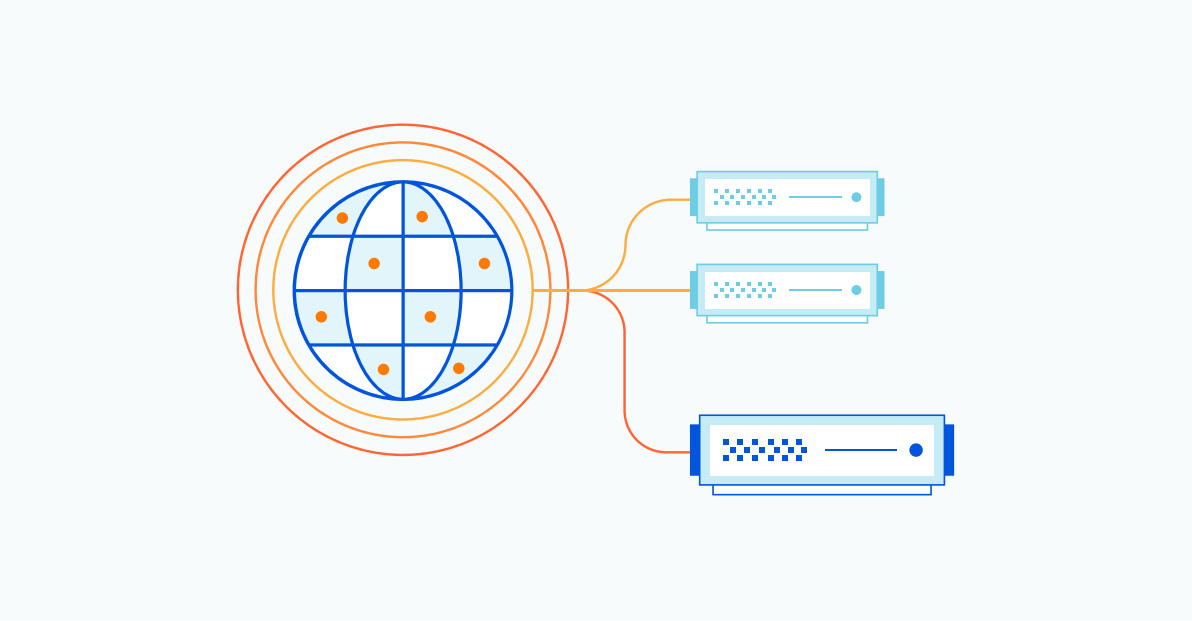
In einem größeren Rahmen kann das Prinzip des Caching mit einem Content Distribution Network (CDN) umgesetzt werden.Ein CDN besteht aus miteinander verbundenen Netzwerkknoten, die Kopien statischer Inhalte lokal zwischenspeichern und in regelmäßigen Abständen aktualisieren. Ein weltumspannendes CDN gewährleistet die nötige Skalierbarkeit und geringe Latenz, um effektiven Fernunterricht anbieten zu können.

Dynamische und interaktive Inhalte

Wie bei statischen Inhalten besteht auch bei anderen und insbesondere bei interaktiven Online-Lernressourcen die Gefahr, dass bei einer Skalierung Probleme auftreten. Allerdings ist der beschriebene Einsatz miteinander verbundener Netzwerkknoten in diesem Fall nicht die beste Lösung. Denn wenn es um Inhalte geht, die häufig oder fast ständig auf den neuesten Stand gebracht werden müssen, würden die CDN-Knoten beim zentralen Webserver kontinuierlich Aktualisierungen anfordern. Bei den Benutzern würde sich das in Form einer höheren Latenz bemerkbar machen, außerdem bestünde die Gefahr einer Überlastung des zentralen Webservers.

Der Ansatz der Lastverteilung (Load Balancing) ist deutlich besser geeignet, Schwierigkeiten mit der Skalierbarkeit bei der Bereitstellung von dynamischen Inhalten zu lösen. Dabei setzt man zur Bearbeitung der Anfragen der Lernenden nicht einen einzelnen Server ein, sondern mehrere, die den Datenverkehr unter sich aufteilen. Dies verhindert die Überlastung eines einzelnen Servers und minimiert die Latenz.

Damit ein Server effektiv mit Load Balancing betrieben werden kann, muss er vollkommen unabhängig agieren können oder sich ausschließlich auf andere Hardware stützen, die ebenfalls der Lastverteilung unterliegt. Wenn alle Server so konfiguriert sind, dass sie denselben Datenbankserver nutzen, kann es sein, dass sich dieser zum Nadelöhr für die Daten entwickelt und die zusätzlichen Server trotz Load Balancing wenig oder keinen Nutzen bringen. Fernunterrichtslösungen erfordern ein durchdachtes Konzept mit bedarfsgerechter Skalierbarkeit. Außerdem benötigen sie eine Systemarchitektur, die es erlaubt, die Vorteile des Load Balancing vollständig auszuschöpfen.

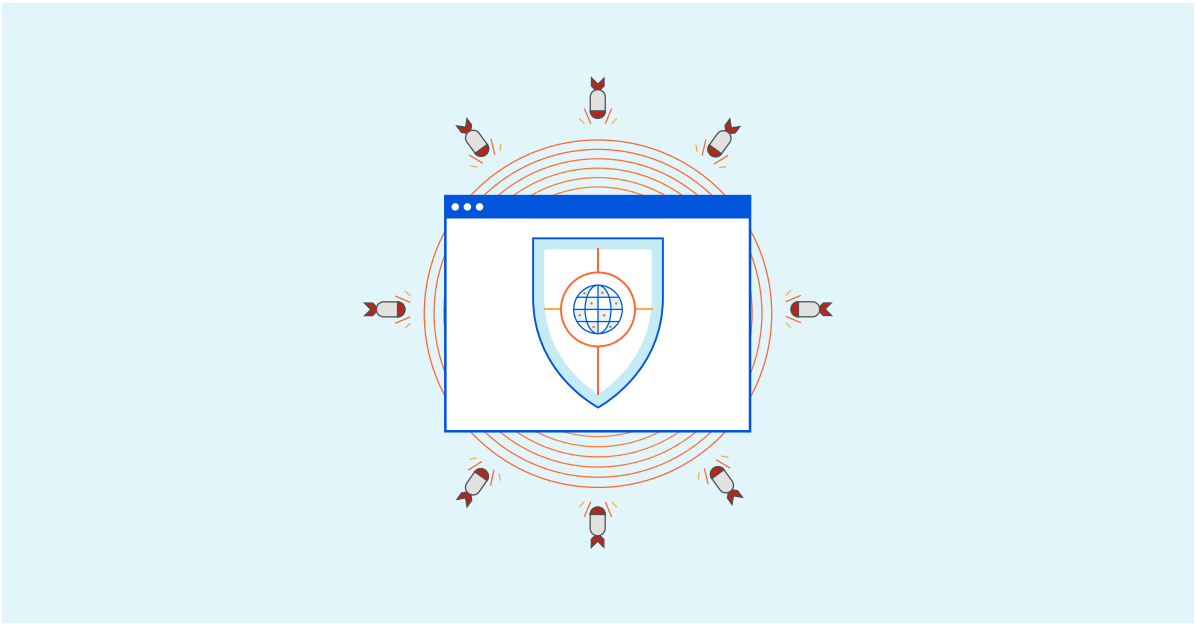


DDoS-Angriffe

Die Häufigkeit von DDoS-Angriffen (Distributed Denial of Service) hat zugenommen. Das hat auch damit zu tun, dass es Cyberkriminellen in Zeiten, in denen das Internet der Dinge (Internet of Things, IoT) und Cloud Computing die Welt erobern, immer leichter fällt, sich kostengünstig Zugang zu Online-Rechenleistung zu verschaffen. Die entsprechend kompromittierten Geräte können die Hacker dann dazu verwenden, einen Service derart mit bösartigem Datenverkehr zu beschäftigen, dass er auf legitime Anfragen nicht mehr reagieren kann.

Auch bei Fernunterrichtslösungen besteht ein beträchtliches Risiko, dass DDoS-Angriffe die Bereitstellung entsprechender Dienste sabotieren. Als viele Bildungseinrichtungen in der ersten Hälfte des Jahres 2020 auf Distance Learning umstellten, verzeichnete man einen Anstieg der DDoS-Angriffe auf ihre Online-Angebote um 350 %.[1]

Hinzu kommt, dass DDoS-Angriffe heute zum Teil mit Erpressungsversuchen kombiniert werden: Der Angreifer verlangt ein Lösegeld und droht mit einem DDoS-Angriff, wenn die betroffene Institution nicht zahlt. Zwar entbehren viele dieser Drohungen jeder Grundlage, aber wenn es an einem wirksamen DDoS-Schutz fehlt, sehen sich Bildungseinrichtungen aufgrund des hohen Risikos für ihre Infrastruktur möglicherweise gezwungen, auf die Forderung einzugehen.

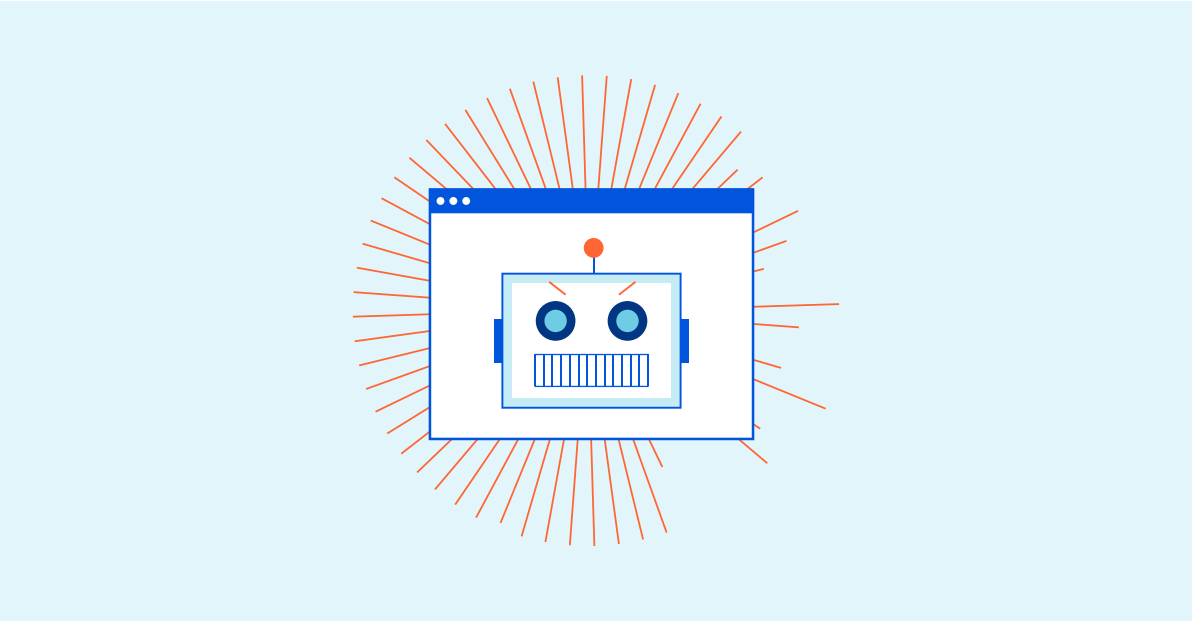


Glücklicherweise stehen selbst Einrichtungen mit relativ knapp kalkulierten Budgets verschiedene Wege zur effektiven Bekämpfung von DDoS-Attacken offen. Dabei sollten sie auf die folgenden Punkte achten:

- Großzügige Bemessung der Abwehrkapazitäten: Es ist verständlich, dass Institutionen aus Kostengründen auf eine bedarfsgerechte Lösung achten. Wenn es dann allerdings zu einem unerwartet schweren Angriff kommt, verursacht ein entsprechendes Upgrade der Dienste möglicherweise zusätzliche Ausfallzeiten.
- Verteilte Abwehr: Das „Scrubbing“ genannte Herausfiltern des DDoS-Traffics sollte dezentral erfolgen; wenn nämlich der gesamte Datenverkehr einer Organisation zu diesem Zweck über einen einzigen zentralen Punkt im Netzwerk umgeleitet wird, fehlt es möglicherweise an der nötigen Skalierbarkeit und die Latenz nimmt zu.
- Abwägung zwischen einer On-demand- und einer Always-on-Lösung: Bei einer On-Demand-Abwehr von DDoS-Angriffen erfolgt der Datenaustausch zwischen den Servern oder der Netzwerkinfrastruktur einer Einrichtung und dem öffentlichen Internet wie gewohnt. Erst wenn ein potenzieller Angriff erkannt wird, kommt es zu einer gründlichen Untersuchung und Filterung des Traffics. Demgegenüber wird der gesamte Datenverkehr bei einer Always-on-Option rund um die Uhr gefiltert. Dieser Ansatz ist zwar üblicherweise teurer als die Abwehr auf Abruf, er bietet aber auch kontinuierlichen Schutz sowie kürzere Reaktionszeiten, weil der Service nicht erst manuell aktiviert werden muss.

Unser E-Book „Fünf Best Practices zur Abwehr von DDoS-Angriffen“ im Cloudflare-Ressourcen-Hub bietet Ihnen weitere Informationen zu DDoS-Abwehrstrategien.

[1] *https://www.infosecurity-magazine.com/news/ddos-attacks-on-virtual-education/*



Kontoübernahmen

Viele Cyberangriffe beginnen damit, dass legitime Benutzerkonten eines Systems gekapert werden. Bei diesen Kontoübernahme-Angriffen geraten die Daten, mit denen sich ordnungsgemäß registrierte Benutzer bei einem Netzwerk, einer Anwendung oder anderen Systemen anmelden, in die falschen Hände. Um an diese Login-Informationen zu kommen, bedienen sich Cyberkriminelle verschiedener Methoden wie Phishing-Angriffen oder Credential Stuffing.

Mit den erbeuteten Daten können die Angreifer sich als legitime Benutzer ausgeben und ihren Machenschaften im Zielsystem nachgehen, indem sie zum Beispiel Schadcode einschleusen oder Daten stehlen. Unter anderem besteht die Gefahr, dass Daten, die durch die Datenschutz-Grundverordnung geschützt sind, auf diese Weise in die Hände von Kriminellen gelangen. Denkbar ist zum Beispiel auch, dass die Angreifer wichtige Datensätze von Schülern oder Studierenden löschen oder erst nach Zahlung eines Lösegeld wieder freigeben.

Angesichts dieser Risiken sollten Bildungseinrichtungen eine Phishing-Abwehrlösung einsetzen, die Angriffe nicht nur auf der Grundlage bekannter bösartiger Inhalte erkennt, sondern auch verdächtige Ausdrucksweisen und andere bislang unbekannte Bedrohungen mithilfe von maschinellem Lernen identifiziert. Ein geeigneter Ansatz ist das E-Mail-Scanning, ein weiterer ist die Verwendung eines sicheren Web-Gateways, das bösartige Websites blockiert und Benutzer am Herunterladen bestimmter Dateitypen hindert.

Credential Stuffing

Auch die öffentlich zugänglichen Anmeldesysteme von Institutionen – ihre virtuellen privaten Netzwerke (VPNs), das Remote Desktop Protokoll (RDP) oder ihre Online-Zugangsportale – bieten Cyberkriminellen Möglichkeiten, die Anmeldedaten legitimer Nutzer herauszufinden. Im Durchschnitt verwendet jeder Anwender dieselben Login-Daten für 13 Online-Konten[2] und viele nutzen unsichere Passwörter, die sich leicht erraten lassen. Beim Credential Stuffing werden Bots eingesetzt, die versuchen, das Passwort eines Benutzers auf diesen Authentifizierungsportalen zu ermitteln. Wenn dies gelingt, kennt der Angreifer die Anmeldedaten des Benutzers und kann auf dessen Account zugreifen.

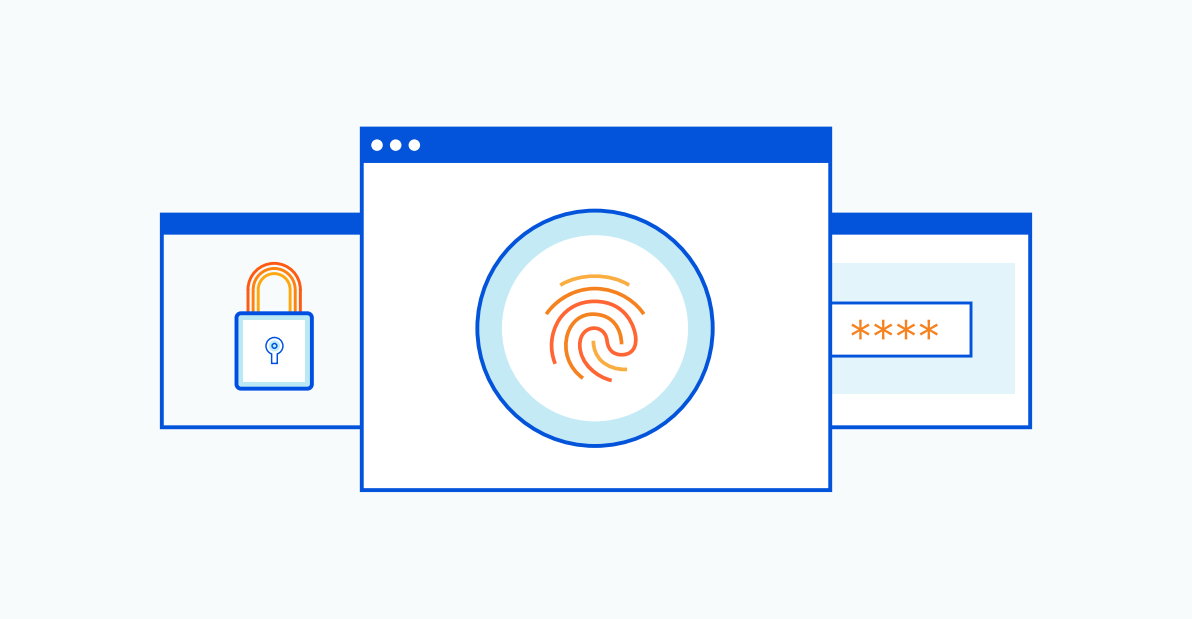
[2] *https://www.lastpass.com/state-of-the-password/global-password-security-report-2019*

Da Credential Stuffing-Angriffe auf Automatisierungen beruhen, müssen Lösungen zur Abwehr dieser Art von Attacken erkennen können, wenn ein Bot aktiv ist. Genauso wichtig ist aber auch die Unterscheidung zwischen hilfreichen und bösartigen Bots.

Die Bandbreite an Methoden zur Identifizierung und Blockierung von bösartigen Bots ist groß, einige Ansätze sind allerdings grundlegend:

- **Durchsatzratenbegrenzung (Rate Limiting):** Begrenzung der Häufigkeit, mit der von ein und derselben IP-Adresse Anfragen an eine Website oder ein Netzwerk gesendet werden können. Dies ist eine effektive Lösung zur Verteidigung gegen Bots, die einfachere Brute-Force-Angriffe durchführen.
- **CAPTCHAs und Zwei-Faktor-Authentifizierung:** Diese beiden Taktiken halten viele Bots komplett von Login-Seiten fern, allerdings können sie auch die Nutzererfahrung beeinträchtigen.
- **Pflege einer Blockier- und Genehmigungsliste für Bots:** Bereits bekannte bösartige Bots können so in Schach gehalten werden, während gleichzeitig gewährleistet ist, dass die Crawler von Suchmaschinen und andere sinnvolle Bots ihre Funktion weiterhin erfüllen können.

Es kann allerdings sein, dass sich diese Lösungen bei besonders raffinierten und spezialisierten Bots als nicht sonderlich wirkungsvoll erweisen. Wenn Sie mehr über die Bot-Abwehr erfahren möchten, empfehlen wir Ihnen das „Malicious Bot Playbook“ (engl.) im Cloudflare-Ressourcen-Hub.

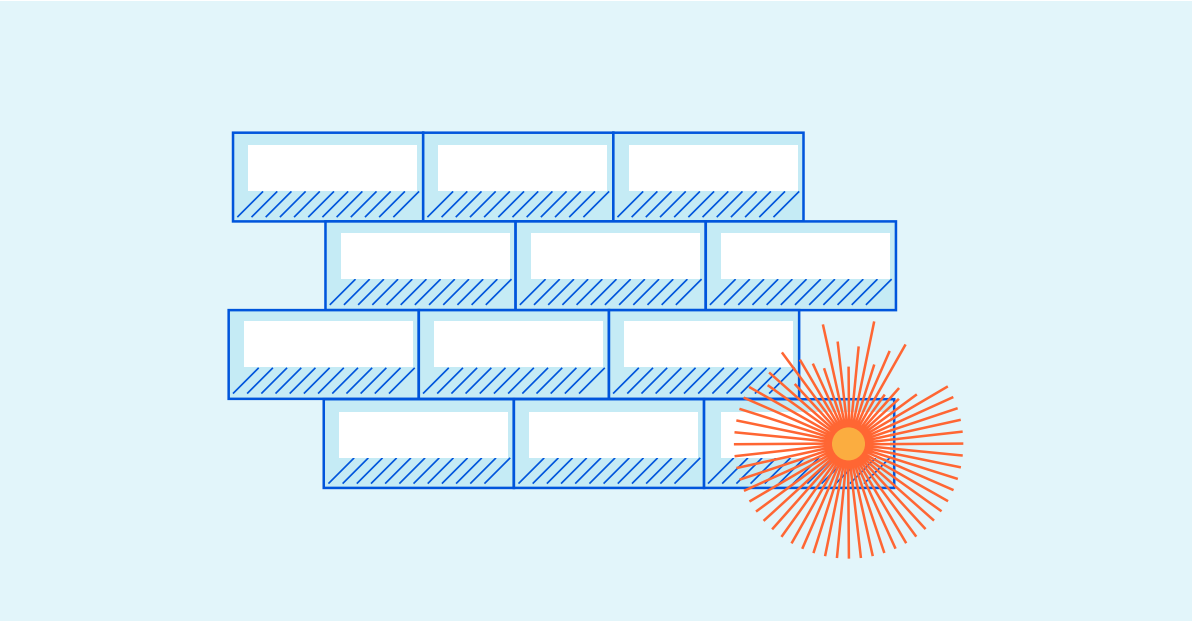


Bösartige Inhalte und Malware

Immer mehr Bildungseinrichtungen setzen auf Fernunterricht und dementsprechend ist auch eine wachsende Anzahl von Systemen mit dem öffentlichen Internet verbunden. Die Lernenden greifen verstärkt auf Webanwendungen zurück, um von den Online-Lernangeboten profitieren zu können. Gemeinsam mit dem Lehrpersonal setzen sie außerdem VPNs, RDP und ähnliche Lösungen für den Remote-Zugriff auf Netzwerke und Rechner ein. Alle diese Systeme müssen vor Cyberbedrohungen geschützt werden.

Absicherung von Internetanwendungen

Manche Internetanwendungen im Bildungsbereich erfassen die verschiedensten vertraulichen Daten. Es ist durchaus denkbar, dass diese Plattformen Informationen speichern, die unter die Datenschutz-Grundverordnung oder vergleichbare Gesetze fallen. Deshalb müssen Bildungseinrichtungen ihre Systeme unbedingt ordnungsgemäß absichern.



Wie jede andere Software können auch Internetanwendungen Sicherheitslücken aufweisen, die Hacker unter Umständen für ihre Zwecke instrumentalisieren. Um Applikationen vor Cyberangriffen zu schützen, muss der Datenverkehr des Netzwerks untersucht werden, damit jegliche Versuche, diese Softwarefehler auszunutzen, erkannt und blockiert werden können.

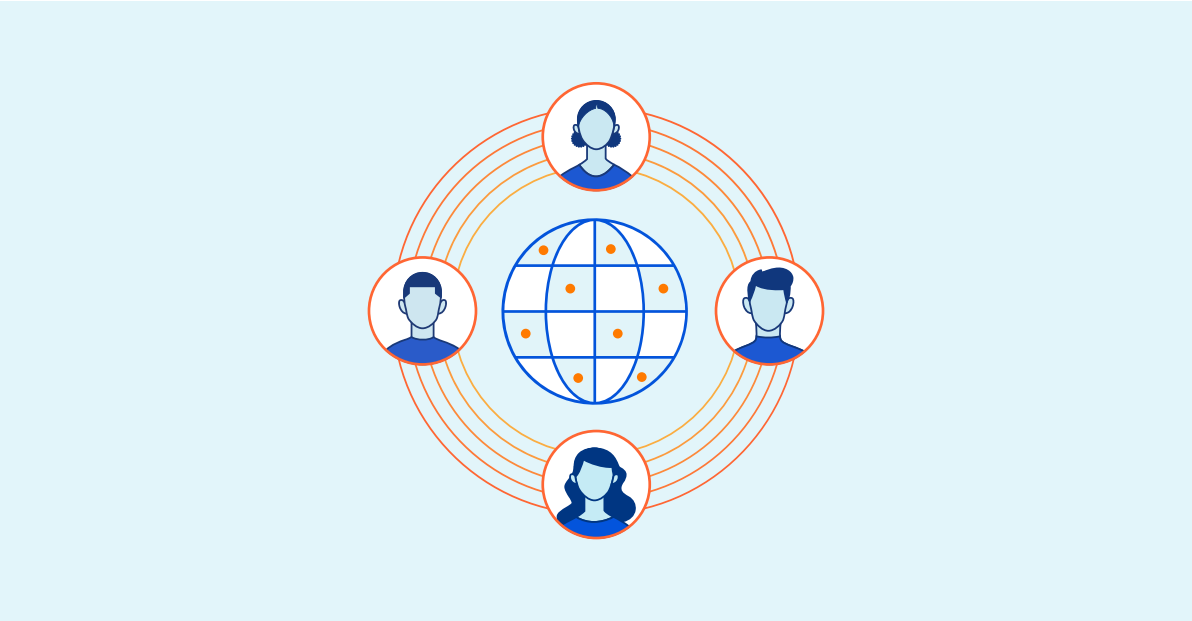
Eine Web Application Firewall (WAF) schirmt eine Vielzahl von Schwachstellen in Webanwendungen ab. Indem sie Attacken sowohl mithilfe von Signaturen als auch durch maschinelles Lernen aufdeckt, kann sie bereits bekannte und neuartige Angriffsarten gleichermaßen identifizieren. So gelingt es, sogar Zero Day-Angriffe auf die webbasierte Infrastruktur einer Institution erfolgreich abzuwehren.

Schutz vor Ransomware

Ransomware gehört zu den Malware-Bedrohungen, die sich derzeit besonders schnell ausbreiten. Wenn eine Ransomware einen Computer befallen hat, verschlüsselt sie die auf dem Rechner gespeicherten Dateien. Dem Nutzer wird mitgeteilt, dass er nur nach Zahlung eines Lösegeld wieder auf seine Daten zugreifen kann. Selbst wenn eine Bildungseinrichtung die nötigen Mittel hat, um die Zahlung sofort zu leisten, kostet es oft auch viel Zeit und Geld, die betroffenen Systeme wiederherzustellen.

Immer häufiger dienen Fernzugriffstechnologien wie VPNs und RDP als Einfallstor für Ransomware. Kennt ein Angreifer die Anmeldedaten eines legitimen Nutzers, kann er sich bei einem Computer einloggen und die Malware installieren. Sobald der Schadcode von dort aus in das Netzwerk der Organisation gelangt ist, verbreitet er sich üblicherweise weiter, indem er weitere Rechner infiziert.

Bildungseinrichtungen benötigen eine Firewall-Lösung, mit der sie den gesamten geschäftlichen Datenverkehr ihrer Netzwerke überprüfen können. Auf diese Weise können sie Ransomware und anderen eingehenden Schadcode erkennen, bevor ihre Computer infiziert werden, sowie Datendiebstahl und insbesondere den Verlust schützenswerter personenbezogener Daten der Lernenden verhindern.



Sicheres Distance Learning mit Cloudflare

Die Covid-19-Pandemie wird irgendwann Geschichte sein, doch die Fähigkeit, den Lehrbetrieb ohne großen Aufwand auf Fernunterricht umzustellen, wird sich für Bildungseinrichtungen auch in Zukunft als wertvoll erweisen. Nicht zuletzt können online angebotene Lernressourcen auch Präsenzveranstaltungen sinnvoll ergänzen. Zudem ist eine Einrichtung mit einer Fernunterricht erlaubenden Infrastruktur gut gewappnet, wenn es wegen schlechten Wetters oder anderer unvorhergesehener Ereignisse zu Störungen des Lehrbetriebs vor Ort kommt.

Die konsolidierte und benutzerfreundliche Plattform von Cloudflare erlaubt es Bildungseinrichtungen, alle Herausforderungen im Bereich IT und Sicherheit zu bewältigen, mit denen sie üblicherweise zu tun haben. Mit einer solchen zentralen und integrierten Lösung vermeiden diese Institutionen unnötige Komplexität. Außerdem sichern sie sich Anpassungs- und Widerstandsfähigkeit, um auch auf überraschende Szenarien reagieren zu können. Das Angebot von Cloudflare umfasst:

- **ein globales Content Delivery Network** mit Rechenzentren in mehr als 200 Städten in aller Welt
- **47 Tbit/s DDoS-Abwehrkapazität** mit einem rund um die Uhr aktiven Schutz am Netzwerkrand
- **eine Web Application Firewall**, die kontinuierlich mit Bedrohungsinformationen der ca. 25 Millionen Websites des Cloudflare-Netzwerks aktualisiert wird
- **eine erweiterte Bot-Abwehr**, die den Datenverkehr unseres Netzwerks mithilfe von maschinellem Lernen und Fingerprinting auf bestimmte Muster hin analysiert und auch die raffiniertesten Bots identifiziert
- **ein sicheres Web-Gateway**, das am Netzwerkrand betrieben wird und damit die Latenz vermeidet, die beim Backhauling des Datenverkehrs zu einem Rechenzentrum in weiter Ferne entstehen würde

Unter www.cloudflare.com/de-de/ erfahren Sie mehr.