OctoGate
EINFACH. SICHER. GESCHÜTZT.

Sicheres WLAN an Schulen

OG

OctoGate IT Security Systems GmbH
Friedrich-List-Str. 42
33100 Paderborn

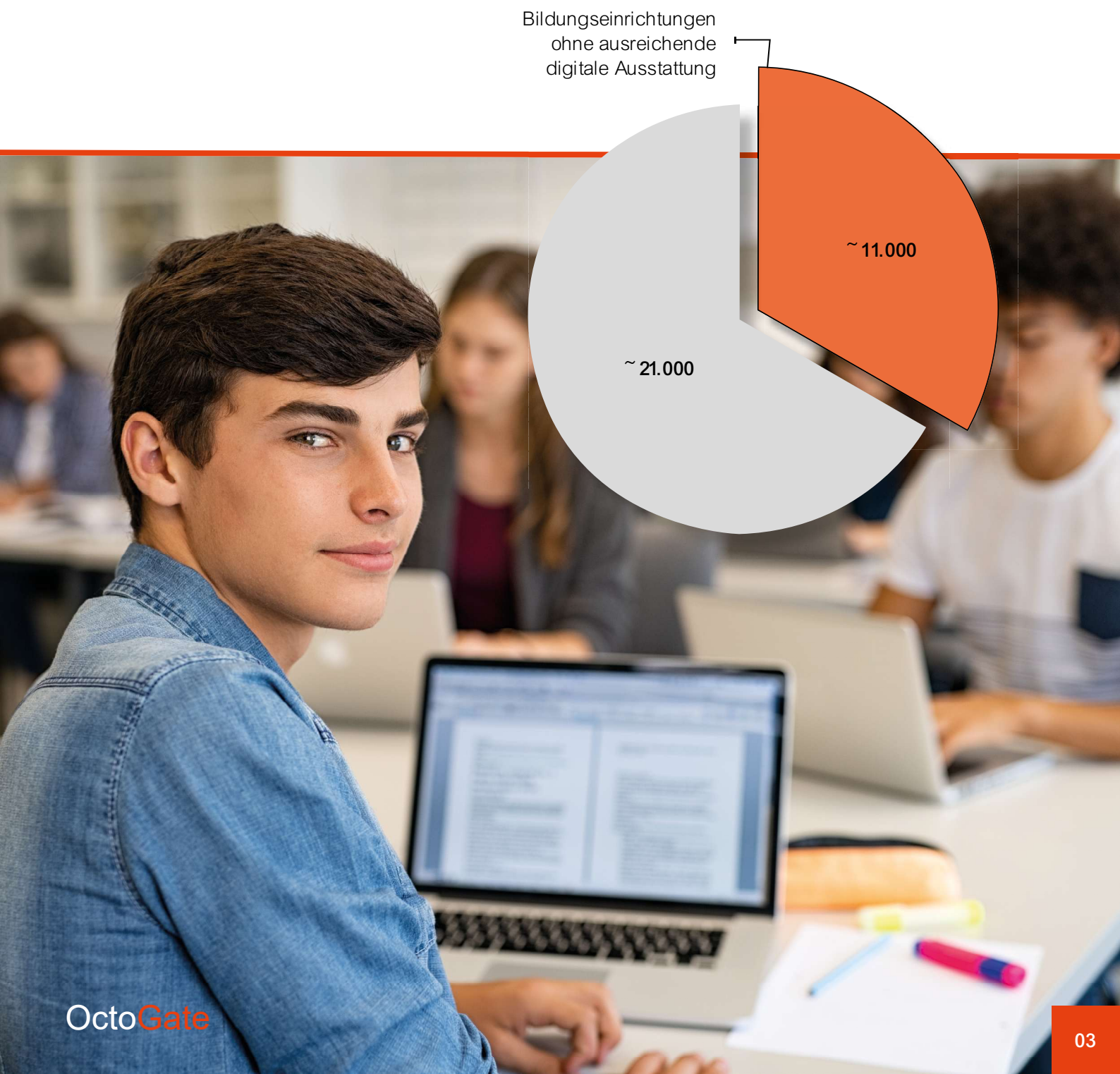
Telefon: +49 5251 18040-70
E-Mail: vertrieb@octogate.de
Web: www.schulfirewall.de

Inhaltsverzeichnis

1. Einleitung

In Deutschland zeigt sich eine deutliche digitale Kluft unter den Schulen. Etwa ein Drittel der knapp 32.000 allgemeinbildenden Bildungseinrichtungen wird als digitale Nachzügler betrachtet. Diese Schulen sind im Vergleich zu anderen nicht ausreichend oder teils gar nicht mit digitalen Ressourcen und moderner Technologie ausgestattet. Als Folge haben Schülerinnen und Schüler, die diese Schulen besuchen, weniger Möglichkeiten, zentrale digitale Kompetenzen zu erwerben, die für ihre persönliche Entwicklung und ihre Zukunft von entscheidender Bedeutung sind.

Dieses Whitepaper untersucht die Bedeutung der digitalen Bildung, die Herausforderungen durch die digitale Kluft und die Rolle einer sicheren und effizienten Netzwerkinfrastruktur bei der Förderung umfassender digitaler Lernumgebungen.



2. Die Bedeutung digitaler Kompetenzen

In einer Zeit, in der Informationen in Hülle und Fülle verfügbar sind und sich manchmal widersprüchlich präsentieren, ist die Fähigkeit, Fakten von Meinungen zu unterscheiden, eine wichtige digitale Kompetenz. Schülerinnen und Schüler müssen lernen, wie sie vertrauenswürdige Informationen von irreführenden oder falschen Inhalten unterscheiden können. Diese Fähigkeit bildet das Fundament für eine informierte und kritische Teilnahme an der Gesellschaft. Darüber hinaus ist das E-Learning bzw. die Online-Bildung in der modernen Welt von großer Bedeutung. Es ist daher wichtig, die digitale Kluft zu überwinden, um allen Schülerinnen und Schülern gleiche Chancen auf eine umfassende digitale Bildung zu ermöglichen.

In Schulen, die als digitale Nachzügler gelten, fehlt es oft an moderner Technologie, wie zum Beispiel interaktiven Whiteboards, Computern oder Tablets und an einer stabilen WLAN-Infrastruktur. Dadurch haben Schülerinnen und Schüler möglicherweise keinen ausreichenden Zugang zu digitalen Lernmaterialien und interaktiven Lernplattformen, die ihnen helfen könnten, digitale Kompetenzen zu entwickeln. Um diese digitale Kluft zu überwinden und sicherzustellen, dass alle Schülerinnen und Schüler gleiche Chancen auf eine umfassende digitale Bildung haben, ist es von großer Bedeutung, dass Schulen angemessen und fachgerecht mit digitalen Ressourcen ausgestattet werden. Eine gezielte Planung und Umsetzung sind daher für die einzelnen Bundesländer unerlässlich.

3. Best Practices für WLAN an Schulen

Um eine solide Basis für die Sicherheit eines WLAN-Netzwerks an Schulen zu bilden, sollte eine ganzheitliche Herangehensweise in Betracht gezogen werden, die folgende Merkmale berücksichtigt:

- ✓ Einfache Bedienbarkeit
- ✓ Flächendeckende Verfügbarkeit
- ✓ Starke Verschlüsselung für Datenübertragung (z. B. WPA3)
- ✓ Zugriffskontrolle mit MAC-Adressfiltern oder Benutzer-Authentifizierung
- ✓ Netztrennung
- ✓ Separater Gastzugang für Besucher mit Zeitbeschränkung
- ✓ Content-Filter mit Jugendschutz
- ✓ Verfügbarkeit von regelmäßigen Sicherheitsupdates

4. Umsetzung der Best Practices für WLAN

Beginnen Sie mit einer gründlichen Netzwerkplanung, um die Anforderungen der Schule zu verstehen. Berücksichtigen Sie die Größe des Campus, die Anzahl der Benutzer, die benötigte Bandbreite und eine eventuell geplante Erweiterung. Eine sorgfältige Planung bildet die Grundlage für eine zuverlässige und leistungsfähige WLAN-Infrastruktur.

Professionelle Standortanalyse
Führen Sie eine detaillierte Standortanalyse durch, um die optimale Platzierung von WLAN-Zugriffspunkten (APs) zu ermitteln. Achten Sie auf die physische Umgebung, Interferenzen, Hindernisse und die Signalreichweite, um eine gleichmäßige Abdeckung sicherzustellen. Im besten Fall hat sich jedoch die Lösung der 1:1 Ausstattung von Klassenräumen und Access Points bewährt. Sprich ein Access Point pro Klassenraum. Hier können die Kosten für eine Ausleuchtung gespart und direkt in Hardware umgewandelt werden.

Skalierbare Infrastruktur
Wählen Sie WLAN-Lösungen, die einfach skalierbar sind und mit der steigenden Anzahl von Benutzern und Geräten wachsen können. Eine flexible Infrastruktur ermöglicht eine reibungslose Erweiterung und zukünftige Upgrades.

Hochwertige Hardware
Investieren Sie in qualitativ hochwertige WLAN-Hardware von renommierten Herstellern. Hochleistungsfähige Access Points und WLAN-Controller gewährleisten eine stabile und zuverlässige Verbindung.

DSGVO-Konforme Hardware Lösungen
DSGVO-konforme Hardware ist wichtig für Schulen, um die Datenschutzvorschriften einzuhalten und die persönlichen Informationen von Schülern und Lehrern zu schützen. Das sorgt für Sicherheit und Vertrauen im Umgang mit digitalen Geräten und Daten.

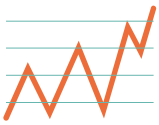
Separate Netzwerke für Schüler, Lehrer und Gäste
Implementieren Sie separate WLAN-Netzwerke für Schüler, Lehrer und Gäste, um die Sicherheit und Leistung des Schulnetzwerks zu gewährleisten. Die Gastnetzwerke sollten vom Hauptnetzwerk isoliert sein.

Sicherheit und Datenschutz
Stellen Sie sicher, dass das WLAN mit modernen Sicherheitsprotokollen wie WPA2/WPA3 verschlüsselt ist, um unbefugten Zugriff zu verhindern. Implementieren Sie auch eine auf Schulbedürfnisse abgestimmte Firewall. OctoGate bietet hier mit der Schulfirewall.de einfache und sichere Lösungen. und andere Sicherheitsmaßnahmen, um das Netzwerk vor Bedrohungen zu

Content-Filter und Jugendschutz
Setzen Sie Content-Filter mit Jugendschutz ein, um den Zugriff auf unangemessene oder ungeeignete Inhalte zu beschränken, insbesondere im schulischen Umfeld. Wir bieten über 81. Mio gefilterte URLs inkl. des BPjM-Moduls der Bundeszentrale für Kinder- und Jugendmedienschutz in über 20 Kategorien.

Bandbreitenmanagement
Implementieren Sie Quality of Service (QoS) und Bandbreitenmanagement, um sicherzustellen, dass wichtige Anwendungen wie Lernplattformen und E-Learning-Tools priorisiert werden und eine optimale Netzwerkperformance gewährleistet ist.

Benutzerfreundlichkeit
Vereinfachen Sie die Benutzeranmeldung und den Zugriff auf das WLAN, insbesondere für Schüler und Lehrer, um die Akzeptanz und Nutzung zu fördern.



Überwachung und Wartung
Filtern Sie in einem Dashboard die relevantesten Daten, um die WLAN-Performance, die Auslastung der APs und andere Netzwerkmetriken zu überwachen. Inventarisieren Sie Ihre Hardware in Standortkonfigurationen um Ausfälle direkt zu lokalisieren.

Schulung und Support:
Nutzen sie Schulungen der Hersteller für das Schulpersonal, um sie bei der effizienten Nutzung des WLANs zu unterstützen. Sollten die Schule oder der Sachaufwandsträger nicht über die nötigen Kapazitäten verfügen, bieten sich geschulte Dienstleister und der Herstellersupport an.

Pädagogischer Mehrwert
Nutzen Sie das WLAN als Werkzeug für den pädagogischen Mehrwert. Die OctoGate Schulfirewall hat Schnittstellen zu Klassenraummanagementsystemen wie z.B. PaedML Windows und dem Schulnetzverwalter. Fördern Sie die Integration von Technologie im Unterricht und bieten Sie Lehrern und Schülern Zugriff auf pädagogisch wertvolle Online-Ressourcen und E-Learning-Materialien.

Durch die Umsetzung dieser Best Practices können Schulen eine leistungsstarke, sichere und benutzerfreundliche WLAN-Infrastruktur schaffen, die den pädagogischen Bedürfnissen gerecht wird und die digitale Bildung unterstützt.

Welche Merkmale lassen sich bereits jetzt schon umsetzen?

1. Ändern des Standard-Passworts
Das Passwort Ihres Routers oder Access Points ist meist schon ein starkes Passwort, welches jedoch leicht zugänglich ist und daher durch eine Kombination aus Buchenstaben, Groß- und Kleinschreibung, Zahlen und Sonderzeichen ersetzt werden sollte.

2. Ändern des Passworts in regelmäßigen Abständen
Es ist sinnvoll das Passwort zum Beispiel alle 6 Monate zu ändern. Somit kann gewährleistet werden das ehemalige Besucher keinen Zugriff mehr auf das WLAN haben.

3. Aktivierung von WLAN-Verschlüsselung
Im Optimalfall verwenden Sie anstatt WPA2-Verschlüsselung den aktuellen Standard der WPA3-Verschlüsselung. Es schützt besonders vor sogenannten Brute-Force-Angriffen und Passwort-Phishing, da nur eine begrenzte Anzahl an Login-Versuchen möglich ist und die Kommunikation zwischen dem WLAN-Netzwerk und dem Gerät verschlüsselt wird.

4. Authentifizierung von Nutzern
Aktivieren Sie die Netzwerk-Authentifizierung durch eine Benutzer-ID und ein individuelles Passwort, damit Sie gewährleisten können das nur autorisierte Nutzer auf das Netzwerk Zugriff erhalten.

5. Clientisolation für Broadcasts und Multicasts
Gerade in öffentlichen WLAN-Netzwerken trägt dies dazu bei, das Risiko von Datenschutzverletzungen und unbefugten Zugriff zu schützen.

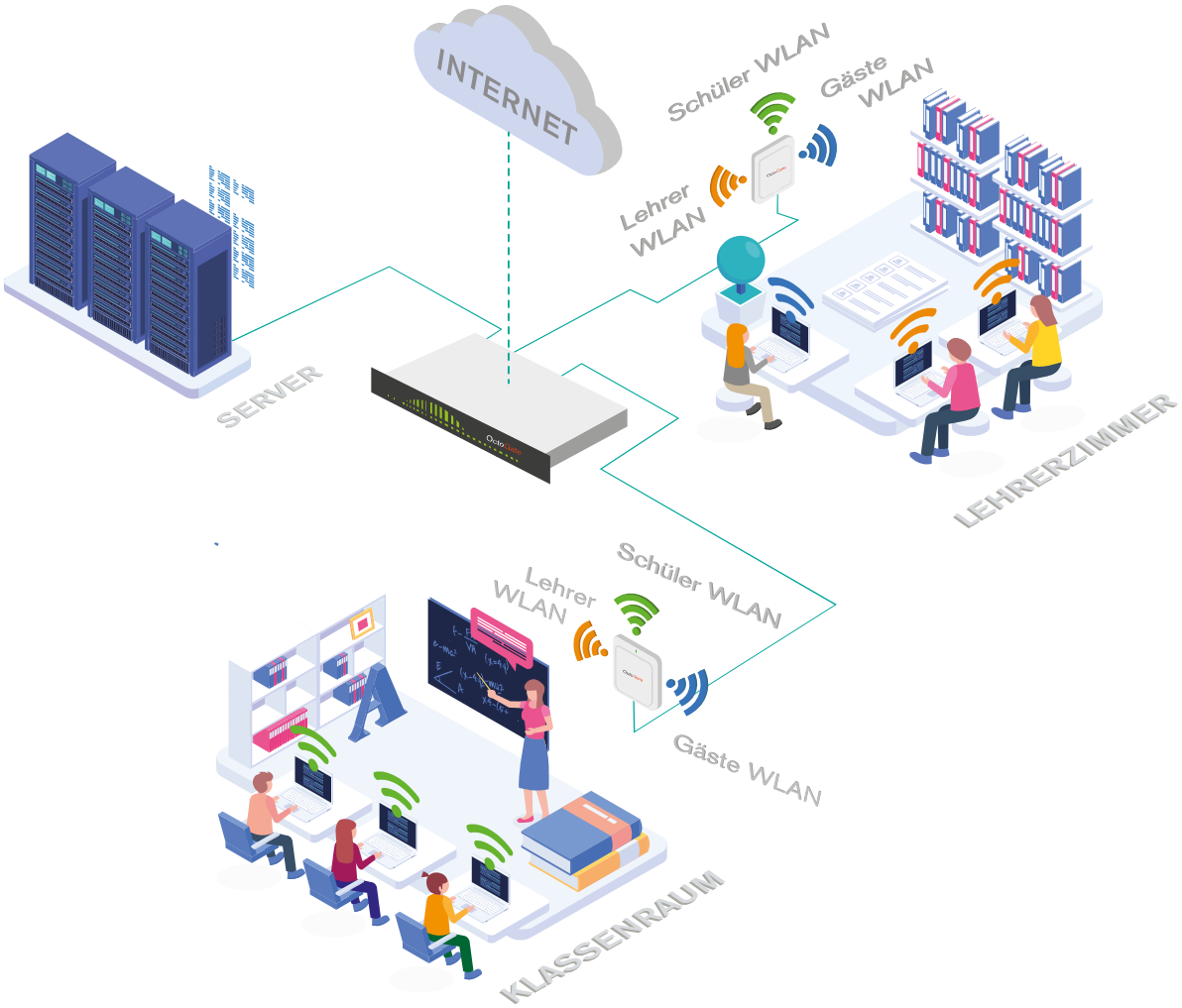
5. Netzwerkaufbau mit separaten Netzen für die pädagogische Nutzung

Schüler WLAN
Dieses Netzwerk ist speziell für Schülerinnen und Schüler ausgelegt und gewährt Zugang zu Bildungsinhalten, Lernplattformen, Online-Ressourcen und anderen schulischen Anwendungen. Es wird sorgfältig abgeschirmt von unerlaubten Inhalten, um eine ungestörte Lernerfahrung sicherzustellen.

Lehrer WLAN
Das Lehrer-WLAN ist für das pädagogische Personal reserviert und bietet erweiterte Berechtigungen sowie Zugang zu speziellen Ressourcen. Dadurch wird Lehrkräften eine effektive Unterrichtssteuerung ermöglicht.

Gäste WLAN
Ein eigenständiger Gastzugang spielt eine zentrale Rolle, um Besuchern wie Eltern, Gästen oder anderen externen Nutzern zum Beispiel bei schulischen Veranstaltungen die Nutzung des Internets zu ermöglichen. Dabei wird das interne Schulnetzwerk vor möglichen Gefahren geschützt. Der Zugang ist zeitlich begrenzt und beschränkt den Zugriff auf schulinterne Ressourcen.

Optional: Verwaltungs WLAN
Dieses Netzwerk ist gezielt für die Schulverwaltung und IT-Administratoren entwickelt worden. Es erlaubt den Zugriff auf Netzwerk- und Serverressourcen, die zur Verwaltung und Wartung der gesamten IT-Infrastruktur benötigt werden.



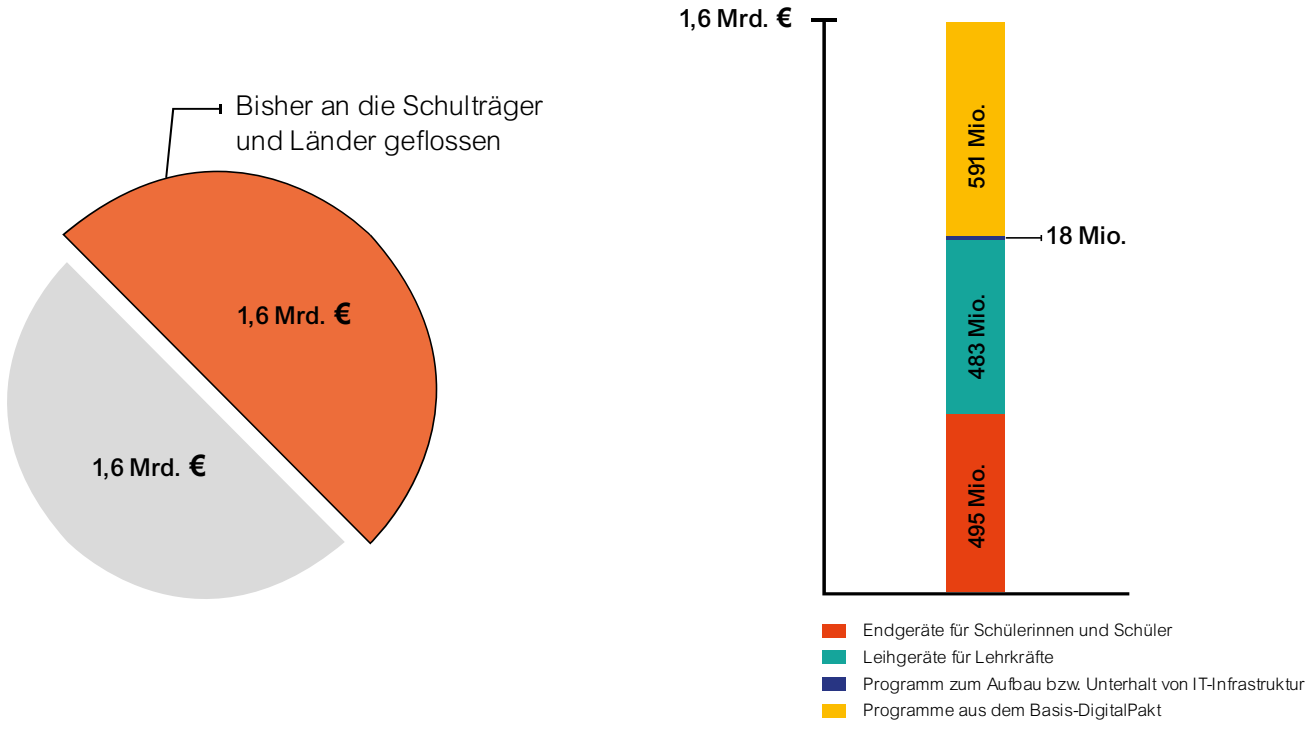
6. DigitalPakt Schule: Förderung der digitalen Bildung

Das DigitalPakt Schule-Programm unterstützt die Steigerung der digitalen Leistungsfähigkeit kommunaler Bildungsinfrastrukturen durch finanzielle Förderung. Diese Initiative spielt eine entscheidende Rolle bei der Überwindung der digitalen Kluft und erfordert eine strategische Mittelallokation, um spezifische Bildungsbedürfnisse zu erfüllen.

Im Rahmen des DigitalPakts Schule gewährt der Bund den Ländern auf Grundlage von Art. 104c des Grundgesetzes Finanzhilfen für Investitionen zur Steigerung der Leistungsfähigkeit der digitalen kommunalen Bildungsinfrastruktur. Der DigitalPakt trat am 17. Mai 2019 in Kraft und sah ursprünglich eine finanzielle Förderung aus dem Sondervermögen in Höhe von 5 Mrd. Euro zwischen 2019 und 2024 vor.

Im Rahmen der Corona-Pandemie wurden die Mittel durch drei Zusatzvereinbarungen in Höhe von je 500 Mill. Euro auf insgesamt 6,5 Mrd. Euro erhöht. Die Länder haben sich gleichzeitig verpflichtet, diese Investitionen mit einem Eigenanteil in Höhe von mind. 10 % der Bundesmittel zu unterstützen und gleichzeitig eigene Maßnahmen im Rahmen ihrer Kultushoheit und in eigener finanzieller Verantwortung zu erbringen. In den Grundmitteltabellen wurden im Ist die für den DigitalPakt Schule relevanten Zuführungen aus dem Bundeshaushalt an das Sondervermögen in 2018 (720 Mill. Euro), 2020 (1,72 Mrd. Euro) und 2021 (571 Mill. Euro) berücksichtigt.

Die anteilig zur Verfügung gestellten Mittel aus den Frequenzerlösen werden hingegen nicht in den Grundmitteltabellen berücksichtigt. Seit Inkrafttreten des DigitalPakt Schule (Stand 30.06.2022) wurden insgesamt Förderanträge bewilligt, die einer Investitionssumme von 3,2 Mrd. Euro entsprachen. An die Schulträger bzw. Länder sind bisher 1,6 Mrd. Euro geflossen. Die abgeflossenen Mittel verteilen sich dabei auf die Sonderprogramme mobile Endgeräte für Schülerinnen und Schüler (495 Mill. Euro), Leihgeräte für Lehrkräfte (483 Mill. Euro) sowie das Programm zum Aufbau bzw. Unterhalt von IT-Infrastruktur in Schulgebäuden (18 Mill. Euro). Weitere 591 Mill. Euro sind für Programme aus dem Basis-DigitalPakt abgeflossen.



Quelle: Statistisches Bundesamt, Bildungsfinanzbericht 2022

7. Implementierung von WLAN-Lösungen eines Herstellers

Warum sollte man bei der Netzwerk-Infrastruktur auf Lösungen aus einer Hand setzen?

In vielen Bereichen hat es sich bewährt, Lösungen vom selben Hersteller zu verwenden. Das Szenario in diesem Fall ist eine Schulfirewall, Switches und WLAN Access Points.

Durch die Verwendung von Einheitslösungen lässt sich von vielen Vorteilen profitieren wie einer nahtlosen Integration, einfacher Verwaltung des Netzwerks und besserer Konfiguration.

Auch ein einheitlicher Support ist nicht zu verachten, da im Falle von Problemen oder Konfigurationsfehlern ein effizienteres Troubleshooting stattfinden kann, da sich die Netzwerkumgebung schneller analysieren und Fehler beheben lassen.

Ein wesentlicher Punkt ist das Einsparen von Kosten, da Personal nicht unnötig für viele verschiedene Hersteller regelmäßig geschult werden muss.

8. Fazit

Die Überwindung der digitalen Kluft an deutschen Schulen ist entscheidend, um Schülerinnen und Schüler mit wichtigen digitalen Kompetenzen auszustatten. Durch eine sichere und effiziente Netzwerkinfrastruktur können Schulen umfassende digitale Bildung fördern und ihre Schülerinnen und Schüler auf eine erfolgreiche Zukunft im digitalen Zeitalter vorbereiten. Die erfolgreiche Umsetzung von Best Practices und Investitionen in zuverlässige WLAN-Lösungen ebnet den Weg für transformative Lernerfahrungen und eine vielversprechende digitale Zukunft für alle Schülerinnen und Schüler. Der DigitalPakt Schule und eine strategische Planung spielen dabei eine entscheidende Rolle, um eine gleichberechtigte digitale Bildung in ganz Deutschland zu ermöglichen. Mit proaktiven Maßnahmen und gezielten Investitionen können deutsche Schulen die digitale Revolution annehmen und die nächste Generation auf den Erfolg in der digitalen Welt vorbereiten.

Webinare & Veranstaltungen

Noch Fragen?

Das kompetente Team von OctoGate hilft Ihnen gerne:

Vertrieb

Telefon: +49 5251 18040-70
E-Mail: vertrieb@octogate.de

Support

Telefon: +49 5251 18040-40
E-Mail: support@octogate.de