Eine Initiative von CISCO

Ihre Anleitung:

IT-Sicherheit und Netzwerk als Fundament für digitale Bildung – Schritt für Schritt zur Umsetzung

Wir machen Digitalisierung einfach!

Wo stehen Sie auf dem Weg zur digitalen Schule? Und wie sicher ist Ihr Konzept?

Wir richten uns mit dieser Anleitung an IT-Leiter*innen, Expert*innen die Security-Konzepte umsetzen und Informations-Sicherheitsbeauftragte bei Kommunen, Schulträgern und öffentlichen Auftraggebern.

Die Initiative begleitet Schulträger und Schulverwaltungen deutschlandweit – bei jedem Schritt. Wir helfen dabei, die aktuellen und zukünftigen Herausforderungen zu überwinden und die Bildung in Deutschland auf ein neues Qualitäts- und Sicherheitsniveau unter den Aspekten der Chancengleichheit und Ortsunabhängigkeit zu heben. Von verlässlichem WLAN bis hin zur Sicherung der schuleigenen Tablets und allem, was dazwischen liegt.

1 ORIENTIERUNG

In der Orientierungsphase stehen Sie am Anfang Ihres Projektes. An dieser Stelle sollten Sie evaluieren, welche Möglichkeiten die digitale Schule bieten soll und wodurch bzw. an welcher Stelle dadurch Risiken entstehen.

2 PLANUNG

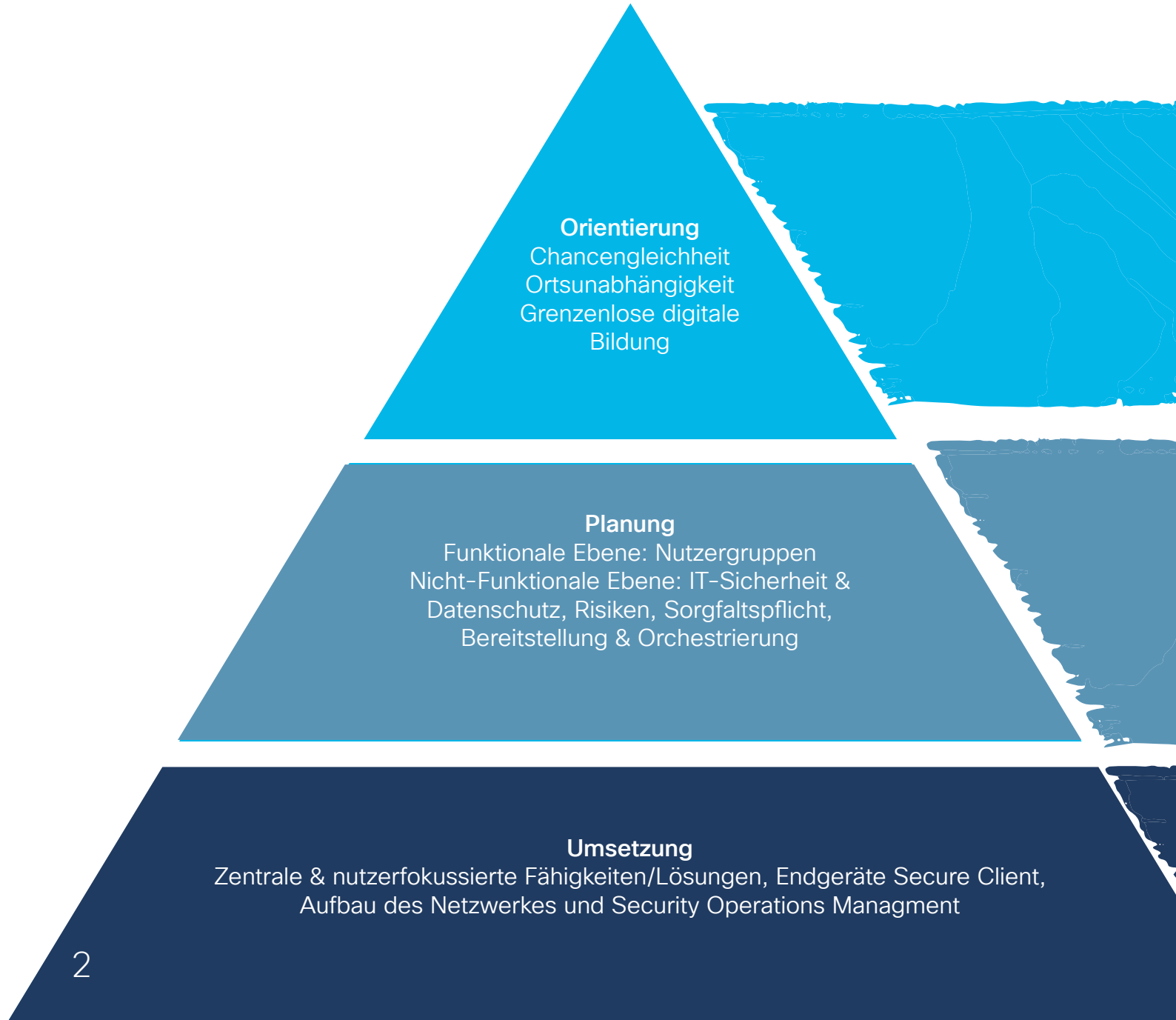
In der Planungsphase werden die Anforderungen an die digitale Schule in ein technisches Fundament an Netzwerk und IT-Sicherheit übersetzt. Sie analysieren die kritischen Daten und Applikationen und leiten daraus die Anforderungen ab. Der Fokus liegt hier auf dem technischen, nicht-funktionalen Mantel, der auf Nutzerebene ein reibungsloses und sicheres Anwendererlebnis ermöglicht.

3 UMSETZUNG

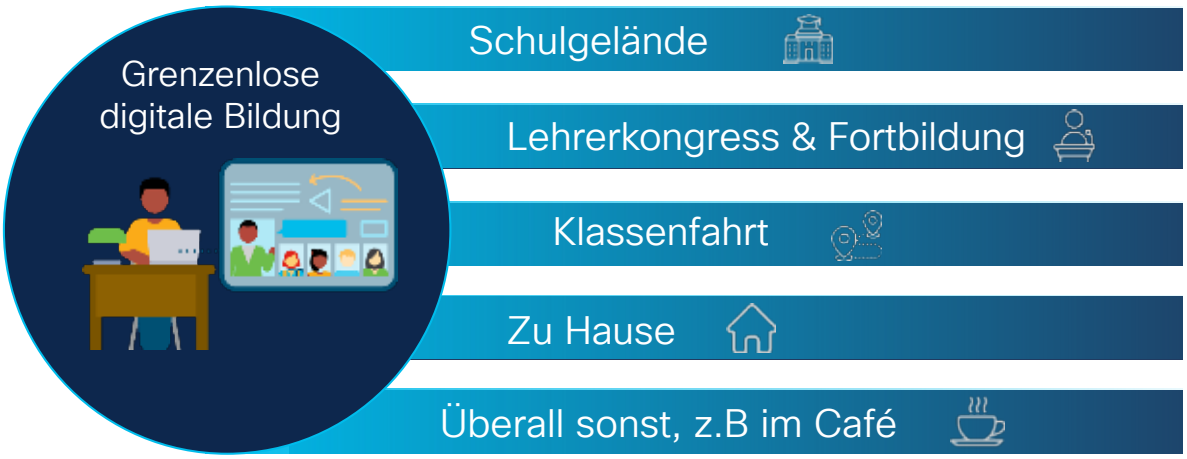
In der Umsetzungsphase bauen Sie Ihr Fundament (Netzwerk und IT-Sicherheit) für eine sichere digitale Schulumgebung und ortsunabhängige Nutzung. Gemeinsam mit Ihrem Partner finden Sie eine individuelle Lösung, wie Ihr Sicherheitskonzept im Rahmen der digitalen Schule umgesetzt und betrieben werden kann.

EINLEITUNG
Pyramide Sicherheitskonzept

Ein gut durchdachtes technisches Netzwerk mit dem Ziel durch grenzenlose digitale Bildung Chancengleichheit und -gerechtigkeit zu verbessern, befähigt die flexible Nutzung von digitalen Lernkonzepten und Medien: überall, jederzeit und für jeden, aber SICHER doch bitte!



EINLEITUNG
Pyramide Sicherheitskonzept



Orientierung

Welche generellen neuen Ziele und Anforderungen gilt es umzusetzen?
Was ist überhaupt das Risiko?
Wie effektiv sind unsere aktuellen Sicherheitsmaßnahmen?
Wie schnell können wir ein unerlaubtes Eindringen entdecken und beheben?

Planung

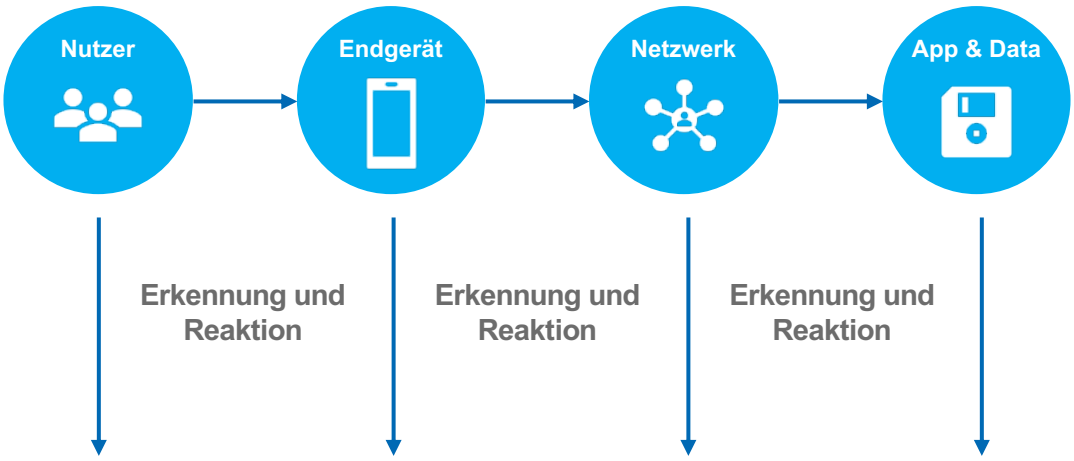
Welche speziellen Anforderungen gilt es umzusetzen?
Wie angreifbar machen wir uns und wie groß ist die Eintrittswahrscheinlichkeit für uns?
Was sind wirksame Gegenmaßnahmen und was sind uns diese Wert?

Umsetzung

Wie kann die Umsetzung der Gegenmaßnahmen und der kontinuierliche Betrieb sehr effizient und effektiv aussehen?
Wie kann gleichzeitig die Komplexität reduziert werden?

Sicherheit auf dem nächsten Level

Da es niemals eine 100%-ige Sicherheit vor Cyberangriffen geben kann ist es entscheidend, dass die Technologien nicht nur als präventive Maßnahmen zu sehen und zu nutzen sind, sondern im Security Operations Management ein ganzheitliches, proaktives und automatisiertes Security Monitoring ermöglichen und auch die kontinuierliche Erkennung von Vorfällen mit entsprechender Analyse und Reaktion maßgeblich erleichtern - genau dafür wurden sie entwickelt.



Ganzheitliches, proaktives & automatisiertes Security Monitoring,
Angriffserkennung, Analyse und Reaktion auf Vorfälle

Security Operations Management

1. Orientierung schaffen

In der Orientierungsphase stehen Sie am Anfang Ihres Digitalisierungsprojektes und Ihres dafür notwendigen Sicherheitskonzeptes. Dafür ist es relevant Ihren eigenen Status zu kennen und die Meilensteine Ihres Sicherheitskonzeptes zu definieren. Die Motivation ist eine grenzenlose digitale Bildung für Lernende und Lehrende zu etablieren, die ausreichend Sicherheit bietet und den Nutzer*innen ein reibungsloses, digitales Anwendererlebnis bietet.

Fazit

Um digitale Bildung in Schuleinrichtungen und Ortsunabhängigkeit zu ermöglichen, ist es unerlässlich ein geeignetes Sicherheitskonzept umzusetzen. Zum einen braucht es dafür Endgeräte, die in puncto Sicherheit gemanaged werden können und zum anderen sollte der Fokus darauf liegen, kritische Daten z. B. in der Verwaltungsebene zu sichern. Nur so kann ein rundum sorgenloses, digitales Bildungserlebnis für alle Beteiligten ermöglicht werden. Die Grundlage sollte der Medienentwicklungsplan sein, aus welchem sich die Anforderungen für ein Fundament an Netzwerk und IT-Sicherheit ableiten lassen.

Chancengleichheit

Die Umsetzung eines sicheren, digitalen Bildungskonzeptes ermöglicht in Ihrer Bildungseinrichtung nicht nur flexibles und zeitgemäßes Lernen für Lehrende und Lernende, sondern verbessert auch die Chancengleichheit und Chancengerechtigkeit aller Beteiligten. Digitale Bildung verbessert die Inklusion und die Teilhabe an der Bildung. Neben sozialen, sprachlichen und kulturellen Herausforderungen können auch körperliche und geistige Herausforderungen gemeistert werden. Digitale Bildung ist als integraler Bestandteil des lebensbegleitenden Lernens zu verstehen. Sie unterstützt die Durchlässigkeit der Bildungssysteme für geregelte, formale und informelle Bildungsübergänge zum Beispiel von der Schule hin zur Ausbildung. Außerdem trägt die digitale Bildung dazu bei, der Vereinbarkeit von Beruf und Familie für Lehrende und Schulverwaltung gerecht zu werden.
Eine hybride Arbeitsweise verbessert die Möglichkeiten der Teilzeit für Lehrende und Personen der Schulverwaltung. Die zeitliche und örtliche Flexibilität macht es möglich hybrides Arbeiten zu meistern und bietet neue Möglichkeiten bei der Unterrichtsgestaltung für alle Beteiligten.

Ortsunabhängige Anwendung

Mit Hilfe eines geeigneten Sicherheitskonzeptes soll ortsunabhängige digitale Bildung für Lernende und Lehrende ermöglicht werden.
Entweder mit einem von Ihrer Schule ausgehändigten Endgerät wie Tablet oder Laptop oder auch mit schülereigenen Smartphones oder Ähnlichem, wenn keine schuleigenen Endgeräte zur Verfügung stehen. Der optimale Zustand ist, wenn Ihre Bildungseinrichtung die Möglichkeit hat Endgeräte zur Verfügung zu stellen- unter dem Gesichtspunkt der Sicherheit empfehlen wir klar schuleigene Endgeräte. Dadurch kann digitale Bildung von überall aus stattfinden: egal ob von Zuhause aus, auf Fortbildungen oder auch auf Klassenfahrten. Machen Sie sich die Umsetzung von neuen Lernkonzepten und Lernortkooperationen zu Ihrem Ziel.

Grenzenlose digitale Bildung

Im Fokus des Projektes steht die sichere und anwenderfreundliche digitale Ausstattung Ihrer Bildungseinrichtung. Digitale Schule bedeutet die Nutzung externer, digitaler Medien zur Lernunterstützung, die Einführung von neuen Lernmethoden, der Einsatz externer Experten und Referenten und die Verwendung digitaler Medien und Inhalte, wie zum Beispiel Lernsoftware und Lernplattformen für Lehrende und Lernende. Hinzu kommt bei den Lehrenden und auf der Verwaltungsebene die Verwaltung und Bearbeitung von kritischen, personenbezogenen Daten in kritischen Applikationen. Das Beispiel digitales Klassenbuch spiegelt diesen Anwendungsfall anschaulich wieder. Hier sind neben unkritischen Daten wie beispielsweise digitale Elternbriefe auch sensible Daten wie Noten hinterlegt, die maximal geschützt sein müssen. Ziel ist es mehrere Anwender mit unterschiedlichen Rechten zu definieren. Der Schutz muss über den Zugriff mit Benutzernamen und Passwort hinausgehen.

2. Planung angehen

In der Planungsphase entwickeln Sie ein fundiertes Sicherheitskonzept, das die Basis für die sichere Digitalisierung Ihrer Schule bildet. Konkret wird analysiert, welche funktionalen (Was soll das System können?) und nicht-funktionalen (In welcher Qualität?) Anforderungen relevant sind, um digitale Bildung an Ihrer Schule nicht nur anwenderfreundlich, sondern auch sicher zu gestalten. Machen Sie sich die IT-Sicherheit zu Ihrem obersten Ziel. Sie beinhaltet technische und operative Maßnahmen, um folgende Fälle zu verhindern:

- **Unbefugten Zugriff auf Daten (Vertraulichkeit)**
- **Unbefugtes Löschen oder Zerstören von Daten (Verfügbarkeit)**
- **Unbefugtes Verfälschen von Daten (Integrität)**

Das Fundament bildet dabei die technische Basis aus Netzwerk und IT-Sicherheit, um Datenschutz zu gewährleisten und dem Schutz vor jugendgefährdendem Inhalt gerecht zu werden. Weitere wichtige Kriterien sollten eine einfache und flexible Orchestrierung sein, um den Nutzer*innen die Einhaltung der IT-Sicherheit so einfach wie möglich zu gestalten.

Richtiges Vorgehen bei der Planung:
Um richtig in die Planungsphase zu starten, unterscheiden Sie zunächst zwei Ebenen. Während die funktionale Ebene sich mit den Nutzer*innen und deren Bedürfnissen auseinandersetzt, betrachten Sie auf nicht-funktionaler Ebene die Anforderungen an Ihre IT-Umgebung. Stellen Sie sich dafür folgende Fragen:

FUNKTIONALE EBENE

WER?
Lehrende, Lernende, Verwaltung, Eltern & Gäste

WAS?
Verwendung kritischer/ nicht-kritischer Daten und Applikationen

WO?
Vor Ort in der Schule (Schulgelände) oder ortsunabhängig

WAS?
Schuleigene Endgeräte oder externe Endgeräte (Bring your own device: BYOD)

NICHT-FUNKTIONALE EBENE

IT-Sicherheit & Datenschutz: Nutzer, Endgeräte, Netzwerk, Applikationen & Daten

Analyse und Behebung von Cyber Risiken und Vorfällen

Erfüllung der Sorgfaltspflicht

Bereitstellung & Orchestrierung

2.1 Planung angehen auf funktionaler Ebene

WER?

Die unterschiedlichen Zielgruppen, egal ob Lehrende, Lernende, die Verwaltung, Eltern oder auch die Gäste haben spezifische Anforderungen und Bedürfnisse, die es in der Planung zu beachten gilt. Alle streben nach einem reibungslosen, digitalen Unterrichts-/Lehr- und Schuleinsatz mit einer ständigen und vollständigen Netzwerkfunktion.

WAS?

Entscheidend für alle unterschiedlichen Zielgruppen ist es digitale Lernplattformen und -medien zu nutzen, Konferenzen abzuhalten und selbstständig im Internet für Recherchen zu surfen. Hierbei handelt es sich um nicht-kritische Applikationen und Aktivitäten. Für Lehrende und die Verwaltung muss außerdem die Möglichkeit bestehen, auf kritische Applikationen und personenbezogene Daten sicher zugreifen zu können.

WO?

All das sollte nicht nur auf dem Schulgelände, sondern auch ortsunabhängig möglich sein. Dies bietet Flexibilität, hybride Unterrichtsmethoden und neue Möglichkeiten bei der Unterrichtsgestaltung für Lehrende und die Verwaltung.

WEM

Zuletzt ist zu klären, wem die vorhandenen Endgeräte gehören. Der optimale Zustand ist, wenn Ihre Bildungseinrichtung die Möglichkeit hat Endgeräte zur Verfügung zu stellen. Es wäre auch möglich eigene, private Endgeräte zu nutzen. Unter dem Gesichtspunkt der Sicherheit empfehlen wir klar die erste Alternative.

Schritt für Schritt...

Behalten Sie den Überblick!

Auf funktionaler Ebene liegt somit der Fokus auf eine ortsunabhängige und vor allem stets abgesicherte Netzwerkkommunikation, die für einen reibungslosen Unterrichts-/Lehr- und Schuleinsatz für Ihre Schüler*innen, die Lehrenden, die Verwaltung sowie Eltern und Gäste Sorge trägt. Es muss geklärt werden von wo aus gearbeitet werden soll, welche Applikationen und Daten verwendet werden und ob es Ihnen als Bildungseinrichtung möglich ist Endgeräte zur Verfügung zu stellen, die den Sicherheitsanforderungen entsprechen und entsprechenden Schutz bieten.

Im nächsten Schritt können nun die Anforderungen der funktionalen Ebene auf nicht-funktionaler Ebene beleuchtet werden.

2.2 Planung angehen auf nicht-funktionaler Ebene

Datenschutz & IT-Sicherheit

Nutzer

Die IT-Sicherheit definiert für den jeweiligen Nutzer oder die Nutzergruppe eine identitäts- und regelbasierte Rechteverwaltung (und dient als Prävention), um das Cyber-Risiko an Ihrer Schule zu minimieren. Neben der Zuordnung von Zugriffsrechten für Netzwerke wie z. B. WLAN oder VPN, wird auch eingeordnet, wie vertrauenswürdig das genutzte Endgerät sein sollte. Stellen Sie sich die Frage, was beim Posture-Check verifiziert werden soll.

Für die Nutzer*innen wird definiert, welche Applikationen, Agenten etc. auf dem schuleigenen Endgerät des Nutzers installiert werden sollten und dürfen. Diese werden kontinuierlich überprüft. Zusätzlich wird in diesem Schritt definiert, welche kritischen Daten und Applikationen der Nutzer*innen verwenden darf und wie sich die Nutzer*innen authentifizieren und autorisieren. Auch hier findet eine kontinuierliche Überprüfung der Vertrauenswürdigkeit der Nutzer*in statt.

Bei einem Aufbau der VPN-Verbindung sollte zusätzlich darauf geachtet werden, dass sich neben Passwort und Benutzername mit einer Mehrfach-Authentifizierung autorisiert wird (MFA).

Netzwerk

Auf nicht-funktionaler Ebene leistet ebenfalls das Netzwerk einen großen Beitrag zur Sicherheit und zum reibungslosen Schulalltag auf funktionaler Ebene. Achten Sie bei Ihrem Netzwerk auf WLAN und LAN, das eine entsprechende (regelbasierte) Segmentierung ermöglicht. Das WLAN sollte zwischen Gästen, Lernenden, Lehrenden, Verwaltung und Endgeräten wie Smartboards und Druckern filtern können, um Mobilität und Sicherheit zu gewährleisten. Die Segmentierung bei LAN wird für nicht WLAN-fähige Endgeräte wie Server benötigt. Daneben ist auch ein SD-WAN in der Schule von Vorteil und sollte in Ihrer Planung berücksichtigt werden. Dies sichert zum einen den direkten Internetzugang in der Schule und zum anderen eine Verbindung zum kommunalen Schulrechenzentrum mit der Fähigkeit Anwendungen zu segmentieren. Außerdem braucht es einen durch eine Mehrfachauthentifizierung gesicherten VPN Zugang in das Schulnetzwerk, da die ausschließliche Verwendung von User und Passwort ein großes Risiko darstellt.

Durch eine entsprechende Firewall (inkl. IDS/IPS) können LAN und WLAN in der Schule abgesichert werden. LAN und WLAN werden durch das Blockieren von unerwünschten und kritischen Internetinhalten mittels DNS-Schutz geschützt. Das kann beispielsweise über diverse Filter sichergestellt werden.

Der VPN Aufbau wird nur zugelassen, wenn auf dem Endgerät keine Auffälligkeiten erkannt werden und der Nutzer*in sich per MFA authentifiziert und autorisiert. Zusätzlich müssen durch E-Mail-Security beim Schul-IT-Provider schadhafte Mails blockiert werden.

Endgeräte

Für eine ganzheitliche Umsetzung Ihres Sicherheitskonzeptes empfehlen wir schuleigene Endgeräte. Die von der Schule verwalteten Endgeräte, dürfen für autorisierte Zwecke verwendet werden und werden dahingehend überwacht. Zentral definierte Regeln können damit bzgl. Nutzer*innen und deren Rechte einfach und lokal umgesetzt werden. Anhand von vorab definierten Regeln werden der Gesundheitszustand und die Schwachstellen der Endgeräte regelmäßig überprüft. Dies bezeichnet man auch als Posture-Check der Endgeräte.

Die kontinuierliche Kontrolle bietet einen hervorragenden Schutz für die Endgeräte Ihrer Schule. Dadurch können z.B. Schwachstellen sowie schadhafte und verdächtige Verbindungen ins Internet, egal ob innerhalb oder außerhalb der Schule, frühzeitig und proaktiv erkannt und blockiert werden (DNS-Schutz), oder aber die Ausführung von unbekannten Dateien überwacht werden. (End-Point- Detection & Response). Eine kontinuierliche und ortsunabhängige Prävention, aber vor allem eine Angriffserkennung und die mögliche Reaktion auf dem Endgerät selbst dienen dem Schutz der Endgeräte und der kompletten IT-Umgebung. Aus diesem Grunde sollte eine End-Point-Detection & Response Lösung bei jedem Endgerät absolute Pflicht sein. So können auffällige Dateien auf dem schuleigenen Endgerät frühzeitig und proaktiv erkannt und beseitigt werden.

Um auch bei Diebstahl lokale Dateien zu sichern, sollten die Festplatten verschlüsselt werden. Am einfachsten ist dieser Schutz mit schuleigenen Endgeräten umzusetzen.

Werden private Endgeräte verwendet, erfordert dies eine spezielle Bewertung, welche Rechte vergeben werden. Hier muss genau analysiert werden, was überprüft und installiert werden kann. Denn wenn nichts überprüft werden kann, besteht ein erhöhtes Risiko für die IT-Umgebung der Schule. Der Netzwerkzugang muss daher eingeschränkt werden.

Auch wenn der Einsatz von eigenen Endgeräten (Stichwort bring-your-own-device; BYOD) möglich ist, liegt unsere Empfehlung wegen einer besseren Überprüfbarkeit und damit einen höheren Beitrag zur Sicherheit, klar auf der Verwendung von schuleigenen Endgeräten. BYOD wäre beispielsweise über ein separates BYOD-WLAN mit eingeschränkten Rechten möglich, um das Risiko für die Lernumgebung zu minimieren.

Applikationen & Daten

Für den sicheren Zugriff auf kritische Daten und Applikationen wird eine Mehrfachauthentifizierung (MFA) eingesetzt. Darüber wird der Nutzer*in authentifiziert und autorisiert. Dies passiert netzwerk- und ortsunabhängig und der Nutzer*in bekommt den Zugriff nur dann, wenn es keinerlei schwerwiegende Auffälligkeiten gibt und das Endgerät als vertrauenswürdig eingestuft wird.

2.2 Planung angehen auf nicht-funktionaler Ebene

Analyse & Behebung von Cyber-Risiken und Vorfällen

Ziel eines Sicherheitskonzeptes für die Digitalisierung Ihrer Schule ist es Risiken im gesamten Kontext der IT-Umgebung zu minimieren, um mögliche Schäden auf ein Minimum zu reduzieren. Risiken im Sinne der IT-Sicherheit sind Schwachstellen, unerwünschte Ereignisse und Nutzung, sowie Angriffe auf das Netzwerk Ihrer Bildungseinrichtung. Dafür müssen Schwachstellen und Risiken auf den schuleigenen Endgeräten kontinuierlich erkannt und bewertet werden. Darauf folgt die Reaktion auf Vorfälle und Angriffe auf dem Endgerät und im Netzwerk selbst. Vorfälle in der Schulumgebung müssen analysiert werden und es bedarf einer Reaktion durch kontextbezogene Angriffserkennung. Die Extended Detection & Response wird mit Hilfe einer XDR Plattform technisch umgesetzt. Organisationsübergreifend müssen dazu im Kontext wichtige Fragen beantwortet werden: Wer oder was ist alles betroffen? Wie kam der Angriff in unsere IT? Wann fand das erste Eindringen statt? Wo genau hat er sich quer bewegt und sich ausgebreitet? Aber vor allem stellt sich die Frage: Was nun?

Erfüllung der Sorgfaltspflicht

Darüber hinaus beinhaltet ein ausgefeiltes Security-Konzept auch die Möglichkeit, die notwendige Sorgfaltsplicht zum Schutz vor der Nutzung von jugendgefährdenden Medien einhalten zu können. Je nach Rolle oder Identität der Nutzer*innen, beispielsweise Lernende unter 18 Jahre, sollten entsprechende Internetinhalte automatisch blockiert und gefiltert werden. Orientierung bietet beispielsweise die Bundesprüfstelle für jugendgefährdende Medien (BPjM Modul). Auch die Sorgfaltspflicht muss ortsunabhängig und zu jeder Zeit im Netzwerk Beachtung finden.

Bereitstellung & Orchestrierung

Eine zentrale Verwaltung, Kontrolle und Transparenz über das Netzwerk, die Netzwerksicherheit und die Netzwerkbenutzer*innen sowie deren Endgeräte und genutzten Anwendungen inklusive einer entsprechenden Verfügbarkeit und Fehlersuche sind die Basis eines funktionierenden Sicherheitskonzeptes Ihrer Schule. Die Softwareverteilung, Verwaltung und Kontrolle der Endgeräte sollten dabei zentral stattfinden. Ziel ist eine intuitive, flexible und datenschutzkonforme Bereitstellung und Verwaltung Ihrer Lernumgebung (Netzwerk, Security inkl. MDM) ohne, dass Sie zusätzliches Personal einsetzen müssen.
Auf Ebene der Nutzenden steht im Fokus, dass sie auch ohne oder mit nur wenig IT-Know-How in einer sicheren IT-Umgebung reibungslos arbeiten können. Dafür müssen die Prozesse im Hintergrund funktionieren: Die kontinuierliche Erkennung und Reaktion auf Vorfälle und Angriffe, die auf dem Endgerät stattfinden, sollten so einfach und nutzerfreundlich wie möglich sein.
In einer zentralen und organisationsübergreifenden Plattform braucht es eine Analyse von Vorfällen mit der Möglichkeit einer entsprechenden Reaktion durch eine kontextbezogene Angriffserkennung in Ihrer Schulumgebung.
Ein agiles Netzwerkmanagement bietet dabei die Grundlage für agiles Lernen. Darunter fallen Adhoc-Admin-Instrumente für den Alltagsgebrauch. Zum Beispiel besteht die Möglichkeit im Klassenraum durch den Lehrer*in selbst das WLAN auf Knopfdruck abzuschalten oder die Bandbreite für besondere Anlässe zu reduzieren. Die System-Administrierung ist dabei standort- und personenunabhängig möglich.

3. Umsetzung

In der Umsetzungsphase haben Sie sich bereits intensiv mit Ihrem Sicherheitskonzept auseinandergesetzt. Nun geht es für Ihre Schule darum das Fundament aus Netzwerk und Security zu bauen und sich damit zu beschäftigen, wie genau es umgesetzt und betrieben werden kann.
Es werden notwendige technische Fähigkeiten und Lösungen bezüglich des Netzwerkes und der IT-Sicherheit geschaffen, die die Basis für die Digitale Bildung an Ihrer Schule bilden. Die Systeme müssen nach Stand der Technik agil, flexibel, sicher, skalierbar und auch wiederverwendbar sein.

Nun können Sie entscheiden, ob Sie Ihr System selbst aufbauen und betreiben oder dies doch lieber als Managed-Service umsetzen möchten. Wichtig ist, dass die reine Co-Existenz aller Fähigkeiten nicht ausreicht, denn es kommt darauf an, wie die Fähigkeiten integriert sind. Idealerweise sollte die Lösung betriebsfertig sein, ohne dass weitere Komponenten ein- oder angebaut werden müssen. Dies vereinfacht die Nutzung und Bereitstellung und verkürzt den Weg zu Ihrer digitalen Schule.

Ein wichtiger Faktor Ihres Sicherheitskonzeptes ist das richtige Security Operations Management. Es ist essentiell, um die entsprechenden Fähigkeiten bezüglich proaktiver und reaktiver Angriffserkennung und Reaktion zu nutzen. Egal ob Schule, IT-Provider der Schule oder Träger, es muss geklärt sein, wer für das Security Operation Management die Verantwortung trägt.

Bestandteile Ihres Sicherheitskonzeptes als Checkliste

Zentrale Fähigkeiten / Lösungen

[ ] Zentrales Mobile Device Management (MDM)
[ ] Zentrale Ende-zu-Ende Verwaltung und Orchestrierung für
- Netzwerk
- Netzwerksicherheit
- Netzwerkbenutzer*in
- Endgeräte und deren Anwendungen

[ ] Identity & Access Management
[ ] Kontinuierliche Angriffserkennung und Reaktion
[ ] Schwachstellenerkennung von Endgeräten (Device Posture Check)

Nutzerfokussierte Fähigkeiten/Lösungen

[ ] Mehrfachauthentifizierung beim Zugriff auf kritische Daten und Applikationen (MFA)
[ ] Mehrfachauthentifizierung beim Aufbau einer VPN-Verbindung
[ ] E-Mail Security

Schul-eigene Endgeräte mit ...

[ ] VPN Client inkl. MFA und Device Posture Check
[ ] DNS Schutz auf Endgeräten inkl. Filter- und Blocklisten für jugend gefährdende Inhalten
[ ] Monitoring der Geräte - Endpoint Detection & Response (EDR)
[ ] Verschlüsselung der Festplatte

Netzwerk

[ ] Regelbasierte Netzwerksegmentierung und -zuordnung für WLAN, LAN und SD-WAN
[ ] VPN Gateway
[ ] Firewall mit IDS & IPS
[ ] Filter- und Blocklisten zur Einschränkung von unerwünschten und als kritisch erachtete Services (Schatten IT)

Extended Detection und Response Plattform (XDR)

[ ] Kont. Security Monitoring und Bewertung der Endgeräte bzgl. Cyber Risiken wie Schwachstellen, Anomalien etc
[ ] Kont. Erkennung von allgemeinen Schwachstellen und Malware in der gesamten IT-Umgebung
[ ] Kont. Erkennung, Analyse und Reaktion auf Vorfälle
[ ] Proaktive Angriffserkennung anhand von bekannten und kritischen Angriffsszenarien

Was sonst?

[ ] Optional Sandbox
[ ] Optional Web Proxy

3. Umsetzung

Vorbeugen, erkennen und schnell reagieren

Egal ob interne Angriffe durch Schüler*innen, die einfach mal versuchen möchten, wie weit sie kommen oder das Leak von Abiturklausuren, unsere Lösung hilft dabei Vorkehrungen zu treffen, die dies verhindern.
Die Lösungen von Cisco Meraki und des Cisco Secure Client bieten durch ihre vielzähligen integrierten Fähigkeiten zahlreiche Möglichkeiten und Mehrwerte ganz im Sinne der „grenzenlosen“ digitalen Bildung.

Sie ermöglichen eine einfache und sichere Nutzung von externen digitalen Medien z. B. YouTube zur Lernunterstützung oder auch von neuen Lernmethoden. Außerdem können externe Expert*innen und Referent*innen in den Unterricht integriert werden.

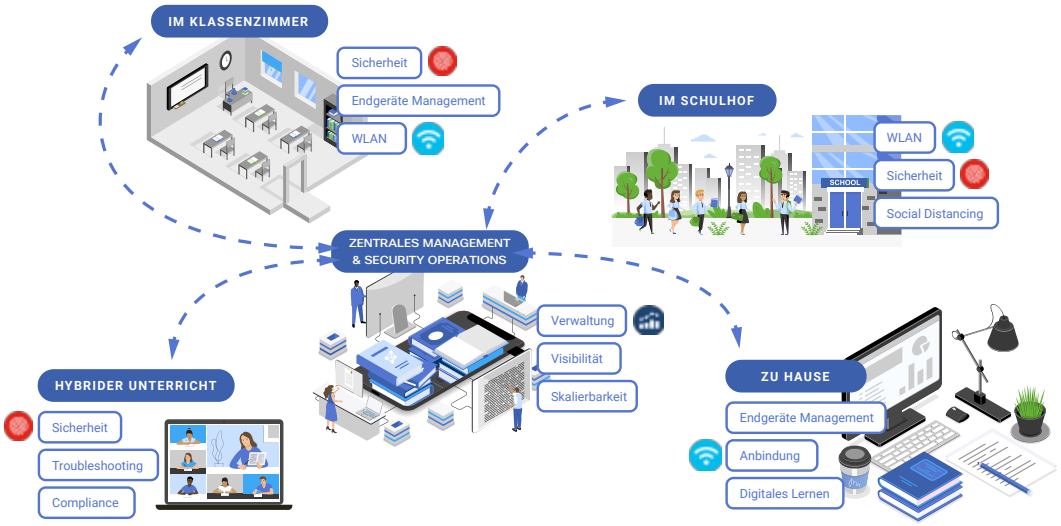
Die Lösungen befähigen Lehrende und Lernende Ihrer Bildungseinrichtung digitale Medien und digitale Inhalte wie beispielsweise Lernsoftware oder -plattformen zu nutzen. Auch die kritische Verwaltung und Bearbeitung von personenbezogen Daten kann problemlos und sicher in digitalen Anwendungen stattfinden.
Neue Lernkonzepte und -kooperationen können flexibel in Ihrer Bildungseinrichtung stattfinden. Die digitale Bildung für Lernende und Lehrende wird ortsunabhängig ermöglicht.

Folgende Cisco Lösungen bieten Ihnen die Möglichkeit und die notwendigen Fähigkeiten, um ein ganzheitliches Sicherheitskonzept zur Digitalisierung Ihrer Schule umzusetzen und ihre Risiken kontinuierlich zu minimieren. Das Fundament bildet dabei Cisco Meraki für LAN, WLAN und SD–WAN Netzwerke für die sichere Schulumgebung:

- **Integriertem Multi Device Management (MDM)**
- **Zentralem Management bzgl Installation, Konfiguration, Monitoring und Optimierung von:**
  - Zugriffsrechten wie z.B. BYOD
  - Einfache Fehleranalyse und -behebung
  - Kinderleichtes ausrollen eines gesamten Netzwerks innerhalb von wenigen Stunden
- **Integrierten Security Fähigkeiten wie Cisco Umbrella DNS-Schutz inkl. Jugendschutzfilter, Rollenbasiert**
- **Netzwerksegmentierung, Firewall / IDS & IPS, Traffic-Analyse & -shaping**
- **Smarte Sensoren für die Messung der Luftqualität, für Tür – und Fensterabsicherungen sowie WLAN abschalten per Knopfdruck z.B. im Klassenraum ohne IT-Kenntnisse**
- **Mögliche Einbindung externer Quellen durch moderne Nutzung der offenen API**
- **Secure Client für schuleigene Endgeräte in der Schule**
  - Meraki Umbrella DNS Roaming Client
  - Duo Mehrfachauthentifizierung (MFA) mit Verhaltensanalyse (Kontextanalyse und Posture Check)
  - Secure Endpoint: Endpoint Detection & Response
  - VPN ins Schulnetzwerk
  - Alternative zu VPN: Duo Beyond für Zugriff auf kritische Applikationen (browserbasiert über http/https)
- **BYOD – Bring your own device**
  - Duo Beyond für den Zugriff auf kritische Applikationen (browserbasiert http/https)
  - Option für Bring-your-own-Device ohne VPN für Schüler*innen

Weitere Mehrwerte für Ihre Schule(n)

- WLAN in der Schule zur Lokalisierung von Personen, Geräten oder Wegefindung
- Gewährleistung der Luft- und Raumqualität durch messen von CO2- und Feinstaubwerten, Temperatur und Geräuschpegel
- Überwachung der Schule gegen unbefugten Zutritt, Vandalismus oder Diebstahl mit smarten Kameras
- Überwachung der Klassenraumbelüftung und Klassenraumauslastung mit Alarmierung während pandemischer Lagen
- Vernetzung und IT-Sicherheit bezüglich Haustechnik
- Stromeinsparungen durch automatisierte Nutzungszeiten
- Nachhaltigkeit durch Herstellerentsorgung
- Abgeordnete Lehrkräfte können sich um den Unterricht kümmern und trotzdem agil eingreifen



Sie haben Fragen?

Kontaktieren Sie uns zu all diesen Themen!
Unsere Expert:innen beraten Sie gerne!

Email:

WIR MACHEN DIGITALISIERUNG EINFACH!

#wirmachendigitalisierungeinfach – eine Initiative von **Cisco Systems GmbH**, **upDATE Gesellschaft für Beratung und Training mbH** und **kommune.digital**.