WHITEPAPER

Bereitstellen einer sicheren Lernumgebung

Schutz für Schüler mit Fortinet

Einleitung

Ob Primar- oder Sekundarbereich, allgemeinbildende oder berufsbildende Schulen – die Bereitstellung einer sicheren Lernumgebung ist ein entscheidender Bestandteil des staatlichen Bildungsauftrags. Heutzutage arbeiten immer mehr Schulen und Bildungseinrichtungen mit Online-Lösungen wie Office 365, Google Classroom und auf AWS oder Azure gehosteten Bildungsanwendungen. Auch Schulnetzwerke, schulübergreifende Systeme und Internet-Zugänge für Mitarbeiter und Schüler werden zunehmend genutzt. Dies alles trägt zur Umsetzung eines zeitgemäßen, anregenden Lehrplans bei, kann jedoch Minderjährige, Lehrkräfte, Schulressourcen und andere Mitarbeiter im Schuldienst gefährlichen Cyber-Bedrohungen aussetzen.

Sicherheitsanforderungen und staatliche Empfehlungen zur Prävention und Security sollen dazu beitragen, dass Schulen und Bildungseinrichtungen ihre Gefährdung durch Cyber-Bedrohungen so gering wie möglich halten. Dazu gehört beispielsweise die Verwendung von inhaltlichen Filtern – so genannten „Content-Filtern" – oder das Blockieren unangemessener Inhalte. Leider lassen sich jedoch heutige Bedrohungen oft nicht eindeutig nur mit Content-Filtern und Firewalls identifizieren. Das ist z. B. bei neuen Malware-Formen der Fall, für die der installierte Virenschutz noch keine Antivirus-Signatur enthält. Auch die schulübergreifende Zusammenarbeit kann zur Gefahr werden, wenn Malware über als vertrauenswürdig geltende Verbindungen übertragen wird, die weder eine Firewall noch einen Content-Filter durchlaufen.

Wussten Sie schon, dass ...

Der Begriff Malware wird häufig mit Ransomware verbunden – der Verschlüsselung von Computer-Festplatten, um Lösegelder für die Freigabe der Daten zu erpressen. Es gibt aber noch viele weitere Arten von Malware, mit denen z. B. Benutzernamen und Passwörter erfasst, persönliche Daten wie Namen oder Adressen gestohlen oder sogar Anwender über die Kamera oder die Aufzeichnung der Tastatureingaben überwacht werden können.

Firewalls, Virenschutz und Content-Filter spielen nach wie vor eine wichtige Rolle beim Blockieren unangemessener Inhalte, aber dennoch kommt es zu Infektionen mit Ransomware wie WannaCry. Die Frage ist: Wie können Schulen und Bildungseinrichtungen einen sicheren Zugriff auf Informationen und die Nutzung von Cloud-Diensten ermöglichen sowie von schulübergreifenden Systemen profitieren, ohne das Lernumfeld durch zu starke Reglementierungen bis hin zur Ineffizienz einzuschränken?

Dieses Dokument richtet sich an alle, die staatliche Empfehlungen und Vorgaben zur digitalen Sicherheit umsetzen und die Eignung der jetzigen IT-Umgebung dahingehend überprüfen möchten. Ein hoher Sicherheitsstandard ist besonders zum Schutz von Minderjährigen wichtig, wie z. B. die Blockierung unangemessener Inhalte durch Web-Filter und Firewalls. Allerdings umfasst eine sichere Umgebung für Minderjährige mehr, als nur den Internet-Datenverkehr zu filtern. In diesem Dokument wird dargelegt, wie Fortinet zu einer sicheren Lernumgebung und einem angemessenen Schutz schulischer Ressourcen zu einem günstigen Preis beitragen kann.

Security im Bildungswesen – mehr als nur eine Firewall

Ein gängiger Ansatz zum Schutz vor Cyber-Bedrohungen besteht darin, zu den bereits installierten Security-Geräten weitere Sicherheitsprodukte hinzuzufügen. Doch dadurch steigt die Komplexität: Es gibt unterschiedlichste Tools für die Geräteverwaltung, bei Beschaffungsverfahren und Support müssen mehrere Anbieter kontaktiert werden und das Netzwerk besteht aus isoliert arbeitenden Geräten, die nicht koordiniert als „ein System" reagieren können. Angesichts des Umfangs und Ausmaßes der Bedrohungen – von durch Ransomware blockierten Computern bis hin zu Schülern, die extremistischen Ansichten ausgesetzt sind – empfiehlt sich ein anderer Ansatz: eine Lösung, die alle schulischen IT-Anforderungen, einschließlich der Sicherheitsfunktionalität, erfüllt und sich unkompliziert verwalten lässt.

Fortinet bietet mit der Fortinet Security Fabric einen modularen Architekturansatz, mit dem neue Bedrohungen schnell erkannt und das gesamte Netzwerk automatisch geschützt werden kann, während die Verwaltung, Überwachung und Konfiguration so einfach wie möglich gehalten wird. Dieser modulare Ansatz ermöglicht die Auswahl der am besten geeigneten Komponenten. Dies bietet greifbare Vorteile für einzelne Schulen, Schulnetze, Bildungseinrichtungen oder auch föderale Behörden, die zentralisierte Dienste für mehrere Schulen und Einrichtungen des Bildungswesens bereitstellen möchten.

Die Philosophie von Fortinet, erstklassige, professionelle Sicherheitslösungen zu wettbewerbsfähigen Preisen anzubieten, kommt den Anforderungen des Bildungswesens entgegen: Schulen und Bildungseinrichtungen können mit Fortinet trotz Haushaltskürzungen und knapper Etats eine einfach zu verwaltende, sichere Konnektivität in hoher Qualität realisieren.

Die Fortinet Security Fabric – ein modularer Ansatz für Schulen

Viele Cyber-Bedrohungen wie WannaCry richten sich nicht gegen bestimmte Ziele, können aber trotzdem zu Störungen des Schulbetriebs bis hin zum Verlust wichtiger Dateien wie Prüfungsunterlagen oder der Notenverwaltung führen. Einige Bedrohungen sind jedoch gezielter und sollten besonders von Schulen stärker ins Augenmerk gefasst werden, wie z. B. die Gefahr, dass Schüler von extremistischen oder ideologischen Gruppen kontaktiert werden. All dies bedeutet, dass Schulen eine Lösung zum Schutz vor einer Vielzahl von Bedrohungen benötigen, die zugleich einfach zu bedienen und zu verwalten ist.

Die Fortinet Security Fabric besteht aus mehreren Technologien, die gemeinsam oder unabhängig voneinander arbeiten. Schulen und Bildungseinrichtungen können bei diesem modularen Ansatz die am besten geeignete Lösung wählen, die sich später an veränderte Anforderungen anpassen lässt. Steht beispielsweise anfangs die Einhaltung von Präventions- und Schutzpflichten an erster Stelle, aber im Lauf der Zeit kommen weitere Security-Anforderungen hinzu, lassen sich zusätzliche Funktionen einfach ergänzen, um das Sicherheitsprofil weiter zu stärken.

Diese Technologien reichen von Firewalls über WLAN-Zugangspunkte, sichere Switche und E-Mail-Gateways bis hin zu Client-Software und sind in einer Vielzahl von Modellen für Implementierungen jeder Größe erhältlich.

Auf den ersten Blick mag sich die Frage stellen, ob diese große Auswahl an Produkten und Lösungen nicht eher für ein Großunternehmen als für eine Bildungseinrichtung infrage kommt. Tatsächlich profitiert auch das schulische Umfeld stark von den meisten Sicherheitslösungen und -produkten, deren Größe und Formfaktor sich auf spezielle Anforderungen abstimmen lässt. Darüber hinaus können viele Security-Komponenten über eine gemeinsame Zentrale verwaltet und überwacht werden, um das tägliche Management so einfach wie möglich zu gestalten.

Mit der Fortinet Security Fabric können Schulen, Bildungseinrichtungen und Schulbehörden ihr Sicherheitsprofil schrittweise durch folgende Maßnahmen verbessern:

1. Erfüllen von Sicherheitsrichtlinien und -empfehlungen
2. Schutzfunktionen, die über reine Sicherheitsmaßnahmen hinausgehen
3. Bereitstellen eines sicheren, einheitlichen Zugangs

1. Erfüllen von Sicherheitsrichtlinien und -empfehlungen

Das Verhindern eines Zugriffs auf schädliche, unangemessene und gefährliche Websites ist wichtig, damit eine Bildungseinrichtung ihre Sicherheitspflichten erfüllen kann. Mit der Fortinet Security Fabric lässt sich verhindern, dass Schüler bösartige Websites besuchen. Auch werden Minderjährige vor unangemessenen Inhalten im Internet geschützt. Dies alles trägt zur Aufrechterhaltung einer sicheren und produktiven Lernumgebung bei.

Mit der Fortinet Security Fabric können Schulen fundierte, automatisierte Entscheidungen darüber treffen, auf welche Websites und Online-Ressourcen Schüler zugreifen und welche Inhalte sie herunterladen dürften – statt den Zugang zu stark zu reglementieren und damit den Bildungsauftrag zu behindern.

BERICHT ÜBER BENUTZERAKTIVITÄTEN (BEISPIEL)

BERICHT ÜBER SCHLÜSSELWÖRTER BEI SUCHABFRAGEN (BEISPIEL)

FUNKTION	FABRIC-KOMPONENTE	NUTZEN FÜR PRÄVENTION, SCHUTZ UND SICHERHEIT
Blockieren des Zugriffs auf unangemessene Websites Überwachen von Suchabfragen bei Google, Bing und Yahoo Detaillierte Browser-Verläufe (Logs) von Benutzern	FortiGate Firewall mit URL-Filter-Subscription	Schulen und Schulbehörden müssen sicherstellen, dass Minderjährige durch geeignete Filter und Überwachungssysteme vor schädlichen und extremistischen Inhalten geschützt werden.
Reporting, Monitoring und Log-Aufbewahrung	FortiAnalyzer	Mit gut verständlichen Berichten und einer zeitlich begrenzten Speicherung von Überwachungsinformationen unterstützt Fortinet Schulen bei der Implementierung von Monitoring-Systemen, um Minderjährige vor unangemessenen Inhalten zu schützen.
Virenschutz für Netzwerk, Computer und Server	FortiGate Firewall mit Antivirus-Subscription auf Netzwerk-Ebene Endpunkt-Schutz mit FortiClient Endpoint Protection	Ein Teil des Schutzes von Minderjährigen vor unangemessenen Inhalten und einer Radikalisierung besteht darin sicherzustellen, dass auf Schüler-Computern keine Malware installiert ist. Malware kann die Rechnernutzung überwachen – z. B. mit einem Keystroke Logger die Tastenanschläge aufzeichnen oder per Fernzugriff die Kamera aktivieren – oder Software installieren, die Minderjährigen anstößige oder unangemessene Inhalte zeigt.
Fernzugriff für Schüler mit Blockierung unangemessener Websites und Inhalte	Endpunkt-Schutz mit FortiClient Endpoint Protection Software	Durch Filtern und Überwachen der Online-Aktivitäten von Schülern außerhalb der Schule können Minderjährige vor unangemessenen und anstößigen Inhalten geschützt werden.

2. Schutz, der über reine Sicherheitsmaßnahmen hinausgeht

Filter und Überwachung sind zwar ein wichtiges Element des Online-Security-Programms von Schulen und Bildungseinrichtungen, sollten aber Teil einer „ganzheitlichen" Sicherheitsstrategie sein. Dazu gehört auch die Abwehr von Bedrohungen, die von Web-Filtern und Firewalls nicht entdeckt werden können – wie per E-Mail verbreitete Malware, Phishing-E-Mail-Kampagnen, über USB-Sticks eingeschleuste Malware und komplexe Bedrohungen, die herkömmlichen signaturbasierten Filtern entgehen.

E-Mail ist die häufigste Methode, um Ransomware und andere Malware sowie unangemessene Inhalte zu verbreiten – entweder durch Anhängen eines infizierten Dokuments oder indem Empfänger zum Anklicken eines Links verleitet werden, der auf eine infizierte Website führt. Firewalls und Web-Filter können jedoch Malware in E-Mails nicht immer identifizieren. Das gilt besonders für neue Malware, für die es noch keine Antivirus-Signaturen gibt.

Weiter sollte ein sinnvoller Schutz nicht nur verdächtige Aktivitäten und Inhalte berücksichtigen, die über das Internet eingeschleust werden können, sondern auch die Verbreitung von Inhalten innerhalb einer Schule oder zwischen kooperierenden Bildungseinrichtungen abdecken.

Die Fortinet Security Fabric unterstützt Schulen mit Web-Filtern, Virenschutz und Überwachungsfunktionen bei der Erfüllung ihrer Präventions- und Sicherheitspflichten. Hiermit lässt sich auch neue Malware erkennen – unabhängig davon, ob sie per E-Mail, auf einem USB-Stick oder über Downloads aus dem Internet eingeschleust werden soll. In den meisten Fällen wird automatisch verhindert, dass Schadsoftware überhaupt in die Schule gelangt. Ein großer Vorteil ist, dass Schulen, Bildungseinrichtungen und Schulbehörden die wichtigsten Security-Komponenten nach Bedarf oder schrittweise implementieren können.

Die leistungsstarken Schutzfunktionen jeder einzelnen Komponente werden durch die Fortinet Security Fabric auf einzigartige Weise erweitert: Alle Security-Komponenten können Informationen austauschen, automatisch aktualisiert werden und abgestimmt wie ein einziges System reagieren. Die effektivste Bedrohungsabwehr wird daher erreicht, wenn die Fabric möglichst viel genutzt wird:

Beim deutschen Bundesministerium für Bildung und Forschung laufen mehrere Programme und Forschungsinitiativen zur Vernetzung und Sicherheit digitaler Systeme (https://www.forschung-it-sicherheit-kommunikationssysteme.de), die auch das Bildungswesen betreffen. Veranstaltungen wie die wissenschaftliche Jahreskonferenz des Forums Privatheit beschäftigen sich u. a. mit der Frage, wie sich Datenschutz und Sicherheitsanforderungen in Schulen und im Privaten für Minderjährige umsetzen lassen. Als Mitglied der Internet Watch Foundation (IWF) bietet Fortinet die notwendigen Security-Funktionen zum Schutz von Kindern und Jugendlichen. Dazu gehört z. B. die Sperrung des Zugangs zu Bildern und Inhalten von Kindesmissbrauch sowie Web-Filter für rechtswidrige und terroristische Inhalte, eine altersgerechte differenzierte Filterung und – neben Web-Filtern für das Internet - auch Filter für den Datenverkehr von Smartphone-Apps. Weitere Informationen erhalten Sie bei Ihrem Fortinet Account Manager oder Ihrem Händler.

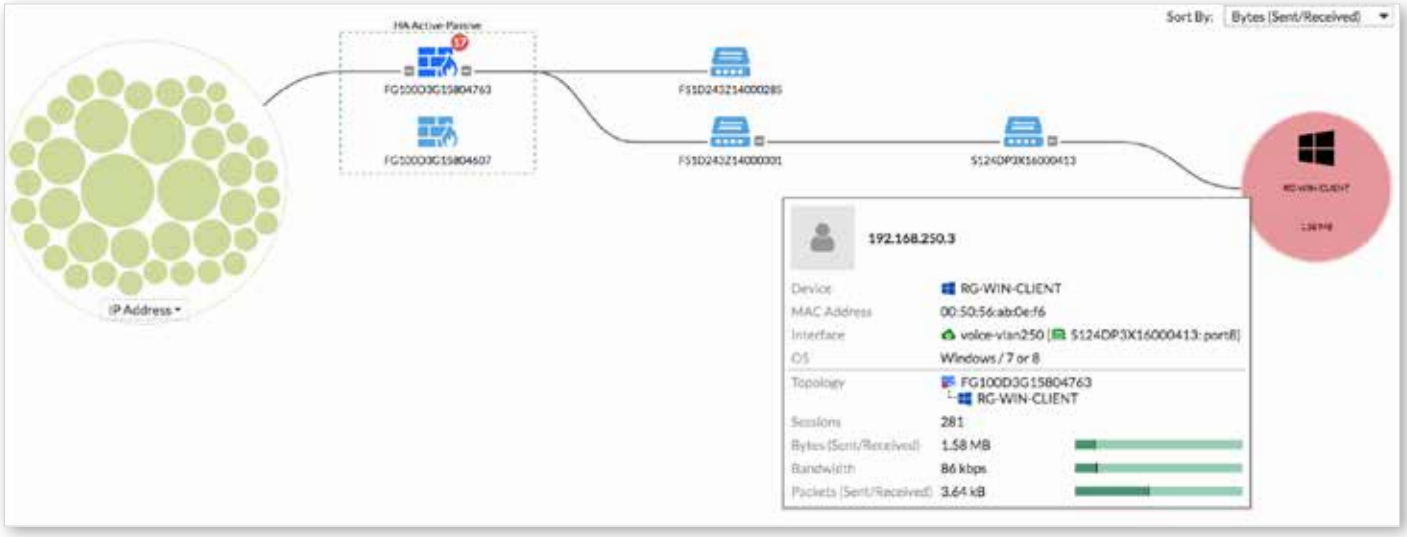
FUNKTION	FABRIC-KOMPONENTE	NUTZEN FÜR PRÄVENTION, SCHUTZ UND SICHERHEIT
Konformitätsprüfung und Quarantäne von Endgeräten	Endpunkt-Schutz mit FortiClient Endpoint Protection	Verhindert, dass unzureichend geschützte Computer mit dem Netzwerk verbunden werden und minimiert das Risiko einer Kompromittierung von Computern sowie die Verbreitung von Infektionen im Schulnetzwerk. Ein unzureichender Schutz zeigt sich z. B. darin, dass es auf einem Rechner keine Antivirus-Software oder keine persönliche Firewall gibt oder Sicherheitslücken nicht durch regelmäßiges Patching geschlossen wurden.
Erkennung unbekannter Malware	FortiSandbox	Identifiziert bislang unbekannte Malware, die von Antivirus-Signaturen und Web-Filtern nicht erkannt werden kann.
Sichere E-Mails: E-Mail-Quarantäne, Spam- und Anti-Phishing-Schutz	FortiMail Kann entweder in Office 365 und andere E-Mail-Lösungen integriert werden oder als eigenständige E-Mail-Plattform dienen.	Erkennt verdächtige E-Mails und Inhalte und stellt diese unter Quarantäne, damit sie nicht an Schüler und Mitarbeiter gesendet werden. Dies reduziert das Infektionsrisiko per E-Mail und schützt E-Mail-Benutzer auch vor neuer Malware.
Erweitertes Monitoring und Reporting	FortiAnalyzer	Wichtig ist zu wissen, was im Schulnetz passiert, damit Sicherheitsvorfälle und -bedrohungen schnell erkannt und behoben werden.
Compliance-Reporting (z. B. PCI) und Multi-Vendor-Monitoring	FortiSIEM	Das Erstellen von Berichten (Reporting) ist ein wesentlicher Bestandteil vieler Konformitätsanforderungen. Erfolgt keine Meldung, kann dies in einigen Ländern zu Geldbußen oder zur Entfernung aus Netzwerken oder Leistungsstrukturen führen.
Überwachung des Cloud-Zugriffs	FortiCASB	Das Überwachen und Scannen von Daten, die in Cloud-Anwendungen wie Dropbox gespeichert sind, erweitert die schulische Bedrohungsabwehr zum Schutz der Lernenden.

3. Sicherer, einheitlicher Zugang

Um die Wahrscheinlichkeit einer Malware-Infektion zu minimieren und die Ausbreitung einer Infektion einzudämmen, ist es wichtig, dass die Durchsetzung der Sicherheitsrichtlinien so nah wie möglich am Endanwender erfolgt. Fehlen auf einem Schüler-Computer z. B. ein aktueller Virenschutz oder Patches, ist es wahrscheinlicher, dass er mit Malware infiziert wird. Kompromittierte Rechner mit Zugang zum vertrauenswürdigen Schulnetzwerk können dann andere Computer in der Schule infizieren. Durch die Durchsetzung der Sicherheitsrichtlinien wird ein Rechner auf dem neuesten Software-Stand gehalten. Unsichere Computer lassen sich lokal isolieren und überprüfen, um das Malware-Risiko zu minimieren.

Entscheidend ist, dass die Security weitestmöglich in das zugrunde liegende Netzwerk integriert wird – ohne die übliche Trennung von Netzwerk-Verbindungen und Netzwerk-Sicherheit. Es empfiehlt sich ein umfassenderer Ansatz, bei dem LAN- und WLAN-Zugänge die Security-Infrastruktur erweitern. Unabhängig von der Art der Verbindung wird so ein konsequentes Sicherheitsprofil mit einheitlichem Schutz erreicht. Dieser Ansatz vereinfacht auch Beschaffungsverfahren und das tägliche Netzwerk-Management.

Die Ethernet-Switche und Wireless Access Points (APs) von Fortinet spielen eine aktive Rolle bei der Bereitstellung einer sicheren Umgebung für Mitarbeiter und Schüler, da sie integriert mit Fortinet-Firewalls und anderen Fortinet-Security-Geräten zusammenarbeiten. Sicherheitsrichtlinien können so auf Ebene des Benutzerzugriffs durchgesetzt werden. Auch die Verwaltung, Konfiguration und Überwachung wird vereinfacht. Benutzer können unter Quarantäne gestellt, der Datenverkehr gefiltert und verschiedene Benutzer voneinander isoliert werden.



TOPOLOGIE-ANSICHT MIT DER SECURITY FABRIC

Fazit

Einrichtungen des Bildungswesens – unabhängig davon, ob sie ihr eigenes Netzwerk betreiben, Teil eines Schulverbandes sind oder es sich um eine Schulbehörde handelt –, sind für die Sicherheit der Lernenden vor schädlichem oder unangemessenem Material verantwortlich. Präventions- und Sicherheitsrichtlinien stellen hierbei den ersten Schritt dar. Zudem besteht aber auch die Notwendigkeit, Mitarbeiter, Schüler und Schulressourcen vor neuen Cyber-Bedrohungen wie Ransomware zu schützen und eine zuverlässige, sichere Lernumgebung zu gewährleisten.

Die Fortinet Security Fabric bietet für diese Zwecke einen modularen Ansatz, der sich durch eine einfache Konfiguration und Überwachung sowie eine hohe Effektivität auszeichnet. Mit geeigneten Security-Komponenten, deren Größe und Funktionalität optimal auf die Sicherheitsanforderungen einer Einrichtung abgestimmt sind, lassen sich Präventiv- und Schutzmaßnahmen im Bildungswesen zu angemessenen Kosten realisieren.

Wenn Sie weitere Informationen wünschen oder sich die Möglichkeiten von Fortinet-Sicherheitslösungen zeigen lassen wollen, wenden Sie sich bitte an Ihren Fortinet Account Manager oder an Ihren Händler.

FORTINET

www.fortinet.com/de

5. Mai 2020, 10:33 Uhr

153859-1-0-DE