Filterlösung/ Proxy für Internetzugang der SuS (vor allem via iPad, Android)

Beitrag von „Schiri“ vom 11. Juli 2018 06:26

Liebe Mitforisten,

seit geraumer Zeit störe ich mich offen gesagt daran, wie kompliziert es an unserer Schule ist, SuS- bzw. auch LuL-Geräte am Netzwerk anzumelden (Anmeldedaten sind für alle individuell vorhanden).

Unter Windows ist das alles kein Problem. Abhängig von der zugewiesenen Rolle greift der Jugendschutzfilter verschieden stark (wobei es auch sehr nervig ist, wenn die SuS plötzlich die Seite der Agentur für Arbeit nicht mehr aufrufen dürfen, aber das ist jetzt ein anderer Hut) und mit dem LogIn mit Hilfe der eigenen Benutzerdaten ist man klar im Netzwerk authentifiziert.

Neben den KuK, die das "schon immer" haben, haben wir nun seit geraumer Zeit aber auch für einzelne Klassen iPads bzw. nutzen Android-Geräte. Beide erfordern ja beim Starten/Aktivieren erstmal keine Anmeldung und sind nicht wie die Windowsgeräte direkt ins Netzwerk eingebunden. Ergo müssen die SuS, wenn sie Internet an den Geräten nutzen wollen, einigermaßen tief in die Einstellungen um den Proxy und ihre Benutzerdaten einzutragen. Dauert bis es bei allen Geräten läuft (wenn es das überhaupt tut) mehrere wertvolle Minuten und stört mich total.

Die Argumentation dahinter ist scheinbar, dass wir gegen geltendes Recht verstoßen, wenn wir SuS ohne persönliche Authentifizierung und entsprechende Filterung ins Netz lassen, was für mich auch prinzipiell total nachvollziehbar ist.

Ich frage mich nur, wie andere Schulen die Authentifizierung im Netzwerk regeln, oder ob sogar in bestimmten Kontexten darauf verzichtet wird. Auch ist mir unklar, ob die Notwendigkeit der Authentifizierung auch für Lehrkräfte gegeben ist. Ich freue mich über den Erfahrungsaustausch :).

Besten Dank!

Beitrag von „hodihu“ vom 11. Juli 2018 17:24

Hallo Schiri,

wir verwenden bei uns seit einigen Jahren keinen "klassischen" Internet-Filter mehr, der ja einerseits immer mit dem Problem der Proxy-Einträge zu kämpfen hat, andererseits bei https-Seiten grundsätzlich gar nicht mehr richtig filtern kann. Hier wird nunmehr per Open-DNS (=Cisco Umbrella) gefiltert. D.h., dass die Endgeräte per DHCP den DNS-Server von Open-DNS mitgeteilt bekommen. Jede DNS-Anfrage, die dort eingeht, wird anhand einstellbarer Black- und Whitelists (ähnlich zum Proxy-Filter) beantwortet oder eben auf eine Sperrseite umgeleitet. Hat eine paar Nach-, für uns aber mehr Vorteile. Was dabei nicht gegeben ist, allerdings laut KM- und Regierungsaussage auch nicht nötig ist, ist die persönliche Authentifizierung der Schüler.

Achja: kost' auch nix 

Viele Grüße
Holger

Beitrag von „kodi“ vom 11. Juli 2018 20:37

Wir nutzen logoDIDACT. Windowsgeräte booten dabei ein Image aus dem Netz, dass sich selbst zurücksetzt.
Tablets und Co binden wir per WLAN mit Radiusauthentifizierung ein. Schüler und Lehrer sind dadurch auch mit anderen Endgeräten mit ihrem Benutzeraccount authentifiziert und der Webfilter greift ebenfalls.

Beitrag von „Landlehrer“ vom 15. Juli 2018 02:20

Wir nutzen den Schulfilter Plus, um den Anforderungen des Kinder- und Jugendschutzes gerecht zu werden.

https://www.time-for-kids.de/produkte/schul...outer-plus.html

---

Beitrag von „madhef“ vom 15. Juli 2018 11:10

> Zitat von Landlehrer
>
> Wir nutzen den Schulfilter Plus, um den Anforderungen des Kinder- und Jugendschutzes gerecht zu werden.

Oh ja... ganz toll. Hatte vor einigen Jahren mit denen eine böse Auseinandersetzung, da u.a. die Seiten der Unfallkasse Hessen nicht mehr aufrufbar waren. "Wir wollen halt sichergehen, dass den Kindern keine Versicherung aufgeschwatzt wird." (frei wiederggegeben)

Beitrag von „Kalle29“ vom 16. Juli 2018 00:39

> Zitat von Landlehrer
>
> Wir nutzen den Schulfilter Plus, um den Anforderungen des Kinder- und Jugendschutzes gerecht zu werden.

Hatten wir auch, wurde aber durch eine "Premium"-Linuxvariante in einer Box ersetzt, die alle HTTP/HTTPS-Anfragen via VPN irgendwo hin umleitet. Das System funktioniert so gut, dass es jeden Tag neu gestartet werden muss, da es die HTTP/HTTPS-Anfragen (also Port 80/443) dann komplett blockt. Was das Ding natürlich nicht filtert sind Anfragen auf anderen Ports, eigene VPNs oder ähnliche Dinge. Unser Schulträger findet das System aber offenbar ganz toll, ein 16 Jähriger mit ner Fritzbox zuhause und einem fünfminütigen Crashkurs über VPN-Zugänge lacht da natürlich nur drüber.

Letztlich frage ich mich, auf welcher Grundlage wir da so einen Aufriss machen. Es ist ja nicht so, dass die SuS nicht ständig ihr Smartphone in der Tasche haben, auf dem you(-porn/-tube/-musik) ohne Probleme jederzeit abrufbar ist. Im Zweifel lass ich nen Windows-Server (oder nen Linuxserver) den DNS-Dienst übernehmen und lasse die Anfragen der Clients dort mittracken. Einmal die Woche die Liste nach gängigem Schund durchsuchen, ein paar Exempel statuieren und fertig wäre die Sache. Stattdessen muss ich mich mit dem Filteranbieter rumschlagen, der auch beispielsweise Skype blockt und damit Austauschkontakte mit Partnerschulen im Ausland verhindert. Die Aufhebung des Filters hierfür hat solange gedauert, dass der Kollege mit seiner Klasse einfach ins Internet Cafe gegangen ist. #neuland

---

Beitrag von „Scooby“ vom 16. Juli 2018 18:35

Wir verwenden eine Sophos UTM (SG230), die uns nicht nur den traffic filtert und den Datenverkehr überwacht, sondern auch die VPN-Zugänge von außen ermöglicht, mehrere virtuelle Netze im Haus zur Verfügung stellt und im Grunde alles macht, was Netzwerksteuerung betrifft (auch sowas wie Load Balancing mehrerer DSL-Leitungen). Dazu braucht es dann auch ein entsprechendes Softwarepaket, hier haben wir uns für das FullGuard-Bundle entschieden (E-Mail Protection, Network Protection, Web Protection, Webserver Protection und Wireless Protection).

Einerseits macht es einfach auch Spaß mit professionellen Tools zu arbeiten (statt mit Nischenprodukten für Schulen), andererseits kann die UTM verlässlich https-Traffic aufbrechen und stellt so sicher, dass geblockte Seiten auch wirklich nicht zugänglich sind.

Funktioniert gut, ist aber halt auch nicht ganz billig.

Beitrag von „Mikael“ vom 16. Juli 2018 18:42

> Zitat von Scooby
>
> ... eine Sophos UTM (SG230)...

Da habt ihr aber einen großzügigen Schulträger: https://utm-shop.de/utm/utm-hardwa...umber=SB2312SEU

4800€ brutto für das erste Jahr (in der "Budget"-Variante), für jedes weitere Jahr kommen knapp 2000€ brutto dazu.

Gruß !

Beitrag von „Scooby“ vom 16. Juli 2018 18:58

> Zitat von Mikael
>
> Da habt ihr aber einen großzügigen Schulträger: https://utm-shop.de/utm/utm-hardwa...umber=SB2312SEU
> 4800€ brutto für das erste Jahr (in der "Budget"-Variante), für jedes weitere Jahr

> kommen knapp 2000€ brutto dazu.

Ja und nein. Vor allem haben wir einen guten EDV-Partner, der bei Sophos alle drei Jahre Projektkonditionen raushandelt. Letztes Mal haben wir für drei Jahre rund 2.700 Euro bezahlt, also etwa 900 Euro / Jahr. Und ja, wir haben in der Tat einen Sachaufwandsträger, der verstanden hat, dass es Sinn macht auf professionelle Produkte zu setzen, weil das die Nachfolgekosten erheblich senkt. Eine Arbeitsstunde meines IT-Partners kostet mich rund 80,- Euro; wenn durch den Einsatz professioneller Hard- und Software 10 Stunden im Jahr eingespart werden, ist das Ding schon bezahlt.

Die Rechnung geht natürlich nur auf, wenn die grundsätzliche Bereitschaft da ist, die Kosten für EDV zu bezahlen und man nicht auf die sog. "Ehda"-Stunden des Systembetreuers setzt (--> das soll der Systembetreuer machen, weil der ist ja eh da).

Beitrag von „Kalle29“ vom 16. Juli 2018 19:01

> Zitat von Scooby
>
> UTM verlässlich https-Traffic aufbrechen

Klär mich hier mal auf. Meines Wissens nach funktioniert das nur, wenn das Gerät quasi einen "man in the middle"-Server simuliert und die nach außen gehende HTTPS-Verschlüsselung ändern und dann nach innen weitergibt. Das bedeutet aber, dass auf dem Gerät alle verschlüsselten Daten im Klartext durchgeleitet werden - beispielsweise meine E-Mailkennwörter und weitere Zugangsdaten? Daten, die ich z.B. über Logineo NRW verschlüsselt übertragen würde, wären auf dem Gerät also entschlüsselt? Oder gibts eine andere Variante, wie das Gerät das leisten kann?

Sollte dies nämlich nur mit der o.g. Variante gehen, wäre das aus meiner Sicht der Tod dieser Plattform, da eine durchgehende Verschlüsselung nicht gewährleistet ist.

Beitrag von „SteffdA“ vom 16. Juli 2018 19:03

> Zitat von Schiri

> Die Argumentation dahinter ist scheinbar, dass wir gegen geltendes Recht verstoßen, wenn wir SuS ohne persönliche Authentifizierung und entsprechende Filterung ins Netz lassen, was für mich auch prinzipiell total nachvollziehbar ist.

Welches konkrete geltende Recht ist das denn?

Beitrag von „Landlehrer“ vom 22. Juli 2018 01:52

> Zitat von Kalle29
>
> Klär mich hier mal auf. Meines Wissens nach funktioniert das nur, wenn das Gerät quasi einen "man in the middle"-Server simuliert und die nach außen gehende HTTPS-Verschlüsselung ändern und dann nach innen weitergibt. Das bedeutet aber, dass auf dem Gerät alle verschlüsselten Daten im Klartext durchgeleitet werden - beispielsweise meine E-Mailkennwörter und weitere Zugangsdaten? Daten, die ich z.B. über Logineo NRW verschlüsselt übertragen würde, wären auf dem Gerät also entschlüsselt? Oder gibts eine andere Variante, wie das Gerät das leisten kann?
> Sollte dies nämlich nur mit der o.g. Variante gehen, wäre das aus meiner Sicht der Tod dieser Plattform, da eine durchgehende Verschlüsselung nicht gewährleistet ist.

Der Schulfilter hat ein selbstsigniertes Zertifikat und hängt sich in die Kommunikation zwischen Client und Server. Die Profis ersetzten selbst Google durch ihre eigene Suchmaschine. 

https://www.time-for-kids.de/loesungen/sichere-suche.html

Beitrag von „Kalle29“ vom 22. Juli 2018 12:25

> Zitat von Landlehrer
>
> Der Schulfilter hat ein selbstsigniertes Zertifikat und hängt sich in die Kommunikation zwischen Client und Server

Also genauso wie ich vermutet habe, richtig? Bei uns war der Kram auch mal angedacht (inkl. Zertifikat, dass wir auf allen Clients verteilen sollten). Aber offenbar hat das jemand gestoppt.

Seit Jahren nix mehr davon gehört.

Beitrag von „Scooby“ vom 22. Juli 2018 14:32

> Zitat von Kalle29
>
> Klär mich hier mal auf. Meines Wissens nach funktioniert das nur, wenn das Gerät quasi einen "man in the middle"-Server simuliert und die nach außen gehende HTTPS-Verschlüsselung ändern und dann nach innen weitergibt.

Soweit ich das verstehe (bin nicht der SysAdmin an der Schule), wird das wohl so sein. Du kannst dich aber beim Hersteller gern selbst informieren:
https://www.sophos.com/de-de/products...management.aspx

Nachdem zunehmend fast der komplette Traffic im Netz über https läuft, setzen lt. Auskunft unseres IT-Dienstleisters mittlerweile die meisten Unternehmen, Banken sowieso, auch Behörden auf entsprechende Dienste, da sie sich ansonsten den Webfilter auch sparen könnten (reicht ja ein kleines s nach http dazuzuschreiben, wenn der Filter anschlägt)...

Beitrag von „Kalle29“ vom 22. Juli 2018 15:03

Ach, da hab ich gar nicht so sehr das Interesse dran (obwohl ich der Admin der Schule bin). Ich warte dann einfach auf eine Antwort des Schulträgers darauf, wie bei einer Umgehung der durchgehenden Verschlüsselung durch dieses System die Nutzungsbedingungen von Logineo.NRW (und vermutlich so ziemlich jedem anderen Dienst) eingehalten werden kann.

> Zitat
>
> Zur Nutzung von LOGINEO NRW ist eine individuelle Anmeldung mit Benutzernamen und Passworterforderlich. Für den Zugriff auf besonders schützenswerte Daten im Daten-SAFE ist darüber hinaus einweiteres Passwort erforderlich.**Die Passwörter sind vertraulich zu behandeln und in regelmäßigen Abständen zu ändern, insbesondere wenndie Vermutung besteht, dass ein Passwort anderen Personen bekannt geworden ist.** Das Arbeiten inLOGINEO NRW unter einem fremden Zugang ist nicht gestattet

Da ist es mir auch relativ wumpe, dass dieser Vorgang automatisiert stattfindet.

Beitrag von „Scooby“ vom 23. Juli 2018 17:06

> Zitat von Kalle29
>
> Ach, da hab ich gar nicht so sehr das Interesse dran (obwohl ich der Admin der Schule bin). Ich warte dann einfach auf eine Antwort des Schulträgers darauf, wie bei einer Umgehung der durchgehenden Verschlüsselung durch dieses System die Nutzungsbedingungen von Logineo.NRW (und vermutlich so ziemlich jedem anderen Dienst) eingehalten werden kann.

So, heute hab ich die Geschichte mal überprüft und bin dabei auf ein durchaus interessantes Loch in unserer "Internet-Sicherheit" gestoßen; insofern vielen Dank für deine kritische Nachfrage. Tatsächlich macht unsere UTM nur URL-Filtering und bricht https NICHT auf. Das führt dazu, dass die google Bildersuche, wenn man google via https aufruft und mit schlüpfrigen Suchwörtern füttert, überaus pikante Ergebnisse ausspuckt und zwar auch in den Computerräumen. Bin mal gespannt, was mein ITler dazu sagt