# Okiełznaj szkolny internet

Coraz więcej szkół w Polsce ma dostęp do internetu. I coraz częściej wśród dyrektorów i nauczycieli pojawiają się wątpliwości: jak połączyć możliwość udostępniania uczniom sieci z ochroną przed nieodpowiednimi treściami.

photopin.com

W 2013 r. dostęp do internetu miało 64 proc. szkół w polskich miastach, na wsiach odsetek ten wyniósł 56 proc. – wynika z danych Komisji Europejskiej. Jednak prawdopodobnie w ciągu 2-3 lat dogonimy europejską czołówkę, gdzie dostęp do internetu ma 90 proc. placówek (np. Litwa i Czechy). Tymczasem jeśli szkoła zapewnia uczniom dostęp do internetu, jej obowiązkiem (a konkretnie – obowiązkiem dyrektorów, nauczycieli i opiekunów szkolnych pracowni komputerowych) jest zabezpieczenie uczniów przed treściami, które mogą zagrozić ich prawidłowemu rozwojowi. Szkoła zobowiązana jest w szczególności zainstalować i aktualizować oprogramowanie zabezpieczające. Poza tym nauczyciel ma obowiązek kierowania się dobrem uczniów, troską o ich zdrowie, postawę moralną i obywatelską z poszanowaniem godności osobistej ucznia. Mówi o tym ustawa o systemie oświaty w artykułach 4 i 4a. Tymczasem w internecie czyha na młodych ludzi coraz więcej zagrożeń, bywa, że ich źródłem są sami uczniowie. A odpowiedzialność za działania uczniów w sieci ponosi dyrektor i nauczyciele. Co zatem zrobić?

## Daleko od ideału

Najprościej byłoby internet w szkole wyłączyć. Ale takie rozwiązanie oznaczałoby nie tyle zatrzymanie w rozwoju (zarówno placówki, jak i jej wychowanków), co regres. Tym bardziej, że w szkołach powszechny jest dziennik elektroniczny, internet w znakomity sposób ułatwia i uatrakcyjnia prowadzenie zajęć, a dla uczniów, korzystających z sieci prawie na okrągło, jest czymś tak naturalnym, jak powietrze.

Szkoły radzą sobie zatem z tym problemem inaczej. Najczęściej korzystają z filtrów programowych zainstalowanych na komputerach. Takie rozwiązanie ma jednak wady. Trzeba je instalować na każdym urządzeniu oddzielnie (opłaty licen-

### Prawo

**Ustawa o systemie oświaty**
**Art. 4.**
Nauczyciel w swoich działaniach dydaktycznych, wychowawczych i opiekuńczych ma obowiązek kierowania się dobrem uczniów, troską o ich zdrowie, postawę moralną i obywatelską z poszanowaniem godności osobistej ucznia.
**Art. 4a.**
Szkoły i placówki zapewniające uczniom dostęp do Internetu są obowiązane podejmować działania zabezpieczające uczniów przed dostępem do treści, które mogą stanowić zagrożenie dla ich prawidłowego rozwoju, w szczególności zainstalować i aktualizować oprogramowanie zabezpieczające.

cyjne także dotyczą każdego urządzenia z osobna), brakuje też raportujących narzędzi administracyjnych powiadamiających administratora o tym, który uczeń złamał regulamin korzystania z internetu. Poza tym w każdej szkole znajdą się szczególnie uzdolnieni informatycznie uczniowie, dla których wyłączenie filtra nie będzie stanowiło problemu. Dodatkowe mankamenty takiego rozwiązania to słaba wydajność (jest ona uzależniona od mocy stacji roboczej, co oznacza, że starsze komputery mogą działać jeszcze wolniej z powodu *zamulenia* przez filtr), brak ochrony WiFi (szczególnie prywatnych urządzeń uczniów – smartfonów, tabletów – na których nie można zainstalować filtra). Uciążliwe są też aktualizacje, które dokonują się na każdym urządzeniu osobno, co w przypadku sporej liczby komputerów w szkole znacznie ogranicza przepustowość łącza internetowego.

## Kompleksowo

Rozwiązaniem, które pozwala wyeliminować powyższe niedogodności jest Unified Threat Management (UTM) – w wolnym tłumaczeniu: zintegrowany system zarządzania zagrożeniami – instalowany między internetem a szkolną siecią. UTM integruje się z dziennikiem elektronicznym lub innymi bazami użytkowników, poza tym chroni i filtruje wszystkie urządzenia w sieci, przy czym nie wymaga instalowania na nich żadnego oprogramowania – aktualizuje się tylko maszynę centralną. Rozwiązanie to chroni jednocześnie sieć LAN i WiFi, filtruje nie tylko strony WWW, lecz także aplikacje. Jest niewrażliwe na zmiany ustawień stacji roboczych a centralny panel administracji i raportowania umożliwia szybki dostęp do informacji o tym, co robią uczniowie. Dodatkowym atutem jest opłata licencyjna, która dotyczy tylko jednego urządzenia, a nie wszystkich stacji.

### UTM – najważniejsze zadania

- współpraca z wieloma systemami (Windows, MacOS, – Firewall
- Web Application Firewall (WAF)
- Antywirus
- Antyspam
- Filtrowanie stron WWW i aplikacji
- Intrusion Prevention System (IPS)
- IPSec VPN, SSL VPN
- Zarządzanie przepustowością łącza
- Zarządzanie kilkoma łączami internetowymi
- Moduł raportujący

## Bat na cybercwaniaka

Korzyści z wdrożenia UTM w szkole jest wiele. Poniżej przedstawiamy je na przykładzie urządzeń Cyberoam UTM.

Rozwiązanie wspiera YouTube for Schools, co oznacza, że możemy zablokować ogólnodostępne treści z YouTube zezwalając jedynie na oglądanie filmów z kategorii EDU. Możemy też blokować nieodpowiednie treści (np. pornografia) na wszystkich urządzeniach przenośnych korzystających ze szkolnej sieci (wymuszenie mechanizmu Google Safe Search). Każdy użytkownik sieci może być poinformowany o zablokowaniu danej strony lub kategorii stron internetowych – wtedy na jego urządzeniu wyświetli się komunikat z informacją o przyczynach blokady. Kolejną zaletą Cyberoam UTM, szczególnie w szkolnej rzeczywistości, jest rozpoznawanie Gadu-Gadu, stron i aplikacji typu proxy (m.in. JAP, Tor, Ultrasurf), które mogą posłużyć uczniom do obejścia standardowych zabezpieczeń (filtrów treści) w celu uzyskania dostępu do nieodpowiednich treści. Nie bez znaczenia jest też możliwość wyświetlania na żywo wszystkich aplikacji uruchomionych na urządzeniach przenośnych w szkole. Chodzi o m.in. Facebooka, YouTube, Skype, Gadu-Gadu, radio internetowe. Administrator ma dostęp do informacji o aktualnym i historycznym użyciu łącza, dzięki czemu może bardzo szybko zidentyfikować użytkowników pobierających duże pliki (filmy, gry), które *zapychają* szkolną sieć.

## Prewencja i edukacja

Cyberoam UTM pozwala na ustawienie polityk bezpieczeństwa dla konkretnego użytkownika lub dla grupy użytkowników. Możemy zatem określić je oddzielnie dla pracowników administracji, nauczycieli, uczniów czy gości – niezależnie od komputerów, z których w danym momencie korzystają (oznacza to, że np. dyrektor, który ma większe uprawnienia niż nauczyciele, może z nich korzystać przy użyciu komputera

znajdującego się w pokoju nauczycielskim – oczywiście po zalogowaniu).

Rozwiązanie to pozwala także na łatwy i skuteczny podział pasma internetowego, zgodnie z naszymi preferencjami. Możemy zatem określić pasmo dla pracowników administracji, dla nauczycieli do wykorzystania podczas lekcji czy na pozostałe cele (np. internet dla rodziców podczas wywiadówek, dla nauczycieli podczas rad pedagogicznych, dla gości itp.). Pasma możemy określić dla konkretnych użytkowników, wybranej aplikacji w wybranym przedziale czasu, np. zapewnić pasmo dyrektorowi w czwartek między 10 a 11 – na czas wideokonferencji z dyrektorem partnerskiej placówki.

Bardzo ważną funkcją Cyberoam UTM jest bogate raportowanie. Pozwala na obserwację stron i aplikacji sieciowych, z których korzystają konkretni użytkownicy. W praktyce oznacza to, że jeśli jakiś uczeń zamieści w sieci nielegalne lub nieodpowiednie treści, będziemy mogli bez problemu określić, kto to był oraz z którego korzystał urządzenia. Dzięki temu w przypadku np. naruszenia prawa przez ucznia (publikowanie obraźliwych, szkalujących treści, naruszenia ciszy wyborczej itp.) odpowiedzialność spocznie na nim, nie zaś na dyrektorze placówki. Podobnie w przypadku pobierania nielegalnych treści z internetu (pirackie filmy, muzyka, oprogramowanie) – także wtedy będziemy mogli bez trudu zidentyfikować konkretną osobę, która naruszyła prawo.

Ciekawą możliwością oferowaną przez Cyberoam UTM jest blokowanie ruchu internetowego z określonych państw. Dzięki temu szkoła może zminimalizować ryzyko ataków sieciowych z krajów, gdzie bezpieczeństwo sieciowe pozostawia wiele do życzenia.

Rozwiązanie to może pełnić także funkcje edukacyjne. Dzięki niemu można uświadomić uczniów, że ich działania w sieci (także w domu) mogą być monitorowane, a co za tym idzie w internecie nikt nie pozostaje anonimowy: na podstawie logów przechowywanych przez określone urządzenia sieciowe Policja (czy inne służby) może z łatwością namierzyć osoby, które w cyberprzestrzeni beztrosko łamią prawo w przeświadczeniu o swojej bezkarności.

## UTM kontra programowy filtr

**Filtr:**
- konieczna instalacja na każdym urządzeniu
- licencjonowanie (opłaty) za każde urządzenie
- brak narzędzi administracyjnych i raportowania
- wrażliwość na uzdolnionych informatycznie uczniów
- wydajność zależna od mocy stacji roboczej
- przy pobieraniu aktualizacji każda stacja robi to oddzielnie (wysysa internet)
- brak ochrony sieci WiFi

**Unified Threat Management:**
- chronione i filtrowane są wszystkie urządzenia w sieci
- nie ma potrzeby instalowania oprogramowania na stacjach roboczych
- aktualizacje dotyczą tylko maszyny centralnej
- centralny panel administracji i raportowania
- jednoczesna ochrona sieci LAN i WiFi
- niewrażliwy na zmiany ustawień na stacjach roboczych
- opłata za licencje tylko dla jednego urządzenia