

To filter or not to filter

Auteur: Hans Walrecht

Inleiding

Ons dilemma is gelukkig minder ernstig dan dat van die arme Hamlet. Toch is het filteren van internet voor onze leerlingen momenteel een hot item. Wat zijn de mogelijkheden? Moeten we wel filteren? Kan het anders?

Laatst liep ik in een oude stad door een straatje waar ik nooit kom. Nu kwam het uit zo via de kortste route naar het centrum te lopen. Tot mijn verrassing zag ik opeens allerlei etalages met levend handelswaar. Onverwachts was ik in de rosse buurt van de stad terechtgekomen. Ik moest toen denken aan internet op school. Daar kunnen leerlingen ook plotseling iets tegenkomen, wat ze niet verwacht hadden. Hoe ga je daar mee om? Als je het van tevoren weet, zou je ze blinddoeken kunnen geven, of een andere straat nemen. Ongetwijfeld zullen er kinderen zijn die stiekem de blinddoek oplichten of na schooltijd nog eens dat straatje gaan bekijken. Dit straatje voor de kinderen verbergen is dus een onmogelijke zaak. Als het de leerkracht evenwel niet lekker zit, kunnen we ook onze toevlucht nemen tot iets waarvoor we allemaal gestudeerd hebben: opvoeding. Met dit overtrokken voorbeeld wil ik de kern van het probleem aangeven: internet is niet goed te filteren, dus zul je wat anders moeten bedenken.

Foute sites

Is het allemaal zo erg gesteld met internet? Ik denk dat het wel meevalt. Zelf ben ik al vanaf de zomer van 1994 bezig met het surfen over internet. Toen waren er nog geen 3000 sites en kwam je alleen ideële instellingen tegen en een enkel onderzoeksinstituut. Nu zijn er honderden miljoenen. Daarbij zijn ook veel sites die helaas informatie geven die wij onze kinderen liever niet willen laten zien. Denk aan sites met foto's van verminkte mensen, foute denkbeelden, pornosites, et cetera. Kom je die dan zo snel tegen? Om de waarheid te zeggen, in al die jaren dat ik informatie zoek op het internet ben ik nog nooit per ongeluk op zo'n site terechtgekomen. Daar moet je specifiek naar zoeken. En dat is nu meteen het probleem. De kinderen krijgen van oudere broers, zussen en vriendjes (en soms vaders!) adressen van foute sites en gaan op school kijken wat daar allemaal te zien is.

Laatst hoorde ik een directeur het volgende zeggen. "Wij geven de kinderen toegang tot internet en ze mogen zien wat ze willen. Het zoeken naar seksplaatjes gaat wel over als het nieuwtje eraf is". Nou, ik ken mensen bij wie dat nooit meer is overgegaan.

Filteren is 'in' op dit ogenblik. Ik wil een aantal mogelijkheden op een rijtje zetten, en daarna eens zien of er misschien alternatieven zijn.

Hoe werkt het?

Filteren is in feite niets anders dan het blokkeren of toestaan van bepaalde sites. Dat filteren kan vanuit twee invalshoeken geschieden. Beide methoden werken met lijsten of databases, waarop websites staan. Bij de 'zwarte lijst' is er sprake van blokkering van sites die je niet mag zien.

Strenger is de 'witte lijst'. Daarop komen alleen de sites voor die toegestaan zijn.

Laten we voor de werking van filters in het algemeen eens het programma *Cyber Patrol* voor netwerken bekijken. Cyber Patrol heeft een witte lijst, de CyberYES list, met sites die een educatieve waarde hebben. Dan is er nog de zwarte lijst, de CyberNOT list, die bijgehouden wordt door een groep onderzoekers. De lijst met verboden sites is lokaal op het netwerk aanwezig en wordt wekelijks automatisch via internet vernieuwd. Dagelijks kunnen de aanvullingen, de HotNOT's, automatisch worden gedownload.

De lijsten met verboden sites zijn meestal versleuteld, maar via de logbestanden van internetfilters kan men toch wel een idee krijgen wat er allemaal is tegengehouden.

Omdat de filtering in het geval van Cyber Patrol lokaal is, kunnen daar allerlei instellingen

worden gemaakt die bij het gedachtegoed op school passen. Verder is het met Cyber Patrol mogelijk in het gebruikersprofiel instellingen te maken ter regulering van het FTP-gebruik, of het uitschakelen van nieuwsgroepen en chatboxen. Om ongewenste bestellingen op internet te voorkomen, kunnen persoonlijke gegevens worden geblokkeerd, zoals naam, adres, telefoonnummer, creditcardnummer, enzovoort.

Ook de tijdstippen waarop internet op het netwerk beschikbaar is, kunnen ingesteld worden. Het voordeel van een filterprogramma op het eigen netwerk is de snelheid waarmee nieuwe filterregels kunnen worden geïmplementeerd.

Slimme filters

Filtering gebeurt op basis van steekwoorden in de tekst van een site. In feite gaat dit wel een beetje kort door de bocht. De filtering zou slimmer moeten zijn. Een stap verder gaat het *Dynamic Document Review* van Symantec. De context van woorden wordt hierbij belangrijker. Als de woorden 'borst' en 'borstkanker' in de tekst voorkomen, zal het vermoedelijk om iets medisch gaan en wordt de site toegelaten. Bij de combinatie 'borst' en 'Pamela Anderson' treedt het filter in werking.

Dan hebben we ook nog de foto's op internet. Dat is vaak onze grootste zorg. *Webwasher*, dat voor scholen trouwens gratis is, gaat erg intelligent om met beelden. Als er een foto op internet staat met veel huidskleur, kan die worden geweerd. Maar als het om Mark van den Hoogenband gaat, moet die foto wel worden doorgegeven want deze zwemkampioen moet misschien wel in een werkstuk verschijnen. Ook hier maakt de context weer verschil. Op basis van foto's, het internetadres en de tekst op de website wordt een waarschijnlijkheidsberekening gemaakt. Na analyse trekt het programma zijn conclusie. Als de tekst bij de zwemkampioen duidelijk sporttermen bevat en de website is een onschuldige omroepsite, wordt de foto doorgelaten. Komen er pornografische termen voor bij de foto, dan wordt die geblokkeerd. In geval van twijfel krijgen de deskundigen een waarschuwing en wordt de site eventueel handmatig op de zwarte lijst gezet.

Mogelijkheden

Op de pc zelf is ook een beveiliging aanwezig. Internet Explorer 5 heeft een rudimentaire vorm van beveiliging aan boord. In het menu <Extra> <internetopties> staat op het tabblad 'Inhoud' de mogelijkheid van internetrestricties vermeld. Bij het inschakelen daarvan kunnen we in de categorieën geweld, naakt, seks en taal vijf niveaus van beveiliging instellen. Standaard staat dat bij 'geweld' bijvoorbeeld op niveau 0; dus geen geweld. Dit blijkt in de praktijk niet echt te werken. Dat klopt ook wel, want het waarderingsysteem is in handen van de Recreational Software Advisory Council (RSAC) en is in feite gebaseerd op zelfregulering door de makers van de sites. De makers van de sites geven dus zelf een RSAC waardering aan hun pagina's. Explorer herkent die en neemt vervolgens actie.

Filtering kan echter ook interessante informatie tegenhouden die in feite erg waardevol is. Een respectabele instelling als de Online Internet Institute (OII) was op zeker moment niet meer bereikbaar: gefilterd. Deze blokkering was volkomen onterecht en een van de medewerkers, Art Wolinsky, ging op onderzoek uit. Om de achtergrond van het probleem te begrijpen is wat meer informatie nodig. Filtering kan gebeuren op basis van een URL, een IP-nummer of een combinatie van beide. Een URL is het adres dat we intikken in de adresbalk van de browser, bijvoorbeeld <http://www.terribleadultsite.com/>. Alle pagina's van deze site worden dus gefilterd. De toename van sites die op de zwarte lijst komen te staan neemt echter explosief toe. Omdat deze lijst erg lang kan worden neemt men steeds vaker toevlucht tot het blokkeren van IP-nummers. IP-nummers zijn in feite de echte internetadressen. Als wij intikken: www.cnn.com, want zoiets is gemakkelijk te onthouden, wordt die naam eerst via speciale naamserver omgezet in het nummer 64.12.50.249. Het blokkeren van een IP-nummer heeft tot gevolg dat er tegelijk honderden sites geblokkeerd kunnen worden. Dit probleem wordt ook in de hand gewerkt door

het toenemende gebruik van IP-Independent Virtual Hosting. Door het nijpende gebrek aan IP-nummers worden op één IP-nummer honderden of duizenden sites aangeboden. Dat was nu ook het geval bij het Online Internet Institute. Hun site bleek ondergebracht te zijn bij een provider die ook vele sekssites bevatte. Art ontdekte na uitgebreid onderzoek in logbestanden van filters dat de IP-blokkering de oorzaak was van de filtering van de OII-site.

Filteren via de zoekmachine

Sommige zoekmachines hebben de mogelijkheid een blokkering aan te brengen. Ik heb er twee getest. Ten eerste Vindex.nl. In deze Nederlandstalige zoekmachine is het mogelijk een kinderslot in te stellen. In Altavista.com heb ik iets dergelijks gedaan door het Family Filter aan te zetten. Ik heb drie testwoorden in beide zoekmachines geprobeerd: *porno* (ligt voor de hand) *borst* (als je iets over onze minister wilt weten in verband met een werkstuk over de gezondheidszorg) en *poesje* (heel onschuldig als een kind iets zoekt in verband met dierendag).

Bij Vindex kun je het wachtwoord instellen door een vraag op te geven en het antwoord. Als dat mis gaat, kun je het kinderslot niet uitschakelen. Hoewel, het werkt met behulp van een cookie, dus als je kijkt in de map Windows\cookies, kom je Vindex tegen. Wissen, en het kinderslot is weg. Bij het Altavista Family Filter idem dito.

Zoekopdracht	Treffers zonder filter	Treffers met filter
Porno	21.631	5
Borst	3.032	5
Poesje	6831	5807

Tabel 1: Test met Vindex.nl filter

Zoekopdracht	Treffers zonder filter	Treffers met filter
Porno	1.772.155	3
Borst	39.931	39.931
Poesje	2387	50

Tabel 2: Test met Altavista filter (Amerika)

Ik moet eerlijk zeggen, bij die laatste vijftig hits ging het voor zover ik kon nagaan om onschuldige sites met verhalen over Felix Domestica en tekeningen van Rien Poortvliet. Maar vlak onder het venster met zoektermen stond 'Related Searches' en dat gaf toch wel wat anders. Deze vorm van filtering voorkomt alleen het vinden van informatie die in het zoekvenster wordt getypt. Het is altijd mogelijk elke site te bekijken die buiten de zoekmachine om wordt ingetypt.

Weerstand

In de Verenigde Staten kwam men al snel met allerlei vormen van filtering. Dat ligt nu eenmaal in de aard van de Amerikanen. Toch legt men zich ook daar niet zonder meer neer bij filtering. Dit jaar trad de Children's Internet Protection Act (CIPA) in werking. Scholen en bibliotheken die hun financiële steun niet willen missen, moeten voldoen aan de veiligheidsregels voor internet en zodoende een filtering toepassen om kinderen te beschermen. Zij moeten een formulier invullen waarin ze akkoord gaan met de wet. De American Library Association (ALA) bestrijdt de CIPA omdat die ongrondwettelijk is. Het gaat tegen het recht op informatie in. En nog erger: bibliotheken worden gedwongen te kiezen tussen het verkrijgen van fondsen en censuur. De gebruikers van de bibliotheken zijn hierbij de verliezers, want die hebben op verafgelegen plaatsen geen toegang meer tot een deel van de informatie.

Wat minder luidruchtig heeft hetzelfde in Nederland gespeeld. Een van de grote voordelen van Kennisnet zou de mogelijkheid tot filtering zijn. Maar ook hier is het juridisch problematisch en ongrondwettelijk om publieke informatie te beperken.

Relevante links

- www.webwasher.com
- <http://veilig.kennisnet.nl>
- www.cyberpatrol.com
- www.ala.org/cipa
- www.enfiltrator.com

Een ander protest komt van de Amerikaanse organisatie Peacefire. Zij is van oordeel, dat de aanwezigheid van een filter meer onrust veroorzaakt dan dat het voorkomt en biedt een programma aan, waarmee zeven filters kunnen worden omzeild. Het Electronic Privacy Information Center ontdekte dat een filter als Family Search, dat door een aantal zoekmachines wordt gebruikt, meer dan negentig procent van de informatie blokkeert die interessant kan zijn voor kinderen. Deze organisatie is dus ook al geen voorstander van filteren.

Nu wel of niet filteren?

Zelf denk ik ook dat je beter niet kunt filteren. Dagelijks komen er sites met fout materiaal bij. Filters lopen daardoor altijd een stap achter. Geen enkel filter is daarom voor honderd procent betrouwbaar. In het beste geval laten ze tussen de tien en vijftien procent van de informatie die we willen blokkeren door. Kortom, dat werkt niet. En is het ten onrechte blokkeren van goede informatie niet veel erger? Blijft over: niet filteren. Een gesprek over wat de kinderen hebben gezien en waarom het dan wel verkeerd was, of waarom iets bij de leerkracht walging opwekt, werkt veel beter dan het zonder meer verbieden en blokkeren. De andere restricties van filterprogramma's, zoals het blokkeren van chatten, kunnen echter wel nuttig zijn.

Wat ook nuttig en soms noodzakelijk is, is het achteraf bekijken waar de kinderen zoal zijn geweest tijdens het surfen. Dat kan in Internet Explorer bijvoorbeeld in het uitklapvenster van de adresbalk, de geschiedenis en eventueel de favorieten. We kunnen ook kijken naar de plaatjes die zijn binnengehaald. We vinden die in: C:\Windows\Local Settings\Temporary Internet Files\Content IE5 en/of C:\Windows\Temporary Internet Files\Content IE5.

Met de browser uit Paint Shop Pro of Thumbsplus is goed te zien wat er aan beeldmateriaal zoal is binnengehaald. Uiteraard is veel hiervan te wissen vanuit Internet Explorer (Extra, internetopties, tabblad Algemeen). Voor de controle achteraf is ook software ontwikkeld, bijvoorbeeld Enfiltrator of SAM.

Internetcontract

We moeten ook zorgen dat de leerkracht kan zien waar de leerlingen mee bezig zijn. Stel de monitoren zodanig op, dat je ze in een oogopslag allemaal kunt zien. Staan de computers in een aparte ruimte opgesteld, zorg dan dat er toezicht is. Ik weet dat een leerkracht in Amerika een groot probleem heeft als kinderen zonder toezicht foute sites zien. Als de leerkracht niet zelf toezicht kan houden, is het misschien mogelijk een ouder in te schakelen.

Een andere mogelijkheid is afspraken maken in de vorm van contractjes. Op de Amerikaanse school Folsom Elementary, zag ik dat de leerlingen contracten ondertekenden waarin ze beloofden de apparatuur goed te behandelen; niet in andermans werk te knoeien; geen zaken te zoeken op internet, waarvan ze weten dat de school en hun ouders niet willen dat ze zoiets zien; niet via internet beledigende taal te gebruiken, enzovoort. Vergelijk het met het pestprotocol wat op een aantal scholen wordt gebruikt.

Geef de leerlingen ook gerichte opdrachten voor het zoeken naar informatie voor werkstukken en spreekbeurten. Een goed voorbeeld is de WebQuest (zie OWG Info 83). Ze verdwalen dan minder snel. Iets als: "Als je klaar bent met je werk, mag je internetten" is natuurlijk dodelijk voor goed gebruik van internet.