

Hoe de scholen ethical werden gehackt

Kennisnet liet in de periode najaar 2006 – voorjaar 2007 vier scholen uit het basisonderwijs (PO) en tien scholen uit het Voortgezet Onderwijs (VO) hacken. Waarom? Was de uitkomst echt zo erg als het AD op 21 januari jl. kopte: “Schoolcomputers zo lek als een mandje”? Maar misschien nog interessanter: wie voerde die hack uit en hoe deden ze dat?

Is it-beveiliging belangrijk op scholen?

Volgens sommige mensen is (it)beveiliging op scholen onnodig, want “wat is daar dan voor waardevoets te vinden voor hackers”? Wat dacht je dan van manipuleren van cijfers, lekken van examenvragen of persoonlijke informatie van docenten (salaris) of leerlingen (adressen), het misbruik van het (draadloze) netwerk voor digitaal pesten, spamruns of hacken van andere organisaties of het negatief in de pers komen doordat je zelf gehacked bent? Of het feit dat een keylogger geïnstalleerd wordt waarmee allerlei wachtwoorden (electronic banking?) worden afgevangen? Het plat komen te liggen van het netwerk tijdens de examenperiode? Welke schooldirecteur wil zijn ict dus niet goed beveiligen?

Dat betekent niet dat beveiliging bij alle scholen hoog op de agenda staat. Iedereen die verantwoordelijk is voor beveiliging, weet hoe lastig het is om beveiliging op de agenda te krijgen en te houden.

Kennisnet wilde aandacht vragen voor beveiliging op scholen, en ging er van uit dat alleen informatie op een site zetten niet genoeg zou helpen. Laten zien hoe kwetsbaar (ook) scholen zijn, zou hopelijk zorgen voor meer aandacht. Er werd contact gezocht met partijen die gespecialiseerd zijn in beveiliging, en daaruit werd Montelbaan gekozen voor het uitvoeren

van een ethical hack, een bedrijf gespecialiseerd in technische vraagstukken aangaande identiteitsmanagement.

Het hoe en wat van de ethical hack

Bij een ‘Ethical hack’ informeer je vooraf de directie, legt uit wat je gaat doen (testen van de beveiliging en een rapport opleveren waarmee zijn ict veiliger gemaakt kan worden, wie wil dat niet) en spreekt af dat verder niemand op de hoogte is van de komende test. Vervolgens benader je de systemen als een computerkraker (hacker, alhoewel de naam cracker beter is ;-)).

Met Montelbaan werd besproken wat getest moest worden. De website van een organisatie is vaak een zwakke schakel, dus die zou worden getest. Daarnaast werd een test op de schoollocatie afgesproken: er zou worden gekeken of er een hackable draadloos netwerk was en of er toegang te krijgen was tot systemen en gegevens van studenten of personeel.

Montelbaan schetste op welke manieren de hack kon worden uitgevoerd. Er was de aanpak waarbij professionele hackers urenlang al hun kunsten zouden botvieren op elke school. Maar die aanpak paste niet in het budget. Er moesten concessies worden gedaan; er werden vier derdejaars informatiekunde-studenten van de Leidsche Hogeschool ingezet als hackers. Voordelen: die hadden daarmee een praktische stage-opdracht, de hack zou goedkoper zijn, en door deskundige begeleiding (four eyes principe: altijd iemand die meekijkt) zou er toch sprake zijn van een degelijke hack.

Aan de slag!

De studenten kregen als opdracht om te bedenken welke tests en tools ze zouden gaan gebruiken. Daarnaast



Pieter Manneke van Montelbaan

moesten ze op papier zetten hoe de communicatie met de school moest plaatsvinden. Bij het benaderen van de scholen moest alleen de directeur begrijpen wat er ging gebeuren, en wat het doel was. Als de directeur instemde mee te werken werd op papier vastgelegd wat er ging gebeuren, wie waarvoor verantwoordelijk was, en wat er zou gebeuren als er onverwacht toch problemen optraden tijdens de hack. Als de hackers op locatie werden ontdekt, moesten ze een brief kunnen laten zien dat ze in opdracht handelden van de directeur.

Nu kon de echte hack beginnen. Elke hack begint met het verzamelen van informatie. Er werd op forums gekeken of er door it-personeel van de school vragen waren gesteld waaruit op te maken was welke componenten in gebruik waren ("wie weet hoe je probleem met versie X van apparaat Y kan oplossen"). Vervolgens werd de "remote test" gestart. Met tools als Axence netTools 3.0, HTTPHEAD en Neotrace Pro werd gekeken welke versie webserver er in gebruik was, waarna kon worden opgezocht op welke bekende vulnerabilities getest kon worden. Met Gfi LANguard en Tenable Nessus werden vervolgens de poorten van de webserver gescanned. Tot slot werd met \$_POST of \$_GET in php/asp gekeken of SQL-injection mogelijk was, om de site te defacen. Bij deze test bleek dat de meeste sites werd gehost door een professionele provider, en die hadden hun zaakjes goed op orde qua patches etc. De 2 scholen die zelf hun site nog hosten, trokken na de ethical hack de conclusie dat het beter was om de hosting uit te besteden.

De hackers komen naar u toe deze zomer

Na de test op afstand werd een test op locatie gedaan. Om de hoeveelheid tijd (en dus kosten) verder te beperken werd afgesproken dat niet eindeloos zou worden gepoogd om accounts van studenten, docenten en de administratie te hacken, maar gewoon een account met rechten van een student en docent te vragen. Natuurlijk werd afgewogen of dan nog wel een representatieve test ontstond. De gedachte was echter dat het relatief eenvoudig was om (zeker als student) een school binnen te lopen, achter een pc plaats te nemen en (vanaf een usb-stick) met hacker-tools te gaan hacken: het zou alleen wat meer tijd en dus geld kosten.

Op locatie werden tools als Gfi-LANguard, Wireshark en onder DOS tools als ping, tracert, netstat, ipconfig, en arp gebruikt om gegevens te verzamelen en werd gekeken welke patches/hotfixes ontbraken en welke poorten en services in gebruik waren. Er werd gekeken of de router en eventueel de netwerkprinter en andere netwerkhardware nog voorzien waren van het standaard admin-wachtwoord. Ook een open deur als controle op het wachtwoord van administrator accounts werd niet overgeslagen. Services als

FTP, SMTP, DNS en dergelijke werden benaderd en gecontroleerd, en op het lokale werkstation werd met pwdump6 en Elcomsoft Windows Password Recovery gepoogd de lokale wachtwoord-database te kraken.

Van dit alles werd een mooi rapport gemaakt. Scholen kregen te zien wat de hackers bij hen hadden gevonden, en konden daarmee hun beveiliging verbeteren. En de media pikte wat krenten uit de pap en kopte dat het allemaal maar slecht gesteld was.

Was het nou echt zo erg gesteld?

Op bijna iedere school was wel iets aan te merken. Zo bleek in 2 gevallen dat een leraar inlogde terwijl zijn activiteiten zichtbaar waren op het digitale schoolbord. En lopen sommige docenten het klaslokaal nog uit terwijl ze nog ingelogd zijn en er geen wachtwoord-lock aan staat. Er werd een onbeveiligd draadloos netwerk gevonden. Niet overal waren de laatste patches geïnstalleerd. Op een school had de locale administrator geen wachtwoord. Op een andere school konden medewerkers bij elkaars e-mail. Op meerdere netwerken bleek het mogelijk het verkeer af te tappen en zo achter wachtwoorden (ook van docenten) te komen. Op enkele servers stonden nog veel poorten open (met een uitschieter van 600!). Er bleken netwerkcomponenten en netwerkgekoppelde printers voorzien van standaard meegeleverde wachtwoorden, die daarmee een potentiële springplank vormen naar de rest van het netwerk.

Maar overal waar je een vergrootglas op zet, vind je wat! Pieter Manneke van Montelbaan had niet het idee dat de situatie erger was dan in andere sectoren: "De meeste scholen zijn zich goed bewust van de situatie. Sommige risico's besluit je te lopen. Leerlingen lopen bij wijze van spreken nog niet met de vuilnisbak naar huis (om te zoeken naar informatie). Een aantal scholen heeft nog geen maatregelen genomen tegen usb-sticks waar je applicaties van kunt starten, maar dat zijn relatief nieuwe ontwikkelingen waar men op termijn zonnig ook maatregelen voor treft."

Voor iedereen die verantwoordelijk is voor it-beveiliging op scholen is het nuttig het rapport in detail door te kijken en te leren van de fouten (en goede oplossingen) van de gehackte scholen:

<http://www.ictopschool.net/software/veiligheid/> . Links naar ondermeer het Penetration Testing Framework vind je o.a. op <http://del.icio.us/raoulteeuwen/security> .

Raoul Teeuwen (raoulteeuwen.blogspot.com) werkt voor Tipping Point en heeft tot begin 2007 6 jaar lang bij Kennisnet gewerkt als projectleider techniek & beheer.