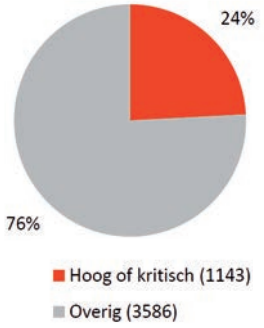
GEMEENTEN ZETTEN ONBEDOELD

SOFTWAREVERSIES VAN GEMEENTELIJKE WEBSYSTEMEN

Ruim een jaar na alle ophef over digitale veiligheid hebben veel gemeenten toch nog verouderde, en daardoor onveilige, websoftware in gebruik. Ze zijn hierdoor kwetsbaar voor misbruik door hackers. Dat blijkt uit een onderzoek van webexpert DongIT, waarbij de softwareversies van websystemen van alle gemeenten in kaart zijn gebracht. Bijna een kwart blijkt niet up-to-date. Soms is software zelfs zo verouderd, dat er überhaupt geen updates meer voor worden ontwikkeld. Per 1 januari 2013 is de Informatiebeveiligingsdienst (IBD) van de VNG opgericht om toe te zien op de veiligheid van gegevens bij lokale overheden.

Tekst: Wouter S. van Dongen, directeur DongIT



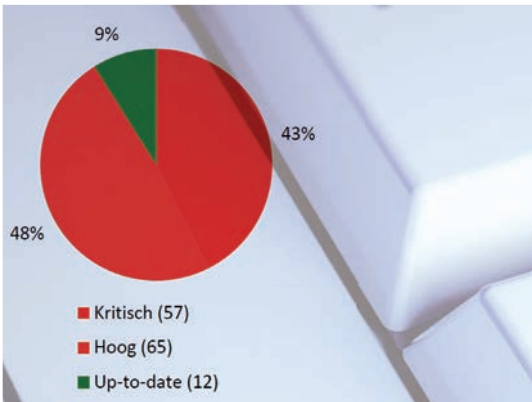
Figuur 1: Totaalimpact op alle domeinen door kwetsbaarheden met een hoge en kritische impact rating.

De DigiNotar-crisis en bevindingen tijdens 'Lektober' hebben eind 2011 aangetoond dat de ICT van gemeenten kwetsbaar is. Dat komt vaak doordat software niet of niet tijdig wordt geüpdatet en onderhouden. Zo maakte de website van DigiNotar gebruik van een verouderd *content management system* dat ruim twee jaar niet was bijgehouden. Ook bleek dat vijftig gemeentelijke systemen draaiden op een verouderde, kwetsbare Windows-versie. In 2012 zijn maatregelen genomen om herhaling te voorkomen. Er zijn verplichte audits en testen voor DigiD-afnemers. Er zijn duidelijke beveiligingsrichtlijnen van het Nationaal Cyber Security Centrum (NCSC), met prioriteit voor versiebeheer. Ook de Informatiebeveiligingsdienst van de VNG heeft gemeenten in januari gewaarschuwd.

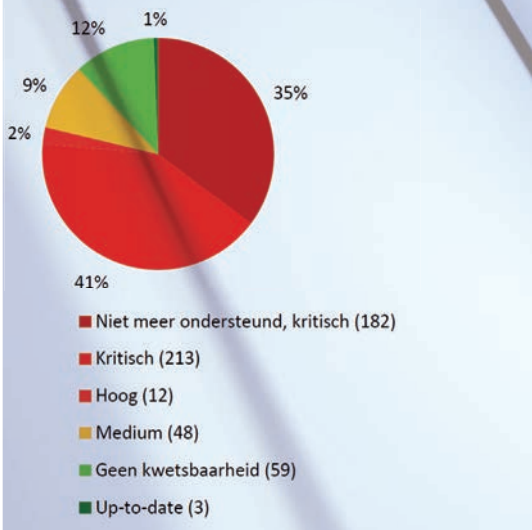
KWETSBAAR

De resultaten van het onderzoek onderstrepen de noodzaak voor een betere bewustwording en aanpak van digitale veiligheid. Bijna een kwart (24 procent) van alle gedetecteerde gemeentelijke systemen kan mogelijk beïnvloed worden door de kwetsbaarheden. Bij een aantal softwarepakketten zoals Drupal, Joomla, phpMyAdmin en ASP.NET zijn zelfs (bijna) alleen kwetsbare softwareversies aangetroffen. Kwetsbaarheden kunnen verstrekkende gevolgen hebben voor de betrouwbaarheid, integriteit en vertrouwelijkheid van het *hele* systeem. Eén websysteem wordt vaak gebruikt voor meerdere doeleinden. Hierdoor kan het mogelijk zijn dat een wel goed beveiligde applicatie met belangrijke data door een vergeten en 'onbelangrijke' applicatie in gevaar wordt gebracht. Ook kan een kwetsbare webapplicatie van gemeente A de data van gemeente B in gevaar brengen. Dat geldt voor gekoppelde data, maar ook voor data die volledig los staan van elkaar. Als verschillende gemeenten hun website op dezelfde webserver hosten (zonder data te delen), kan een kwetsbaarheid van de ene gemeente gebruikt worden om via de web-

SOMS IS SOFTWARE ZELFS ZO VEROUDERD, DAT ER ÜBERHAUPT GEEN UPDATES MEER VOOR WORDEN ONTWIKKELD



Figuur 2: Versiestatus ASP.NET



Figuur 3: Versiestatus PHP

DEUR OPEN VOOR HACKERS

VAAK VEROUDERD

OVER HET ONDERZOEK

Om zo veel mogelijk websystemen in kaart te brengen heeft DongIT een script geschreven dat met verschillende technieken zo veel mogelijk informatie probeert te verzamelen. Hiervoor zijn diverse tools op een creatieve manier aan elkaar gekoppeld. Die tools zijn gewoon publiek beschikbaar, maar er werd ook gebruikgemaakt van zoekmachines zoals Google en Bing. In totaal werden 5.271 gemeentelijke domeinen (webadressen) gevonden, waarvan 4.729 actief. Achter elk domein kan weer andere software aanwezig zijn en naar alle domeinen werd een verzoek verstuurd waar de software op reageert. Uit deze reactie kan afgeleid worden welke softwareversie aanwezig is. Het onderzoek is net zoiets als aanbellen bij een huis en dan kijken wie er opendoet, maar dan digitaal. Laagdrempelig, met eenvoudig beschikbare tools, zonder dat er 'gehackt' wordt. Maar op een dergelijke manier informatie verzamelen over software is wel vaak het eerste wat een hacker doet. Want met de verzamelde informatie is het mogelijk zeer doelgericht systemen aan te vallen. Op internet kan in sommige gevallen kant-en-klare code gevonden worden om de kwetsbaarheid te misbruiken.

PRAKTISCHE TIPS OM GEMEENTELIJKE SYSTEMEN TE BEVEILIGEN

- Houd de bewustwording van digitale veiligheid hoog op de agenda en maak duidelijk beleid.
- Wees continu bewust van welke systemen er draaien, creëer een actueel totaaloverzicht.
- Bepaal welke applicaties publiek toegankelijk dienen te zijn. Scherm alle overige systemen goed af.
- Zorg voor een duidelijke taakverdeling bij op het up-to-date houden van alle systemen, het is regulier en frequent werk.
- Hanteer het document *ICT beveiligingsrichtlijnen voor webapplicaties* van het Nationaal Cyber Security Centrum.
- Gebruik continu een geautomatiseerde veiligheidsscan en laat periodiek een aanvullend onderzoek uitvoeren naar de webveiligheid.

server bij de data van een andere gemeente te komen.

UPDATES

Het bijhouden van updates (versiebeheer) van alle websystemen is dus een essentieel onderdeel van ICT-beveiliging. De meeste systeembeheerders zijn zich hier gelukkig van bewust, maar vaak gaat het toch niet goed. Soms gebeurt de update niet tijdig genoeg, waardoor systemen weken of

HET BIJHOUDEN VAN UPDATES VAN ALLE WEBSYSTEMEN IS EEN ESSENTIEEL ONDERDEEL VAN ICT-BEVEILIGING

maanden kwetsbaar blijven. Soms wordt de update helemaal niet uitgevoerd, omdat functionaliteiten na de update niet meer naar behoren werken of omdat een totaaloverzicht van software ontbreekt. Ook worden minder belangrijk geachte systemen vaak verwaarloosd.

Meer weten?
Het volledige rapport is beschikbaar via www.dongit.nl