




Peter van den Hoogen (52)

Organisatie:	Gemeente Delft
Functie:	Adjunct Vakteamhoofd Informatiediensten
In dienst sinds:	2005 
Afdeling:	50 mensen
Verantwoordelijkheid:	het infrastructuurbeleid, het beheer van de infrastructuur en het beheer van IT-projecten.
Studie:	HTS Werktijdbouwkunde en bedrijfseconomie, nadien diverse cursussen en trainingen.

**‘Mobiele media
vormen de grootste
dreiging voor
IT-security’**

Peter van den Hoogen van gemeente Delft:

‘Overheden moeten goede voorbeeld geven’



De gemeente Delft wil een voortrekkersrol spelen op het gebied van internetdienstverlening aan burgers. En dus maakt adjunct vakteamhoofd informatiediensten Peter van den Hoogen al sinds 1980 de opkomst van de automatisering en het internet van dichtbij mee. Zijn speerpunt is de beveiliging van IT-diensten en bewustwording onder gebruikers.

Peter van den Hoogen gaat ver terug in zijn geheugen bij de vraag of hij kan terugblikken op IT-beveiliging in de afgelopen jaren. “In 1987 was ik één van de gelukkigen die een van de eerste vier PC’s kreeg toen de gemeente ging automatiseren. Er was één printer en het uitwisselen van informatie deden we met een floppy. Dat kun je je nu niet meer voorstellen, he”, grijnst Van den Hoogen die nu adjunct vakteamhoofd informatiediensten is bij de gemeente Delft. “In 1990 volgde het eerste eenvoudige netwerk en acht jaar later werden alle gemeentelijke locaties met elkaar verbonden. We hebben nu zo’n vijf hoofdlocaties en 23 andere locaties die via een integraal netwerk met elkaar zijn verbonden. In die tijd heeft de gemeente ook de domeinnaam delft.nl geclaimd al hadden we niet eens een website.”

De tijden zijn enorm veranderd, weet ook Van den Hoogen. “De eerste jaren had nog nooit iemand gehoord van virussen, worms of trojans. Ook phishing en andere bedreigingen bestonden uiteraard nog niet. Op het moment dat we startten met de gemeentelijke locaties aan elkaar te knopen en met internet aan de slag gingen, werden de bedreigingen reëel.” Op de vraag hoe gemeente Delft zijn beveiliging nu

heeft ingericht, blijft Van den Hoogen een tijdje stil. “We hebben onze IT-security opgebouwd in verschillende lagen. Meer wil ik er eigenlijk niet over vertellen, want dat vind ik toch nog altijd een beetje riskant.”

Jaarlijkse audits

Dat het met de beveiliging van de IT van zijn gemeente wel goed zit, weet Van den Hoogen door de jaarlijkse audits. Van den Hoogen werkt met een informatiebeveiligingsplan en krijgt eens per jaar een externe audit. Voor de specifieke onderdelen en afdelingen van de gemeente zijn er ook jaarlijkse audits. Het gaat dan om het netwerk van GBA waar alle Nederlandse gemeenten bij zijn aangesloten en informatie uitwisselen. En Delft doet mee in Suwinet dat gebruikt wordt door de dienst Werk, Inkomen & Zorg waarvoor de gemeente ~~Delft~~ meedoet in Gemnet. “Om op die separate netwerken te kunnen worden aangesloten, moet je als gemeente aan allerlei eisen voldoen”, legt Van den Hoogen uit. “Zo moeten we onze aanpak van antivirus goed geregeld hebben, moeten we regelmatig updates uitvoeren, een goede password policy hebben en moeten we voldoen aan een scala van beheersmaatregelen.”

Vanuit het college van Burgemeester en Wethouders is betrekkelijk weinig aandacht voor de beveiliging van de ICT. “We komen positief uit de jaarlijkse audit en dus bemoeit de politiek zich er niet dagelijks mee. Dit is prima zo. De overheid moet het goede voorbeeld geven ~~en secure~~ door betrouwbaar te zijn. Overheden kunnen het zich niet permitteren om onveilige activiteiten te doen omdat ze over allerlei vertrouwelijke gegevens van burgers beschikken. Als gemeente hebben we de verantwoordelijkheid om goed op die gegevens te passen.”

Complexiteit

IT-security is op diverse vlakken van belang voor de gemeente Delft. Zo kunnen burgers verschillende diensten of formulieren gebruiken of afnemen via het internet. “Daar komt zelfs een behoorlijke omzet uit”, zegt Van den Hoogen. “Pine-wood heeft ons ondersteund met het opstellen van protocollen en het platform waarop onze webapplicaties draaien. Het is allemaal redelijk complex en toch denk ik niet dat het eenvoudiger kan. Veiligheid zorgt vaak toch voor een hogere complexiteit.”

Met die complexiteit in het achterhoofd heeft de gemeente Delft al twaalf jaar geleden gekozen voor Pinewood. Van den Hoogen waardeert de aandacht voor kwaliteit. “Pinewood is de afgelopen jaren flink gegroeid en toch hebben alle medewerkers de aandacht te houden op kwaliteit. Dat vind ik knap. Het is ook slim dat het bedrijf nooit concurreert op prijs en altijd op kwaliteit. Dat is ook de reden dat ze er destijds bij die tender uitsprongen.”

Gebruiker als zwakke schakel

Ook intern is beveiliging van groot belang. De gebruikers binnen de gemeente moeten de IT-infrastructuur en applicaties namelijk zonder problemen kunnen gebruiken. “Medewerkers vinden beveiliging onbelangrijk totdat ze er zelf last van krijgen”, zegt Van den Hoogen. “IT-security is dus steeds meer een zaak van gebruikers. Technisch gezien kun je een heleboel beveiligen, maar het gaat om bewustwording bij de mensen. Zij zijn de zwakke schakel in security.”

Terwijl hij spreekt, haalt Van den Hoogen trots een boekje uit de kast.

“Iedere medewerker die bij ons komt werken, moet een protocol onder-

tekenen en daarnaast krijgen ze dit boekje.

Hierin hebben we beschreven hoe de gemeente met de informatiebeveiliging omgaat. Dit boekje is een van de eerste stappen die we hebben genomen om gebruikers bewust te maken van informatiebeveiliging.

Vaak zijn ze zich helemaal niet bewust van de gevaren en dan kunnen ze onintentioneel schade aanrichten. Door het boekje weten ze

wat ze wel en niet kunnen doen. Dat heeft veel meer waarde dan enkel techniek.

Geen enkele organisatie kan het uiteindelijk redden met alleen technische beveiligingsmaatregelen op het gebied van informatiebeveiliging.”

Een andere maatregel die gemeente Delft heeft genomen, heeft te maken met de regulering van websites. Aanleiding daarvoor was het ongecontroleerde surfgedrag door medewerkers. Dit speelde met name in de beginperiode dat zij internet op de werkplek kregen. “Het bleek dat mensen enorm veel tijd kunnen steken in surfen en downloaden”, knipoogt Van den Hoogen. “Websites zijn nu onderver-

**‘Gebruikers vinden
beveiliging onbelangrijk
toldat ze er last
van krijgen’**

deeld in categorieën en het management heeft vervolgens besloten welke medewerkers welke categorieën moesten kunnen bekijken. De rest is afgeschermd.”

Mobiele apparatuur

Toekomstige bedreigingen ziet Van den Hoogen in vooral draagbare media en randapparatuur. “Websites, PC’s en netwerken zijn inmiddels allemaal niet meer dan een commodity geworden. Juist de randapparatuur zoals mobiele telefoons is nog niet uitontwikkeld, waardoor er op dit terrein nog veel mogelijkheden voor beveiligingsrisico’s zijn. Sterker nog, juist daar gaat de grootste dreiging vanuit.” Het management van de gemeente Delft werkt met mobiele telefoons van HTC. Zij gebruiken die voor meer dan alleen email en internetbrowsen. “De afspraak is dat er in principe **er** geen bedrijfskritische informatie op mag staan. Maar ja, mobiele telefoons hebben steeds meer geheugencapaciteit tegenwoordig. Net als USB-sticks voor dataopslag. Voor zover gebruiken medewerkers ze weinig voor dit doel. Dit komt mede omdat we de mensen er bewust van hebben gemaakt dat niet te doen”, aldus Van den Hoogen. “Ook onze laptops zijn wat dat betreft redelijk dichtgetimmerd. Maar kwaadwillende gebruikers kunnen natuurlijk altijd omwegen vinden. Dus moeten we er als organisatie door bewustwording voor zorgen dat mensen die omweg niet willen zoeken.”

Millenniumproof

Het is duidelijk dat Van den Hoogen in de loop der jaren veel en bijzondere zaken op het gebied van IT-security heeft meegemaakt. Een achteraf bijna bizarre situatie speelde zich af rond de millenniumwisseling. “Wat we toen hebben gedaan”, zegt Van den Hoogen lachend. “Iedereen was bang dat we zouden worden overvallen door de meest vreselijke virussen. Dus hebben we een aantal voorzieningen losgekoppeld van het netwerk. Een van de applicaties was de webmailclient. Die internetmail lieten we een tijd lang binnenkomen op een stand alone computer waar een mevrouw alle mailtjes monitorde, uitprintte en verdeelde onder de medewerkers. Dat zou nu echt niet meer kunnen met de hoeveelheid mails vandaag de dag. Die arme mevrouw zou binnen een kwartier overspannen zijn.” ●