Shadow-IT bij de overheid

Een onvermijdelijk gevaar?

Ze zijn razend handig: WhatsApp, Dropbox, WeTransfer, Gmail, Google Docs, Trello, conversieprogrammaatjes. Of wat te denken van een virtuele server bij Amazon Web Services (AWS) om even wat dingetjes te doen die niet via de gewone IT-omgeving kunnen? Welkom in de wereld van shadow-IT: software waarvan de IT-afdeling zegt dat het niet gebruikt mag worden, maar die de IT-eindgebruiker een oplossing biedt. Shadow-IT is een enorme risicofactor voor de overheid. Maar niemand kent de exacte omvang ervan.

Door **Erik Bouwer**
Beeld **iStock/Barry Hage**

Gemak, dat is een van de redenen waarom werknemers gebruikmaken van shadow-IT. Een inmiddels berucht voorbeeld is dat van toenmalig minister van EZ Henk Kamp (2016). Hij gebruikte Gmail – ook voor het versturen van staatsgeheime informatie – omdat het makkelijker werken was in de avond en in het weekend. Shadow-IT omvat alle IT-oplossingen die medewerkers binnen een organisatie gebruiken zonder dat dat is toegestaan en bekend is bij de IT-afdeling. Het kan gaan om zelf aangeschafte hardware of software. Zelfs de Nationaal Coördinator Terrorismebestrijding en Veiligheid erkent de rol van het gemak: “Eindgebruikers hebben behoefte aan makkelijke manieren om hun werk uit te voeren. Waarschijnlijk ligt die overweging ten grondslag aan de toename van schaduw-ICT.”

Gebruiksgemak staat niet op zichzelf. IT-eindgebruikers kunnen verschillende redenen hebben om niet-officiële IT te gaan gebruiken. Gebruiksonvriendelijke applicaties, trage verbindingen, gebrek aan functionaliteit in bestaande voorzieningen, en soms zelfs gebrekkige adoptie van geheel nieuwe applicaties kunnen werknemers naar alternatieve oplossingen sturen. Daarbij wordt nieuwe technologie snel en gemakkelijk door consumenten omarmd en vervolgens mee naar het werk genomen. Wanneer je WhatsApp op je desktop of laptop hebt gezet, is het plotseling een ontzettend handige tool om te chatten en bestanden mee te sturen. Soms ontwikkelt succesvolle consumentensoftware zich tot bedrijfssoftware: denk aan Skype, tien jaar geleden nog not done, nu is

het onderdeel van de Microsoft-familie. Soms is het de IT-afdeling die vernieuwing tegenhoudt: ‘over vier maanden bent u de eerste’ of: ‘wat wilt u er allemaal mee gaan doen?’.

Daarmee stimuleren CIO’s onbedoeld het gebruik van alternatieven, aldus Marco Gianotten, CEO van onderzoeks- en adviesbureau Giarte. “Als de eindgebruiker niet meer naar de IT-afdeling wil of zijn gewenste oplossing staat niet in de zogenaamde servicecatalogus van IT, dan koopt de eindgebruiker het elders in. Naast eenvoudige toepassingen zijn er inmiddels ook complete oplossingen en services verkrijgbaar, bijvoorbeeld voor het opbouwen van datalakes of het ontwikkelen van machine learning toepassingen. Die zijn vaak minder zichtbaar voor de IT-auditors. Voor steeds meer werknemers is experimenteren met nieuwe software – snel iets uitproberen – antwoord op de vraag naar het gebruik van data en het besturen van processen. Vaak belanden op deze manier data buiten de eigen organisatie, bijvoorbeeld omdat ze worden geüpload naar een service.”

Binnen de overheid is het ‘experimenteren’ met technologietools jarenlang nadrukkelijk gepropageerd door vernieuwers, bijvoorbeeld door het netwerk Ambtenaar 2.0. In het boek ‘Nieuwe ideeën en praktische tips om te werken in overheid 2.0’ wordt gesproken over ‘andere manieren van samenwerken en je een weg banen door een alsmaar groeiende berg aan informatie’. Als ambtenaar moet je openstaan voor die ontwikkelingen en nieuwsgierig zijn naar de mogelijkheden om je werk nog beter te doen, aldus de auteurs. “Het veiligste is dus altijd om te werken binnen de overheid: op je eigen netwerkschijf of op Rijksweb. Maar dat is niet altijd mogelijk: als je wilt samenwerken en kennisdelen over de grens van je eigen organisatie heen, dan ben je toch aangewezen op internet als platform. En het aanbod van functionaliteiten op internet is zo groot en divers, als je daarmee efficiënter je werk kunt doen en betere resultaten kunt behalen dan is het bijna onverantwoord om die meerwaarde te laten liggen.” En verderop: “Iedereen met een internetverbinding kan thuis en op het werk gebruikmaken van een groot potentieel aan nieuwe middelen en instrumenten om efficiënter z’n werk in te richten, breder en effectiever samen te werken en interactiever met burgers te werken.”

Maar ook in de relatief recente ‘Gedragsregeling voor de digitale werkomgeving’ uit 2016 (2) staat te lezen: “De digitale werkomgeving biedt veel mogelijkheden. Het is belangrijk dat medewerkers zich bewust zijn van de risico’s die digitaal werken met zich meebrengt.” Verderop gevolgd door: “Het aanbod van openbare apps en online voorzieningen is groot. Gebruik die openbare voorzieningen alleen voor openbare informatie. Er kleven aan deze openbare voorzieningen ernstige bezwaren, zoals risico’s op het gebied van het eigenaarschap van de informatie, de beschikbaarheid, juistheid en volledigheid en de beveiliging en vertrouwelijkheid van de informatie.”

Omvang

Shadow-IT heeft betrekking op niet toegestane activiteiten. Dat maakt het lastig een indicatie van de omvang te geven. Partijen die iBestuur hierover wilde spreken, reageerden terughoudend. Een schatting is dat meer dan 35 procent van alle cloudgebaseerde softwaretoepassingen in organisaties zonder toestemming van de IT-afdeling zijn aangeschaft (3).

“Op departementen wordt vaak gebruikgemaakt van illegale webapplicaties zoals Google Drive, Trello, Appear-in, WeTransfer, Prezi en toepassingen voor video conferencing. Op alle niveaus delen ambtenaren vertrouwelijke informatie via WhatsApp”, aldus een bron binnen de Rijksoverheid. “Degene die zijn handen op deze informatie kan leggen, heeft een enorm datalek te pakken. De regels schrijven voor dat voor het gebruik van nieuwe webbased applicaties die niet binnen het standaard aanbod vallen en waarbij data van derden betrokken zijn, officieel toestemming van de CIO van het departement nodig is. Vaak is dat de secretaris-generaal: een onwerkbare beleidsregel.” En als een departement al functionaliteit ontwikkelt die het gebruik van shadow-IT moet terugdringen, is het resultaat meestal dat deze applicaties te laat komen, te ingewikkeld zijn en minder goed werken, aldus dezelfde bron.

Volgens Gianotten ligt het voor de hand dat shadow-IT juist bij de overheid een omvangrijk probleem is. “Bij aanbestedingen wordt vooraf gespecificeerd wat er precies wordt ingekocht. Vandaag beslissen dat je morgen iets nieuws wilt uitproberen past daar niet bij. Door aanbestedingen zijn werkplekken vaak volledig dichtgetimmerd. We zijn bang dat er anders iets fout gaat. Maar als de overheid meer agile zou werken – incrementeel, stapsgewijs – levert dat wellicht betere resultaten op dan de mislukkende megalomane IT-projecten zoals we die nog steeds tegenkomen bij de overheid.” Gianotten draait het vraagstuk liever om: “Je zou kunnen zeggen dat een gebrek aan shadow-IT een probleem is. Shadow-IT faciliteert creativiteit, vernieuwing, innovatie. Ik denk dat daarvoor juist meer ruimte moet zijn – uiteraard met duidelijke kaders.”

> Op alle niveaus delen ambtenaren vertrouwelijke informatie via WhatsApp

Risico’s

Het gebruik van schaduw-IT brengt meerdere risico’s met zich mee. De aanschaf, het gebruik en het beheer vallen buiten de controle van de IT-organisatie. Veiligheidsrisico’s kunnen daardoor niet gemonitord en gemitigeerd worden, ook omdat bij shadow-IT het zicht op updates en de kwaliteit van software ontbreekt. Het levert onduidelijkheid op welke gegevens zich waar bevinden. Dat vergroot de kwetsbaarheid voor aanvallen, en vergroot de kans op datalekken, en problemen met adresboeken.

Het gebruik van shadow-IT draagt ook bij aan een onjuist beeld van de IT-architectuur, van het gebruik van infrastructuur, van software (en behoeften van medewerkers) en van kosten (betaalde oplossingen staan niet op het budget van IT). Vaak worden aangekochte voorzieningen wel aangezet, maar niet uitgezet, zoals bij virtuele machines. Deze zaken worden problematisch als IT wordt uitbesteed, opnieuw wordt aanbesteed of als er integraties moeten plaatsvinden.

Ook bij de gemeente Amsterdam wordt het probleem van shadow-IT herkend. Ger Baron, CTO van gemeente Amsterdam, legt uit dat specifieke afdelingen voor dagelijkse werkprocessen eigen softwarepakketten gebruiken die geen onderdeel uitmaken van de standaard digitale werkplek. Die applicaties werken beter als ze op een standalonesysteem draaien. “Dat vindt de gemeente niet wenselijk, maar het wordt gedoogd omdat de performance van de infrastructuur suboptimaal is: niet snel genoeg om grote hoeveelheden data te verwerken.” Omdat de gemeente steeds meer samenwerkt met partijen buiten de eigen organisatie, wordt er steeds meer gebruikgemaakt van oplossingen zoals WeTransfer, Dropbox en WhatsApp. Dat wordt gedoogd “zolang er geen vertrouwelijke informatie mee wordt gedeeld. Voor een transparant bestuurlijk proces wil je eigenlijk dat communicatie traceerbaar is.”

Medewerkers van het innovatielab van de gemeente Amsterdam maken regelmatig gebruik van AWS-omgevingen, bijvoorbeeld om nieuwe, intern ontwikkelde softwarecomponenten te testen. Ook hier geldt dat dit buiten de officiële servicecatalogus valt en dat er geen persoonsgegevens mogen worden gebruikt. Baron schat in dat hier twintig tot dertig mensen mee werken. “Voor professionals op het gebied van data science en development willen we ruimte bieden om nieuwe technologie te ontwikkelen en te testen of te kopen. Dat wil je snel en laagdrempelig kunnen testen, dus zonder trajecten die maanden duren. Dat moet gaan om het uitproberen, het moet niet een nieuwe standaard worden. Afspraken zijn onder meer: experimenteer op systemen die geen deel uitmaken van het gewone interne netwerk, maar in een afgezonderde omgeving. En maak geen koppelingen met bestaande systemen en gebruik synthetische data.”

Groeiende gebreken

Wie gaat zoeken, vindt een ondoordringbare warboel aan regels, richtlijnen en voorschriften over het gebruik van technologie binnen de overheid. De laatste loot aan deze boom is de nieuwe Baseline Informatiebeveiliging Overheid (BIO, 2019) die moet zorgen voor één basisniveau voor informatiebeveiliging binnen de gehele overheid op basis van internationale normen voor informatiebeveiliging (NEN-ISO/IEC 27001 en NEN-ISO/IEC 27002). De BIO verwijst naar allerlei onderliggende regelingen, zowel gericht op inkoop als op gebruik (zie ook het artikel op pagina i14).

Ondertussen constateerde de Algemene Rekenkamer afgelopen maand dat de Rijksoverheid de informatiebeveiliging nog steeds niet op orde heeft en dat die zelfs is verslechterd ten opzichte van vorig jaar. Met als schrijnend voorbeeld het ICT-systeem voor de omzetbelasting uit 1982, dat niet meer geschikt is om aanpassingen in belastingpercentages door te voeren. Ook het IT-beheer vertoont groeiende gebreken. Als een van de oorzaken wordt aangevoerd: een veelheid aan verouderde systemen. In de nieuwe BIO komt het begrip shadow-IT niet voor. De vraag is wat nieuwe, geïntegreerde richtlijnen bijdragen aan gedragsverandering zolang het onderliggende probleem onopgelost blijft.

Bronnen

1) *https://www.informatiehuishouding.nl/documenten/richtlijnen/2016/6/23/gedragsregeling-digitale-werkomgeving-bzk*
2) *Stadtmueller, L. (2013). The Hidden Truth Behind Shadow IT Six trends impacting your security posture. Stratecast and Frost & Sullivan; 50 Years of Growth, Innovation and Leadership, 1-13.*