Security Architectuur voor een werkende overheid

Peter Rietveld, 8-12-2019.

Dat informatietechnologie onmisbaar en overal is, en de ontwikkelingen steeds sneller gaan zodat we ze niet meer kunnen bijbenen is zo vaak gesteld dat het cliché zwaar versleten is. Het voornaamste resultaat van die versnelling wordt echter te weinig benoemd; legacy, technical debt of ICT-verkrotting. ICT is heel goed in het toevoegen van sexy nieuwe spullen en functies, onderhouden van bestaande systemen en het uitfaseren van achterhaalde zaken lukt vrijwel niemand. De techniek schrijdt voort maar de manier waarop we IT en ICT-projecten besturen, zijn kansloos achterop geraakt. De techniek kan het wel, maar de mensen niet. En ondanks alle verhalen is ICT bovenal mensenwerk.

De volgende reeks drama's ontvouwt zich dan ook in volle vaart: de data revolutie. De lokale overheid is al blij met een succesvolle update van het desktopbesturingsysteem op het gemeentehuis of een migratie naar Azure, maar word binnenkort de regisseur van de smart city en data driven besturing. Het implementeren van AI is niet alleen hip en innovatief; het is ook een IT project, maar dan wel een heel grote. Het model van lokale autonomie en regie betekent dat AI moet concurreren om schaars talent met andere gevoelige dossiers als jeugdzorg en ondermijning. De praktijk is nu al dat kleinere overheden, net als de meeste andere kleine organisaties achter het net vissen bij de jacht op talent. En door de snelle toenamen van de complexiteit worden eisen aan het talent ook nog steeds hoger – zodat er steeds minder mensen de juiste kwalificaties zullen hebben.

Overheden en bedrijfsleven worstelen met deze veenbrand die de economische groei remt en de betrouwbaarheid van systemen en de daarvan afhankelijke instanties ondermijnt. Een van de meest zichtbare resultaten is een niet te beveiligen infrastructuur van systemen uit de vorige eeuw – die een steeds groter deel van de schaarse ICT-specialisten opslokt die met spuug en plakband de boel bij elkaar houden en beveiligen. Zo verhoogt beveiliging de kosten van ICT, echter zonder dat er een navenante stijging van de baten bijkomt.

Verkrotting is het gevolg van zwakke regie

De verhalen zijn over het algemeen overal hetzelfde.

- We weten niet of we een aanpassing kunnen doen zonder per ongelijk iets stuk te maken. Dus we doen de aanpassing niet.
- We weten niet of we een bepaalde voorziening kunnen uitschakelen omdat we niet weten wie of wat het allemaal gebruikt. Dus bergen oude zooi blijft gewoon draaien.
- De software is te oud om nieuwe standaarden te dragen. Dus we kunnen niet mee in de transitie – en moeten de updates uitschakelen. De gemiddelde cybercrimineel verheugt zich nu al.

We snappen onze eigen spullen niet. Te veel, te complex, boven de menselijke maat. En wat je niet snapt kun je niet beveiligen. Of onderhouden: als onzekerheid regeert, is stilstand het resultaat. Oftewel: ondermaatse regie bij gebrek aan inzicht en overzicht is de basis van het overgrote deel van beveiligingsincidenten – de IT heeft tal van redenen om noodzakelijke veranderingen niet door te voeren en wordt na

verloop van tijd overspoelt door de steeds hogere boeggolf. De ontregeling die indertijd voor de millennium bug voorspeld werd, manifesteert zich nu in falende cybersecurity en afstortende IT projecten. Een van de eerste zaken die sneuvelt als de ICT-architectuur verwaarloosd wordt, is beveiligbaarheid: het beveiligen van een verwaarloosde en verweesde ICT is bij voorbaat kansloos.

De rol van (security) architectuur
In security speelt hetzelfde als in de jaren tachtig in de IT: versnippering. Eerst was beveiliging vrij simpel: we verschuilen ons achter een firewall; alles binnen is goed en alles buiten is fout en de beveiliging is geconcentreerd op het poortgebouw.

Toen de simpele muur om de organisatie niet meer bleek te werken, begin deze eeuw, kwam er een stortvloed van beveiligingsmiddelen bij en het eind is voorlopig niet in zicht. Het ideaal is nu de gelaagde beveiliging van ‘Defence in Depth’, waarin al die maatregelen en complexe spullen samenwerken. Van een simpele stadsmuur met één poort werd onze beveiliging een complex en gelaagd geheel aan fortificaties en egelstellingen met geheime tunnels alle kanten op. Dat vraagt overzicht, regie en een regisseur. Als het gaat om regie, werkt ieder voor zich helemaal niet. Overheden die niet samenwerken, zullen op het cyberfront onherroepelijk falen. Samenwerken is echter afhankelijk van menselijke capaciteit, en de meeste overheden zijn te klein om het talent te kunnen vinden en te behouden.

Vanuit beveiliging geredeneerd is de autonomie van kleinere bestuurlijke entiteiten veel te groot. Samenwerken voor veiligheid zal de komende jaren moeten overgaan in samengaan. Deze transitie zal de Nederlandse overheden en de lappendeken van samenwerkingen op IT-gebied – niet alleen met elkaar maar ook met de ketenpartners - moeten transformeren tot één enterprise. Zo zullen overheden na een federatieve overgangsfase meer als franchisenemers in een formule werken dan als autonome entiteit. Onder één enterprise architectuur – niet allemaal hetzelfde, maar wel samenhangend. Dit vraagt een centralisatie van ICT – en dat is een enorme verandering. Om dit mogelijk te maken is een centraal enterprise architectuur proces één van de onmisbare onderdelen, een essentiële succesfactor.

Eén kanttekening. Enterprise security architectuur komt voort uit enterprise architectuur, wat weer voortkomt uit IT. Het probleem hiervan is dat beiden, zowel enterprise architectuur als enterprise security architectuur, soms te smal worden gezien. De enterprise architect ontwerpt IT-systemen en de enterprise security architect zet er security-functies op. Klaar. Toch?

Niet klaar! De praktijk is anders, security gaat niet alleen gaat over functies van het systeem, maar ook over het beheer, het onderhoud en het gebruik van de systemen. Je moet je dus ook bezighouden met processen, met mensen, met hoe de organisatie is ingericht. Je moet geen systeem neerzetten als je niet weet hoe je het gaat onderhouden. Zonder een samenhangende manier van werken zijn de IT projecten van nu de kamervragen van de toekomst.

Nog een kanttekening. Te veel architecten denken in abstractie stippen op de horizon en zien zichzelf als een toekomstmaker, een soort beleidsmaker. Dat is echter niet de hoofdtaak: architectuur in haar verschillende gedaanten levert de inhoudelijke kant van de regie – het neemt niet ‘de macht’ over. De belangrijkste rol van security

architectuur is niet bepalen, maar uitleggen. Hoe zit de boel nu in elkaar? Welke mogelijkheden zijn er? Wat verandert er met project X of update Y. Zo zal de architect de bestuurder kunnen uitleggen hoe het zit, wat de keuzes zijn en wat de praktisch uitwerking van de opties zijn. Architectuur is veel meer dan adviseren wat te doen. Een goed en integer ingericht architectuurproces staat ten dienste van besturing.

Security by design; Ontwerpen vanuit de basis
Anno 2020 streven we naar Security by Design. Dat gaat echter bepaald niet vanzelf. De term security by design komt uit de hoek van software engineering. De associatie met software is er nog steeds, maar zoals security ook veel meer omvat dan het toevoegen van beveiligingsfuncties aan computersystemen is ook security by design niet alleen een kwestie van software maken of aanpassen. Een architect is een ontwerper, een security architect ontwerpt veiligheid. Om het iets concreter te maken: het gaat om beschikbaarheid, integriteit en vertrouwelijkheid.

- Beschikbaarheid: je zorgt dat de juiste mensen ergens bij kunnen (identity en access management).
- Integriteit: je zorgt ervoor dat mensen de informatie in het systeem niet onbedoeld kunnen veranderen (access management).
- Vertrouwelijkheid: je zorgt ervoor dat de mensen die er niet bij mogen komen, dit ook niet kunnen (access management).

Security, en dus ook security by design, gaat in de basis om deze drie doelen. Voor alle drie geldt natuurlijk dat er geen gaten in de software zitten (pentesten, vulnerability en patchmanagement), waardoor onbevoegden de informatie zouden kunnen manipuleren of weggooien.

Het specifieke van security by design is dat je deze doelen niet los ziet van alle overige processen, maar dat je zorgt voor veiligheid in elke stap van elk project en van elke ontwikkeling. Ook daaruit volgt weer dat we het niet moeten hebben over techniek alleen. Want wie gaat die techniek gebruiken, welke procedures hebben ze daar voor nodig en wie zorgt ervoor dat alles volgend jaar ook nog werkt? Techniek heb je nodig, ja zeker, maar voor al deze drie basisdoelen geldt dat het ook gaat over processen, procedures, en uiteindelijk vooral over mensen.

De belangrijkste taak van de enterprise security-architect is het ontwerpen van goed bestuurbare security, oftewel governance. Hoe komen we van de gefragmenteerde silo’s van nu naar een gesloten digitaal front dat sterk genoeg is om de digitale infrastructuur nu en later te beveiligen. Dat is de discussie die we als Nederlandse IT- en security-architecten willen voeren met de overheid.

Kansen voor Nederlandse bedrijven
Met de ondersteuning voor AI van rijkswege, zoals het strategisch actieplan SAPAI biedt, kunnen Nederlandse bedrijven wellicht beter de concurrentie aan met China en de VS. Helaas is zonder een ingreep in het huidige ICT landschap het gekozen spoor, optimaal gebruik van AI bij de publieke taak- en zaakuitvoering, kansloos.

We mikken met subsidie en scholing op hetzelfde segment als de andere landen: de technologie die hopelijk goed geïmplementeerd en toegepast wordt. Met een geringe bijstelling van onze focus kunnen we slimmer en effectiever concurreren. Klassiek in

de ICT is de rol van integrator, die de technologie van een ander integreert en praktisch in past. Er gaat altijd veel meer geld om in de succesvolle integratie van technologie dan in het maken ervan. En integratie is per definitie lokaal en mensenwerk van een grote groep, wat dus niet weggekocht kan worden.

Door de lokale vraagkant volwassener te maken kan het Nederlandse bedrijfsleven leren vernieuwende technologie succesvol in en toe te passen. De meest effectieve manier die de overheid heeft om de vraagkant goed te organiseren is de eigen ICT. Een integrator die bijvoorbeeld de gemeente Rotterdam heeft geholpen om tot smart city te verbouwen, is prima geëquipeerd om hetzelfde voor Hamburg of Philadelphia te doen.