Cybersecurity

als enabler van digitale transformaties

Op welke manier draagt **cybersecurity** bij aan **Social**, **Mobile, Analytics** en **Cloud**?

Cybersecurity is een directe enabler van de vier belangrijke digitale transformaties van deze tijd: Social, Mobile, Analytics en Cloud.

Highlights

- Cybersecurity is een enabler van digitale transformaties bij organisaties.
- Goede security maakt organisaties wendbaar bij nieuwe ontwikkelingen.
- Cybersecurity biedt waarde en kansen voor de organisatie.
- Zonder cybersecurity neemt de kwetsbaarheid van je primaire processen toe.
- Cybersecurity is daardoor een thema voor in de bestuurderskamer.

Aanleiding

Cybersecurity wordt nog te vaak alleen als een kostenpost gezien, doordat de betekenis van security voor primaire processen van organisaties buiten beschouwing wordt gelaten. De businesscase van cybersecurity-investeringen wordt hierdoor te negatief ingeschat en voorstellen ter verbetering van de cybersecurity leggen het in de praktijk onterecht af tegenover andere prioriteiten. In dit artikel kijken we daarom naar het belang van cybersecurity voor organisaties als enabler van de digitale transformaties van deze tijd: Social, Mobile, Analytics en Cloud.

Social, Mobile, Analytics en Cloud (SMAC)

De impact op organisaties van technologieën op het gebied van Social, Mobile, Analytics en Cloud is zo fundamenteel dat vaak wordt gesproken over digitale transformaties om de veranderingen te beschrijven. Met Social, Mobile, Analytics en Cloud worden de volgende trends aangeduid:

- Social gaat over het verbinden van de omgeving van de organisatie door social media, het communiceren met die omgeving en het versterken van de eigen reputatie.
- Mobile gaat over de veranderingen die met name de smartphone heeft gebracht op de manier waarop we communiceren. Als voorbeeld kan daar de mogelijkheden voor e-mail onderweg of messaging worden genoemd.
- Analytics, ook Big Data of simpelweg 'Information' genoemd, gaat over de mogelijkheden om alle beschikbare data om te zetten in toegevoegde waarde voor organisaties.
- De impact van Cloud-technologie is te relateren aan het overal direct beschikbaar zijn van data. Voor organisaties betekent Cloud ook kostenefficiëntie, flexibiliteit en schaalbaarheid.

Cybersecurity als enabler

Cybersecurity is een directe enabler voor de vier digitale transformaties. Security ondersteunt innovatie doordat in een veilige omgeving sneller kan worden geëxperimenteerd met nieuwe technologieën voor nieuwe producten of diensten die op alle verschillende apparaten en platformen toegankelijk zijn. Klanten en andere stakeholders kunnen door cybersecurity nieuwe mogelijkheden geboden worden, zoals (veilige) inzage in het eigen klantendossier of online bankieren. Dit brengt klanten directer in controle over hun eigen informatie en de diensten die ze willen betrekken.

Om de rol van cybersecurity als enabler te maximaliseren, is het uiteraard essentieel om de security goed in te richten. Met een slecht inzicht in de belangen van de organisatie, een onduidelijk beeld van risico's en ad hoc georganiseerde maatregelen en architectuur, zal cybersecurity slechts een belemmering vormen voor nieuwe ontwikkelingen. Een goed ingerichte cybersecurity beweegt mee met de primaire processen van de organisatie, zodat de gewenste wendbaarheid in de primaire processen

van de organisatie wordt ondersteund door een flexibele security eromheen.

Social

De Social-trend voor organisaties betreft het zorgvuldig in verbinding komen met de omgeving van de organisatie door social media. Social zorgt ervoor dat organisaties op innovatieve wijze contact kunnen maken met burgers en klanten (en vice versa). De mogelijkheden om effectief contact te houden met klanten en burgers zijn verveelvoudigd en tevens vereenvoudigd. De interactie is directer en sneller. Hierbij gaat het zowel om de interne communicatie in organisaties als de interactie met omgeving.

Tegelijkertijd verandert ook het verwachtingspatroon van de omgeving. Burgers en klanten verwachten dat organisaties sociaal worden: dat er snel gereageerd wordt op vragen, opmerkingen en klachten. Het maakt daarbij voor hen niet uit via welk medium zij deze vragen kunnen stellen. De snelle interacties en de toename van digitale toegangspunten in de organisatie vragen om een goed beveiligde omgeving, zodat er geen onbevoegd toegang ontstaat tot data van buiten en dat de data die niet naar buiten mag gaan, ook beschermd blijft.

Mobile

De Mobile-trend heeft grote impact op de security van organisaties. Bring Your Own Device (BYOD) is een voorbeeld van mobiel en hyperconnected acteren binnen een organisatie. Ook 'Het Nieuwe Werken' brengt met zich mee dat medewerkers via verschillende apparaten op verschillende locaties toegang hebben tot hun werkomgeving. Net als bij de Social-trend neemt het aantal digitale toegangspunten tot organisaties door Mobile sterk toe. Het is niet mogelijk om zonder security-waarborgen op deze nieuwe wijze te werken. Een organisatie kan niet meer worden georganiseerd zoals vroeger: als een kasteel met een slotgracht en de ophaalbrug als enig toegangspunt. Tegenwoordig kan de ophaalbrug gemakkelijk worden omzeild. Neem bijvoorbeeld een selfservice-portal als eHerkenning voor ondernemers. Hier kunnen ondernemers met een digitale sleutel meerdere diensten bij meerdere overheidsinstanties afnemen. Cybersecurity maakt deze vernieuwende dienstverlening mogelijk. Het stelt wel hoge eisen aan de security-architectuur en de vaardigheden om het dataverkeer te monitoren. Door monitoring kan adequaat worden ingegrepen bij ongeoorloofde toegang door hackers of door misbruik van accounts. Het ontwikkelen van deze monitoring en detectiecapaciteiten in de organisatie is de komende cybersecurity-trend.

Analytics

De digitale transformatie door Analytics, ook 'Big Data' of 'Information' genoemd, houdt ook verband met intelligent monitoren. De transformatie die Analytics mogelijk maakt, kent nadrukkelijk twee kanten. Aan de ene kant bieden grote hoeveelheden aan beschikbare informatie - en de intelligente tools om daarin verbanden te herkennen - veel mogelijkheden voor organisaties. Analytics heeft de potentie om dienstverlening te verbeteren op basis van niet eerder ontdekte patronen in grote hoeveelheden data. Binnen het veiligheidsdomein biedt Analytics de kans om toezicht, handhaving en opsporing te versterken. Uit het Trends in Veiligheid 2014 onderzoek van Capgemini, uitgevoerd door TNS NIPO, blijkt dat de Nederlandse bevolking steeds vaker een actievere houding van de overheid verwacht als het gaat om de aanpak van cybercriminaliteit. Van de Nederlanders is 88% een voorstander van een actiever optreden. Opsporingsdiensten maken gebruik van Analytics om te voldoen aan deze maatschappelijke verwachting. Strafbare feiten worden door een gerichte toepassing van Analytics eerder blootgelegd en digitale forensische onderzoekers analyseren bewijsstukken sneller en effectiever.

Aan de andere kant veroorzaken de mogelijkheden van Analytics grote zorgen in het maatschappelijk debat over het waarborgen van privacy van burgers. Uit het Trends in Veiligheid 2014 onderzoek blijkt ook dat het vertrouwen in de overheid dat zij de privacy van burgers voldoende beschermt, langzaamaan afneemt. Deze twee uitkomsten geven het spanningsveld tussen meer veiligheid en privacy direct aan. Als de overheid effectief wil optreden, negeert ze de kansen van Analytics niet. Het waarborgen van de privacy van burgers is daarbij essentieel om het vertrouwen van burgers in de overheid op het gebied van privacy te behouden. Zeker nu de overheid steeds meer digitaal wil communiceren met burgers en daarbij persoonlijke data opslaat, zal de overheid transparant moeten zijn betreffende de doelen waarvoor het de gegevens gebruikt. Burgers moeten erop kunnen vertrouwen dat hun gegevens niet voor andere doelen worden gebruikt dan waarvoor ze zijn verzameld, en dat deze zogeheten 'function creep', zeer beperkt blijft.

Transparant cybersecurity-beleid en passende cybersecurity-maatregelen kunnen ongeoorloofd gebruik van gegevens begrenzen. Enerzijds door de toegankelijkheid tot de Big Data van buiten de organisatie te beveiligen. Anderzijds door ongeautoriseerd inzicht in gegevens binnen organisaties te limiteren. Cybersecurity-maatregelen ondersteunen in organisaties de naleving van privacywetgeving, zoals de Wet politiegegevens en de Wet justitiële en strafvorderlijke gegevens, door juiste archivering van data. Ook actief identity en access management, zodat toegang en autorisaties tot gebouwen, afdelingen en applicaties wordt bijgehouden, is een praktische oplossing voor het borgen van privacy.

Cloud

Cloud-technologie is de laatste van de vier digitale transformaties. De transformatie door Cloud-technologie

maakt bezit van data minder relevant dan toegang en beschikbaarheid. Organisaties, maar ook individuen, zetten steeds meer privacygevoelige data in Cloud-diensten vanwege de flexibiliteit, de toegankelijkheid en de lage kosten. Voor organisaties die snel groeien of snel nieuwe dienstverlening willen aanbieden, is de schaalbaarheid in de Cloud van groot voordeel. Een van de belangrijkste randvoorwaarden om de transitie naar Cloud voor organisaties en burgers succesvol te kunnen maken, is door maximaal in te zetten op het beschermen van de veiligheid van data in de Cloud en het waarborgen van privacy.

Op het gebied van Cloud is de overheid op dit moment zeer actief in het verbinden van bestaande informatiebronnen en databases in allerlei knooppunten. In deze - veelal Cloud-achtige - structuren zijn gegevens beschikbaar voor eindgebruikers, maar ze worden vaak niet meer bij de eigen organisatie gehost, waardoor data en eindgebruikers fysiek van elkaar zijn gescheiden. De inzet op het verbinden van bestaande informatiebronnen wordt gedreven door de wens om primaire processen effectiever en efficiënter te laten verlopen. Voorheen gescheiden beleidsvelden worden via deze knooppunten naar elkaar toegebracht om uiteindelijk primaire processen te versterken. De drie decentralisaties van jeugd, werk en zorg van het Rijk naar gemeenten zijn daar momenteel een in het oogspringend voorbeeld van. In deze reorganisatie worden onder meer zeer privacygevoelige gegevens uit medische dossiers en justitiële dossiers bij elkaar gebracht in knooppunten bij gemeenten. Het verbinden van dergelijke verschillende informatieregimes stelt zeer hoge eisen aan het securitybeleid en de ingebouwde maatregelen voor beveiliging en privacy. Vraagtekens over de security in deze knooppunten kan het welslagen van de decentralisaties sterk hinderen.

Conclusie

Het succesvol integreren van de digitale transformaties in organisaties is sterk afhankelijk van de enabling functie van cybersecurity. De meerwaarde die cybersecurity biedt voor organisaties lijkt daarmee eindeloos. Het benadrukken van de rol van cybersecurity als enabler, maakt de businesscase voor cybersecurity-investeringen sterker. Binnen de cybersecuritygemeenschap dient de eigen focus daarom sterker gericht te zijn op de functie van enabler voor de vier transformaties.

Over de auteurs

Drs. Matthijs Ros, drs. Laurens van Nes en Lieke Schepers MSc zijn respectievelijk als managing consultant en consultant actief op het gebied van openbare orde en veiligheid. Specifiek richten zij zich op vraagstukken op het vlak van intelligence en cybersecurity.

Contactgegevens

Voor meer informatie kunt u contact met de auteurs opnemen via **matthijs.ros@capgemini.com, @matthijsros, laurens.van.nes@capgemini.com en lieke.schepers@capgemini.com**