

ICT-innovaties en winkelautomatisering

De crisis hakt er flink in, ook in de retail. Volgens het in oktober verschenen rapport *Trends in retail 2009-2010* (CapGemini) zijn consumenten voorzichtig geworden. 'Heb ik het echt nodig?', vragen zij zich af. Onderscheidend vermogen helpt de retailer ondanks de crisis beter te presteren. Winkelinnovaties helpen daarbij. Maar veel innovaties zijn gestoeld op ICT-oplossingen. Dit heeft consequenties voor de winkelautomatisering.

TIM WATERS *

Steeds meer innovaties in de retail hebben een relatie met ICT. Al deze ICT-oplossingen komen uit verschillende hoeken van de organisatie en hebben vaak andere belangen. De marketingafdeling gebruikt *nar-rowcasting* om de consument beter te bereiken in de winkel. Security gebruikt HD-camera's om de beveiliging aan te scherpen. En ICT gebruikt *Voice over IP* (VoIP) om de onderlinge telefoniekosten te beperken. Deze technologieën hebben één ding gemeen: ze maken gebruik van het computernetwerk waarover ook de bedrijfsapplicaties zoals het POS-systeem (kassasysteem) gaan. Hierdoor wordt de

netwerkapparatuur en -verbindingen helpt om de kans op een incident te verkleinen.

Beveiligingsbelangen

Om grip te krijgen op dit soort zaken zult u bovenal geïnformeerd moeten zijn. Geïnformeerd over nieuwe projecten die consequenties hebben voor het netwerk. Als er dan een project wordt gestart, bent u er tijdig bij om (rand-)voorwaarden te stellen. Uiteraard hoeft u die voorwaarden niet zelf op te stellen. U kunt tenslotte ook een technisch onderlegde medewerker in het project laten participeren. Deze persoon dient dan de be-

werk afnemen. Het simpele netwerk van vroeger met maar één applicatie wordt een complexe brei van informatie-uitwisselingen. Hierdoor worden het beheer en het maken van aanpassingen ingewikkelder en neemt de kans op fouten toe. In grotere projecten ziet men dan soms details over het hoofd. Later in het project blijken deze dan voor problemen of inconsistenties te zorgen. Na veel tijd en moeite wordt het probleem dan uiteindelijk gevonden. Maar ondertussen loopt het project wel al achter op schema en worden de mogelijke baten niet gerealiseerd. Dergelijke problemen kunnen worden opgelost door alle informatiestromen grondig te analyseren. Na deze analyse kunnen de informatiestromen die elkaar niet 'bijten', worden samengevoegd. Dit reduceert de complexiteit en komt dus de betrouwbaarheid ten goede.

Het is zaak om als security manager dicht op het project te zitten

winkelautomatisering als geheel in steeds grotere mate afhankelijk van het netwerk. Een incident op het netwerk heeft dan ook een grotere impact dan vroeger. Een goed afgewogen mix van maatregelen kan de impact van het wegvallen van het netwerk verkleinen. Zo kunnen kassa's autonoom worden gemaakt, zodat ze bij uitval kunnen doordraaien. Maar ook redundantie aanbrengen in

veiligings-/kwaliteitsbelangen te behartigen en mag geen operationele rol binnen het geheel hebben. Ook kunt u, wanneer de kennis niet aanwezig is binnen de organisatie, een derde partij consulteren.

Minder betrouwbaar

Door de toename van ICT-oplossingen - en daarmee de complexiteit - kan de betrouwbaarheid van het net-

Ook kan het zijn dat bij de implementatie van een innovatie het netwerk verzadigd raakt. Kenmerkend is dat op het drukste moment van de dag problemen beginnen op te spelen. Logisch, hoe drukker het in de winkel is hoe drukker het ook op het netwerk wordt.

Bijvoorbeeld bij het gebruik van IP-camera's wordt er op drukke mo-



menten meer informatie over het netwerk gestuurd. Dit komt doordat er meer klanten in de winkel lopen, waardoor de camera meer bewegingen registreert. Deze beeldwijzigingen worden vervolgens via het netwerk naar de registratieserver gestuurd. Meer bewegingen betekent dus ook meer dataverkeer over het netwerk. Een andere factor is uiteraard het hogere aantal transacties van het POS-systeem. Hoe drukker het in de winkel is, hoe meer transacties er worden gedaan. Ook andere systemen zoals informatiezuilen of retourbalies vragen dan meer netwerkbandbreedte. Hierdoor kan het zijn dat telefoongesprekken haperen of uitvallen, of PIN-transacties falen. Veelal kunnen deze problemen worden voorkomen wanneer men bij de implementatie capaciteitsbeheer in het project opneemt. De leverancier van de nieuwe ICT-oplossing kan een goede schatting geven van het verwachte netwerkverbruik. Hierdoor kan men voor ingebruikname van de innovatie maatregelen nemen. Zo kan men de capaciteit van het netwerk opschalen of belangrijke informatiestromen prioriteren, zodat er een grotere zekerheid ontstaat dat bij congestie belangrijke informatiestromen intact blijven of niet vertragen. Het is zaak om als security manager dicht op het project te zitten. Hierdoor kunt u de beveiligingsbelangen van de organisatie binnen het project behartigen. U kunt zo (mede) bepalen welke (nieuwe) informatiestromen welke prioriteit krijgen. En u kunt aangeven welke informatiestromen eventueel samengevoegd kunnen worden.

Leveranciers over de vloer

Die nieuwe oplossingen brengen meestal nog iets anders met zich

mee: leveranciers. Want de implementatie van het project is pas het begin. Daarna begint de onderhouds-lifecycle. En tenzij uw (ICT-)afdeling al deze oplossingen zelf gaat onderhouden, krijgt u meer leveranciers over de vloer. Hierdoor ontstaat vaak verwarring en onvrede bij het winkelpersoneel. Want wie moeten zij nu bellen voor dat probleem? En hoe weten zij dat de monteur inderdaad is wie hij zegt dat hij is? Vooral dat laatste is met het oog op *skimming* een actueel probleem. Om dit te voorkomen kan men een procedure instellen. Hierin kan men met leveranciers een afspraak maken dat monteurs zich altijd vooraf aanmel-

teit extra verifiëren. Dit kan bijvoorbeeld door de monteur naar zijn rijbewijs of paspoort te vragen. Iets wat hij toch al op zak moet hebben.

Conclusie

Door de huidige moeilijke markt moet de retail meer dan ooit innoveren om de klant te blijven boeien. De hiermee vaak samenhangende toename van ICT-systemen brengt complexiteit en risico's met zich mee. Grotere afhankelijkheid van netwerkverbindingen is daar een voorbeeld van. Een ander risico is dat de complexiteit van het netwerk toeneemt, waardoor men het overzicht kwijtraakt. Hierdoor ontstaan sneller fou-

Bij het gebruik van IP-camera's wordt er meer informatie over het netwerk gestuurd

den. Dit kan dan bijvoorbeeld bij een centraal contactpunt op het hoofdkantoor. Dit kan vervolgens ook in de winkel, maar dan uitsluitend bij één of twee personen. Bijvoorbeeld bij lokaal ICT-personeel of de hoofdcaissière. Dit voorkomt dat een kwaadwillende verwarring zaait door zich zogenaamd vooraf te hebben aangemeld bij een afwezig persoon. Eventueel kan ter verificatie een door de leverancier of het centrale contactpunt vooraf doorgegeven ticketnummer worden gevraagd. Een andere oplossing is dat monteurs zich moeten kunnen legitimeren door middel van een speciaal pasje. Op dit pasje staat een nummer waarmee via het centrale contactpunt of de leverancier de identiteit van de monteur geverifieerd kan worden. Als er geen foto op de pas aanwezig is, kan het winkelpersoneel de identi-

ten. Ook brengt het groeiende aantal leveranciers van ICT-oplossingen in de winkel risico's met zich mee. Deze risico's kunnen - wanneer benoemd en geanalyseerd - verkleind worden. Dit kan onder andere door:

- » expliciet betrokken zijn bij relevante nieuwe projecten vanuit de beveiligingsfunctie;
- » vanuit de beveiligingsfunctie voorwaarden stellen aan de beveiliging en algemene inrichting van de innovaties;
- » een procedure inrichten waarbij leveranciers zich vooraf moeten melden;
- » een centraal punt inrichten dat leveranciercontacten verwerkt. «

* Tim Waters is adviseur informatiebeveiliging met als specialisatie ICT-security bij LBVD Informatiebeveiligers (tim.waters@lbvd.nl)