

CASE STUDY:



Tripwire software geeft inzicht in ongeautoriseerde wijzigingen

CHANGE EN CONFIGURATION MANAGEMENT CORE BUSINESS VOOR ALEX BELEGGERSBANK

Alex Beleggersbank was in 1999 de eerste partij in Nederland die zich helemaal toegedeed op on-line beleggen. Inmiddels bedient de bank 100.000 klanten en is het de grootste aanbrenner van particuliere orders op zowel de aandelen- als de optiebeurs van Euronext Amsterdam. Alleen al in 2006 verwerkte het bedrijf 3,2 miljoen orders. Dit vraagt om systemen met maximale beschikbaarheid, veiligheid en schaalbaarheid. Tegelijkertijd is de markt van on-line beleggen een zeer concurrerende markt, waarbij met name innovatiekracht een belangrijk onderscheidend kenmerk is. De systemen van Alex moeten dus snel en veelvuldig kunnen veranderen. Om te zorgen dat alleen geautoriseerde wijzigingen worden doorgevoerd zet Alex, op advies en onder begeleiding van security-partner Pinewood, vanaf deze zomer ook de software van Tripwire in.

Alex ontwikkelt alle software zelf en ongeveer een kwart van alle medewerkers is dan ook actief op het gebied van IT. Om de kwaliteit van de systemen en dienstverlening onverminderd hoog te kunnen houden heeft Alex de laatste jaren vooral op het gebied van processen belangrijke wijzigingen doorgevoerd.

TESTEN EN AUTORISEREN

Van de ca. 240 medewerkers is een kwart werkzaam in de IT, waarvan 40 ontwikkelaars. Ed Lanen, Manager ICT: “Het acceptatietesten vindt plaats in een schaduwomgeving, of acceptatieomgeving. Als de test goed bevonden wordt dan wordt de wijziging geautoriseerd. Wat ik vandaag autoriseer in de testomgeving, komt vervolgens ook in productie. Als dat gebeurt, dan is dat dus conform verwachting, en dan hoef ik het niet te zien. Ik wil alleen de gevallen zien waar iets mee aan de hand is. De onverwachte wijzigingen.”

Naast de ontwikkelaars zijn er ca 20 beheerders. Zij beheren de IT infrastructuur. “In formele zin zijn aanpassingen die beheerders in productie doen allemaal wijzigingen. Zo ook parameterwijzigingen”, zo vervolgt Ed Lanen. “Bij Alex hebben wij er echter voor gekozen dat alleen infrastructuurwijzigingen die een aantoonbaar risico zijn voor de stabiliteit, via het changeproces in productie worden genomen. Dat betekent dus een grijs gebied. Waar eindigt beheer en begint een wijziging? Deze inschatting is in het verleden wel eens verkeerd gegaan en dat leidde direct tot verstoringen. Tripwire maakt dit nu zichtbaar.”

“Het is cruciaal om dit wijzigingsproces ook technisch goed af te dekken. Wij controleren nu met Tripwire of er wijzigingen zijn doorgevoerd die niet door de formele changeproces zijn gegaan. Het is de bedoeling dat het preventief werkt, zodat medewerkers er vooraf al rekening mee houden en een betere inschatting van de risico's maken. Onze beheerders kunnen zelf beheertaken uitvoeren in productie en software in productie brengen. Met Tripwire kunnen we echter voortdurend zien of er iets gebeurd is dat niet had mogen gebeuren. Doordat iedereen weet dat deze controle plaatsvindt is het systeem daarmee preventief geworden.”

IMPLEMENTATIE IS BEDRIJFSKUNDIGE UITDAGING

Wat Ed Lanen betreft is de implementatie van een tool als Tripwire vooral een bedrijfskundige uitdaging, veel meer dan een technische. “In juli 2006 zijn we voor het eerst met de software van Tripwire in aanraking gekomen, en deze zomer gaan we live. Je moet eerst acceptatie creëren en draagvlak hebben. Tripwire werd toch als een controlemiddel gezien en als zodanig wekte het de weerstand op van degene die zich gecontroleerd voelen. Daar moet je begrip voor hebben. We hebben de beheertaak en de verantwoordelijkheid voor Tripwire daarom niet neergelegd bij Technisch Beheer. Het is volgens mij namelijk niet verstandig om de controle neer te leggen bij de afdeling die zelf de wijzigingen in productie brengt. We hebben er dus voor gekozen het systeem en de verantwoordelijkheid ervoor neer te leggen bij het Support & Test Center, verantwoordelijk voor het gehele Change Management. Een duidelijke functiescheiding.”

VERTROUWEN KWEKEN

Als Tripwire nu een ongeautoriseerde wijziging tegenkomt dan gaan de beheerders en het Support & Test Center samenzitten om te bezien of er geen onnodige risico's zijn genomen. Tripwire is ook niet alleen een controlemiddel. Ook incidenten laten zich nu veel makkelijker opsporen en lokaliseren. Alle wijzigingen zijn nu beter in kaart gebracht en er zijn dus ook voordelen voor de beheerafdeling, bij het oplossen van problemen.

Tripwire kijkt per dag, of met enige regelmaat naar welke bestandjes er veranderd zijn. Er zijn daarbij potentieel oneindig veel veranderingen en je moet dus heel goed instellen wat je wel en wat je niet teruggekoppeld wilt hebben. Ed Lanen: “Tripwire is in zekere zin een SLA-beheertool, ik vind het eigenlijk geen audit tool, daar is het te operationeel voor, te gedetailleerd. “Om het zo te kunnen instellen dat je precies de rapportages krijgt die je nodig hebt hebben we nauw samengewerkt met onze vaste partner Pinewood. Om te bepalen wat je wél wilt zien en niet wilt zien, moet je echt wel even de tijd nemen. Pinewood is de eerste en enige partij in Nederland die volledig gecertificeerd is op Tripwire. De consultants van Pinewood hebben daarnaast ook nog eens bijzonder veel ervaring in de financiële sector. Zij weten als geen ander welke informatie wel of niet nuttig is.”

Tripwire is geïnstalleerd op alle systemen: servers, firewalls, netwerkcomponenten en desktops. Op alle apparaten worden Tripwire agents geïnstalleerd die periodiek rapporteren of op dat systeem iets veranderd is. Daarnaast vindt ook agentless monitoring plaats.

ROI

Ed Lanen: “Als het gaat om de meetbaarheid van het succes van Tripwire dan is dat niet snel in absolute getallen uit te drukken. Het is wat mij betreft een succes als het aantal infrastructurele incidenten daalt en de beschikbaarheid toeneemt. Daarmee meet je meer kwalitatief dan de ROI. Twee jaar geleden hebben we ons testproces ingericht, en daarbij ook nooit echt gemeten wat het ons nu bespaard heeft, maar we weten nu wel dat niemand het meer zou willen missen. Iedereen is overtuigd van het nut. Dat gaat met Tripwire net zo.”



Ed Lanen, Manager ICT bij Alex bellegersbank