

Webwasher houdt content veilig met behoud van performance

UNIVÉ VEEGT INTERNETSTRAAT SCHOON

Medewerkers van verzekeraar Univé zijn voor een belangrijk deel van hun werk afhankelijk van een betrouwbare en veilige internetverbinding. Verschillende interne en externe verzekeringsapplicaties zijn momenteel hoofdzakelijk beschikbaar via het web. De beveiliging van de verbinding tussen het landelijke bedrijfsnetwerk en het internet – de internetstraat - is dus cruciaal. Security-partner Pinewood adviseerde en implementeerde Webwasher van Secure Computing voor het scannen van het internetverkeer van 150 locaties, zonder verlies van performance.

Het netwerk van Univé omvat vier centrale vestigingen in Assen, Alkmaar, Heerlen en Zwolle, maar ook de kantoren en bijkantoren van de zogenaamde zelfstandige Onderlingen. In totaal zijn dit zo'n 150 locaties, verdeeld over Nederland. Op al deze vestigingen ondersteunt het netwerk in totaal circa 3.200 medewerkers. Als een coöperatieve vereniging zonder winstoogmerk biedt deze totaalaanbieder van verzekeringen naast brand-, schade- en zorgverzekeringen ook levensverzekeringen en hypotheeklen aan particuliere en zakelijke klanten. Momenteel heeft Univé ongeveer 1,3 miljoen verzekerden die in totaal 3,7 miljoen verzekeringen hebben afgesloten. Hiermee is Univé één van de grootste verzekeraars van Nederland.

In principe gaat al het Univé-internetverkeer via een centrale koppeling met het internet. Die 'internetstraat' staat in Zwolle. Nijland: "Onze medewerkers surfen heel wat af voor hun werk. Maar dat betekent dus niet dat ze het internet afschuimen naar interessante websites. We bieden de vestigingen toegang tot onze centrale systemen, bijvoorbeeld voor het opmaken van online offertes. Dat kan vanuit de kantoren, maar ook buitendienstmedewerkers kunnen deze applicatie op afstand benaderen. Daarnaast zijn de verzekeringswereld verschillende bedrijfskritische applicaties alleen nog via internet beschikbaar. Deze worden dan op afstand gehost. Een voorbeeld is een applicatieomgeving voor de efficiënte afhandeling van autoschades, waar naast verzekeraars ook schade-experts en schadeherstelbedrijven toegang tot hebben. Natuurlijk is die verbinding momenteel goed beveiligd met wachtwoorden en tokens. Maar er staan bijvoorbeeld ook foto's van schadeauto's op die site. Hackers en virusbouwers zouden die illustraties kunnen misbruiken om virussen en andere schadelijke code te distribueren."

CAPACITEITSPROBLEMEN

De internetstraat van Univé is in de loop van de tijd steeds verder uitgebreid. In de praktijk betekent dat dat het internetverkeer en de content van en naar het netwerk door heel wat systemen heen moet. Naast externe en interne firewalls en antivirusoplossingen gebruikt Univé ook een proxy en contentfilters. Afgelopen zomer kwam de balans tussen beveiliging en netwerkprestaties onder druk. "Vooral met contentscanning zaten we tegen de de grens van het aantal gebruikers aan dat deze oplossing kon ondersteunen. Om performance-problemen voor de eindgebruikers voor te blijven, moesten we actie ondernemen. In eerste instantie leek een uitbreiding van de scancapaciteit voldoende. Maar dat zou slechts tijdelijk verlichting brengen. Bovendien betekende extra systemen ook weer extra schakels met de bijbehorende vertraging in het scanproces, inclusief extra beheer. Pinewood suggereerde een andere oplossing. Zij zijn bekend met onze omgeving omdat ze in eerdere projecten al interne firewalls en proxies hadden geleverd en geïmplementeerd. Mede daarom zijn we een pilot met de Webwasher van Secure Computing gestart. Inzet van deze appliance voor contentscanning bleek ons op verschillende vlakken voordelen te bieden. Die vormden het uitgangspunt om met Pinewood in overleg te gaan over de prijs en benodigde functionaliteit. Bij Univé doen we dat altijd in een team dat bestaat uit iemand met de technische kennis en een specialist op het vlak van inkoop. Samen zijn we daar goed uitgekomen."

COMPLETE SCANS

De Webwasher biedt Univé uitgebreide controle op webverkeer. Deze controle bestaat uit URL-filtering, inclusief een real-time reputatiesysteem voor websites en antivirus. Een andere module biedt anti-malware-ondersteuning. Door actieve contentscanning op basis van business rules voor het uitvoeren van actieve code houden we malware, spyware, trojans en andere schadelijke (malicious) code buiten het netwerk. Maar ook op andere vlakken kwam deze oplossing tegemoet aan de eisen. Nijland: “De aanleiding van deze keuze waren capaciteitsproblemen. En die hebben we nu getackeld. In de huidige situatie kunnen we een flinke groei van ons internetverkeer en de uitbreiding van het aantal eindgebruikers prima aan zonder dat we daarvoor extra systemen hoeven te plaatsen. Ook de functionaliteit is door de modulaire opbouw snel uitbreidbaar.” Ook wat betreft de garantie van de netwerkprestaties sluit de nieuwe appliance goed aan op de wensen omdat deze gebruik maakt van het zogenaamde ICAP-protocol. “Door de directe communicatie tussen beveiligingssystemen vindt het scanproces niet meer per definitie in lijn plaats. Via ICAP stuurt onze Blue Coat proxy de content direct door naar de Webwasher waardoor de processen als het ware parallel lopen. Dat scheelt dus kostbare tijd en komt de snelheid en gebruikerservaring ten goede. Daarvan profiteren de eindgebruikers.”

FUSIEPROCES

Het belang van de schaalbaarheid, uitbreidbaarheid en performance van de huidige beveiligingsomgeving is nog groter omdat Univé momenteel midden in een fusietraject zit. Binnen afzienbare termijn zal de organisatie samengaan met de fusieorganisatie VGZ-IZA-TRIAS (VIT). Deze zorgverzekeraars zijn hoofdzakelijk actief in Zuid-Nederland en vormen dus een goede aanvulling op de Univé-activiteiten die zich voornamelijk op Midden- en Noord-Nederland concentreren. Nijland zegt hierover tot slot: “Capaciteitsuitbreiding was een van de redenen om de beveiliging van de directe koppeling tussen internet en ons eigen netwerk aan te passen en aan te scherpen. Naast maximale beveiliging speelde schaalbaarheid en toekomstvastheid van de oplossing ook een belangrijke rol. En zonder nu op de zaken vooruit te willen lopen, is de inrichting van huidige netwerkbeveiliging zeker geschikt voor de nieuwe situatie met een omvangrijker netwerk.”



Dirk-Jan Nijland