

Geen virussen in Bronovo

Bronovo

Bronovo is een middelgroot algemeen ziekenhuis in Den Haag, dat landelijk bekendstaat als het ziekenhuis van het Koninklijk Huis. Het is één van de onderdelen van de Stichting Bronovo-Nebo.

Locaties

De Stichting Bronovo-Nebo bestaat uit drie onderdelen: Bronovo, Verpleeghuis Nebo (beide in Den Haag) en Gezondheidscentrum Wassenaar (in Wassenaar).

Centrale ICT-ondersteuning

De dienst Informatie- en Communicatietechnologie en Automatisering biedt ICT-ondersteuning aan de eigen bedrijfsonderdelen van de Stichting Bronovo-Nebo én aan enkele verzorgingshuizen.

Situatiebeschrijving

Zowel de administratieve als medische processen zijn afhankelijk van feilloos werkende informatiesystemen. Doeltreffende bescherming tegen spam, virussen en malware is een must.

Als er één sector is waar veiligheid boven alles gaat, is het wel de gezondheidszorg. Aangezien die zorg afhankelijk is van informatiesystemen, moeten ook die adequaat beveiligd zijn. De Haagse Stichting Bronovo-Nebo heeft die beveiliging toevertrouwd aan KPN. Met behulp van de geavanceerde systemen van MessageLabs houdt KPN spam, virussen en andere bedreigingen buiten de deur.

Verplicht

“Als zorgorganisatie zijn we verplicht om aan strenge veiligheidseisen te voldoen”, licht Willem Bron toe. Hij is beheerder infrastructuur bij Stichting Bronovo-Nebo. “NEN-norm 7510 schrijft voor dat de beschikbaarheid, integriteit en vertrouwelijkheid van alle informatie die nodig is om patiënten verantwoorde zorg te bieden, gewaarborgd moet zijn. Bovendien moeten de maatregelen voor informatiebeveiliging controleerbaar zijn. Afgezien van die formele eisen willen we natuurlijk ook koste wat kost voorkomen dat medische processen stil komen te liggen doordat een systeem met een virus besmet is. De schade zou enorm zijn, om nog maar te zwijgen van de gevolgen voor onze reputatie.”

Beveiliging in the cloud

Stichting Bronovo-Nebo gebruikt al sinds 2006 externe scan- en filterdiensten om ongewenste, en potentieel gevaarlijke, e-mail te onderscheppen en veilig internetverkeer te waarborgen. Door de steeds strengere veiligheids- en verantwoordingseisen ontstond de behoefte aan een geïntegreerd beveiligingssysteem met uitgebreide rapportagefaciliteiten en de mogelijkheid om zelf ‘aan de knoppen’ te zitten. KPN voorzag daarin met ‘Mail- en Webscan’.

Deze diensten zijn gebaseerd op die van KPN-partner MessageLabs, een bedrijf dat toonaangevend is in messaging- en web-beveiligingsdiensten. MessageLabs heeft wereldwijd twaalf onderling verbonden rekencentra, waar de computers informatie van miljarden berichten realtime combineren tot de meest uitgebreide database van internetbedreigingen ter wereld. Zodra er maar ergens in de wereld een nieuw virus opduikt, is dit dan ook direct bekend bij de gebruikers van de KPNdienstverlening. De beveiligingssoftware wordt continu geüpdatet met die informatie.

Verbinding minder belast

Omdat de beveiliging op internetsniveau – in the cloud – werkt, waren er geen aanpassingen in de software of hardware nodig. Besmette of ongewenste mail en content wordt al onderschept vóór deze het Bronovo-netwerk bereikt. De 200 servers, de 900 werkstations en de rest van de infrastructuur van Stichting Bronovo-Nebo zijn 100% beschermd tegen virussen, een unieke garantie die is vastgelegd in de service level agreement met KPN. Dat KPN zo’n garantie durft af te geven, is ook gebaseerd op de uitstekende ervaringen met de beveiliging: in de acht jaar dat KPN deze dienstverlening biedt, is er bij geen enkele van de honderden klanten een virus binnengekomen. Bijkomend voordeel van de hoogwaardige beveiliging is dat de beschikbare internetbandbreedte niet onnodig belast wordt.

Bron: “Binnenkort krijgen we sneller internet, maar tot voor kort moesten we het doen met een verbinding van slechts 10 Mbit per seconde. Wekelijks zijn er 20.000 e-mails, inkomend en uitgaand.

Zo'n 30% daarvan is spam. Nu dat al wordt afgevangen vóór het hier binnenkomt, scheelt dat behoorlijk in de belasting van de verbinding. Het is overigens erg handig dat je ook dat soort verkeerscijfers uit het systeem kunt halen."

Zelf sturen

Bron is nog om een andere reden zeer tevreden met de nieuwe beveiligingsdienst van KPN. "Wekunnen zelf veel meer sturen. Bepaalde categorieën websites blokkeren bijvoorbeeld. Eventueel zelfs op bepaalde tijden of voor bepaalde groepen medewerkers. Ook kunnen we bepaalde bestandstypen tegenhouden. Vroeger moesten we daar via de e-mail een verzoek voor indienen. Het is veel flexibeler én voordeliger om dat zelf te doen."

Ook de rapportagemogelijkheden bevalen Bronovo uitstekend. "Ik krijg automatisch wekelijks een rapportage van de mail/web-scan. Daarop kan ik zien wat er is afgevangen aan spam en virussen. Mocht er een keer een 'false positive', een e-mail die ten onrechte als spam is aangemerkt tussen zitten, dan kunnen we die ook zelf alsnog binnenhalen en eventueel de afzender als 'veilig' kenmerken. 'False positives' komen overigens zéér zelden voor. In de week-rapportages kan ik ook zien of medewerkers virussen verspreiden. Want dat kan natuurlijk ook nog, bijvoorbeeld via een van huis meegenomen usb-stick. Daarnaast gebruik ik de rapportagetool enkele keren per jaar om specifieke vragen te beantwoorden. In principe kun je ook de internetactiviteit van elke medewerker volgen. Dat doen we, en dat schrijft de regelgeving ook voor, alleen als er vermoeden van misbruik of iets dergelijks is, en dan nog alleen met toestemming van het management. Maar goed – ook deze functie kan in voorkomende gevallen uitkomst bieden."

Meer informatie

Kijk voor meer informatie over onze dienstverlening op kpn.com/corporatemarket of stuur een e-mail naar info.nl@kpn.com.

Uitdaging

Beveilig de netwerken van Stichting Bronovo-Nebo tegen internetbedreigingen zoals virussen, spam, spyware, andere ongepaste inhoud en misbruik zodat de zorg- en dienstverlening hier op geen enkele manier door kan worden belemmerd en voldaan wordt aan alle geldende veiligheidseisen.

Oplossing

KPN sluit de Stichting Bronovo-Nebo aan op de systemen van partner MessageLabs voor spamfiltering, bescherming tegen virussen, phishing, spyware, Trojan horses, wormen, andere malware en ongewenste content. Via een selfservice portal kan de stichting de beveiligingsinstellingen finetunen en rapportages op maat maken.

Meerwaarde

De Stichting Bronovo-Nebo voldoet aan alle veiligheidseisen, de administratieve en medische systemen zijn continu beschermd. Bijkomende voordelen: een minder belaste internetverbinding, opties om te sturen in het e-mail- en internetverkeer en toegang tot uitgebreide informatie over het internetgebruik in de organisatie.

Ervaring

"Tijdens een gesprek met KPN is deze oplossing aan de orde gekomen. Voor ons blijkt het ideaal. Het activeren van de dienstverlening gebeurde op afstand. Daar hoefde niemand voor langs te komen. Voor een vast bedrag per maand hebben we nu in principe nergens omkijken meer naar."
