Nadat in 2012 een hacker via een beveiligingslek kon inloggen op systemen van KPN nam het bedrijf een groot aantal extra maatregelen. Een daarvan was de aanstelling van Jaya Baloo als Chief Information Security Officer. Zij is verantwoordelijk voor de interne cyber security: de digitale veiligheid van de KPN-diensten en de bescherming van klantgegevens. *Door Daphne Riksen*

‘Voor cyber security is onderzoek van onschatbare waarde’

Jaya Baloo, Chief Information Security Officer KPN

‘Door de hack begin 2012 werd duidelijk wat er bij KPN ontbrak op het gebied van cyber security’, vertelt Baloo. ‘Om te beginnen was er onvoldoende awareness binnen de organisatie. Iedereen moet het belang snappen van informatiebeveiliging en hoe customer privacy issues hun dagelijkse werk beïnvloeden. Ook was de beveiliging niet centraal genoeg geregeld. Na de hack hebben we meer mensen in dienst genomen die zich specifiek bezig houden met de detectie van incidenten.’

‘Er bestaat geen silver bullet tegen digitale onveiligheid’

CyberLympics

Om de situatie te verbeteren nam Baloo diverse maatregelen. Er kwam een team voor cyber securitybeleid en -strategie, dat één centraal en overkoepelend beleid opstelde voor de veiligheid van de KPN-infrastructuur. ‘Er staan bijvoorbeeld gedetailleerde richtlijnen in voor network administrators, maar ook de

Global CyberLympics

eisen die KPN stelt aan software- en hardwareleveranciers', legt Baloo uit. Een ander team werkt via hacking aan proactieve detectie van kwetsbaarheden, en het Security Operations Center zoekt reactief naar patronen in informatie afkomstig van allerlei bronnen. Een andere maatregel was dat het Computer Emergency Response Team werd uitgebreid.
'Toen ik met deze baan begon, had cyber security gelukkig op hoog niveau al prioriteit. Onze CEO Eelco Blok is voorzitter van de Cyber Security Raad en dat hielp bij de interne bewustwording van de problematiek. Wat ook helpt: meedoen aan de internationale hackwedstrijd Global CyberLympics! In 2013 werd het KPN-team Europees kampioen; dit jaar zijn we door naar de finale voor het wereldkampioenschap. Daardoor is binnen de organisatie veel enthousiasme ontstaan voor cyber security.'

Duizenden aanvallen per dag

Ondanks al die maatregelen heeft het KPN-netwerk nog steeds te maken met duizenden aanvallen per dag. 'Er bestaat geen *silver bullet* tegen digitale onveiligheid', zegt Baloo. 'Je kunt niet alles voorkomen, daarvoor gaan de ontwikkelingen te snel.' Een belangrijke verbetering zou zijn als bedrijven die hard- en software aan telecombedrijven leveren al hun producten zouden voorzien van *security by design* en *privacy by design*. 'Het is voor ons als telecombedrijf onmogelijk alle apparatuur die we inkopen voortdurend te controleren. Dan zouden onze diensten onbetaalbaar worden. Er is brede marktdruk nodig om leveranciers hiertoe te dwingen, want niemand heeft hiervoor voldoende macht of inkoopkracht.' De lobby van hard- en software-leveranciers rondom de Europese Cyber Security Strategy is haar dan ook een doorn in het oog. 'Die strategie geldt voor iedereen behalve voor juist deze leveranciers. Dat is absurd.'
Baloo is een groot voorstander van open source, omdat daardoor iedereen toegang heeft tot de gebruikte protocollen, de code kan bekijken en fouten kan ontdekken die een veiligheidsprobleem veroorzaken. 'Maar helaas biedt ook open source geen garanties, zoals we dit voorjaar hebben gezien bij de Heartbleed-affaire. Niemand had dit beveiligingslek in de Open SSL-software gevonden.'

Inspiratie

De situatie in Nederland op het gebied van cyber security is positief, vindt Baloo. 'We zijn ons hier allemaal bewust van het probleem. Er is een Nationaal Cyber Security Centrum en we hebben een uitstekende Nationale Cyber Security Research Agenda, die mij veel inspiratie biedt voor programma's bij KPN. Voor cyber security is onderzoek van onschatbare waarde.' Vandaar dat KPN betrokken is bij twee projecten van het NWO-programma Cyber Security (zie kader) en daarnaast samenwerkt met de Radboud Universiteit, de TU Delft, TNO en universiteiten in de VS. Baloo: 'Een ondergeschoven kindje op onderzoeksgebied is cyber intelligence: het vergaren en analyseren van informatie over opvallend netwerkverkeer en afwijkende patronen. Daarvoor zou meer aandacht moeten komen.' Ook is er behoefte aan gebruiksvriendelijke tools, bijvoorbeeld voor encryptie van e-mails. 'Dankzij Snowden heeft het publiek de problematiek wel in het vizier, maar de oplossingen zijn niet laagdrempelig genoeg. Je oma moet ze ook kunnen gebruiken. Waarom is er zo weinig innovatie op dit gebied in Nederland en Europa?'

Blijvende inspanning

Voor een goed veiligheidsniveau is blijvende inspanning nodig van zowel de private als de publieke sector. 'Er kunnen altijd nieuwe kwetsbaarheden ontstaan, dus alleen preventie is niet voldoende. Het bedrijfsleven moet daarom ook mankracht en geld inzetten voor detectie van en adequate respons op incidenten.'
De rol van de overheid zou vooral moeten liggen op het delen van informatie en het verhogen van awareness. 'Ik ben geen voorstander van nog een toezichthouder of nog een meldplicht, omdat ik er niet van overtuigd ben dat dat leidt tot verbetering van de dienstverlening van bedrijven.' Baloo is ook niet blij met het conceptwetsvoorstel Computercriminaliteit III. 'Als dat wordt aangenomen mag de politie met een rechterlijk bevel zowel in Nederland als daarbuiten computers van verdachten hacken. Dat vind ik veel te ver gaan.' I/O

Meer informatie
KPN Privacy & Security: //corporate.kpn.com/voor-nederland/privacy-security.htm
White paper Security en privacy van KPN: //corporate.kpn.com/voor-nederland/privacy-security.htm
Global CyberLympics: //cyberlympics.org

KPN en NWO-projecten
Het NWO programma Cyber Security is gericht op de ontwikkeling van producten, diensten en kennis voor de veiligheid van de digitale samenleving. NWO heeft samen met aanvankelijk vier, en later zes ministeries twee rondes in cyber security research gefinancierd. Bij twee van deze onderzoeksprojecten is KPN is betrokken. *The personal information security assistant* (PISA), dat in de eerste financieringsronde werd geselecteerd, heeft als doel om risico's in de informatiebeveiliging te verlagen door zich te richten op eindgebruikers, met name consumenten. Voor hen wordt onder meer een toolkit ontwikkeld. *Own Your Own Identity*, een project uit de tweede ronde, betreft privacy-vriendelijke authenticatie van gebruikers op basis van attributen in plaats van hun identiteit, met behulp van de SIM-kaart in een mobiele telefoon.