

Discussie over dilemma's informatiebeveiliging

Waar trek je de grens?

Informatiebeveiliging is voor veel organisaties een weerbarstig onderwerp. Vaak is het geen 'core business', maar meestal is er wel het besef dat er risico's worden gelopen en is er dus dat knagende gevoel 'er iets mee te moeten'. Maar wat? En hoe? *Security Management* bracht twee ervaringsdeskundigen bij elkaar om over deze dilemma's te discussiëren en zocht het antwoord op de vraag waar de grens kan worden getrokken. [ARJEN DE KORT](#)

In de week dat de veiligheid van de meeste overheidswebsites even niet meer kan worden gegarandeerd, treffen *Matthijs Verburg* (directeur/eigenaar Meurs HRM) en *Hans Labruyère* (mede-eigenaar LBVD) elkaar om te discussiëren over een aantal dilemma's rond informatiebeveiliging. Niet alleen een praatje over de Diginotar-affaire zorgt ervoor dat het ijs snel breekt, het feit dat de heren elkaar sinds kort ook vanuit een leverancier (Meurs HRM) – klant (LBVD) relatie kennen is daar mede debet aan.

Open versus dicht

Meurs HRM is leverancier van een groot aantal HRM-diensten en -pro-

ducten. Informatiebeveiliging staat al een aantal jaren op de agenda en valt beleidsmatig in twee delen uiteen.

Eenzijds is er de eigen bedrijfsvoering, waarbij het intern delen van informatie wordt gestimuleerd en er sprake is van een 'open' organisatie. Anderzijds zijn er de softwareservices die het bedrijf zelf ontwikkelt en inclusief hosting aan klanten beschikbaar stelt, en waarvoor het beleid behoudender is: er wordt voldaan aan de geldende veiligheidsstandaarden en er is een streng veiligheidsbeleid met wisselende wachtwoorden, waardoor kan worden gesproken van een meer gesloten of 'dichte' organisatie.

Balans

'Als HRM-bedrijf werken we veelvuldig met gegevens van kandidaten. Dat is persoonlijke informatie, waarmee wij vertrouwelijk moeten omgaan. Die gegevens moeten dan ook goed beveiligd zijn.' Hiermee komt Verburg al direct tot de essentie als het gaat om het belang van informatiebeveiliging binnen zijn bedrijf.

Verburg stelt dat het hier 'natuurlijk niet om staatsgeheimen gaat', maar volgens Labruyère is dat niet de issue. 'Het gaat denk ik vooral om de vraag of Meurs over vijf jaar nog bestaat. En een van de dreigingen hiervoor is dat jullie niet goed op jullie informatie passen. Doe je dat niet, dan is dat namelijk de snelste manier om de tent te moeten sluiten.'

Labruyère komt meteen met een praktijkvoorbeeld van briefpapier met een bedrijfslogo dat eenvoudig door kwaadwillenden is te ontvreemden of na te maken, waarmee het bedrijf vervolgens veel schade kan worden berokkend. Verburg reageert instemmend: 'Je hebt gelijk, maar als ik op dat niveau onze beveiliging moet inrichten, dan wordt het bijna onmogelijk om op een normale manier met elkaar te werken. Natuurlijk moet je niet naïef zijn, want gelegenheid maakt de dief. Maar de ba-

Kerngegevens

Bedrijf	: Meurs HRM
Activiteit	: psychologisch advies, assessments, coaching, training
Vestigingen	: Woerden (hoofdvestiging), Zwolle. Roemenië (softwareontwikkeling)
Medewerkers	: 80
Bedrijf	: LBVD
Activiteit	: Informatiebeveiligers op het gebied van Techniek, Organisatie en Mens
Plaats	: Delft
Medewerkers	: 12



Foto: Eduard van der Worp

Matthijs Verburg (Meurs HRM): 'Onze basishouding is dat we veel vertrouwen aan elkaar geven. Dat is naar mijn idee de beste beveiliging tegen kwaadwillendheid.'

sishouding hier is dat we veel vertrouwen aan elkaar geven. Dat is naar mijn idee de beste beveiliging tegen kwaadwillendheid. Je moet dan ook een balans vinden tussen mensen prettig behandelen en beveiliging. Voor de

gaat nadenken over de vraag of hij er iets mee moet. Om dan vervolgens met droge ogen te kunnen zeggen "Nee, dat hoeft niet, want we nemen het risico". Maar het risico niet zien, het onbewust onbekwaam, dat is lastig.' En richting

gaan. Tegelijkertijd moet je op tijd de gaten dicht en zorgen dat er beveiligingsmaatregelen worden genomen. Dat ben ik helemaal met Hans eens, want het is niet zo dat alles vanzelf wel goed komt als je een bepaalde bedrijfscultuur hebt.'

'Maar hoe stevig zijn dan die beveiligingsmaatregelen? En hoe heb je die ingericht?', wil Labruyère meteen van hem weten. 'Ik denk daarbij niet aan technische maatregelen, maar ik heb het dan over een niveau hoger en de vraag of je iets moet met vertrouwelijkheid, beschikbaarheid, integriteit, bescherming van de informatie. Je zegt ja dat moeten we, maar wat moet je er mee?'

Verburg: 'Wij moeten een kandidaat kunnen vertellen dat zijn persoonlijke informatie goed beveiligd is. Dat bereken we door ons met elkaar steeds bewust te zijn van het belang van dit onderwerp en door beveiligingsmaatregelen te nemen voor het beschermen van vertrouwelijke informatie.'

Regels

In de ogen van Labruyère is dat inderdaad het juiste antwoord. Maar hij heeft weer een vervolgvraag paraat, namelijk hoe je dat dan doet? Volgens hem ontkomt je er dan namelijk niet aan om regels op te stellen, deze naar de medewerkers te communiceren, en ervoor te zorgen dat iedereen zich eraan houdt om problemen te voorkomen.

Verburg is het in principe met hem eens, maar stelt realistisch vast dat regels kunnen worden genegeerd. 'Daarom moet je vooral met elkaar delen wat je belangrijk vindt. Je kunt afspraken maken, maar het allerbelangrijkste voor mij is dat je medewerkers inzicht biedt. Dat is een belangrijker wapen dan een regel opschrijven. Daarom hebben wij hier zo min mogelijk regels.' 'In jouw ideale wereld kan dat misschien', aldus Labruyère, 'maar in de werkelijke wereld – althans de wereld die ik elke dag zie – is dat niet altijd zo. Je hebt maar één medewerker nodig die in de fout gaat ...'

'Maar helpt een regel dan wel?', reageert Verburg.

Labruyère: 'Dat is geen garantie, dat ben ik met je eens. Maar als er geen regels zijn, kun je er nauwelijks wat aan' »

'Voor de belangrijkste risico's moet je maatregelen treffen, maar het houdt een keertje op'

belangrijkste risico's moet je uiteraard maatregelen treffen, maar ergens houdt het wel een keertje op.'

Bewustzijn

Medewerkers bewust maken van de risico's die het bedrijf loopt, is een van de maatregelen die bij Meurs in dat kader worden getroffen. Verburg schetst deze aanpak: 'Wij betrekken de mensen die bij ons verantwoordelijk zijn voor de veiligheid van onze software en services er actief bij, zodat zij ook zelf de dynamiek voelen als wij een klant moeten garanderen dat de gegevens van zijn medewerkers goed beveiligd zijn.' Labruyère reageert kritisch, want in zijn ogen is dat meer de manier waarop je het doet. 'Mijn missie is dat iemand

Verburg: 'En de vraag is natuurlijk of jouw invloed zover gaat dat jouw goede wil en ook de uitvoering daarvan tot in de tweede of derde graad gaat. Want jouw mensen hebben ook allemaal weer hun netwerk. Vertrouwen is mooi, maar ...'

Hier onderbreekt Verburg hem: 'Maar je moet je geen angst laten aanpraten. Ik denk dat je dan een bedrijfscultuur creëert, waarin je elkaar niet vertrouwt. Dan kun je het pad inslaan van een extra regel en een extra vangnet, maar dat maakt het slechtste in mensen los. Dus moet je de balans bewaken tussen vertrouwen geven en mensen zinvol bezig laten zijn. Daarbij hoort ook dat je ze behandelt als volwassenen die met verantwoordelijkheden kunnen om-



Hans Labruyère (LBVD) over informatiebeveiliging: 'Wat niet hoeft, moet je vooral ook laten. Maar dat is wat anders dan helemaal niets doen.'

doen. Met regels kun je tegen zo iemand in ieder geval nog juridische stappen ondernemen.'

Alert

Voor Verburg is alertheid echter belangrijker dan regels. 'Het risico van te veel regels, voorschriften en beveiligingsmaatregelen is dat mensen lui

ging. Veel regels opstellen die vervolgens worden genegeerd, dat heeft niet veel zin.'

Op de vraag hoever hij daarin dan wil gaan, is Verburg duidelijk: 'Wat regels betreft gaat het mij alleen om de noodzakelijke. Dan heb je het over de wettelijke, en een aantal technische zodat je niet zomaar bij informatie

'Je kunt afspraken maken, maar het allerbelangrijkste is dat je medewerkers inzicht biedt'

worden. Als ze een vreemde zien lopen, denken ze dat het wel in orde zal zijn, omdat er bijvoorbeeld al zoveel controles zijn uitgevoerd. Het resultaat daarvan is dat niemand een ander nog aanspreekt. Mensen alert maken is dus misschien wel een veel krachtiger wapen dan iedereen door een detectiepoortje te laten gaan. Dat gaat wat mij betreft ook op voor informatiebeveili-

kunt komen. Maar verder wil ik vooral het inzicht van de medewerkers zo groot mogelijk hebben, zodat zij zelf kunnen beslissen welke informatie ze wel of niet delen. Ik wil daarin niet krampachtig zijn. Natuurlijk moet je kijken waar de zwakke plekken zitten en daarop je maatregelen nemen. En je moet kijken wat er in de tijd verandert, want wat vandaag veilig is, is dat

morgen niet meer. Maar het gaat mij erom niet de hele wereld dicht te timmeren met beveiligingsmaatregelen. Belangrijker is je bewust te blijven van je risico's en op basis daarvan beslissingen te nemen. Ook de beslissing om iets niet te beveiligen, als je die maar bewust neemt.'

Labruyère valt hem daarin bij. 'Wat niet hoeft, moet je vooral ook laten. Maar dat is wat anders dan helemaal niets doen. Ik vraag altijd aan mijn gesprekspartner: denk erover na, denk erover na wat je kan gebeuren, en vraag je af of je het kunt betalen als er iets misgaat. Doet hij dat, dan is mijn missie geslaagd.'

Grens

Afsluitend richt de discussie zich op de vraag wat voor een bedrijf als Meurs HRM acceptabele risico's zijn. Verburg schetst daarom maar eens zijn ideaalbeeld van informatiebeveiliging. 'Mijn ideaal is eigenlijk dat iedereen in de organisatie weet wat de meest gevoelige informatie is die we met elkaar delen - zowel mondeling, op papier, als digitaal - die goed in de beveiligingshiërarchie kan duiden, en vervolgens ook snapt waarom we met elkaar bepaalde beveiligingsmaatregelen treffen. Dan geloof ik dat we onze zaken op orde hebben en hebben we niet veel regels nodig.' En hoe erg is het dan, mochten zaken eventueel misgaan? Verburg: 'We willen informatie delen, dat is belangrijk voor ons werk. Dat gebeurt op een dermate grote schaal, dat volledig beveiligen niet kan. De vraag is dan welke informatie wij wel of niet moeten beschermen. De discussie die je dan krijgt, is dezelfde als die rond Wikileaks speelt, namelijk of het wel zo kwalijk is dat die informatie op straat ligt. Want hoe schadelijk is dat nu eigenlijk? Ik vind het leuk om deze discussie ook in ons bedrijf te voeren.'

Labruyère: 'En nu komt de dochter van Willem-Alexander en Maxima hier een test afnemen en iemand van jouw mensen lekt de resultaten. Hoe erg is dat?'

Verburg: 'Dat vind ik schadelijk. Hiermee wordt de privacy van een kandidaat geschonden, wat raakt aan de kern van onze business. Dat is van een andere orde en dat is voor mij een harde grens.'

