

motivator



Certificering is een cirkel van continue verbetering

in dit nummer o.a.

- 2 DLP beperkt risico van zwerfende informatie
- 2 Motiv benoemd tot Cisco IronPort Gold Partner
- 3 Motiv helpt Omroep West naar een multimediale toekomst
- 3 Data moet leidend zijn bij applicatieontwikkeling
- 4 Trends in Security 2010
- 4 Agenda

Motiv heeft de internationaal gerespecteerde ISO-certificeringen 9001:2008 en 27001:2005 behaald. Voor klanten geeft dit de garantie dat de dienstverlening en de informatiebeveiliging voldoet aan de strengste criteria. Door het risico-denken vanuit klantperspectief levert Motiv constante en hoogwaardige toegevoegde waarde aan haar klanten' aldus Vincent Kalkhoven, directeur operations van Motiv, 'De certificeringen maken dat meetbaar en aantoonbaar.'

Kalkhoven is vanzelfsprekend trots op de erkenning waarvoor de ISO-certificeringen staan. 'Dat danken we vooral aan al het voorwerk dat Margaret Stavast, onze manager Finance & Control, en onze corporate security officer Pim van den Hoff hebben verricht. Zij werkten hard aan het beschrijven van alle processen, het definiëren van de rollen en het formaliseren van de daarbij behorende maatregelen.' Stavast en Van den Hoff weigeren echter alle lof alleen voor zichzelf te accepteren. 'Vanzelfsprekend kregen wij dit niet voor elkaar zonder de inzet, betrokkenheid en motivatie van al onze medewerkers,' zegt Stavast. 'We waren daarom het meest verheugd met de lof in de audit van KEMA Quality voor de hoge mate van security awareness bij alle medewerkers van Motiv.'

Motiv verkreeg de ISO 9001:2008 certificering voor het kwaliteitsbeleid

van de organisatie, en de maatregelen die genomen zijn voor het verhogen van de klanttevredenheid. Het Information Security Management System (ISMS) van Motiv behaalde de ISO 27001:2005 certificering. Daarmee toont Motiv aan dat het beveiligingsmechanisme heeft geïmplementeerd die waardevolle, vertrouwelijke en bedrijfskritische gegevens beschermen. 'De certificering betekent echter niet dat we op onze lauweren mogen rusten,' zegt Kalkhoven. 'Het is een continu proces van meten en verbeteren.'

Die cirkel van continue verbetering volgt de stappen Plan, Do, Check, Act. 'Dat is de meerwaarde van het werken met ISO-standaarden,' aldus Stavast. 'Het stelt ons in staat onze kwaliteit continu te verbeteren.' Een van de belangrijkste gevolgen van deze aanpak is dat kwaliteitseisen,

risicoanalyse en informatiebeveiliging een integraal onderdeel zijn van al onze processen.'

'We beoordelen ook steeds of de maatregelen die we namen ook hebben opgeleverd wat we ervan verwachtten,' voegt Van den Hoff daar aan toe. 'Als dat niet zo is, moeten we die maatregel niet vol blijven houden, maar tijd en moeite steken in de ontwikkeling van iets wat wel werkt.' Kalkhoven: 'We leggen dat ook uit aan onze medewerkers. We geven per afdeling aan welke maatregelen we nemen om doelstellingen te halen. De afdelingen controleren vervolgens minimaal drie keer per jaar of dat naar behoren werkt. Zo ontstaat een continue evaluatie van de klanttevredenheid en van al onze doelstellingen, maatregelen en processen. Dat betekent dat we heel aandachtig omgaan met alles wat we doen. Behalen marketingcampagnes bijvoorbeeld het gewenste effect of werkt de sleutelprocedure naar behoren? Door hier al op afdelingsniveau heel bewust mee bezig te zijn, kan het management wat meer afstand nemen en krijgt het overzicht dat nodig is om proactief en tijdig bij te sturen.'

Motiv is een sterk groeiende organisatie. Hoe zorgt het bedrijf ervoor dat de processen niet steeds opnieuw vormgegeven hoeven te worden als er nieuwe functies gecreëerd moeten worden? 'We beschrijven alle processen op basis van rollen,' zegt Kalkhoven. 'Momenteel verzorgt onze inside salesafdeling bijvoorbeeld ook de inkoop, dus deze rol is nu aan hen toebedeeld. Als er op enig moment een inkoopmanager of -afdeling komt, hoeft het proces niet te veranderen, alleen gaat de rol op hen over. Met deze werkwijze kunnen we nog een aanzienlijke periode doorgroeien. Mocht het proces echter niet meer bij een bepaalde rol passen, kunnen we eenvoudigweg binnen het kwaliteitssysteem de processen en rollen aanpassen.'

Motiv is open over de lessen die geleerd zijn en de verbeteringen die daar uit voort komen. Dat geldt voor de audit, de procescontroles vanuit de afdelingen, maar ook voor ieder project dat het bedrijf afrondt. 'Wij ronden onze projecten af met een persoonlijk gesprek met de klant waarin we het project evalueren. De resultaten van dit gesprek worden meegenomen op het

projectdechargeformulier' zegt Stavast. 'Daarmee geven we openheid en eerlijkheid en klanten belonen dat met vertrouwen. Tenslotte draait het bij beveiliging altijd in de eerste plaats om vertrouwen. Onze managers houden ook tijdens de uitvoering van het project de vinger aan de pols. Niet alleen door te spreken met het management, maar juist met de mensen op de werkvloer. Alleen door gewoon vragen te stellen maken we meetbaar hoe tevreden de klant is.'

Uiteindelijk komt dat ook de ISO-certificeringen weer ten goede, stelt Van den Hoff. 'De auditors kijken ook naar deze evaluaties, dechargeformulieren en naar wat we met de terugkoppeling hebben gedaan.'

Per slot van rekening zit de auditor op de stoel van de klant. De ISO-certificering is daarom bovenal een bewijs dat Motiv bouwt aan relaties met klanten. Vertrouwen groeit door eerlijkheid over succes, maar ook over wat er beter kan. Daarom laten we onze klanten altijd weten of er iets fout ging, wat de risico's waren en hoe het opgelost is. Informeren is altijd beter dan excuseren. ●



DLP beperkt risico van zwervende informatie

Data Loss/Leakage Prevention

Data Loss of Leakage Prevention lijkt een keuze te willen maken tussen het beschermen van bedrijfskapitaal tegen diefstal of onoplettendheid. Feitelijk maakt het niet uit of gegevens met opzet of per ongeluk verloren raken. 'Het gaat erom te voorkomen dat vertrouwelijke en gevoelige bedrijfsinformatie openbaar gemaakt wordt', vertelt Bart Verhaar, security consultant bij Motiv.

'Bij een inbraak is het duidelijk dat spullen door een moedwillige onverlaat gestolen zijn. Ondanks dat u er alles aan hebt gedaan om dit te voorkomen. Maar hoe zit dat als de voordeur wagenwijd open stond? Of als de spullen op straat staan vanwege een verhuizing? Is er ook sprake van diefstal als u per ongeluk uw nieuwe tv bij het grofvuil heeft gezet, in plaats van de oude? Bij Data Loss of Leakage Prevention gaat het om dezelfde vraagstukken. Data loss betekent diefstal, bijvoorbeeld door hackers, maar ook het verliezen van gegevens op een fysieke media-drager, zoals een USB-stick. Bij data leakage is er sprake van het moedwillig of door onoplettendheid openbaar maken van bedrijfskritische gegevens. Bijvoorbeeld door een vertrouwelijk document naar het verkeerde e-mailadres te sturen. Iedere interpretatie is anders, maar de conclusie is dezelfde: gevoelige data moet worden beschermd.'

'Wat is gevoelige data? Ook dat kan op meerdere manieren worden

uitgelegd. Een klein advocatenkantoor kan relatief meer vertrouwelijke documenten bevatten dan een grote multinational. DLP is daarom een vraagstuk dat in alle lagen van het bedrijfsleven belangrijk is. En in alle functielagen binnen een organisatie. Want iedereen gebruikt informatie op zijn eigen manier. Door goed in kaart te brengen welke data beschermd moet worden, ontstaat een zekere rust. Men hoeft zich tenslotte niet meer druk te maken over alles wat er op systemen staat.'

'Als er eenmaal is vastgesteld welke gegevens gevoelig zijn, is de volgende vraag om hoeveel data dat precies gaat. Veel bedrijven investeren zwaar in allerlei beveiligingsoplossingen, terwijl misschien maar 3 tot 5 procent van de gegevens daadwerkelijk het predicaat 'gevoelig' verdient. Er zijn echter ook gradaties van gevoeligheid. Het is lastig dat allemaal te lokaliseren en te classificeren.'

'Informatie is steeds meer zwervende. Mogelijk zijn gegevens opgeslagen

in een fileshare of een database. Sommige medewerkers kopiëren ze echter ook naar de harde schijf van hun desktopcomputer. Data wordt getransporteerd over e-mail, netwerkverbindingen, op USB-sticks en laptops. Iedere implementatie van een DLP-oplossing begint daarom met het beantwoorden van deze vragen. De eerste vragen, welke informatie is gevoelig en waar bevindt zich deze, zijn een kwestie van beleid en strategie. Vanuit het thema IT in Control kan Motiv op het gebied van strategie en beleid adviseren. We kunnen ook helpen met analyses en bij het opstellen van beleidsregels rond het gebruik van gevoelige data. En erop toezien dat deze ook nageleefd worden.'

'De volgende vraag, hoe beschermen we de gevoelige data, is technisch van aard. Ook in dit geval biedt Motiv een antwoord dankzij een omvangrijk portfolio aan hoogwaardige DLP-oplossingen. We komen dit graag eens met u bespreken. Natuurlijk volledig op basis van vertrouwelijkheid.' ●

Motiv benoemd tot Cisco IronPort Gold Partner

Uitgebreide kennis van e-mail security en DLP wordt beloond met Gold status

IJsselstein, februari 2010 – Motiv is door Cisco benoemd tot Gold Partner voor IronPort. Motiv, die de oplossingen van IronPort al geruime tijd in haar portfolio heeft, ontvangt deze status dankzij haar uitgebreide en bewezen kennis van e-mail security en veilig en verantwoord internetgebruik. De appliances van IronPort bieden oplossingen voor e-mail security en secure web gateways.



Motiv Managed Security Services

Security is een vak. Motiv realiseert zich dat als geen ander. Vandaar dat wij security tot onze kernactiviteit hebben benoemd.

Met onze dienst Motiv Managed Security Services (Motiv MSS) nemen we u de zorg voor informatiebeveiliging volledig uit handen. Motiv MSS is leverbaar als standaardpakket tot het met uitgebreid maatwerk afgestemd op uw netwerkinfrastructuur en informatiebeveiligingsbeleid. En dit bieden we aan tegen een vaste prijs. Krachtig en helder.

Motiv biedt de volgende standaard oplossingen:

- MSS Beveiligde Internettoegang (Managed Firewall)
- MSS E-mail Security
- MSS Veilig Websurfen
- MSS Veilig Telewerken
- MSS Authenticatie (hardware token/sms token)
- MSS Intrusion Detection & Prevention (Managed IDP)
- MSS SIEM



Motiv school in Oeganda officieel geopend

'Opening grote happening met 1000 aanwezigen'

IJsselstein/Kakuuto, februari 2010 – Motiv heeft op maandag 15 februari de Motiv school in Oeganda officieel geopend in het bijzijn van zo'n 1000 aanwezigen. De school biedt ruimte aan 200 kinderen. Naast de opening van de school heeft Motiv een cheque overhandigd van € 15.000,- ten behoeve van maaltijden. Dit bedrag is tot stand gekomen dankzij sponsoring van zakenrelaties van Motiv.

Met dank aan de sponsors en donateurs die het voedselproject in Oeganda mogelijk hebben gemaakt:

Broere Catering, E-wine, Mr.Present Merchandising, Schouten & Nelissen Persoonlijke & organisatie-ontwikkeling, Studio Incognito buro voor de vorm, Zeekhoe Communicatie, Techaccess Value Added IT Distribution, Avnet Technology Solutions, Westcon Security, RSA, Blue Coat Systems, Check Point Software, Infoblox, Juniper Networks en Cisco IronPort, Joan-knecht Accountants, Prorisc, JOM-IT en BSN Medical.





Motiv helpt Omroep West naar een multimediale toekomst



Omroep West riep de hulp van Motiv in om de nieuwe satellietwagen te verbinden met het bedrijfsnetwerk. De samenwerking ging zo voortvarend, dat West bij toenemende innovatie op de kennis en expertise van Motiv bleef rekenen. Dankzij Motiv is Omroep West klaar voor een multimediale toekomst.

Omroep West is de publieke en regionale omroep voor het noordelijk deel van de provincie Zuid-Holland. De radio- en televisieomroep ontstond in 2002 uit een fusie van Radio West en TV West. Omdat internet een even belangrijk component is in de omroepactiviteiten als radio en televisie, werd het bedrijf in 2006 omgedoopt tot Omroep West.

Eelco de Vroom, coördinator ICT en onderhoud: 'Na de fusie werden de systemen eenvoudigweg bij elkaar gezet en onderling verbonden. Zo lang dat werkte, keek niemand er naar om. Het werd steeds lastiger om deze uitbreiding aan activiteiten te blijven ondersteunen met een inefficiënte, organisch gegroeide infrastructuur.'

Met satellietverbinding in hoger sferen

Begin 2008 werd het duidelijk dat de bestaande situatie niet kon worden gehandhaafd, vertelt De Vroom. 'We namen toen een nieuwe, geavanceerde satellietwagen in gebruik voor het televisienieuws. Deze moest gekoppeld worden aan de televisiestudio van TV West. De open netwerkverbinding vanuit de satellietwagen vroeg bovendien om een goede afscherming. We wilden natuurlijk niet dat iedereen daar zomaar bij kon. De bestaande systemen konden dat echter niet afdoende regelen.'

De Vroom zocht daarom een ICT-dienstverlener aan wie West een beveiligde verbinding tussen satellietwagen en bedrijfsnetwerk kon toevertrouwen, maar ook het beheer en onderhoud. 'Ik had in het verleden al kennis gemaakt met Motiv en zij brachten dat probleemloos voor elkaar.'

SURFnet maakt informatie toegankelijk

Het is daarom geen wonder dat Omroep West ook voor volgende, steeds grotere projecten, op Motiv rekende. Zo stapte de omroep in 2008 over op het systeem van SURFnet, een netwerkinfrastructuur voor samenwerking tussen onder meer regionale radio- en televisiezenders. Dankzij SURFnet kunnen zij multimediale bestanden, zoals hoge kwaliteit beeld en geluid, delen en uitwisselen.

'Zelfs de kleinste verbinding met SURFnet vraagt al om 1 GBps', zegt De Vroom. 'Dat konden onze firewalls niet aan. We hebben toen het advies uitgebracht om ook hiervoor de hulp van Motiv in te roepen. Naast het vertrouwen dat we in hen stelden, was het voor ons belangrijk dat Motiv al bekend was met onze uitzendingomgeving. Motiv heeft daardoor aan een half woord voldoende.'

De open samenwerkingsstructuur betekent dat SURFnet hoge eisen stelt aan authenticatie en autorisatie van

gebruikers. Beveiliging voor de diensten is een noodzakelijke randvoorwaarde. Motiv bracht daarom eerst de beveiligingsstructuur in kaart. De Vroom: 'Door verder te vragen, bracht Motiv alle kwetsbaarheden in ons netwerk naar boven.' Deze beantwoordde het bedrijf met een SSG 550 Secure Services Gateway van Juniper Networks. Deze firewall beschermt datastromen met een set van Unified Threat Management (UTM)-beveiligingsfuncties. Hiertoe behoren onder meer stateful firewall, IPSec VPN, IPS, antivirus (inclusief anti-spyware, anti-adware, anti-phishing), anti-spam en web filtering.

Een ander voordeel van de samenwerking met Motiv is dat West het beheer en onderhoud van de firewall ook uit handen kon geven. 'Wij hebben het fully managed bij Motiv ondergebracht', zegt De Vroom. 'De systemen staan bij ons op locatie, maar Motiv controleert ze op afstand vanuit haar service center. Zodra er onderhoud nodig is (vaak gaat het om preventieve maatregelen) ondernemen ze direct actie.'

West Digitaal maakt Omroep West multimediaal

Vervolgens is Omroep West in 2009 begonnen met een groot project, West Digitaal genaamd. 'Het doel hiervan is de creatie van een volledig multimediale en interactieve combinatie van radio, televisie en internet', zegt De Vroom. 'Daarvoor moesten we de hele infrastructuur voor het redactiesysteem omvormen om video- en radiomontages mogelijk te maken op iedere werkplek. Deze moesten vervolgens direct op internet gepubliceerd kunnen worden. De capaciteit van de bestaande netwerkinfrastructuur was daar echter niet toereikend voor.'

Motiv was voor Omroep West wederom de logische keuze en heeft eerst een grondige analyse gemaakt van de bestaande infrastructuur. 'Motiv implementeerde een Juniper EX 4200 ethernet-switch', zegt De Vroom. 'Dit is een betrouwbaar systeem, dat bovendien flexibel en schaalbaar is. Hierdoor kan het meegroeien met onze organisatie, zonder dat we aanvankelijk met dure overcapaciteit zitten. Ook voor deze switch geldt dat Motiv het beheer en onderhoud volledig overnam. Tenslotte had Motiv zich al bewezen als betrouwbare partner met veel kennis van zaken.'

De ethernet-switch ondersteunt de 70 redactionele werkplekken van West, en bereidt het bedrijf meteen voor op IP-telefonie door het hele pand. 'Motiv zorgt ervoor dat de veiligheid gewaarborgd is, zodat niemand van buitenaf op het netwerk kan komen. Dat is een hele prestatie, want onze netwerken moeten zo open mogelijk zijn. Tenslotte werken hier journalisten, dus we kunnen niet de toegang tot websites ontzeggen die bij veel andere bedrijven op een blacklist staan.'

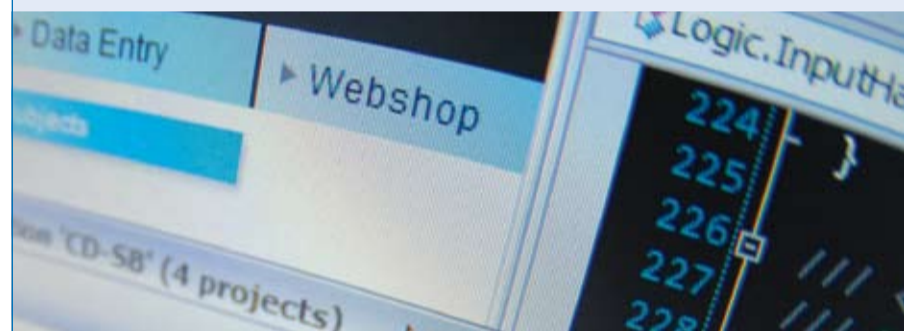
Het grootste voordeel van de samenwerking met Motiv noemt De Vroom het feit dat hij de verantwoordelijkheid op zich kan nemen voor een technische infrastructuur die hij niet zelf beheert of onderhoudt. 'Daardoor hoeven wij er niet continu tussen te zitten, maar we worden ook niet buiten gesloten.' ●

Data moet leidend zijn bij applicatieontwikkeling

Dit jaar viert Internet Explorer van Microsoft haar vijftiende verjaardag. Deze browser opende het wereldwijde web voor de massa en veranderde onze levens radicaal. Het is daarom een goed moment om eens vijftien jaar vooruit te kijken. Waar zal de evolutie van internet toe leiden? En wat betekent dit voor applicatieontwikkeling vandaag?

Browsers, zoals Netscape, Mosaic en Internet Explorer, waren feitelijk de eerste webgebaseerde applicaties. Ze maakten het surfen door, zoeken in, en bijdragen aan het prille internet voor iedereen mogelijk. De rest is, zoals dat heet, geschiedenis. Met Web 2.0 werken zelfs de grootste digibeten met de meest complexe applicaties. Overal waar men maar wil en met ieder aan internet gekoppeld apparaat. Zolang de applicaties maar gebruiksvriendelijk en intuïtief ontwikkeld zijn, kan iedereen er mee uit de voeten.

Web 3.0 staat voor internet dat niet langer een aanvulling is op computersystemen, maar dat de computer zelf is. Wat betekent dit voor applicatieontwikkeling in de komende 15 jaar? 'Iedere evolutie is een natuurlijk gevolg van de huidige situatie', zegt Rohald Boer, Business Line Manager van Motiv. 'Vooruitkijken begint daarom altijd met een terugblik. Voor applicatieontwikkeling brengt retrospectief een interessant gegeven aan het licht: applicaties werden tot nog toe gezien als fysieke gebruiksvoorwerpen. Dit komt voort uit de evolutie van techniek. Want wat is techniek anders dan alles wat je inzet om te bereiken wat je wilt, zonder dat je het van nature bezit.'



Vanaf de tijd dat we jagers-verzamelaars waren, door de agrarische en industriële revoluties, tot aan het informatietijdperk hebben we altijd gebruiksvoorwerpen uitgevonden om ons leven te vergemakkelijken. De telefoon, de auto en zelfs de eerste computers waren weliswaar revolutionair, maar op zichzelf staande apparaten. Totdat er softwareapplicaties kwamen die deze technologieën samen brachten. 'De telefoon bijvoorbeeld, heeft jarenlang weinig voortgang gemaakt, totdat begin 1990 de eerste mobieltjes kwamen', aldus Boer. 'Binnen tien jaar is de telefoon geëvolueerd tot een complete computer in je broekzak.'

Integratie en samenwerking van techniek zorgt ervoor dat applicatieontwikkeling in een enorme stroomversnelling komt. 'Dit zorgt ervoor dat niet de apparatuur, maar de data leidend wordt voor toekomstige applicaties', vertelt Corné de Keizer, Security Consultant van Motiv. 'Data is echter geen voorwerp, maar juist ongreepbaar en transparant. Daar moet het bedrijfsleven nog even aan wennen. Op korte termijn zullen vrijwel alle applicaties webgebaseerd zijn. Computerapparatuur is dan louter een manier om hier toegang tot te krijgen.'

'Dat leidt tot twee conclusies', zegt Boer. 'Als applicatieontwikkelaars krijgen we steeds meer te maken met SaaS en met databeveiliging. Motiv bereidt zichzelf en haar klanten hier nu al op voor. We zetten nu al complete applicaties in onze cybercentra, die via internet gebruikt worden. Bedrijven hoeven hierdoor de data en de applicaties, en de onderliggende systemen, niet zelf meer te beheren en te onderhouden.'

Wat databeveiliging betreft zorgt Motiv voor sterke authenticatie bij de toegang tot de gegevens, die zich 'ergens in de cloud' bevindt. De Keizer: 'De data wordt benaderd in een beschermd stuk van de cloud. Een belangrijke richtlijn daarbij is het gedachtegoed van het Jericho Forum. Dat betekent dat beveiliging verder gaat dan alleen het afschermen van data voor onbevoegden.' Ook het rubriceren, classificeren en categoriseren van data wordt daarom steeds belangrijker, voegt Boer daar aan toe. 'De enorme hoeveelheid informatie maakt het lastig om gegevens terug te vinden. Ook daarbij kijken we naar toepassingen die vandaag al gebruikt worden. Er zijn veel applicaties die nu nog op het niveau van gadget hangen, waaruit blijkt dat (geo)grafische duiding en bewerking van informatie in de toekomst belangrijk wordt. Toepassingen zoals Layar, Google Maps en de multitouch, tactiele schermen, zoals we nu al zien op de iPhone en iPad van Apple en Windows Media Surface, worden dan gemeengoed.'

Hoe zullen deze 'speeltjes' in de toekomst worden gebruikt? Boer: 'Wanneer de status en geldigheidsduur van informatie is vastgelegd zorgen deze applicaties ervoor dat ook de locatie van de informatie bekend is. Dan wordt het mogelijk gegevens (geo)grafisch te ordenen. Informatie verplaatst zich bijvoorbeeld door een bedrijf, dus is het belangrijk vast te stellen waar de verantwoordelijkheid ervoor ligt. In de toekomst zal het daarom mogelijk zijn visueel weer te geven waar informatie zich bevindt. Het kan vervolgens via een grafische interface verplaatst en bekeken worden. Als een bedrijf meerdere vestigingen heeft, wordt het mogelijk documenten en andere bestanden van de ene naar de andere vestiging te 'slepen' op het scherm. Dat past ook helemaal in de Microsofts visie op technologie. Informatie en internet worden steeds meer visueel.' ●



SMS-authenticatie: dankzij een SMSje zeker weten wie er aanklopt



Ondernemers weten inmiddels hoe belangrijk beveiliging is bij toegang op afstand tot netwerken. Het verstrekken van gebruikersnamen en wachtwoorden is niet meer afdoende. Hardware tokens versterken de beveiliging, maar zijn nog altijd erg kwetsbaar. Motivator vroeg Bart Verhaar, security consultant van Motiv naar de beste oplossing. Het antwoord is verrassend eenvoudig: een SMSje.

Bedrijven willen hun netwerken voor steeds meer mensen open zetten. Naast medewerkers wil men ook toegang verlenen aan partners, leveranciers en klanten. Daarom kiest men tegenwoordig voor extra beveiligingsmaatregelen, weet Verhaar. 'Bijvoorbeeld door naast de gebruikersnaam en het wachtwoord een extra inlogcode te vereisen. Dit kan door middel van tokens die verstrekt worden aan de gebruiker. Deze calculators maken automatisch een extra beveiligde code aan. Veel mensen kennen de tokens die banken verstrekken voor toegang tot online bankieren.'

Een token is een extra maatregel om de identiteit van de gebruiker te controleren. Dit zorgt voor sterke authenticatie, beveiliging op basis van wie de gebruiker is (gebruikersnaam), wat de gebruiker weet (wachtwoord) en wat de gebruiker heeft (token). Echter, tokens blijken erg gevoelig voor verlies of diefstal. 'Veel mensen laten het apparaat op kantoor, in een bureaula of thuis slingeren,' aldus Verhaar. 'Heeft men het onderweg vaak nodig, dan bestaat het risico dat het apparaat ergens vergeten wordt.'

Als er één apparaat is dat mensen nagenoeg nooit uit het oog verliezen, dan is het de mobiele telefoon. 'Op een congres over mobiele telefonie vroeg een spreker onlangs of iedereen zijn telefoon eens tevorschijn wilde halen,' vertelt Verhaar. 'Daarna vroeg hij de mensen om het mobieltje aan degene rechts naast hem te geven. Er ging meteen een huivering door die zaal. De mobiele telefoon is een uitbreiding van onze identiteit geworden, ons hele leven zit er vaak in. Het is daarom logisch om de veiligheid van een token te combineren met de persoonlijke bewaking van mensen voor hun mobiele telefoon.'

De oplossing voor sterke authenticatie bij toegang tot bedrijfsnetwerken op afstand is een SMSje. Verhaar: 'SMS-authenticatie is een krachtige oplossing voor tele- en thuiswerkomgevingen. Niet voor niets zien we dat SMS-authenticatie vooral in het bedrijfsleven de tokens vervangt. Bovendien is SMS-authenticatie

veel goedkoper dan hardware tokens. Dat geldt voor de licenties, maar vooral voor het beheer. Daarom zijn er ook voor de consumentenmarkt grote voordelen te behalen met SMS-authenticatie. Zo bieden veel zakelijke en financiële dienstverleners hun klanten de mogelijkheid om op een website hun klantgegevens in te zien en te wijzigen. Daarvoor is het verstrekken, beheren en onderhouden van hardware tokens echter te omslachtig, tijdrovend en duur.'

SMS-authenticatie kan direct worden geïmplementeerd, zonder dat dure apparaten ingekocht, opgeslagen en gedistribueerd moeten worden. 'Het is bovendien erg gebruiksvriendelijk,' zegt Verhaar. 'Mensen hoeven geen extra apparaat op te halen of bij zich te houden. Dit maakt SMS-authenticatie ook mogelijk voor medewerkers en klanten die slechts sporadisch toegang op afstand nodig hebben.'

Voor consumenten is SMS-authenticatie een uitkomst, waarmee een bedrijf de klanttevredenheid flink kan verhogen, vervolgt Verhaar. 'Klanten willen tegenwoordig hun eigen gegevens aan kunnen passen. Dankzij internet weet men tegenwoordig wel hoe klantsystemen werken. Ze willen dan niet langdurig in de wacht staan om een adreswijziging door te geven. Met SMS-authenticatie hoeft dat ook niet meer.'

SMS-authenticatie is typisch een dienst die bedrijven prima in de cloud af kunnen nemen. Hierdoor hoeft een bedrijf geen kosten te maken voor hardware of beheer en hebben ze er geen omkijken meer naar. Motiv biedt haar SMS-authenticatiedienst tegen een vast bedrag, per maand, per gebruiker. Maar zijn bedrijven niet huiverig om een extern bedrijf toegang te geven tot hun personeels- of klantensystemen? Verhaar: 'Onze klant behoudt de volledige verantwoordelijkheid over de administratie. Zij voegen eenvoudigweg een mobiel telefoonnummer toe aan het werknemers- of klantenbestand in hun lokale directory. Ze bepalen ook zelf de toegangsrechten voor deze gebruiker. Daarom hoeft Motiv alleen de mobiele telefoongegevens en gebruikersrechten uit te lezen. We zullen dus nooit gegevens overnemen of opslaan. Daarna kan Motiv op basis van die autorisatie SMSjes versturen met tijdelijke, extra beveiligde toegangscode. Deze zijn gebaseerd op Flash-SMS, wat betekent dat de codes niet opgeslagen worden op de mobiele telefoon. Ze verschijnen en verdwijnen automatisch.'

Vanzelfsprekend is, naast beheer en beveiliging, ook de beschikbaarheid van de dienst bij Motiv in goede handen. 'Onze systemen hiervoor zijn dubbel uitgevoerd in twee cybercentra,' aldus Verhaar. 'We hebben ook goede afspraken gemaakt met onze partner die de SMSjes verstuurt. Dit is een Nederlandse SMS-provider die directe lijnen heeft met alle Nederlandse mobiele telefontelefonieaanbieders. Uit testen blijkt dat een SMSje heel snel door deze partner geleverd wordt. Binnen 4 seconden na inloggen ontvangt de gebruiker al een SMS met inlogcode.'

Doordat Motiv veel klanten heeft die gebruik maken van de SMS-authenticatiedienst kan het bedrijf goed adviseren over licentiepakketten. Verhaar: 'Door ervaringscijfers kunnen wij goed schatten hoeveel SMSjes een klant zal gebruiken. Daarbij houden we ook rekening met het feit dat bedrijven meer werknemers en klanten zullen aansluiten op deze dienst, juist omdat het zo gebruiks- en klantvriendelijk is.' ●

Trends in Security 2010

Visies van de experts in informatiebeveiliging

Donderdag 20 mei 2010 vindt voor de derde keer het 'Trends in Security'-seminar plaats. Motiv vertelt u graag haar visie op het gebied van informatiebeveiliging. Naast het Motiv Magic quadrant nemen we u mee in het onderwerp data loss prevention en gaan wij dieper in op de beveiligingsrisico's van social media.

Programma

Het middagseminar 'Trends in Security' start om 13:00 uur.

13:00 uur Ontvangst met koffie, thee en broodjes

13:30 uur Welkom door Gerard de Weerd (sales manager)

13:45 uur Trends in Security 2010 – Bastiaan Bakker

Een kijkje in de keuken van Motiv. Welke trends zullen doorbreken in informatiebeveiliging? Welke beveiligingsmaatregelen zijn hot in 2010? Reactie van Motiv met innovaties in ons portfolio. Bastiaan zal ook het nieuwe Motiv Magic Quadrant voor security presenteren. Welke oplossingen zijn gegroeid ten opzichte van de vorige jaren? Wat is hot en waarmee kunt u beter nog even wachten?

14:30 uur Data Loss Prevention - Hype of trend (Corne de Keizer)

Data Loss Prevention of Data Leakage Prevention is zeker een hype. Er wordt veel over geschreven, er zijn veel concrete nieuwe oplossingen op het gebied van DLP. Bescherming van vertrouwelijke informatie is een logische stap in relatie tot beveiliging. Wat komt er bij kijken om interne informatie te classificeren? Kan dit projectmatig worden ingevoerd? En wat zijn de maatregelen die partijen zoals Microsoft, Cisco en RSA hebben opgenomen in het portfolio? In drie kwartier wordt u geïnformeerd over de visie en aanpak van Motiv.

15:15 uur Social media - nachtmerrie of uitkomst (Bart Verhaar)

Social media zoals YouTube, Twitter en Hyves bieden mooie kansen. Echter, deze nieuwe manier van werken past niet in het standaard beveiligingsplaatje voor internet-beveiliging. Standaard netwerk firewalls zijn niet geschikt voor beveiliging van web 2.0. Standaard security proxies worden web 2.0 klaargemaakt. Maar hoe gaat u hiermee om? Motiv geeft haar visie. Maak een gedragscode voor internet waarbij social media expliciet is opgenomen en neem maatregelen waar nodig.

16:00 uur Borrel na afloop – napraten met bezoekers en Motiv

Inschrijven

Inschrijven is kosteloos. U kunt zich inschrijven via een mail naar events@motiv.nl of via onze website www.motiv.nl. Bij een bevestiging wordt een routebeschrijving naar De Olifant in Breukelen meegestuurd.

A G E N D A

Motiv Café

De Motiv-borrels zijn inmiddels een begrip in ICT-security land. Iedere 13e van de maand bent u van harte welkom in het Motiv Café. Tijdens deze informele netwerkbijeenkomsten ontmoeten medewerkers, klanten en fabrikanten elkaar onder het genot van een drankje en een hapje. Ook de komende maanden heeft Motiv weer een aantal verrassende borrels gepland.

Woensdag 12 mei 2010

Live muziek in skybox No. Nine bij PSV

Vrijdag 11 juni 2010

Haringparty met voor de tiende keer de Big Band