

# De buitenwereld op je netwerk

Het Nieuwe Werken en Bring Your Own Device zijn ontwikkelingen waarmee steeds meer organisaties te maken krijgen. Draadloze netwerken zijn een aanjager hiervan. Een belangrijk gevolg van het toenemende gebruik van draadloze netwerken, is dat je als organisatie te maken krijgt met 'nieuwe' gebruikers. Hoe regel je dan je beveiliging? JAN BUIS \*

**D**raadloze netwerken zijn een belangrijke aanjager van Het Nieuwe Werken, zo onderstreept ook een recent onderzoek van IDC. Gedreven door productiviteitsverhoging, kostenreductie en veranderend gebruikersgedrag worden er nieuwe eisen gesteld aan hoe een bedrijf werknemers faciliteert in hun functioneren. Dit fenomeen heeft een aanzienlijke impact op de manier waarop organisaties hun informatiebeveiliging inrichten.

De inzet van draadloze netwerken zal hierin nog meer de boventoon gaan voeren. Umts/HsxPA, oftewel 3G (in de toekomst LTE) en wifi (op 2.4 GHz en 5 GHz op zowel de A- als de N-band) zijn daarbij de leidende stan-

## Het zakelijk gebruik van privé-middelen levert wel meer vrijheid op, maar is niet vrijblijvend

daarden voor spraak, data- en videoverkeer. Binnen kantooromgevingen zal wifi op basis van een wlan (*wireless local area network*) met *access points* en routers overwegend ingezet worden wat draadloze communicatie betreft. Dat heeft te maken met kosten- en praktische overwegingen. Veel moderne gebouwen hebben veel metaal in de constructie en beschikken over ramen met

UV-filters. Daardoor is het 3G-signaal binnen het pand vaak veel minder sterk. In dat opzicht volstaat het 3G-netwerk niet om in de behoefte van de mobiele werkers te voorzien. Een wifibasisstation heeft als voordeel dat het qua capaciteit vijf à tien keer zoveel aankan als een 3G-antenne.

### Gebruikersklassen

Een belangrijk gevolg van dit toenemende gebruik van draadloze netwerken binnen bedrijven is het feit dat je als organisatie te maken krijgt met 'nieuwe' gebruikers. Er zijn in bedrijfs-situaties drie, soms vier klassen gebruikers van een draadloos netwerk te onderscheiden.

De meeste zakelijke omgevingen hebben te maken met de eigen medewer-

kers, eenmalige bezoekers en frequente externe gebruikers. Daarbij valt te denken aan onderhoudsmonteurs, het schoonmaakbedrijf en externe adviseurs. Binnen zorginstellingen kan hier nog een vierde klasse aan worden toegevoegd, te weten de bewoners dan wel patiënten.

Deze verschillende gebruikersklassen vereisen dat er verschillende 'toegangs-

poorten' worden gecreëerd om te voorkomen dat een bezoeker toevallig de sleutels tot de kluis krijgt. De eigen medewerkers hebben de meeste rechten en zullen moeten worden gefaciliteerd om zo snel en efficiënt mogelijk toegang te krijgen tot de systemen, waar de beveiligingsvoorschriften dat toelaten.

### Wachtwoorden

Te vaak wordt er nog vanuit de techniek gedacht en gewerkt vanuit deels verouderde paradigma's. Een goed voorbeeld daarvan is het gebruik van wachtwoorden. Tegenwoordig kunnen op hoog niveau beveiligingscertificaten worden gebruikt om binnen de kantooromgeving toegang tot een draadloos netwerk te krijgen, waarmee automatisch een deel van de aanmeldprocedure wordt uitgevoerd.

Deze certificaten worden door de IT-afdeling op de laptop, tablet of smartphone geïnstalleerd en zorgen ervoor dat de gebruiker bij betreding van het pand binnen het draadloze netwerk geauthenticeerd wordt en toegang krijgt tot het wlan. Dat levert de gebruiker veel minder kopzorgen op dan steeds wisselende en verplicht moeilijke wachtwoorden met verschillende letters en leestekens erin.

Wachtwoorden worden in zo'n geval gebruikt voor toegang tot specifieke onderdelen van de systemen en voor applicaties. Het gebruik van een 'single sign-on' toepassing op basis van wie je



Foto: SNS Reaal

Veel bedrijven hebben inmiddels ook een beleid geformuleerd om het gebruik van privé IT-middelen toe te staan op de werkvloer.

bent, waar je bent en wat je weet, kan de inlogprocedure voor toepassingen verder vereenvoudigen zonder de data-beveiliging te compromitteren. Deze applicaties verplaatsen de wachtwoordcomplexiteit naar de achtergrond en kunnen zeer granulair de toegangsrechten helpen inregelen.

Wanneer eigen medewerkers vanaf een andere locatie toegang willen tot de bedrijfssystemen, is de meest aangewezen manier een VPN (*Virtual Private Network*). Dit concept dateert al uit de jaren negentig van de vorige eeuw en is een veilige manier om via het internet twee (netwerken van) computers met elkaar te verbinden over een internetverbinding.

Op het toestel van de gebruiker moet een VPN-client worden geïnstalleerd, die via een zogeheten tunnel contact zoekt met het bedrijfsnetwerk. Mits goed geconfigureerd is het even veilig als een 'vaste' verbinding. Naast VPN-clients voor pc's en notebooks zijn er steeds meer en betere VPN-clients beschikbaar voor smartphones en tablets.

### Beleidsregels

Van werknemers die hun eigen apparaten willen aansluiten op het bedrijfs-

netwerk, mag wel worden verwacht dat ze beseffen dat ze de organisatie tegemoetkomen op het gebied van met name veiligheid. Veel bedrijven (volgens een internationaal onderzoek van de Aberdeen Group 75 procent) hebben inmiddels ook een beleid geformuleerd om het gebruik van privé IT-middelen toe te staan op de werkvloer.

Deze beleidsregels kunnen zeer uitgebreid zijn of heel summier, maar omvatten globaal allemaal deze uitgangspunten:

- » Gebruikers ondertekenen een document voor redelijk gebruik en staan toe dat de IT-afdeling bij hun toestel kan, mocht dat nodig zijn voor ondersteuning.
- » De IT-afdeling zal dan het hierboven besproken digitale certificaat installeren om authenticatie te kunnen uitvoeren. Hiermee krijgt de gebruiker veilige toegang tot bedrijfsbronnen en kan het bedrijf de toegangspatronen van de gebruiker bijhouden. Vaak krijgt de gebruiker hiermee ook meteen toegang tot e-mail en kalenderfuncties.
- » Gebruikers stemmen ermee in om *remote wiping software* te installeren in het geval een *device* verloren raakt, gestolen wordt of wanneer de werknemer het bedrijf verlaat. In het

laatste geval is het overigens belangrijk dat de interne HR-systemen goed geïntegreerd zijn met de systemen voor *identity management*, om ervoor te zorgen dat een uitgeschreven werknemer ook direct de toegang tot het bedrijfsnetwerk ontzegd wordt.

Met een dergelijk beleid wordt het aan BOYD'ers (*bring your own device*) duidelijk gemaakt dat het zakelijk gebruik van hun privé-middelen wel meer vrijheid oplevert, maar niet vrijblijvend is.

### Buitenwereld binnen

Het Nieuwe Werken is, zoals eerder al omschreven, een *full circle* fenomeen. Nieuwe gebruikersgroepen willen voor korte of langere tijd toegang tot uw netwerk. Onder invloed van het feit dat steeds meer apparaten communiceren via het Internet Protocol (IP) zijn dat steeds vaker ook mensen die niet direct IT-gerelateerd werk doen.

Hierbij valt te denken aan technici voor klimaatsystemen of bijvoorbeeld voor hartmonitoring. Bij een storing zullen ze ter plekke op hun laptop de informatie over het systeem willen uitlezen om een diagnose te kunnen stellen dan wel te kunnen controleren of een reparatie succesvol is geweest.

De vraag hierbij is hoe deze mensen te faciliteren in hun werk. Je wilt ze immers toegang geven tot het netwerk zelf, maar niet tot bedrijfsinformatie. Het meest eenvoudig is dan je netwerk te virtualiseren, oftewel de draadloze bandbreedte te scheiden in verschillende 'kanalen' met elk hun eigen karakteristieken.

Mensen die niet beschikken over de vereiste beveiligingscertificaten, krijgen met een wachtwoord toegang tot het semivuile netwerk. Dat biedt toegang tot gefilterd internet (geen porno en malafide websites) om hun taken uit te voeren. De beveiliging van het apparaat of systeem is de verantwoording van de leverancier ervan en valt buiten het bereik van de IT-beheerders. «

\* Jan Buis, international director bij Lancom. Met dank aan Wim Bos, directeur bij Lumiad.