Het verborgen gevaar van fout geconfigureerde basisstations in een draadloos netwerk

De afgelopen jaren is door de IT-industrie veel aandacht besteed aan het gevaar van niet-geautoriseerde netwerkgebruikers en onbekende basisstations (access points) binnen een bestaand draadloos netwerk. Vele jaren zijn er besteed aan het schrijven van de benodigde autorisatiestandaarden en het opsporen van de onbekende (rogue) basisstations. Verrassend weinig aandacht is er besteed aan een meer voor de hand liggende en zeer gevaarlijke situatie; die van het fout geconfigureerde basisstation.

Jan Buis

Zoals in de inleiding is gesteld, heeft de huidige generatie van basisstations voor het gebruik binnen bedrijven en andere grote omgevingen, een dozijn aan mogelijkheden om de beveiliging te optimaliseren:

- Encryptie om de data door de lucht te beveiligen (WPA, WEP, ..);
- Open en gesloten netwerken; wel of geen netwerknaam herkenbaar in de lucht (BSSID);
- Toegang verlenen door het gebruik maken van een lijst met een product unieke code (MAC-address; ACL);
- Een authenticatie server, waar de gebruiker eerst zichzelf aanmeldt, alvorens toegelaten te worden op het netwerk (b.v.: RADIUS);
- Het scheiden van gebruikers en hun toegangsmethodieken over diverse virtuele netwerken (VLAN; meerder SSID's);
- Specifieke software die per gebruiker een beveiligde verbinding opzet (VPN);

Hoe meer gebruik wordt gemaakt van bovengenoemde mogelijkheden, des te beter zal het netwerk beveiligd zijn. Andersom zal een netwerk toegang verlenen aan niet geautoriseerde gebruikers als de bovengenoemde mogelijkheden niet worden ingezet of zelfs wegvallen, met alle gevolgen van dien.

Er hoeft maar één basisstation fout geconfigureerd te zijn en het gehele netwerk ligt open voor een ieder die maar toegang wil hebben. Een fout geconfigureerd basisstation is net zo gevaarlijk of zelfs gevaarlijker dan een bewust geplaatst onbekend basisstation welke probeert mee te luisteren. De combinatie van beide kan leiden tot het geheel blootleggen van een netwerk. Hierdoor kunnen anderen toegang tot het netwerk en de daar achterliggende servers krijgen.

Intussen is de huidige generatie van basisstations en specifieke zoekers (sniffers/probes) in staat om de bewust geplaatste meeluisterende basisstations te lokaliseren en in vele gevallen te storen of zelfs uit te schakelen. Daarentegen zal het vinden van een fout geconfigureerd basisstation in grote netwerken hetzelfde zijn als het zoeken naar een spelt in een hooiberg. Door het feit dat de basisstations een legitiem onderdeel van het bestaande draadloos netwerk zijn, zal er geen waarschuwing worden gegeven van het binnendringen van niet geautoriseerde gebruikers. Zolang het basisstation goed functioneert, zullen gebruikers maar ook netwerkbeheerders geen notie hebben van een foute configuratie. Fout geconfigureerde basisstations en slecht uitgevoerde beveiligingen kunnen met gemak weken of maanden onopgemerkt blijven.

Figuur 1: wireless access point

Het gevaar van een fout geconfigureerd basisstation is extreem groot. Uit onderzoek is gebleken dat ze veel voorkomen en dat huidige beheerorganisaties hier niet bewust van zijn, waardoor de te nemen acties niet worden genomen. Eigenlijk spelen vele organisaties gevaarlijk spel, waarbij men er automatisch van uitgaat dat alles goed is geregeld. Hoe groter het netwerk, hoe meer locaties, des te meer risico's er ontstaan.

Ontstaan

Potentiële redenen die leiden tot fout geconfigureerde basisstations zijn:

- Onduidelijke of slecht gecommuniceerde configuratierichtlijnen;
- Configuratiefouten tijdens de installatie, waarbij vele installateurs geen beveiligings-experts zijn of waarbij men zelfs geografisch gebruik maakt van verschillende installateurs;
- Menselijke fouten tijdens het oplossen van andere netwerkproblemen;
- Basisstations die in haar originele status (factory default) terugkeren tijdens een upgrade of reboot;
- Het veranderen van beveiligingsrichtlijnen die niet binnen de gehele infrastructuur worden toegepast (bijvoorbeeld van WPA naar WPA2);
- Basisstations die aan netwerken worden toegevoegd met een andere beveiligingsrichtlijn en niet automatisch opnieuw worden geconfigureerd;
- Inbrekers (hackers) die bewust beveiligingstoepassingen uitzetten om het netwerk te bereiken.

Onbeheerd is onveilig

Als een netwerk niet wordt beheerd, dan is deze per definitie niet veilig. De enige manier om de veiligheid van een draadloos netwerk met bedrijfskritische informatie te garanderen, is het implementeren van een gecentraliseerd beheerssysteem, waarbij het netwerk automatisch wordt geconfigureerd en bewaakt.

Een degelijk netwerkbeheerssysteem dient aan de volgende voorwaarden te voldoen:

- Automatische detectie van nieuwe en/of onbekende basisstations;
- Gecentraliseerd uitvoeren van beveiligingsrichtlijnen;
- Automatisch configureren van de basisstations, waar dan ook in het netwerk;

Het constant bewaken van het netwerk en direct de gevonden problemen rapporteren en daar waar toegestaan deze direct herstellen.

Automatische detectie van basisstations

De eerste stap om te voorkomen dat er fout geconfigureerde basisstations in het netwerk aanwezig zijn, is een accurate detectie van elk aanwezige basisstation, losstaande van merk of het model en de tussenin aanwezige switches en/of routers. Binnen de draadloze wereld bestaan hiervoor diverse open protocollen zoals HTTP en SNMP en de typische

merkafhankelijke protocollen als CDP, OSU of WNMP. Deze protocollen geven de mogelijkheid om automatisch het netwerk te scannen, de basisstations te lokaliseren en de gewenste configuratie te downloaden.

Gecentraliseerd uitvoeren van beveiligingsrichtlijnen

Eenmaal alle basisstations gevonden, dienen alle configuratierichtlijnen eenduidig te zijn gedefinieerd en centraal gewaarborgd, waarnaar zij constant worden toegepast over het gehele draadloze netwerk. Omdat richtlijnen centraal dienen te worden toegepast, moet men wel de flexibiliteit blijven behouden om diverse andere specifieke richtlijnen voor andere locaties te kunnen toepassen. Hierbij kan gedacht worden aan opleidingscentra versus ontwikkelingscentra.

Automatisch configureren

Als eenmaal alle richtlijnen zijn gedefinieerd, dienen deze te worden toegepast op alle basisstations van het draadloze netwerk. In een netwerk met meerdere basisstations, zal de configuratie van elk basisstation apart, veel, heel veel tijd in beslag nemen, met een grote kans op menselijke fouten. Een gecentraliseerd beheerssysteem dient deze taken automatisch uit te voeren, door elke basisstation te configureren, te rebooten (daar waar nodig) en te testen alvorens het volgende basisstation in te richten. Elke fout tijdens het uitvoeren van de configuraties dient gemeld te worden en bij kritische fouten of een constante fout dient het proces stil te worden gelegd. De fout moet eerst opgelost worden voordat er opnieuw kan worden geconfigureerd. Indien alle basisstations de juiste configuratie hebben gekregen, kan het netwerk vrij voor gebruik worden gegeven. Door het automatiseren van de gelijksoortige handelingen, zoals de configuratie per basisstation, is de kans zeer gering dat een foute configuratie wordt toegepast.

Het constant bewaken van het netwerk en direct de gevonden problemen rapporteren en daar waar toegestaan deze direct herstellen

Het zal nooit voldoende zijn om de eerst gemaakte configuratie als juiste te beschouwen. Het constant onderhouden en bewaken van de gevoerde richtlijnen is meer dan essentieel. Omdat handmatige bewaking van elk basisstation apart onhandig en zeer tijdrovend is, is een geautomatiseerd proces aanbevelenswaardig. Op het moment dat een basisstation niet meer voldoet aan de gevoerde richtlijnen, dient het beheersysteem dit te melden en, mits toegestaan, ook direct te herstellen.

Draadloze netwerken net zo veilig zijn als bedrade netwerken

Met enige regelmaat meldt de media de risico's van draadloze netwerken en demonstreert dit door middel van de zogenaamde "war-drives". Vele organisaties, waaronder de wifi-alliances, leveranciers en netwerkgebruikers, hebben diverse handleidingen op de markt gebracht waarin duidelijk wordt beschreven hoe een basisstation en een draadloos netwerk zo optimaal mogelijk beveiligd kan worden. Als gebruiker van een draadloos netwerk en al jaren actief in deze markt, ben ik er van overtuigd dat de middelen om een veilig draadloos netwerk te hebben, aanwezig zijn. Ik zou graag van deze gelegenheid gebruik willen maken om de aangegeven mogelijkheden onder de aandacht te brengen en zo veel mogelijk te implementeren en veiligheidsrichtlijnen bedrijfsbreed op te zetten. Een automatisch beheers-systeem specifiek hierop toegerust, zal het gehele proces vereenvoudigen en zekerstellen dat de toegepaste richtlijnen tijdens het gebruik worden gewaarborgd.

"Through 2006, 70% of successful WLAN attacks will occur because of misconfigured access points or client software." Gartner Group (August 2004)

Jan Buis is Director Sales & Business Development Noord-Europa van AirWave Wireless inc. jan.buis@airwave.com, www.airwave.com

Innoveren kan niet zonder toekomstvisie

Toekomstbeheersing wordt een belangrijk onderdeel van de bedrijfsvoering. Centraal in het proces staat de vertaalslag van markt- en technologische ontwikkelingen naar innovatieve en zakelijke toepassingen. Recente voorbeelden bij Ahold en Shell geven aan hoe belangrijk het is voor organisaties om ontwikkelingen tijdig in te schatten en te vertalen naar de eigen organisatie, toepassingen en competenties. Maar niet alleen bedrijven worstelen met de vertaalslag, ook de overheid slaagt er niet in om met behulp van technologische innovaties meerwaarde voor hun organisaties en voor de burger te creëren.

Drs. R. J. M. van Oirschot MBA

De centralere rol die het bedrijfsleven inneemt binnen de maatschappij brengt een aantal verantwoordelijkheden met zich mee die de organisatie als individuele entiteit overstijgen. Niet alleen de eigen aandeelhouders moeten worden tevredengesteld, ook de stakeholders hebben meerdere, verschillende belangen bij het welzijn van een organisatie. Het optimaliseren van deze complexe belangenmatrix vereist een uitvoerbare strategie waar een heldere visie aan ten grondslag ligt. Toekomstbeheersing maakt het mogelijk om innovatieve ontwikkelingen te analyseren op toegevoegde waarde voor de eigen organisatie. Het richt zich op het dichten van de kloof tussen organisatievraagstukken enerzijds en (technologische) innovaties anderzijds.

Lonely and confusing

Helaas vergt de korte termijn operatie alle aandacht van de beslissers. Toch moet de toekomst op z'n minst in beeld blijven wil de korte termijn überhaupt opportuun zijn. Maar welke toekomst is relevant? Niet iedere nieuwe ontwikkeling zal inhoudelijk invloed hebben op de organisatie. Afhankelijk van de grootte van ondernemingen, de zwaarte van de concurrentie, het type product of dienst dat in de markt gezet wordt of de fase waarin de markt zich bevindt, zal een organisatie wisselend op veranderingen (moeten) reageren. Daar komt bij dat veranderingen elkaar in een steeds sneller tempo opvolgen; managers zijn door de snelheid van veranderingen niet meer in staat goed onderbouwde beslissingen te nemen. De overweldigende hoeveelheid aan informatie, creëert bij deze groep het gevoel dat de controle over de omgeving hen uit de handen glipt. De zaken goed doen door alleen te varen op ervaring