Installatierichtlijn routers, alarmering i.v.m. Pin verkeer

VEB®

Vereniging Erkende Beveiligingsbedrijven

Inhoud

1. Inleiding

Door wijzigingen in de infrastructuur van bedrijven en particulieren krijgen erkende beveiligingsbedrijven steeds vaker te maken met voor hen (soms) nieuwe infrastructuren.
De traditionele analoge lijn, de ISDN lijn en de Digi Access verbindingen verdwijnen of zijn inmiddels al vervangen door nieuwe oplossingen, gebaseerd op netwerkaansluitingen.
Vanuit de VRKI wordt aanbevolen om, afhankelijk en behorend bij een bepaald risico, de juiste configuratie in elektronische maatregelen te gebruiken.
Daarvoor kunt u gebruik maken van de documenten:

- VRKI voor woningen februari 2015 (D03-375)
- VRKI voor bedrijven februari 2015 (D03-376)

Voor de bepaling van de juiste wijze van doormelden kunt u gebruik maken van het document:

- VRKI alarmtransmissie, samenvatting hoofdstuk 6 Definities beveiligingsmaatregelen 2014

Met een correcte risico-inventarisatie is het op basis van de NEN-EN 50136-1 eenvoudig te bepalen aan welke specifieke eisen de alarmverbinding moet voldoen.

Auteur Jan Kuipers
Voorzitter VEB

Bestuur VEB

Woerden, juli 2015

Deze installatierichtlijn is met de meeste zorg samengesteld. Ondanks dat, is het mogelijk dat er fouten zijn ingeslopen in de tekst. De auteur noch de VEB kunnen aansprakelijk worden gehouden voor eventuele fouten. Bovendien zijn bepaalde eisen uit de normen en regelgeving slechts summier weergegeven. Raadpleeg altijd de geldende regelgeving en de documentatie en de installatievoorschriften.

Hou vooral rekening met de regelmatig veranderende wet- en regelgeving!

2. Beveiliging in combinatie met ander gebruik van de router

Steeds vaker zien we dat dezelfde netwerkaansluiting ook gebruikt wordt voor andere doeleinden, waaronder VoIP, streaming video (TV), Pin en mailverkeer. Dat is het grote voordeel van een breedband netwerkverbinding. Waar een risico of probleem kan ontstaan is in de situatie waarbij verschillende gebruikers van dat netwerk specifieke instellingen vragen van de router. Dan is de kans groot dat er conflicten kunnen ontstaan die de juiste werking en/of kwaliteit van het netwerk negatief kunnen beïnvloeden. Het is dus van belang dat er duidelijke afspraken gemaakt worden waar de verantwoordelijkheid ligt van het netwerk en wie verantwoordelijk is voor het beheer ervan.

Note: Al deze verbindingen worden geregeld met de router die zich over het algemeen in de meterkast bevindt en bij grotere netwerkinstallaties ook vaak in de IT ruimte geplaatst is.

3. Configureren van de router

Om gezamenlijk van deze verbinding gebruik te kunnen maken is het van belang dat er afspraken gemaakt worden over de wijze van configureren van deze router. Op hoofdlijnen komt het er op neer dat er twee mogelijkheden zijn waar u mee te maken kunt krijgen, namelijk een gecertificeerd netwerk en een niet gecertificeerd netwerk.

3.1. Gecertificeerd netwerk

Bij een gecertificeerd netwerk is het voor de beveiligingsinstallateur of andere gebruikers meestal niet mogelijk zelf wijzigingen aan te brengen aan de configuratie van de router. Het beheer is in handen van een netwerkbeheerder en de router is deugdelijk afgeschermd met één of meerdere wachtwoorden.

Mocht er behoefte zijn aan bepaalde specifieke instellingen waaronder port-forwarding, dan is het van belang dat de aan te brengen wijzigingen tijdig bekend worden gemaakt bij degene die het netwerk beheert. Vaak is dat de lokale IT manager, soms is het een extern bedrijf die dit voor de betreffende klant verzorgt. Hoewel dit wellicht in eerste instantie als belemmerend over kan komen, is dit in de praktijk voor u als erkend installateur de meest veilige situatie. De verantwoordelijkheid van het beheer van het netwerk en de daarbij behorende instellingen ligt immers volledig bij uw opdrachtgever.

3.2. Niet gecertificeerd netwerk

Bij een niet gecertificeerd netwerk is het voor de beveiligingsinstallateur vaak mogelijk zelf wijzigingen aan te brengen aan de configuratie van de router. Dat is een onwenselijke situatie. Het is immers eenvoudig om de configuratie aan te passen zonder op de hoogte te zijn van mogelijk al belangrijke instellingen die voor andere gebruikers ingesteld staan. Een voorbeeld hiervan is de combinatie met PIN verkeer.

De verantwoordelijkheid van de juiste configuratie van de router ligt altijd bij de opdrachtgever en niet bij de beveiligingsinstallateur. U neemt dus een bepaald risico als u wijzigingen aanbrengt aan de configuratie van deze router. Daarmee heeft u de verantwoordelijkheid voor deze handelingen en kunt u aansprakelijk gesteld worden voor de eventuele gevolgen ervan. Een voorbeeld hiervan is het niet meer (of deels niet meer) functioneren van bijvoorbeeld het PIN verkeer. Dit kan grote gevolgen hebben voor de continuïteit van uw opdrachtgever en hij kan u aansprakelijk stellen voor de geleden schade.

4. Installatieadvies m.b.t aansluiten op de router

Advies is om bij niet gecertificeerde netwerken en dus ook alle overige netwerken die open zijn of met een standaard wachtwoord vergrendeld zijn (lees: fabrieksinstellingen), wijzigingen altijd uit te laten voeren door degene die de verantwoordelijkheid heeft over de router. Bent u dat niet, ga dan niet zelf aan de slag met het wijzigen van de configuratie en lever wensen m.b.t. port-forwarding op schrift aan bij de opdrachtgever en laat hem het aanbrengen van deze wijzigingen door de verantwoordelijke verzorgen.

5. Bekabeling

De bekabeling uitvoeren conform de daarvoor geldende installatierichtlijnen. Bij voorkeur gebruik maken van de standaard patch kabels die daarvoor beschikbaar zijn. Sommige fabrikanten van beveiligingsapparatuur leveren standaard deze kabel bij een nieuw systeem. Wanneer u zelf bekabeling aanlegt, zorg ervoor dat er alleen gebruik gemaakt wordt van een goed fabricaat UTP datakabel (minimaal UTP Cat5e). Bij voorkeur aan 2-zijdes afmonteren met een RJ45 jack in een data doosje en vanaf daar met een standaard patchkabel naar de actieve apparatuur. Indien er direct RJ45 plugjes aan de kabel worden geknepen gebruik dan een UTP Cat5e kabel met bijbehorende Cat5e plug of een Cat6 kabel met bijbehorende Cat6 plug. I.v.m. aderdikte zijn dit verschillende modellen pluggen. Het gebruik van een goede kwaliteit RJ45 tang is noodzakelijk en voorkomt dat de aders schuin of niet volledig in de plug worden aangeknepen. Een UTP kabel heeft standaard een massieve ader, gebruik daarom altijd RJ45 plugjes geschikt voor een massieve kern. Voor een massieve kern en soepele kern bestaan dus ook verschillende modellen pluggen en ook daarvoor geldt dat u de juiste plug gebruikt. De RJ45 plugjes of jacks aanbrengen conform de standaard kleuren codering*. Altijd de kabel testen met een daarvoor bedoeld testapparaat alvorens hij aangesloten wordt op de router en of beveiligingscentrale. Zo voorkomt u dat er problemen kunnen ontstaan op het vaak al draaiende netwerk.

*zie voorbeeld kleur codering data

6. DHCP of vast IP adres

De router deelt de private IP-adressen automatisch uit aan de computers van een lokaal netwerk. Daarvoor gebruikt de router een protocol met de naam DHCP (Dynamic Host Configuration Protocol). In de netwerkinstellingen van de computers op het netwerk stel je in dat het netwerk gebruik maakt van DHCP (on). Het is ook mogelijk om DHCP (off) in te stellen. Men dient dan de private IP adressen handmatig op betreffende randapparatuur in te stellen.

7. Port forwarding of port mapping

Port forwarding maakt het mogelijk om externe computers (bijvoorbeeld openbare machines op het internet) te verbinden met een bepaalde computer binnen het lokale netwerk (LAN). Deze worden namelijk standaard geblokkeerd door de firewall.

Om deze blokkering door de firewall op te heffen dien je handmatig de betreffende poort open te zetten en te verwijzen naar het juiste IP adres. Zorg ervoor dat deze ingesteld staat op TCP (of TCP en UDP) om eventueel problemen te voorkomen.

8. Instellingen vanuit een provider

Sommige telecom providers configureren een router en zo kunnen zij bepalen welke fysieke LAN poort van de router welke functionaliteit biedt:

Een voorbeeld hier van is:
LAN poort 1 : Klant LAN
LAN poort 2 : PIN over IP
LAN poort 3 : Alarm over IP
LAN poort 4 : Voice over IP

In dit soort situaties wordt door de provider deze informatie beschikbaar gesteld aan de klant en zo weet de installateur precies welke poort op de router hij kan gebruiken voor de alarmapparatuur. Soms gaat dit vergezeld van een kleine werkinstructie.

9. Aanbevelingen voor gebruik van de router

Algemene aanbevelingen:

- Verander niet de default configuratie voor DHCP (default on);
- Probeer vast te stellen welk deel van de IP adressen onder DHCP vallen;
- Verander niet de LAN IP-range op de gebruikers interface;
- Wees voorzichtig met port forwarding
  (geef geen toegang naar de TCP en/of UDP poorten van de PIN Betaalterminals of de Alarm terminals);
- Ga altijd in overleg met de klant over handelingen aan de router;
- Vraag de klant de handelingen zelf uit te voeren of dit te laten doen door een IT specialist;
- Neem niet zomaar de verantwoordelijkheid over, de aansprakelijkheid neem je dan ook over.

Kortom: het lijkt vanuit klantgerichtheid en een goede dienstverlening misschien vanzelfsprekend om wijzigingen aan de configuratie van de router zelf te gaan doen. Maar dat is niet zo vanzelfsprekend. Met name in die gevallen waar duidelijk is dat er meerdere diensten gebruik maken van de router is het risico groot en kunt u aansprakelijk gesteld worden voor de door u verrichte handelingen.