Een veiliger thuisnetwerk

Ton Valkenburgh

De belangrijkste component van de huidige apparatuur is de software. Die maakt o.a. aanpassingen aan nieuwe ontwikkelingen mogelijk. Op een zeker moment stopt de ondersteuning van de fabrikant. Als het apparaat met het internet verbonden moet zijn, wordt het vanaf dan een veiligheidsrisico: het thuisnetwerk wordt dan onveiliger. Hoe lossen we dat op?)

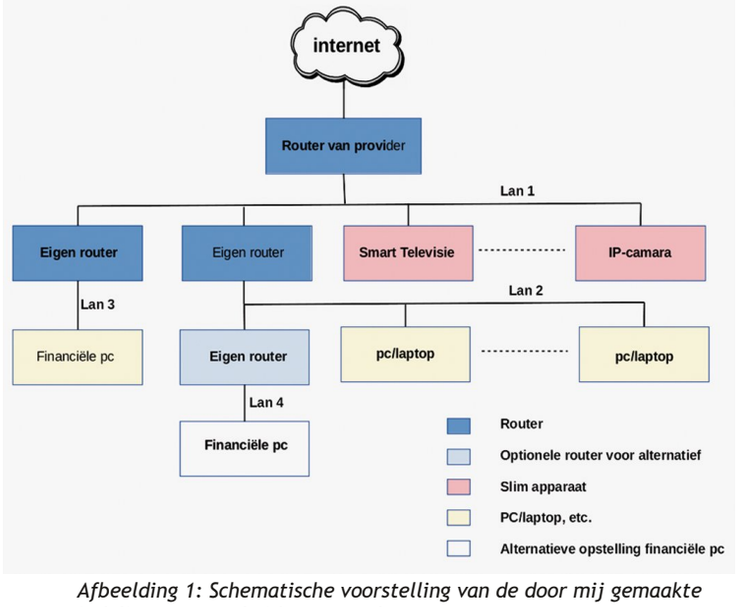
1.Inleiding

Het aantal slimme apparaten neemt hand over hand toe. Ze veroveren onze woning. Slimme televisies, telefoons, deurbellen, thermostaten, bewakingscamera's en wat er nog verder op ons afkomt. Er komt een moment dat ze niet meer door de fabrikant worden ondersteund. Dan zijn ze een potentieel gevaar voor ons thuisnetwerk. Om ze dan maar naar de milieustraat te brengen is niet erg duurzaam. Ook om na een paar jaar weer een nieuwe televisie te kopen is financieel niet aantrekkelijk. We moeten dus zorgen dat ze geen gevaar voor onze gegevens op de pc, laptop of tablet vormen.

Een aantal jaren geleden ontdekte ik dat als de router van mijn netwerkprovider een update kreeg, mijn veiligheidsinstellingen in de router niet meer functioneerden. Ik moest alle vinkjes verwijderen en weer toevoegen. Daarna werkte hij weer als vanouds. Om te voorkomen dat ik steeds moest checken of de beveiliging nog werkte zoals ik wilde heb ik een eigen router aangeschaft. Deze router heb ik achter de router van mijn provider gezet. Nu ik de updates van mijn eigen router zelf in de hand heb, kan ik rustiger slapen.

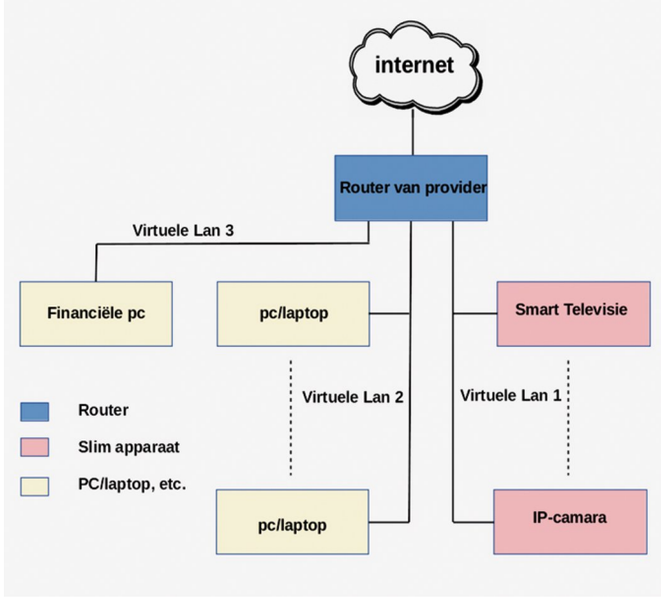
2.Gescheiden netwerken

De beste beveiliging bereik je door een fysieke scheiding. Door de extra router is dat eenvoudig te bereiken. De potentieel kwetsbare apparaten worden direct met de router van de netwerkprovider verbonden en de pc's, laptops en smart phones met actuele besturingssystemen achter de eigen router (zie afbeelding 1).



Afbeelding 1: Schematische voorstelling van de door mij gemaakte indeling met gescheiden netwerken

Ik gebruik een aparte laptop voor internetbankieren. Die heb ik ook achter een eigen router geplaatst. Om extra beveiligingsopties te hebben installeerde ik DD-WRT (link 1) in deze router. De laptop voor internetbankieren draait onder Linux. Dat reduceert de kans op malware nog verder. De financiële laptop zit met een bekabeld LAN aangesloten op de router; ik vind namelijk dat je financiële zaken niet via een wifi-verbinding moet doen. Ik geef twee mogelijke plaatsen voor de financiële pc aan. De alternatieve plaats in het netwerk zal voor de meesten van ons de enige reële optie zijn bij een bekabeld netwerk. Twee kabels naar bijvoorbeeld de zolder is meestal niet mogelijk. Bij het alternatief is een extra router niet echt nodig. Als je nog een router over hebt, kun je ook de slimme apparaten achter die extra router plaatsen. LAN 1 is de plek voor alle apparaten waarbij de beveiliging niet meer zeker is. Je kunt denken aan smarttelevisies die geen updates meer krijgen, set-up-boxen, oude tablets en beveiligingscamera's. LAN 2 gebruik je voor je pc's, laptops, netwerkprinter, netwerkscanner, Netwerk Attached Storage (NAS) en tablets, respectievelijk smartphones met een actueel besturingssysteem.



3.Virtuele LAN's

Afbeelding 2: Netwerk met virtuele LAN's

Er zijn ook routers die virtuele LAN's ondersteunen. Je heb dan geen fysieke scheiding, maar in de programmatuur van de router is ingesteld dat deze netwerkdelen elkaar niet kun-

nen zien. Dit is minder veilig dan een fysieke scheiding, want een fout in de programmatuur is gauw gemaakt. Als de router van de provider geen virtuele LAN's ondersteunt, kan er een eigen router achter de router van de provider worden geplaatst. De potentieel onveilige apparaten kunnen in dit geval dan weer direct achter de router van de provider worden geplaatst. Het wordt in dit geval een hybride netwerk.

4.Domotica en 'Internet of Things'

De apparaten voor domotica die met internet moeten worden verbonden, plaats je het liefst in LAN 2. Als echter na verloop van tijd blijkt dat er geen updates meer komen, zou je ze naar LAN 1 moeten verhuizen. De vraag is of je dat wel wilt. Het idee dat door een veiligheidslek iemand je verwarming op 30°C zou kunnen zetten is geen prettig idee. Feitelijk zou je domotica-apparaten om die reden helemaal niet met het internet moeten verbinden. Dat geldt ook voor 'Internet of Things'-apparaten. Dat is wel tegenstrijdig met de naam. Zijn dergelijke apparaten – zeker op termijn – wel veilig genoeg om met het internet te zijn verbonden? Uiteindelijk stoppen fabrikanten met updates. Vervang je ze dan door nieuwe versies?

5.Routerinstellingen

Een belangrijk aspect van netwerkbeveiliging is het instellen van de router. Omdat routers van de diverse fabrikanten nogal verschillen, is het lastig om alle belangrijke aspecten goed te duiden. Functionaliteit en terminologie verschillen erg. Ik geef daarom hier een aantal mogelijkheden. Welke je kunt gebruiken is afhankelijk van de router, maar ook van hoe ver je wilt gaan met het beveiligen. Leg in ieder geval vast welke aanpassingen je hebt gedaan. Als het later niet lukt een apparaat aan te sluiten, kan het heel goed liggen aan de goede beveiliging die je hebt gekozen.
De IP-adressen die routers standaard gebruiken is afhankelijk van fabrikant en type. Deze zijn algemeen bekend. Als je wifi gebruikt kan iedereen zien welke router je hebt en dus welke adresreeks. Dat maakt het inbreken via wifi makkelijker. Stel dus in je router een andere adresreeks in. doet dat door in de router het derde octet (*xxx.yyy.**333**.zzz*) te wijzigen en het eerste IP-adres anders te kiezen dan de standaard.
Het is verstandig om alle apparaten een vast IP-adres te geven. De meeste routers hebben een lijst van deze vaste adressen. Daarin koppel je het MAC-adres (link 2) van een apparaat aan een IP-adres. Mocht de router dit niet ondersteunen of is het aantal vaste adressen te beperkt dan stel je de 'lease time' van een IP-adres op maximaal. De apparaten kun je gewoon automatisch (DHCP link 3) hun IP-adres laten verkrijgen. Hierna stel je het maximaal aantal adressen in de router in op het totale aantal apparaten dat met die router wordt verbonden. Op deze wijze verklein je de kans dat iemand via bijvoorbeeld wifi in kan breken op jouw netwerk; alle beschikbare adressen zijn namelijk bezet.
De firewall in de router heeft een groot aantal mogelijkheden. Die zijn uiteraard niet bij iedere router het zelfde. Als algemene regel schakel je in de router de protocollen uit die je niet gebruikt. Hieronder volgt een lijst met de belangrijkste blokkades:

- WAN toegang blokkeren. Dat geldt niet alleen voor toegang tot de instellingen van je router, maar eigenlijk voor alle toegang tot je pc of thuisnetwerk.
- Port scan blokkeren. Maak je IP adres onzichtbaar op internet. Op internet draaien allerlei programma's van hackers - al dan niet met een overheidslicentie - die zoeken naar gaten bij internet hosts. Als je niet direct gezien wordt, ben je al weer een stapje veiliger.
- Veel mensen vinden het leuk om vanaf hun telefoon toegang te hebben tot hun muziekverzameling op hun pc. Dit is eigenlijk heel onverstandig. Want zo'n toegang via UPnP (link 4) is één van de bekende lekken in routers. De functie UPnP is dus een van de eerste functies die je in de firewall van je router moet uitschakelen. Tenslotte kun je net zo goed je muziekverzameling op een SD-kaartje zetten en die in je telefoon stoppen. Scheelt dataverkeer over het internet en is met de huidige geheugenkaartjes en mp3-compressie makkelijk te realiseren. Ik begrijp dat dit geen pleidooi is voor de Nexus en iPhone, maar het is absurd dat daar geen geheugenkaart in kan. Misschien om je hun muziekservice te laten gebruiken?
- ICMP berichten blokkeren. Het 'Internet Control Message Protocol' wordt gebruikt voor het beheer, maar maakt je ook zichtbaar op het internet. Dus ook dit moet je blokkeren. Je provider heeft het niet nodig; die kijkt wel in je modem/router als er problemen zijn.
- IDENT. Het aanvragen van de identiteit van de gebruiker van een verbinding. Wordt gebruikt door hackers, dus blokkeren.
- Fragmented IP Packets blokkeren. Met gefragmenteerde 'IP packets' probeert men je router over de kop te laten gaan en zo een kans creëren om in te breken. Dus blokkeren.
- 'IP Flood' of 'SYN Flood' detectie. 'SYN Flood' is een manier van Denial-Of-Service aanval. De router kan er ook fouten door gaan maken. Daarom is het verstandig om zowel 'SYN Flood' als 'IP flood' detectie te activeren. Er is echter een nadeel, want het kan netwerkvertraging geven.
- Multicast blokkeren. Met Multicast (link 5) wordt nog weinig gedaan. Dus je gebruikt het waarschijnlijk niet. Met blokkeren zul je niets missen. Sommige ISP's gebruiken multicast voor hun IP-TV service. In dit geval dus wel ingeschakeld laten.
- VPN. Als je geen 'Virtual Private Netword' (IPSec- of PPTP) functie gebruikt voor bijvoorbeeld je werk, kun je dit blokkeren. Op VPN kom ik later nog terug.

Je kunt in sommige routers nog veel meer instellen. Je kunt dan ook bijvoorbeeld filteren op IP-poort (link 6), IP-adres en MAC-adres. Bij het filteren op IP-poort blokkeer je bepaalde functies, zodat die bijvoorbeeld niet door een 'Trojaans paard' kunnen worden gebruikt. Denk aan poort 25 waarmee mail wordt verstuurd. Je gebruikt bijvoorbeeld voor je mail een beveiligde poort en blokkeert dus de onbeveiligde poort 25. Het beste is om alle poorten die je niet gebruikt te blokkeren. Dit vergt echter vaak wel wat uitzoekwerk. Met het blokkeren van MAC-adressen kun je voorkomen dat je netwerkprinter of NAS vanaf het internet kan worden benaderd.
Je wifi-verbinding moet je uiteraard goed beveiligen. De router zendt continu het signaal uit dat hij er is. Hij is dan te identificeren onder zijn 'Service Set Identifier' (SSID). Kies voor de SSID een unieke naam die geen relatie heeft met jouw naam, adres of wat dan ook. Een willekeurige cijfer- of lettercombinatie is het beste. Het uitzenden van de SSID kun je uitzetten; je bent dan minder zichtbaar in de ether. Helaas kunnen niet alle apparaten die contact met de router moeten maken dit aan. Dit vergt dus wat experimenteren met de draadloze apparaten die je gebruikt. Uiteraard gebruik je een versleutelde verbinding. Minimaal WPA2/AES. Als jouw router WPA3 ondersteunt, kies dan voor WPA2+WPA3 en 'Protected Management Frames' (PMF). Als een apparaat niet kan verbinden, schakel dan je PMF uit. De sleutel die je kiest moet lang zijn. Het liefst meer dan 24 bits. Als laatste zet je alle draadloze apparaten in de lijst van toegestane MAC-adressen.
Als de router goed functioneert maak je een back-up van de configuratie en berg je deze goed op. Dit doe je na iedere wijziging. Zet de datum in de bestandsnaam.

6.PC- en laptopinstellingen

In de pc en laptop stellen we in de firewall de volgende verdedigingslinie in. Voor Windows vind ik ZoneAlarm (link 7) een goede keuze als firewall. De Windows-firewall is on-

doorzichtiger en blokkeert standaard geen ongewenst uitgaand verkeer naar Microsoft. Voor Linux vind ik ‘Firewall Configuratie’ erg toegankelijk. In principe laat je geen enkel verkeer naar de pc toe. Soms zal dat toch nodig zijn. Zo ontdekte ik dat mijn netwerkscanner alleen werkte als ik hem toegang gaf tot mijn pc. Soms heb je het nodig om bestanden over te zetten van een pc/laptop van of naar een tablet/telefoon. Kies er dan voor om alleen dat specifieke IP-adres toegang te geven. Hier blijkt gelijk het voordeel van die vaste IP-adressen.

7.Toegang vanaf internet

Sommigen willen misschien toegang tot hun netwerk vanaf het internet. Ik raad dat altijd af. We zien dat zelfs ‘professionele’ netwerkbeheerders moeite hebben om hun netwerk inbraakvrij te houden. Waarom zou jij dat beter kunnen? Als je het echt wilt, moet je alleen toegang via een VPN toestaan. Laat in ieder geval geen internettoegang tot de instellingen van jouw router toe. In sommige routers kun je instellen welk IP-adres toegang heeft tot de beheerfunctie van de router. Zo kun je regelen dat alleen de beheerders-pc toegang heeft tot die essentiële functie.

Twee routers achter elkaar maakt het lastig om toegang vanaf internet te regelen. Je kunt dan het best kiezen voor het netwerk met virtuele LAN’s. Mocht de router van je provider geen virtuele LAN’s ondersteunen, dan moet je een eigen router inzetten. De router van de provider laat je in ‘bridge mode’ zetten.

8.Nawoord

Ik heb een aantal oplossingen aangereikt om je thuisnetwerk veiliger te maken. Hopelijk helpt het je om te overwegen welke ideeën relevant zijn in jouw situatie. Als je ze allemaal toepast ben je echter nog steeds niet 100% veilig. Het gevaar loert ook nog uit andere hoeken. Denk maar aan bijvoorbeeld Phishing. Technische oplossingen alleen zijn niet genoeg. De zwakste schakel blijkt toch meestal iiizelf. Soms door het ne-

Links

1. https://dd-wrt.com/
2. https://nl.wikipedia.org/wiki/MAC-adres
3. https://nl.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol
4. https://www.security.nl/posting/39877/
5. https://nl.wikipedia.org/wiki/Multicast
6. https://nl.wikipedia.org/wiki/TCP-_en_UDP-poorten
7. https://www.zonealarm.com/