Nationaal Cyber Security Centrum
Ministerie van Veiligheid en Justitie

Beveilig apparaten gekoppeld aan internet

Factsheet FS-2012-07

versie 1.1 | 17 december 2012

Steeds meer verschillende apparaten worden aan een thuis- of kantoornetwerk gekoppeld. Door onjuiste configuratie ontstaat het risico dat deze apparaten direct vanaf internet te benaderen zijn. Kwaadwillenden kunnen zo de informatie die is opgeslagen in deze apparaten opvragen of veranderen. Ook is het apparaat, afhankelijk van het type, mogelijk op afstand te bedienen.

In dit factsheet wordt de problematiek toegelicht en worden mogelijke consequenties geschetst. Ook wordt uitgelegd wat u kunt doen om vast te stellen of uw apparaten kwetsbaar zijn voor misbruik vanaf het internet en worden concrete stappen beschreven waarmee u eventuele kwetsbaarheden weg kunt nemen. Dit factsheet richt zich tot de technisch redelijk bekwame lezer. Vraag een ervaren gebruiker om hulp wanneer u moeite heeft om de adviezen op te volgen.

Achtergrond

Steeds meer apparaten zijn voorzien van een vaste of draadloze netwerkaansluiting. Dit biedt de mogelijkheid om het apparaat te verbinden met een computernetwerk. Netwerkprinters, scanners, webcams, apparatuur voor netwerkopslag (NAS), televisies en apparatuur voor huisautomatisering (zoals thermostaten en verlichting) worden aan het thuis- of kantoornetwerk gekoppeld. Vaak worden in deze apparaten gegevens opgeslagen die vervolgens via het netwerk beschikbaar zijn. Ook kan de apparatuur via het netwerk verbinding maken met het internet. Zo kunt u bijvoorbeeld met uw televisie op het internet surfen.

Deze apparaten vereisen adequate beveiligingsmaatregelen, net als de computers in uw netwerk. Om uiteenlopende redenen is het niet altijd mogelijk om de maatregelen die u treft voor uw computer ook toe te passen op deze apparaten. Zo kunt u uw televisie niet van antivirussoftware voorzien omdat deze geen mogelijkheid heeft om zelf deze software te installeren. Uw thermostaat biedt vermoedelijk geen mogelijkheid om de toegang op afstand te beveiligen met een wachtwoord en het is vaak niet eenvoudig om updates voor de (besturings)software van deze apparaten te installeren, als u er al achter komt dat er een update beschikbaar is.

Probleemstelling

Omdat het maar beperkt mogelijk is om deze apparaten te beveiligen, is het voor kwaadwillenden relatief eenvoudig om zich toegang te verschaffen tot opgeslagen informatie

De belangrijkste feiten:

- Mogelijk zijn er, naast computers, ook andere apparaten met uw netwerk verbonden, zoals printers, scanners, televisies, webcams en apparatuur voor netwerkopslag (NAS).
- Het blijkt dat dergelijke apparatuur in een aantal gevallen vanaf internet bereikbaar is.
- Deze apparatuur moet, net als computers, afdoende beveiligd worden tegen misbruik door kwaadwillenden.
- Wij raden u aan om ervoor te zorgen dat deze apparatuur niet vanaf het internet bereikbaar is.
- Indien bereikbaarheid van apparaten vanaf internet noodzakelijk voor u is, tref dan afdoende maatregelen om deze toegang te beveiligen.

en de functionaliteit van het apparaat; de aard van het apparaat bepaalt wat de mogelijke consequenties zijn:

- **Printer.**
  Een kwaadwillende kan printopdrachten sturen naar de printer of de documenten lezen die door anderen naar de printer worden gestuurd. Soms zijn documenten die eerder zijn geprint nog te achterhalen. Als de printer een webinterface heeft, kan ook deze kwetsbaarheden bevatten die kunnen worden uitgebuit.
- **Scanner.**
  Een kwaadwillende kan meelezen met documenten die gescand worden. Moderne netwerkscanners bevatten interne opslag van gescande documenten. Ook deze opgeslagen documenten kunnen voor een kwaadwillende toegankelijk zijn. Als de scanner een webinterface heeft, gelden dezelfde risico's als bij webinterfaces van printers.
- **Webcam.**
  Een kwaadwillende kan meekijken met het zichtbare beeld van de webcam, ook als u de webcam niet zelf gebruikt. Als de webcam ook een microfoon heeft, kan een kwaadwillende meeluisteren met de omgeving.
- **Netwerkopslag/NAS.**
  Een kwaadwillende kan alle opgeslagen bestanden zoals documenten en foto's inzien, veranderen of verwijderen. Ook kan de kwaadwillende zelf bestanden toevoegen die, als u ze opent, uw computer infecteren met malware.
- **Televisie.**
  Een kwaadwillende kan uw televisie met malware infecteren waardoor de gegevens die u in de browser invoert, afgeluisterd of gemanipuleerd kunnen worden. Dit is vooral relevant als u deze browser gebruikt voor gevoelige toepassingen als internetbankieren of als u betaalde diensten afneemt via interactieve televisie. Ook kan uw televisie zo onderdeel worden van een botnet.
- **Thermostaat/huisautomatisering.**
  Een kwaadwillende kan deze apparaten op afstand bedienen. Hierdoor kan hij, afhankelijk van het type apparaat, bijvoorbeeld de temperatuur in huis aanpassen, de beveiligingsinstallatie in- en uitschakelen of de garagedeur openen en sluiten.
- **Andere apparaten.**
  Ook andere type apparaten zoals spelcomputers kunnen met uw netwerk verbonden worden. Het is te verwachten dat er in de toekomst nog meer apparaten verbonden worden met een computernetwerk.

Om bovengenoemde risico's te beperken is het nodig om de toegang tot het betreffende apparaat zo beperkt mogelijk te houden. Dit betekent dat deze apparaten niet bereikbaar moeten zijn vanaf het internet. Ook als het apparaat enige mogelijkheid tot toegangsbeveiliging biedt, zoals beveiliging met een gebruikersnaam en wachtwoord, dan nog kan het apparaat kwetsbaarheden bevatten die het ongeschikt maken voor directe bereikbaarheid vanaf het internet.

Is het noodzakelijk dat bepaalde apparaten toch via het internet bereikbaar zijn? Tref dan aanvullende maatregelen ter beveiliging van deze apparaten.

Ben ik kwetsbaar?

Door onderstaande stappen te zetten kunt u zelf bepalen of apparaten die verbonden zijn met uw netwerk mogelijk ook vanaf het internet bereikbaar zijn.

1. inventariseer welke apparaten verbonden zijn met uw netwerk;
2. bepaal of deze apparaten via het internet bereikbaar zijn.

SHODAN

Kwaadwillenden die online bereikbare apparatuur zoeken, scannen het internet om verbonden apparaten te vinden. Het vereist enige technische kennis om dit werk uit te voeren. De zoekmachine SHODAN (shodanhq.com) vergemakkelijkt dit zoekwerk door bereikbare apparatuur doorzoekbaar te maken. Gevorderde gebruikers kunnen SHODAN ook zelf gebruiken om na te gaan of op hun externe IP-adres apparatuur via het internet bereikbaar is.

Inventariseren van verbonden apparaten
Loop door uw huis of kantoorgebouw en noteer alle apparaten die (mogelijk) met het netwerk zijn verbonden. Denk ook aan apparaten die draadloos met het netwerk zijn verbonden. De eerdergenoemde opsomming van typen apparaten vormt hierbij een leidraad. Twijfelt u of een apparaat draadloos met het netwerk verbonden is, raadpleeg dan de logbestanden of het statusscherm van uw router of ander netwerkapparaat. Het apparaat zou hierin terug te vinden moeten zijn.

Bepalen van bereikbaarheid vanaf internet
Controleer of de toegang tot apparaten op uw netwerk vanaf internet is afgeschermd. De eenvoudigste manier om deze afscherming te bereiken is door middel van een firewall. Een firewall zorgt er, mits juist ingesteld, voor dat alleen gewenst verkeer vanaf het internet wordt toegelaten tot uw netwerk. De internetrouter van uw internetprovider bevat vaak een firewall. In de configuratie van deze router kunt u nagaan of de firewall is ingeschakeld.

Sommige routers bieden verbonden apparaten de mogelijkheid om zichzelf vanaf het internet bereikbaar te maken met behulp van het Universal Plug & Play-protocol (UPnP, ook bekend als DLNA). Met dit protocol kan uw computer zichzelf bereikbaar maken op het internet om bijvoorbeeld bestanden uit te wisselen. Als echter andere apparaten ook dit protocol gebruiken, zijn ook deze apparaten mogelijk via internet bereikbaar. Een apparaat kan zichzelf alleen met UPnP vanaf het internet bereikbaar maken als UPnP op de internetrouter ingeschakeld is. U kunt in de configuratie van uw router of in de handleiding van het verbonden apparaat vinden of gebruik wordt gemaakt van UPnP.

Wat kan ik doen?

Bij het beveiligen van apparaten tegen aanvallen vanaf internet raden wij u aan om de toegang vanaf het internet alleen toe te staan als deze voor u noodzakelijk is. Staat u toegang vanaf internet toe, tref dan aanvullende maatregelen ter beveiliging. Daarnaast kunt u voorkomen dat gevoelige informatie via het internet bereikbaar is door deze eenvoudigweg niet op uw netwerkopslag op te slaan.

Maatregelen om toegang vanaf internet te voorkomen

- Configureer de firewall in uw internetrouter zo dat deze geen verbindingen toelaat vanaf het internet. Raadpleeg de handleiding van uw router voor instructies.
- Schakel UPnP uit op alle apparaten die met het netwerk verbonden zijn en die niet bereikbaar moeten zijn vanaf het internet. Deze functionaliteit kan ook onder andere namen zoals Personal Cloud of Media Server in de configuratie van een apparaat voorkomen. Raadpleeg de handleiding van het desbetreffende apparaat voor instructies.
- Overweeg om UPnP op uw router uit te schakelen (let op: dit kan problemen opleveren bij sommige toepassingen, bijvoorbeeld voor het uitwisselen van bestanden). Raadpleeg de handleiding van uw router voor instructies.[1]
- Schakel met het netwerk verbonden apparaten uit als u ze niet gebruikt.

Maatregelen om netwerktoegang te beveiligen

- Apparatuur wordt vaak geleverd met standaardinstellingen. Die standaard-instellingen zijn gericht op een brede groep gebruikers en voldoen niet om het apparaat afdoende te beveiligen. Apparatuur die u in de winkel koopt, moet u daarom altijd instellen volgens de gebruikershandleiding. Koopt u apparatuur tweedehands, dan geldt dit nog sterker, omdat u niet weet in welke opstelling deze door de vorige eigenaar is gebruikt.
- Stel toegangsbeveiliging met een gebruikersnaam en sterk wachtwoord in op alle met het netwerk verbonden apparaten die dit ondersteunen.
- Maak gebruik van versleutelde verbindingen voor uw communicatie met deze apparaten. Stel hiervoor in dat uw apparaat gebruikmaakt van HTTPS, of maak het alleen bereikbaar via een virtual private network (VPN) met uw router. Als uw apparaat dit ondersteunt, vindt u instructies in de handleiding.
- Installeer beschikbare beveiligingsupdates voor de besturingssoftware (firmware) van

[1] Om te voorkomen dat een apparaat bereikbaar is vanaf internet, moet UPnP uitgeschakeld zijn op het apparaat en/of op de router. Als UPnP op beide is ingeschakeld, is het apparaat mogelijk vanaf het internet bereikbaar.

het apparaat. U kunt achterhalen of er updates zijn voor uw apparaten op de websites van de leveranciers. Sommige apparaten kunnen ook zelfstandig updates downloaden en installeren. Instructies voor installatie vindt u in de handleiding.

> Raadpleeg de handleiding van uw apparaten om na te gaan of er meer beveiligingsmaatregelen beschikbaar zijn.

Tot slot

Is er informatie van u op het internet gelekt, ondanks maatregelen die u hebt getroffen? In het factsheet 'Help, mijn gegevens zijn op internet gelekt' vindt u stappen die u kunt nemen als u dit is overkomen.

In de toekomst zullen steeds meer apparaten in uw huis of kantoor met het netwerk verbonden zijn. Dit betekent dat u zich bewust moet zijn van de bijbehorende risico's. Vaak kunnen deze relatief eenvoudig worden weggenomen door toegang vanaf internet onmogelijk te maken of enkele extra maatregelen te treffen.
Met bovenstaande informatie kunt u een inschatting maken van de risico's en bepaalt u maatregelen die u kunt treffen om veilig met deze toegenomen verbondenheid van uw apparatuur om te gaan.

Handelingsperspectief

1. Bepaal welke apparaten zoals printers, scanners, webcams, televisies en netwerkopslag (NAS) met uw netwerk verbonden zijn.
2. Stel de firewall van uw internetrouter zo in dat deze apparaten niet bereikbaar zijn vanaf internet.
3. Schakel UPnP (of DLNA) uit op deze apparaten.
4. Stel toegangsbeveiliging met een gebruikersnaam en wachtwoord in op deze apparaten.
5. Gebruik, waar mogelijk, versleutelde verbindingen zoals HTTPS om met deze apparaten te communiceren.
6. Bezoek regelmatig de website van de leverancier om na te gaan of er updates voor de (besturings)software (firmware) van de apparaten zijn. Installeer firmware-updates als deze beschikbaar zijn.
7. Stel eventuele andere beschikbare beveiligingsmaatregelen op deze apparaten in. Raadpleeg de handleiding voor een overzicht.