Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Basis-beveiligingsmaatregelen slimme apparaten (IoT)

Factsheet FS-2012-07 | versie 1.2 | herzien mei 2023

We gebruiken steeds meer slimme apparaten, zoals televiesies, webcams en apparatuur voor huis- en kantoorautomatisering (zoals thermostaten en verlichting). Deze apparaten – ook wel Internet of Things (IoT) genoemd – worden doorgaans aan een thuis- of kantoornetwerk en het internet gekoppeld om 'slimme' functionaliteiten te bieden. Door onjuiste configuratie, inadequaate veiligheidsmaatregelen en kwetsbaarheden in de hard- of software ontstaat het risico dat deze apparaten direct vanaf het internet te benaderen zijn door ongeautoriseerde personen. Kwaadwillenden kunnen hiermee het apparaat van afstand bedienen, informatie stelen of toegang krijgen tot het thuis- of kantoornetwerk. 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.

Doelgroep

Dit factsheet richt zich op thuiswerkers en kleinere organisaties. Het bevat tastbare voorbeelden en handelingsperspectieven die gebruikers met een beperkte achtergrond in digitale beveiliging uit kunnen voeren.

Samenwerkingspartners

Dit factsheet is mede tot stand gekomen door de bijdragen van het Digital Trust Center (DTC) en de Rijksinspectie Digitale Infrastructuur (RDI).

De belangrijkste feiten

Mogelijk zijn er, naast computers, ook andere smart-apparaten met uw netwerk verbonden, zoals printers, scanners, webcams of televisies. Dergelijke apparatuur wordt steeds vaker ontworpen om verbonden te zijn met het internet. Mogelijk zijn deze apparaten niet voldoende beveiligd.

Onvoldoende beveiliging kan risico's opleveren voor uw bedrijfsvoering. Bekijk daarom of u de connectiviteit nodig heeft voor uw bedrijfsvoering en besef dat elke vorm van connectiviteit een risico oplevert.

Ga in eerste instantie na of connectiviteit noodzakelijk is voor het functioneren van het apparaat. Indien connectiviteit van apparaten vanaf internet noodzakelijk is, tref dan afdoende maatregelen om deze toegang te beveiligen. Als de connectiviteit niet nodig is kunt u er het beste voor zorgen dat het apparaat geen verbinding maakt met het internet.

Probleemstelling

Slimme apparaten zijn in een korte tijd razend populair geworden. Veel producenten verleiden consumenten met slimme apparaten die nieuwe functionaliteiten toe voegen (in vergelijking met hun 'domme' voorgangers). Denk hierbij aan het bedienen van uw verlichting van afstand met uw telefoon. Beveiliging wordt niet altijd voldoende meegenomen bij de ontwikkeling van slimme apparaten. Zo kunnen basale beveiligingsmaatregelen ontbreken en kunnen slimme apparaten kwetsbaar zijn voor digitale aanvallen.

Omdat slimme apparaten doorgaans minder goed (te) beveiligen zijn, vormen ze voor kwaadwillenden een interessant doelwit. Doelwitten worden onder andere gevonden door online zoekmachines, zoals SHODAN, die zich richten op het identificeren van (slecht geconfigureerde) apparaten. Door toegang te krijgen tot het apparaat kan een kwaadwillende beschikking krijgen over de informatie die is opgeslagen op het apparaat. Ook kan deze hiermee de functionaliteit van het apparaat misbruiken. De aard van het apparaat bepaalt wat de mogelijke consequenties zijn. Zo zou een kwaadwillende via de scanner documenten kunnen inzien, of kantoorautomatiseringsapparaten zoals thermostaten of verlichting aan of uit kunnen zetten.

Als smart apparaten zoals lampen, koelkasten, omvormers en televisies gekoppeld zijn aan het thuis- of bedrijfsnetwerk kunnen deze apparaten gebruikt worden om het achterliggende netwerk te bereiken. In dit geval dienen deze apparaten als *stepping-stone* die een kwaadwillende actor kan gebruiken om het netwerk in te komen. De dreiging van kwetsbare slimme apparaten is dus niet alleen een probleem voor het desbetreffende apparaat zelf, maar ook voor het achterliggende netwerk. Daarnaast kunnen geïnfecteerde apparaten gebruikt worden als onderdeel van een IoT-botnet om andere netwerken aan te vallen (e.g. een DDoS aanval).

Een eigenschap van slimme appraten is dat ze makkelijk in te brengen zijn in het bestaande netwerk. Denk bijvoorbeeld aan een WiFi accesspoint dat iemand nog thuis had liggen om het bereik in de vergaderruimte te vergroten of een internetradio voor op de werkvloer. Deze apparaten worden in dergelijke gevallen vaak in gebruik genomen zonder na te denken over de bijbehorende cyberrisico's, met als gevolg dat er geen passende beveiligingsmaatregelen worden genomen.

Om bovengenoemde risico's te beperken is het nodig om de toegang tot het betreffende apparaat zo beperkt mogelijk te houden. Is het

noodzakelijk dat bepaalde apparaten toch via het internet en/of netwerk bereikbaar zijn? Tref dan aanvullende beveiligingsmaatregelen.

Ben ik kwetsbaar?

Door onderstaande stappen te zetten kunt u zelf bepalen hoe kwetsbaar u bent voor digitale aanvallen via slimme apparaten.

1. Inventariseer welke slimme apparaten u heeft;
2. Bepaal of deze apparaten verbonden zijn met het internet en/of uw netwerk.

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. Raadpleeg de website veiliginternetten.nl[1] voor hulp bij het inventariseren van uw slimme apparaten.

Bepalen of uw apparaten verbonden zijn met het internet en/of uw netwerk.

Om te bepalen welke apparaten (draadloos) met uw netwerk of het internet verbonden zijn, kunt u het statusscherm en de logbestanden van uw router of ander netwerkapparaat raadplegen. Het apparaat zou hierin terug te vinden moeten zijn. Controleer hierbij ook of de toegang tot deze apparaten 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. Het modem van uw internetprovider bevat vaak een firewall. In de configuratie hiervan kunt u nagaan of de firewall is ingeschakeld.

Wat kan ik doen?

Het is belangrijk dat u zich bewust bent dat elk (slim) apparaat in uw netwerk een mogelijke ingang voor een kwaadwillende persoon vormt. Bij het beveiligen van apparaten raden wij u aan om de toegang vanaf het internet alleen toe te staan als dit noodzakelijk is. Staat u toegang vanaf internet toe, tref dan aanvullende maatregelen ter beveiliging.

Krijg en houd grip op uw slimme apparaten

1. Controleer voordat u een bepaald apparaat aanschaft of het desbetreffende apparaat of merk last heeft van kwetsbaarheden op uitgebrachte apparaten. Dit geeft u een inzicht in de beveiligingswaarde die u kan verwachten van het apparaat. Daarnaast is het van belang om inzichtelijk te hebben hoe lang een product nog ondersteund blijft door de producent voordat u het desbetreffende product aanschaft. Zo voorkomt u het risico om een product aan te schaffen dat bijna End of Life is en dus niet lang meer ondersteund zal blijven.

2. Zorg ervoor dat u een up-to-date inventaris heeft van uw slimme apparaten. Zijn er apparaten in uw netwerk waar u geen weet van had? Zorg ervoor dat u beheer voert over deze apparaten en passende maatregelen treft.

Beheer de netwerktoegang tot uw slimme apparaten

1. Configureer de firewall in uw internetrouter zodat deze geen verbindingen toelaat vanaf het internet die niet door u geïnitieerd zijn. Raadpleeg de handleiding van uw router voor instructies.
2. Schakel UPnP uit in de modem/router. UPnP maakt het mogelijk om uw apparaten eenvoudig te verbinden (zonder configuratie), maar het is belangrijk om na te denken of dit

[1] Doe je updates (veiliginternetten.nl)

gewenst is. 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.

3. 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.
4. Segmenteer uw slimme apparaten van de rest van uw netwerk. Een eenvoudige manier om dit te doen is om uw slimme apparaten enkel toegang te geven tot uw gastennetwerk. De meeste modems / routers hebben een mogelijkheid om een dergelijk netwerk eenvoudig aan te leggen.

Configureer en beheer uw slimme apparaten.

1. Apparatuur wordt vaak geleverd met standaardinstellingen, zoals standaardwachtwoorden. Deze 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.
2. Stel tweefactorauthenticatie in voor toegangsbeveiliging op alle met het netwerk verbonden apparaten die dit ondersteunen.
3. Installeer beschikbare beveiligingsupdates voor de besturingssoftware van het apparaat. U kunt achterhalen of er updates zijn voor uw apparaten op de websites van de leveranciers. Sommige apparaten kunnen ook zelfstandig automatisch updates downloaden en installeren. Is dit het geval dan is het advies deze updates te installeren. Instructies voor installatie vindt u in de handleiding.
4. Raadpleeg de handleiding van uw apparaten om na te gaan of er meer beveiligingsmaatregelen beschikbaar zijn en pas deze toe.
5. Evalueer periodiek of uw verbonden apparaten correct geconfigureerd zijn en de laatste updates hebben verwerkt. Controleer daarbij periodiek of uw apparaat nog actief wordt ondersteund door de producent.

Tot slot

Heeft u behoefte om meer te weten te komen over het beveiligen van uw netwerk en apparaten? Raadpleeg dan de basismaatregelen van het NCSC. Wilt u meer weten over IoT? Bezoek dan de website van het Digital Trust Center[2] voor aanvullende informatie.

[2] Beveiligingstips voor Internet of Things (IoT) | Digital Trust Center (Min. van EZK)