socured
TAKING CARE

Het dreigingslandschap voor OT en het IoT

Het dreigingslandschap voor OT en het IoT

Succesvolle oplossingen zijn tegenwoordig vaak afhankelijk van het combineren van veel onderdelen, waaronder hardware, software en clouddiensten, vaak in een IoT-oplossing. Het IoT is meer dan alleen verbonden apparaten: het gaat om de informatie die deze apparaten verzamelen en de krachtige, snelle inzichten die uit die informatie kunnen worden afgeleid. Daarom zijn IoT en andere ingebedde en operationele technologieën belangrijke zakelijke, operationele en beveiligings-onderwerpen geworden. De beveiliging van het IoT en OT wordt in directiekamers en bij discussies over wetgeving steeds meer gezien als een belangrijk onderwerp, deels vanwege de toenemende frequentie en ernst van aanvallen in het afgelopen jaar. Deze wildgroei van aanvallen heeft ook gezorgd voor meer bewustzijn over de mate waarmee aanvallen in het digitale domein gevolgen voor het fysieke domein kunnen hebben. Een computeraanval op Colonial Pipeline zorgde rechtstreeks voor de sluiting van de grootste benzineleiding in de Verenigde Staten. Een inbraak bij de Oldsmar-waterinstallatie leidde tot een gevaarlijke situatie, omdat de aanvallers toegang kregen tot de software van het SCADA-systeem en dat gebruikten om de concentratie van natriumhydroxide (een bijtende chemische stof) in het water te verhogen. Een hack bij een leverancier van beveiligingscamera's leidde tot het openbaar maken van gevoelige beelden uit ziekenhuizen, van politiediensten en vele andere bedrijven.

Al deze ontwikkelingen onderstrepen de noodzaak voor organisaties om hun IoT- en OT-systemen te beveiligen. Organisaties zijn meer dan ooit met elkaar verbonden, wat leidt tot meer blootstelling van verouderde OT-apparaten en -omgevingen, waaronder apparaten en omgevingen die voorheen relatief geïsoleerd waren. Aan de andere kant bevinden de nieuwste IoT-apparaten (zoals slimme tv's en sensoren) zich in zowel OT- als IT-omgevingen. Als we al deze informatie in de context van privacyzorgen en regelgeving bekijken, is het duidelijk dat er behoefte is aan een brede aanpak die naadloze beveiliging en beheer voor alle OT- en IoT-apparaten mogelijk maakt.

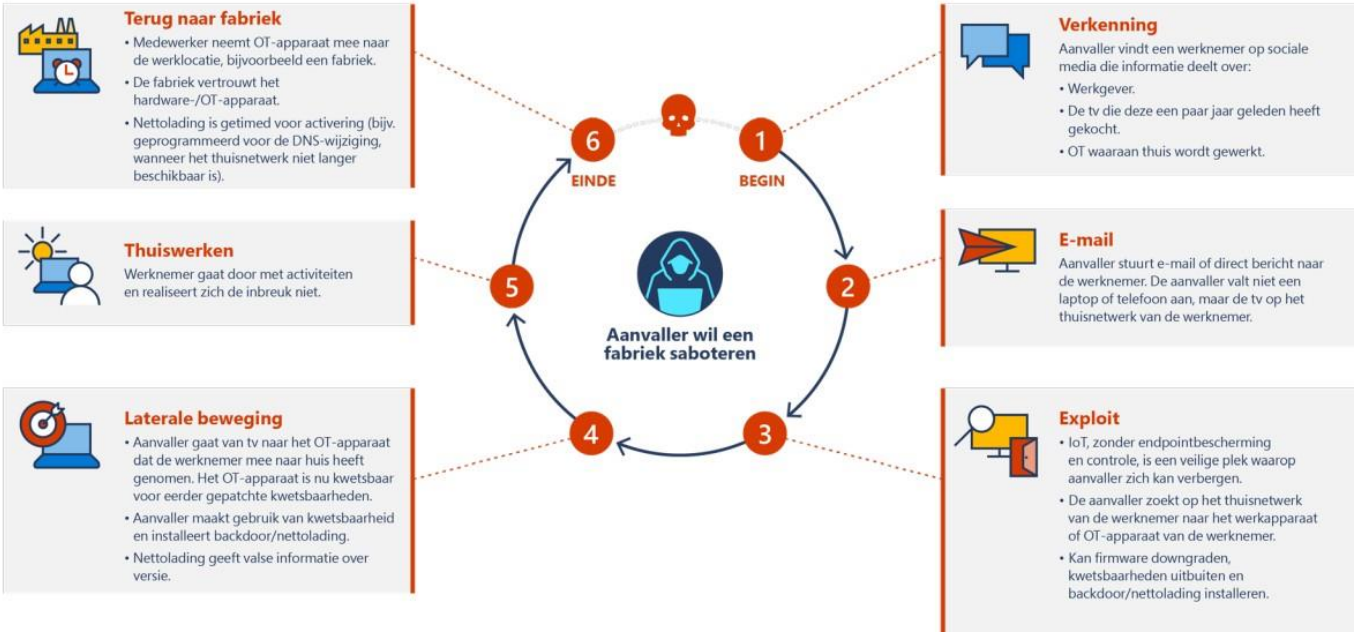
"Deze wildgroei van aanvallen heeft ook gezorgd voor meer bewustzijn over de mate waarmee aanvallen in het digitale domein gevolgen voor het fysieke domein kunnen hebben."

VERANDERENDE DREIGINGEN

Bedrijven hebben te maken met veranderende dreigingen en vernieuwende malware. Deze aanvallen zijn het afgelopen jaar ook in aantal en ernst toegenomen. Vanuit technisch oogpunt was de bedoeling van bijvoorbeeld de Triton-aanval op de veiligheidsbesturing in een petrochemische faciliteit in het Midden Oosten om grote structurele schade aan de faciliteit en mogelijk dodelijke slachtoffers te veroorzaken.

De aanvallers kregen een voet aan de grond in het IT-netwerk en gebruikten vervolgens de al op het netwerk aanwezige legitieme middelen om toegang te krijgen tot het OT-netwerk waar ze hun eigen malware plaatsten.

Hoe een aanvaller via het IoT een bedrijf kan binnendringen



WE RADEN ORGANISATIES MET IOT- EN OT-APPARATEN DE VOLGENDE RISICOBEPERKENDE STRATEGIEËN AAN:

Patchen, patchen, patchen

Volg de instructies van de leverancier voor het patchen van getroffen producten.

Zorg voor bewaking

als patchen niet kan. Aangezien de meeste verouderde IoT- en OTapparaten geen agents ondersteunen, moeten een voor het IoT en OT geschikte NDR-oplossing (netwerkdetectie en -respons)79 en een SIEM-/ SOAR-oplossing80 worden gebruikt om apparaten automatisch te ontdekken en

voortdurend te controleren op afwijkend of ongeautoriseerd gedrag, zoals communicatie met onbekende lokale of externe hosts.

Zorg voor bewaking

als patchen niet kan. Aangezien de meeste verouderde IoT- en OTapparaten geen agents ondersteunen, moeten een voor het IoT en OT geschikte NDR-oplossing (netwerkdetectie en -respons)79 en een SIEM-/ SOAR-oplossing80 worden gebruikt om apparaten automatisch te ontdekken en voortdurend te controleren op afwijkend of ongeautoriseerd gedrag, zoals communicatie met onbekende lokale of externe hosts.

Verklein het aanvalsoppervlak

Elimineer onnodige internetverbindingen met OT-controlesystemen en implementeer VPN-toegang (virtueel privénetwerk) met MFA wanneer externe toegang is vereist.

Segmenteer

Netwerksegmentatie is belangrijk, omdat dit de mogelijkheden voor aanvallers om zich zijwaarts door de infrastructuur te bewegen en middelen te compromitteren beperkt. IoT-apparaten en OT-netwerken moeten met firewalls van bedrijfs-IT-netwerken worden geïsoleerd.

DE ZEVEN EIGENSCHAPPEN VAN GOED BEVEILIGDE APPARATEN

We raden aan om te zorgen dat de hardware en het besturingssysteem van je eigen apparaten en die van je leveranciers veilig zijn ontworpen en geïmplementeerd, goed bestand zijn tegen inbraak en mechanismen en processen bevatten die de beveiliging continu bewaken en zo nodig waarschuwingen geven en de beveiliging herstellen. Door uitgebreid onderzoek en tests hebben we zeven eigenschappen bepaald die gelden voor alle zelfstandige, met internet verbonden apparaten die als zeer veilig worden beschouwd. In veel gevallen zijn in deze goed beveiligde apparaten extra beveiligingsmaatregelen toegepast, maar in alle gevallen is elk van deze zeven eigenschappen aanwezig. Samen bieden deze zeven eigenschappen een fundament voor de beveiliging van de hardware, software-architectuur en het besturingssysteem van apparaten, cloudcommunicatie en clouddiensten.

1. HARDWAREMATIGE VERTROUWENSBASIS

De identiteit en integriteit van het apparaat worden door de hardware beschermd. Fysieke tegenmaatregelen zijn bestand tegen side-channel-aanvallen.

- Heeft het apparaat een unieke, niet-vervalsbare identiteit die niet van de hardware kan worden gescheiden? Wordt de integriteit van de apparaatsoftware door de hardware beveiligd?

2. DIEPGAANDE VERDEDIGING

Meerdere lagen maatregelen tegen bedreigingen. Tegenmaatregelen beperken de gevolgen van een succesvolle aan op één bepaalde vector.

- Blijft het apparaat ook veilig als er een beveiligingsmechanisme wordt doorbroken?

3. KLEINE VERTROUWDE COMPUTEROMGEVING

Privésleutels zijn opgeslagen in een met hardware beveiligde kluis en niet toegankelijk voor software. Software wordt gescheiden in zichzelf beschermde lagen.

- Wordt de code voor het afdwingen van de beveiliging beschermd tegen bugs in andere software op het apparaat?

4. DYNAMISCHE COMPARTIMENTEN

Door hardware afgedwongen barrières tussen softwareonderdelen voorkomen dat een inbreuk zich naar andere onderdelen kan verspreiden.

- Wordt een storing in één onderdeel beperkt tot dat ene onderdeel? Kunnen er nieuwe compartimenten worden toegevoegd om nieuwe bedreigingen tegen te gaan?

5. VERIFICATIE ZONDER WACHTWOORD

Een met een niet-vervalsbare cryptografische sleutel ondertekende token die de identiteit en authenticiteit van het apparaat aantoont.

- Kan het apparaat zichzelf identificeren met certificaten of andere tokens die door de hardwarematige vertrouwensbasis zijn ondertekend?

6. FOUTRAPPORTAGE

Een softwarefout, zoals bufferoverschrijding veroorzaakt door een aanvaller die beveiliging onderzoekt, wordt gemeld aan een foutanalysesysteem in de cloud.

- Meldt het apparaat fouten, zodat die kunnen worden geanalyseerd en de juistheid van de uitvoering op het apparaat kan worden gecondoleerd en nieuwe dreigingen kunnen worden herkent?

7. VERNIEUWBARE BEVEILIGING

Een update maakt het apparaat veiliger en trekt gecompromitteerde middelen voor bekende kwetsbaarheden of beveiligingslekken in.

- Wordt de apparaatsoftware automatisch bijgewerkt? Kan de TCB-software van het apparaat snel en zonder andere code voor het apparaat opnieuw te verpakken worden bijgewerkt?

MEER LEZEN?

Ransomware: een veranderend bedrijfsmodel

Download

Phishing en andere kwaadaardige e-mails

Download

BEDANKT VOOR HET LEZEN VAN DEZE WHITEPAPER. HEEFT U NOG VRAGEN OVER HET ONDERWERP?

Neem dan gerust contact met ons op via info@socured.nl of 020 708 55 65.

Socured
Klokkenbergweg 50A
1101 AP AMSTERDAM-ZO
Tel.: 020 708 55 65
info@socured.nl
www.socured.nl

Onderdeel van Socia

Over Socured

Socured is gevestigd in Amsterdam en is onderdeel van Socia. Socia helpt al meer dan 15 jaar haar klanten op het gebied van IT en heeft inmiddels een mooie voetafdruk achtergelaten bij veel bedrijven in Nederland als het gaat om IT-diensten.