DE ON2IT IOT REACH AND RISK ASSESSMENT

EEN QUICK SCAN VAN JOUW IOT SECURITY POSTURE

Uit ervaring weten we hoe moeilijk het is om zicht te houden op de explosie van intelligente devices in elk netwerk, ongeacht je branche. Veel van deze devices staan niet op de cybersecurity radar.

Tegelijkertijd is IoT letterlijk overal. Van je op AliBaba gekochte beveiligingscamera tot de robots in de autofabriek, de bloeddrukmeter in het ziekenhuis of de smart tvs op kantoor en in de huiskamer. Met onze IoT Reach and Risk Assessment krijg je inzicht.

DE UITDAGING

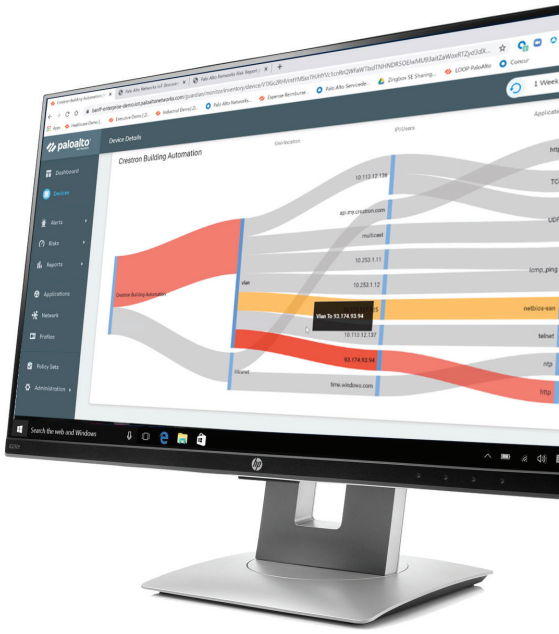
IoT is overal

Vandaag de dag bestaat bij een gemiddeld bedrijf meer dan 30% van alle op het netwerk aangesloten endpoints uit IoT apparaten. Deze cijfers zullen naar verwachting alleen nog maar blijven groeien. Een rapport van Gartner voorspelt dat de toepassing van IoT endpoints dit jaar zal stijgen tot 5.81 miljard.

Deze stijging is onontkoombaar, maar er komt wel het een en ander bij kijken. Beveiligingsteams zijn al belast met het beschermen van IT-endpoints die zijn verbonden met het bedrijfsnetwerk. In het nieuwe normaal – met het uitdagende concept van IoT aan het roer – krijgen ze ook te maken met uitdagingen die voortkomen uit de groei van het aantal IoT apparaten.

In het kort loop je bij IoT tegen het volgende aan:

- **Inventaris:** geen goed begrip van welke IoT apparaten zich in het network bevinden en hoe je nieuwe apparaten kunt volgen;
- **Bedreigingen:** gebrek aan geïntegreerde beveiliging in besturingssystemen van IoT apparaten die moeilijk of onmogelijk te patchen zijn;
- **Hoeveelheid data:** het is moeilijk toezicht te houden op enorme hoeveelheden data die worden gegenereerd door zowel beheerde als onbeheerde IoT apparaten;
- **Eigenaarschap:** beheer van IoT apparaten door verschillende teams binnen het bedrijf leidt tot nieuwe risico's;
- **Diversiteit:** de enorme diversiteit in IoT-apparaten qua grenzeloze vormen en functies;
- **Operations:** IoT-apparaten zijn cruciaal voor kernactiviteiten, maar voor de IT-afdeling moeilijk te integreren in hun dagelijkse cybersecurity operations.



Waar moet een goede IoT oplossing aan voldoen?

IoT komt niet uit de lucht vallen, en raakt op veel manieren aan de strategie en maatregelen die we voor de 'gewone' IT en OT dagelijks gebruiken, zowel in het eigen datacentrum als in de cloud. Daarnaast hebben cybersecurity bedrijven in de afgelopen jaren specifieke oplossingen voor IoT security aan hun portfolio toegevoegd.

Je IoT oplossing moet bieden:

- **Volledig inzicht in alle IoT apparaten die met het bedrijf verbonden zijn;**
  Het is belangrijk om inzicht te hebben in je attack surface. Dit is waar je IoT security lifecycle begint. Om je IoT middelen te kunnen begrijpen, moet je apparaat detectie gebruiken om volledig inzicht te verkrijgen.
- **Proactieve monitoring van IoT apparaten om voortdurend risicovol gedrag te detecteren;**
  Je zult je IoT apparaten te allen tijden actief moeten monitoren. Real-time monitoring, rapportages en alerting zijn cruciaal voor organisaties om IoT risico's te beheren.

MET DE ON2IT REACH AND RISK ASSESSMENT KRIJG JE INZICHT IN:

- Het aantal IoT apparaten in je netwerk;
- De kwetsbaarheden en het risico dat je loopt;
- De effectiviteit van je huidige securitymaatregelen;
- Gedetecteerde malware / malicious activity.

Je devices worden in onze rapportage voorzien van risico-profielen en inzicht in bekende kwetsbaarheden. Hiermee helpen we je om prioriteiten te bepalen binnen de organisatie.

Na de scan ontvang je van ons een Executive Report en aan de hand van een Powerpoint Presentatie zullen wij de bevindingen aan je presenteren.

Dit rapport geeft inzicht in je IoT apparaten, welke risico's er zijn, wat voor soorten traffic er zijn en welke applicaties er in gebruik zijn.

ON2IT's Managed Security Services

IoT Security is slechts een onderdeel van je algehele cybersecurity. Onze Reach and Risk Assessment biedt een moment opname, waar onze managed services een stap verder gaan.

ON2IT's Managed Security Services is een oplossing waarbij wij je totaal ontzorgen op het gebied van IT-security. Door middel van onze managed services kijken we continu naar je devices en bij een geconstateerde bedreiging wordt er door ons mSOC direct actie ondernomen.

Onze dienstverlening is volledig gebaseerd op de Zero Trust securitystrategie. Met Zero Trust kies je voor het effectief verkleinen van het aanvalsoppervlak van het gehele netwerk,

- **Geautomatiseerd risk-based aanbevelingen voor beveiligingsbeleid en handhaving;**
  Je IoT oplossing moet makkelijk inzetbaar zijn, zonder dat je extra infrastructuur of investering nodig hebt. Een ideale oplossing maakt gebruik van je huidige firewall voor een uitgebreide en geïntegreerde beveiliging. De oplossing moet automatisch beveiligingsbeleid aanbevelen en beleid afdwingen gebaseerd op het risiconiveau en de mate van verdachte activiteiten die wij detecteren in je IoT infrastructuur.
- **Snelle acties om bekende bedreigingen te voorkomen;**
  De gevarieerde aard van IoT apparaten zorgt voor een sterk gedistribueerde omgeving in je netwerk, met talrijke punten van compromis. Inzichten voortkomend uit de vorige stappen zorgen voor betere detectie en preventie van bekende dreigingen, en een betere afweer tegen bedreigingen.
- **Snelle detectie en respons op onbekende bedreigingen;**
  Je IoT oplossing moet in staat zijn om een nieuwe aanpak te benutten, gebaseerd op een collectieve threat intelligence engine die real-time malware analyse levert en je IoT apparaten beschermd tegen zero-day aanvallen.

ON2IT AND PALO ALTO NETWORKS: ZERO TRUST INNOVATORS

ON2IT's volledige steun voor Palo Alto Networks technologie sinds 2009 laat zien dat cybersecurity innovatie in ons bloed zit.

ON2IT is een Palo Alto Networks ASC Elite, ATP, CPSP, MSSP, CSSP, Diamond Partner, winnaar van een Traps Global Award en Managed Services Partner van het jaar.

Wereldwijd bieden wij managed cybersecurity diensten voor organisaties met complexe en dynamische IT-infrastructuren. Onze managed diensten zijn modulair, schaalbaar en kosteneffectief, en altijd gebaseerd op Zero Trust.

We are on to it, and you?

VOOR MEER INFORMATIE OVER ONZE REACH AND RISK ASSESSMENT:

Hogeweg 35, 5301 LJ Zaltbommel, Nederland
Email: sales@on2it.net - Tel: (+31) 088 22 66 200

5717 Legacy Drive, Suite 250, Plano, TX 75024, USA
Email: sales@on2it.net - Tel: (+1) (214) 206 8446