Workshop Defender for IoT (tekst til Azure Marketplace)

Innledning

Move er spesialister på IT-infrastruktur, nettverk og sikkerhet. Vi setter daglig opp servere og nettverk til store og små virksomheter i Norge. Uansett om virksomhetene har lokal infrastruktur, bruker Azure, Azure Stack HCI eller andre plattformer, så har vi spisskompetansen på å sette opp miljøene på best mulig måte.

Dagens trusselbilde fordrer også at miljøene er så sikre som mulig. OT og IoT enheter er en blindsone for mange IT avdelinger, og disse løsningene bærer ofte preg av sårbarheter og sikkerhetsutfordringer. Det er her Defender for IoT kommer inn i bildet.

Ved å ta i bruk Defender for IoT kan man gjennom nettverkstrafikk passivt lytte og bygge en baseline for normal trafikk i IoT eller OT nettverk. Man kan også samle informasjon om løsningene og overvåke nettverkstrafikk slik at alarmer kan utløses dersom det kommer uforutsette endringer.

Defender for IoT funksjonalitet, bruksområder og forbehold

Defender for IoT installeres enten som en ferdig Microsoft «Hardware Appliance» eller som en virtuell sensor som kan hostes på sentral infrastruktur eller i en VM på lokasjonen man skal overvåke. Sensorene har sentralt management i Azure, men kan også aksesseres direkte på sensor i full offline modus.

Defender for IoT vil gi et bilde av hvilke enhetstyper, hardware-leverandører, proprietære og vanlige protokoller man har på lokasjonen, samt et kart over kommunikasjon mellom enhetene og mot eller fra internett. Proprietære OT protokoller blir dissekert, informasjonen blir lært og Defender for IoT vil så alarmere på eventuelle avvik fra dette i tillegg til øvrige alarmer for nettverksovervåkning. Disse alarmene kan tas videre inn i kundens SOC-tjeneste for å ha løpende overvåkning på lokasjonene.

Sikkerhetsrapporter genereres av Defender for IoT som viser til sårbarheter, porter som er åpne, fjernaksess mellom enheter, passord som sendes i klartekst i nettet og mye mer. Denne rapporten kan brukes til å rapportere sikkerhetstilstand i en «Secure Score»-prosent, og kan løpende forbedres for å høyne sikkerheten på lokasjonen.

For å få mest mulig ut av denne løsningen er den avhengig av å se nettverksinformasjon på ganske lavt nivå, så en gjennomgang av nettverksutstyr og muligheter for SPAN og arkitektur er svært sentralt i denne løsningen.

Lisensiering

Lisensene til Defender for IoT prises i antall enheter per «site». Prisene finnes her.

- 100 Enheter XS
- 250 Enheter S
- 500 Enheter M
- 1000 Enheter L
- 5000 Enheter XL

Workshop
Move tilbyr en to dagers workshop i Defender for IoT. Vi vil sammen utforske funksjonaliteten i Defender for IoT, mulighetsrommet i nettverksinfrastrukturen og se det opp mot virksomhetens egne behov. Formålet med workshopen er å gi virksomheter et solid beslutningsgrunnlag til å vurdere innføring av Defender for IoT.

Workshopen inkluderer følgende aktiviteter:

- *Avklaring av forretningsbehov og sikkerhetsmål*
- *Demonstrasjon av funksjonalitet og muligheter*
- *Integrasjonsmuligheter mot SIEM løsninger*
- *Anbefaling av lisensplan i tråd med virksomhetens behov*
- *Demonstrasjon med virksomhetens egne data via Packet Capture filer (kunde stiller med disse selv, eller med hjelp fra oss)*
- *Gjennomgang av anbefalt implementeringsplan av Defender for IoT*

Gjennom workshopen utarbeides implementeringsplanen i konteksten av kundes behov og ønsker.

Tid: 16 timer
Pris: 28 000.-