axians

Een concreet plan als basis voor een volwassen security-strategie

THE BEST
OF ICT WITH A
HUMAN TOUCH

Om te bepalen hoe jouw organisatie het gewenste security-niveau kan behalen, moet je eerst inventariseren op welk security maturity-level de organisatie zich nu bevindt. Dit doe je aan de hand van een Security Maturity Review. De resultaten hiervan bieden vervolgens de input voor de roadmap waarin wordt vastgelegd hoe je de gap wil overbruggen tussen het huidige en gewenste security-niveau. Hierbij worden vijf levels aangehouden. Wat deze inhouden lichten we in deze leaflet toe.

De toegevoegde waarde voor jouw organisatie

- Volledige review op alle aspecten van security: software, mensen en proces.
- Totaalinzicht in de volwassenheid van je security met een overzichtelijk managementdashboard.
- Duidelijke prioriteiten en aanbevolen acties in een roadmap naar solide, volwassen security.

AXIANS.NL | info.nl@axians.com

VINCI ENERGIES

Level 1
Initial

Een organisatie bevindt zich op het eerste level wanneer de basis van 'Identify' en 'Protect' op orde zijn. Dit houdt in dat je zicht hebt op en begrijpt welke security-oplossingen je hebt, en wat de risico's zijn. Daarnaast heb je preventieve maatregelen genomen en zet je preventieve middelen optimaal in.

Level 2
Developing

De volgende stap die we adviseren is het operationeel hebben van Endpoint Security (EDR). Voor organisaties die in het kader van compliance met Security Incident & Event Manager (SIEM) aan de slag willen, kunnen hiervoor tevens alvast de basis aanleggen. Ook kan je een start maken met Extended Detection & Response (XDR). Hierbij ga je aan de slag met de integraties die geautomatiseerde respons faciliteren/realiseren en later in level 4 draagt dit bij aan het vormen van de samenwerking tussen EDR en NDR.

Level 3
Defined

Om level 3 te behalen moet de organisatie een volledig security-beleid hebben ingericht. Hieronder valt bovendien het vastleggen van het proces dat gevolgd moet worden in het geval van bijvoorbeeld een cyberaanval of datalek, inclusief de manier waarop de organisatie omgaat met de gevolgen (Incident Response Plan). Ook het aanstellen van een CISO behoort tot dit level, evenals de basis aanleggen voor de pijler 'Recover'.

Level 4
Managed

Doorgroeien naar level 4 is mogelijk wanneer je voldoet aan drie punten. Allereerst adviseren we organisaties om middels Netwerk Security (NDR) inzicht te krijgen in het daadwerkelijk actieve netwerkverkeer. Daarnaast wordt een Security Orchestration, Automation & Response (SOAR) -platform geadviseerd en een Security Operations Center (SOC) -team. Dit kan een SOC in eigen beheer zijn, maar je kan je SOC-diensten ook uitbesteden.

Level 5
Optimized

Indien het voor jouw organisatie relevant is, kan je ervoor kiezen om ook level 5 te behalen. Hiervoor bouw je verder aan en optimaliseer je de XDR voor de organisatie. Ook voeg je overige MDR-oplossingen toe, zoals Identity Threat Detect & Response en API Detect & Response. De laatste toevoeging is het implementeren van darkweb/exposure monitoring.

Krijg grip op security

We helpen je graag met het stap voor stap ontwikkelen van de beste security-architectuur, passend bij jouw organisatie. We kijken samen naar waar je staat, waar je naartoe wil, hoe je daar komt én hoe je daar blijft. Weten wat we voor jouw organisatie kunnen betekenen? Vul het contactformulier in op axians.nl/cybersquad.