SIT: Security Insights and Training

SIT back and relax

Met onze dienst SIT nemen we je belangrijke en vaak tijdrovende werkzaamheden op het gebied van cyber security preventie uit handen. We stippen de onderdelen kort aan.

Scannen op vulnerabilities binnen het netwerk

Wij plaatsen een virtual appliance op strategische plekken binnen je netwerk. Met maar liefst 8 verschillende scan-engines scannen de appliances bekende vulnerabilities op al je verbonden apparaten. Dat geldt voor Windows, Linux servers en werkstations, maar ook voor bijvoorbeeld switches, printers en IoT devices.

Scannen op vulnerabilities van buitenaf

Dagelijks voeren we een scan uit op je externe IP-adressen en SaaS webapplicaties. Ook deze scan voeren we uit met 8 krachtige scan-engines. Zowel op je externe beschikbare applicaties, maar bijvoorbeeld ook op je website! Zelfs als die uitbesteed is kun je hiermee ernstige reputatieschade voor jouw organisatie voorkomen!

Dark en Deep web data

Met uitgebreide dagelijkse scans op het deep en dark web laten we je zien wat er allemaal van en over jouw organisatie te vinden is. Denk bijvoorbeeld aan gelekte passwords, accountgegevens, copy/paste websites en tal van andere gegevens die hackers in staat kunnen stellen makkelijk je omgeving binnen te dringen. Door tijdig actie te ondernemen op basis van de gevonden gegevens kan veel kwaad en herstelwerk voorkomen worden.

Rapportage

Elke dag ontvang je van ons een glashelder rapport met een geclassificeerd overzicht van gevonden vulnerabilities. Uiteraard adviseren we je over een zo efficiënt mogelijke strategie en werkwijze en kunnen we je desgewenst verdere ondersteuning bieden.

Hacker alerts

Net als bij de interne scan appliances plaatsen we op strategische plekken binnen het netwerk een aantal Honeypots. Deze virtual appliances 'lokken' hackers door een groot aantal bekende en kwetsbare tcp/ip-poorten open te zetten. Als een hacker in deze val trapt wordt er direct een alert gegenereerd en kun je actie ondernemen om erger te voorkomen.

Security awareness training

Een belangrijk onderdeel van onze dienst SIT is eveneens het trainen van de eindgebruiker. Kwaadwillenden maken namelijk steeds meer gebruik van de onwetendheid of onkunde van de eindgebruiker en dringen via phishing e-mails, usb-sticks, SMS'jes of social engineering het bedrijfsnetwerk.

Wij trainen je collega's en testen hun kennis periodiek met eigen phishing security awareness campaigns. Ook hier geldt: de kracht zit in herhaling. Het is dan ook aan te raden om meerdere trainingen te laten volgen. Eindgebruikers krijgen toegang tot training filmpjes en infosheets, al dan niet gebaseerd op het resultaat van de awareness campaign. Uiteraard ontvang je zelf uitgebreide rapportages over de resultaten.

Controle krijgen en houden

Met de Axle-IT SIT service leveren we je alle benodigde informatie voor het krijgen en houden van controle over je security landschap. Hierbij zie je waar de zwakke punten zitten zodat je die zo snel mogelijk kunt verhelpen.

Natuurlijk helpen we je daar ook graag verder mee met onze andere producten en diensten zoals Patch Management, Privilege Management en Endpoint Detection and Response.

Meer weten? Of wil je een demo of proefversie aanvragen?
Neem contact op met Axle-IT via info@Axle-IT.nl, 0347-799 801 of je accountmanager.