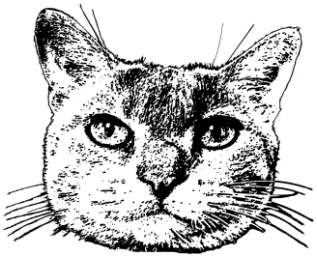


INFORMATIESHEET DIENSTVERLENING OPEN KAT

DOOR IP-ZORG (www.ip-zorg.nl)

19 APRIL 2024

Achtergrond IP-Zorg (www.ip-zorg.nl)

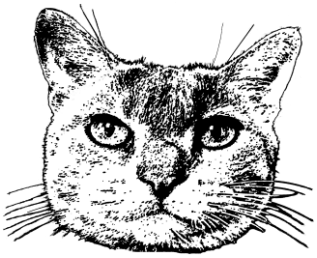
Stichting IP-Zorg (Informatieveiligheid en Privacy in de zorg) is in 2019 ontstaan vanuit de gedachte dat samenwerking binnen de zorg op gebied van informatiebeveiliging en privacy belangrijk is, zodat niet steeds door zorginstellingen opnieuw het wiel hoeft te worden uitgevonden. Stichting IP-Zorg is een netwerkorganisatie die zich ten doel stelt verbinding tot stand te brengen tussen personen en organisaties die binnen de zorg- en welzijnssector actief zijn op het gebied van informatieveiligheid en privacy. Het biedt zorginstellingen en andere betrokkenen de gelegenheid om op de hoogte te blijven van actuele ontwikkelingen.
De Stichting heeft geen winstoogmerk en is opgericht vanuit ideële motieven.

Waarom meer aandacht voor cyberweerbaarheid

Zorginstellingen worden steeds vaker doelwit van cybercriminelen, waarbij aanvallen meer doelgericht en beter voorbereid plaatsvinden. Omdat deze aanvallen lucratief zijn (denk aan ransomware) investeren criminelen hier ook steeds meer in. Juist daarom speelt cyberweerheid een belangrijke rol in NIS2, de nieuwe Europese richtlijn voor cybersecurity waar ook zorginstellingen zich binnenkort aan moeten houden.
Daar komt bij dat zorginstellingen meer te maken krijgen met een complex en divers IT-landschap, toenemende digitale gegevensuitwisseling en een toenemende afhankelijkheid van IT. Dit stelt zorginstellingen voor grote uitdagingen waar men vaak met een (te) beperkt budget mee moet omgaan.

Toelichting OpenKAT

Door het Ministerie van VWS is tijdens de Corona periode de zogenaamde Kwetsbaarheden Analyse Tool als opensource oplossing (OpenKAT) ontwikkeld, met name om te beschikken over de mogelijkheid om vast te stellen dat de vele organisaties die coronatests wilden gaan uitvoeren en hiervoor gevoelige persoonsgegevens moesten verwerken, hun beveiliging voldoende op orde hadden. OpenKAT is hierna door VWS doorontwikkeld om in de zorgsector breed te kunnen worden ingezet voor het vergroten van de cyberweerbaarheid en zal de komende tijd nog verder worden verbeterd en aangevuld. OpenKAT controleert, registreert en analyseert de status van ICT-systemen. Hiervoor worden netwerken en servers gescand, kwetsbaarheden geanalyseerd en rapportages met bevindingen opgesteld. Het integreert de meest gebruikte scantools in een modulair framework, heeft toegang tot externe databases met bekende kwetsbaarheden, registreert de bevindingen in een eigen OpenKAT database en combineert alle informatie overzichtelijk in een rapportage. Juist deze functionaliteit geeft organisaties de mogelijkheid op efficiënte wijze te werken aan hun cyberweerbaarheid en hier meer grip op te krijgen. Daarnaast biedt de registratie in de eigen database om hierover ook verantwoording af te leggen, bijvoorbeeld bij audits.



ip-zorg
Informatieveiligheid en privacy in de zorg

Eenmalige externe scan

Deze dienst maakt gebruik van het OpenKAT-framework en biedt inzicht in mogelijke kwetsbaarheden voor 1 domein plus maximaal 10 onderliggende hosts.
De mogelijke kwetsbaarheden die gevonden kunnen worden in deze dienst hebben betrekking op:

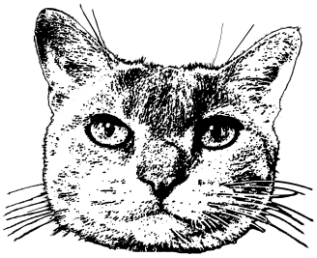
Voor het opgegeven domein:
Onjuiste DNS instellingen voor email, onveilige verbindingen van het opgegeven te scannen domein, openstaande poorten, onveilige verbindingen van het opgegeven te scannen domein, openstaande poorten, afwijkingen van de webserver configuratie ten opzichte van de beveiligingsstandaarden, status basisbeveiliging van DNS en gevonden kwetsbaarheden / CVE's (Common Vulnerabilities and Exposures).

Voor de gevonden onderliggende hosts:
Onveilige verbindingen, openstaande poorten, afwijkingen webserverconfiguratie tegen de basis beveiligingsstandaarden en gevonden kwetsbaarheden / CVE's.

Er wordt een OpenKAT bevindingenrapport opgeleverd naar aanleiding van de uitgevoerde scan inclusief één maal per jaar een mondelinge toelichting via MS Teams op basis van een analyse vanuit Stichting IP-Zorg. Tijdens de toelichting leggen wij de gevonden kwetsbaarheden uit en zullen aangeven welke partij in principe benaderd moet worden om de kwetsbaarheden op te lossen.

OpenKAT abonnement op externe scanning

Deze dienst maakt op dezelfde wijze als bij 1) gebruik van het OpenKAT-framework,en biedt inzicht in mogelijke kwetsbaarheden voor 3 domeinen (gelieerd aan de organisatie) en maximaal 25 hosts per domein. De inhoud van de scan is dezelfde als de hiervoor toegelichte externe scan en geeft inzicht in dezelfde kwetsbaarheden.
Het abonnement biedt daarnaast een doorlopende scan, alsmede vastlegging van de bevindingen en de oplossing hiervan in een database. Omdat dit de mogelijkheid biedt in de tijd terug te gaan, kan worden aangetoond dat actief invulling wordt gegeven aan cyberweerbaarheid, hetgeen bijvoorbeeld bij audits een belangrijke meerwaarde heeft.
Optioneel kan op basis van nacalculatie hiermee ook ondersteuning worden gegeven bij onderzoek naar specifieke incidenten/kwetsbaarheden.
Iedere 4 maanden wordt een OpenKAT bevindingenrapport naar aanleiding van de uitgevoerde scanning opgeleverd. Eén keer per jaar wordt een mondelinge toelichting via MS Teams aangeboden op basis van een analyse vanuit Stichting IP-Zorg op de rapportage. Tijdens de toelichting leggen wij de gevonden kwetsbaarheden uit en zullen aangeven welke partij in principe benaderd moet worden om de kwetsbaarheden op te lossen.



OpenKAT Portaal

De inhoud van de dienst komt overeen met 2), maar aanvullend hierop is de organisatie volledig zelfstandig in staat om OpenKAT in te regelen voor wat betreft te scannen objecten, zoals domeinnamen, ipadreseen, hosts. De organisatie beschikt hiermee over een eigen mogelijkheid om op ieder moment te rapporteren over de scans. Daardoor kunt u terug in de tijd rapporteren over gevonden kwetsbaarheden en wanneer deze opgelost zijn. Dit is een groot voordeel bij diverse audits.
Het OpenKAT portaal wordt door IP-Zorg ingericht voor het eerste gebruik, waarbij het eerste domein geactiveerd scanbaar wordt opgeleverd.
Het portaal mag gebruikt worden voor het scannen van maximaal 10 domeinen en maximaal 25 hosts per domein. De organisatie dient eigenaar/gebruiker te zijn van deze domeinen en dus zelf intern de vrijwaring hiervoor te hebben georganiseerd dan wel dit alsnog zelf te regelen (denk aan aan diensten die worden afgenomen bij derden). Dit geldt ook voor hosts en IP-adressen die de organisatie wenst te scannen.
Er worden maximaal 5 gebruikers voor de organisatie geactiveerd om in te kunnen loggen in uw OpenKAT portaal.
Optioneel kan worden gekozen voor een dagdeel gebruikerstraining voor een bedrag van € 500,00.

Interne scans (specifieke oplossing met offerte op maat)

Naast de uitvoering van externe scans ondersteunt het framework van OpenKAT ook interne scans op de infrastructuur van organisaties; hiervoor is het echter wel nodig om een VM te installeren op de interne omgeving. Deze wordt beheerd door IP-Zorg, verzamelt de scandata en kan deze overzetten naar de OpenKAT omgeving van IP-Zorg voor analyse en rapportage. Omdat deze dienstverlening een hoog maatwerk karakter heeft, zal op basis van wensen van de organisatie een hierop toegespitste offerte worden opgesteld.

Tot slot

Bij het abonnement en het portaal wordt technisch beheer van de OpenKAT omgeving volledig door IP-Zorg gedaan (updates, nieuwe releases). Ook wordt uiteraard de mogelijkheid geboden om gebruik te maken van de verdere doorontwikkeling en houden wij de klant op de hoogte. Stichting IP-Zorg neemt deel aan het OpenKAT stakeholdersoverleg met VWS en is dus nauw betrokken bij de verder doorontwikkeling en nieuwe mogelijkheden. Voor dit jaar verwachten wij uitgebreidere scanmogelijkheden, verbeteringen ten aanzien van rapportages en voorbereiding op NIS2.