dhs addsecurity
Endpoint Protection
Dienstbeschrijving

Auteur(s): Ruben Gerrits

Datum: 13 september 2023
Kenmerk: DB_addsec_EPaaS_V1
Status: Definitief

dhs informatisering
Kanaalstraat 12b
5347 KM Oss
Nederland

0412-653800
info@dhs.nl
www.dhs.nl
kvk 16052550

btw NL008180349B01
Rabobank
iban NL64 RABO 0140440062
swift RABONL2U

adding value

Inhoudsopgave

dhs informatisering
Kanaalstraat 12b
5347 KM Oss
Nederland

0412-653800
info@dhs.nl
www.dhs.nl
kvk 16052550

1 Endpoint Protection-as-a-Service

1.1 Introductie

De dagelijkse risico's waarmee bedrijven worden geconfronteerd zijn aanzienlijk toegenomen. Cybercriminelen ontwikkelen voortdurend nieuwe en geavanceerde aanvalsmethoden om kwetsbaarheden te exploiteren. Malware, ransomware en phishing-aanvallen behoren tot de meest voorkomende bedreigingen. Deze aanvallen kunnen leiden tot gegevensdiefstal, financiële verliezen, bedrijfsonderbrekingen en reputatieschade.

In de moderne digitale wereld is het beveiligen van onze endpoints, zoals servers, computers, laptops en mobiele apparaten, daarom van cruciaal belang geworden. Bedrijven en organisaties worden voortdurend geconfronteerd met een breed scala aan dagelijkse risico's, variërend van geavanceerde cyberaanvallen tot schadelijke malware en kwaadaardige insiders. Het effectief aanpakken van deze risico's vereist een proactieve en geavanceerde beveiligingsaanpak.

Bovendien evolueren de aanvalstechnieken voortdurend, waarbij aanvallers zich meer richten op de endpoints als de zwakke schakels in de beveiligingsketen. Ze proberen vaak onopgemerkt te blijven door zich te vermommen als legitieme gebruikers of door zich te verspreiden binnen een netwerk zonder detectie. Het is van cruciaal belang om deze geavanceerde bedreigingen in realtime te kunnen detecteren en er snel op te reageren voordat ze ernstige schade kunnen aanrichten.

dhs komt om deze reden met de Endpoint protection-as-a-Service dienstverlening. Een dienstverlening welke erop gericht is om uw endpoints, en dus bedrijfsvoering, continu veilig te houden.

Endpoint Protection-as-a-Service (EPaaS) geeft **dhs** de mogelijkheid om verdachte activiteiten op de endpoints te identificeren en te analyseren. Dit zodat wij snel kunnen reageren op bedreigingen voordat ze zich verspreiden of permanente schade aanrichten. Daarnaast biedt Endpoint Protection-as-a-Service ook de mogelijkheid om preventieve maatregelen te nemen door proactief kwetsbaarheden te identificeren, verdachte bestanden te isoleren en gebruikersactiviteiten te monitoren.

1.2 Wat is Endpoint Protection

Endpoint Detection & Response (EDR), wat de officiële naam is van deze state-of-the-art ontwikkeling, is een geavanceerde beveiligingstechnologie dat zich richt op het identificeren, opsporen en reageren op verdachte en schadelijke activiteiten op endpoints binnen een netwerk. Het gaat verder dan de traditionele antivirusoplossingen door geavanceerde analyse- en detectietechnologieën te gebruiken om zowel bekende als onbekende bedreigingen te identificeren. EDR-oplossingen bewaken voortdurend endpoints en verzamelen uitgebreide gegevens over de activiteiten en gebeurtenissen welke zich voordoen op het endpoint.

- **Realtime detectie**
  EDR-oplossingen monitoren endpoints voortdurend in realtime, waardoor ze verdachte activiteiten en afwijkend gedrag direct kunnen detecteren.

- **Gedragsanalyse**
  EDR maakt gebruik van geavanceerde analyse- en detectietechnieken, zoals gedragsanalyse, machine learning en threat intelligence. Hiermee worden zowel bekende als eerder onbekende bedreigingen (zero-day) te identificeren. Hierdoor kan het systeem afwijkende patronen en indicatoren van bedreigingen (IOC's) herkennen.

- **Rapid Response**
  Daarnaast biedt EDR een uitgebreide incidentresponsmogelijkheid. Hiermee zijn we in staat om gedetecteerde incidenten grondig te onderzoeken, de oorzaak te achterhalen en gepaste tegenmaatregelen te nemen om de schade te beperken en om herhaling te voorkomen.

- **Proactief**
  EDR helpt bij het snel identificeren en patchen van kwetsbaarheden op endpoints, waardoor proactieve maatregelen genomen kunnen worden potentiële aanvalsvectoren te elimineren. Het stelt ons ook in staat om verdachte bestanden te isoleren en niet normale gebruikersactiviteiten te monitoren.

- **Rapportage**
  Een uitgebreide rapportagefunctionaliteit zorgt ervoor dat we inzicht kunnen krijgen in de beveiligingsstatus van de endpoints. Hiermee kunnen we organisaties assisteren in het kunnen voldoen aan regelgevende vereisten en audits.

Al met al biedt EDR een krachtige beveiligingslaag voor endpoints, waardoor er proactief geacteerd kan worden op bedreigingen. Door deze geavanceerde technologieën en de kennis en kunde van **dhs** te combineren in één dienst, stelt Endpoint Protection-as-a-Service organisaties in staat om het algehele beveiligingsniveau te verhogen en snel te reageren op het voortdurend evoluerende dreigingslandschap.

1.3 Waarom "as-a-Service"?

Het investeren in, en het up-to-date houden van, enterprise waardige security oplossingen is een kostbare en tijdrovende aangelegenheid voor veel organisaties. Daarbij is er specifieke kennis nodig om beleidsregels en beveiligingsmaatregelen in te richten en te matchen met de bedrijfsvoering van de organisatie.

Toch wordt de behoefte van dergelijke oplossingen met de dag groter, al was het maar omdat het risico met de dag groter wordt dat organisaties slachtoffer worden van bijvoorbeeld ransomware of datadiefstal. Het is niet de vraag of dat een beveiligingsincident gaat plaatsvinden, maar wanneer deze gaat plaatsvinden.

dhs heeft als missie om iedere organisatie zo goed mogelijk te beveiligen tegen dit soort beveiligingsincidenten. Om deze reden heeft **dhs**, in samenwerking met haar partners, een dienst gelanceerd welke het mogelijk maakt om iedere organisatie te voorzien van de best mogelijke endpoint protection technologie welke er in de markt te verkrijgen is.

De "as-a-Service" dienstverlening komt vooral tot uiting in het feit dat de organisatie volledig ontzorgd wordt in het beheren en onderhouden van het EDR systeem. **dhs** en het online platform zorgen voor de benodigde integraties, bewaking en rapportage.

1.3.1 De voordelen

De voordelen van Endpoint Protection as-a Service (EPaaS) ten opzichte van standaard anti-virus oplossingen zijn:

- **Automatische en continu updates**
  Endpoint Protection-as-a-Service wordt continu bijgewerkt met de nieuwste beveiligingsupdates en -functies, zonder dat de organisatie zich zorgen hoeft te maken over handmatige upgrades. Dit zorgt ervoor dat de beveiliging altijd up-to-date is.

- **Schaalbaarheid**
  Endpoint Protection-as-a-Service biedt bescherming voor diverse endpoints, waaronder Windows-, macOS en Linux, en kan eenvoudig op- en afgeschaald worden. Dit zorgt voor uniforme beveiliging in heterogene IT-omgevingen.

- **Geavanceerde dreigingsdetectie**
  Het AI(Artificial Intelligence)-gedreven platform kan onbekende en zero-day bedreigingen detecteren, waardoor uw organisatie beter beschermd is tegen geavanceerde aanvallen, welke door traditionele antivirusoplossingen worden gemist.

- **Proactieve beveiliging**
  De EDR oplossing van **dhs** maakt gebruik van machine learning om bedreigingen te detecteren en te voorkomen voordat ze schade kunnen aanrichten. Dit proactieve beveiligingsniveau kan helpen bij het voorkomen van inbreuken voordat ze zich voordoen.

- **Isolatie en herstel**
  Naast detectie biedt de dienst ook direct mogelijkheden voor isolatie en herstel, waardoor bedreigingen geïsoleerd kunnen worden om verdere verspreiding te voorkomen. Daarnaast kunnen systemen snel hersteld worden naar een "gezonde" toestand.

1.4 Inhoud van de dienst

Zoals beschreven is Endpoint Protection-as-a-Service een dienst welke, voor een maandelijks bedrag per endpoint (desktop, laptop, tablet, server etc.), geleverd wordt aan de organisatie. De initiële installatie, configuratie vallen buiten de scope van de "as-a-Service" dienstverlening en worden separaat aangeboden.

dhs biedt de volgende zaken aan binnen de dienst Endpoint Protection-as-a-Service:

1. **Endpoint Protection Platform**
   dhs maakt voor haar dienstverlening gebruik van een zéér veilig en state-of-the-art platform van haar partner, een absolute "leader" op het gebied van deze vorm van endpoint protection. De technologie van dit platform is normaliter alleen beschikbaar voor grote organisaties of overheidsinstanties. **dhs** heeft met haar partner een model ontwikkeld, waardoor iedere organisatie gebruik kan maken van dit platform binnen de "as-a-Service" dienstverlening van **dhs**.

2. **Ondersteuning voor medewerkers**
   Door de extra beveiligslaag op de endpoints, kan het zijn dat een gebruiker bestanden niet kan downloaden of openen, of dat zijn of haar device zelfs preventief afgesloten wordt van het netwerk. Dit is natuurlijk uiterst vervelend voor de medewerker, maar soms noodzakelijk om ervoor te zorgen dat er geen virussen of ransomware binnen gehaald worden of dat er frauduleuze handelingen worden uitgevoerd op een endpoint.

   De **dhs** servicedesk staat klaar voor deze medewerkers om de gedetecteerde dreiging te onderzoeken en tegen maatregelen te nemen. Doelstelling is altijd om ervoor te zorgen dat de medewerker zo snel mogelijk zijn werkzaamheden kan continueren, echter zonder dat dit risico's vormt voor de ICT-infrastructuur, bedrijfsdata en continuïteit van de organisatie.

3. **Beheer en onderhoud**
   Het eenmalig installeren en configureren van een Endpoint Protection oplossing is niet afdoende. Dagelijkse beheer is benodigd om een dergelijke oplossing beschikbaar en up-to-date te houden. Om deze reden biedt de dienst de volgende activiteiten:

   a. **Endpointbeheer**: het koppelen en ontkoppelen van endpoints aan de EDR-oplossing;
   b. **Rapportage:** Het op verzoek opleveren van rapportages met betrekking tot incidenten, etc.;
   c. **Support**: Gebruikersvragen of problemen met de EDR-oplossing kunnen rechtstreeks gemeld worden bij de **dhs** servicedesk.

2 Setup en planning

De Endpoint Protection-as-a-Service dienstverlening wordt volledig, passend bij de organisatie haar wensen en eisen, geïntegreerd en geconfigureerd. Deze setup dienst kent een eenmalige vaste investering op basis van de "**dhs** Standaard Installatie" definitie.

De inhoud van deze installatie procedure is als volgt:

- **Inventarisatie**
  Voor de roll-out van de zogenaamde EPaaS agents, is het noodzakelijk om een volledig en up-to-date beeld te hebben van alle te beschermen endpoints. Denk hierbij aan alle devices, besturingssytemen, servers, etc.
  Op basis hiervan worden de definitieve aantallen bepaald, eventuele uitzonderingen besproken en policies e.d. vastgesteld.

- **Roll-Out & Learning Mode**
  Een tweede belangrijke stap is het uitrollen van de agents. Enerzijds wordt er in deze fase bepaald hoe agents het beste geautomatiseerd uitgerold kunnen worden (bijv. via Microsoft Intune) én anderzijds worden de uitrol zelf volledig uitgevoerd. Deze uitrol kan uitgevoerd worden, ook als er al een bestaande antivirus oplossing aanwezig is op de devices / endpoints.

  In de periode die daar op volgt, veelal twee (2) tot vier (4) weken, opereert het Endpoint Protection product in een zogenaamde "Learning Mode". Doelstelling hierbij is dat het product het gebruikersgedrag en machine gedrag leert kennen. Immers, om afwijkingen in gedrag te herkennen, dient het normale gedrag eerst vastgesteld te worden.

- **Activatie**
  Na dat de "Learning Mode" periode voltooid is, kan het product geactiveerd worden. Vanaf dit moment neemt de Endpoint Protection dienstverlening de complete bescherming van de devices over. Eventuele overbodige andere antivirus oplossingen kunnen worden verwijderd én medewerkers kunnen vanaf dat moment hun vragen en problemen kwijt bij de **dhs** servicedesk.

3 Dienstverlening dhs

Voor alle diensten beschreven in dit document, als ook overige diensten geleverd door **dhs** onder de merknamen van **dhs addcloud**, **dhs addcontrol**, **dhs addwireless**, **dhs addsecurity**, **dhs addmobility** en **dhs addbackup**, geldt dat deze onderhevig zijn aan een onderliggende "Service Level Agreement (SLA)". Deze Master SLA is opvraagbaar bij **dhs** en/of te downloaden via de website van dhs (www.dhs.nl).

4 Contractduur, looptijd en verlenging

De dienst **dhs** Endpoint Protection-as-a-Service wordt u aangeboden als een abonnement per endpoint met een bepaalde contractlooptijd.

- Standaard wordt deze overeenkomst aangegaan voor een periode van 12 maanden;
- De overeenkomst is niet tussentijds opzegbaar, maar wel aanpasbaar in aantallen;
- Opzegging dient schriftelijk en uiterlijk 1 maand voorafgaande aan de einddatum te geschieden;
- Indien geen opzegging heeft plaatsgevonden wordt de overeenkomst automatisch maandelijks verlengd;
- Overige bepalingen en voorwaarden staan beschreven in de onderliggende Service Level Agreement (Master SLA) en de Algemene Voorwaarden.