Grant Thornton

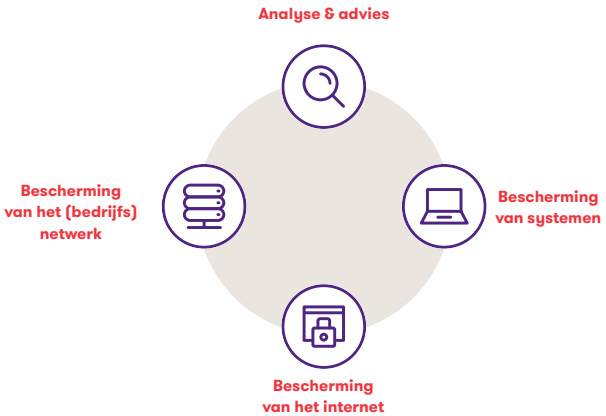
An instinct for growth™

Grant Thornton CyberHunter

Gebruik ik niet ergens verouderde softwareversies in mijn bedrijf? Hoe weet ik snel of mijn medewerkers op phishing berichten klikken? Waar begin ik met cybercrime beveiliging? Hoe pak ik dit aan? Relevante vragen. Informatiebeveiliging en cyberweerbaarheid zijn vandaag de dag essentieel. Wij helpen u. Grant Thornton CyberHunter (hierna te noemen CyberHunter) is een belangrijk onderdeel in onze aanpak. Dus leggen we deze dienstverlening hier voor u uit.

CyberHunter geeft inzicht in mogelijke kwetsbaarheden

Onze CyberHunter dienstverlening geeft u inzicht in onveilig gebruik door uw medewerkers en in kwetsbaarheden in uw internetverkeer, uw netwerk en uw informatiesystemen. Om dit te kunnen doen plaatsen we onze CyberHunter sensor in uw organisatie. Met CyberHunter sporen we onder andere geautomatiseerde aanvallen, fouten in configuraties, ontbrekende patches, aanvallen door hackers en ongewenst gedrag of uitbraken van malware (zoals ransomware) op.



Aandachtsgebieden

Een goed samenspel tussen technologie, processen en mensen; daar gaat het om bij uw weerbaarheid tegen cyberrisico's. Met CyberHunter zoeken wij naar kwetsbaarheden in uw omgeving. Tevens geven wij advies welke basisbeveiligingsmaatregelen binnen uw organisatie kunnen worden verbeterd, om zo uw cyberweerbaarheid te verhogen. Wij doen dat binnen drie gebieden, waarvoor wij u losse modules aanbieden: voor internet, netwerk en systeembeveiliging. Bij elke module krijgt u toegang tot de cybersecurity expertise van Grant Thornton. Hier komen ze.

Internet protection, ofwel internetbeveiliging

- De Internet protection module van CyberHunter simuleert een aanval op uw infrastructuur die via internet toegankelijk is. CyberHunter zoekt de mogelijke ingangen tot uw interne netwerk – via bijvoorbeeld configuratiefouten of verouderde software.
- De CyberHunter sensor analyseert al het in- en uitgaande verkeer tussen het interne netwerk en het Internet. Dat levert u inzicht in kwaadaardig verkeer en mogelijke aanvallen.
- Als de CyberHunter sensor kwaadaardig verkeer signaleert rapporteert hij dit aan ons.
- Wij onderzoeken de potentiële kwetsbaarheden en bepalen hun ernst. Ook kijken wij naar mogelijke verbanden tussen deze kwetsbaarheden.

Network protection, ofwel (bedrijfs)netwerkbeveiliging

- De network protection module van CyberHunter zoekt in het netwerk naar kwetsbaarheden in de configuratie en verouderde software op systemen, zoals op computers, servers, printers, telefoons. Die kwetsbaarheden geven een aanvaller de kans om toegang te krijgen tot deze systemen of tot applicaties of gevoelige gegevens.
- Wij onderzoeken de potentiële kwetsbaarheden om te bepalen hoe ernstig deze zijn. Ook kijken wij hier of er verbanden zijn tussen de gevonden kwetsbaarheden.

Device protection, ofwel systeembeveiliging

- De device protection module van CyberHunter kan verifiëren of gedetecteerde aanvallen een impact hebben op systemen. Daarnaast helpt device protection bij het beschermen tegen ransomware en andere vormen van malware.
- Deze module kan aanvallen detecteren en blokkeren, nog voordat een aanval een systeem of gebruiker bereikt.
- Device protection blijft ook actief systemen beschermen wanneer devices onderweg worden gebruikt. Dus bijvoorbeeld tijdens een zakenreis of wanneer een publiek wifi-netwerk wordt gebruikt.

Analyse en advies

Bij alle drie de modules krijgt u onze expertise erbij.

- Technologie kan niet alle cyberrisico's identificeren en oplossen, daarom analyseren wij de data en technische kwetsbaarheden en vertalen die naar dreigingen voor uw organisatie. Ook doen wij aanbevelingen om deze cybersecurityrisico's te mitigeren. De geïdentificeerde kwetsbaarheden en aanbevelingen bespreken wij met u op vaste contactmomenten.
- Alle geïdentificeerde kwetsbaarheden ziet u op een online dashboard. Via dit dashboard heeft u altijd inzicht in de kwetsbaarheden per systeem en in de lopende onderzoeken.
- Het online dashboard kan ook worden gebruikt om data te exporteren. Bijvoorbeeld bij het gebruik van een 'Vulnerability Management Tracking' of ticketsysteem binnen uw organisatie.

Wat levert het op?

- Door actueel inzicht en overleg zorgt CyberHunter voor een continue verbetering van de cyberweerbaarheid van uw organisatie.
- Actueel inzicht in de systemen die zich op het netwerk bevinden: assetmanagement.
- U krijgt actueel inzicht in kwetsbaarheden en aanvallen op uw netwerk, systemen en applicaties.
- Kwaadaardige aanvallen kunnen we (indien gewenst) automatisch blokkeren.
- U krijgt actueel inzicht in kwetsbaarheden en risico's via een veilig online dashboard.
- U heeft vaste contactmomenten om uw cyberonderwerpen met onze cybersecurity experts te bespreken.
- De CyberHunter sensor wordt eenvoudig geïmplementeerd en het heeft geen impact op het netwerk. Ook niet op de snelheid van het netwerk.
- Uw organisatie kan met de hulp van CyberHunter aan de AVG-eisen voldoen.

Contact

Ook weten hoe u de cyberweerbaarheid van uw organisatie kunt verhogen? Migiel de Wit-Beets vertelt u er graag meer over. U hoeft hem alleen maar even te bellen.

Migiel de Wit-Beets
Partner
T 088 676 91 86
E migiel.de.wit@nl.gt.com

Grant Thornton
An instinct for growth™