SAFELY ENABLING BUSINESS

VISIE OP SECURITY, INFRASTRUCTURE & SERVICES

"Door gebruik te maken van automation, machine learning en artificial intelligence in de architectuur en bij operationele processen en tooling, wordt technologie vele malen efficiënter en slimmer ingezet."

Er ligt een turbulent en bijzonder jaar achter ons. Vooral de ransomware aanvallen WannaCry, NotPetya, BadRabbit en de vulnerability die ontdekt werd in de veilig geachte WPA2 wifi encryptie keys zijn ons bijgebleven. Een jaar waarin wederom het dreigingsniveau en het aantal incidenten is toegenomen. Een jaar waarin duidelijk is geworden, dat iedere organisatie of persoon een potentieel target is. Ondanks dat er zelden een ransom betaald wordt, is de impact van een security-incident groot. Naast productiviteitsverlies hebben organisaties te maken met de operationele en financiële gevolgen.

Hoewel het maturiteitsniveau van met name grotere organisaties gestegen is (bron: CSBN 2017) en de noodzaak en aandacht voor detectie en respons wederom wordt bevestigd door onze relaties, is het informatiebeveiligingsniveau in de breedte nog steeds onvoldoende.

INSIGHT SERVICES

Naar aanleiding van de door ons in Europa uitgevoerde security maturity assessments (SMA), blijkt dat het merendeel van de organisaties met de komst van GDPR en het verhogen van het maturiteitsniveau een volle agenda heeft.

Een gerichte assessment is de perfecte methodiek om te bepalen wat het security maturityniveau van uw organisatie is. Na het assessment, die uitgevoerd wordt door een consultant van het cyber security advisory services team, ontvangt u een helder rapport met duidelijke aanbevelingen en prioriteiten zodat u weet hoe u uw security maturityniveau stapsgewijs kunt verhogen voor de drie pijlers: people, process en technology. Voor meer inzicht kunt u tevens phishing campaigns, health checks, malwaredetectie, penetratietesten, vulnerability en perimeter patrol assessments laten uitvoeren.

DE ARCHITECTUUR

Voor het designen en realiseren van infrastructuur en security architecturen gebruiken wij het adaptive security architecture model van Gartner. De veranderende mindset voor organisaties die dit model met zich meebrengt is het belangrijkste aspect. De continuous response mindset en de investering in geïntegreerde prevention, detection, response en prediction oplossingen zijn cruciaal bij het realiseren van deze architectuur.

Een geïntegreerde architectuur (platform), dient te bestaan uit componenten om cyberattacks succesvol tegen te gaan én dient optimale beschikbaarheid, capaciteit en flexibiliteit te bieden. Dit geeft u het juiste fundament voor de detectie en preventie eisen. De juiste (multi vendor) technologie is belangrijk maar een goede integratie en vergaande automation zijn cruciaal voor de correcte werking, aangevuld met de people en process kant voor detectie en respons.

AUTOMATION EN OPERATIONAL EXCELLENCE

Door in de infrastructuur maar met name bij operationele processen en tooling gebruik te maken van technieken zoals machine learning en artificial intelligence, is het mogelijk de technologie efficiënter en slimmer in te zetten. Door best practices in te zetten, te toetsen en te ontwikkelen gaat preventie naar een hoger niveau. Operational excellence vormt een uitdaging voor organisaties daar het dagelijks beheer complexer is geworden en specialistische kennis vereist is. Onze Operate service (NOC service) helpt u hierbij. Wij zorgen voor de juiste inzet van de technologie en verbeteren de integratie tussen onderlinge systemen.

PRIMAIRE AANVALSMETHODEN

Om uw organisatie te beschermen tegen security incidenten is het van belang te weten waar mogelijke zwakheden zitten, of via welke methoden de meeste incidenten veroorzaakt worden. De belangrijkste besmettingshaard is email. Eén op de negen personen heeft het afgelopen jaar last ondervonden van email malware. In toenemende mate vormt zogenaamde Business Email Compromise (BEC) een belangrijke dreiging. Emails die ogenschijnlijk vanuit een executive gestuurd worden, komen steeds vaker voor. Met een stijgend gemiddelde van ruim vijf per maand is dit zeker een aandachtsgebied in 2018. Onze email security oplossing biedt preventie voor bovenstaande gevaren maar biedt ook bescherming voor spam, scam, virussen, phishing, domain spoofing, typosquating en malicious URL's. Uiteraard speelt de inrichting van email authenticatie door de inzet van DMARC een rol bij de implementatie.

> Email fraud / Impostor Email of Business Email Compromise (BEC) is een ander type aanval die meestal doorgelaten wordt.

Ook het endpoint is een belangrijke besmettingshaard. De traditionele signature-based oplossingen bieden niet meer de juiste bescherming. Voor de huidige besmettingen is een geïntegreerde protectie, detectie en respons oplossing (EPP en EDR) nodig. Onze SecurePrevent Endpoint service detecteert dreigingen door gebruik te maken van op big data analysed gebaseerde wiskundige algoritmes.

Niet alleen het risico op een breach wordt aanzienlijk minder, ook de respons na een breach wordt eenvoudiger. Daarbij worden dreigingen in een vroegtijdig stadium gestopt, waardoor de impact op de organisatie kleiner is. Het terugzetten van een back-up is bijvoorbeeld niet meer nodig. Onze ThreatClean service vindt tijdens het onboarding proces altijd wel (potentieel) gecompromitteerde endpoints met niet eerder ontdekte malware of anderszins ongewenste software (PUP's). Na de ThreatClean begint uw organisatie met een 'schone lei'. Omdat de techniek achter de SecurePrevent Endpoint service altijd werkt, ook wanneer een endpoint geen verbinding met het internet heeft, is uw omgeving maximaal beschermd.

EMAIL EN ENDPOINT SECURITY

De noodzaak voor een premium endpoint en email security oplossing of service is duidelijk. Met onze eigen testmethode en intern onderzoek wordt email en endpoint security gerealiseerd. Dit kan volledig flexibel as-a-service of door middel van een subscription geleverd worden. Aandacht voor visibility, rapportage en forensische mogelijkheden nemen wij daar uiteraard in mee.

CLOUD APPPLICATIES

Het gebruik van zakelijke cloud applicaties is het afgelopen jaar sterk toegenomen. Het belang van controle over uw bedrijfskritische data in cloud omgevingen willen wij daarom nogmaals onderstrepen. Door de inzet van een cloud access security broker (CASB) oplossing in combinatie met een proxy of next generation security gateway, krijgt u inzicht en grip op het gebruik van uw (zakelijke) cloud applicaties.

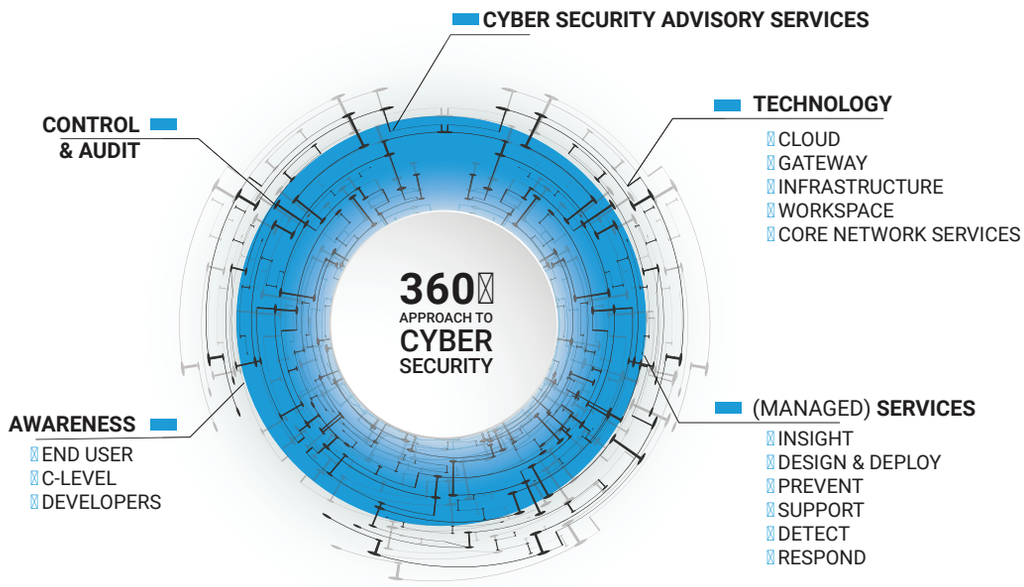
APPLICATION SECURITY

Webservices en internet applicaties worden via een application delivery fundament ontsloten. Functionaliteiten zoals intelligente load balancing, applicatie optimalisatie en applicatie security zijn binnen een application delivery network (ADN) van groot belang. Door de toepassing van virtualisatie, microsegmentatie en automation kunt u ook encrypted traffic management (SSL visibility) aan uw ADN toevoegen. Dit zijn integrale onderdelen van onze datacenter en security architectuur oplossingen.

IOT SECURITY EN LOCATION BASED SERVICES

Ieder device dient op een gecontroleerde manier toegang te krijgen tot uw netwerk en het dient inzichtelijk te zijn waar en wanneer dit gebeurt. De aangesloten IoT systemen vormen een security uitdaging en vereisen een geavanceerde network access control oplossing. De Mirai bot aanval heeft laten zien, dat er op grote schaal onvoldoende beveiligde IoT devices ingezet konden

THE 360° APPROACH TO CYBER SECURITY



worden. Door middel van segmentering en de inzet van Entity Behaviour Analysis (EBA) systemen in uw infrastructuur kunt u dit voorkomen.

Door location based services in combinatie met de grote hoeveelheid beschikbare data van een gebouw of stad in te zetten, zijn wij in staat slimme keuzes te maken bij de inrichting en het gebruik van ruimtes en kunnen gebruikers op een intelligente manier navigeren naar de juiste locatie.

DATA GOVERNANCE & DATA SECURITY TO THE NEXT LEVEL

Uit onderzoek blijkt, dat 91% van alle organisaties geen proces heeft om "data eigenaren" te traceren en 76% van alle organisaties kan niet bepalen wie de (semi-)ongestructureerde data kan benaderen. Bij veel organisaties is in de loop van de jaren de Active Directory (AD) door vervuiling onbeheersbaar geworden. Rechten worden wel uitgedeeld maar niet ingetrokken als een medewerker (tijdelijk) een andere rol vervult of uit dienst treedt. Over het algemeen krijgt een medewerker meer rechten naarmate hij langer werkzaam is bij een organisatie. De vervuiling wordt nog groter als rechten "gekloond" worden voor nieuwe medewerkers. Nesting (groepen in groepen) biedt voordelen maar brengt door de complexiteit ook risico's met zich mee.

Door inzicht te krijgen in het gebruik van, en de toegang tot ongestructureerde data binnen Windows, Exchange, Sharepoint, Unix/Linux en Office365 krijgt u hier meer grip op. Door middel van machine learning technieken en diepgaande analyse rond user behaviour kunnen tevens patronen en afwijkingen gesignaleerd worden.

SD-WAN

Het toepassen van SD-WAN technologie, de SD-Branch oplossing, lost voor branch locaties operationele en technische uitdagingen op, en biedt een passend platform voor LAN en WAN. SD-Branch is ontworpen vanuit een security visie met een hoge mate van flexibiliteit voor het kunnen sturen van verkeer. Centraal geconfigureerde role-based policies worden vanuit een branch gateway toegepast en internetverkeer kan gecontroleerd (inclusief stateful firewall, application firewall en deep packet inspection) en gericht gestuurd worden naar het private datacenter (inclusief WAN compressie) of direct naar het internet (split tunneling). Zero touch provisioning zorgt voor een efficiënte en snelle uitrol van de branch locaties.

INTENT-BASED NETWORKING EN SECURITY

Er is altijd een 'next big thing' in onze markt. Van Fabrics naar SDN in de datacenters tot SD-WAN en de volgende trend biedt zich alweer aan " Intent-Based Networking Systems (IBNS). Rajesh Ghai, researcher van IDC noemt IBNS kortweg "networking automation" maar Gartner beschrijft het als middleware welke de intelligentie levert die voorheen alleen beschikbaar was bij networking en

security engineers (rapport ID: G00323513). Het gaat uit van machine learning technieken en orchestration voor automatische netwerk configuraties en geeft visibility over de status van de infrastructuur.

Intent-based networking is geen product maar lifecycle management software die de status van het design, implementatie en operate van de netwerk en security infrastructuur zichtbaar maakt.

Hoewel intent-based networking prematuur is, zien wij dat veel vendors zich ontwikkelen op dit gebied. Het duurt zeker nog een jaar voordat dit mainstream wordt en dat belemmert de innovatie. Bekijk de video 'What is Intent-Based Networking?'

CLOUD STRATEGIE EN CLOUD SECURITY

In de hybrid cloud omgeving (waar public cloud en SaaS diensten geïntegreerd zijn met de private cloud) is het mogelijk om workloads seamless te verplaatsen tussen de private en de verschillende public cloud aanbieders (cross-cloud architecture). Security is hierbij een integraal onderdeel en het Software Defined Datacenter (SDDC) speelt hierin een cruciale rol. Zonder het SDDC, is het vrijwel onmogelijk een ware hybrid cloud te bouwen waarvan security, workload mobility en application delivery een integraal onderdeel uitmaken.

CONTEXTUAL THREAT INTELLIGENCE

Onze cyber threat intelligence service SecureInsight Intelligence biedt u gerichte informatie over dreigingen en trends, specifiek voor uw organisatie of binnen een bepaald segment (bijvoorbeeld healthcare of finance). Door context specifieke intelligentie (automatisch) toe te voegen in de infrastructuur (bijvoorbeeld in firewalls, DNS, proxy) kunnen applicatie of protocol gerichte aanvallen gedetecteerd en afgeslagen worden.

SECURITY ANALYSIS USE CASES

Onze 24/7 SecureDetect SIEM – security analysis service is primair gebaseerd op de log data uit uw omgeving. Het is van groot belang dat de veelal enorme hoeveelheid data verrijkt en automatisch verwerkt wordt, zodat onze security analisten zich kunnen focussen op de relevante data en events. De standaard use cases worden continu ontwikkeld en aangevuld met nieuwe use cases, waarbij als referentie gebruikgemaakt wordt van CIS Critical Security Controls v6.1 en ISO27002:2014.

Naast de standaard use cases (zoals suspicious usage of privilege accounts, potentially unwanted programs/ processes, possibly compromised accounts, malware outbreak, brute force attempts, ransomware identification, suspicious usage of DNS), kunnen er voor u ook specifieke use cases ingeregeld worden.

Managed Services - Een uniek onderscheid van onze totale Managed Services is de combinatie van Operate services en security analysis services, waardoor wij niet alleen security incidenten kunnen detecteren maar ook daadwerkelijk correctief kunnen ingrijpen en proactief kunnen adviseren.

SIEM tools (zoals LogPoint of Splunk) bieden de mogelijkheid alle machinedata te verwerken, eenvoudig te doorzoeken en overzichtelijk te presenteren. Aanvullende nieuwe technieken/oplossingen zoals UEBA of Network Traffic Analysis (NTA) sensors verhogen de detectie op afwijkingen. Gecombineerd met onze ervaren CDC analisten, automation, processen en de intelligentie welke ingebracht wordt (contextual threat intelligence) bent u verzekerd van de juiste security analyse.

SAFELY ENABLING BUSINESS

Organisaties dienen de digitale risico's te evalueren en zich te richten op het verbeteren van detectie en respons voor die onvermijdelijke cyberaanval. Gepassioneerde en ervaren specialisten helpen u bij de cyber security uitdagingen in een dynamisch applicatie landschap. Vanuit onze vier kernwaarden customer first, highly innovative, easy to do business with and respect and trust wordt de juiste stap bepaald voor uw security strategie.

Laten wij samen in 2018 de volgende stap op de security maturity ladder zetten!

Peter Mesker, CTO SecureLink Nederland