Whitepaper

Bestendige beveiliging tegen cyberaanvallen

secity_

INHOUDSOPGAVE

01 Introductie, Keuzewijzer, Security Roadmap

03 Uitleg verschillende diensten uit de Roadmap

03 Ik wil mijn IT Security op dit moment meten

04 Ik wil doorlopend bezig zijn met IT Security

05 Ik wil de optimale roadmap volgen om mijn IT Security te verbeteren

08 De verschillen tussen een pentest en MSSP

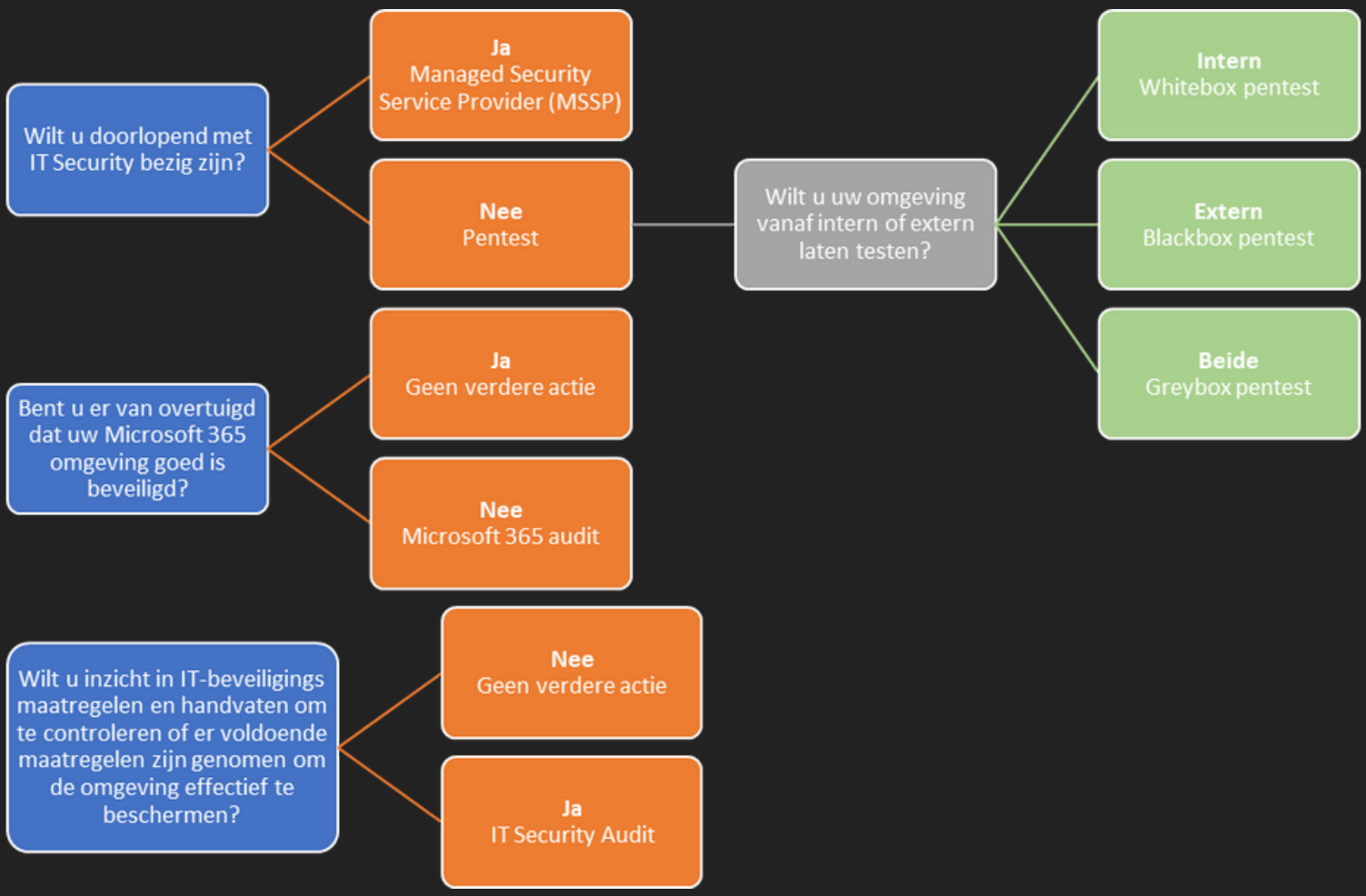
09 Over Secity

1. INTRODUCTIE

Doordat er dagelijks nieuwe kwetsbaarheden worden ontdekt in applicaties, besturingssystemen en databases, kan de kwaliteit van de netwerkbeveiliging veranderen. Steeds meer organisaties vragen zich dan ook af wat de actuele status van hun beveiliging is en of ze kwetsbaar zijn voor interne en externe aanvallen.

2. KEUZEWIJZER

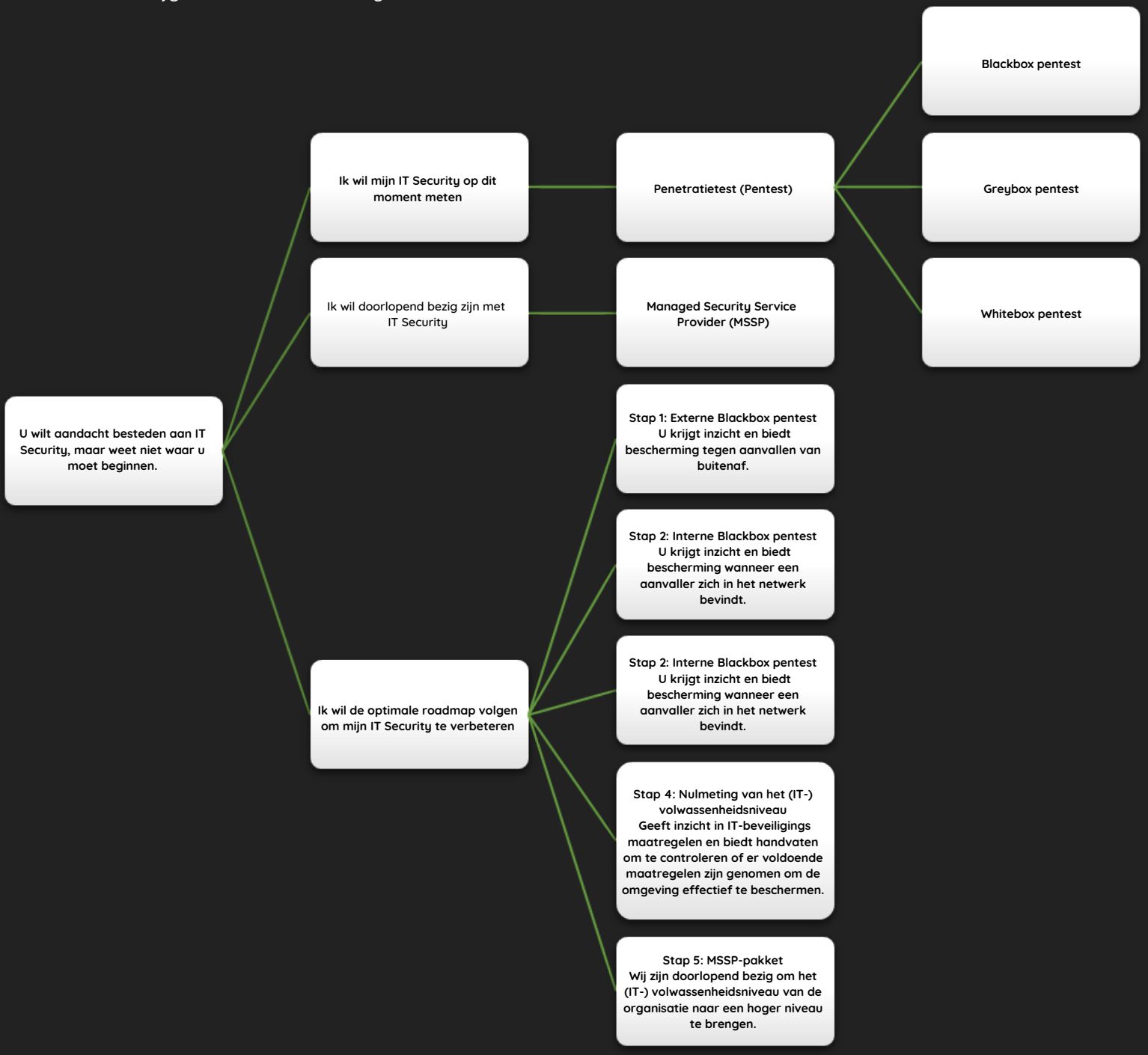
Het kiezen van een IT Security-dienst die past bij uw bedrijf vergt aardig wat technische kennis. Elk bedrijf is immers anders en elk startpunt verschilt. De onderstaande keuzewijzer kan u helpen met het krijgen van een gerichtere focus voor de beveiliging van uw IT-infrastructuur.



3. SECURITY ROADMAP

Veel mensen zullen in de bovenstaande keuzewijzer uitkomen bij een losse audit. Veel mensen denken dat doorlopend bezig zijn met IT Security veel werk is en relatief weinig oplevert. Niets is minder waar, door onze jarenlange ervaring in de IT Security hebben wij gezien dat doorlopend met IT security bezig zijn ervoor zorgt dat uw bedrijf bestendig beter beveiligd is tegen cyberaanvallen van buitenaf.

We hebben gemerkt dat veel bedrijven weten dat ze iets met IT Security willen doen, maar niet weten wat ze willen óf precies nodig hebben. Daarom hebben wij een roadmap opgesteld die deze bedrijven helpt inzicht te krijgen in hun IT Security behoefte.



4. UITLEG VERSCHILLENDE DIENSTEN UIT DE ROADMAP

Wellicht zijn termen als "pentest" en "MSSP" voor u nog onvoldoende bekend, daarom leggen we u in dit hoofdstuk graag uit wat deze termen betekenen en op welke manier deze diensten kunnen bijdragen aan uw IT-beveiliging.

4.1 IK WIL MIJN IT SECURITY OP DIT MOMENT METEN

4.1.1 Penetratietest (Pentest)

Een pentest helpt het in kaart brengen of en waar een organisatie kwetsbaar is. Tijdens de pentest maken wij gebruik van open source tooling, in house ontwikkelde applicaties en commercieel beschikbare tooling om kwetsbaarheden in kaart te brengen.

Naast het in kaart brengen van kwetsbaarheden van het netwerk, geeft een pentest ook inzicht welk verhoogd risico uw netwerk loopt door de bedreigingen die op dat moment actueel zijn. Door het afwegen van de kwetsbaarheden enerzijds en de bedreigingen anderzijds kan een inschatting worden gemaakt van het risico en de consequenties voor uw organisatie.

Om de technische IT-beveiligingsrisico's van misbruik van (web)applicaties en IT-infrastructuren in kaart te brengen zijn er meerdere methodes mogelijk: een blackbox-, greybox- of whitebox pentest.

4.1.2 Black box pentest

Bij een Black box pentest krijgt de ethische hacker vooraf geen enkele informatie over uw IT-infrastructuur en de onderliggende architectuur van een applicatie. Wél spreken wij vooraf een scope om te garanderen dat het onderzoek wat oplevert. Onze pentester benadert de omgeving als een echte aanvaller. Een Black box pentest is nuttig wanneer u voor de eerste keer een pentest uitvoert en een algemeen beeld wilt krijgen van het beveiligingsniveau.

4.1.3 White box pentest

Bij een White box pentest krijgen wij volledige toegang tot het netwerk of applicatie en daarnaast wordt het ontwerp van het netwerk gedeeld. Doordat onze ethisch hackers veel informatie hebben kunnen zij de pentest zeer grondig uitvoeren. Deze methode wordt veelal toegepast op een beperkte scope, denk hierbij aan een applicatie die zeer belangrijk (bedrijfskritisch) is voor uw bedrijf.

4.1.4 Greybox pentest

Een Greybox pentest is een combinatie van een Blackbox en een Whitebox. Een hacker krijgt voorafgaand aan de audit beperkte informatie over het netwerk en achterliggende systemen, zoals een gebruikersaccount in het systeem of de applicatie. Onze pentesters beschikken tijdens de Greybox pentest over ongeveer evenveel voorkennis als bijvoorbeeld een klant, medewerker of een goed geïnformeerde hacker. Een Greybox pentest wordt vaak toegepast om te kijken hoe veilig een omgeving is vanuit een klant- of medewerkersperspectief.

4.2 IK WIL DOORLOPEND BEZIG ZIJN MET IT SECURITY

4.2.1 Managed Security Services Provider (MSSP)

Een IT Security Roadmap stelt organisaties in staat om zonder grote investeringen gebruik te maken van het volledige IT-beveiligingsdienstenpakket van Secity tegen een vast bedrag per maand. Op deze manier kunnen we een doorlopend plan creëren die de IT Security structureel verbeterd. Onze IT Security Roadmap is gebaseerd op de "hacker cycle". Een hacker gaat vaak systematisch te werk met betrekking tot het uitbuiten van zwakheden binnen de IT-omgeving waarbij een IT Security Roadmap het perfecte "tegengif" is om uw IT-omgeving te beschermen.

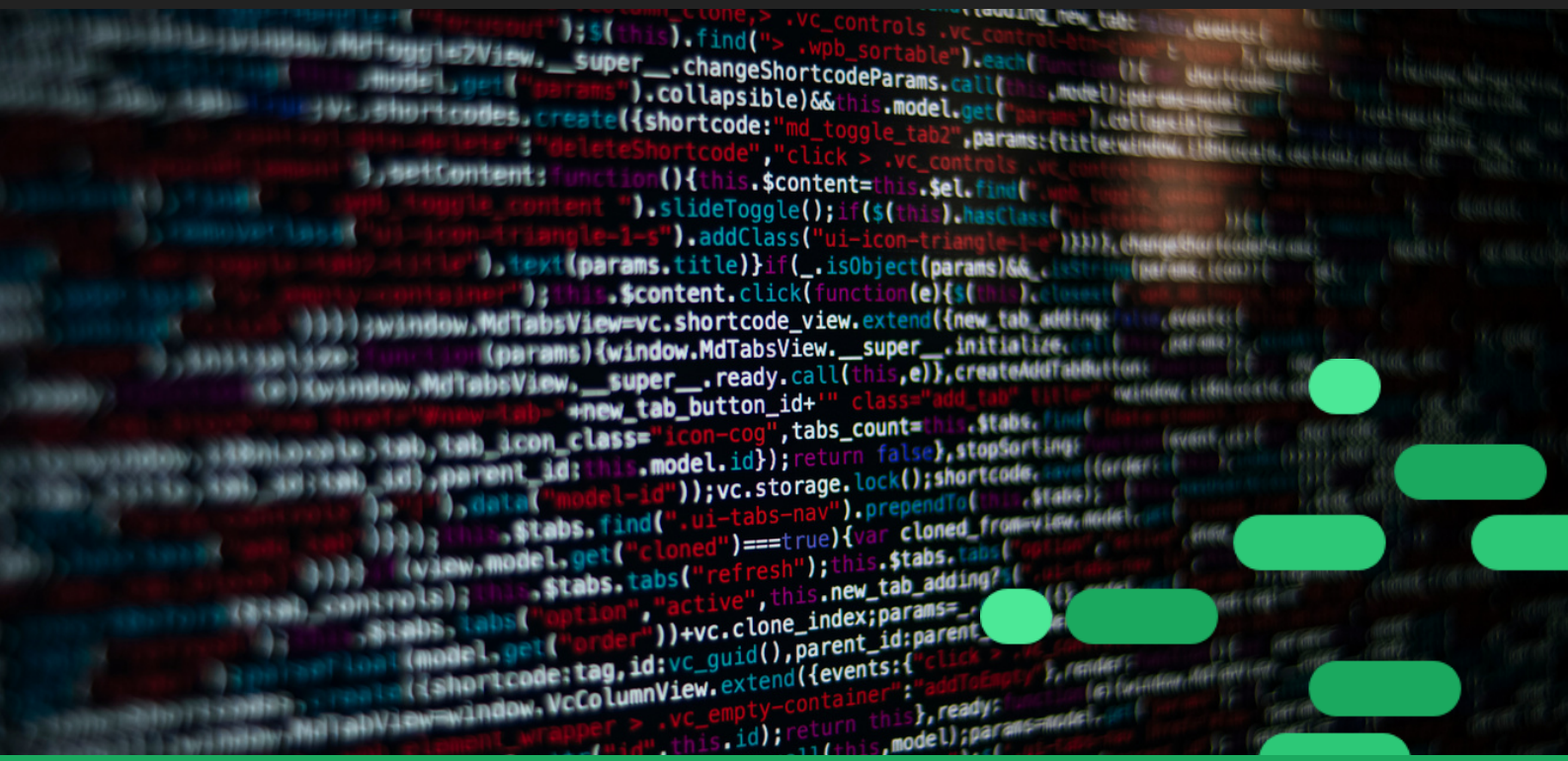
Een IT Security Roadmap biedt een aantal grote voordelen:

- Goed inzicht in (jaar)planning IT-beveiligingsonderzoeken
- De beschikking over een vaste adviseur met kennis van de situatie en de organisatie
- Beter inzicht in IT-beveiligingskosten
- Reservering capaciteit;
- Minder administratieve handelingen voor elk deelproject
- Periodieke voortgangsbesprekingen

Of u zich nu wilt beschermen tegen geautomatiseerde, gerichte of gelegenheidsaanvallen, ons MSSP-model is ontworpen voor bedrijven die op een volwassen manier met hun IT Security aan de slag willen. Het geeft snel inzicht in de interne en externe attack surface van de organisatie en de huidige stand van zaken.

Elk bedrijf is anders en elk startpunt verschilt. Daarom werken wij met een nulmeting om het huidige securityniveau van een bedrijf te “meten”. Bij een risico-inventarisatie (of IT Security audit) loopt een security consultant in een persoonlijk gesprek gestructureerd door een vragenlijst heen om op hoofdlijnen de belangrijkste aspecten van IT Security zoals de omgeving, volwassenheid en de scope in beeld te brengen. Op basis van de input baseren wij de volgorde van de IT Security roadmap.

Nadat de overeenkomst is getekend zal samen met u de planning worden vastgesteld tijdens een kick-off meeting, hierna zullen wij de planning definitief maken en bevestigen zodra ook formeel overeenstemming over de opdracht is bereikt.

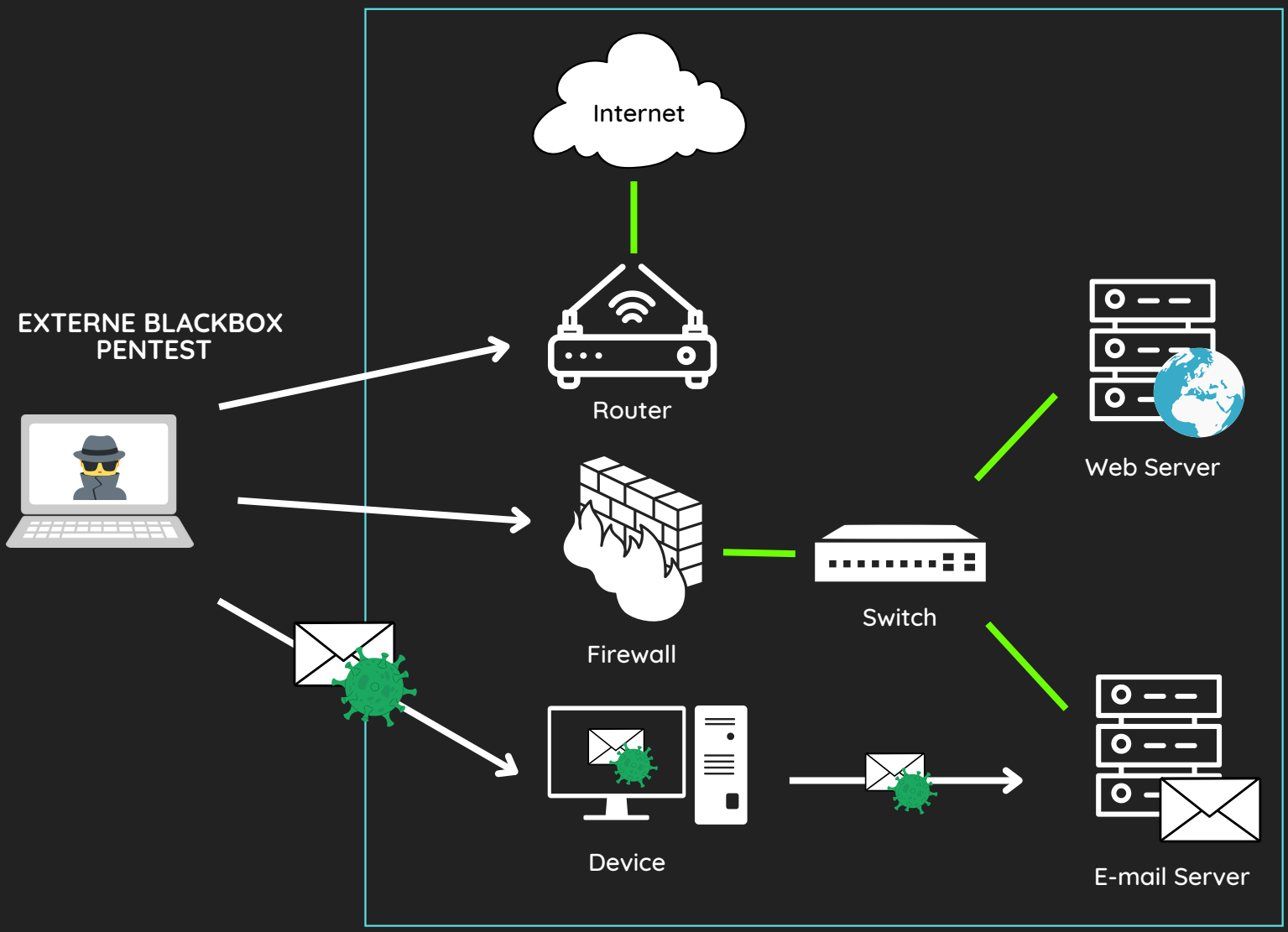


4.3 IK WIL DE OPTIMALE ROADMAP VOLGEN OM MIJN IT SECURITY TE VERBETEREN

4.3.1 Externe Blackbox Pentest

Als eerste stap adviseren we om een audit uit te laten voeren op diensten die via het internet toegankelijk zijn. Hierbij wordt er gekeken of het voor een aanvaller mogelijk is om via het internet toegang te krijgen tot vertrouwelijke informatie. Ook platforms als Microsoft 365 zijn hierbij belangrijk, vaak wordt er gebruik gemaakt van de standaard instellingen en wordt er niet effectief gebruik gemaakt van de beveiliging die een platform zoals Microsoft 365 biedt.

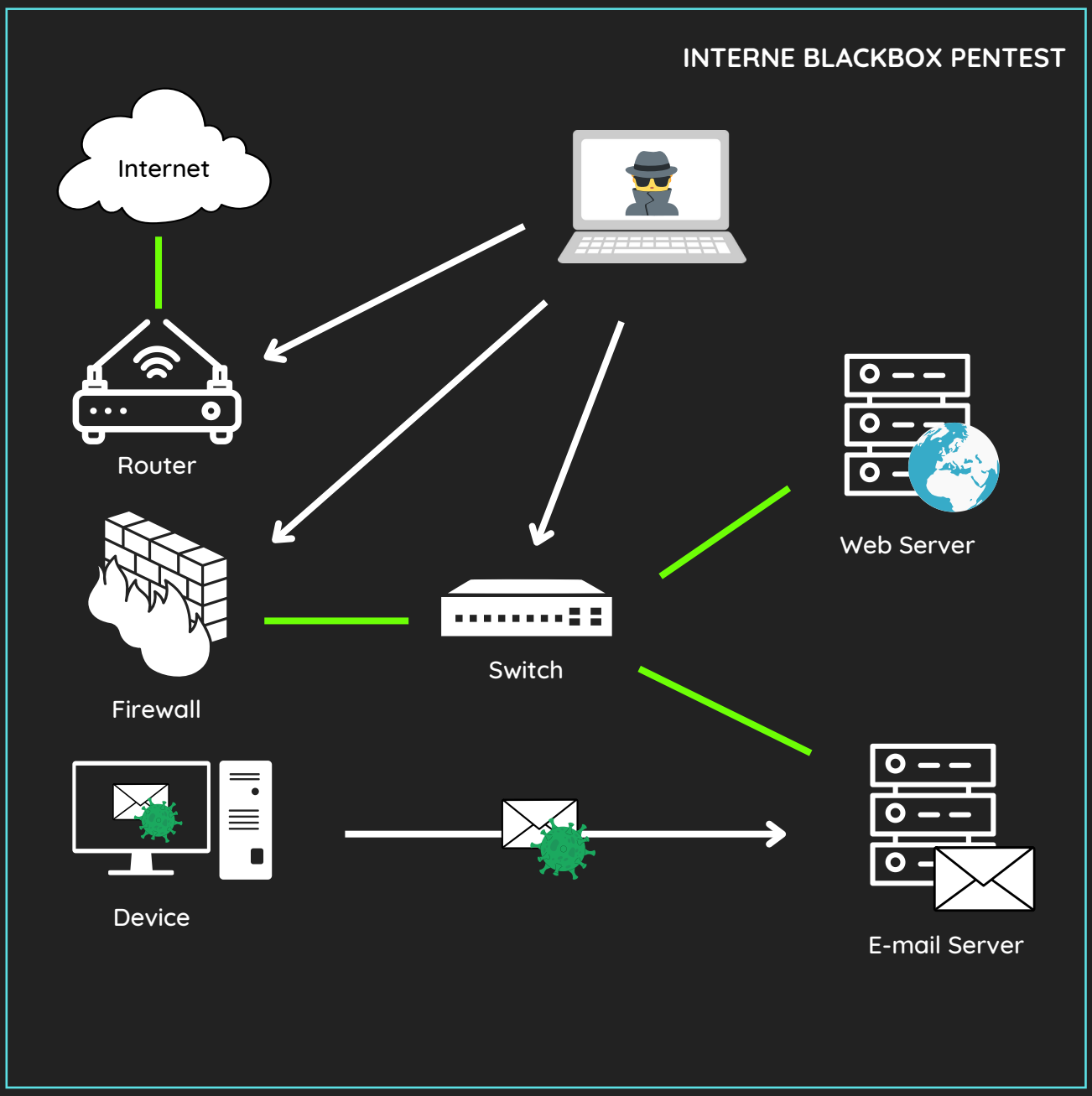
Een Externe Blackbox Pentest geeft inzicht en biedt beschermingen tegen aanvallen van buitenaf.



4.3.2 Interne Blackbox Pentest

Wanneer de buitenkant op orde is, wordt het tijd om intern te controleren waar een aanvaller toegang tot kan hebben wanneer er bijvoorbeeld een werkstation van een werknemer wordt overgenomen door middel van een phishingaanval. Staan bijvoorbeeld de servers met vertrouwelijke informatie en de werkstations in hetzelfde netwerk? Zijn er configuratiefouten gemaakt of er is er wel gebruik gemaakt van de beveiligingsinstellingen die applicaties bieden? Dit komt naar boven tijdens een interne pentest.

Een Interne Blackbox Pentest geeft inzicht en biedt bescherming wanneer een aanvaller zich in het netwerk bevindt.



4.3.3 Interne Whitebox Vulnerability en Configuratie scan

Nadat er effectief is gekeken of er van buitenaf en intern geen kwetsbaarheden zijn waar een aanvaller zonder login gegevens toegang tot heeft, wordt het tijd om de configuraties op werkstations en servers zelf te controleren.

Een Interne Whitebox Vulnerability en Configuratie scan geeft inzicht en bescherming in de kwetsbaarheden per server en werkstations.

4.3.4 Nulmeting van het (IT-) volwassenheidsniveau

Wanneer de servers, werkstations en netwerken zijn gecontroleerd, wordt het tijd om aan het beleid te gaan werken. Dit doen we aan de hand van 18 critical control points (dit zijn 18 categorieën met in totaal zo'n 183 subcontrols). Hierin worden vraagstukken behandeld zoals: Is er documentatie over de werkstations en servers met betrekking tot welke software er is geïnstalleerd en wordt dit regelmatig up-to-date gehouden. Is er op elk werkstation een malwarescanner geïnstalleerd en is de harde schijf encrypted? Heeft elke gebruiker een sterk password en is hier een policy voor? Is er een update policy voor server en werkstations en is dit vastgelegd?

Een Nulmeting van het (IT-) volwassenheidsniveau geeft inzicht in IT-beveiligingsmaatregelen en biedt handvatten om te controleren of er voldoende maatregelen zijn genomen om de omgeving effectief te beschermen.

De kracht van de bovenstaande 4 stappen is dat we beginnen om de omgeving te bekijken door de ogen van een aanvaller en zo snel mogelijk de kwetsbaarheden in beeld hebben die dan door de IT-afdeling op basis van prioriteit kan worden opgelost (stap 1 en 2). In stap 3 worden de kwetsbaarheden per systeem in beeld gebracht. In stap 4 wordt het (IT-)volwassenheidsniveau van de organisatie naar een hoger niveau gebracht.

DE VERSCHILLEN TUSSEN EEN PENTEST EN HET MSSP-MODEL

MSSP-model	Pentest
Doorlopend bezig met security	Momentopname
Doorlopende externe vulnerabilty scans en monitoren attack surface	Eenmalige externe scan
Periodieke interne vulnerabilty scan	Eenmalige interne scan
Alle onderdelen van het netwerk worden doorlopen op basis van security thema's	Geen security thema's
Bij nieuwe grote vulnerabilty wordt dit opgepakt in een nieuw security thema	Geen security thema's
Onderdelen van een pentest wordt verdeeld over de roadmap	De volledige omgeving wordt binnnen korte tijd (+-1 week) doorgelicht.
Ondersteuning bij security vraag stukken	Geen ondersteuning bij security vraag stukken
Security Roadmap	Actionable data + management rapport
Minder administratieve handelingen voor elk deelproject	Vrijwaring per pentest benodigd
Periodieke voortgangsbesprekingen	Eenmalig na bespreken
Nulmeting inbegrepen	Nulmeting is een losse audit
Phising campagne inbegrepen	Phising campagne is een losse module

Over Secity

Het team van Secity heeft al jarenlange ervaring in de IT Security. Het team zet zich iedere dag in om informatiestructuren te beveiligen en bescherming te bieden tegen hackers. Secity is een jong bedrijf, met een hecht team. Onze focus ligt bij het behouden van de persoonlijke aanpak. Wij willen niet zomaar een extern bureau zijn, maar aanvoelen als uw collega.

De sfeer binnen Secity ademt positiviteit en veerkracht. Binnen het team werken we gestructureerd en pragmatisch. De focus ligt daarbij op de ontwikkeling binnen het team. De wereld van hacken staat niet stil en we zijn graag voorbereid op welke hacktechniek dan ook. Hoe beter en meer up-to-date het team is, hoe zekerder u bent van een veilig bedrijfsnetwerk.

Bent u na het lezen van deze whitepaper benieuwd hoe wij uw bedrijf kunnen helpen bij het beveiligen van uw informatiestructuren en de bescherming tegen hackers? Neem dan geheel vrijblijvend contact op via de volgende contactgegevens:

Secity BV
Westerstraat 8
1829 BN Oudorp
+31 8 5130 5220
info@secity.nl

Volg ons ook op LinkedIn