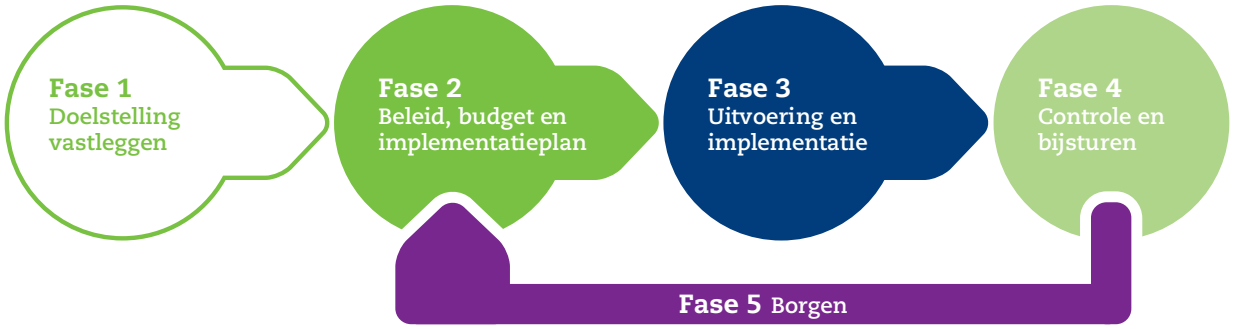
Effectief Beveiligen in de praktijk

Organisaties weten dat hun informatiebeveiliging op orde moet zijn. Toch is het in de praktijk vaak lastig om te bepalen welk beveiligingsniveau goed aansluit bij de organisatiedoelstellingen en -cultuur. Pinewood biedt met Effectief Beveiligen een pragmatische benadering voor het in kaart brengen van potentiële dreigingen en risico's om daar beleid, maatregelen en implementatie op af te stemmen.



Doeltreffende aanpak

Of u nu informatiebeveiliging voert vanuit de noodzaak tot een certificering of vanuit goed huisvaderschap, het is belangrijk dat de maatregelen die getroffen worden in lijn zijn met de cultuur en belangen van de organisatie. Uit onderzoek blijkt echter dat veel organisaties (ruim 40%[1]) slecht kunnen bepalen welke investeringen ze moeten doen voor een accurate informatiebeveiliging. Pinewood kan de beveiligingsrisico's voor uw organisatie in kaart brengen en daar passende maatregelen op afstemmen met de 'Effectief Beveiligen'-aanpak.

Effectief Beveiligen biedt organisaties uiteenlopende voordelen. We zetten de belangrijkste alvast voor u op een rij:

Modulaire aanpak

U bepaalt zelf welke stappen en maatregelen voor uw organisatie van belang zijn en welke u zelf, of in samenwerking met Pinewood wilt uitvoeren.

Integrale aanpak

Wij benaderen informatiebeveiliging als een 3-dimensionaal proces dat organisatie, techniek en personeel combineert.

Effectieve investering

Maximale effectiviteit, omdat beleid en maatregelen afgestemd zijn op het optimale beveiligingsniveau voor de organisatie.

Potentiële besparingen

Ineffectieve maatregelen worden teruggedraaid.

Ervaren partner

Pinewood ondersteunt u met advies en begeleiding bij het nemen van de juiste maatregelen en het realiseren van een werkbaar resultaat.

Proactief

Overgang van reactieve naar proactieve beveiliging, waardoor de focus verschuift van incidenten oplossen naar anticiperen op potentiële risico's.

Duurzaam resultaat

Pinewood gelooft in een open manier van werken, waarin samenwerking met onze relatie centraal staat. Alleen zo kunnen wij duurzame resultaten leveren. Dit betekent dat wij projecten in het kader van Effectief Beveiligen altijd uitvoeren in samenwerking met medewerkers uit alle lagen van de organisatie. Deze aanpak draagt

[1] Cyber Watch Survey Report, IT Governance, 2013

bij aan de bewustwording en betrokkenheid bij de individuele medewerker. U kunt zelf de juiste beveiligingsprioriteiten stellen en daar een doelgericht beleid voor opstellen of de daarbij benodigde maatregelen instellen. Met deze resultaatgerichte aanpak komen alle relevante aspecten van beveiliging (beleid, techniek en mens) aan de orde zonder extra kosten. Dan is beveiliging niet langer een technische noodzaak, maar levert het een concrete bijdrage aan de informatiebeveiligingsstrategie.

In de praktijk

Fase 1 Een passend beveiligingsniveau

Elk project begint met het in kaart brengen van de organisatie, relevante wet- en regelgeving, normenkaders en best practices. Vaak wordt gebruik gemaakt van een gap-analyse, nulmeting of risico-inventarisatie.

Fase 2 Beleid vaststellen

Na de inventarisatie worden de maatregelen concreet vastgesteld, inclusief budget en een implementatieplan. Het eerder vastgestelde beveiligingsniveau is een integraal onderdeel van de maatregelen. Het implementatieplan is een blauwdruk voor de inrichting van de beveiliging, samen met overige prestatie-indicatoren zoals scope, doorlooptijd en kwaliteit.

Fase 3 Implementatie

De geselecteerde maatregelen worden concreet uitgevoerd. Bijvoorbeeld door informatie en informatiesystemen te classificeren of met de herziening van de netwerkinfrastructuur. Daarnaast is er ook ruime aandacht voor de rol en bewustwording van management en medewerkers.

Fase 4 Informatiebeveiliging is continu

Effectieve beveiliging moet meetbaar zijn. Beleid, maatregelen en projecten moeten concreet bijdragen aan het bereiken van een passend beveiligingsniveau. Door frequente toetsing is steeds duidelijk of maatregelen, processen en procedures nog voldoen. Worden de doelstellingen gehaald en wordt de directie via rapportages voorzien van de juiste informatie? Deze resultaten zijn een basis voor aanpassingen, uitbreiding van de scope of het opstarten van nieuwe projecten. Effectief Beveiligen wordt hiermee een continu proces.

“Door frequente toetsing en beoordeling of maatregelen succesvol zijn wordt Effectief Beveiligen een continu proces”

Fase 5 Borgen

Organisaties zijn steeds in beweging en ook externe omstandigheden veranderen voortdurend. Om het beveiligingsniveau steeds af te stemmen op deze dynamiek is het noodzakelijk om de effectiviteit van genomen maatregelen goed te bewaken en te borgen.

Over Pinewood

Wij verenigen organisatorische en technische kennis en kunnen klanten op elk aspect van informatiebeveiliging ondersteunen. Met deze heldere methodiek helpen we organisaties verder, ongeacht het actuele beveiligingsvraagstuk of beveiligingsniveau. Onze activiteiten zijn flexibel en volledig afgestemd op de aanwezige kennis en ervaring binnen uw organisatie. Wij zijn adviseur of klankbord, maar kunnen organisaties ook volledig ontzien. Het resultaat is een effectieve beveiliging tegen verantwoorde investeringen.

Wilt u meer weten hoe Effectief Beveiligen uw organisatie kan helpen?
Kijk dan op www.pinewood.nl of neem contact op via 015-251 36 36.

PINEWOOD
Specialist in informatiebeveiliging

Pinewood bv
Delftechpark 57
2628 XJ Delft
T (015) 251 36 36
info@pinewood.nl
www.pinewood.nl