

Optimaliseer uw basisinfrastructuur

Dynamische IT voor Het Nieuwe Werken





Executive Summary

Doelgroep

Deze whitepaper is bestemd voor IT-directeuren, managers en medewerkers die verantwoordelijk zijn voor de basisinfrastructuur van hun organisatie, met inbegrip van servers, desktops, laptops en netwerken. Leidinggevendenden die de IT-activiteiten binnen hun organisatie aansturen en line-of-business managers die vertrouwen op IT-oplossingen bij het behalen van hun strategische doelen kunnen er ook hun voordeel mee doen.

Beoogde organisaties

Organisaties van iedere omvang kunnen positieve resultaten behalen uit de informatie en aanbevelingen in deze whitepaper.

Doelstelling

Deze whitepaper wil aangeven wat de voordelen zijn van het optimaliseren van uw basisinfrastructuur. En inzicht bieden over welke oplossingen op het gebied van basisinfrastructuur u nu het meeste voordeel zouden opleveren. Zodra u een idee hebt welke oplossingen de juiste zijn voor uw organisatie, hopen wij dat u contact opneemt met uw account manager bij Microsoft of met een Microsoft partner, om vervolgens een plan te ontwikkelen om uw basisinfrastructuur te optimaliseren. Deze whitepaper geeft ook een aantal aanbevelingen waar u kunt beginnen.

Abstract

IT-professionals staan onder steeds grotere druk om de strategische doelen van hun organisaties te ondersteunen. Tegelijkertijd hebben ze te maken met steeds complexer wordende IT. Infrastructuur optimalisatie biedt IT-manager een methodologie en routekaart om het actuele optimalisatieniveau van hun IT-infrastructuur te herkennen. En vervolgens de prioriteiten en projecten te bepalen die hen in staat zullen stellen om hun infrastructuur van een 'basic' niveau naar een 'dynamic' niveau te brengen. Gedurende dit proces kunnen organisaties verbeteringen aanbrengen in de volgende voorzieningen: Identity en Access Management, Desktop, Device and Server Management, Security en Networking, Data Protection en recovery en IT en Security Process.

In termen van basisinfrastructuur levert Microsoft oplossingen op vier belangrijke gebieden: server infrastructuur optimalisatie, branch infrastructuur optimalisatie, virtualisatie en desktop infrastructuur optimalisatie. Deze whitepaper geeft richtlijnen die helpen vaststellen welke oplossingsgebieden de beste resultaten behalen.



Inleiding

Nooit eerder hebben IT-afdelingen aan zoveel druk en verwachtingen moeten voldoen. In een steeds veranderende wereldmarkt zoeken bedrijven naar elke mogelijkheid om voordeel op hun concurrentie te kunnen behalen. En streven ze tegelijkertijd naar een grotere omzet, winst en klanttevredenheid. IT speelt een belangrijke rol bij deze pogingen.

Helaas hebben veel IT-afdelingen moeite te voldoen aan de verwachtingen die men van hen heeft als facilitators van strategische processen. Een van de redenen is dat veel IT-afdelingen vinden dat het grootste deel van hun tijd en budget opgaat aan onderhoud van wat er al is, in plaats van aan het ontwikkelen van nieuwe, strategische voorzieningen. En inderdaad: volgens de schattingen van veel analisten gaat 80% van het IT-budget op aan onderhoud. Een van de voornaamste factoren hiervoor is de complexiteit van IT.

De meeste IT-managers hebben te maken met meerdere desktop- en serveromgevingen. En met de integratie van oude en nieuwe systemen en workloads en verschillende point solutions die zijn geïmplementeerd om deze systemen te onderhouden en te beheren. Helaas voegen point solutions vaak een eigen complexiteit toe aan IT.

Het probleem wordt nog versterkt door de snelheid waarmee vandaag de dag veranderingen op de organisaties afkomen. Of het nu om bedrijven, overheden of non-profitsectoren gaat, technologische innovatie en wereldwijde concurrentie creëren samen met andere factoren een dynamische omgeving waarin het voor IT steeds moeilijker wordt om tijdig te voldoen aan steeds veranderende behoeften. Zodoende is het op één lijn brengen van de huidige bedrijfsbehoeften met de IT-prioriteiten een voortdurende bron van wrijvingen. Met als gevolg dat hoe minder flexibel een IT-organisatie is, des te groter is de kans dat zij uit de pas gaat lopen.

IT speelt een cruciale rol bij de pogingen van een bedrijf om de concurrentie voor te blijven en een grotere omzet, winst en klanttevredenheid te behalen

IT speelt een cruciale rol bij de pogingen van een bedrijf om de concurrentie voor te blijven en een grotere omzet, winst en klanttevredenheid te behalen.

Infrastructuur optimalisatie

Om aan deze uitdagingen tegemoet te komen, wenden toonaangevende bedrijven zich tot processen die hun infrastructuur bepalen. Ze bekijken ze in het licht van algemene IT-voorzieningen en plannen meerjarige verbeteringen die specifieke projecten omvatten om deze voorzieningen op een logische en geordende manier volwassener te maken. Het eindresultaat is een dynamische IT-omgeving. Als dit juist wordt gedaan, zorgt een dynamische IT-infrastructuur ervoor dat er betere resultaten worden behaald en dat er vertrouwen is dat IT bedrijfssuccessen mogelijk maakt.

Managers die de strategische waarde van een dynamische IT-infrastructuur erkennen, denken anders over de investeringen. Zij zoeken naar mogelijkheden om de complexiteit te verminderen, routinematige processen te automatiseren, en flexibiliteit te integreren in hun systeemresources. Zij begrijpen dat een interessante technologie of tool niets toevoegt als het niet kan worden geïntegreerd in de bestaande toolset voor systeembeheer. Zij beseffen dat het verlagen van de kosten een noodzakelijk doel is, maar dat het aanspreken van het potentieel bij kenniswerkers en het ondersteunen van concurrerende bedrijfsprocessen nóg meer waarde toevoegt aan een organisatie. En, misschien wel het meest belangrijk, managers in een dynamische IT-omgeving zien elke investering in de context van een systematische en gestructureerde vooruitgang. Dus niet noodzakelijkerwijs als doel op zichzelf, maar als een ontwikkeling naar meer flexibiliteit, efficiëntie en wendbaarheid.

Microsoft Infrastructuur optimalisatie is ontwikkeld met behulp van de best practices in de industrie en de ervaringen van Microsoft met haar zakelijke klanten. Het levert een methodologie waarmee u, Microsoft en de technologiepartners van Microsoft de technologische infrastructuur kunnen doorlichten en verbeteren. Het is gebaseerd op Gartner's Infrastructure Maturity Model en het Architecture Maturity Model dat is ontwikkeld aan het MIT (Massachusetts Institute of Technology). Infrastructuur optimalisatie geeft u de mogelijkheid om de actuele status van uw IT-infrastructuur te begrijpen, vervolgens te verbeteren, en tegelijkertijd de positieve effecten te ontdekken op het gebied van kosten, beveiliging, beschikbaarheid en wendbaarheid.

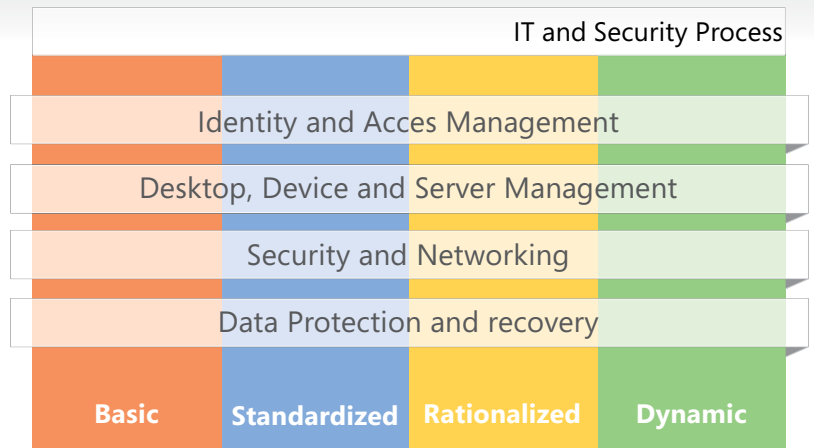
Om bedrijven - en in het bijzonder IT-managers en -werknemers - te helpen bij het bereiken van een dynamische IT-omgeving, heeft Microsoft een methodologie en raamwerk ontwikkeld waarmee u het optimalisatieniveau in uw IT-infrastructuur kunt verbeteren. Verscheidene aspecten van deze pogingen tot optimalisering richten zich op de basisinfrastructuur van een bedrijf, de productiviteitsinfrastructuur en het applicatieplatform.

Basisinfrastructuur optimalisatie

Basisinfrastructuur optimalisatie (Core IO) levert een uitgebreide, bewezen en efficiënte methodologie om infrastructuur te verbeteren. Basisinfrastructuur optimalisatie wordt ondersteund door een model dat toegang geeft tot technologie, services, tools en richtlijnen. Basisinfrastructuur optimalisatie kan ertoe bijdragen dat uw IT-kosten beheersbaar worden en uw bedrijf beter in staat is om IT-projecten succesvol te implementeren.

Model

Het basisinfrastructuur optimalisatiemodel stelt u in staat na te denken over de uitdagingen die zich voordoen, de gebieden te selecteren die u als eerste wilt verbeteren, en uw activiteiten te organiseren om die prioriteiten uit te voeren. Het model schetst een voortgang door vier fases van optimalisatie. En het illustreert de strategische waarde en zakelijke voordelen om zich van een 'basic' optimalisatiefase, waarin de infrastructuur algemeen beschouwd wordt als 'kostenpost', naar een 'dynamic' infrastructuur te begeven waarbij de bedrijfs-waarde van de infrastructuur duidelijk begrepen wordt en wordt gezien als een strategisch goed.



Voordelen van infrastructuur optimalisatie

Basisinfrastructuur optimalisatie van Microsoft is ontworpen om IT-kosten te beheersen, beveiliging en beschikbaarheid te verbeteren, en flexibiliteit te vergroten zodat klanten als u minder tijd en geld kwijt zijn aan onderhoud en meer tijd kunnen besteden aan het ontwikkelen en faciliteren van nieuwe voorzieningen en services die het bedrijf vooruithelpen.

Voordelen van optimalisatie van uw basisinfrastructuur zijn onder andere:

<p>Kostenbeheersing</p> <p>hogere volwassenheidsfasen kunnen besparingen opleveren tot 80% op arbeidskosten in IT</p>	<p>Betere beveiliging en beschikbaarheid</p> <p>een geoptimaliseerde basisinfrastructuur kan leiden tot meer bedrijfscontinuïteit, verbeterde compliance en betere, meer beveiligde toegang tot netwerkresources</p>	<p>Meer wendbaarheid</p> <p>organisaties kunnen aanzienlijke verbeteringen behalen bij het leveren van sneller reagerende IT-services en de wendbaarheid vergroten</p>
--	---	---



Wat kunt u verwachten van een geoptimaliseerde infrastructuur?

IT is een strategische enabler en staat aan de basis van de voorsprong op de concurrentie

- Gebruik van resources wordt geoptimaliseerd en uw IT-afdeling zal de noodzakelijke voorzieningen kunnen leveren binnen de beperkingen van budget en menskracht.
- Bedrijfsbehoeften kunnen proactief worden aangepakt en opgelost.
- IT is flexibeler kan beter reageren op wijzigingen. Het zal daardoor sneller schaalbaar zijn en eerder nieuwe resources kunnen leveren zodra de vraag toeneemt.

Beveiligingsdreigingen zijn beheersbaar en condition monitoring voorkomt uitval up-to-date

- Beveiligingsbeheer is geïntegreerd in desktops, servers en netwerken; schendingen zijn zeldzaam en onder controle.
- Het aanbrengen van beveiligingspatches door de hele organisatie wordt gestroomlijnd en gebeurt bijna in realtime.
- Automatisering maakt patch-timing mogelijk op basis van urgentie en load-balancing vereisten.

Belangrijke software-implementaties worden gestroomlijnd en applicaties blijven

- Softwaredistributie is in hoge mate geautomatiseerd. Preproductie testen zijn gereduceerd.
- Updates worden centraal beheerd en conformiteit is verzekerd.
- IT heeft goed inzicht in het gebruik van softwarelicenties en is in staat toekomstige behoeften nauwkeurig te voorspellen.

Compliance met IT-beleid is automatisch, uniform en zelf-documenterend

- Configuraties van desktops en servers worden gecontroleerd waardoor ze minder kwetsbaar zijn voor veiligheidsschendingen en helpdesks minder vragen te verwerken krijgen.
- Vertrouwelijke gegevens worden beschermd.
- Compliance aan regelgeving is robuust en gestroomlijnd.

Business-units zien IT als een gewaardeerde partner

- Kosten zijn lager en beter te beargumenteren. Betere planning en beheer leiden tot beter gebruik van resources.
- Downtime komt minder voor en duurt korter.
- IT en business staan op één lijn en werken proactief samen.

Het vaststellen van uw behoefte aan infrastructuur optimalisatie

Wanneer weet u dat uw IT-infrastructuur serieus aandacht nodig heeft? Over het algemeen is dat eenvoudig zichtbaar: IT draait inefficiënt, projecten zijn reactief. Op het oog lijkt de beveiliging prima in orde maar toch zijn er regelmatig problemen die voor onrust zorgen. De omgeving is moeilijk te controleren. Kosten zijn hoog en interne klanten raken gefrustreerd door de slechte service en trage reacties.

Kenmerken van organisaties die behoefte hebben aan infrastructuur optimalisatie zijn:

Complexe infrastructuur en beheerprocessen

- Hoge kosten voor het leveren van de meest basale IT-voorzieningen.
- Weinig controle over client-computerconfiguraties.
- Alle vestigingen bevinden zich in hun eigen bunker en vereisen ieder hun eigen IT-resources.

Infrastructuur kan de veranderende bedrijfsbehoefte niet bijhouden

- Vraagpieken veroorzaken service-onderbrekingen.
- Verhogingen in kosten van hulpprogramma's treffen de basis IT-voorzieningen.
- Kansen voor het bedrijf worden gemist en managers zijn gefrustreerd door IT.

IT overbelast door routinetaken en het 'blussen van vuurtjes'

- Reactieve houding ten opzichte van beveiligingsdreigingen, gericht op opruimen en niet op preventie.
- Frequente service-onderbrekingen.
- Beveiligingsbeheer is moeizaam en inconsistent.

Implementaties zijn langdurig of worden niet uitgevoerd

- Resources zijn lang buiten bedrijf, zowel gedurende de voorbereiding als tijdens de uitrol.
- Beveiligings- en softwareupdates gebeuren handmatig, langzaam en onregelmatig.
- Nieuwe voorzieningen worden vertraagd en benadelen zo het concurrentievermogen.

Compliance met beveiligings- en overheidswetgeving inconsistent

- Beveiligingswaarschuwingen en -bedreigingen onderbreken normale activiteiten.
- Backup en herstel gebeurt onregelmatig en is onbetrouwbaar.
- E-mail postvakken stromen over van de spam.

Organisaties die hun basisinfrastructuur nog niet hebben geoptimaliseerd worstelen met beheerproblemen. Vaak stapelen de problemen zich op als verbeteringsprojecten worden toegepast die de wortels van het kwaad niet kunnen aanpakken vanwege inefficiency en slechte prestaties. Deze basisoorzaken zijn over het algemeen de complexiteit van het systeem en verouderde, arbeidsintensieve processen.

Tegelijkertijd ondernemen veel bedrijven projecten ter ondersteuning van belangrijke bedrijfsprocessen. Maar hun onderliggende technische infrastructuur is niet in staat deze nieuwe voorzieningen te verwerken. Zo worden de beloofde voordelen nooit behaald, of alleen behaald tegen aanzienlijke kosten.



Het infrastructuur optimalisatiemodel gebruiken

Deelnemen aan een infrastructuur optimalisatie reis betekent committeren aan een proces, maar niet noodzakelijkerwijs aan één leverancier of technologieplatform. Terwijl de infrastructuur optimalisatiemodellen korte termijn projecten kunnen helpen identificeren die hiaten zullen dichten en actuele problemen zullen verlichten, kan het bouwen van een lange termijn verbeteringsplan een infrastructuur garanderen die zich aanpast aan de behoeften van het bedrijf, waarde behaalt uit voorgaande IT-investeringen, en een robuust platform levert waarop LOB- en kenniswerkerapplicaties kunnen worden gebouwd.

De Infrastructuur optimalisatiemodellen zijn tools waarmee prioriteiten voor IT kunnen worden vastgesteld. Waarmee over een periode van een aantal jaren een effectieve reisroute kan worden uitgestippeld naar een dynamische IT-omgeving. Een succesvol gebruik van de modellen houdt het nemen van een paar basisstappen in, ondersteund door een uitgebreide interne beoordeling door uw IT-team. Microsoft en haar partners hebben een uitgebreide ervaring in het begeleiden van organisaties door deze processen en vormen een grote bron van informatie.

STAP 1 Bepaal op welk punt u zich bevindt

Breng de technologieën, processen en het beleid in kaart die van toepassing zijn op uw desktops, datacenters en netwerkinfrastructuur. Bestudeer specifieke voorzieningen en leg vast waar uw organisatie zich bevindt in termen van volwassenheidsfasen. Als u uw IT-volwassenheid voor elk van de voorzieningen vastlegt, dient u in het bijzonder aandacht te besteden aan projecten die zijn gebouwd op een zachte ondergrond. Zorg dat u geen geavanceerde voorzieningen bouwt op zwakke basisvoorzieningen, die eigenlijk al vervangen hadden moeten worden voordat u de geavanceerde voorzieningen ging implementeren. En misschien moet u projecten die ieder apart prima in orde leken heroverwegen of annuleren, wanneer ze niet voldoen aan uw huidige situatie.

STAP 2 Bepaal uw doel en stippel een verbeteringsplan voor de lange termijn uit

Terwijl de meeste organisaties een dynamische situatie nastreven, is het voor sommige industrieën juist zinvol om zich uitsluitend te richten op kostenoptimalisatie. De volgende stap in het proces is het vaststellen van de juiste richting voor uw organisatie. Een van de meest waardevolle aspecten van de infrastructuur optimalisatiemodellen is hun ondersteuning van meerjarige plannen. Het aanwijzen van korte termijnprojecten die een basis leggen en lange termijn initiatieven die de concurrentiepositie van bedrijven verbeteren, leveren een roadmap voor budgetplanning, resource-toewijzing en de zekerheid van business buy in. Deze benadering zorgt er ook voor dat uw verbeteringsprojecten uitgebalanceerd zijn en dat noodzakelijke integratiepunten worden herkend en aangepakt.

STAP 3 Implementeer de juiste high-impact projecten om vooruit te komen in het model

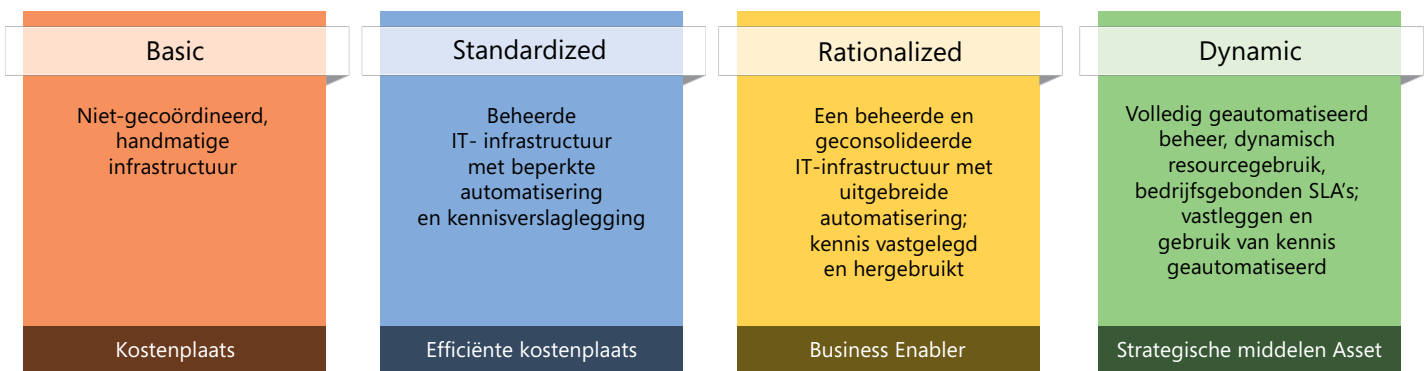
Er zullen ongetwijfeld meer tekortkomingen en hiaten zijn dan u binnen één budgetjaar kunt aanpakken. Dat is prima. Infrastructuur optimalisatie is ontworpen om u te helpen de projecten die u oppakt op een logische manier en op basis van prioriteit af te handelen. Identificeer de tekortkomingen in uw infrastructuur met de volgende kenmerken:

- Bepaalde voorzieningen hebben een belangrijke achterstand in volwassenheid ten opzichte van andere.
- Een cruciale voorziening die de basis kan vormen voor concurrerend vermogen of differentiatie ontbreekt of is niet volledig ontwikkeld.
- Toekomstige oplossingen zijn op bepaalde onderdelen afhankelijk van voorzieningen die nog niet zijn geïmplementeerd.

Het beheren van de specifieke projecten in de context van een dynamische IT-visie plaatst het werk van de IT-organisatie in een wereld die het financieel- en bedrijfsmanagement verstaat en waardeert. Om de stappen 1 en 2 te voltooien, kan het handig zijn om de beschrijvingen van de verschillende volwassenheidsfasen te beoordelen om te zien welke uw huidige situatie het beste beschrijft (stap 1). Door deze beschrijvingen te beoordelen kunt u ook beslissen welke kant u op wilt (stap 2).

Volwassenheidsfasen

Infrastructuur optimalisatie stelt de volwassenheidsfasen vast van elke IT-voorziening, uitgaand van uw huidige technologieën en processen. Het is ook nuttig bij het identificeren en prioriteren van verbeteringspogingen. Ongeacht de IT-voorziening waar u zich op richt, kunt u uw bedrijf naar een dynamische IT-situatie voeren. De volwassenheidsfasen zijn 'basic', 'standardized', 'rationalized' en 'dynamic'.



Basic

De fase 'basic' binnen infrastructuur optimalisatie wordt gekenmerkt door handmatige, lokale processen met een minimum aan gecentraliseerd beheer:

- IT governance is verwaarloosbaar aangezien er geen beleid is op het gebied van beveiliging en compliance. Of omdat het beleid inconsistent is in de uitvoering.
- Kennis van de algehele gezondheid van de applicaties en services ontbreekt door een gebrek aan tools en resources.
- Binnen IT is er geen medium voor het delen van de opgebouwde kennis.
- De omgeving is moeilijk te controleren voor IT en kent hoge kosten voor desktop- en serverbeheer. IT is vaak reactief met betrekking tot beveiligingsdreigingen.
- Software-implementaties, beveiligingsupdates en services gaan gepaard met veel handelingen en hoge kosten.

Standardized

De fase 'standardized' binnen infrastructuur optimalisatie introduceert controles via standaarden en beleid voor het beheer van desktops, mobiele apparaten en servers:

- Er wordt een geïntegreerde directory service gebruikt bij het beheer van resources, veiligheidsbeleid en netwerktoegang.
- Organisaties erkennen de waarde van basisstandaarden en –beleid maar hebben deze nog niet geïmplementeerd binnen de gehele infrastructuur.
- Over het algemeen worden alle software-implementaties, software updates en desktopservices pas geleverd als de eindgebruiker daar het initiatief voor neemt.

- Voorraadbeheer van hardware en software vindt plaats op basis van een redelijk proces en licentiegebruik wordt onregelmatig beheerd.
- Beveiliging is verbeterd met een locked-down perimeter, maar de interne beveiliging heeft nog wel enige verbetering.

Rationalized

De fase 'rationalized' binnen infrastructuur optimalisatie kenmerkt zich door lage beheerkosten van desktops en servers, en een geoptimaliseerd beleid.

- Beveiliging is proactief en de reactie op bedreigingen is snel en gecontroleerd.
- Het gebruik van zero-touch implementatie minimaliseert de kosten, reduceert de implementatietijd, en vermindert het aantal technische uitdagingen.
- Het proces om desktops te beheren is zeer low-touch en het aantal images is minimaal.
- Er is accuraat voorraadbeheer van hardware en software en er worden alleen licenties en computers gekocht die nodig zijn.
- Beveiligingsmaatregelen omvatten strikte regels en controle, van desktops tot servers en van firewall tot extranet.

Dynamic

Als een organisatie een dynamische fase van infrastructuur optimalisatie bereikt, wordt IT een strategische enabler die ervoor zorgt dat het bedrijf de concurrentie voorblijft:

- De kosten zijn volledig onder controle en er bestaat uitwisseling tussen gebruikers en informatie, desktops en servers.
- Gebruikers van mobiele apparaten kunnen gebruik maken van bijna dezelfde services en voorzieningen als op kantoor.
- Processen zijn volledig geautomatiseerd en vaak ingebed in de technologie zelf zodat IT beheerd wordt op basis van de bedrijfsbehoeften.
- Aanvullende investeringen in technologie leveren specifieke, directe en meetbare bedrijfsvoordelen op.
- Door middel van zelfvoorzienende software en quarantaineachtige systemen wordt beheer van software-updates en compliance uitgevoerd volgens vastgestelde beveiligingsregels.

Basisinfrastructuur optimalisatievoorzieningen

De voorzieningen binnen het basisinfrastructuur optimalisatiemodel zijn als volgt. Meer gedetailleerde beschrijvingen kunt u vinden in de bijlage.

Identity and Access Management

Identity and Access Management omvat de administratie van mensen en middelen. Zoals toegang tot resources door mobiele werknemers, klanten en partners buiten de firewall. En oplossingen die moeten worden geïmplementeerd om identiteitsgegevens als synchronisatie, wachtwoordbeheer en gebruikers provisioning te beheren en te beschermen.

Desktop, Device and Server Management

Desktop, Device and Server Management omvat het beheer van desktops, mobiele apparaten en servers, met inbegrip van planning en implementatie van patches, besturingssystemen en applicaties binnen het gehele netwerk. Daarnaast levert het richtlijnen over hoe u virtualisatie en branch office technologieën kunt gebruiken om uw IT-infrastructuur te verbeteren.

Security and Networking

Security and Networking omvat de bescherming van informatie en communicatie, met inbegrip van waarborgen tegen ongeautoriseerde toegang. Tegelijkertijd richt Security and Networking zich op oplossingen die de IT-infrastructuur beschermen tegen denial-aanvallen en virussen zonder de toegang tot bedrijfsresources te verliezen.

Data Protection and Recovery

Data Protection and Recovery omvat de processen en tools die IT gebruikt voor backups en het opslaan en terugzetten van informatie en applicaties. Aangezien informatie zich vermenigvuldigt, staan organisaties onder steeds grotere druk om die informatie te beveiligen en, indien nodig, een kosteneffectieve en tijdsbesparende wijze van herstel te bieden.

IT and Security Process

IT and Security Process levert richtlijnen op basis van best practices in de industrie. Dit omvat het op de juiste manier bekostigen van het ontwerpen, ontwikkelen, gebruiken en ondersteunen van oplossingen. En tegelijkertijd het streven naar een hoge mate van betrouwbaarheid, beschikbaarheid en beveiliging. Hoewel krachtige technologie noodzakelijk is om tegemoet te komen aan de behoefte van bedrijven aan betrouwbare, beschikbare en uitermate veilige IT-diensten, is technologie alléén niet voldoende. Uitmuntende processen en getraind personeel met duidelijk afgebakende rolverdelingen en verantwoordelijkheden zijn ook noodzakelijk.



Microsoft heeft een aantal oplossingen op het gebied van basisinfrastructuur vastgesteld waarop bedrijven die de waarde van hun IT-investeringen willen maximaliseren zich kunnen richten.

Desktopinfrastructuur

Verander uw desktopinfrastructuur van een kostenplaats in een strategisch goed door snelle, betrouwbare en uiterst beveiligde desktop-oplossingen te bieden



Serverinfrastructuur

Beheers de kosten van uw serverinfrastructuur, verbeter de serviceniveaus en streef flexibiliteit na met geïntegreerde oplossingen voor serverbeheer, beveiliging en identiteitsbeheer



Het Nieuwe Werken



Branch Infrastructuur

Beheers de kosten door het verminderen van on-site ondersteuningsvereisten, verhoog het gebruik van hardware en bandbreedte en vereenvoudig backup en herstel



Geïntegreerde virtualisatie

Streef een grotere efficiëntie na via geïntegreerde end-to-end virtualisatie en verlaag tegelijkertijd de kosten, maximaliseer de systeembeschikbaarheid en streef naar operationele flexibiliteit

Server infrastructuur optimalisatie

Beheers de kosten van uw serverinfrastructuur, versterk beveiliging en compliance. En streef naar flexibiliteit bij geïntegreerde oplossingen voor datacenterbeheer, secure messaging en samenwerking, en bescherming van informatie en beveiligde toegang.

U kunt geïntegreerde Microsoft-technologieën gebruiken om het beheer en de beveiliging van uw serverinfrastructuur te optimaliseren. Bedrijven hebben meer CPU-kracht nodig om overeind te blijven in de huidige digitale marktplaats. Tegelijkertijd ondergaat de servertechnologie een snelle verandering met innovaties in virtualisatie, clustering en serverconsolidatie. En dat leidt vaak tot een grotere systeemcomplexiteit. In deze omgeving ontwikkelen succesvolle bedrijven hun serverinfrastructuur van een kostenplaats tot een strategisch goed, en creëren daarmee een flexibeler IT-omgeving met verbeterde serviceniveaus en lagere totale kosten van eigendom (TCO). Het basisinfrastructuur optimalisatiemodel biedt best practices en specifieke projecten om bedrijven te helpen bij het ontwikkelen van hun visie op geoptimaliseerde servers. Een visie die leidt tot beheersbare kosten, verbeterde beveiliging en beschikbaarheid, en meer flexibiliteit.

Virtualisatie

Virtualisatietechnologieën werken door de hele infrastructuur heen en leveren gedeelde en flexibele resources. Voor servers kan bijvoorbeeld virtualisatie worden gebruikt om meerdere besturingssystemen tegelijkertijd op dezelfde fysieke server te laten draaien, waarbij elk besturingssysteem toch werkt als zelfstandige computer. Microsoft levert een krachtige set technologieën en richtlijnen ter ondersteuning van omvangrijke virtualisatie binnen server workloads en desktopapplicaties. Waardoor IT virtuele en fysieke servers kan beheren in een vertrouwde en geïntegreerde omgeving waarin de complexiteit van systemen is verminderd en de operationele efficiëntie verbeterd. Een IT-infrastructuur die is gebouwd met virtualisatie- en beheertechnologie van Microsoft, geeft bedrijven de mogelijkheid om dynamisch serverresources toe te wijzen, workloads te leveren via gestroomlijnde processen, beschikbaarheid gedurende geplande en niet-geplande downtime zo veel mogelijk te verbeteren, een krachtig disaster-recovery proces te garanderen, en een optimaal gebruik van resources na te streven. Door het beheer van virtuele workloads te integreren met het beheer van fysieke servers en de desktopinfrastructuur, kunnen IT-afdelingen de kostenbesparingen van serverconsolidatie onder controle brengen en tegelijkertijd de complexiteit van systemen verminderen.

Branch infrastructuur optimalisatie

Voor IT-beslissers die een omvangrijke of complexe branch infrastructuur beheren, levert Microsoft een infrastructurele oplossing die is gebaseerd op het meest recente Windows® besturingssysteem. Hiermee kunt u besparen op IT-kosten, de beveiliging en beschikbaarheid van uw IT-resources verbeteren, en de flexibiliteit van uw bedrijf vergroten. Deze voordelen gaan verder dan het beheer en de beveiliging van branch datacenters via gecentraliseerde en gedistribueerde oplossingen voor de branche infrastructuur.

Effectieve branch oplossingen reduceren de noodzaak voor u om IT naar elke locatie te sturen voor implementaties en assistentie. Bovendien kan hierdoor de hoeveelheid IT-hardware in de verschillende vestigingen worden geconsolideerd. Het opslaan van informatie bij de vestigingen kan worden geautomatiseerd en gecentraliseerd, daarbij kan de netwerkefficiëntie worden gemaximaliseerd. Geïntegreerd en uitgebreid beveiligingsbeheer zorgt ervoor dat de vestigingen eenzelfde niveau van beveiliging hebben als het hoofdkantoor. U kunt applicaties binnen het netwerk met een muisklik uitrollen of wijzigen met behulp van vertrouwde oplossingen die gebaseerd zijn op de bestaande Windows-omgeving. Hierdoor krijgen werknemers in de vestigingen dezelfde IT-voorzieningen als de werknemers op het hoofdkantoor.

Desktop infrastructuur optimalisatie

Desktop infrastructuur optimalisatie stelt u in staat de complexiteit van uw desktop infrastructuur te verminderen om implementaties te versnellen, het beheer te stroomlijnen, en de beveiliging te vergroten.

Factoren als globalisatie, mobiliteit en beveiligingsdreigingen zorgen voor ongekende eisen aan de IT-afdelingen bij het leveren van een geoptimaliseerde desktopinfrastructuur. Succesvolle bedrijven komen aan deze eisen tegemoet door hun desktop infrastructuur te ontwikkelen van kostenplaats tot strategisch goed. Terwijl tegelijkertijd de TCO wordt verlaagd en de serviceniveaus en flexibiliteit van de organisatie worden verbeterd. Het basisinfrastructuur optimalisatiemodel biedt best practices en specifieke projecten om bedrijven vooruit te helpen naar deze geoptimaliseerde desktopstatus en belicht specifieke oplossingen voor PC Lifecycle Planning, Standard Image Deployment, Desktop Virtualization, Automation van IT-beheer en Comprehensive Security. Extra voordelen zijn grotere uptime van het systeem, hogere productiviteit van de eindgebruiker, betere bescherming van bedrijfsinformatie, en eenvoudiger IT-compliance.

Bepalen welk oplossingsgebied de voorkeur krijgt

Stel uzelf de volgende vragen wanneer u bepaalt op welk gebied u zich als eerste gaat richten:

Ervaart u problemen met laag servergebruik, "server sprawl", hoge kosten voor het datacenter, Server & Virtualisatie complexiteit van het datacenter en dergelijke?	→	Server & Virtualisatie
Wilt u het aantal desktop images in uw organisatie verminderen, desktopconfiguraties desktop centraal beheren via groepsbeleid of implementaties en upgrades stroomlijnen?	→	Desktop
Wilt u de beveiliging en beschikbaarheid van uw messaging- of samenwerkingsomgevingen verbeteren?	→	Server
Hebt u een groeiend aantal directories om toegang tot netwerkresources te beheren? Weet u zeker dat de juiste personen toegang hebben tot de informatie die ze nodig hebben en dat de overigen hiervan zijn afgesloten?	→	Server
Wilt u een beheeroplossing implementeren voor het monitoren van cruciale servers?	→	Server
Wilt u de mogelijkheid hebben de beveiliging van externe toegang tot interne systemen te automatiseren door identiteiten te federaten over bedrijfsgrenzen heen, synchronisatie te automatiseren, provisioning en deprovisioning van digital identiteiten binnen bedrijfssystemen en LOB-applicaties door een uitgebreide, identity lifecycle-beheeroplossing te implementeren?	→	Server
Wilt u de netwerkbeveiliging kunnen controleren op beleidsniveau met actuele, geïntegreerde weergaves van de beveiligingsstatus van het totale netwerk, inclusief de mogelijkheid om in te zoomen?	→	Server
Voelt u de noodzaak om de beveiliging te verhogen voor specifieke serverapplicaties (zoals Exchange Server, SharePoint® Server en instant messaging) met geïntegreerde, tuned, multi-engine, anti-malware beveiligingsoplossingen die worden beheerd en bijgewerkt vanaf een console?	→	Server
Wilt u uw gebruikers in staat stellen vertrouwelijke e-mails te beschermen, toegang tot bepaalde documenten af te schermen en gevoelige content te beveiligen?	→	Server
Wilt u beveiligde toegang vanaf elke plek mogelijk maken om zodoende applicaties en gegevens te beschermen en bedrijfswaarde toegankelijk te maken in de serverinfrastructuur?	→	Server
Wilt u alleen beveiligde en geautoriseerde toegang tot netwerken en applicaties toestaan via een end-to-end oplossing met netwerk-perimeter bescherming en krachtig authenticatie- en identiteitsbeheer?	→	Server
Wilt u geïntegreerde end-to-end virtualisatie implementeren voor het test- en productie virtualisatieworkloads? Wilt u workloads consolideren om implementatie te stroomlijnen?	→	Virtualisatie
Wilt u de systeemcomplexiteit verminderen door uw virtuele en fysieke serverinfrastructuur te beheren via een gedeelde console en de provisioning stroomlijnen tussen fysieke en virtuele servers?	→	Virtualisatie
Wilt u de servers kunnen monitoren in uw vestigingen vanuit een centrale locatie, reageren op foutberichten, problemen met afdrucken en bestanden oplossen en problemen voorkomen voor ze uw bedrijfsvoering in gevaar brengen?	→	Vestiging
Vindt u het moeilijk een evenwicht te vinden tussen de behoeften van de werknemers in de dochterbedrijven en de behoefte aan centraal beheerde IT-resources?	→	Vestiging



Een technologiepartner en ondersteuning kiezen

Hoewel u waarschijnlijk aanzienlijke voordelen zult behalen door het implementeren van oplossingen voor hierboven genoemde oplossingsgebieden zult u - net als de meeste bedrijven en technologieprofessionals - over een beperkt budget en resources beschikken. Bovendien is uw huidige infrastructuur op een aantal gebieden misschien al meer geoptimaliseerd dan u denkt en op andere gebieden misschien nog niet geoptimaliseerd genoeg. Als gevolg hiervan zult u op de korte termijn het meeste voordeel behalen door u eerst te beperken tot één oplossingsgebied. Zodra u een gebied hebt gekozen waarop u zich wilt richten, dient u eerst te overwegen met welke technologiepartners en technologieën u wilt gaan werken en hoe die u kunnen helpen bij het optimaliseren van uw infrastructuur

Microsoft is uw technologiepartner

Microsoft is erop gericht de werknemers van organisaties als de uwe de mogelijkheden te geven om hun bedrijf verder te helpen. Van begin af aan is het ons doel geweest software te leveren die mensen in staat stelt hun creativiteit, fantasie en denkracht te gebruiken. Door de jaren heen heeft Microsoft die visie verder uitgedragen. We bieden oplossingen aan mensen die zelfstandig werken, maar ook aan dynamische teams en aan organisaties met een geografisch verspreid werknemersbestand. Deze enterprise-ready oplossingen behelzen niet alleen software maar ook best practices, richtlijnen en implementatiediensten zodat u een oplossing snel en tegen lage kosten en weinig risico succesvol kunt implementeren. Met de laatste golf aan innovaties is het nu de ideale tijd om te evalueren hoe de infrastructuuroplösungen van Microsoft uw organisatie het beste kunnen dienen. Microsoft blijft erop gericht u te helpen bij het behalen van de meeste waarde uit uw IT-investeringen en bij het bieden van nieuwe mogelijkheden.

Microsoft biedt zijn klanten een uniek voorstel:

- Onze software is vertrouwd en betrouwbaar
- Onze oplossingen zijn geïntegreerd en compleet
- Onze software is ontworpen om samen te werken met andere software



Aanbevolen acties en volgende stappen

U dient de volgende handelingen te overwegen bij het verbeteren van de optimalisatie van uw basisinfrastructuur:

- 1** Werk samen met uw Microsoft partner, als u dit al niet gedaan hebt, bij het vaststellen van de huidige volwassenheidsfase van uw basisinfrastructuur.
- 2** Beoordeel de beschrijvingen van elk van de oplossingsgebieden zoals ze staan beschreven in dit document. En beslis welk gebied momenteel voor uw bedrijf het meeste voordeel zou bieden. Identificeer op basis van uw huidige volwassenheidsfase van de infrastructuur welke technologieprioriteiten en verwante projecten u kunnen helpen bij het verbeteren van uw basisinfrastructuur. Welke oplossing nu het meest waardevol is voor uw organisatie.
- 3** En tenslotte, heb vertrouwen! De projecten en methodes die zijn ontworpen door de technisch specialisten bij Microsoft zijn in de dagelijkse praktijk uitgebreid getest en verbeterd. U kunt erop vertrouwen dat u bij het optimaliseren van uw infrastructuur uw IT-kosten kunt beheersen, de beveiliging en beschikbaarheid van uw infrastructuur kunt verbeteren, en de flexibiliteit van uw organisatie kunt vergroten.

Bijlage

Volwassenheidsfases van basisinfrastructuur optimalisatievoorzieningen

Niet alleen helpt het basisinfrastructuur optimalisatiemodel u bij het vaststellen van uw volwassenheidsfase, het categoriseert ook de verschillende aspecten van uw basisinfrastructuur waarop u uw aandacht moet richten. Deze aspecten, oftewel "voorzieningen", richten zich op de kerncomponenten van de basisinfrastructuur van een bedrijf. Hieronder volgen de gedetailleerde beschrijvingen van elke volwassenheidsfase voor iedere voorziening in de basisinfrastructuur optimalisatie.

Identity and Access Management

Identity and Access Management omvat de administratie van mensen en middelen. Zoals toegang tot resources door mobiele werknemers en klanten en partners buiten de firewall. En oplossingen die moeten worden geïmplementeerd om identiteitsgegevens als synchronisatie, wachtwoordbeheer en gebruikersprovisioning te beheren en te beschermen.

Basic

Een basic Identity and Access Management infrastructuur wordt gekenmerkt door onverschillig of inconsistent IT-beleid en -standaarden met betrekking tot authenticatie en beveiliging. Gebruikers kunnen zelfs per systeem andere digitale ID's hebben. Het komt regelmatig voor dat er geen tools voor geïntegreerde servergebaseerde identiteit of toegangsbeheer zijn en dat er geen directoryservices zijn geïmplementeerd om de meeste gebruikers te authenticeren. Het gebruik van wachtwoorden is beperkt of inconsistent en er bestaat geen consistent proces voor het toewijzen van toegang tot resources. In feite bestaat er nauwelijks enige bescherming tegen ongeautoriseerde toegang tot gevoelige gegevens. Administratieve rechten zijn slecht geregeld en de meeste gebruikers werken standaard als "administrator". Hierdoor zijn netwerken kwetsbaar voor malware en neemt de TCO toe omdat gebruikers ongeautoriseerde systeemwijzigingen kunnen aanbrengen. Dit is van invloed op IT en in het bijzonder op de helpdesk.

Organisaties in deze fase kunnen problemen ondervinden bij het voldoen aan overheidswetgeving en zullen een drukbezochte helpdesk hebben.

Standardized

Organisaties in deze fase gebruiken Active Directory® alleen voor authenticatie. Gebruikers hebben eenvoudig toegang tot het niveau "administrator" en beveiligingssjablonen worden toegepast op standaardimages. De hoeveelheid digitale identiteiten is lager en de helpdesk heeft het minder druk, maar er zijn geen voorzorgsmaatregelen voor het toewijzen van resources aan specifieke gebruikers. Desktops zijn niet onderhevig aan groepsbeleid.

Rationalized

In deze fase gebruiken bedrijven directorytools om desktop- en serverconfiguraties en beveiliging te beheren. In deze fase hebben bedrijven ook oplossingen geïnstalleerd om informatie te beschermen. Ze hebben op rollen gebaseerd beheer geïmplementeerd en stellen een platform vast voor het implementeren van compliance aan wetgeving. Deze organisaties zijn in staat om gebruikerssystemen en gegevens te herstellen na gebruikersfouten, stroomuitval en technische onderbrekingen.

Dynamic

In een dynamische fase van Identity and Access Management wordt gebruikers-provisioning centraal beheerd vanuit heterogene systemen. Dynamische organisaties gebruiken federated identiteitsbeheer.

Desktop, Device and Server Management

Desktop, Device and Server Management omvat het beheer van desktops, mobiele apparaten en servers. Het omvat de planning en implementatie van patches, besturingsystemen en applicaties binnen het gehele netwerk. Daarnaast levert het richtlijnen over hoe u virtualisatie en branch office technologie kunt gebruiken om uw IT-infrastructuur te verbeteren.

Basic

Er zijn geen desktopstandaarden voor hardware, besturingsystemen of applicaties in de basic fase van Desktop, Device and Server Management. Automatisch patch-beheer komt zelden voor. Organisaties bezitten nog geen desktop image strategieën om gebruikersproductiviteit te optimaliseren door consistent gebruik van actuele software. Het beheren van meerdere desktops is moeilijk en gebruikers ervaren regelmatig technische onderbrekingen. Servers worden niet gemonitord. Een gebrek aan provisioning van mobiele apparaten betekent dat deze organisaties geen overzicht hebben van hun mobiele applicaties of van hun implementatie-ondersteuning. Er wordt veel naar de helpdesk gebeld en er zijn lange wachttijden voordat problemen worden opgelost.

Standardized

In deze fase hebben organisaties een begin gemaakt met het vereenvoudigen van Desktop Device en Server Management. Dit gaat via automatisch patch-beheer en een gespecificeerde set aan standaard desktop- en serverimages. Desktop image strategieën zijn gebaseerd op images die het besturingssysteem, antivirus software, beheertools, productiviteitssuites (zoals Microsoft Office system) en LOB-applicaties bevatten. Deze organisaties hebben een consistent plan voor het beheer van 80% van hun desktops maar voeren nog geen compatibiliteitstesten uit om vast te stellen of iedere applicatie correct draait voordat deze overal wordt geïmplementeerd. Ze hebben een geconsolideerd en vereenvoudigd beheer voor 80% van hun testomgevingen en gebruiken monitoringoplossingen voor 80% of meer van hun cruciale servers. Niet alleen leveren ze beveiligingsregels met inbegrip van het gebruik van PIN's om ongeautoriseerde toegang tot mobiele apparaten tegen te gaan, maar ze hebben ook policy-enforcement tools als remote wipe. Ze hebben maatregelen achter de hand voor zowel mobiele apparaten als niet-pc's.

Rationalized

Organisaties in de volwassenheidsfase Rationalized voor Desktop, Device and Server Management, gebruiken het Windows Vista® besturingssysteem, Windows XP Service Pack 2 (SP2) of Windows 2000 als het primaire besturingssysteem voor de desktops om patchbeheer te vereenvoudigen. De installatie van de image van hun besturingssysteem op de desktops hebben zij geautomatiseerd. Op serverniveau is de software distributie voor 80% van hun desktops (zowel fysiek als virtueel) geautomatiseerd. Geautomatiseerd beheer en tracering van hardware en software geeft de IT managers een overzicht van de bezittingen van het bedrijf en waar ze zich bevinden. Deze organisaties gebruiken virtualisatie en gecentraliseerde beheertools om netwerk servers, services en printers in zowel het centrale netwerk als in de vestigingen eenvoudig te beheren. Ze hebben een consistent plan voor het beheer van hun besturingsystemen en ze hebben een oplossing om de compatibiliteit van applicaties te testen. Service-level agreement (SLA) monitoring van cruciale servers, met inbegrip van IT-serviceniveaurapportage, houdt in dat netwerkproblemen worden gevonden, gediagnosticeerd en gerepareerd voor ze downtime kunnen veroorzaken. Certificaat provisioning en autorisatie van mobiele apparaten vereenvoudigt het apparaatbeheer. Het gebruik van 802.1x certificaten helpt bedrijven bij het beschermen en controleren van toegang tot netwerkresources via een betere draadloze beveiliging dan de traditionele WEP of non-secured netwerken.

Organisaties kunnen thin-client webapplicaties leveren op mobiele apparaten via Wireless Application Protocol (WAP) of Hypertext Transfer Protocol (HTTP) zodat mobiele werkers toegang hebben tot bedrijfsinformatie. De beveiliging en stabiliteit van desktop- en mobiele omgevingen is consistent, zowel binnen als buiten de firewall.

Dynamic

Bedrijven die een fase van dynamische IT hebben bereikt, gebruiken een oplossing voor capaciteitsanalyse voor een overzicht van de bestaande capaciteit en om er zeker van te zijn dat deze ook ten volle wordt benut. Ze gebruiken Virtual Hard Disk (VHD)-manipulatie voor dynamische applicatietoegang en herstel voor desktopapplicaties. Desktopvirtualisatie maakt het mogelijk om meerdere besturingssystemen te gebruiken voor simpele migraties en gestroomlijnde implementaties. Virtual workload management en provisioning geven een grotere controle bij het beheer van utilisatie en het afwegen van workloads om tegemoet te kunnen komen aan SLA's en veranderende bedrijfsbehoeften. Standaardconfiguraties voor alle servers, applicaties en hardwaretypes worden gedefinieerd, onderhouden en ge-audit.

Er bestaat een geautomatiseerd patchbeheer voor mobiele en non-client-computers. Niet alleen implementeren deze organisaties model-enabled, service-level monitoring van desktops, applicaties en servers, maar ze kunnen ook hun verbonden mobiele apparaten - die een standaard besturingssysteem gebruiken - pro-actief beheren en monitoren. IT-managers hebben een gecentraliseerde oplossing voor het installeren van software en content op mobiele apparaten die continue toegeleverd worden. Gebruikers hebben toegang tot LOB-applicaties van binnen of buiten het kantoor.

Security and Networking

Security and Networking omvat de bescherming van informatie en communicatie, met inbegrip van beveiliging tegen ongeautoriseerde toegang. Tegelijkertijd richt Security and Networking zich op oplossingen die de IT-infrastructuur beschermen tegen denial-aanvallen en virussen terwijl tegelijkertijd de toegang tot bedrijfsresources behouden blijft.

Basic

In de volwassenheidsfase Basic voor Security and Networking is er een gebrek aan elementaire beveiligingsstandaarden die gebruikers beschermen tegen virussen en hackers. Antivirussoftware met automatische updates ontbreekt gewoonlijk op de meeste desktops. Er is geen gecentraliseerde firewall voor de meeste systemen, en er zijn geen interne servers voor Domain Name System (DNS) en Dynamic Host Configuration Protocol (DHCP) netwerkservices.

Standardized

In de fase Standardized is er antivirussoftware geïnstalleerd op desktops en non-client-computers. Maar multilayered beveiligingsmodellen zijn nog niet uitgerold binnen het netwerk, van de perimeter door de firewall-, server-, desktop- en applicatielagen. De IT-infrastructuur kent enige automatisering en wordt centraal beheerd. Er is een gecentraliseerde firewall opgezet en organisaties hebben interne DNS- en DHCP-netwerkservices.

Rationalized

Organisaties in de fase Rationalized hebben een oplossing voor toegang op afstand geïmplementeerd waardoor het voor gebruikers veiliger wordt om netwerkresources van buiten het netwerk te benaderen. Ze hebben beveiligde server-to-server isolatie geïmplementeerd om te voorkomen dat niet vertrouwde applicaties andere applicaties of serverinstances zullen doen crashen. Er is op basis van beleidsregels een firewall geïnstalleerd op servers en desktops om de netwerk- en desktopactiviteiten te monitoren op kwaadwillend of ongewild gedrag. Gecentraliseerde certificaatservices in een public key infrastructure (PKI) worden gebruikt om gegevens te beveiligen en het beheer van ID-gegevens van resources binnen en buiten de organisatie te beheren. Er is een beveiligd draadloos netwerk geïmplementeerd.

Dynamic

In de fase Dynamic wordt een geïntegreerde oplossing voor bedreigingsbeheer en mitigatie gebruikt op de client- en serverranden. Een quarantaine-oplossing voor niet-gepatchte en geïnfecteerde desktops en mobiele apparaten draagt bij tot het isoleren van virussen. Organisaties in deze fase gebruiken ook Session Initiation Protocol (SIP) voor beveiligde communicatie via presence. Gecentraliseerd, Active Directory- based groepsbeleid wordt gebruikt om IPSec-beleid en -filters te distribueren om het beveiligingsniveau op hardware van eindgebruikers te verhogen.

Data Protection and Recovery

Data Protection and Recovery omvat de processen en tools die IT gebruikt voor backups en het opslaan en terugzetten van informatie en applicaties. Aangezien informatie zich vermenigvuldigt, staan organisaties onder steeds grotere druk om die informatie te beveiligen en een kosteneffectieve en tijdsbesparende wijze van herstel te leveren indien dat nodig is.

Basic

Organisaties in de fase Basic van Data Protection and Recovery hebben geen standaardbeleid op het gebied van gegevensbeheer en er bestaan overal eilanden van gebruikersgegevens: op het netwerk, in file shares, op non-standard servers, in persoonlijke profielen, websites en op lokale computers. Slechts een klein deel van deze informatie wordt opgeslagen. Als er al gegevens worden opgeslagen, gebeurt dit lokaal en is er geen backup- en herstelproces voor de meest cruciale servers. Een gebrek aan archivering en backup maakt het naleven van wetgeving moeilijk. Bedrijfsgegevens in applicaties en cruciale systemen lopen het risico verloren te gaan door het gebrek aan een disaster-recovery plan. Deze organisaties hebben geen user-state migratie beschikbaar die ervoor zorgt dat nieuwe technologieën soepel en foutloos werken. Hun processen voor gegevensherstel zijn niet getest.

Standardized

In de fase Standardized beschikken organisaties over backup- en herstelprocessen voor cruciale servers, maar zijn problemen met betrekking tot de onbetrouwbaarheid van tapes en trage gegevensoverdracht zeker nog niet opgelost. Het beheer van gebruikers- en applicatiegegevens is niet gecentraliseerd. Er zijn standaarden voor lokale opslag neergelegd in de 'Mijn Documenten' folders van de gebruiker, maar de informatie is niet doorgestuurd of opgeslagen. Elke backup van gebruikersgegevens vindt alleen plaats op werkgroepniveau. Er is enige automatisering van user-state migratie beschikbaar voor technologie-uitrol. Herstelprocessen voor mission-critical applicaties zijn getest.

Rationalized

In deze fase beschikken organisaties via virtualisatie over backup- en herstelprocessen voor een aantal servers en voor alle servers via SLA's. Herstelprocessen voor zowel mission-critical applicaties als gegevens zijn getest. Informatie wordt opgeslagen op tape die zich bevindt in een local area network (LAN) en wordt beheerd op bedrijfsniveau. Tijdens backups kan er een dip in de LAN- en serverprestaties zijn. User states worden bewaard en hersteld voor technologie-implementaties. Deze organisaties voldoen nog niet aan alle regelgeving voor deze branche.

Dynamic

Continue gegevensbescherming garandeert bedrijfscontinuïteit en hoge beschikbaarheid door het snel herstellen van de toegang tot informatie en systemen met failover-voorzieningen. Dynamische IT-organisaties hebben backup- en herstelprocessen voor alle servers met SLA's en desktopgegevens. In deze fase wordt naleving van complexe regelgeving mogelijk. Services op het gebied van bedrijfscontinuïteit worden geïmplementeerd, met inbegrip van gegevensclassificatie en beleidsdefiniëring.

IT and Security Process

IT and Security Process levert richtlijnen op basis van best practices in de industrie met betrekking tot het op de juiste manier bekostigen van het ontwerpen, ontwikkelen, gebruiken en ondersteunen van oplossingen waarbij tegelijkertijd een hoge mate van betrouwbaarheid, beschikbaarheid en beveiliging wordt gegarandeerd. Alhoewel krachtige technologie noodzakelijk is om tegemoet te komen aan de behoefte van bedrijven aan betrouwbare, beschikbare en uitermate veilige IT-diensten, is technologie alleen niet voldoende. Uitmuntende processen en getraind personeel met duidelijk afgebakende rolverdelingen en verantwoordelijkheden zijn eveneens noodzakelijk.

Basic

Processen zijn informeel, zonder SLA's. Eindgebruikers hebben geen aanspreekpunt voor het oplossen van problemen met het besturingssysteem of producten in de infrastructuur. Organisaties in deze fase ontberen uitgebreide beveiligingsstrategieën en -beleid. Risicoanalyse wordt sporadisch of helemaal niet uitgevoerd. De weinige planning op het gebied van incident-response is gewoonlijk ongecoördineerd en antiviruscontroles en netwerkbeveiliging worden inconsistent uitgevoerd. De basis identiteitsbeveiliging is aanwezig en de identiteiten van gebruikers, apparaten en services worden beheerd met behulp van basisprocessen. Deze organisaties moeten nog een consistent beleid ontwikkelen op het gebied van beveiliging voor alle apparaten op het netwerk. En op het gebied van consistente processen voor het onderkennen en updaten van beveiligingsproblemen op deze apparaten. Ze ontberen een allesomvattend plan en proces om gegevens te classificeren en beveiligingscontroles toe te passen. Basistechnologieën worden toegepast om gegevensintegriteit te beveiligen.

Standardized

In deze fase is het bestaan van SLA's gewoon, hoewel nog steeds op basis van verwachting en niet op basis van een formele overeenkomst. Er is een geformaliseerde helpdeskfunctie en een proces voor incident- en probleembeheer maar deze zijn niet volledig gedocumenteerd. Hoewel er geen consistent proces voor risicoanalyse bestaat, beschikken deze organisaties over standaardtechnologieën voor identiteitsbeveiliging en een proces voor het identiteitsbeheer van gebruikers, apparaten en services. Clientbeveiliging en een (niet-gedocumenteerd) netwerkbeveiligingsproces zijn aanwezig. Eenvoudig configuratiebeheer verbetert de effectiviteit van IT en implementaties in de toekomst, maar de processen voor het aanbrengen van beveiligingsupdates, en het testen van de naleving op alle netwerkverbonden IT resources zijn nog niet gedocumenteerd. Identificatie van netwerkverbonden apparaten is niet gedocumenteerd, net als de processen voor software-aankoop voor het evalueren van beveiligingsregels. Standaardtechnologieën binnen de organisatie beschermen de vertrouwelijkheid en integriteit van gegevens.

Rationalized

IT-activiteiten zijn proactiever maar het proces van risicoanalyse wordt nog steeds op een inconsistente manier overgebracht aan de business. Er bestaat een plan hoe te reageren op incidenten maar er is nog te weinig training voor degenen die zouden moeten reageren. Door IT opgestelde SLA's en een geformaliseerde help-deskfunctie zijn geïmplementeerd - samen met technologieën en processen voor identiteitsbescherming - maar organisaties missen de kennis om goede kosten-baten analyses te maken voor de bedrijfseigenaren. IT-managers kunnen netwerkverbonden apparaten identificeren, deze beschermen met de voorgeschreven technologieën en efficiënt beveiligingsupdates installeren. Client- en serverbescherming wordt gebruikt, maar er zijn nog geen beveiligingsoplossingen om filtering, scanning of controle van inkomende content te leveren voordat deze op de server aankomt (controle van het Postvak bijvoorbeeld). Het uitvoeren van tests op alle aangeschafte of ontwikkelde software zorgt ervoor dat er wordt voldaan aan beveiligingseisen. Er bestaat een beheerd proces voor het classificeren van gegevens en het aanbrengen van beveiligingscontroles.

Dynamic

Consistente beveiligingsprocessen en -beleid helpen bij het beveiligen van bedrijfsgegevens. Het IT-personeel is uitermate geschoold. Het beveiligingsbeheer van de webserver is gestroomlijnd voor efficiëntie. IT scorecards en dashboards worden gebruikt om rapporten en kosten-baten analyses te maken voor de bedrijfseigenaren.

Bedrijfsprofiel BRAIN FORCE

BRAIN FORCE is een gespecialiseerde System Integrator. BRAIN FORCE optimaliseert ICT-infrastructuren met als doelstelling complexe technologie in organisaties beheersbaar te maken en gebruikers een krachtige en wendbare werkomgeving te bieden. Dit wordt gedaan door de ontwikkeling van best practices, effectieve processen en slimme software voor Microsoft-, Citrix- en VMware-omgevingen. Daarnaast worden via BRAIN FORCE Managed Services innovatieve beheerdiensten aangeboden, waarmee uw omgeving betrouwbaar en up-to-date blijft.

BRAIN FORCE heeft negen vestigingen in zeven Europese landen en telt momenteel 850 medewerkers. De jaarlijkse omzet bedraagt meer dan 70 miljoen euro en BRAIN FORCE is genoteerd aan de beurs van Wenen. Meer details kunt u vinden op www.brainforce.com.

Klanten

BRAIN FORCE loopt voorop in het Nieuwe Werken en ondersteunt al vele jaren gerenommeerde organisaties, zoals Bugaboo International, Waterschap de Dommel, Koninklijke BAM Groep NV, APX-ENDEX, Waterschap Aa en Maas, Kennemer Gasthuis, Amphia Ziekenhuis, Erasmus Medisch Centrum, Hogeschool Arnhem en Nijmegen, Vanboeijen, ROC Midden Brabant, Gemeente Hilversum en verschillende stadsdelen in Amsterdam.

Partners

Om de beste oplossing voor onze klanten te leveren, werkt BRAIN FORCE samen met partners. BRAIN FORCE is Microsoft Gold Partner en beschikt over de volgende competenties: Desktop Platform, Identity and Security, Midmarket Solution Provider, Server Platform, Systems Management, Unified Communications, Virtualization en Volume Licensing. BRAIN FORCE is in Nederland de eerste gecertificeerde Microsoft Services Ready-partner op het gebied van desktop en office deployment (DOWO). Wij zijn Windows 7 First Wave Partner, Application Compatibility Factory Partner en gecertificeerd voor Desktop Deployment (DDPS), Exchange (EDPS), SharePoint (SDPS) en Forefront Planning Services (FDPS).

BRAIN FORCE is Citrix Silver Solution Advisor en één van de eerste partners voor V-Alliance, het gezamenlijke programma in server- en desktopvirtualisatie van Microsoft en Citrix.

Atos Origin, Fujitsu, Getronics, Logica en Valid zijn Enterprise partners met betrekking tot Packaging Robot[®]. Daarnaast is BRAIN FORCE VMware Enterprise Partner, en partner van New Horizons Computer Learning Centers. Quest?, Res Powerfuse? AppDNA, Flexnet, Wise, Novell.

Voor de levering van licenties en Software Asset Management-diensten werkt BRAIN FORCE samen met Agile, Solimas en ManageSoft. HP is met LeftHand oplossingen partner voor storage oplossingen.

Uniek aan BRAIN FORCE:

- Eerste in Nederland gecertificeerde Microsoft Services Ready partner
- V-Alliance partner van Microsoft en Citrix
- System Integrator van het jaar 2010 voor de overheidsmarkt
- Windows 7 launch partner
- Marktleider op het gebied van applicatiemanagement.
- Slim kennis delen via best practices.
- Voorspelbaar ontwerp- en implementatietrajecten dankzij uitgewerkt architectuurmodel.
- Voortdurende innovatie en automatisering beheertaken d.m.v. Research & Development.
- Eigen ontwikkelde IT-beheer software: Packaging Robot en Workspace Manager.



Microsoft[®]

© 2008 Microsoft Corporation. Alle rechten voorbehouden. Microsoft en andere handelsmerken in dit document zijn handelsmerken of geregistreerde handelsmerken van de Microsoft-groep van bedrijven.

Alle overige handelsmerken zijn het eigendom van hun respectieve eigenaren.

Optimaliseer uw basisinfrastructuur 2008 - 2009