KASPERSKY lab

BEST PRACTICES

Security Controls

kaspersky.com/nl

SECURITY CONTROLS - BEST PRACTICES

Cyberspionage en door staten gesponsorde dreigingen zijn de laatste tijd regelmatig in het nieuws. Het is echter een feit dat dezelfde technologie ook tegen bedrijven als het uwe kunnen en zullen worden gebruikt.

U kunt internet niet vergrendelen en u kunt niet alles zien wat er in realtime in uw netwerk gebeurt. Maar u kunt het wel beheren en controleren. En u kunt zeker controleren wat er gebeurt wanneer uw eindgebruikers ergens op klikken of iets installeren wat ze beter niet hadden kunnen doen. Wij weten hoe...

1. NIET GEWOON BLOKKEREN, MAAR CONTROLEREN

Sociale media, slimme apparaten, webapplicaties, spam, phishing, schadelijke websites, social engineering, malware. IT-beheerders kampen steeds vaker met steeds complexere dreigingen via steeds verder vervagende grenzen.

En dat zijn alleen nog maar de risico's die uw bedrijf van buitenaf bedreigen. Wat dacht u van de activiteiten van eindgebruikers die uw bedrijf blootstellen aan inbreuken op de beveiliging en gegevens? Schadelijke code ingesloten in online games, schadelijke links in applicaties voor sociale netwerken, malware verborgen in ogenschijnlijk onschuldige kantoordocumenten... Criminelen maken tegenwoordig misbruik van vulnerability's in verband met de toegang van individuele gebruikers tot bedrijfsnetwerken en de gevoelige gegevens die zich daarin bevinden.

Controlesystemen voor applicaties, apparaten en het web, in combinatie met krachtige anti-malwaretechnologie, kunnen uw bedrijf beschermen zonder aan productiviteit en flexibiliteit in te leveren. Neem de technologie in uw bedrijf in eigen hand met deze eenvoudig te implementeren controlesystemen voor het web, applicaties en apparaten.

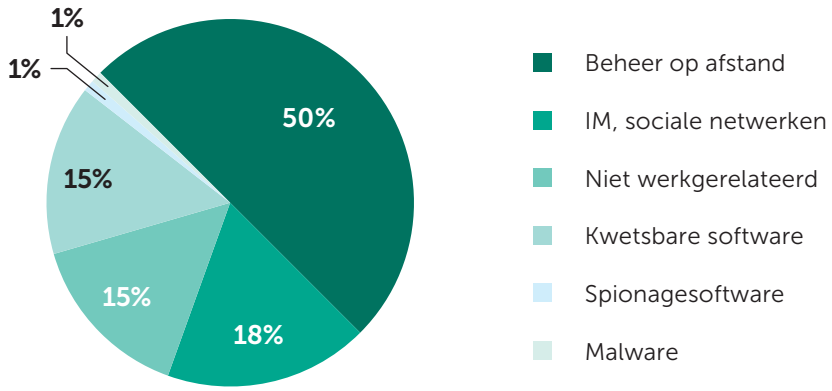
Pas op de app

In een hyper-verbonden wereld zijn vulnerability's in webapplicaties een favoriete achterdeur geworden voor cybercriminelen. Alleen al in 2014 detecteerde en neutraliseerde Kaspersky Lab meer dan **6,2** miljard aanvallen die vanaf online resources wereldwijd werden uitgevoerd[1]; in 2013 was dat nog **1,7** miljard[2]. Deze aanvallen werden uitgevoerd door **9,7** miljoen verschillende hostcomputers[3]. Kaspersky Lab detecteert dagelijks zo'n **325.000** nieuwe schadelijke bestanden[4].

1 op de **14** downloads bevat malware[5], en downloads simpelweg blokkeren helpt maar tot op zekere hoogte ... elke dag voeren criminelen malware uit die erop is gericht vulnerability's in legitieme bedrijfssoftware te misbruiken: applicaties van derden vertegenwoordigen gemiddeld **75** procent van de vulnerability's[6].

1 Kaspersky Security Bulletin, december 2014
2 Kaspersky Security Bulletin, december 2013
3 Kaspersky Security Bulletin, december 2014
4 Kaspersky Security Bulletin, december 2014
5 Kaspersky Security Bulletin, december 2014
6 Secunia Vulnerability Review 2014

De realiteit voor IT-beveiligingsprofessionals is dat de zwakste schakel in de beveiligingsketen vaak al in hun systemen zit – of bij hen zit.



2. APPLICATION CONTROL EN WHITELISTING: DREIGINGEN BUITENSLUITEN, BEVEILIGINGSINBREUKEN VOORKOMEN

Application control en dynamische Whitelisting-technologie kunnen u helpen systemen te beschermen tegen bekende en onbekende dreigingen door beheerders volledige controle te geven over de typen applicaties en programma's die op hun endpoints mogen worden uitgevoerd, ongeacht het gedrag van de eindgebruikers.

In essentie kunt u met application control effectiever beleidsregels voor beveiliging en beleid maken en doorvoeren:

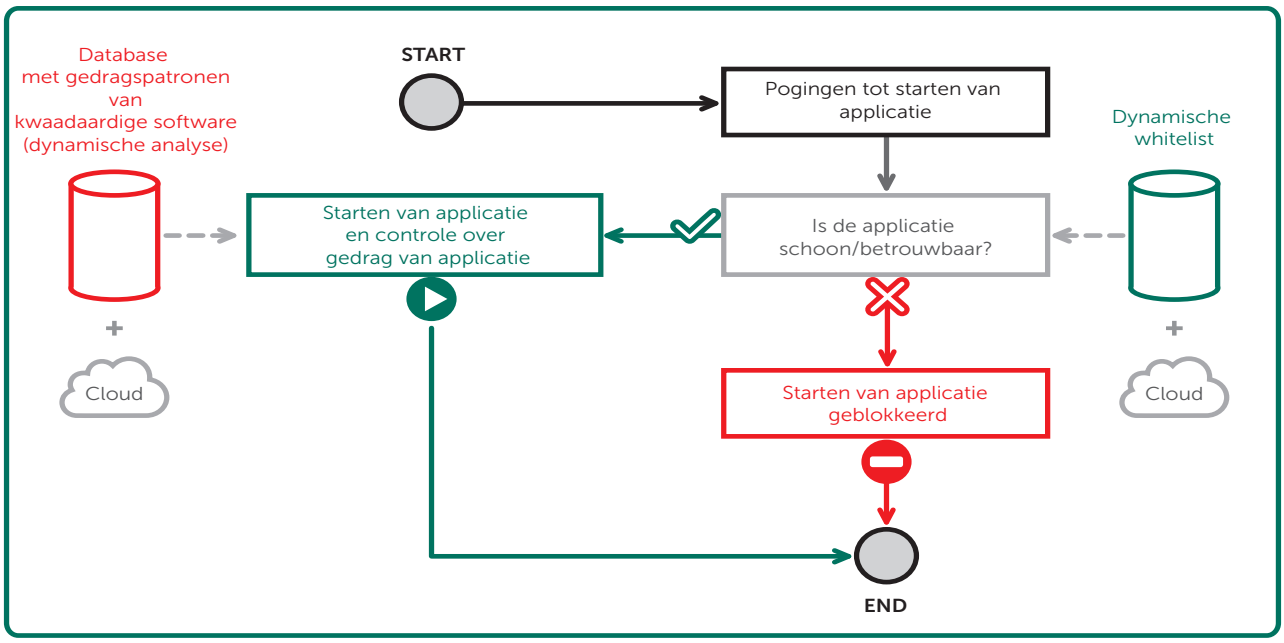
- **Application Startup Control**: het starten van applicaties toestaan, blokkeren, controleren. Verhoog de productiviteit door de toegang tot niet-zakelijke applicaties te beperken.
- **Application Privilege Control**: de toegang van applicaties tot systeemresources en gegevens reguleren en controleren, applicaties classificeren als vertrouwd, niet-vertrouwd of beperkt.
- **Application Vulnerability Scanning**: proactieve bescherming tegen aanvallen die op vulnerability's in vertrouwde applicaties zijn gericht.
- **Applications Monitoring**. IT moet niet alleen in staat zijn bepaalde applicaties te blokkeren of toe te staan, maar ook kunnen monitoren hoe applicaties zich gedragen – welke resources ze gebruiken, tot welke typen gebruikersgegevens ze toegang zoeken of wijzigen, of ze naar registers schrijven, enzovoort. Met die informatie kunt u voorkomen dat welke applicatie dan ook acties uitvoert die het endpoint in gevaar brengen en het netwerk waarmee dat endpoint is verbonden.

  Constante, realtime monitoring van (en door wie) toegang wordt verkregen tot applicaties helpt u gebruikspatronen vast te stellen op basis waarvan u beleidsregels kunt aanscherpen met betrekking tot eindgebruikersvereisten en dreigingen.

Whitelisting – kracht en controle in de kern

Als application control het voertuig voor effectieve bescherming tegen complexe dreigingen is, is dynamische Whitelisting de motor die het aandrijft. Whitelisting is in feite een van de best practices van elke succesvolle applicatiecontrolestrategie. Kortom: zonder Whitelisting hebt u geen echte applicatiecontrole.

Whitelists zijn lijsten met vertrouwde applicaties die IT-professionals kunnen gebruiken om een extra laag beveiliging toe te voegen aan bestaande controlesystemen. Wanneer een poging wordt gedaan om een applicatie uit te voeren, wordt deze automatisch gecontroleerd aan de hand van de Whitelist; staat de applicatie daarin, dan mag deze worden uitgevoerd volgens de beheerderspecifieke beleidsregels. Is de applicatie niet in de lijst opgenomen, dan wordt deze geblokkeerd tot een beheerder er goedkeuring aan geeft. Zie het als de portier die uw endpoint bewaakt.



Overweeg een Default Deny-benadering wat Whitelisting betreft

Een Default Deny-configuratie is de effectiefste beveiligingsinstelling gezien de steeds verder gaande dreigingsvectoren. Default Deny blokkeert gewoon alle applicaties op alle werkstations, behalve applicaties die beheerders expliciet hebben toegestaan.

Hoewel u met een strategie van alles blokkeren niet echt vrienden maakt op kantoor, zijn Default Deny-strategieën gebaseerd op effectieve Whitelisting zodat uw eindgebruikers een zekere mate van flexibiliteit overhouden.

Het gaat er niet zozeer om absoluut alles te blokkeren als wel precies te bepalen wat u gaat toestaan.

De beste manier om erachter te komen hoe een Default Deny-scenario in uw bedrijf zou uitpakken, is het gewoon uit te proberen. In een sandbox-omgeving kunt u de werkelijke effecten zien van de implementatie van Default Deny in uw IT-systeem en met de nodige aanpassingen, zonder dat uw systemen of gebruikers er hinder van ondervinden. U zult bij het uitproberen wellicht verrast zijn hoe weinig uw gebruikers in de praktijk van deze strategie zullen merken.

Whitelisting-databases gebruiken

U besluit dus met Whitelisting te gaan werken. Maar u kunt uw werktijd niet steeds besteden aan het samenstellen, aanpassen en bijwerken van lijsten met acceptabele, 'veilige' applicaties. Sta er eens bij stil: het gaat niet alleen om de controle van een paar bedrijfsapplicaties – wat dacht u van zaken als printerstuurprogramma's, netwerkinfrastructuursoftware of updates?

Dynamische, constant bijgewerkte en gemonitorde Whitelist-databases vormen de kern van de effectiefste oplossingen. Beheerders kunnen dan met een gerust hart met andere taken aan de slag, in de wetenschap dat geautomatiseerde, constant bijgewerkte Whitelisting-databases op de achtergrond hun werk doen.

Andere tools die u nodig kunt hebben

Een Whitelisting- en applicatiecontrole-oplossing van goede kwaliteit is op basis van best practices te implementeren, zonder de complexiteit van handmatige selectie van de talloze softwarecomponenten die zelfs in kleine bedrijven een rol spelen in de dagelijkse gang van zaken. Een goed programma maakt uw leven er niet alleen gemakkelijker op, maar omvat ook diverse functies op basis van best practices, waaronder:

- **Inventarisatie**: U kunt niet iets meten of monitoren waarvan u niet weet dat u het hebt. De beste Whitelisting-programma's beginnen met een software-inventarisatie. Stel een overzicht van geïnstalleerde software in het netwerk samen en houd het bij in een handige indeling, wat de analyse vergemakkelijkt. Maak het leven voor uzelf ook gemakkelijker door een oplossing met automatische inventarisatie te kiezen. Dat scheelt u de tijd (en de hoofdpijn) om alle beetjes software in uw onderneming op te sporen. Bijkomend voordeel: u kunt ongewenste apps vinden en verwijderen en de goede apps behouden.

- **Categorisatie**: Wijs functionele categorieën toe aan geïnstalleerde software (bijvoorbeeld besturingssystemen, bedrijfssoftware, ontwikkelaarstools, randapparaten, browsers, multimedia). Dit maakt het voor beheerders gemakkelijk om bedrijfsgerelateerde applicaties te identificeren — en applicaties te blokkeren die ten koste gaan van de productie. Slim gebruik van categorieën betekent dat u niet precies hoeft te achterhalen met welke games uw eindgebruikers hun tijd zitten te verdoen; u kunt gewoon die hele categorie blokkeren. Mochten ze iets volslagen onbekends ontdekken, dan zet u het gewoon zelf op de lijst. Bovendien kunnen uw verkennende tests met Default Deny u ertoe aanzetten om nieuwe categorieën te maken op basis van uw bevindingen.

- **Vertrouwde updates**: Zorg voor regelmatige updates van toegestane software en sluit eventuele nieuwe of eerder niet-ontdekte vulnerability's uit. Daartoe behoren patching, systeembeheerprocessen en andere software-implementatieprogramma's.

- **Flexibele implementatieregels**: Kwaliteitsoplossingen zijn voorzien van een breed scala aan vooraf gedefinieerde regels voor de meest voorkomende scenario's. Dat is een goed uitgangspunt om mee aan de slag te gaan, maar als uw Whitelisting-implementatie zich ontwikkelt, wilt u instellingen voor de unieke omstandigheden in uw bedrijf kunnen bijstellen en aanpassen.

  Beperk uzelf niet met een oplossing die geen scala aan mogelijkheden voor flexibele aanpassingen biedt – u hebt bijvoorbeeld opties nodig voor factoren als bestandsnamen, bronmappen of leveranciers. U hebt waarschijnlijk ook flexibiliteit nodig wat betreft MD5 ('vingerafdrukken' voor gegevens) of 'hashes' – technieken die voorkomen dat criminelen (of vasthoudende werknemers) uw Whitelist omzeilen door verboden applicaties en bestanden als geoorloofd te camoufleren.

- **Denk mondiaal, handel lokaal**

  U moet altijd werken vanuit een mondiale Whitelist-database die allesomvattend en dynamisch is – u hebt simpelweg niet de tijd of de resources om zoiets zelf te doen: er bevinden zich bijvoorbeeld bijna 500 miljoen unieke bestanden in de Whitelist-database van Kaspersky Lab.

  Op een doorsneedag uploadt Kaspersky Lab meer dan een miljoen bestanden – genoeg om een speciaal Whitelisting-lab bezig te houden. Mondiale databases moeten permanent beschikbaar en toegankelijk zijn in de cloud. Nu leveranciers van vele toonaangevende applicaties hun producten constant bijwerken of nieuwe versies uitbrengen, blijft met constant bijgewerkte mondiale databases het risico van 'valse meldingen' beperkt.

  De behoefte aan mondiale databases erkennen betekent niet dat u uw eigen, volledig lokale Whitelist-database, geldig voor alleen uw eigen netwerk, niet moet aanpassen. Kies een oplossing die dat ondersteunt, vooral als u uw eigen aangepaste applicaties ontwikkelt.

- **Ga voor goud**

  Een gouden image is uw sjabloon voor de perfecte installatie: Al uw bedrijfskritische applicaties en instellingen, geïmplementeerd volgens best practices en afgestemd voor optimale prestaties.

  In de echte wereld krijgen IT-professionals zelden de gelegenheid om met een volledig schone lei te beginnen – maar of u nu met splinternieuwe computers aan de slag gaat die nog nooit verbinding met internet hebben gehad, of uw Whitelist langzaam maar zeker bijstelt op basis van vooraf bestaande technologieën, u moet altijd een 'gouden image' ontwikkelen. Of u de gouden image nu gebruikt als referentiepunt terwijl uw applicatiecontroleprogramma zich ontwikkelt, of ervoor kiest er het platform voor uw Default Deny-strategie van te maken, een oplossing die u ondersteunt bij het maken en ontwikkelen ervan, maakt uw leven er een stuk eenvoudiger op. Vooral als u er een kant-en-klare 'algemene' sjabloon bij krijgt om mee te werken.

Black of white? Allebei!

Whitelisting staat alleen de uitvoering van vooraf goedgekeurde applicaties toe en is daarmee de tegenhanger van traditionele anti-virus (ofwel 'Blacklisting'), waarbij software wordt geblokkeerd nadat deze is gedefinieerd als schadelijk. Door de twee technologieën onder één dak samen te brengen, sluit u in feite zowel de achterdeur als de voordeur naar uw IT-huis af.

Een combinatie van Whitelisting en Blacklisting biedt een optimaal scenario met meerlaagse beveiliging op basis van best practices. Whitelisting kan de prestaties van anti-virusprogramma's juist opvijzelen; applicaties in de Whitelist hebben immers niet dezelfde intensieve, regelmatige niveaus van controle nodig, zodat u systeemresources uitspaart en de prestaties van applicaties verbetert.

3. DEVICE CONTROL

U hebt uitgezocht welke applicaties wel en niet op uw endpoints mogen worden uitgevoerd; zorg nu voor hetzelfde hoge niveau van controle over apparaten.

Beperk het insiderrisico voor uw organisatie aanzienlijk door beleidsregels rondom het gebruik van verwijderbare apparaten en media centraal bij te houden. Denk daarbij aan USB, flashstations, cd/dvd, smartcards, enzovoort. Of u zich nu zorgen maakt om een ontevreden werknemer die gevoelige gegevens naar een USB-stick kopieert, of gewoon wilt voorkomen dat geïnfecteerde draagbare apparaten verbinding maken met uw endpoint of netwerk, apparaatbeheer biedt daartoe een flexibele benadering.

Hier zijn enkele mogelijkheden om te overwegen wanneer u een apparaatbeheerprogramma wilt implementeren:

- **Definieer uw klassen**: Verschillende apparaten hebben verschillende capaciteiten en brengen dus verschillende dreigingen met zich mee. Het is relatief eenvoudig om bijvoorbeeld in het geval van een beeldscanner een Default Deny-beleid te implementeren. Maar schakel een USB-poort uit en u kunt diezelfde poort ook niet meer gebruiken voor beveiligde, op tokens gebaseerde VPN-toegang. Daarom hebt u het volgende nodig...
- **Granulariteit**: Om verschillende regels in te stellen voor verschillende apparaten en, inderdaad, verschillende gebruikers en toepassingen. Beheerders moeten beleidsregels kunnen toepassen voor verschillende apparaten, zoals alleen-lezen, blokkeren, lezen en schrijven.

  Deze granulariteit moet zich uitstrekken tot het kunnen beperken van welk type bestanden kunnen worden overgezet, het tijdstip waarop een bepaald beleid van kracht wordt, het type apparaat dat is toegestaan, en wanneer. Uw leven wordt een stuk aangenamer in dit opzicht als u deze regels tegelijkertijd op meerdere apparaten kunt toepassen.

  Voor nog meer controle moet u de mogelijkheid hebben om een beleid toe te passen op het specifieke serienummer van een willekeurig apparaat. Dan kunt u beleidsregels en rechten instellen voor specifieke apparaatmodellen en individuele gebruikers, waarbij andere medewerkers geen toegang tot de gegevens op het apparaat hebben.
- **Toegangscontrole**: Hiermee hebt u volledige controle over de toegang tot specifieke apparaattypen voor geselecteerde gebruikers en groepen gedurende specifieke tijdsperioden. Deze functionaliteit kan nuttig zijn als u bijvoorbeeld probeert de afdrukkosten na werktijd te beperken.

- **Encryptie**: Een van de best practices voor apparaatbeheer is encryptie. We hoeven u niet te vertellen hoe gemakkelijk USB-sticks of flashstations kwijtraken of gestolen worden. Er zijn beleidsregels mogelijk om encryptie te verplichten voor specifieke apparaattypen.

- **Integratie met Active Directory**: Omdat u niet elke individuele gebruiker in het bedrijf achter de vodden wilt zitten om beleidsregels toe te passen, stelt u gewoonweg uw apparaatbeheerbeleidsregels in en pusht die naar uw gedefinieerde gebruikersbestand.

4. BENT U ALLEEN?

Nog een laatste vraag – wie gaat al die goede dingen doen? U? En is dit alles wat tot uw IT-taken behoort? Werken met controlesystemen, of het beheren van de beveiliging in het algemeen, is misschien maar één onderdeel van uw werk, maar we hopen wel dat uw bedrijf het belang van dat ene onderdeel inziet, net zoals wij dat doen.

Als u alleen of deel van een klein team bent, moet u de beveiliging kunnen beheren als onderdeel van een breder geheel en wel vanaf één scherm, in plaats van tussen consoles heen en weer te lopen.

Aan de andere kant maakt u wellicht deel uit van een groot beveiligingsteam, zodat uw taak zich op één gebied toespitst - bijvoorbeeld apparaatbeheer. In dat geval hebt u een beveiligingssysteem nodig met RBAC (Role-Based Access Controls), zodat alleen u de beveiliging voor dat onderdeel beheert.

Maar u zou niet moeten hoeven kiezen. Er is geen reden waarom dezelfde beveiligingscontrolesystemen niet eenvoudig te beheren zijn door één duizendpoot of door verschillende leden van een druk team. Het draait allemaal om integratie. Een beveiligingssysteem waarbij alles, met inbegrip van de controlesystemen, samenwerkt als één platform, is vrijwel altijd een goede zaak.

TOT SLOT...

Steeds veranderende dreigingen betekenen dat organisaties niet meer wegkomen met alleen het blokkeren van malware en andere dreigingen nadat ze zijn gedetecteerd. Krachtige blacklisting-technologie blijft nodig in elke goede beveiligingsstrategie, maar volledige bescherming kan alleen worden bereikt met een meerlaagse benadering.

U hebt de capaciteit nodig om uw bedrijf te beschermen tegen traditionele malware, maar ook tegen dreigingen via ogenschijnlijk legitieme bronnen: vulnerability's in vertrouwde applicaties, schadelijke code ingesloten in populaire websites, phishing-aanvallen via e-mail of schadelijke software die misbruik maakt van functies voor de automatische uitvoering van draagbare media.

De speciale mondiale Whitelisting-database van Kaspersky Lab is wereldwijd toonaangevend: wij zijn het enige IT-beveiligingsbedrijf met een speciaal Whitelisting-laboratorium dat wordt ondersteund door een team van ervaren experts. Alle via één scherm, waarmee u de controle in handen hebt zonder onnodig gedoe.


Twitter.com/
Kaspersky


Facebook.com/
Kaspersky


Youtube.com/
Kaspersky

Kaspersky Lab
kaspersky.com/nl

Alles over internetbeveiliging:
www.securelist.com

Zoek een partner bij u in de buurt:
http://www.kaspersky.com/nl/partners

KASPERSKY lab