KASPERSKY lab

BEST PRACTICES

Systems Management

kaspersky.com/nl

SYSTEMS MANAGEMENT - BEST PRACTICES

Verbeter de beveiliging en beheer de complexiteit met gecentraliseerde IT-beheertools.

Niet-gepatchte vulnerability's in populaire applicaties behoren tot de grootste gevaren voor de IT-beveiliging van bedrijven. Dit risico wordt verergerd door een toenemende IT-complexiteit. Als u niet weet wat u hebt, hoe kunt u het dan beveiligen? Deze gids met best practices laat u zien hoe...

De toenemende diversiteit aan platformen, apparatuur, software en applicaties maakt het werk er voor IT-beheerders niet eenvoudiger op en leidt onder meer tot complexiteit en een zware belasting van de resources. Apparaten en software zijn niet de enige zaken die zich vermenigvuldigen; Kaspersky Lab detecteert elke dag 350.000 nieuwe dreigingen, waarvan er vele specifiek zijn ontwikkeld om te profiteren van vulnerability's in populaire bedrijfsapplicaties en om toegang te krijgen tot gevoelige gegevens, geld te stelen of systemen te blokkeren tot er losgeld is betaald.

Complexiteit ondermijnt beveiliging, efficiëntie en groei. Er ontstaat ruimte voor fouten en u bent minder goed in staat controle uit te oefenen over wijzigingen. Effectief systeembeheer is een goed begin ter ondersteuning van best practices voor optimaal gebruik van uw IT-middelen en ondersteuning van een meerlaagse beveiligingsstrategie die raad weet met steeds veranderende dreigingen. Wij weten hoe.

1. CENTRALISEREN, AUTOMATISEREN, CONTROLEREN

Begin met enkele fundamentele stappen die elk bedrijf kan nemen om IT-prestaties te optimaliseren, kosten te verlagen, serviceniveaus te verhogen en flexibiliteit te verbeteren:

- Standaardiseer de desktop- en laptopstrategie en beperk images tot een minimum.
- Beheer de instellingen en configuraties voor pc's, laptops en mobiele apparaten vanaf een centrale locatie.
- Implementeer en onderhoud uitgebreide beveiligingstools.
- Automatiseer hardware- en software-inventarisaties, softwaredistributie, vulnerabilityscanning, patchbeheer en andere routinetaken.
- Maak remote probleemoplossing en software-installatie mogelijk, ook voor externe vestigingen.
- Implementeer Role-Based Access Control – pas gecentraliseerde consoleweergaven op basis van rollen en rechten aan.
- Voor ondernemingen worden door de integratie met SIEM-systemen de werklast en tools van beheerders geminimaliseerd en de rapportage vereenvoudigd.

Wanneer essentiële routinetaken, van beveiliging tot probleemoplossing, worden geautomatiseerd, hoeft men niet langer achter de feiten aan te lopen en kan men een strategische rol aannemen waarin de zakelijke behoeften op één lijn liggen met en worden ondersteund door IT-beleid. Automatisering kan helpen de fouten te beperken die vaak optreden bij handmatige processen in complexe systemen.

2. EFFECTIEF IMAGEBEHEER EN EFFECTIEVE IMPLEMENTATIE

Elk jaar worden er nieuwe hardware en applicaties geïmplementeerd, naast regelmatige upgrades van software, besturingssystemen, patching en applicatie-updates. Dat zijn tijdrovende en dure processen die complexer worden naarmate inventarisaties groeien.

U kunt veel tijd en middelen besparen door een ‘Golden Image’, een volledig geoptimaliseerde masterimage (of kopie) van een volledig systeem, voor te bereiden en te beheren. Deze 'perfecte' systeemconfiguratie wordt opgeslagen in een speciale inventarisatie in het netwerk en kan naar behoefte worden geïmplementeerd. Voor bedrijven die migreren naar een nieuw besturingssysteem, kunnen imagebeheer, -inventarisatie en -implementatie worden geautomatiseerd. Dit biedt het echte voordeel dat de implementatie na werktijd kan worden uitgevoerd met behulp van Wake-on-LAN-technologie – meer tijdsbesparing en minder werkonderbrekingen voor eindgebruikers.

Met een effectief gebruik van images worden besturingssystemen met optimale beveiligingsinstellingen geïmplementeerd. Vergeet niet de images zelf te beveiligen, idealiter door de toegang tot alle images onder meer als volgt te beveiligen en te bewaken:

- Gebruik sterke wachtwoorden.
- Bescherm certificaten voor clientverificatie.
- Toegangscontroles ter bescherming van de gebruikte 'referentiecomputer' voor vastlegging van het gebruikte besturingssysteem voor de gouden image – dit voorkomt dat schadelijke software onbedoeld in de image wordt opgenomen.
- Zorg ervoor dat de image wordt opgeslagen op een veilige locatie, waar de image geen gevaar loopt.
- Pas beveiligingspatches en -updates toe op het referentiesysteem, zodat alle nieuw geïmplementeerde systemen optimaal zijn beveiligd.

Met effectief imagebeheer kunt u het gekozen besturingssysteem voor alle apparaten in uw netwerk standaardiseren. Kies een oplossing waarmee het beheer van images kan worden geautomatiseerd en gecentraliseerd. Maak het uzelf nog eenvoudiger door te kiezen voor een oplossing waarbij gegevens van eindgebruikers automatisch worden opgeslagen.

Kijk voor extra controle en flexibiliteit naar een oplossing waarmee OS-images na het maken kunnen worden bewerkt. UEFI-ondersteuning, de mogelijkheid om een opstart-flashstation te maken met Windows PE en de optie om een OS-image te importeren uit een distributiepakket, zijn allemaal functies die de bruikbaarheid en efficiëntie verder zullen verbeteren.

3. INSTALLATIE EN IMPLEMENTATIE VAN SOFTWARE OPTIMALISEREN

Software-upgrades. Nieuwe software. Nieuwe versies van huidige software. Als elke computer in het bedrijf handmatig wordt geüpgraded, blijft er geen tijd over voor andere taken. Software-implementatie kan worden geautomatiseerd en geoptimaliseerd zodat de gevolgen voor het netwerk minimaal blijven en alles volledig transparant wordt voor eindgebruikers. Enkele tips voor best practices:

- Houd implementatieopties open door een oplossing te kiezen die naast standaard MSI-pakketten ook andere uitvoerbare bestandstypen ondersteunt, zoals exe, bat of cmd.
- Wees flexibel met implementaties: met opties waarmee u zowel on-demand als gepland implementaties kunt uitvoeren, hebt u meer flexibiliteit. Geplande implementaties zijn met name handig in scenario's met grote pakketten; voer de implementaties buiten kantooruren uit wanneer het netwerk zo stabiel mogelijk is. Kaspersky Systems Management maakt de automatische installatie van ruim 100 populaire applicaties mogelijk, geïdentificeerd via Kaspersky Security Network. Ze kunnen indien nodig na werktijd worden geïnstalleerd.
- Kies een oplossing die remote implementaties vanaf één console mogelijk maakt. Verminder het verkeer naar externe vestigingen met Multicast-technologie voor lokale softwaredistributie.
- De functionaliteit om installatiepakketten aan te passen, biedt meer flexibiliteit doordat installatieparameters in overeenstemming met beleidsregels kunnen worden ingesteld.
- Kies een oplossing die remote probleemoplossing mogelijk maakt: geen frustrerende telefoongesprekken met eindgebruikers meer. Met remote probleemoplossing bespaart u tijd en moeite en worden problemen snel en rechtstreeks opgelost. Gebruikersrechten en sessielogboeken/-audits voegen een extra beveiligingslaag aan externe sessies toe.

Door de implementatie en upgrades van software te automatiseren en te optimaliseren, kunt u de richtlijnen voor best practices standaard instellen voor uw bedrijf. In situaties met meerdere locaties of meerdere systemen kan controle over de software-implementaties u helpen de complexiteit en de fouten terug te dringen die ontstaan bij routinematige, handmatige processen.

4. NEEM HET BEHEER VAN GEBRUIKTE MIDDELEN IN HANDEN

Precies weten welke apparaten en applicaties in uw netwerk worden gebruikt, is een belangrijk element van effectieve IT-beveiliging. Dat geldt ook voor inzicht in welke gebieden aandacht nodig hebben.

Best practices houden onder meer volledig zicht op alle software en hardware die in het netwerk worden gebruikt. Automatische apparaatherkenning helpt hierbij en zorgt ervoor dat aan alle verplichtingen wordt voldaan. Verdere stappen zijn onder andere:

- **Software-inventarisatie**: Automatiseer de compilatie van inventarisaties en zorg voor volledige zichtbaarheid en controle. Met deze lijst hebben beheerders controle over het gebruik en kunnen zij eindgebruikers waarschuwen als zij ongeoorloofde/ongelicentieerde software gebruiken en zo nodig het gebruik van ongewenste applicaties blokkeren. Met een goed beheer en goede controle van softwarelicenties in het gehele bedrijf spaart u vaak heel gemakkelijk kosten uit en elimineert u uitgaven voor onnodige software.

- **Hardware-inventarisatie en apparaatherkenning**: Maakt een compleet overzicht van elk gebruikt apparaat in het netwerk mogelijk. Automatiseer het herkennen en melden van nieuwe hardware zodat u op de hoogte blijft, wijzigingen kunt volgen en ongebruikte apparaten uit het netwerk kunt verwijderen. Network Access Control (NAC) betekent dat gastapparaten veilig aan het netwerk kunnen worden toegevoegd en worden geblokkeerd als ze niet aan de beveiligingsvereisten voldoen of als er andere beleidsregels op zijn toegepast.

- **Licentieplanning**: Met een ordelijke inventarisatie is het licentiegebruik overeenkomstig afdelingsvereisten gemakkelijker te beheren – u merkt bijvoorbeeld dat gebruikers op de accountafdeling onnodige licenties voor grafische ontwerpsoftware hebben die opnieuw zouden kunnen worden geïmplementeerd of uitgefaseerd. Daarnaast biedt een helder beeld van licenties de mogelijkheid tot up-to-date beheer.

- **Rapportage**: Gecentraliseerde rapporten geven uitgebreide informatie over alle software en hardware in het netwerk, plus de gebruiksgeschiedenis. Inzicht op basis van deze rapporten maakt het beheer van het gebruik onder groepen op elk niveau mogelijk.

Licentiecontrole kan tijdrovend en complex zijn. Wanneer u deze taak automatiseert, bespaart u niet alleen tijd maar weet u ook zeker dat het bedrijf voldoet aan enkele best practices zoals naleving, kosteneffectief software- en hardwarebeheer en uitgebreid inzicht in uw netwerk. Een kleine moeite met grote voordelen.

5. SCHAKEL GEAVANCEERDE VULNERABILITYBEOORDELING EN PATCHBEHEER IN

Het beheren en toepassen van software-updates en tegelijkertijd controleren op mogelijke vulnerability's is een van de belangrijkste, meest uitdagende en meest intensieve taken van de IT-afdeling.

IT-beheerders worden continu geconfronteerd met nieuwe, doelgerichte dreigingen en criminelen scannen systemen voortdurend op zwakke plekken. Het is dus van groot belang dat beveiligingslekken worden gevonden en opgelost voordat er misbruik van wordt gemaakt.

Vulnerabilitybeoordeling voert deze taak voor u uit: het scannen van de apparaten en software in het netwerk op zwakke plekken die kunnen worden misbruikt. Gevonden zwakke plekken kunnen worden opgelost met patchbeheer, waarbij de nodige updates of reparaties worden toegepast op alle computers in het netwerk.

Vulnerabilitybeoordeling kan naast een effectieve patchbeheerstrategie worden gebruikt en u helpen cybercriminelen een stap vóór te blijven. Wij weten hoe:

- **Altijd up-to-date**: Verouderde software op servers en werkstations stelt het bedrijf aan aanvallen bloot. Met geautomatiseerde softwarescans worden vulnerability's snel gedetecteerd en geprioriteerd.

Kaspersky Systems Management maakt de snelste automatische levering van patches en updates mogelijk voor software van Microsoft en andere software. Voor nog meer controle krijgen beheerders meldingen over de status van patchinstallaties. Niet-kritieke fixes kunnen via Wake-on-LAN worden uitgesteld tot na werktijd, zelfs als de computers zijn uitgeschakeld. Met Multicast-technologie kunnen patches en updates lokaal naar externe vestigingen worden gedistribueerd, zodat er minder bandbreedte nodig is.

Door de implementatie van software-updates en de bijbehorende administratieve taken te automatiseren, minimaliseert u de downtime die ontstaat door de implementatie, de controle en het ongedaan maken van patches.

- **Genereer rapporten**: Voer rapporten uit op scans voor nog een laag aan inzicht in de IT-beveiliging van uw organisatie. Onderzoek en rapporteer potentiële zwakke plekken, houd wijzigingen bij en krijg gedetailleerd inzicht in de patchstatus van elk apparaat en systeem in het netwerk.

Gerichte aanvallen, geavanceerde aanhoudende dreigingen, geautomatiseerde aanvallen en zero-day beveiligingslekken verkorten de tijd tussen de ontdekking van het probleem en het misbruik. Door beoordelingen en patchimplementatie te automatiseren en te plannen, kunnen IT-beheerders deze processen stroomlijnen zonder in te leveren op de effectiviteit ervan.

6. GECENTRALISEERD BEHEER EN ROLE-BASED ACCESS CONTROL

Door het centraliseren en automatiseren van belangrijke taken voor beveiliging, configuratie en beheer, zoals vulnerabilitybeoordeling, patch- en update-distributie, inventarisatiebeheer en het uitrollen van applicaties, besparen IT-beheerders niet alleen tijd, maar wordt ook de beveiliging geoptimaliseerd.

Eén geïntegreerde beheerconsole, het Kaspersky Security Center, ondersteunt via één interface het beheer van de systeembeveiliging voor alle desktops, mobiele apparaten en virtuele endpoints in het netwerk. In complexe bedrijfsnetwerken maakt Role-Based Access Control (RBAC) de aanpassing van consoleweergaven en -functionaliteit mogelijk op basis van de rol, rechten en machtigingen van de beheerder. Een bepaalde beheerder kan bijvoorbeeld alle IT-beveiligingsbeheergebieden op de console zien, maar alleen de functies voor vulnerability en patchbeheer bewerken.

7. SIEM-INTEGRATIE VOOR BEDRIJFSOMGEVINGEN

Veel organisaties, in het bijzonder ondernemingen, gebruiken SIEM-systemen (Security Information and Event Management) om logboeken en andere beveiligingsgerelateerde gegevens te verzamelen voor analysedoeleinden. Beveiligingssystemen die kunnen rapporteren aan toonaangevende SIEM-systemen, ontlasten de beheerder en de benodigde tools, terwijl het rapportageproces binnen de onderneming wordt vereenvoudigd.

Kaspersky Systems Management integreert met IBM QRadar en HP ArcSight voor het overzetten van events.

TOT SLOT...

Softwarevulnerability's zijn de focus van goed geplande, doelgerichte aanvallen geworden op bedrijven van elke omvang. Effectief applicatie- en patchbeheer in combinatie met vulnerabilitybeoordeling en andere mogelijkheden voor systeembeheer kunnen zorgen voor een geïntegreerde benadering van de IT-beveiliging in uw bedrijf.

Systems Management van Kaspersky is een beheerde component van het Kaspersky Security Center. Alle functies kunnen vanuit deze centrale console worden beheerd via logische, intuïtieve opdrachten en interfaces voor de automatisering van routinetaken voor IT-beheer en een betere beveiliging van uw bedrijf.


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