Microsoft

Betere beveiliging van het besturingssysteem Met Windows Server 2016

De steeds verfijndere aanvallen vereisen nieuwe beveiligingslagen.

Door nieuwe cyberdreigingen wordt het voor IT-afdelingen alsmaar moeilijker om gegevens en toepassingen te beveiligen. De aanvallen worden steeds geavanceerder, waarbij vaak wordt gebruikgemaakt van bevoorrechte beheerdersreferenties die zijn gehackt. Dankzij de referentie kunnen aanvallers lang onopgemerkt blijven en op elk moment een verwoestende aanval uitvoeren.

Met name gevirtualiseerde virtuele omgevingen lopen een risico. Virtuele machines beschikken namelijk niet over de oplossingen voor hardwarebeveiliging waarover fysieke servers beschikken. Omdat virtuele machines worden geïnstantieerd door bestanden die kunnen worden gekopieerd en gewijzigd, heeft elke aanvaller met toegang tot de opslag van de infrastructuur, het netwerk of computerresources meteen bevoegdheden voor alle virtuele machines die niet worden gecontroleerd. Het is voor een aanvaller dan ook heel eenvoudig om de VM's met uw SQL en domeincontroller naar een USB-station te kopiëren en er met uw waardevolle gegevens vandoor te gaan.

Beveiligen, detecteren en reageren

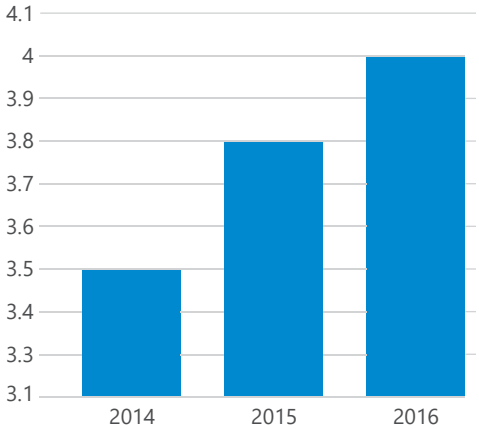
Windows Server 2016 bevat ingebouwde technologieën tegen schendingen om aanvallen op uw systemen te voorkomen en ervoor te zorgen dat u voldoet aan het nalevingsbeleid. Zelfs als een aanvaller een ingang in uw omgeving heeft gevonden, beperken de ingebouwde beveiligingslagen in elk Windows Server 2016-systeem de schade die kan worden toegebracht. Tijdens de implementatie worden verschillende functies voor isolatie van referenties en beveiliging tegen bedreigingen ingesteld. U kunt indien gewenst nog extra beveiligingsfuncties instellen om:

- Pass-the-Hash-aanvallen en andere pogingen tot het hacken van beheerdersreferenties te blokkeren.
- Te voorkomen dat op de servers malware en ransomware wordt geïnstalleerd.
- Snel gedrag te identificeren dat duidt op een schending van de server.
- De beveiliging voor uw fysieke servers uit te breiden naar uw virtuele machines.

"Afgeschermde virtuele machines verwijderen een hostingobstakel en maken absoluut het verschil. Alleen Microsoft beschikt momenteel over deze technologie."

– Philip Moss
Chief Product Officer
Acuutech

Globale kosten van gegevensschendingen per organisatie ($M)



De kosten van gegevensschendingen nemen elk jaar toe en bedragen momenteel gemiddeld vier miljoen dollar per incident.

Bron: Cost of Data Breach Study, IBM, Ponemon

Betere beveiliging van het besturingssysteem

Windows Server 2016 biedt eersteklas beveiliging waarmee organisaties kunnen voldoen aan de strengste organisatie- en industrienormen. De infrastructuur en toepassingen worden on-premises en in de cloud beveiligd op fysieke en virtuele servers.

"Met afgeschermde virtuele machines kunnen we de VM-werkbelasting beter beveiligen. In het verleden was dit complex of simpelweg onmogelijk. Nu schermen we de virtuele machines gewoon af. Dat is alles.."

– Rand Morimoto, President, Convergent Computing

Bedrijven moeten het volgende doen:	Voorbeeld van een bedreiging:	Windows Server 2016 helpt als volgt:
Beheerdersreferenties beveiligen	Via een Pass-the-Hash-aanval krijgt een aanvaller de beschikking over beheerdersreferenties voor het netwerk van een ziekenhuis. De aanvaller gebruikt de referenties om toegang tot vertrouwelijke patiëntgegevens te krijgen.	Met Just Enough Administration en Just-in-Time Administration kunt u voorkomen dat aanvallers toegang krijgen tot belangrijke gegevens, zelfs als ze toegang hebben tot beheerdersreferenties. Met Credential Guard voorkomt u dat beheerdersreferenties worden gestolen via Pass-the-Hash- en Pass-the-Ticket-aanvallen. Remote Credential Guard voorziet in SSO (eenmalige aanmelding) voor Remote Desktop Protocol-sessies (RDP) zodat de referenties niet aan de RDP-host hoeven te worden doorgegeven.
Servers beveiligen, dreigingen opsporen en op tijd reageren	Een aanvaller heeft met ransomware op servers van een universiteit ervoor gezorgd dat gebruikers geen toegang hebben tot belangrijke gegevens over studenten en onderzoeken zolang er geen geld wordt betaald aan de aanvaller.	Met Device Guard zorgt u ervoor dat alleen toegestane binaire bestanden kunnen worden uitgevoerd. Met controlestroombeveiliging kunt u aanvallen op het geheugen voorkomen. Windows Defender helpt ook bij de beveiliging tegen bekende beveiligingsproblemen zonder impact voor serverrollen (zoals webservers).
	Een ontwikkelaar van Line-Of-Business-toepassingen downloadt code van het openbare internet om deze in haar toepassing te integreren. De gedownloade code bevat malware die via de gedeelde kernel activiteit in andere containers kan bijhouden.	U kunt containertoepassingen isoleren met Hyper-V-containers zonder wijzigingen aan te brengen in de installatiekopie van de container. U kunt de impact van de aanval minimaliseren dankzij de functies voor implementatie van Just-Enough-besturingssystemen van Nano Server.
Snel schadelijk gedrag opsporen	Malware probeert toegang te krijgen tot Aanmeldingsgegevensbeheer op een Windows-server om zo toegang tot de gebruikersreferenties te krijgen.	U kunt de beveiligingscontrole optimaliseren met uitgebreide logboekregistratie voor detectie van bedreigen. Dit omvat controletoegang tot de kernel en andere gevoelige processen. Met deze gedetailleerde gegevens kan Microsoft Operations Management Suite (OMS), een beheersysteem voor beveiligings- en informatiegebeurtenissen, informatie leveren over potentiële aanvallen via de functie Log Analytics.
Virtualiseren zonder concessies aan de beveiliging	Een aanvaller heeft toegang tot de beheerdersreferenties bij een bank, waardoor hij toegang heeft tot gevirtualiseerde Active Directory-domeincontrollers en SQL-databases waarin de gegevens over de rekeningen van klanten zijn opgeslagen.	U kunt afgeschermde virtuele machines, VM's van de tweede generatie, maken die een virtuele TPM hebben en zijn versleuteld met BitLocker. De VM's kunnen alleen op goedgekeurde hosts in de infrastructuur worden uitgevoerd. De Host Guardian-service zorgt ervoor dat elke host de beveiligingsstatus moet controleren voordat afgeschermde virtuele machines worden opgestart of gemigreerd.

Zet de volgende stap. Ga naar www.Microsoft.com/WindowsServer2016 voor meer informatie.

Microsoft