BEST PRACTICES

BEDREIGINGS-PREVENTIE Basics

jamf

Wat hebben fietsen, een standbeeld van een paard, helikopters en een wenkbrauwloos portret van een vrouw met elkaar gemeen? Leonardo da Vinci, natuurlijk! Deze typische homo univiversalis uit de Renaissance maakte een of andere versie van deze voorwerpen, waarvoor hij kennis nodig had van schilderen, beeldhouwen, wiskunde, natuurkunde, techniek enz.

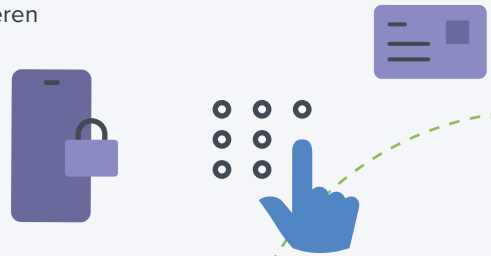
Voor organisaties met beperkte middelen kan het voelen alsof je de 'Renaissance-man' van je bedrijf moet zijn: leidinggevende, manager, IT-professional, boekhouder enzovoort. Bij Jamf kunnen we je belastingen niet doen, maar we kunnen je wel helpen om de belangrijkste aspecten van bedreigingspreventie te leren kennen en om te leren wat je in gedachten moet houden als best practices bij het beoordelen van je strategie voor bedreigingspreventie.

Wat is bedreigingspreventie?

Bedreigingen komen van verschillende bronnen en methodes. Ze kunnen eruit zien als een bijlage in een e-mail, een sms of een oproep om in te loggen op je bankrekening, websites die er *bijna* vertrouwd uitzien of helemaal nergens op lijken, zoals in het geval van apparaten met verouderde software met beveiligingslekken.

Bedreigingspreventie werkt achter de schermen om:

- te beschermen tegen bekende ransomware,Trojaanse paarden enz.
- AI te gebruiken om onbekende bedreigingen te identificeren
- te waarschuwen voor verdachte activiteiten
- te blokkeren tegen phishing-aanvallen en schadelijke websites
- de gezondheid van je apparaten te monitoren en registeren



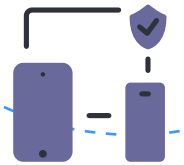
Heeft mijn organisatie bedreigingspreventie nodig?

Kort antwoord: Ja! Dat is ook zo. Ongeacht de grootte van je organisatie: als je bedrijfsgegevens hebt, moeten deze worden beschermd. Je organisatie *zal uiteindelijk* het slachtoffer worden van uitbuiting door cybersecurity, op zijn minst gericht, dus het is belangrijk om het risico hierop en de impact die een aanval zou hebben op je organisatie te verkleinen.

Aan de slag met bedreigingspreventie

Bedreigingen voorkomen betekent je apparaten en je netwerk beschermen. Een goed begin is om ervoor te **zorgen dat je apparaten up-to-date zijn**: verouderde besturingssystemen en apps met ongepatchte kwetsbaarheden maken het voor kwaadwillenden veel gemakkelijker om in je systemen te komen.

Het implementeren van een antivirus en EDR (Endpoint Detection and Remediation) tool verbetert je beveiliging nog verder. Antivirus werkt op de achtergrond om **bekende bedreigingen te identificeren** door het herkennen van verdachte activiteiten, informatie in bestanden die duidt op malware, schadelijke websites en IP-adressen, en nog veel meer. EDR gaat verder door **gebruik te maken van artificial intelligence (AI) en machine learning (ML) om bedreigingen te identificeren** die niet goed bekend zijn: cyberaanvallen ontwikkelen zich elke dag tot geavanceerdere en complexere bedreigingen, dus vergelijken met een database met bekende bedreigingen is niet genoeg.



Misschien klinkt dit als te veel om aan te pakken—wij zijn hier om je een oplossing te bieden. Jamf biedt oplossingen voor apparaatbeheer om je apparaten up-to-date te houden en je tegelijkertijd inzicht te geven in de compliance van het beveiligingsbeleid. En onze beveiligingssoftware beschermt je apparaten tegen bekende en onbekende bedreigingen zonder de gebruiker te belasten. Of je Jamf nu gebruikt voor je beheer- of beveiligingsoplossingen, houd deze best practices in gedachten:

1. Eisen dat apparaten en software de meest recente besturingssystemen (OS) draaien en dat apps worden beheerd, geverifieerd en bijgewerkt.

2. Vertrouw niet simpelweg op de meest veilige out-of-box hardware. Bescherm je Apple vloot en gebruikers met een op Apple gerichte oplossing voor eindpuntbescherming.

3. Laat technologie *voor* je werken en integreer AI en ML in je beveiligingsstrategie met EDR.

Meer informatie? In ons e-book Bedreigingspreventie voor beginners gaan we dieper in op tactieken en oplossingen voor bedreigingspreventie.

Of als je er klaar voor bent, kun je onze software eens proberen.

jamf

www.jamf.com/nl/