BlackBerry

Whitepaper

DOOR AI GESTUURDE BEVEILIGING VOOR EEN MOBIELE WERELD

Hoe BlackBerry Mobile Threat Defense gebruikmaakt van AI-gebaseerde cyberbeveiliging om mobiele apparaten te beveiligen en de gebruikerservaring te vereenvoudigen

Interessant feit: Er zijn nu meer mobiele apparaten ter wereld – meer dan 7 miljard – dan er mensen zijn.[1] Het zou dus ook geen verrassing moeten zijn dat meer dan de helft van alle apparaten die tegenwoordig met het internet zijn verbonden, mobiele apparaten zijn.[2] Inderdaad, er zijn nu meer Android™-verbindingen met het internet dan Windows®-verbindingen.[3]

De explosie van mobiele apparaten heeft echter ook een duistere keerzijde: de opkomst van mobiele malware- en cyberaanvallen. Een recent rapport van Verizon geeft aan dat nu bij één op de drie aanvallen op bedrijven een mobiel apparaat het doelwit is.[4] Ook neemt de frequentie van de aanvallen toe: in de afgelopen jaren is het aantal mobiele malware-incidenten met dubbele of zelfs driedubbele cijfers gestegen.[5]

De gevolgen van mobiele aanvallen kunnen enorm zijn, met kosten die vergelijkbaar zijn met de kosten van “traditionele” cyberaanvallen op servers en desktopcomputers. Brancheanalist Aberdeen schat dat mobiele phishing-aanvallen bedrijven meer dan USD 200 miljoen kosten, waarbij de mediane kosten op ongeveer USD 500.000 liggen.[6] De recente CopyCat-aanval, waarmee 14 miljoen Android-apparaten werden geïnfecteerd, leverde de hackers in twee maanden tijd USD 1,5 miljoen aan gestolen advertentie-inkomsten op.[7]

De realiteit is dat mobiele apparaten een bijzonder aantrekkelijke ingang voor uiteenlopende kwaadwillende partijen bieden. Apps die naar mobiele telefoons worden gedownload, kunnen bijvoorbeeld eenvoudig als vector voor malware worden benut. Mobiele netwerken kunnen worden gecompromitteerd met behulp van man-in-the-middle-technieken om mobiel verkeer te onderscheppen. Voor mobiele eindpunten blijkt de kans op compromittering ruim twee keer zo hoog te zijn als voor servers.[8] Wat nog zorgwekkender is, is dat gebruikers een mobiele aanval vaak helemaal niet in de gaten hebben. Malware staat soms wel meer dan een jaar ongemerkt op een apparaat terwijl die al die tijd gegevens en resources steelt.[9]

Mobiele aanvallen in cijfers

- **Jaarlijks vinden er meer dan 42 miljoen** mobiele malware-aanvallen plaats[10]
- **63%** van de grayware-apps lekt het telefoonnummer van het apparaat[11]
- **Bijna 1 op de 5** zakelijke en branche-apps lekt persoonlijke gegevens[12]
- Cyberaanvallen op smartphones zijn in de eerste helft van 2019 met 50% toegenomen ten opzichte van 2018[13]
- **25%** van de lekken blijft één tot vier jaar lang onopgemerkt[14]

Van optioneel naar verplicht

In verband met de zeer reële en toenemende kans op aanvallen, voeren bedrijven hun bescherming tegen mobiele gevaren op. De groeiende populariteit van BYOD-regelingen (Bring Your Own Device) op het werk heeft het voor organisaties echter lastiger gemaakt om doeltreffende risicobeperkende maatregelen in te voeren. Omdat de huidige generatie technisch goed onderlegde gebruikers hun apparaten nu zowel privé als zakelijk verwachten te gebruiken, hebben de meeste bedrijven besloten om privé-apparaten op de werkplek niet meer te verbieden. Ook pogingen om diverse controlemechanismen in te voeren om alle mobiele apparaten “onder beheer” te stellen, zijn voor het merendeel ondoenlijk gebleken.[15]

Voor steeds meer bedrijven ligt de oplossing in de invoering van Mobile Threat Defense (MTD), een verzameling snel opkomende mobiele beveiligingsvoorzieningen. Deze oplossingen gaan verder dan traditionele EMM-oplossingen (Enterprise Mobile Management), doordat ze een extra beveiligingslaag bieden: ze voorkomen en detecteren bedreigingen, voeren herstelmaatregelen uit en verbeteren de algehele beveiligingsgebruiken voor de volledige mobiele vloot en toepassingen van een organisatie.

“De noodzaak voor Mobile Threat Defense… is duidelijk voor elke onderneming die haar mobiele transformatie serieus neemt”, schrijft Jason Koestenblatt in Enterprise Mobility Exchange.[16] Volgens Gartner zal in 2020 30% van de organisaties MTD hebben ingevoerd, ten opzichte van nog geen 15% in 2019.[17]

Zero Trust: De basis van mobiele beveiliging

Volgens Aberdeen zouden de doeltreffendste oplossingen voor mobiele beveiliging moeten zijn gebaseerd op het principe van “Zero Trust”. Dit concept, dat meer dan 15 jaar geleden is ontwikkeld, houdt in dat “toegang tot bedrijfsresources altijd wordt verleend op voorwaarde dat zowel vóór als na de eerste verbinding een bepaalde mate van zekerheid wordt verkregen voor apparaten, gebruikers, en normale gedragingen en locaties.”[18]

Zero Trust vormt de basis voor de aanpak van de continu aanwezige risico’s met betrekking tot beveiliging, privacy en naleving van regelgeving die uit het gebruik van mobiele apparaten voortvloeien. MTD-oplossingen die gebruikmaken van Zero Trust-principes controleren alle mobiele apparaten op risico’s en kwetsbaarheden voordat gebruikers toegang krijgen tot de infrastructuur en gegevens van het bedrijf. Vervolgens bewaken ze doorlopend het beveiligingsprofiel en de status van alle mobiele apparaten, inclusief het gebruikersgedrag, zolang die apparaten verbinding hebben.[19]

De beste MTD-oplossingen bieden continu bescherming tegen cyberaanvallen en dwingen strenge authenticatie af in risicovolle situaties (“Zero Trust”). Tegelijkertijd stroomlijnen ze ook de toegang voor gebruikers die onder normale werkomstandigheden en op bewezen veilige locaties toegang tot systemen willen hebben (“Zero Touch”).

Zoals Aberdeen uitlegt, is het doel van MTD niet om je gebruikers te vertragen, maar om ze te helpen sneller te werken in normale gebruiksomstandigheden die een laag risico vormen. Anders gezegd: MTD-oplossingen die op Zero Trust-principes zijn gebaseerd, zijn goed in het bieden van bescherming tegen het “slechte” – alle mobiele dreigingen die uw organisatie grote schade kunnen berokkenen – terwijl ze ook het “goede” mogelijk maken: alle bewezen voordelen op het gebied van productiviteit, gemak en schaalbaarheid die mobiele apparaten de onderneming opleveren.[20]

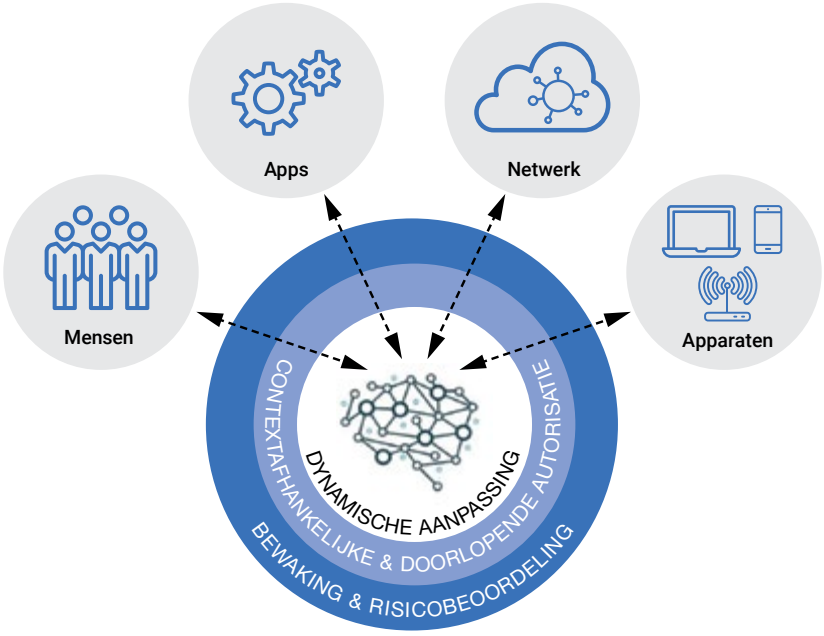
BlackBerry Protect: Overbrugging van kloof tussen Zero Trust en Zero Touch

De mogelijkheid om strenge mobiele beveiliging te integreren met slimme beleidsaanpassing is wat BlackBerry “de overbrugging van de kloof tussen Zero Trust en Zero Touch” noemt. Dit is een van de kernvoorzieningen van BlackBerry Protect®, de geavanceerde MTD-oplossing van BlackBerry.

De door kunstmatige intelligentie (artificial intelligence, “AI”) aangestuurde bedreigingendetectie van BlackBerry Protect werkt continu aan de bescherming van alle eindpunten en mobiele apparaten, zonder de eindgebruikers in de weg te zitten. Het combineert de beste elementen van de Zero Trust- en Zero Touch-architectuur om de beleidsregels en beveiligingsniveaus automatisch aan te passen op basis van de locatie, het gedrag en het apparaat van de gebruiker.

BlackBerry Protect integreert met BlackBerry UEM en gebruikt kunstmatige intelligentie om uw mobiele eindpunten te beveiligen tegen zero-day-bedreigingen.

Zero Trust-architectuur van BlackBerry



Doorlopende eindpuntbeveiliging

Tegenwoordig gebruiken organisaties BlackBerry Protect om hun mobiele apparaten te beschermen tegen geavanceerde, kwaadwillige bedreigingen, als aanvulling op de beveiligingsbasis waar BlackBerry® Unified Endpoint Manager (UEM) voor zorgt. De MTD-oplossing bewaakt bedreigingen voor zowel apparaten als toepassingen en gaat verder dan de beveiliging die BlackBerry's toepassingscontainers bieden.

Apparaten. Signaleert kwetsbaarheden en potentiële schadelijke activiteiten door toezicht te houden op updates van het besturingssysteem, systeemparameters, apparaatconfiguraties en systeembibliotheken.

Toepassingen. Gebruikt sandboxing, codeanalyses en appbeveiligingstests om malware en grayware te herkennen.

Daarnaast maakt BlackBerry Protect gebruik van detectie op basis van kunstmatige intelligentie en machine learning om malware te vinden die eventueel via gesideloade toepassingen binnenkomt. Dit voegt een extra beveiligingslaag toe aan het BlackBerry® Dynamics™ SDK-platform, BlackBerry's geavanceerde containerisatieoplossing voor mobiele apps. Bedrijven en hun partners kunnen nu een volledig pakket veilige toepassingen bouwen en aanpassen die op voor bedrijven toegankelijke apparaten kunnen worden geladen.

BlackBerry Protect kan nieuwe, opkomende bedreigingen voor de cyberbeveiliging detecteren en voorkomen. Het voorspellend vermogen is gemiddeld 25 maanden.

Geavanceerde bescherming tegen bedreigingen

Hoewel er veel oplossingen voor mobiele bedreigingen verkrijgbaar zijn, biedt BlackBerry Protect een unieke, krachtige set voorzieningen.

Het voordeel van de kunstmatige intelligentie van BlackBerry Cylance
BlackBerry Protect maakt gebruik van BlackBerry® Cylance®, dat in de branche bekend staat om zijn AI-technologie en geavanceerde machine-learningmogelijkheden. De cyberbeveiligingsoplossing BlackBerry Cylance beschermt tegen bekende en onbekende malware, aanvallen zonder bestanden, en zero-day-uitvoeringen van payloads.

Beveiliging voor alle beheerde en BYO-apparaten
Wanneer BlackBerry Protect is geïntegreerd in het BlackBerry UEM-platform, kunnen organisaties er gerust op zijn dat hun hele mobiele vloot wordt beveiligd, zonder dat medewerkers apps van derden hoeven te onderhouden. Omdat bovendien de noodzaak voor handmatige configuratie van VPN's of VDI's wegvalt, kunnen organisaties de productiviteit van hun medewerkers verhogen en de kosten verlagen.

Eén handig overzicht
Met BlackBerry Protect hoeft u geen afzonderlijk product of aparte console op te zetten en te configureren, omdat BlackBerry Protect nauw is geïntegreerd in de BlackBerry UEM-server en -toepassingen. Dit houdt in dat de beveiligings- en beheerfunctionaliteit op één handige plek beschikbaar is.

Mobile Threat Defense om uw hele mobiele vloot te beschermen

- Beschermt mobiele eindpunten tegen malware- en phishing-aanvallen
- Scant mobiele toepassingen op bestaande malware
- Biedt volledige eindpuntbeveiliging voor alle apparaten, waaronder BYOD-apparaten
- Rechtstreeks geïntegreerd in BlackBerry® Dynamics™-apps en beheerd door BlackBerry UEM

BlackBerry tot leider uitgeroepen in de IDC MarketScape-rapporten over de segmenten UEM, EMM en EMM voor implementaties van robuuste/IoT-apparaten

IDC heeft BlackBerry in drie recente IDC MarketScape-onderzoeken opnieuw erkend als leider in het marktsegment Enterprise Mobility. Deze bevindingen bevestigen wederom de status van BlackBerry als voorkeursleverancier voor ondernemingen en overheden die software en services nodig hebben om mobiele apparaten én ingebouwde apparaten in de IoT-wereld te beveiligen.

- Een leider – IDC MarketScape: Worldwide Unified Endpoint Management Software 2019–2020 Vendor Assessment (documentnr. US45355119, november 2019)
- Een leider – IDC MarketScape: Worldwide Enterprise Mobility Management Software 2019–2020 Vendor Assessment (documentnr. US45353719, november 2019)
- Een leider – IDC MarketScape: Worldwide EMM Software for Ruggedized/IoT Device Deployments 2019–2020 Vendor Assessment (documentnr. US45353819, november 2019)

Conclusie

Bedrijven staan voor een zware taak. Ze moeten het hoofd bieden aan de groeiende dreiging van malware-aanvallen op mobiele apparaten, en met name op de apps die daarop worden uitgevoerd.

Beveiligingsanalisten uit de branche zijn het met elkaar eens: bedrijven moeten zich meer richten op het keren van het tij van mobiele bedreigingen, van malware-phishing tot en met datalekken, spyware en nog veel meer. Mobiele apparaten lopen twee keer zo veel kans op compromittering als desktops en servers, en kwaadwillende partijen gebruiken mobiele eindpunten vaak als springplank om zich toegang te verschaffen tot bedrijfsnetwerken en de waardevolle assets binnen die netwerken.

MTD-oplossingen zijn het antwoord op dit probleem en steeds meer bedrijven nemen dan ook MTD in hun beveiligingsbudget op. Toch zijn niet alle oplossingen hetzelfde. Door gebruik te maken van kunstmatige intelligentie en machine learning, levert BlackBerry een unieke mobiele beveiligingsoplossing die niet alleen de bescherming van Zero Trust biedt, maar ook de aanpasbare flexibiliteit van Zero Touch om het productieve potentieel van mobiele werknemers te ontketenen.

Meer informatie

Ga voor meer informatie over BlackBerry Protect naar www.blackberry.com/mtd.

Eindnoten

1 "How Many Phones Are in the World?," Bankmycell.com.
2 "Desktop vs. Mobile vs. Tablet Market Share Worldwide – November 2019," StatCounter.
3 "Mobile Threat Defense Now a Necessity for Enterprises," Enterprise Mobility Exchange.
4 "Mobile Security Index 2019," Verizon.
5 "The Current State of Mobile Malware," Wandera.
6 "'Zero Trust' For Enterprise Mobility: The Brakes that Help Your Users Go Faster," Aberdeen.
7 "How the CopyCat malware infected Android devices around the world," Check Point Software Technologies.
8 "'Zero Trust' For Enterprise Mobility: The Brakes that Help Your Users Go Faster," Aberdeen.
9 Ebd.
10 "Mobile malware evolution 2017," Kaspersky Lab.
11 "2019 Internet Security Threat Report," Symantec.
12 "2017 Mobile Leak Report," Wandera.
13 "Mobile malware attacks are booming in 2019: These are the most common threats," ZDNet.
14 "'Zero Trust' For Enterprise Mobility: The Brakes that Help Your Users Go Faster," Aberdeen.
15 Ibid.
16 "Mobile Threat Defense Now A Necessity For Enterprises," Enterprise Mobility Exchange.
17 Gartner, Market Guide for Mobile Threat Defense, Nov. 2019.
18 "'Zero Trust' For Enterprise Mobility: The Brakes that Help Your Users Go Faster," Aberdeen.
19 Ibid.
20 Ibid.

Over BlackBerry

BlackBerry (NYSE: BB; TSX: BB) levert intelligente beveiligingssoftware en services aan ondernemingen en overheden over de gehele wereld. Het bedrijf beveiligt op dit moment meer dan 500 miljoen eindpunten, waaronder 150 miljoen auto's. Het in Waterloo, Ontario, gevestigde bedrijf maakt gebruik van kunstmatige intelligentie en machine learning om innovatieve oplossingen te leveren op het gebied van cyberbeveiliging, veiligheid en gegevensprivacy, en is een leider op het gebied van eindpuntbeveiligingsbeheer, versleuteling en ingebouwde systemen. BlackBerry heeft een duidelijke visie: om een verbonden toekomst mogelijk te maken die u kunt vertrouwen.

BlackBerry. Intelligente beveiliging. Overal.

Ga voor meer informatie naar BlackBerry.com en volg @BlackBerry.