

Gehackte applicaties vormen gevaar voor het bedrijfsnetwerk



Werknemers gebruiken steeds vaker persoonlijke mobiele apparaten op de werkvloer. Het overgrote merendeel van de mobiele applicaties is inmiddels echter gekraakt, waardoor IT-afdelingen steeds vaker te maken krijgen met onveilige applicaties die door werknemers op smartphones en tablets zijn geïnstalleerd. Dit leidt tot onveilige situaties. Hiervoor waarschuwt het beveiligingsbedrijf Arxan Technologies.

Het bedrijf concludeert in een infographic dat maar liefst 97% van de top 100 meest gedownloadde betaalde apps voor het Android-platform is gehackt. Op het iOS-platform ligt dit percentage met 87% eveneens hoog. Het bedrijf waarschuwt dat deze mobiele applicaties door hackers kunnen worden gebruikt als uitgangspunt bij een cyberaanval op een bedrijfsnetwerk.

Een gehackte applicatie is niet per definitie kwaadaardig. Het kan hierbij ook gaan om een betaalde applicatie waarvan de beveiliging is gekraakt zodat deze gratis kan worden verspreid. In andere gevallen zijn apps wel kwaadaardig en hebben hackers de software bijvoorbeeld doelbewust voorzien van malware om toegang te verkrijgen tot mobiele apparaten. Ook kunnen hackers adware (ongevraagde advertenties) aanbrenge in de gehackte mobiele applicaties.

De hoeveelheid applicaties die zijn gehackt varieert sterk per soort. Zo is 70% van de financiële apps op het iOS-platform en 95% van de financiële apps op het Android-platform gehackt. Als we echter kijken naar medische applicaties heeft Arxan Technologies op het iOS-platform geen enkele gekraakte applicatie kunnen vinden. Op het Android-platform is dit een ander verhaal. 90% van de medische applicaties voor het Android-platform is gehackt. Vaak alleen beschikbaar via alternatieve app winkels

Bij de waarschuwing moet een kleine kanttekening worden geplaatst. Het overgrote merendeel van de gekraakte applicaties waar Arxan Technologies over spreekt zijn uitsluitend beschikbaar via alternatieve appwinkels, die standaard niet beschikbaar zijn op het iOS- en Android-platform. Gebruikers moeten in de meeste gevallen dan ook bewust op zoek gaan naar gehackte applicaties, waardoor de meeste werknemers dit soort applicaties niet snel zullen gebruiken.

Desondanks lopen bedrijven wel degelijk het risico geconfronteerd te worden met gehackte applicaties, die zeker niet altijd veilig zijn. Arxan Technologies waarschuwt dan ook terecht dat gehackte mobiele applicaties als uitgangspunt kunnen worden gebruikt voor het opzetten van een cyberaanval op een bedrijfsnetwerk. De Bring Your Own Device (BYOD)-trend maakt het dan ook noodzakelijk dat bedrijven aandacht besteden aan de beveiliging van mobiele applicaties op de persoonlijke apparaten van werknemers.