Suid-Afrikaanse Tydskrif vir Natuurwetenskap en Tegnologie
ISSN: (Online) 2222-4173, (Print) 0254-3486

’n Hoëvlak-model vir die byvoeging van forensiese gereedheid tot mobiele toestelbestuur

Authors:
Elsabé Ros, HS Venter

Affiliations:
Departement Rekenaarwetenskap, Universiteit van Pretoria

Corresponding author:
Elsabé Ros
elsabe.ros@gmail.com
Departement Rekenaarwetenskap, Universiteit van Pretoria, Privaatsak X20, Hatfield, 0028

How to cite this article:
Elsabé Ros, HS Venter, ’n Hoëvlak-model vir die byvoeging van forensiese gereedheid tot mobiele toestelbestuur, *Suid-Afrikaanse Tydskrif vir Natuurwetenskap en Tegnologie* 37(1) (2018)

A high-level model for providing forensic readiness to mobile device management: Existing mobile device management software used to manage smart devices in organizations, is purely preventative and do not offer historical data. Adding digital forensic readiness enables investigation of incidents without impacting employees’ usage of their devices.

In die era voordat slimfone populêr geraak het, was dit taamlik maklik vir besighede om toegang tot hul netwerke, stelsels en inligting te beheer. Baie besighede het die waarde daarvan gesien om slimfone vir besigheidsdoeleindes te gebruik, maar vir besighede om ’n slimfoon aan elke werknemer te verskaf is nie altyd moontlik nie. Daarom het baie besighede besluit om werknemers toe te laat om hul eie slimfone te gebruik, wat bekend staan as “Bring your own device” (BYOD). Hierdie beleid hou egter risiko’s vir besighede in, omdat hierdie slimfone nie aan hulle behoort nie en ook nie deur hulle beheer word nie, maar deur eienaars van die toestelle. Een van die populêre oplossings vir hierdie probleem is ’n mobiele toestelbestuur (“Mobile device management”) stelsel. Mobiele toestelbestuurstelsels is egter slegs voorkomend, wat beteken dat wanneer ’n voorval plaasvind, die ondersoekers nie historiese data oor die gebruik van die slimfoon kan bekom nie.

Digitale forensiese gereedheid (DFG) fokus daarop om die koste van forensiese ondersoeke te verminder en om enige data relevant tot ’n ondersoek so vinning en akkuraat as moontlik bymekaar te maak (Tan 2001). Deur DFG tot ’n bestaande mobiele toestelbestuurstelsel te voeg, kan aan besighede beide die voorkomende aspek van die stelsel en die krag van forensiese gereedheid bied. Daar is drie komponente in ’n mobiele toestelbestuurstelsel, naamlik ’n mobiele kliënt, ’n bediener en ’n databasis (Open Mobile Alliance 2016). Hierdie drie komponente word aangepas om DFG aan die stelsel te voorsien.

Die mobiele kliënt, wat voorheen net toegang geblokkeer het, kan nou agterkom wanneer die gebruiker van die slimfoon ’n aksie probeer uitvoer wat nie toelaatbaar is nie. Wanneer die mobiele kliënt so ’n situasie bespeur, maak dit data bymekaar oor die gebruiker se aksies en laai die data na die bediener op. Die bediener ontvang die data en stoor dit in die databasis. Die data word geassosiëer met die gebruiker wat die aksies geneem het.

Aangesien hierdie data moontlik gebruik kan word in kriminele sake, is dit belangrik dat die integriteit van die data in ’n geregshof bewys sal kan word. Dit word gedoen deur ’n toetskode (“checksum”) te gebruik. Die toetskode is ’n waarde wat verkry word deur verskeie wiskundige operasies op die data uit te voer. Die waarde wat verkry word is uniek tot die data en sal verander as die data enigsins verander. Deur te wys dat die toetskode van die data dieselfde gebly het regdeur die proses, kan bewys word dat die data nie verander het nie.

Hierdie model laat besighede toe om data van werknemers se persoonlike slimfone te kry, ten einde onwettige aksies te verhoed. Die feit dat die oplossing outomaties werk, verminder kostes en bespoedig ondersoeke. Hierdie oplossing kan wel die privaatheid van werknemers skend, omdat data oor hul aksies bymekaar gemaak word. Aangesien hierdie oplossing egter vir groot besighede ontwerp is, kan besighede dit ’n voorwaarde van indiensneming maak dat werknemers tot die gebruik van die stelsel instem.

Literaatuurverwysings

Open Mobile Alliance, 2016, Device Management Architecturem aanlyn geraadpleeg op 11 Augustus 2018 by http://www.openmobilealliance.org

Tan, J., 2001, *Forensic Readiness Assessment*. Cambridge, MA:@ Stake, 1-23.

Nota: ’n Seleksie van referaatopsommings: Studentesimposium in die Natuurwetenskappe, 2–3 November 2017, Universiteit van Pretoria, Suid-Afrika. Reëlingskomitee: Prof Rudi Pretorius (Departement Geografie, Universiteit van Suid-Afrika); Dr Hertzog Bisset (Suid-Afrikaanse Kernenergie-korporasie – Necsa); Prof Marilé Landman (Departement Chemie, Universiteit van Pretoria).