DE TIJD

Smartphone werknemer maar zelden beveiligd

12 april 2017 01:00

Heel wat Belgische bedrijven hebben geen systeem om de smartphones van hun werknemers te beschermen tegen cyberinbraken in het interne bedrijfsnetwerk.

Slecht een op de tien Belgische bedrijven heeft een systeem in werking dat de toegang tot het interne bedrijfsnetwerk via mobiele toestellen van werknemers beschermt. Dat meldt het onderzoeksbureau Computer Profile, dat 890 Belgische bedrijven bevraagde. Het maakt hun **interne netwerk kwetsbaar voor cybercriminelen** die via de smartphone van werknemers binnen willen dringen.

Heel wat bedrijven geven werknemers een smartphone om taken uit te voeren. Omdat **mobiele toestellen** de werkvloer verlaten en ook privé gebruikt worden, hebben ze extra beveiliging nodig. Bedrijven hebben de keuze om alle werknemers eenzelfde toestel te geven of om volgens het Bring Your Own Device-principe de werknemer te laten kiezen welk toestel hij wil. Hoe meer variatie, hoe complexer de beveiliging moet zijn.

Android

Door de versnippering van de smartphonemarkt en vooral van Android-toestellen, zijn er heel wat onveilige toestellen. Apple, dat soft- en hardware in handen heeft, kan een update van het besturingssysteem opleggen. Bij Android hebben de hardwareproducenten de keuze tussen verschillende versies, waardoor niet alle toestellen de nieuwste en best beveiligde versie draaien. Die keuze probeert Google nu terug te schroeven om met Apple te kunnen concurreren. Toch worden vooral toestellen van Apple en Samsung aangeraden als bedrijfssmartphones *(zie hieronder)*.

Een smartphone verbindt zich met heel wat **wifinetwerken op verschillende locaties**. Wie zich bijvoorbeeld op een terrasje verbindt met een wifi-hotspot verhoogt het gevaar voor hacking of malware. ‘De meeste grote lekken komen vooral via mobiele toestellen, omdat die kwetsbaarder en mobieler zijn’, zegt Sofien Ben Sassi, product manager EMM bij Proximus. De telecomoperator beveiligt de toestellen van zijn werknemers en biedt de dienst ook aan klanten aan.

Apart werkgedeelte

Erwin Geirnaert van het cybersecuritybedrijf Zion Security haalt ook aan dat heel wat bedrijfsleiders hun smartphone en bedrijfslaptop thuis laten als ze naar China, de Verenigde Staten of Rusland reizen. ‘Ze gaan ervan uit dat zodra ze op een buitenlands netwerk zitten, er al hackers in hun toestel zitten.’

Om het veiligheidsrisico in te dijken is er nood aan een systeem dat de toegang tot het interne netwerk via de mobiele toestellen afschermt. Met **Enterprise Mobility Management (EMM)** wordt het toestel opgesplitst in een **privaat en een werkgedeelte.** De apps in het werkgedeelte krijgen de nodige beveiliging en versleuteling.

EMM-systeem

De **kostprijs** van zo'n beveiligingssysteem ligt tussen 2 en 8 euro per maand per gebruiker, de bouw van apps niet inbegrepen. 'Zodra het systeem er staat, is het vrij eenvoudig en goedkoop om nieuwe apps toe te voegen', zegt Ulrik Van Schepdael van Mobco, een bedrijf dat EMM-systemen bouwt.

Een goed EMM-systeem moet ook **gebruiksvriendelijk** zijn. 'We willen geen ellenlange wachtwoorden onthouden of authentificatiestappen doorlopen. Het moet simpel en veilig', zegt Van Schepdael.

Verregaande controle over de werknemers hun toestellen betekent **niet dat de werkgever ook toegang krijgt tot de persoonlijke data.** Het bedrijf krijgt via een EMM enkel controle over de data en apps die het zelf op het toestel zet. Persoonlijke berichten en foto's blijven afgeschermd.

Bron: De Tijd
