Cyber Weerbaarheidscentrum Greenport

Mobiele apparatuur

Bijna elke werknemer heeft een mobiel apparaat. Zoals een tablet of smartphone. Je kunt van alles met een mobiel apparaat: internetten, e-mailen en sms'en, maar ook whatsappen, facebooken en skypen. Hoe beveilig je mobiele apparaten? En hoe zorg je ervoor dat niet iedereen precies weet waar je bent en welke data je rondstuurt?

Beveilig je mobiele apparatuur

Je mobiele apparaat staat vol zakelijke en belangrijke informatie. Denk bijvoorbeeld aan de contactgegevens van zakelijke relaties op je tablet, de e-mails van klanten op je smartphone en je administratie op de laptop. Stuk voor stuk informatie waarvan je niet wil dat een cybercrimineel die inziet of kopieert. Door de mobiele apparaten van je bedrijf te beveiligen, kun je voorkomen dat dit gebeurt.
Zorg ervoor dat de mobiele apparaten van jouw onderneming goed beveiligd zijn. Een minimale beveiliging bestaat uit het uitvoeren van de laatst beschikbare software-updates, het veranderen van de standaardinstellingen, zoals die van wachtwoorden en toegangscodes, en het maken van een back-up. Op die manier gaat belangrijke bedrijfsinformatie niet verloren als een apparaat kwijt, defect of gestolen is.

Geavanceerde informatie over het beveiligen van mobiele apparatuur

Mobiele apparaten zoals smartphones en tablets zijn overal om ons heen en worden aan verschillende diensten en services gekoppeld. Ze zijn niet meer weg te denken uit het hedendaagse bedrijfsleven. Waar moet je aan denken bij het beveiligen van je mobiele (bedrijfs)apparatuur?

Gebruik Mobile device management

Als er veel smartphones beveiligd moeten worden, is het gebruik van Mobile Device Management (MDM) aan te raden. Een MDM-systeem houdt het gebruik van de mobiele apparatuur nauwlettend in de gaten. Bovendien kan het apparatuur isoleren en data wissen als het kwijtraakt of wordt gestolen. Ook kunnen de meeste MDM-systemen websites filteren en kun je als beheerder een white- of blacklist creëren die diensten en/of services toestaat of blokkeert.

Een groot voordeel van een MDM-systeem is dat je op afstand alle (of een subset) mobiele apparaten kan voorzien van organisatiebrede accountinstellingen zoals wifi, VPN en Exchange instellingen. Mocht je om privacyredenen voor je werknemers geen MDM-oplossing willen gebruiken is Mobile Application Management (MAM) ook een goed alternatief.

Update de software op je mobiele apparaat

Groot of klein, voor alle organisaties geldt dat het erg belangrijk is dat alle apparaten voorzien zijn van de laatste updates. Dit geldt voor apps die op de apparatuur zijn geïnstalleerd maar ook zeker voor het besturingssysteem (iOS, Android, etc.). Zorg ervoor dat werknemers geen apps vanaf een website of onbekende bron kunnen installeren, maar laat enkel toe dat dit vanuit een vertrouwde omgeving gebeurt, zoals de iOS Appstore of Google Playstore.

Bekijk goed welke rechten een app van het apparaat wil en of jij het daar mee eens bent. Heeft een app die je medewerker gebruikt voor videoconferenties toegang tot de zakelijke agenda of locatiegegevens? Vraag jezelf dan af of dit wel zo logisch is en bekijk goed of deze rechten wel echt noodzakelijk zijn voor de werking van de dienst.

Gebruik officiële firmware; 'root' systemen niet

Ook is het niet aan te raden om smartphones of tablets binnen de organisatie te jailbreaken of rooten. Op deze manier kun je, tegen de bedoeling van de fabrikant in, als gebruiker toegang krijgen tot het root-account en daarmee volledige beheer van het apparaat. Wanneer je dit doet is de garantie van het toestel niet meer geldig en kun je geen gebruik meer maken van ondersteuning van de leverancier. Softwarepatches vanuit het besturingssysteem worden niet meer geïnstalleerd waardoor het systeem mogelijk veel belangrijke beveiligingsupdates misloopt. Tevens is er veel malware in omloop die het specifiek voorzien heeft op rooted smartphones en tablets. Met name omdat de apparatuur door het rooten administratieve rechten heeft gekregen is dit voor een aanvaller extra interessant.

Dit document is gebaseerd op de documenten 'Mobiele apparatuur' en 'Geavanceerde informatie over het beveiligen van mobiele apparatuur'' van het Digital Trust Center. De originele documenten zijn te vinden via https://www.digitaltrustcenter.nl/informatie-advies/mobiele-apparatuur en https://www.digitaltrustcenter.nl/geavanceerde-informatie-over-het-beveiligen-van-mobiele-apparatuur