BYOD – kas firmadel tasub lubada oma töötajatel kasutada isiklikke seadmeid?

10 aastat tagasi Autor: Iteraction.ee

Kujuta ette olukorda, kus sinu ettevõttes on töötajatel töövahendid (sülearvuti, tahvelarvuti või nutitelefon), mis vastavad nende isiklikele eelistustele ja teevad neid rõõmsamaks. Mis veel parem, nad maksid nende eest ning kannavad ka ise hoolt seadmete eest. Kõige tipuks teevad nad tööd oma lõunapauside ajal või peale tööpäeva lõppu – see on üks peamine idee, mis on BYOD trendi taga. Muidugi pole kõik päris nii roosiline, kuid siiski teel selles suunas.

Tutvustamegi selles loos neljatähelist lühendit BYOD, toome välja selle IT strateegia rakendamise positiivseid ja negatiivseid külgi ning anname soovitusi ka selle rakendamiseks.

FOTO: (CC) INTEL FREE PRESS

Mis on BYOD?

BYOD ehk *Bring Your Own Device* tähendab sisuliselt seda, et ettevõte laseb töötajatel teha tööd ja pääseda seejuures ligi vajalikule infole läbi nende endi isiklike seadmete, olgu selleks siis süle- ja tahvelarvutid või nutitelefonid. Isiklike seadmete kasutamisel ettevõttes räägitakse ka eraldi BYOD strateegiast, kuna see nõuab IT poolelt mõningaid muutusi.

Mis on BYOD rakendamise eelised ja riskid?

Järgnevalt loetleme BYOD positiivseid ja ka negatiivseid külgi, et igaühel oleks lihtsam ise otsustada, kas BYOD on see, mille suunas liikuda või mitte.

BYOD plussid:

+ Üldiselt BYOD puhul maksavad töötajad täielikult ise oma seadmete riistvaralise poole eest ning lisaks ka teatud määral või täielikult kõnede ja tarkvaralise poole eest, seda eriti just näiteks nutitelefonide puhul. Good Technology State of BYOD Report toob välja, et ettevõtetes, kus on BYOD strateegia, maksavad töötajad seadmete eest ise 50% juhtudest ja teevad seda rõõmuga. See aga säästab ettevõttele otseselt raha.

+ BYOD puhul kasutavad töötajad töö tegemiseks just neid seadmeid, millega nad tunnevad end kõige mugavamalt ning mis neile kõige enam meeldivad. See omakorda kasvatab töötajate rahulolu. Töötajad on õnnelikumad!

+ Töötajad vahetavad tihemini oma seadmeid uute vastu, kui ettevõte ise seda teeks. Ning neil on võimalus uuendada seadet just siis, kui tunnevad selleks vajadust. Osad töötajad soovivad omada uusimaid seadmeid, miks neile seda siis keelata?

+ Suurem produktiivsus. Nagu tahvelarvutite artiklis varasemalt oleme ka maininud, teevad töötajad mobiilsete seadmetega rohkem tööd. BYOD on mõeldudki just mobiilsetele seadmetele ning julgustab kasutajaid olema mobiilsemad läbi oma lemmikseadmete kasutamise. Inteli poolt oma töötajate seas tehtud uuringust selgus, et töötajad teevad sel juhul iga päev kuni 51 minutit rohkem tööd.

+ Töövahendeid hoitakse paremini, kuna töötajad on nendesse isiklikult investeerinud.

+ BYOD puhul on seadmed korralikumad, kuna ei ole lähtutud ettevõtte IT eelarve piirangutest. Sageli tähendab see selliseid telefone ja arvuteid, mida ettevõtte enda IT eelarve soetada ei lubaks.

+ Töötajad saavad teha natuke tööd isegi vabal ajal või kontorist väljas, näiteks vastata mõnele kliendi mailile või kõnele. See tagab aga ettevõttele suurema operatiivsuse nii klientide kui ka jooksvate probleemide suhtes.

+ Uued töötajad, kes tulevad oma isiklike seadmetega, vajavad vähem aega harjumiseks, kuna on need seadmedon juba varem selgeks õpitud. See vähendab ka IT tugiisikute (helpdeski) töökoormust.

+ Kui töötajatel võimaldatakse kasutada isiklikke seadmeid, siis võib see tähendada seda, et on võimalik palgata parem töötaja. Ehk potentsiaalsete kandidaatide ring on laiem. Näiteks töötajad, kes on harjunud tegema tööd Apple'i arvutitel, ei pruugi olla huvitatud töö juures Windowsi kasutamisest või vastupidi.

BYOD miinused:

- Uuringufirma Gartner läbiviidud uuringust selgus, et kolmandikul töötajaist, kes kasutavad isiklikku nutitelefoni ka tööasjade puhul, on olnud turvaprobleeme, millest nad pole enda tööandajat teavitanud. Lisaks ainult 15% töötajatest olid sõlminud mingisuguse BYOD lepingu.

- Ettevõte IT pool kaotab suure osa kontrollist just töötajate riistvara üle. See tähendab suuremat turvariski.

- Kui tööarvuti või –seadme puhul saab lihtsalt teha töötajale selgeks, mis on lubatud ja mis mitte, siis on palju keerulisem hakata piirama töötaja vabadusi tema isiklikul seadmel. Selle vastu aitavad vaid selge ja konkreetne BYOD strateegia ja vähemalt minimaalsed firma-poolsed turvareeglid.

- Kui ettevõttel on mingid andmete turvalisuse kohustused, näiteks sõltuvalt valdkonnast (PCI DSS, HIPAA või GLBA jne), siis peab neid jälgima ka BYOD puhul.

- Kui töötaja lahkub ettevõttest, siis peavad olema selged poliitikad, kuidas saada kätte vajalikud andmed ta telefonist või sülearvutist. Lisaks võib olla probleemiks see, et kui kliendid on harjunud talle helistama, siis tuleb see ümber korraldada.

- Neljandik BYOD kasutajatest on olnud pahavara või häkkimiste ohvrid. Selle vastu aitab ettevõtte IT-poolne töötajate harimine ning teatud turvareeglite kehtestamine.

- Isiklike seadmete puhul kasutavad neid lisaks töötajale sageli veel muudki inimesed, näiteks pereliikmed, sõbrad jne.

- Töötajate toodud seadmetega võib olla ühilduvuse probleeme, mis tulenevad näiteks rakenduste versioonide erinevustest, platvormide mittesobivusest, valedest konfiguratsioonidest ja puudulikust riistvarast, mis ei toeta vajalikke protokolle.

- Kuna BYOD puhul saab seadmeid vajadusel kaughallata, siis tekitab see probleeme töötajate isikliku info privaatsuse osas.

- Töötajad võivad nõuda isikliku seadme kasutamise eest töö tegemisel lisatasu (suurem kulumine jne), kuid sel juhul kaotab juba BYOD osa oma mõttest (kulude poolelt).

- Juriidiliselt - kes vastutab siis, kui seade läheb kriitiliste andmetega kaduma?

- Küsimuseks on ka see, et kas ettevõtte IT osakond peab hooldama töötajate isiklikke seadmeid või lasub see kohustus töötajatel endil? Probleemiks IT poolele on ka hallata kõiki neid erinevate platvormidega seadmeid.

- BYOD võib olla IT poolele üks suur õudus, kuna puudub kontroll ja standardiseeritus; kõigele lisaks on keeruline kindlaks teha, et töötajate isiklik seade on üldse sobilik töö tegemiseks.

- Isiklikud seadmed võivad tekitada tööajal segavaid faktoried, nagu sõpradega suhtlemine, mängud jne.

- BYOD puhul ei saa ettevõte näiteks mobiilside operaatoritelt nii suuri soodustusi ning sageli peab ettevõte kompenseerima töötajate kallimaid mobiili- ja interneti pakette.

Mõnined soovitused BYOD´i kasutamiseks ettevõttes

Kui sinu ettevõttes kasutavad töötajad juba isiklikke seadmeid oma töö tegemiseks (ja pääsevad ka ligi ettevõtte andmetele), aga sul puudub BYOD poliitika, siis tasub seda kaaluda ja maandada seeläbi teatud valdkondades riske.

Näiteks ettevõtte poolt hostitud emaili ja kalendri platvormi kasutamine pakub võimalust blokeerida seadmelt töömailidele ligipääs seadme kadumisel või vargusjuhtumite puhul. Lisaks - ettevõtte poolne pilv, kus hoitakse faile, aitab töötajatel neile küll igalt poolt vajadusel ligi pääseda, kuid samas pakub ettevõttele võimalust kontrollida nende failide kasutamist. Ovumi läbiviidud uuringu kohaselt kasutab 60% töötajatest niikuinii isiklikke seadmeid ettevõtte infole ligipääsemiseks. See tähendab, et ettevõttel on BYOD isegi siis, kui see pole ametlikult reguleeritud! Uuringu kohaselt võivad 25% neist seadmetest olla isegi ilma antiviiruseta. BYOD puhul sisuliselt reguleeritakse natuke seda, mida töötajad nagunii teevad.

BYOD-st pehmem lahendus on CYOD (***choose your own device***), mille puhul ettevõte ostab töötajatele sellised seadmed, mis neile enim meeldivad (või annab valida). Sel juhul on seadme omanik ettevõte ning omab seeläbi ka rohkem õigusi ja kontrolli (lahkumise puhul saab töötaja selle näiteks, sõltuvalt töölepingust, välja osta).

Tasub luua lihtne ja läbipaistev BYOD poliitika, mis toob selgelt välja selle, mida ettevõte võib töötajate seadmetes asuvast infost monitoorida ja mis on täiesti privaatne.

BYOD puhul tasuks ka rakendada tulemuste põhist töö mõõtmist ja mitte niivõrd keskenduda laua taga istutud tundide kokkuliitmisele. See võimaldab tuua välja ka mobiilselt tehtud töötunnid.

Pane tähele, kuidas su töötajad eelistavad töötada, sest sageli leiavad nad efektiivseid ja uusi lahendusi, kuidas oma tööd paremini organiseerida. Näiteks, kui nad kasutavad omavahel suhtlemiseks mõnda uut rakendust, siis ei maksa tormata seda kohe blokeerima, vaid pigem kaaluda selle ametlikku rakendamist ettevõtte poolt.

Ettevõte peab võtma kasutusele mobiilsete seadmete haldamise lahendused. Nende hulgas näiteks vajadusel seadmetelt info eemaldamine.

5 peamist asja, mida tuleb teha BYOD rakendamisel:

- Kõigil seadmetel peab olema parool
- Ettevõtte infot ei tohi kunagi hoida lokaalselt (seadmes)
- Andmed peavad olema kapseldatud ning varundatud, pidevalt
- Rakendusi võib laadida vaid saitidelt, mis on heaks kiidetud IT osakonna poolt
- Mobiilsed seadmed peavad toetama võimekust kustutada kaughalduse teel kogu info juhtudel, kui seade läheb kaduma või varastatakse

Kokkuvõtteks: BYOD või mitte?

BYOD eeldab mõningast kompromissi nii töötaja kui ka tööandja poolelt. Töötaja peab olema nõus vähemalt minimaalsete ettevõtte poolsete turvanõuetega oma isiklikus seadmes ning tööandja peab seevastu olema valmis loovutama kontrolli IT riistvaralise poole üle ning usaldama töötajat rohkem. Tänu nutitelefonide ja tahvelarvutite pealetungile on BYOD kasvav trend, ning lähemas tulevikus võivad ettevõtted nii või teisiti sellega rohkem kokku puutuda. Kui sul pole veel BYOD strateegiat, siis tasub kaaluda selle rakendamist.

Artikkel on pärit **Iteraction.ee** blogist.

- Lahendused

- Tahvelarvutid
- Sülearvutid
- Androidiblog