BRING YOUR OWN DEVICE?

CapaSystems
...because time matters

BRING YOUR OWN DEVICE
GIVER SØVNLØSE NÆTTER

Mix af personlige og forretningsmæssige applikationer på ét og samme device kan give it-afdelingerne sikkerhedsmæssige grå hår

Vi gør det faktisk alle – bruger det samme device på arbejdet og privat. Det gælder vores smartphone, tablet, bærbar m.v. Ingen tvivl om, at det er smidigt og omkostningsbesparende for både bruger og arbejdsgiver. Men hvad med virksomhedens sikkerhed i dette univers af personlige og business apps, som Bring Your Own Device-kultur (BYOD) bidrager med?

Der krydses konstant mellem business og pleasure, hvilket giver brugeren større tilfredshed og øger produktiviteten, da det i løbet af et splitsekund er muligt at veksle. BYOD giver også mulighed for at reducere omkostningerne og tiden, der anvendes på at konfigurere devices og supportere brugerne. Men en klar udfordring i denne BYOD-kultur er sikkerheden. Især de mere pleasure-orienterede apps er mere lukrative for hackere – og så er virksomhedens data i fare for at blive inficeret med malware og andet skidt.

Undersøgelser viser, at danskerne hele tiden øger bruges af apps på deres smartphone, og kobler vi landene Tyskland, Norge, Sverige og UK til, så er gennemsnittet ligeledes stigende. Oven i det er vi alle hyppige gæster på sociale medier af mere personlig karakter (f.eks. Facebook, Twitter eller Instagram). Af ovenstående lande (inkl. Danmark), er vi som brugere knapt så tilbageholdende som tidligere, når det kommer til at købe via mobilen. Der foretages indkøb på nettet via vores smartphones, og angreb på devicet, sikkerheden og data er derfor i den grad til stede! Og når vi så via IT-devicet benytter virksomhedens VPN-forbindelse, åbnes sikkerhedssluserne til virksomhedens data for alvor op.

Malware kommer ind via disse apps og "æder" af virksomhedens båndbredde med bl.a. nedsat hastighed og produktivitet til følge – og taler vi om føromtalte lande med høje timelønninger, så kan det på sigt koste virksomhedens konkurrenceevne.

Det interessante er derfor at se på, hvordan man stopper BYOD-sikkerhedsbristen uden at gå på kompromis med brugerens produktivitet og fleksibilitet.

Der er gjort mange forsøg rundt om i organisationerne, dog med begrænset succes, da tiltag som bl.a. kryptering, sikkerhedstjek og IT mobilpolitikker sjældent håndhæves, når det kommer til stykket.

En anden måde at forsøge at tage styring og få kontrol med sikkerheden på er ved helt at forbyde download af udvalgte apps. Dette mødes dog med stor utilfredshed hos brugerne – hvorfor skal de nu slette deres favoritspil? Det er også sådan, at brugerne via bagveje nok skal finde ud af, at fastholde deres favoritspil, for uanset alle gode hensigter, så er virksomhedens sikkerhed ikke noget af det første, der tænkes på. Her indtager convenience og pleasure en langt større rolle.

Virksomhederne kan dog også søge at holde styr på og kontrollere brugerens apps via Mobile Device Management software, der giver central styring af softwareudrulning og konfigurationsændringer på alle devices. Løsningerne giver i flere tilfælde mulighed for enkelt og hurtigt at udføre udrulning af både enkel og kompleks software uden at inddrage eller forstyrre slutbrugeren, ligesom IT-afdelingen er i stand til at udrulle såvel enterpriseapplikationer som applikationer fra Apple App Store og Google Play til både iOS og Android devices.

Truslen fra BOYD er topaktuel, og giver forståeligt nok mange CIOs søvnløse nætter, for hvad kan et databrud ikke resultere i? Tænk blot, hvis man som virksomhed er i gang med et revolutionerende gennembrud, og der så sker et hacker-angreb. Flere års research er tabt på gulvet og det med store økonomiske tab til følge.

Dette sikkerhedsproblem er langt fra et nyt fænomen men toprelevant at diskutere med jævne mellemrum, da nye opfindelser og kreative hackere kontant rykker ved trusselsbilledet. Og det er ikke en option at sætte et stort kryds over BYOD.

MaaS360 står bag udviklingen af

"THE TEN COMMANDMENTS OF BYOD"

– 10 råd, der kan være fornuftige at læne sig op ad i forbindelse med Bring Your Own Device:

1. Lav sikkerhedspolitikken før I anskaffer jer teknologien
2. Hav det fulde overblik over antallet af devices og notificer brugerne, inden I gør noget
3. Udrulning skal være simpel, sikker og kunne konfigurere devices på samme tid
4. Udrulning og konfigurationsændringer skal foregå enkelt og hurtigt uden at forstyrre brugere
5. Giv brugerne en velfungerende self-service-platform, så de selv kan agere
6. Pas på de personlige informationer og forklar virksomhedens "privacy policy" for medarbejderne
7. Hold data fra virksomheden og personlig data skarpt adskilt
8. Hav styr på jeres dataforbrug – opsæt gerne tærskelværdier og hjælp brugerne på den måde
9. Hav konstant overblikket over de devices, der benyttes i virksomheden – overholdes sikkerhedspolitikken?
10. Overvej hvordan BYOD vil få indflydelse på virksomhedens ROI

CAPASYSTEMS

CapaSystems er en dansk ejet softwarevirksomhed, der giver IT-afdelinger i ind- og udland mulighed for at sikre deres brugere optimal udnyttelse af IT-devices. Det gør vi ved at udvikle softwareløsninger, der er i stand til at informere, automatisere samt standardisere IT-infrastrukturen og slutbrugerens IT-arbejdsredskab.

CapaSystems er fokuseret på at levere løsninger og services, der giver mærkbar værdi. Det er vigtigt for os, at vores kunder har følelsen af at være i centrum, og derfor tager vi input derfra seriøst og udvikler software, der indeholder den funktionalitet, som skal til for at sikre den mest optimale IT-arbejdsplads.

CapaSystems
...because time matters

Book et møde

Vil du vide mere så ring til os og book en præsentation af vores produkter, der kan spare dig og virksomheden vital tid!

CapaSystems A/S
Roskildevej 342C • DK-2630 Taastrup

Tel. (+45) 70 10 70 55

www.capasystems.dk