Byod u uredskom poslovanju

Juraga, Leopold

Undergraduate thesis / Završni rad

2017

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Pula / Sveučilište Jurja Dobrile u Puli**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:137:817713

Rights / Prava: In copyright / Zaštićeno autorskim pravom.

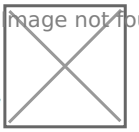
Download date / Datum preuzimanja: **2024-03-29**



Repository / Repozitorij:

Digital Repository Juraj Dobrila University of Pula





Sveučilište Jurja Dobrile u Puli
Odjel za informacijsko-komunikacijske tehnologije

LEOPOLD JURAGA

BYOD U UREDSKOM POSLOVANJU

Završni rad

Pula, 2017.

Sveučilište Jurja Dobrile u Puli
Odjel za informacijsko-komunikacijske tehnologije

LEOPOLD JURAGA

BYOD U UREDSKOM POSLOVANJU

Završni rad

JMBAG: 0242002095, izvanredni student

Studijski smjer: Informatika

Predmet: Informatizacija uredskog poslovanja

Znanstveno područje: Društvene znanosti
Znanstveno polje: Informacijske i komunikacijske znanosti
Znanstvena grana: Informacijski sustavi i informatologija
Mentor: Doc. dr. sc. Darko Etinger

Pula, 2017.

IZJAVA O AKADEMSKOJ ČESTITOSTI

Ja, dolje potpisani Leopold Juraga, kandidat za prvostupnika informatike ovime izjavljujem da je ovaj Završni rad rezultat isključivo mojega vlastitog rada, da se temelji na mojim istraživanjima te da se oslanja na objavljenu literaturu kao što to pokazuju korištene bilješke i bibliografija. Izjavljujem da niti jedan dio Završnog rada nije napisan na nedozvoljen način, odnosno da je prepisan iz kojega necitiranog rada, te da ikoji dio rada krši bilo čija autorska prava. Izjavljujem, također, da nijedan dio rada nije iskorišten za koji drugi rad pri bilo kojoj drugoj visokoškolskoj, znanstvenoj ili radnoj ustanovi.

Student

_____

U Puli, 16. rujna, 2017 godine

IZJAVA
o korištenju autorskog djela

Ja, Leopold Juraga dajem odobrenje Sveučilištu Jurja Dobrile u Puli, kao nositelju prava iskorištavanja, da moj završni rad pod nazivom „BYOD u uredskom poslovanju“ koristi na način da gore navedeno autorsko djelo, kao cjeloviti tekst trajno objavi u javnoj internetskoj bazi Sveučilišne knjižnice Sveučilišta Jurja Dobrile u Puli te kopira u javnu internetsku bazu završnih radova Nacionalne i sveučilišne knjižnice (stavljanje na raspolaganje javnosti), sve u skladu s Zakonom o autorskom pravu i drugim srodnim pravima i dobrom akademskom praksom, a radi promicanja otvorenoga, slobodnoga pristupa znanstvenim informacijama.
Za korištenje autorskog djela na gore navedeni način ne potražujem naknadu.

U Puli, 16.09.2017.

Potpis

_____

SADRŽAJ

1. UVOD 1
2. UREĐAJI 2
2.1. Odabir uređaja 2
2.1.1. Odabir pametnog telefona ili tableta 3
2.1.2. Odabir prijenosnog računala 3
2.2. Odabir operativnog sustava 3
2.2.1. Operativni sustav za pametni telefon ili tablet 3
2.2.2. Operativni sustav za prijenosno računalo 5
2.3. Razmatranje o ostalim stavkama 7
2.3.1. Veličina zaslona i rezolucija 8
2.3.2. Težina 8
2.3.3. Vrijeme trajanja baterije 9
2.3.4. Prostor za pohranu podataka 9
2.3.5. Izdržljivost 9
2.3.6. Priključci i mrežna komunikacija 9
2.3.7. Sigurnost 10
3. SIGURNOST 11
3.1. Uređaji na poslu u odnosu na uređaje za posao 11
3.2. Izazovi BYOD sigurnosti 12
3.3. Potreba za BYOD sigurnošću 14
3.4. Doprinos dionika i zaposlenika 18
3.5. Definiranje BYOD sigurnosne politike 19
3.6. Procjena tehnoloških mogućnosti poduzeća 22
3.7. Razmatranje BYOD sigurnosnih rješenja 23
3.7.1. Šifriranje podataka 24
3.7.2. Kontrola instalacije aplikacija 25
3.7.3. Kontejnizacija 26
3.7.4. Lista nepoželjnih aplikacija 26
3.7.5. Lista poželjnih aplikacija 27
3.7.6. Ostale BYOD sigurnosne mjere 28
4. PREDNOSTI I NEDOSTACI BYOD-A 29
4.1. Prednosti BYOD-a 29
4.2. Nedostaci BYOD-a 30
5. SUSTAV UPRAVLJANJA MOBILNIM UREĐAJEM 31
6. ZAKLJUČAK 33
LITERATURA 34
POPIS SLIKA 36
SAŽETAK 37
ABSTRACT 38

1. UVOD

Zbog vremena u kojem živimo velika većina zaposlenika u svim djelatnostima posjeduje pametne telefone, tablete, prijenosna računala i/ili druge uređaje.

Cilj ovog rada je analizirati BYOD[1] politiku u uredskom poslovanju. BYOD se također još naziva i BYOT[2], BYOP[3] i BYOPC[4]. BYOD politika dozvoljava zaposlenicima donošenje vlastitih mobilnih uređaja na radno mjesto te korištenje istih za pristup službenim aplikacijama i informacijama te radne okoline. Ovakvom politikom poslodavac ne mora nabavljati zaposlenicima uređaje koje će oni koristiti u te svrhe, a ujedno time izbjegava i dodatne troškove. BYOD politika također ima i drugih prednosti, ali isto tako i nedostataka koji mogu poslodavcu uzrokovati probleme ukoliko on i zaposlenici ne primjene BYOD politiku na ispravan način. U nastavku će ovo biti detaljno razrađeno.

[1] Bring Your Own Device – Donesi Svoj Vlastiti Uređaj
[2] Bring Your Own Technology – Donesi Svoju Vlastitu Tehnologiju
[3] Bring Your Own Phone – Donesi Svoj Vlastiti Telefon
[4] Bring Your Own PC – Donesi Svoje Vlastito Osobno Računalo

2. UREĐAJI

Tržište nudi veliki broj različitih vrsta pametnih telefona, tableta, prijenosnih računala te drugih uređaja. BYOD rješenje zahtijeva udovoljenje određenih kriterija prilikom odabira uređaja. Ti uređaji moraju udovoljavati određenim kriterijima kao što su tehničke specifikacije, verzije operativnog sustava i ostalo.

2.1. Odabir uređaja

Prilikom odabira vrste uređaja potrebnih zaposlenicima za izvršavanje njihovih poslova treba uzeti u obzir uređaje koje zaposlenici posjeduju te koji su im potrebni za izvršavanje istih. Ako zaposlenici posjeduju dovoljan broj potrebnih uređaja onda se takva BYOD politika može početi projektirati, ali u suprotnom poslodavac mora odlučiti o potrebnom broju i načinu nabave istih (može ih on nabaviti, a biti će u hipotekarnom vlasništvu zaposlenika ili će ih nabaviti zaposlenik sa ili bez financijskog poticaja).

Pametni telefoni ili tableti sa pripadajućim BYOD rješenjem dovoljni su u onim poduzećima čiji zaposlenici dobivaju samo neke informacije ili upite. Nakon primitka iste prosljeđuju lokalnom aplikacijom instaliranom na uređaju ili web aplikacijom internetskog preglednika uređaja. U ovom slučaju nije im potrebno prijenosno računalo kao ni BYOD rješenje za računala. S druge strane BYOD rješenje za pametne telefone ili tablete nije zadovoljavajuće ako zaposlenici na svom radnom mjestu: pišu tekstove, programiraju, obrađuju multimediju ili obavljaju druge poslove za koje im je neophodno prijenosno računalo s BYOD rješenjem za isti. Ukoliko poslodavac ima potrebu za oba BYOD rješenja ista se primjenjuju kroz novo rješenje koje omogućava obavljanje svih poslova u poduzeću upotrebom pametnih telefona i/ili tableta i/ili prijenosnih računala.

2.1.1. Odabir pametnog telefona ili tableta

Pametni je telefon svojom veličinom i težinom idealan za terenski rad jer se za obavljanje takvog posla uređaj stalno nosi sa sobom. Tablet je nasuprot pametnom telefonu idealan za neku uslužnu djelatnost gdje veličina nije bitna jer se uređaj ne mora stalno nositi sa sobom.

2.1.2. Odabir prijenosnog računala

Kod odabira prijenosnog računala treba se odlučiti između klasičnog ili 2 u 1 laptop računala. 2 u 1 laptop je uređaj koji uz standardnu fizičku tipkovnicu ima i zaslon na dodir sa tipkovnicom što mu omogućava funkcioniranje kao tablet. Kod nekih modela on se vrlo jednostavno može pretvoriti u tablet odvajanjem fizičke tipkovnice od zaslona. Kod drugih modela pretvaranje u tablet ostvaruje se okretanjem iste za 360 stupnjeva. Odabir prijenosnog računala ovisit će o tome dali zaposlenikov posao zahtijeva nabavku klasičnog ili 2 u 1 laptop računala.

2.2. Odabir operativnog sustava

Izborom pravog operativnog sustava koji će zaposlenici koristiti trebaju se uzeti u obzir i aplikacije potrebne zaposlenicima za obavljanje njihovih zadaća.

2.2.1. Operativni sustav za pametni telefon ili tablet

Na tržištu pametnih telefona i tableta najrasprostranjeniji operativni sustavi su Google-ov Android i Apple-ov iOS. Postoje i alternativni operativni sustavi koje će poslodavci najvjerojatnije zaobići u implementaciji BYOD rješenja u poslovanju poduzeća. Poslodavac će se sukladno tome vjerojatno odlučiti za jedan, drugi ili oba. Izbor oba ujedno može neznatno uvećati troškove poslovanja. Kako bi se BYOD rješenje ispravno primijenilo neovisno o upotrijebljenim operativnim sustavima izvršitelju softverskog rješenja može biti uzrokovana potreba za dodatnim vremenom i sredstvima. Uvođenje BYOD rješenja za različite operativne sustave mora imati

pokriće u istom ili sličnom prikazu i primjeni.

Apple svoj iOS operativni sustav instalira na svoje pametne telefone (iPhone) i tablete (iPad). Operativni sustav iOS je zatvorenog tipa pa ga drugi proizvođači pametnih telefona i tableta ne mogu koristiti na svojim uređajima. Druga poduzeća koja bi željela koristiti njihove uređaje tijekom primjene BYOD rješenja uz izmijene nekih dijelove operativnog sustava to ne mogu uraditi zbog njegove zatvorenosti.

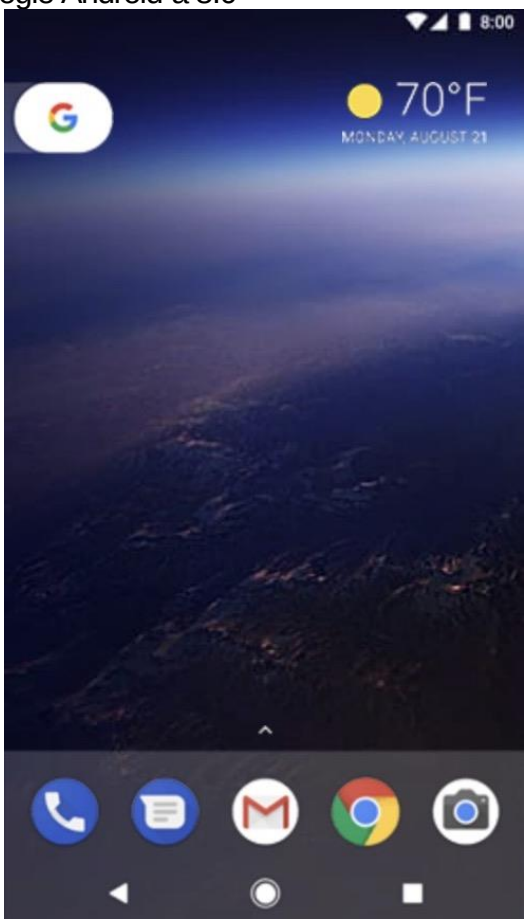
Slika 1. Početni zaslon Apple iOS 11 beta 6



Izvor: https://en.wikipedia.org/wiki/IOS

Android je s druge strane Google-ov operativni sustav otvorenog tipa (engl. open source) koji proizvođači pametnih telefona i tableta instaliraju na svoje uređaje. Isto tako moguće ga je mijenjati i prilagođavati prema svojim potrebama.

Slika 2. Početni zaslon Google Android-a 8.0



Izvor: https://en.wikipedia.org/wiki/Android_(operating_system)

Oba operativna sustava jednostavno je koristiti te imaju jako slično korisničko sučelje koje omogućava jednostavni prelazak u korištenju između jednog i drugog. U skladu sa zahtjevima uvođenja BYOD rješenja preferirani operativni sustav-sustavi biti će odabrani.

2.2.2. Operativni sustav za prijenosno računalo

Na tržištu prijenosnih računala postoje uređaji koji koriste Microsoft-ov Windows ili Apple-ov macOS operativni sustav. Postoje i alternativni operativni sustavi koje će poslodavci najvjerojatnije zaobići u implementaciji BYOD rješenja u poslovanju poduzeća. Poslodavac će se sukladno tome vjerojatno odlučiti za jedan, drugi ili oba. Izbor oba ujedno može neznatno uvećati troškove poslovanja. Kako bi se BYOD rješenje ispravno primijenilo neovisno o upotrjebljenim operativnim sustavima

izvršitelju softverskog rješenja može biti uzrokovana potreba za dodatnim vremenom i sredstvima. Uvođenje BYOD rješenja za različite operativne sustave mora imati pokriće u istom ili sličnom prikazu i primjeni.

Apple svoj macOS operativni sustav instalira na svoja prijenosna računala. Operativni sustav macOS je zatvorenog tipa pa ga drugi proizvođači prijenosnih računala ne mogu koristiti na svojim uređajima. Druga poduzeća koja bi željela koristiti njihove uređaje tijekom primjene BYOD rješenja uz izmijene nekih dijelove operativnog sustava to ne mogu uraditi zbog njegove zatvorenosti.

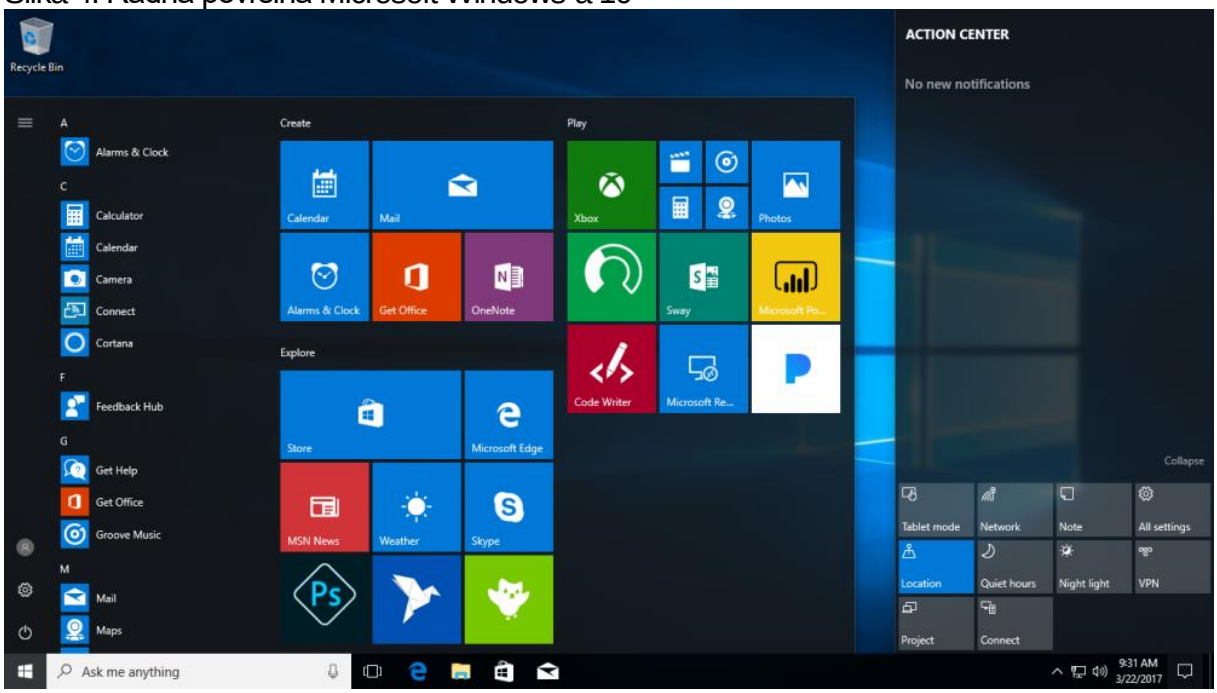
Slika 3. Radna površina Apple macOS-a High Sierra beta 1



Izvor: https://en.wikipedia.org/wiki/MacOS

Windows je Microsoft-ov operativni sustav zatvorenog tipa kojeg Microsoft i ostali proizvođači prijenosnih računala instaliraju na svoje uređaje. Isti je od početka bio namijenjen korištenju na bilo kojem računalu. Druga poduzeća koja bi željela koristiti njihove uređaje tijekom primjene BYOD rješenja uz izmijene nekih dijelove operativnog sustava to ne mogu uraditi zbog njegove zatvorenosti.

Slika 4. Radna površina Microsoft Windows-a 10



Izvor: https://en.wikipedia.org/wiki/Microsoft_Windows

Oba operativna sustava imaju slično korisničko sučelje koje omogućava brzi prelazak u korištenju između jednog i drugog. U skladu sa zahtjevima uvođenja BYOD rješenja preferirani operativni sustav-sustavi biti će odabrani.

2.3. Razmatranje o ostalim stavkama

Postoje također i druge stavke koje pridonose odabiru uređaja a to su: veličina i rezolucija zaslona, težina uređaja, vrijeme trajanja baterije, veličina prostora za pohranu podataka, fizička izdržljivost kod naprezanja (pad, udarac itd.), priključci i mrežne mogućnosti. Navedene stavke nisu presudne u prvim koracima uvođenja rješenja, tijekom stvaranja i izgleda koncepta BYOD-a. Ove stavke su bitne tijekom projektiranja, specificiranja i nabave uređaja sa karakteristikama koje su im potrebne kako bi BYOD rješenje funkcioniralo ispravno i djelotvorno. Uređaj nije prikladan ako ne zadovoljava neki od zadatih kriterija u primjeni BYOD rješenja.

2.3.1. Veličina zaslona i rezolucija

Veličina zaslona treba ovisiti o sadržaju koji će se prikazivati na uređaju dok rezolucija zaslona treba biti minimalno 720p (1280x720) kako bi se dobio minimalno zadovoljavajući DPI[5]. DPI je mjera gustoće piksela (točaka) na liniji dužine od 1 inč-a (2.54 cm), a izračuna se na slijedeći način:

$$dijagonalna\ rezolucija\ u\ pikselima = \sqrt{(širina\ rezolucije\ u\ pikselima)^2 + (visina\ rezolucije\ u\ pikselima)^2}$$

$$DPI = \frac{dijagonalna\ rezolucija\ u\ pikselima}{dijagonala\ zaslona\ u\ inč - ima}$$

Minimalni DPI zaslona pametnog telefona trebao bi biti oko 294 jer je to DPI za 5 inč-ni zaslon sa rezolucijom 720p a to se dobije slijedećim izračunom:

$$dijagonalna\ rezolucija\ u\ pikselima = \sqrt{1280^2 + 720^2} = 1468.6$$

$$DPI = \frac{1468.6}{5} = 293.72$$

Minimalni DPI zaslona tableta trebao bi biti oko 147 jer je to DPI za 10 inč-ni zaslon sa rezolucijom 720p a to se dobije slijedećim izračunom:

$$dijagonalna\ rezolucija\ u\ pikselima = \sqrt{1280^2 + 720^2} = 1468.6$$

$$DPI = \frac{1468.6}{10} = 146.86$$

2.3.2. Težina

Pošto će velika većina zaposlenika svoje uređaje nositi na posao težina bi morala biti što manja ali ne bi smjela biti presudan faktor pogotovo u odnosu na vrijeme trajanja baterije i veličinu prostora za pohranu podataka.

[5] Dots per inch – broj točaka po inč-u

2.3.3. Vrijeme trajanja baterije

Pošto zaposlenici moraju koristiti uređaj tijekom cijelog radnog vremena trajanje baterije bi trebalo biti 7+ sati kako bi zadovoljilo ovaj kriterij.

2.3.4. Prostor za pohranu podataka

Veličina prostora za pohranu podataka ovisi o tome koliko se lokalno pohrani podataka. Ako se koristi neka oblak (engl. Cloud) usluga kao Google Drive ili pak vlastito rješenje onda veličina prostora za lokalnu pohranu nije toliko ključna. Isti bi trebao biti toliki da nakon instaliranja svih potrebnih aplikacija ostane dovoljno slobodnog prostora za daljnje pohranjivanje podataka i instaliranja potrebnih aplikacija. Ukoliko se većina ili svi podaci pohranjuju lokalno na uređaj onda treba vidjeti koliko će prostora za pohranu biti potrebno za takve potrebe. Prilikom odabira veličine prostora za pohranu podataka treba voditi računa o zaposlenikovim potrebama u poslovnoj i osobnoj upotrebi uređaja.

2.3.5. Izdržljivost

Ovisno o uvjetima rada potreban je uređaj sa adekvatnom mehaničkom izdržljivošću. Ako se uređaj npr. upotrebljava na nekom gradilištu gdje može pasti sa veće visine ili pak biti oštećen na druge načine onda je potrebno nabaviti uređaj koji to može izdržati.

2.3.6. Priključci i mrežna komunikacija

Tipovi priključka koje uređaj posjeduje su bitni zbog dodatne periferije koja se spaja na uređaj kao npr. miš, tipkovnica, itd.

Tipovi mrežne komunikacije kao npr. Wi-Fi, Bluetooth, LAN, itd. su bitni radi povezivanja na Intranet poslodavca i Internet.

2.3.7. Sigurnost

Kako se ne bi nehotično ugrozila sigurnost podataka poduzeća zaposlenike je potrebno educirati o upotrebi uređaja implementiranih u BYOD rješenju. Tema sigurnosti je detaljnije razrađena u nastavku.

3. SIGURNOST

Sigurnost je tema za koju Nate Lord 2016. u članku za Digital Guardian navodi: „BYOD ostaje velika prilika i izazov za poduzeća. Prateći pravi pristup identificiranja BYOD rizika i razvijanjem učinkovite BYOD politike moguće je iskoristiti prednosti BYOD-a bez dodavanja značajnog rizika.

Ako vaša tvrtka omogućuje zaposlenicima da donose vlastite računalne uređaje na radno mjesto bez obzira radi li se o pametnim telefonima, tabletima ili prijenosnim računalima potrebna vam je BYOD sigurnosna politika. U početku su zaposlenici na radnom mjestu koristili samo uređaje koji su vlasništvo tvrtke. Danas su se pametni telefoni i tableti brzo proširili na potrošačkom tržištu do te mjere da gotovo svaki zaposlenik dolazi na posao s vlastitim uređajem povezanim na internet. To znači veću mogućnost da zaposlenik prouzroči sigurnosne rizike u vašem poduzeću.“

Iz ovoga se zaključuje da je tehnološki razvoj omogućio zaposlenicima da na posao dolaze sa računalom u džepu te njime budu spojeni sa cijelim svijetom. Te dvije stvari zbog toga mogu stvoriti sigurnosne rizike poduzeću ali se pravilnom BYOD politikom mogu izbjeći.

3.1. Uređaji na poslu u odnosu na uređaje za posao

Uređaji na poslu u odnosu na uređaje za posao tema je za koju Nate Lord 2016. u članku za Digital Guardian navodi: „Jedna je stvar ako zaposlenik donese vlastiti uređaj na posao te ga izričito koristi za osobnu komunikaciju. Ova praksa još uvijek može stvoriti rizike, ali najznačajniji sigurnosni rizici povezani su s zaposlenicima koji upotrebljavaju osobne uređaje za obavljanje posla, bilo da šalju e-poštu vezanu za posao ili pristupaju tvrtkinim sigurnim aplikacijama s vlastitih pametnih telefona ili tableta.

Razlika je u osnovi da u prvom slučaju zaposlenici koriste svoje osobne uređaje na poslu, a u drugom zaposlenici koriste svoje osobne uređaje za obavljanje posla.

Uređaji koji se donose na radno mjesto, a nemaju pristup mreži tvrtke obično nisu problematični, međutim preventiva je nužna u svim slučajevima sa strogim i jasno definiranim BYOD politikama i primjenama.“

Ova dva načina primjene uređaja se možda na prvi pogled čine sličnima ali nisu. Kako je Nate Lorde gore naveo uređaji zaposlenika na poslu ne predstavljaju toliki sigurnosni problem kao oni njihovi uređaji koje koriste u radne svrhe. Sigurnost je dakako potrebna i za uređaje zaposlenika koje oni koriste na poslu, ali ti uređaji neće biti glavni uzročnik sigurnosnih problema BYOD rješenja već njihovi uređaji korišteni u radne svrhe.

3.2. Izazovi BYOD sigurnosti

Izazovi BYOD sigurnosti je tema za koju Nate Lord 2016. u članku za Digital Guardian navodi: „Sigurnost BYOD-a često je izazov za velika poduzeća te male i srednje tvrtke. To proizlazi iz činjenice kako bi tvrtke bile efikasnije moraju uspostaviti neki oblik kontrole nad pametnim telefonima, tabletima i prijenosnim računalima koji nisu u vlasništvu tvrtke već su osobna imovina zaposlenika. Kako je BYOD postao sve prisutniji, a svijest o sigurnosnim rizicima narasla BYOD sigurnosne politike postaju sve šire primijenjene i prihvaćene od strane tvrtki i njihovih zaposlenika.

Donošenje svog vlastitog uređaja prevladava kod svih zaposlenika. Zapravo, istraživanje tvrtke Tech Pro Research iz Studenog 2014. pokazalo je da je 74% organizacija ili već dopustilo zaposlenicima da donose vlastite uređaje na posao ili su to planirali napraviti, a prema novijim podacima tvrtke Trend Micro taj je broj sada preko 82%. Tvrtke koje usvajaju BYOD imaju korist od smanjenih hardverskih i softverskih troškova, ali istodobno BYOD postavlja dodatne obaveze IT odjelima koji moraju održavati uređaje kao i osigurati da BYOD ne omogući nepotrebne ranjivosti mreže i podataka tvrtke. Zanimljivo je da je u istraživanju Tech Pro Research-a između 26% ispitanika koji nisu usvojili ili ne planiraju usvojiti BYOD najčešće navedeni razlozi za neprimjenu BYOD-a zabrinutosti za sigurnost.“

Slika 5. Stvaranje BYOD-a sigurnim



Izvor: https://digitalguardian.com/blog/ultimate-guide-byod-security-overcoming-challenges-creating-effective-policies-and-mitigating

Izazovi BYOD sigurnosti je tema za koju Centar za poslovnu sigurnost 2017. na svojoj stranici navodi: „Moderna tehnologija učinila je naš život lakšim i zanimljivijim, ali nam je i stvorila i nove probleme. Špijunaža, sabotaža, krađa podataka – ovi pojmovi su bili razlog mnogih besanih noći šefova tvrtki i prije pojave interneta. Digitalna era im je donijela još veće glavobolje. Jer dok su nekada fascikle morale biti fizički prokrijumčarene iz ureda, danas je za to dovoljan jedan klik mišem ili dodir prstom."

Može se zaključiti da je zaposlenikovo donošenje osobnih uređaja na posao stvorilo nove sigurnosne izazove poduzećima. Ona sada moraju biti sposobna uspostaviti nova sigurnosna rješenja koja im prije nisu bila potrebna.

3.3. Potreba za BYOD sigurnošću

Potreba za BYOD sigurnošću tema je za koju Nate Lord 2016. u članku za Digital Guardian navodi: „U 2013. globalno istraživanje CIO-a[6] od strane Gartner's Executive Programs pronalazi da je 38% tvrtki predviđalo da će prestati nabavljati uređaje zaposlenicima do 2016. godine. Gartner je dalje predvidio da će do 2017. polovica poslodavaca zahtijevati od zaposlenika da nabave vlastiti uređaj za radne potrebe.

Zanemarujući ove trendove i predviđanja, BYOD ima svoj vlastiti zamah: Ovum-ova anketa na 4.371 zaposleniku širom svijeta u 2013. otkrila je da gotovo 70% zaposlenika koji posjeduju pametni telefon ili tablet iste koriste za pristup podacima tvrtke. Naime 67,8% anketiranih ispitanika koji posjeduju pametni telefon ili tablet nose svoje uređaje na posao. Među njima 15,4% ispitanika donosi svoje uređaje na posao bez znanja informatičkog odjela, a 20,9% to čini unatoč politikama tvrtke koje zabranjuju BYOD.

Ovi rezultati prikazuju vjerojatnost da će zaposlenici koristiti osobne mobilne uređaje za obavljanje poslovnih aktivnosti bez obzira da li tvrtka ima prethodno saznanje o tome i/ili politike koje se tiču korištenja osobnih uređaja. Drugim riječima, tvrtke koje odluče zanemariti vjerojatnost korištenja osobnih uređaja ignoriraju ono što bi moglo biti ozbiljan sigurnosni rizik.“

[6] Chief information officer – Šef informatičkog odijela

Slika 6. BYOD Rizici

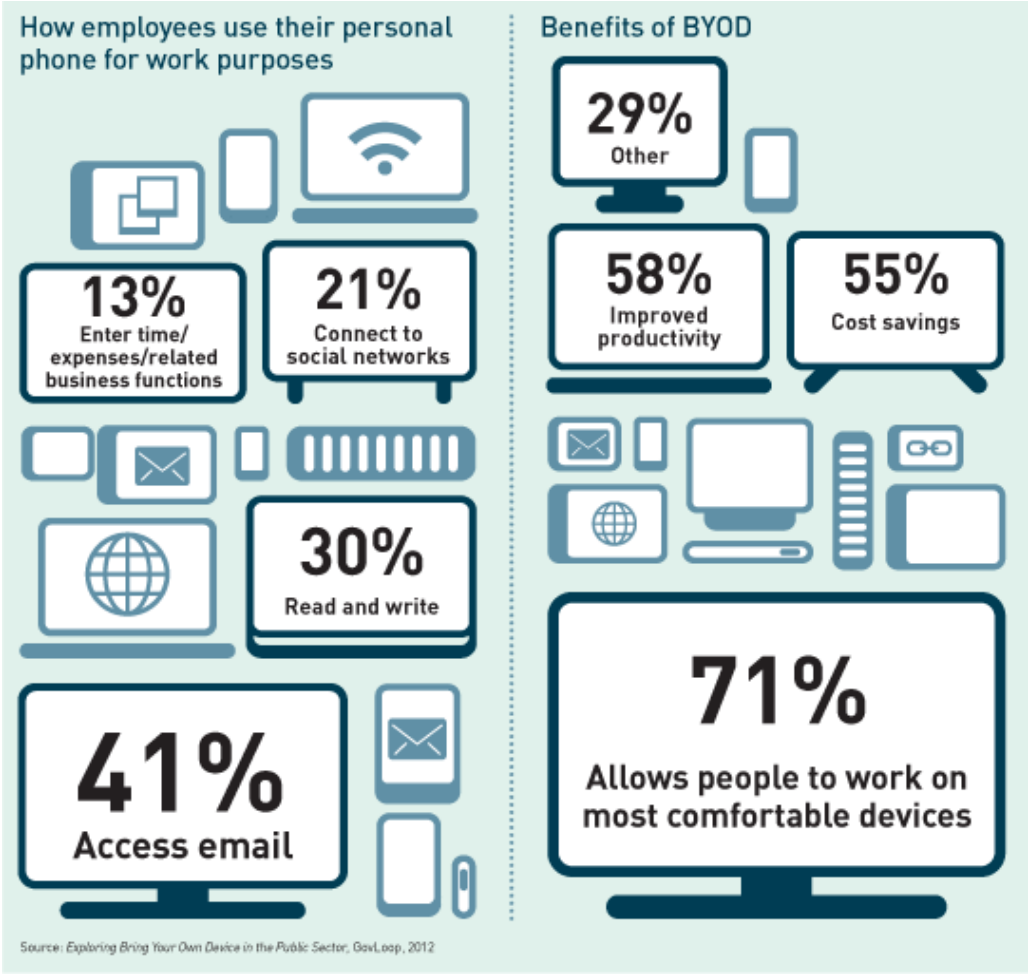


Izvor: https://digitalguardian.com/blog/ultimate-guide-byod-security-overcoming-challenges-creating-effective-policies-and-mitigating

Također Nate Lord 2016. u članku za Digital Guardian još navodi: „Poslodavci imaju dvije mogućnosti: prigrliti BYOD donošenjem BYOD politika i sigurnosnih mjera kako bi praksa bila sigurnija ili potpuno zabraniti BYOD i pronaći način za provođenje toga. Za većinu tvrtki ima smisla prihvatiti trend BYOD-a i kapitalizirati[7] prednosti koje nudi, kao što je povećana produktivnost zaposlenika i veće zadovoljstvo zaposlenika kroz bolju ravnotežu između radnog i privatnog života, uz istovremenu implementaciju sigurnosnih mjera koje ublažavaju uključene rizike.“

[7] Kapitalizirati – pretvoriti/pretvarati što u kapital «prema» https://jezikoslovac.com/word/kk3p, Jezikoslovac, 03.08.2017 u 9:52

Slika 7. BYOD korisnički trendovi



Izvor: https://digitalguardian.com/blog/ultimate-guide-byod-security-overcoming-challenges-creating-effective-policies-and-mitigating

Potreba za BYOD sigurnošću tema je za koju Centar za poslovnu sigurnost 2017. na svojoj stranici navodi: „Danas je poslovnom čovjeku nezamislivo funkcionirati bez računala, tableta te posebno smartphona. Bez svega navedenog jednostavno ne može pratiti dinamiku današnjeg poslovanja. Iako smo svjesni svih rizika nismo spremni odreći se mogućnosti koja nam omogućuje tehnologija. U tom slučaju moramo biti svjesni pratećih rizika i odgovorni u sprječavanju posljedica.

Zbog sve šire primjene mobilnih uređaja njihovo korištenje predstavlja sve veći sigurnosni rizik za poslovne subjekte. Prema jednom istraživanju više od 50% zaposlenika često ili vrlo često pohranjuju osjetljive podatke tvrtke na svojim nesigurnim prijenosnim računalima, tabletima, smartphonima ili drugim mobilnim uređajima. Kada netko od tih zaposlenika izgubi svoj mobitel u taksiju, kafiću i sličnim

mjestima povjerljivi podaci mogu završiti u zlonamjernim rukama.

Drugi razlog zbog čega su mobilni uređaji prijetnja sigurnosti poslovanja je potencijalna opasnost da se malware nesvjesno instalira na uređaj, te ako "zaraženi" mobilni uređaj ima pristup zaštićenoj mreži tvrtke, može omogućiti prodor u mrežu kao i neovlašteno otjecanje podataka bez obzira na stupanj sigurnosti. Malware se može pokupiti iz raznih aplikacija, e-mailova te ostati neotkriven od strane korisnika.

Istraživanje provedeno od strane B2B International za tvrtku Kaspersky Lab pokazalo je da 38 posto tvrtki primjenjuje neke vrste ograničenja korištenja mobilnih uređaja, kao što su zabrane pristupa određenim mrežnim resursima. Oko 19 posto ima potpunu zabranu korištenja mobilnih uređaja za radne aktivnosti, ali samo 11 posto tvrtki koriste Mobile Device Management (MDM) softvere kako bi se osigurala usklađenost s politikom korporativne sigurnosti.

Unatoč mnogim tvrtkama koje ne postavljaju nikakva ograničenja uporabe osobnih uređaja (smartphona, tableta i prijenosnih računala), istraživanje je pokazalo da 34 posto ispitanika smatra da mobilni uređaji predstavljaju značajnu prijetnju poslovanju.

Vezano za predmetno istraživanje viši sigurnosni istraživač tvrtke Kaspersky Lab, David Emm rekao je da dopuštenje zaposlenicima da koriste svoje mobilne uređaje na radnom mjestu može dovesti do poboljšanja produktivnosti i kreativnosti, ali također može donijeti povećani sigurnosni rizik. Organizacije trebaju pažljivo odvagnuti prednosti takve prakse u odnosu na moguće rizike.“

Kako poduzeća prije nisu imala potrebu za sigurnošću osobnih uređaja zaposlenika nisu se bavila tim mogućim sigurnosnim problemom. Pošto sve više zaposlenika na svoja radna mjesta dolazi sa svojim osobnim uređajima potreba za sigurnošću od prijetnji koje bi ti uređaji mogli stvoriti postala je vrlo bitna.

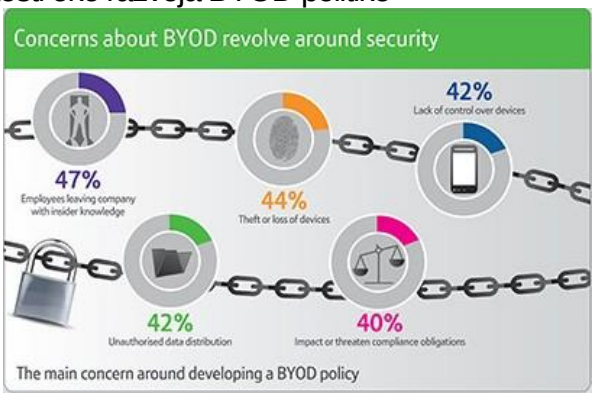
3.4. Doprinos dionika i zaposlenika

Doprinos dionika i zaposlenika je tema za koju Nate Lord 2016. u članku za Digital Guardian navodi: „Da bi se prilagodile rastućoj upotrebi BYOD-a mnoge tvrtke među velikim, malim i srednjim poduzećima mogu biti sklone trenutnom začetku kreiranja politike, ali taj pristup često nailazi na zapreke. Prvi korak prije rada na politici je pridobivanje podrške dionika[8] i zaposlenika.

Dionici će biti neophodni za proces planiranja politike pružajući raznolike perspektive iz različitih odjela i interesa unutar organizacije. Rukovoditelji, ljudski resursi, financije, IT službe i sigurnosni tim trebaju biti zastupljeni u timu upravljanja BYOD projektom i svaki od njih može doprinijeti razvoju te politike.

Pored ovih dionika zaposlenikovo učešće je neophodno za stvaranje učinkovitih BYOD pravila. Slijepo stvaranje pravila utemeljenih isključivo na interesima tvrtke može dati negativne povratne efekte. Pravila koja su previše ograničena ili ne pružaju podršku za odgovarajuće uređaje dovest će do umanjenog sudjelovanja zaposlenika, a na kraju će dovesti do rasipanja resursa koje je tvrtka uložila u izradu pravila.“

Slika 8. Glavne zabrinutosti oko razvoja BYOD politike



Izvor: https://digitalguardian.com/blog/ultimate-guide-byod-security-overcoming-challenges-creating-effective-policies-and-mitigating

Također Nate Lord 2016. u članku za Digital Guardian još navodi: „Anketa zaposlenika učinkovit je način dobivanja podataka o: uređajima koje zaposlenici

[8] Dionik – onaj koji ima udjela u čemu; sudionik «prema» https://jezikoslovac.com/word/wpjv, Jezikoslovac, 03.08.2017 u 9:52

trenutačno upotrebljavaju (i koje će vjerojatno kupiti u budućnosti, budući da tvrtkina BYOD politika mora podržavati i te uređaje), ono što zaposlenici vide spram prednosti i nedostataka zbog upotrebe vlastitih uređaja u radne svrhe i koje aplikacije smatraju potrebnim kako bi mogli obavljati poslovne zadatke na svojim osobnim uređajima. Na primjer neki su zaposlenici možda zabrinuti za vlastitu privatnost ako koriste svoje osobne uređaje za posao. Opskrbljeni tim podacima možete početi izrađivati BYOD politiku koja se bavi tim zabrinutostima i obuhvaća cijeli niz uređaja koje će vaši zaposlenici vjerojatno upotrebljavati.“

Da bi se prava BYOD politika uvela i stvorila za neko poduzeće ono se mora konzultirati sa dionicima i zaposlenicima. U protivnom se neće stvoriti ispravna BYOD politika koja uvažava potrebe dionika i zaposlenika. Takva politika koja ne uvažava potrebe dionika i zaposlenika može samo naškoditi poduzeću jer može dovesti do njene odbojnosti kod dionika i zaposlenika.

3.5. Definiranje BYOD sigurnosne politike

Definiranje BYOD sigurnosne politike je tema za koju Nate Lord 2016. u članku za Digital Guardian navodi: „Definiranje BYOD sigurnosne politike ključni je korak u održavanju sigurnosti poduzeća kada zaposlenici donose svoje uređaje na radno mjesto. Unatoč širokoj upotrebi osobnih uređaja na radnom mjestu iznenađujuće je da zapravo samo 39% poduzeća ima uvedenu BYOD politiku, prema istraživanju Software Advice kod 385 odraslih Amerikanaca koji koriste svoje uređaje za pristupanje mreži svog poduzeća.

Istraživanje koje je proveo Software Advice u kolovozu 2014. također je pokazalo da 41% poduzeća nema BYOD politiku, a dok drugih 20% ispitanika nije bilo sigurno dali njihova poduzeća imaju ili nemaju BYOD politike. Više od polovice ispitanika izvijestilo je da su datoteke poduzeća prebacili na svoje uređaje, a 49% je izjavilo da ne instaliraju sigurnosna ažuriranja odmah po izdavanju.

Ovi podaci otkrivaju jasnu potrebu da poduzeća preuzmu vodeću ulogu u uspostavljanju čvrstih BYOD politika kao i edukaciju zaposlenika u praksama

prihvatljivim za korištenje osobnih uređaja u poslovanju poduzeća ili za pristupanje aplikacijama ili podacima poduzeća.

TechTarget SearchMobile Computing navodi nekoliko bitnih elemenata BYOD politike uključujući:

- Prihvatljivu upotrebu (kojim aplikacijama i imovini je zaposlenicima dopušteno pristupanje sa njihovih osobnih uređaja?)
- Minimalne potrebne sigurnosne kontrole za uređaje
- Komponente koje pruža poduzeće (kao što su SSL certifikati za provjeru autentičnosti uređaja)
- Prava tvrtke na izmjene u uređaju (poput daljinskog brisanja za izgubljene ili ukradene uređaje)

Jonathan Hassell u članku za CIO opisuje nekoliko dodatnih komponenti učinkovitih BYOD politika, kao što su određivanje dopuštenih vrsta uređaja i uspostavljanje stroge sigurnosne politike za sve uređaje. Na primjer potrošači mogu odustati od upotrebe ugrađenih sigurnosnih značajki kao što su mogućnost zaključavanja zaslona uređaja ili zahtijevanje zaporki jer ove značajke stvaraju dodatne nepovoljne korake korisniku. Zaposlenici su motivirani da koriste ove jednostavne značajke kada postoje jasna pravila poduzeća, a čak i jednostavne mjere mogu poboljšati sigurnost poduzeća.

Osim toga, vaša BYOD politika trebala bi jasno navesti uslužna pravila za BYOD uređaje, uključujući nivo dostupne podrške IT-a za zaposlenike koji se povezuju s mrežom poduzeća, podršku instaliranim aplikacijama na osobnim uređajima te podršku za rješavanje konflikata između osobnih aplikacija i aplikacija poduzeća.“

Slika 9. Mobilna sigurnosna politika



Izvor: https://digitalguardian.com/blog/ultimate-guide-byod-security-overcoming-challenges-creating-effective-policies-and-mitigating

Također Nate Lord 2016. u članku za Digital Guardian još navodi: „Vaša BYOD politika trebala bi jasno navesti vlasništvo nad aplikacijama i podacima, kao i aplikacije koje su dopuštene ili zabranjene te nadoknade (npr. hoće li tvrtka nadoknaditi zaposlenicima standardnu naknadu za korištenje, platiti za određene aplikacije ili dio mjesečnih računa?). Također bi trebala navesti sigurnosne zahtjeve za BYOD uređaje (npr. dali će poduzeće osigurati aplikaciju za sigurnost mobilnog uređaja koja mora biti instalirana na uređajima zaposlenika prije nego što im se odobri pristup podacima poduzeća ili će se zaposlenicima omogućiti odabir vlastitih sigurnosnih rješenja pod uvjetom da zadovoljavaju kriterije navedene od strane vašeg IT odjela?).

Odlazak zaposlenika također je važno razmatranje tijekom izrade vaše BYOD politike. Što se događa s podacima tvrtke koji su možda pohranjeni na uređaju zaposlenika kada isti napusti tvrtku? Definiranje jasnih politika koje objašnjavaju postupke koji se moraju pratiti kada se zaposlenik odvoji od poduzeća, kao što je brisanje uređaja zaposlenika od strane IT-a, treba detaljno objasniti u pisanim pravilima.

Konačno rizici, odgovornosti i odricanja od odgovornosti trebaju biti prikazana u pisanoj BYOD politici. To uključuje odgovornost poduzeća spram osobnih podataka zaposlenika ukoliko se uređaj mora obrisati zbog sigurnosne predostrožnosti, kao i

odgovornost zaposlenika zbog neovlaštenog širenja osjetljivih podataka poduzeća uzrokovanih nemarnošću ili zloupotrebom zaposlenika.“

Gornjim istraživanjem navedenim od strane Nate Lord-a može se konstatirati da je nedovoljan broj poduzeća uveo BYOD politiku. Zbog toga je vjerojatnost da će zaposlenici u poduzećima koja nisu uvela BYOD politiku stvoriti sigurnosne prijetnje veća nego u onima koja su ju uvela. Poduzeća bi zbog toga trebala preuzeti primarnu ulogu definiranja BYOD politika te također i obuku zaposlenika za pravilno korištenje njihovih uređaja u radne svrhe. Isto tako poduzeća bi trebala težiti definiranju što ispravnije BYOD politike koja će obuhvatiti sve njegove potrebe kao i potrebe svih učesnika u njegovom poslovanju.

3.6. Procjena tehnoloških mogućnosti poduzeća

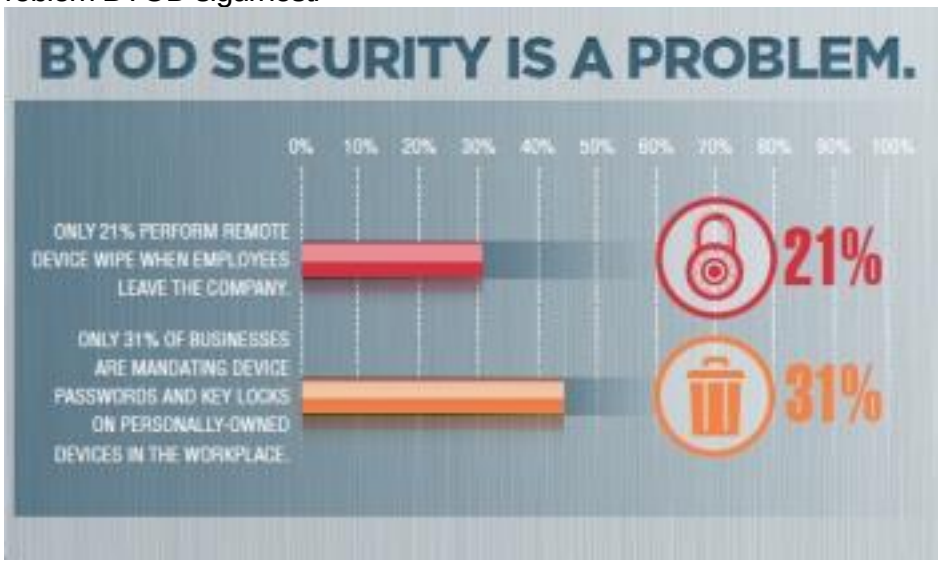
Procjena tehnoloških mogućnosti poduzeća tema je za koju Nate Lord 2016. u članku za Digital Guardian navodi: „Uz stvaranje i komuniciranje o vašoj BYOD politici morate osigurati da na raspolaganju imate odgovarajuće tehnološke resurse. Procjena vaših trenutačnih mogućnosti pomoći će identificirati i popuniti praznine kako bi se osiguralo uspješno uvođenje BYOD-a.

Nedostatak nadzora je jedna od najčešćih zabrinutosti vezanih za implementaciju BYOD-a. Poduzeća koja implementiraju BYOD politike moraju imati odgovarajuće osoblje u svojim odjelima za IT podršku kako bi pomogli zaposlenicima kod postavljanja i pružanja kontinuirane podrške i nadzora. Nisu sva rješenja kompatibilna sa svim uređajima ili operativnim sustavima. Tvrtke se mogu odlučiti za kupnju softverskog rješenja kompatibilnog s različitim uređajima ili mogu smatrati važnijim značajke i ponuditi drukčije rješenje za različite uređaje i OS-e.

Poduzeća bi trebala implementirati mjere i postupke za provjeru instalacije sigurnosnih rješenja na svim uređajima koji pristupaju podacima tvrtke. Oni također trebaju stvoriti protokole za identifikaciju i provođenje politika vezanih uz procjenu rizika različitih aplikacija i određivanje koje se konkretne aplikacije smatraju sigurnima kao i koje bi trebale biti zabranjene. Konačno, ako je povrat sredstava uključen u

politiku BYOD-a treba razmotriti proračunska pitanja i odgovarajuće resurse dodijeljene toj svrsi.“

Slika 10. Problem BYOD sigurnosti



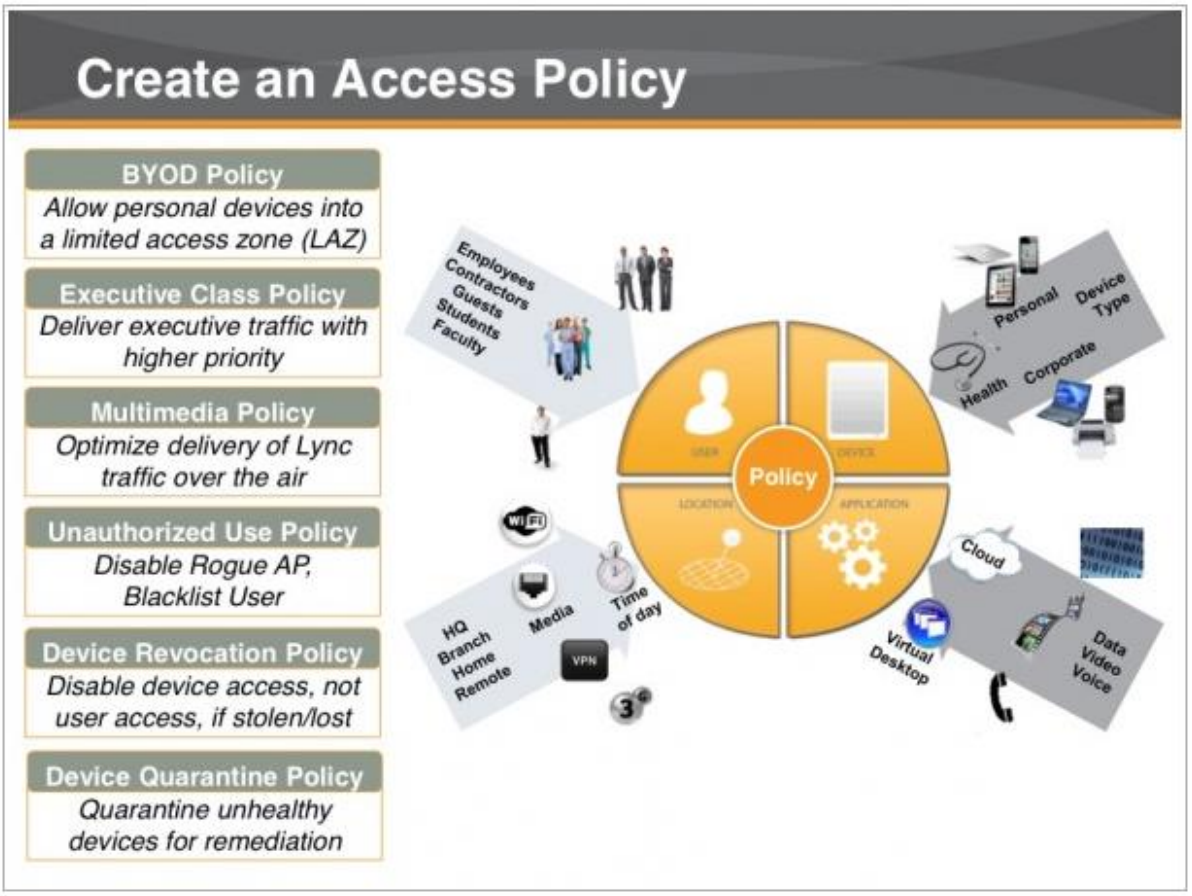
Izvor: https://digitalguardian.com/blog/ultimate-guide-byod-security-overcoming-challenges-creating-effective-policies-and-mitigating

Poduzeća moraju biti svjesna svojih tehnoloških mogućnosti kao i onih tehnoloških područja o kojima imaju manje saznanja radi ispravnog uvođenja BYOD-a. Ovo je potrebno zbog rješavanja svih mogućih sigurnosnih prijetnji.

3.7. Razmatranje BYOD sigurnosnih rješenja

Razmatranje BYOD sigurnosnih rješenja tema je za koju Nate Lord 2016. u članku za Digital Guardian navodi: „Nakon što su vaši sustavi i protokoli postavljeni, za uspjeh BYOD-a ključno je pružanje kontinuiranog obrazovanja zaposlenika o važnosti prihvatljive primjene kao i o osnovama vjerodostojnosti sigurnosti podataka. Osim toga, prava sigurnosna rješenja mogu smanjiti rizik za vaš BYOD i omogućiti tečno provođenje vaše politike. Postoji nekoliko elemenata koji bi trebali biti navedeni od strane učinkovitog BYOD sigurnosnog rješenja. Idealno rješenje je ono koje obuhvaća nekoliko ili sve te elemente i olakšava sveobuhvatnu strategiju mobilne sigurnosti.“

Slika 11. Stvaranje BYOD pristupne politike



Izvor: https://digitalguardian.com/blog/ultimate-guide-byod-security-overcoming-challenges-creating-effective-policies-and-mitigating

Poduzeća bi trebala obučavati zaposlenike da svoje uređaje koje koriste u radne svrhe pravilno upotrebljavaju unutar BYOD rješenja. Slijedeće teme će detaljnije razraditi sigurnosna rješenja koja se mogu koristiti za BYOD politiku.

3.7.1. Šifriranje podataka

Šifriranje podataka je tema za koju Nate Lord 2016. u članku za Digital Guardian navodi: „Budući da se upotrebom BYOD-a preuzimaju podaci izvan kontrole mnogih drugih sigurnosnih mjera poduzeća bitno je da ona šifriraju osjetljive podatke tijekom mirovanja i prijenosa. Šifriranje osigurava zaštićenost sadržaja osjetljivih datoteka čak i u najgorem slučaju kao što je ukraden uređaj ili promet presretnut preko nesigurne mreže.

Zahtijevanje upotrebe složenih zaporki nudi nekakvu zaštitu, ali šifriranje je bolje. Kako ovaj članak u InfoSec Institute-u navodi: „Kako bi se osigurala zaštita, poduzeća moraju implementirati šifriranje tijekom cijelog životnog vijeka podataka (u mirovanju i prijenosu). Kako bi se spriječio neovlašteni pristup i održalo šifriranje u slučaju sigurnosnog proboja IT odjel zabrinutog poduzeća trebao bi preuzeti kontrolu nad ključevima za šifriranje.““

Svi podaci poduzeća bi uvijek trebali biti šifrirani kako i u slučaju da budu ukradeni ne mogu biti upotrebljivi.

3.7.2. Kontrola instalacije aplikacija

Kontrola instalacije aplikacija je tema za koju Nate Lord 2016. u članku za Digital Guardian navodi: „IT neke kontrole dostupne kod određenih uređaja i operativnih sustava može iskoristiti za vršenje kontrole nad aplikacijama instaliranim na zaposlenikovom uređaju. Na primjer Apple iOS uređaji mogu se konfigurirati tako da se onemogući pristup App Store-u, a Android uređaji mogu se konfigurirati tako da blokiraju instalaciju aplikacija izvan Google Play Store ili aplikacija s neprikladnim sadržajem.

Međutim, za većinu tvrtki nije praktično rješenje ograničavanje zaposlenikovih mogućnosti spram preuzimanja ili instaliranja aplikacija na vlastite uređaje za osobnu upotrebu. Ove metode su slične mjerama poduzetim sa svrhom roditeljske kontrole, pa je prirodno da će se zaposlenici vjerojatno osjećati kao da je to povreda njihove slobode. Većina zaposlenika očekuje da će moći upotrebljavati svoje osobne uređaje po vlastitoj želji van radnog vremena, kad ne obavljaju posao ili nisu povezani s osiguranom mrežom tvrtke, što čini druga rješenja mnogo praktičnijim za BYOD sigurnost.“

Ovo daje poduzećima mogućnost da odluče koje aplikacije će zaposlenici moći instalirati ili ne instalirati na svoje uređaje. Ipak ovo nije najbolje rješenje za BYOD politiku jer to može naljutiti zaposlenike koji tada mogu misliti da se želi kontrolirati koje će aplikacije oni koristiti na svojim uređajima van poslovnih aktivnosti.

3.7.3. Kontejnizacija

Kontejnizacija je tema za koju Nate Lord 2016. u članku za Digital Guardian navodi: „Kontejnizacija je metoda kojom se dio uređaja u biti može izdvojiti u svoj vlastiti zaštićeni spremnik, zaštićen zasebnom lozinkom i reguliran zasebnim skupom pravila od ostatka aplikacija i sadržaja na uređaju. To omogućava zaposlenicima da uživaju u potpunom neometanom korištenju njihovih uređaja u slobodno vrijeme bez uvođenja sigurnosnih rizika u mrežu tvrtke. Kada je korisnik prijavljen u kontejnizirano područje, nedostupne su osobne aplikacije i druge značajke kojima spremnik ne upravlja. Kontejniziranje je dopadljivo rješenje koje ne ograničava sposobnost zaposlenika za upotrebljavanje njihovih vlastitih uređaja kako žele, dok uklanja mogućnost da zaposlenici koriste ili pristupaju aplikacijama koje ne zadovoljavaju sigurnosni nivo tvrtke prilikom rada.

Kontejniziranje ograničava korporativnu odgovornost bez utjecaja na osobnu upotrebu, ali loša strana je da ono ne štiti osobne podatke zaposlenika na uređajima koji su izgubljeni ili ukradeni i moraju biti obrisani. To je izazov koji se lako prevladava sa pravilnim stvaranjem pričuvne kopije osobnih podataka.“

Ovom metodom poduzeće može na uređajima zaposlenika stvoriti zaštićeni spremnik u kojemu se nalazi sve što je zaposleniku potrebno za izvršavanje radnih obaveza. Ovaj spremnik je zaštićen nekom vrstom autorizacije a još bi trebao biti i šifriran. Ovime se omogućava zaposlenicima da svoje uređaje mogu koristiti za vlastitu upotrebu kako žele, a kad su na poslu mogu koristiti aplikacije za posao na koje ne mogu utjecati aplikacije van spremnika. Ovo pruža poduzeću sigurnost od nesigurnih aplikacija ili drugih mogućih prijetnji onemogućavajući im da utječu na aplikacije i datoteke poduzeća.

3.7.4. Lista nepoželjnih aplikacija

Lista nepoželjnih aplikacija je tema za koju Nate Lord 2016. u članku za Digital Guardian navodi: „Lista nepoželjnih aplikacija je pojam koji opisuje proces blokiranja ili zabrane specifičnih aplikacija za koje je zaključeno da predstavljaju rizik sigurnosti

poduzeća. Lista nepoželjnih aplikacija je također metoda koju neke tvrtke koriste da zaposlenicima ograniče pristup ka aplikacijama koje mogu sprječavati produktivnost, kao igre ili aplikacije društvenih mreža. Usluge dijeljenja datoteka su još jedna kategorija aplikacija koje se često nalaze na listama nepoželjnih aplikacija, budući da tvrtke strahuju da bi se osjetljive informacije mogle namjerno ili nehotice dijeliti od strane zaposlenika s neovlaštenim trećim stranama.

Ograničavanje pristupa aplikacijama koje ne zadovoljavaju sigurnosne kriterije vašeg poduzeća može biti učinkovito, lista nepoželjnih aplikacija se često ne koristi za BYOD, jer taj proces znači kontroliranje pristupa aplikacijama na osobnim uređajima zaposlenika tijekom i izvan radnog vremena. Naravno, to predstavlja problem nekim zaposlenicima koji uživaju u igranju Pokémon-a GO kada nisu na poslu.“

Ovime poduzeće može na uređajima zaposlenika blokirati one aplikacije koje smatra nesigurnim i nepoželjnim za njih. Time se smanjuje utjecaj istih na povećanje sigurnosnog rizika. Ovo može izazvati kod zaposlenika razmišljanje da se provodi kontrola o aplikacijama koje oni koriste van njihovih poslovnih aktivnosti.

3.7.5. Lista poželjnih aplikacija

Lista poželjnih aplikacija je tema za koju Nate Lord 2016. u članku za Digital Guardian navodi: „Lista poželjnih aplikacija jednostavno je suprotna od liste nepoželjnih aplikacija. Umjesto da blokira pristup listi određenih aplikacija, lista poželjnih aplikacija dopušta pristup samo listi odobrenih aplikacija. Često se smatra učinkovitijim procesom jednostavno zbog ogromnog broja aplikacija i web stranica koje postoje. Ponekad je prekasno čekati da neki zaposlenik preuzme neku aplikaciju i iskoristi ju za prijenos podataka kako bi se utvrdilo da ona predstavlja sigurnosni rizik.

Lista poželjnih aplikacija zaobilazi ovaj problem jednostavno ne dopuštajući pristup ničemu osim ako je unaprijed odobreno kao sigurno od IT-a. Naravno kao i lista nepoželjnih aplikacija ona može stvoriti probleme za BYOD blokiranjem pristupa aplikacijama koje bi zaposlenici možda željeli koristiti van radnog vremena.“

Ovime poduzeće može na uređajima zaposlenika omogućiti one aplikacije koje smatra sigurnim i poželjnim za njih. Time se smanjuje utjecaj svih ostalih aplikacija koje mogu izazvati povećanje sigurnosnog rizika. Ovo može izazvati kod zaposlenika razmišljanje da se provodi kontrola o aplikacijama koje oni koriste van njihovih poslovnih aktivnosti.

3.7.6. Ostale BYOD sigurnosne mjere

Ostale BYOD sigurnosne mjere tema je za koju Nate Lord 2016. u članku za Digital Guardian navodi: „Postoji niz drugih sigurnosnih mjera koje se ponekad koriste kao dio sveobuhvatnog BYOD sigurnosnog programa. Antivirusni softver instaliran na pojedinačnim uređajima je na primjer često glavna osnova takvih sigurnosnih programa. Tvrtke mogu kupiti više licenčni softver i instalirati ga na BYOD uređaje ili jednostavno zahtijevati od zaposlenika da instaliraju vlastiti i verificiraju sa IT-om zaštićenost njihovih uređaja. Pošto sve više zlonamjernih programa cilja mobilne uređaje vrlo je stvaran rizik da takav zlonamjerni program utječe na mrežu tvrtke putem osobnog uređaja zaposlenika.

Nadziranje je još jedna komponenta koja se ponekad koristi kao dio BYOD sigurnosnog programa, iako sa različitim mišljenjima. IT može implementirati sustave koji nadziru GPS lokaciju uređaja zaposlenika ili internetski promet na pojedinačnim uređajima. Iako se ovi sustavi nadzora mogu pokazati blagotvornim za otkrivanje neuobičajene aktivnosti ili lociranje izgubljenog uređaja, mnogi smatraju da ta rješenja previše zadiru u privatnost zaposlenika.“

Postoje i ostale sigurnosne mjere (nadziranje GPS-a te internetskog prometa itd. uređaja, antivirusni programi itd.) koje se mogu primijeniti za BYOD rješenje. One same po sebi nisu dovoljno učinkovite već bi trebale biti kombinirane sa drugim mjerama i rješenjima kako bi se dobilo najbolje, a time i najpravilnije sigurnosno rješenje za BYOD. To rješenje bi trebalo sagledati sve aspekte poduzeća kako bi se omogućio odabir najboljih sigurnosnih mjera i rješenja te stvorilo BYOD sigurnosno rješenje najbolje za to poduzeće.

4. PREDNOSTI I NEDOSTACI BYOD-A

BYOD rješenje pruža određene prednosti poduzećima. Dali će se isto primijeniti treba odlučiti obzirom na moguće prednosti i nedostatke koji su navedeni u daljnjem tekstu.

4.1. Prednosti BYOD-a

Na stranici COMODO-va sustava upravljanja mobilnim uređajem navodi se: „Postoje različite prednosti za tvrtke koje usvajaju i potiču BYOD primjenu…

- Povećava produktivnost (Zaposlenici mogu uvijek raditi koristeći svoje uređaje za pristup poslu, mogu čak i provjeriti e-poštu te ažurirati prezentacije dok su na odmoru ili dok putuju prema kući. To dovodi do povećanja produktivnosti za bilo koju tvrtku.)
- Pomaže tvrtkama poboljšati moral zaposlenika. (Zaposlenici rade s uređajima koji su im ugodniji te su stoga zadovoljniji kad rade na mjestima gdje se potiče BYOD.)
- Pomaže u smanjenju troškova, osobito malim i srednjim poduzećima. (Novac koji treba uložiti u kupnju hardvera, softvera itd. može se iskoristiti za druge svrhe dok zaposlenici koriste svoje uređaje za rad. Tako na vrlo izravan način mala i srednja poduzeća mogu imati koristi od BYOD-a.)
- Prema stručnjacima BYOD pomaže poboljšanju odnosa između zaposlenika i IT odjela.
- BYOD pomaže tvrtkama da budu u tijeku tehnoloških promjena pošto zaposlenici koristeći osobne uređaje ostaju tehnološki aktualni a iste koriste u tvrtki za rad.
- Posjedovanje BYOD politika može pomoći tvrtkama u privlačenju novih zaposlenika jer postoji mnogo ljudi koji bi voljeli koristiti vlastite mobilne uređaje i za posao.“

Zbog ovih prednosti BYOD je zanimljiv poduzećima, a to su i glavni razlozi zbog kojih ga ona žele primijeniti.

4.2. Nedostaci BYOD-a

COMODO-v sustav upravljanja mobilnim uređajem također navodi: „Iako BYOD ima svoje prednosti, isto tako nije lišen nedostataka. Evo pregleda nedostataka ovog rastućeg trenda...

- Sigurnosna pitanja velika su zabrinutost za tvrtke koje usvajaju BYOD. (Većina IT stručnjaka vjeruje da usvajanje BYOD-a uzrokuje ozbiljne sigurnosne probleme bilo kojoj tvrtki i podacima koje tvrtka pohranjuje na svojim sustavima/mreži. Sigurnosne prijetnje proizlaze zbog povećanog broja ljudi koji bi pristupali podacima tvrtke putem drugih uređaja i zbog toga što bi zlonamjerni softver mogao prodrijeti putem bilo kojeg BYOD uređaja koji nije pravilno zaštićen.)
- Datoteke i podaci tvrtke kojima zaposlenici mogu slobodno pristupati koristeći svoje uređaje, također mogu završiti u pogrešnim rukama. (Takvi podaci lako mogu biti viđeni ili ukradeni od zlonamjernih autsajdera[9].)
- BYOD uređaji također mogu biti ukradeni ili izgubljeni, što bi također uzrokovalo povrede podataka.
- IT odjeli u tvrtkama u kojima je primijenjen BYOD trebaju odoljeti ogromnom pritisku u potpori, upravljanju i osiguranju svih BYOD uređaja.“

Ovi nedostaci BYOD-a su glavni uzrok zbog kojeg ga neka poduzeća ne žele primijeniti, dok ga neka druga poduzeća možda žele primijeniti ali se zbog istih dvoume.

[9] Autsajder – onaj koji se ne prihvaća kao član neke grupe «prema» https://jezikoslovac.com/word/vc33, Jezikoslovac, 03.08.2017 u 9:52

5. SUSTAV UPRAVLJANJA MOBILNIM UREĐAJEM

Sustav upravljanja mobilnim uređajem tema je za koju Nate Lord 2016. u članku za Digital Guardian navodi: „Rješenja za upravljanje mobilnim uređajima (MDM[10]) nude ravnotežu između potpune kontrole za poslodavce i potpune slobode za zaposlenike, nudeći mogućnost implementiranja, osiguranja i integracije uređaja na jednu mrežu te potom centralno nadziranje i upravljanje tim uređajima. MDM područje još je uvijek u svojim začecima i nije lišeno svih problema. Na primjer ovaj članak u CIO-u navodi da bi neka poduzeća mogla iskoristiti prednost naprednijih značajki dostupnih uz MDM, stvarajući manje idealno korisničko iskustvo koje je previše ograničavajuće i navodi zaposlenike na odbojnost BYOD programu poduzeća.“

COMODO na svojoj stranici navodi da njegov MDM sustav radi na slijedeći način:

- „Upisuje uređaj povezan s mrežom tvrtke uz pomoću upravitelja uređaja kako bi osigurao postupak provjere autentičnosti te provjerio da li je uređaj originalan
- Šifrira vezu između MDM VPN-a i MDM Gateway poslužitelja
- MDM uređaj komunicira s poslužiteljem upravljanja mobilnim uređajem i generira sigurnu vezu za mrežni pristup s MDM poslužiteljem.
- Poslužitelj tada prikuplja informacije o uređaju kako bi se osigurale postavke grupnih pravila na uređaju.
- Aplikacija MDM uređaja se potom autorizira pomoću upravitelja mobilnog uređaja
- MDM uređaj je tada ovlašten za pristup uslugama na korporativnoj mreži“

[10] Mobile device management – upravljanje mobilnim uređajima

Također COMODO na svojoj stranici za svoj MDM sustav navodi da on pruža ove prednosti:

- „Uvjereni ste u redovita skeniranja za pronalaženje zlonamjernih programa
- Generira listu nepoželjnih i poželjnih aplikacija
- Ograničava pristup uređaja korporativnim mail-ovima
- Osigurani ste šifriranom komunikacijom
- Čuva zapis vaših aktivnosti
- Pomaže upravljati svim uređajima s jedne ujedinjene konzole
- Provodi sigurnost podataka i uređaja
- Zajamčeno vam je potpuno upravljanje aplikacijama“

Uz ove prednosti također je jako bitno da MDM sustav podržava što više različitih sustava kako bi se obuhvatilo sve uređaje koje zaposlenici posjeduju. MDM sustavom se dobiva jednostavno upravljanje svim mobilnim uređajima zaposlenika te njihovo osiguranje od raznih mogućih prijetnji.

6. ZAKLJUČAK

Iz obrade teme „BYOD u uredskom poslovanju“ zaključuje se da je primjena BYOD pravila u poduzećima neophodna. Obujam primjene BYOD pravila ovisi od poduzeća do poduzeća jer nisu sva ista te nemaju iste uvjete i navike zaposlenika. Zaposlenici nekog poduzeća možda se ne mogu svojim uređajima spajati na Internet preko mreže poduzeća dok u drugom poduzeću to mogu. Tom poduzeću su onda potrebna BYOD pravila kako bi se riješile moguće prijetnje za mrežu poduzeća. Zbog toga IT mora raditi na implementaciji sigurnosnih rješenja prikladnih za to poduzeće.

Zaposlenici imaju ključnu ulogu u BYOD politici jer su oni ti koji koriste svoje uređaje na radnom mjestu te bi edukacija zaposlenika trebala biti prioritet kod uvođenja BYOD pravila. Svaki korak kod implementacije BYOD politike treba biti pažljivo isplaniran od kreiranja, primjene pa do izvedbe. Poduzeće također treba biti u mogućnosti pružati odgovarajuću podršku za BYOD tijekom njegove implementacije.

BYOD sigurnosno rješenje bi trebalo maksimalno smanjiti sigurnosne rizike ali istodobno omogućiti poduzeću da koristi sve prednosti BYOD-a. Iako u poduzeću možda ne planiraju primijeniti BYOD moraju biti svjesni da postoje rizici kad zaposlenici donose i koriste svoje uređaje na poslu. Shodno tome trebali bi poduzeti korake ka eliminaciji tih rizika.

Sve BYOD-ove prednosti nadmašuju njegove manjkavosti te poduzeća ne bi trebala pokušavati zabraniti njegovu primjenu već ga primijeniti, ali na ispravan način kako bi maksimalno umanjila nedostatke te maksimalno iskoristila njegove prednosti.

Gornje se može postići primjenom MDM sustava koji će udovoljiti svim zahtjevima poduzeća. Taj MDM sustav će time omogućiti adekvatno upravljanje mobilnim uređajima u svrhu maksimiziranja BYOD-ovih prednosti te maksimalnog smanjivanja njegovih nedostataka.

LITERATURA

Časopisi:

1. Yeboah-Boateng E. O. i Boaten F. E., Bring-Your-Own-Device (BYOD): An Evaluation of Associated Risks to Corporate Information Security, International Journal of Information Technology (IT) & Engineering, Svezak 4, Broj 8, 2016, str. 12-30
2. Varbanov R., APPLICATIONS OF THE BYOD CONCEPTION – BENEFITS,
3. RISKS AND APPROACHES, Business Management / Biznes Upravlenie, Svezak 24, Broj 2, 2014, str. 80-99
4. Greengard S., BYOD Increases Productivity and Job Satisfaction, Baseline, 14.04.2014, str. 1-1
5. Richmond R., Morrison K. M. i Lim E., What Do You Do When an Employee with Access to Your Company's Trade Secrets Leaves to Work for a Competitor?, Employee Relations Law Journal, Svezak 43, Broj 2, 2017, str. 36-44

Internetski izvori:

1. Android (operating system) – Wikipedia, 24.07.2017. u 14:51, Android (operating system), Wikipedia, https://en.wikipedia.org/wiki/Android_(operating_system), 01.08.2017. u 12:41
2. iOS – Wikipedia, 11.07.2017. u 17:01, iOS, Wikipedia, https://en.wikipedia.org/wiki/IOS, 01.08.2017. u 12:41
3. Microsoft Windows – Wikipedia, 01.08.2017. u 04:55, Microsoft Windows, Wikipedia, https://en.wikipedia.org/wiki/Microsoft_Windows, 01.08.2017. u 13:18
4. Windows 10 – Wikipedia, 01.08.2017. u 06:18, Windows 10, Wikipedia, https://en.wikipedia.org/wiki/Windows_10, 01.08.2017. u 13:18
5. macOS – Wikipedia, 27.07.2017. u 06:55, macOS, Wikipedia, https://en.wikipedia.org/wiki/MacOS, 01.08.2017. u 13:18
6. Dots per inch – Wikipedia, 28.07.2017. u 20:55, Dots per inch, Wikipedia, https://en.wikipedia.org/wiki/Dots_per_inch, 01.08.2017. u 14:40

7. Pixel density – Wikipedia, 10.07.2017. u 17:43, Pixel density, Wikipedia, https://en.wikipedia.org/wiki/Pixel_density, 01.08.2017. u 14:40
8. Lord N., The Ultimate Guide to BYOD Security, 11.10.2016., Overcoming Challenges, Creating Effective Policies, and Mitigating Risks to Maximize Benefits, DigitalGuardian, https://digitalguardian.com/blog/ultimate-guide-byod-security-overcoming-challenges-creating-effective-policies-and-mitigating, 04.08.2017. u 5:52
9. What is BYOD?, Benefits of BYOD (Bring Your Own Device) Policy, COMODO, https://dm.comodo.com/what-is-byod/, 04.08.2017. u 5:52
10. Bring your own device – Wikipedia, 11.09.2017. u 7:48, Bring your own device, Wikipedia, https://en.wikipedia.org/wiki/Bring_your_own_device, 11.09.2017 u 19:25
11. Korištenje osobnih mobilnih uređaja u poslovne svrhe – Centar za poslovnu sigurnost, 10.05.2017., Korištenje osobnih mobilnih uređaja u poslovne svrhe, Centar za poslovnu sigurnost, http://www.cps-zg.hr/info/koristenje-osobnih-mobilnih-uredaja-u-poslovne-svrhe/, 12.09.2017. u 14:47
12. Mobile Device Management, Why Mobile Device Management, COMODO, https://dm.comodo.com/, 12.09.2017. u 17:44

Ostali Izvori:

1. Greengard S., BYOD Increases Productivity and Job Satisfaction, Australian National Audit Office, 2014.
2. Agudelo C. A., Bosua R., Ahmad A. i Maynard S. B., Understanding Knowledge Leakage & BYOD (Bring Your Own Device): A Mobile Worker Perspective, Australasian Conference on Information Systems, Adelaide, 2015.
3. Downer K. i Bhattacharya M., BYOD Security: A New Business Challenge, Proceedings of The 5th International Symposium on Cloud and Service
4. Computing, 2015.
5. Sobers A., BYOD and the Mobile Enterprise – Organisational challenges and solutions to adopt BYOD, Aston University, Birmingham

POPIS SLIKA

Slika **Stranica**

Slika 1. Početni zaslon Apple iOS 11 beta 6 4
Slika 2. Početni zaslon Google Android-a 8.0 5
Slika 3. Radna površina Apple macOS-a High Sierra beta 1 6
Slika 4. Radna površina Microsoft Windows-a 10 7
Slika 5. Stvaranje BYOD-a sigurnim 13
Slika 6. BYOD Rizici 15
Slika 7. BYOD korisnički trendovi 16
Slika 8. Glavne zabrinutosti oko razvoja BYOD politike 18
Slika 9. Mobilna sigurnosna politika 21
Slika 10. Problem BYOD sigurnosti 23
Slika 11. Stvaranje BYOD pristupne politike 24

SAŽETAK

Tema ovog rada je analiza zahtijeva potrebnih kako bi se BYOD politika mogla pravilno implementirati u nekom poduzeću. Nabavka uređaja jedan je od glavnih faktora za implementaciju BYOD politike. Uređaji moraju zadovoljiti određene zahtjeve koji ovise o poduzeću. Istraživanje pokazuje da mnoge tvrtke ne primjenjuju ili ne planiraju primijeniti BYOD politiku zbog bojazni koje se odnose na sigurnosne prijetnje. Unatoč tome istraživanja pokazuju rast broja poduzeća koja dozvoljavaju zaposlenicima donošenje osobnih uređaja na posao. Uvođenje BYOD politike nije potrebno samo onim poduzećima u kojima se osobni uređaji koriste za obavljanje posla već i u onima gdje se ne koriste, a iz razloga jer je upravljanje i tim uređajima potrebno radi pravilne sigurnosne politike. BYOD politika posjeduje prednosti i nedostatke koje treba komparirati te razmotriti dali je obzirom na njegove nedostatke isplativa njegova primjena. MDM sustav omogućava poduzećima upravljanje mobilnim uređajima sa jednog centraliziranog mjesta kao i rješavanje sigurnosnih problema BYOD-a.

Ključne riječi: BYOD, poduzeće, uređaj, sigurnost, MDM

ABSTRACT

The topic of this paper is the analysis of requirements necessary to make a BYOD policy properly implemented in a company. Procuration of a device is one of the main factors for implementing a BYOD policy. Devices must meet certain requirements that depend on the company. A research shows that many companies do not implement or do not plan to implement a BYOD policy for fear relating to security threats. Despite this, research shows a growth in the number of companies that allow employees to bring their personal devices to work. The introduction of a BYOD policy is not only necessary for those companies where personal devices are used for doing work but also in those where they are not used, because management of these devices is also needed for a proper security policy. BYOD policy has advantages and disadvantages that need to be compared, and then consider if due to its disadvantages its implementation is profitable. The MDM system enables companies to manage mobile devices from one centralized location as well as solving BYOD security issues.

Key words: BYOD, company, device, security, MDM