BYOD - Korištenje privatnih uređaja u poslovne svrhe

 Termin **BYOD** je gotovo nemoguće izbjeći u IT krugovima. **BYOD** je akronim za ***Bring Your Own Device*** ili mogućnost korisnika da za poslovne potrebe donese vlastiti uređaj (računalo, mobitel, tablet, itd...). Sve veći broj osoba koristi tzv. *smart* uređaje, prijenosna računala različitih dimenzija. Ti uređaji uvelike eliminiraju potrebu za korištenjem stolnih računala i/ili laptopa. Povezani su na Internet ali i na poslovne sustave organizacije. Korištenje vlastitog uređaja donosi niz prednosti, ali i rizika poslovanju.

Što BYOD znači za posao, a što za informacijsku sigurnost?

U današnje vrijeme pritisak na IT u pogledu sigurnosti i upravljanja promjenama je sve veći, a *budget* sve manji. Korisnici zahtijevaju najnovije, najmodernije tehnologije, kako bi ostali kompetitivni na tržištu, traže brzu dostupnost informacija i pristup aplikacijama izvan prostora organizacije.

BYOD, kao i svaki drugi sustav treba sistematski planirati, implementirati, nadzirati i poboljšavati, što je poznato kao **PDCA** (***Plan Do Check Act***) ciklus. BYOD, ispravno implementiran, smanjuje troškove organizacije, te podiže razinu produktivnosti i dobiti.

Zanimljiv je podatak da preko 60% zaposlenika već koristi vlastiti uređaj u jednom ili više aspekata poslovanja. Korištenje vlastitih uređaja nije više pitanje tipa da ili ne, već kako! Ne smije se pretpostaviti da će korisnici prestati koristiti svoje uređaje samo zato što ste to propisali; većina će ih nastaviti koristiti, ali izvan radara, bez nadzora.

Kako implementirati BYOD?

Ovisno o poslovanju, kulturi, zakonskim i regulativnim odredbama, kao i načinu upravljanja rizikom, organizacija će odrediti način na koji će sustav biti implementiran. Naravno, ako je procijenjeni rizik prevelik, organizacija može u potpunosti zabraniti korištenje vlastitih uređaja, ali sustav nadzora bi i u tom slučaju trebao biti postavljen.

Najbolji put je implementacija pravila korištenja vlastitih uređaja (BYOD politika). Prvi korak u stvaranju BYOD sustava je postavljanje pravih pitanja:

- Kojim sustavima korisnici mogu i/ili trebaju pristupiti s vlastitih uređaja? (Sadrže li ti sustavi povjerljive ili osjetljive informacije? Postoje li dodatne zaštite pristupa sustavu, kao *two-factor authentication* ili slično?)
- Koji korisnici imaju stvarnu potrebu za istim? (Dio korisnika može imati stvarnu potrebu, ali ostali ne trebaju pristup. Cilj je smanjiti izloženost na najmanju moguću mjeru.)
- Sadrže li uređaji povjerljive podatke? (Povjerljivi podaci su arhivirani na uređaju? Kako su štićeni? Postoji li enkripcija?)
- Tko je vlasnik uređaja? (Vlasnik uređaja je uglavnom korisnik, ali podaci na njemu su vlasništvo organizacije.)
- Tko postavlja sigurnosne postavke uređaja? (Sigurnosne postavke uglavnom postavlja korisnik ili administrator sigurnosti. Najbolji pristup je mogućnost postavljanja sigurnosti na razini uređaja, tako da se podaci štite i u slučaju njegove krađe ili gubitka.)
- Softver na uređajima je razvijen ili odabran *in-house* ili je korisnički? (*In-house* softver je prilagođen poslovanju organizacije i generalno je sigurniji od onog kojeg korisnik sam odabere. Npr. email klijent, sustav za enkripciju i sl.)
- Kako ćemo mjeriti učinkovitost propisanih kontrola? (Potrebno je razviti sustav mjerenja

učinkovitosti postavljenih kontrola.)
- Kako ćemo nadzirati korištenje korisničkih uređaja? (Potrebno je razviti metodologije i procedure nadzora korištenja uređaja od strane djelatnika.)
- Na koji način motivirati zaposlenike da koriste svoje uređaje na prikladan i siguran način? (Korisnike treba educirati o ispravnom i sigurnom korištenju uređaja i poslovnih aplikacija. Stalno podizanje svijesti i upoznavanje s opasnostima je kritično za održavanje i podizanje razine sigurnosti BYOD.)

Odgovor na ova pitanja daje osnovne podatke za razumijevanje rizika i prednosti korištenja BYOD u Vašoj organizaciji.

Kako zaštiti BYOD?

Korištenje BYOD definitivno predstavlja rizik za poslovanje, najčešće prisutan kao rizik od krađe podataka, neovlaštenog pristupa aplikacijama i sustavima organizacije, gubitku reputacije i sl. Ako smo utvrdili da korisnici trebaju koristiti vlastite uređaje, iste moramo zaštiti na odgovarajući način u svrhu smanjenja izloženosti rizicima, ali moramo paziti da u isto vrijeme ne otežamo rad korisnicima, jer taj put najčešće vodi do zaobilaženja pravila i stvaranja novih rizika.

- Kompleksne lozinke za pristup uređaju ili druge metode pristupa (crtanje uzorka i sl.).
- AV – antivirusna zaštita.
- DLP – *Data Loss Prevention* – zaštita od gubitka podataka.
- Potpuna enkripcija memorije, zamjenjivih medija i podataka u prijenosu.
- MDM – *Mobile Device Management* sustav za potpuno uklanjanje podataka s uređaja u slučaju krađe ili gubitka.
- Kontrola dozvoljenih aplikacija.
- Redovite kontrole uređaja.
- Pristup poslovnim aplikacijama isključivo kroz VPN

Zaštita uređaja kroz sve gore navedene razine otežava posao potencijalnim napadačima u krađi podataka, a organizaciji daje dovoljno kontrole nad uređajem u slučaju njegovog gubitka ili krađe.

Ne zaboravite zaštiti ostale uređaje koji se povezuju sa BYOD!

BYOD je gotovo neizbježan faktor u današnjem poslovanju. Implementiran ispravno, predstavlja blagoslov za organizaciju i njene zaposlenike. Implementiran loše, postaje noćna mora za organizaciju i sigurnosni tim.

sri, 2013-06-05 13:01 - Darie Marić**Kategorije:** Informacijska sigurnost [1]
Vote: 0

No votes yet

Source URL: https://sysportal.carnet.hr/node/1235

Links
[1] https://sysportal.carnet.hr/taxonomy/term/32