Kuidas saada aru ja mida teha, kui IT administraator kuritarvitab ettevõtte usaldust?

11 aastat tagasi - 20.03.2015 Autor: Iteraction.ee

Üldiselt usaldavad ettevõtted oma IT spetsialiste, kes tagavad nende IT infrastruktuuri ja süsteemide toimimise. Kuigi valdav enamus süsteemiadministraatoritest on ausad, töökad ja võibolla aeg ajalt ka liigselt vähe hinnatud (muide on olemas System Administrator Appreciation Day), siis oleme ausad: ka nende seas on inimesi, kellel võivad tekkida halvad kavatsused, kiusatus lisasissetuleku järele või kättemaksuhimu nende arvates ebaõiglase kohtlemise korral.

IT administraatorite puhul on see probleem just eriti terav, kuna neile usaldatud firma tundliku info hulk on sageli väga suur ning neil on kontroll ettevõtte jaoks väga oluliste süsteemide üle. Antud artiklis toome välja mõned levinumad olukorrad, kus konfikt võib tekkida ning anname soovitusi, kuidas sääraseid probleeme ennetada.

Kust saavad probleemid alguse?

Probleemid IT administraatoritega põhinevad tavaliselt kas vale inimese valimisel või liiga vähesel ettevõtte poolsel kontrollimisel nende töö üle.

Kuna IT administraatoritel on võrdlemisi suur ligipääs firma siseinfole ning nende kontrollida on ka olulised rakendused, siis kui juhtub selline olukord, kus IT admin pöörab firma vastu, toob see kaasa sageli väga suuri probleeme. Näiteks ei pääse inimesed ettevõttes enam võrgule ja rakendustele ligi ja ei saa tööd teha, klientide info võib kaduda ettevõtte serveritest, süsteem nakatuda pahavaraga, tootmine seiskuda jne – kõik sõltub sellest, kui olulist rolli mängib IT antud ettevõttes. Kusjuures paljudel juhtudel võivad säärased laheneda valesti käitunud süsteemiadministraatori huvides, sest ettevõttel pole lihtsalt muud valikut. Seetõttu on eriti oluline veenduda näiteks IT spetsialisti palkamisel või teenuspartneri valikul nende usaldatavuses. Tuleb teha korralik taustakontroll ning veenduda mis inimesega on tegu.

Tasub mainida, et enamus probleemidest tuleneb ka sellest, et IT administraatori või teenuspartneri töö üle puudub otsene kontroll (ettevõtte juhtkonda ei huvita IT pool ning oluline on lihtsalt, et kõik toimiks). See annab aga IT poolega tegelejatele vaba voli tegeleda ükskõik millega.

Paljudel juhtudel ei tule probleemsed juhtumid üldse avalikuks, kuna firma ei esita süüdistusi, mis võiksid tuua kaasa maine ja usalduse languse klientide hulgas.

Oht on suurem just väiksemate ettevõtete hulgas, milledel pole tavaliselt IT haldamiseks ja kontrollimiseks piisavalt ressursse ning kõik on korraldatud ühe isiku poolt. Seevastu juhtkond on hõivatud pigem olulisemate teemadega ning IT asjadest ka väga ei huvituta.

Järgnevalt toome välja mõned levinumad olukorrad, kus IT administraator ei käitu ettevõtte huvides ning hiljem pakume välja mõned soovitused, kuidas neid olukordi märgata ning mida nende puhul ette võtta:

Kas usaldad oma IT administraatorit?

1. IT administraator tegutseb oma parema äranägemise huvides ega järgi etteantud IT poliitikaid:

Tegemist on olukorraga, kus ettevõttel on kindlad IT poliitikad, näiteks on välismaal asuva emafirma poolt peale surutud riistvara või tarkvara lahendused, mis ei pruugi firmas töötavale IT administraatorile meeldida.

Oma parema äranägemise järgi otsustab ta kasutada aga teisi tootjaid või minna ümber korporatsiooni piirangutest. IT probleemide ilmnedes võib aga äkitselt selguda, et teistsugune lahendus ei toimi ning see võib tekitada ettevõttele ka majanduslikku kahju või vajadust lisainvesteeringute järele. Kusjuures see probleem võib esile kerkida ootamatult, kuna firma juhtkond ei ole

tavaliselt väga kursis IT poolel toimuvaga ning IT administraatoriel on paljus osas vabad käed.

Ekstreemsem variant antud olukorrast on see, kus IT administraatorile on antud väga palju vabadust ja liiga vähe kontrolli ning hiljem on kogu süsteem ehitatud tema äranägemise järgi ning vaid temal on selle olulistele komponentidele ligipääs. Maailmast on juhtumeid, kus seejärel keeldub admin andmast teistele kui asjatundmatutele isikutele ka „oma süsteemile“ vajalikke juurdepääse.

Kuidas sellist probleemi ennetada: Üldiselt on hea, kui olulisemate süsteemide haldamisse on kaasatud mitu isikut, kellel on vajalik juurdepääs. See on tegelikult hea kas või puhkuste ajal süsteemiadministraatori asendamiseks. Lisaks peaksid olema süsteemid korraldatud vastavalt parimatele praktikatele (näiteks ITIL) või siis korporatsiooni nõuetele ning seda tuleks aeg ajalt sõltumatu osapoole poolt ka kontrollida.

2. IT administraator kasutab ettevõtte riistvara isiklikes ärihuvides:

Antud probleem tuleneb jällegi sellest, et IT administraatori töö üle on väga vähene kontroll ning tal on sisuliselt süsteemis vaba voli. See tähendab näiteks seda, et IT admin hostib näiteks oma isiklikku veebisaiti (mis võib müüa ükskõik mida) ettevõtte serverites ning on olnud juhuseid, kus ta on selleks loonud väga keerulised tulemüüri reeglid, et võimaldada märkamatut ligipääsu ettevõtte võrgule.

Selliste olukordade vastu aitavad võidelda tõhusad võrgu juurdepääsude ja haldustööriistad, mis teavitavad kui näiteks mingeid paroole on muudetud või keegi pääseb ligi võrgu sisule, millele ta ei tohiks. Kindlasti võiks olla ülevaade võrgust rohkematel isikutel, kui vaid see üks süsteemiadministraator.

3. Süsteemiadministraator luurab töötajate järel:

Isiklikust vaatevinklist on see vast kõige ebameeldivam variant. IT administraator, kes pidevalt jälgib töötajaid ning luurab nende järgi, loeb nende e-maile, teab nende paroole, näeb nende pilte ja külastatud veebisaite ning kõike muud, mis peaks olema privaatne. Selline asi võib juhtuda, kui keegi ei kontrolli IT administraatorit ning pole tehtud piisavalt tööd ka sobiva isiku valimisega.

Kui ettevõttes on vaid üks IT inimene, kes vastutab ja kontrollib kogu IT poolt, siis tuleb teha talle kindlasti väga põhjalik taustauuring ning veenduda, et tegemist on ka isikuomadustelt sobiva inimesega, keda võib tõesti usaldada. Mitme inimese või usaldusväärse teenuspartneri korral on see probleem palju väiksem, kuna sel juhul on kontrollimise võimalus suurem. Lisaks peab ühe IT inimese korral olema ettevõtte juhtkonna poolt suurem kontroll tema tegemiste üle. Räägime artiklis hiljem, mida tasuks täpsemalt nõuda.

4. IT admin nuhib firma saladusi ning lekitab neid konkurentidele või kasutab ettevõttele nõudmiste esitamiseks:

IT administraatorid kontrollivad süsteeme, võrke ning ka andmebaase ja segeli on neil ligipääs kliendiinfole, pakkumistele, intellektuaalsetele varadele ja muudele tundlikele andmetele. Seda infot võivad nad lekitada näiteks konkurentidele ja saada seejuures ise kasu või minna konkurendi juurde tööle koos firma ärisaladustega. IT spetsialistid võivad sellist infot kasutada ka näiteks oma firma tarvis ning tihti võib olla seda keeruline hiljem tõestada. Kui nad ei ole näiteks nõus mingite ettevõtte projektide või tegevustega, siis võivad nad lekitada tundlikku infot ka avalikusesse või meediasse, mis omakorda võib kahjustada ettevõtte mainet.

Lahendus: Tuleb tagada see, et vaid volitatud isikutel on ligipääs tundlikule infole ning nende isikutega tuleb allkirjastada eraldi konfidentsiaalsusleping, mis kehtib ka pärast ettevõttest lahkumist. See küll otseselt ei pruugi neid takistada, kuid võib panna nad eelnevalt järele mõtlema. Lisaks tasub panustada IT administraatorite heaolusse ning tekitada olukord, kus tal puuduks vajadus sääraste tegevuste järele. Muuhulgas hõlmab see mõistlikku palka ning viisakaid töötingimusi.

5. IT administraatoriga minnakse tülli või ta vallandatakse tema jaoks mittearusaadavatel põhjustel:

Tegemist on vast ühe levinuma põhjusega, mis võib tõugata IT spetsialiste võtma ette ettevõtet kahjustavaid tegevusi. Selliste juhtumite puhul võib firma jääda näiteks ilma ligipääsust oma süsteemile, kaotada olulisi faile (näiteks kodulehe failid) ning kahjustada seeläbi oma mainet ja usaldust klientide silmis, jääda ilma potentsiaalsetest tellimustest jne.

Mida siis teha, kui asi on läinud nugade peale ja IT spetsialist on näiteks järsult vallandatud? Esimene ja kõige olulisem asi on pärast sellist olukorda tõkestada selle IT administraatori igasugune ligipääs ettevõtte võrku ja failidele (muuta paroolid, deaktiveerida/kustutada ta kasutajad jne). Lisaks peaks kogu ettevõtte jaoks olulisest infost olema varukoopiad (backups), mis võimaldavad näiteks juhul kui ettevõtte koduleht on kustutatud, taastada need failid varundus-serverist. Carnegie Melloni andmetel juhtuvad sellised asjad kõige sagedamini 10 päeva enne töötaja ametlikku viimast tööpäeva, seega tasuks selleks eelnevalt valmis olla. Aga siin juhul on kõige kindlam variant üldse üritada vältida suurte konfliktide tekkimist ja asjade nugade peale minekut.

Mida annab omalt poolt ära teha, et ennetada võimalikke probleeme seoses oma IT spetsialistidega?

Kuidas kontrollida IT spetsialisti tööd?

Anname mõned soovitused, mida saavad ettevõtted oma poolt teha, et vältida keerulisi olukordi kuidas tuleks käituda. See kehtib eriti just väiksemate ettevõtete puhul.

1. Paroolide haldus – süsteemi haldavate IT spetsialistide kõrval peaksid juhtkonnal olema samuti kõik ligipääsud ja paroolid kõigile süsteemi osadele. Neid paroole oleks soovitatav iga mõne aja tagant muuta ning juhtkond peaks olema kõigist parooli muudatustest ka teadlik. Kui juhtkonnal on peamine kontroll ja sõnaõigus juurdepääsude ja paroolide osas ning nad tunnevad oma IT süsteemi piisavalt, siis on väiksem võimalus, et neid oma süsteemist välja lukustatakse või ettevõttele läbi IT kahju tekitatakse.

2. Koheselt pärast koostöö lõppemist tuleb deaktiveerida töötajate ning ka näiteks arendajate kontod – tuleb sulgeda nende kõikvõimalikud ligipääsud süsteemile (näiteks ligipääsud andmebaasidele, võrguseadmetele, serveritele jne). Ei ole mõtet eeldada, et isik kellega koostöö on lõppenud seda ise teeks. Väiksema ettevõtte puhul ei pea juhtkond küll ise tegelema IT asjadega, kuid tasuks lasta omale need mõned olulisemad asjad selgeks teha, et vajadusel deaktiveerida kontosid või piirata juurdepääsuõigusi. Eriti, kuna sageli kulub selleks vaid mõni klikk. Õigel ajal deaktiveeritud kontod ning selge ülevaade juurdepääsudest ning nende kontrollimine on efektiivne vahend, mis ennetab suuremaid probleeme. Kui töösuhe ei lõppenud töötaja arvates õiglaselt, siis võib kättemaksu soov tekkida alles mõni aeg pärast nende valldandamist.

3. Regulaarsed raportid – Ettevõtte juhtkond toetub oma otsustes ja töös finantsandmetele ja raportitele ning sarnane olukord peaks olema ka IT poolega. Need regulaarsed raportid ja dokumendid võiks anda ülevaate võrgu juurdepääsudest (eriti olulised on kaugjuurdepääsud), lisaks ka suurematest muutustest süsteemis ja andmetes ning õigusi omavatest admin kasutajatest. Tasuks aeg ajalt teha ka koosolekuid IT administraatoritega, et omada mingitki ülevaadet firma IT süsteemidest. Kui juhtkond on piisavalt kursis oma ettevõtte olulisemate IT süsteemidega, siis on keerulisem teha seal muudatusi, mida võidakse ettevõtte vastu ära kasutada. Lisaks, kui ülemused hoiavad asjadel silma peal, siis ei hakka töötajad nii lihtsalt usaldust kuritarvitama ning tegelema valede asjadega.

4. Vali hoolega IT konsultante/partnereid – Kui väiksem firma kasutab oma IT poole paremaks korraldamiseks väliste konsultantide või teenuspartnerite abi, siis tasuks veenduda, et nad mõtlevad ikka ettevõtte huvides. Võib näiteks juhtuda,

et „IT partner“ soovitab osta erinevat riistvara või tarkvara, mida tegelikult üldse vaja pole ning pakkuda välja lahendusi pigem oma rahakoti täitmise huvidest lähtudes.

Üks viis kuidas seda vältida, on näiteks valida IT partneriteks ettevõtteid, kes on ise partnerid suurte riistvara ja tarkvara tootjatega (Microsoft, Dell jne) ja omavad vastavaid sertifikaate ning kellel on välja toodud ka ülevaade olulisematest klientidest. See tähendab, et nad mõnes mõttes vastutavad oma partnerite ees ning lisaks annavad näiteks välja toodud peamised kliendid märku nende usaldatavusest ning on võimalik täpsemalt nende kaudu saada infot antud teenuspartneri kohta.

Iteractionis oleme ka ise mitmel korral sattunud olukorda, kus meilt soovitakse pakkumist lahendusele (näiteks serverile), mis ilmselgelt ei ole mõistlik antud ettevõtte jaoks (näiteks tohutult võimas ja liiga kallis). Hiljem asja uurides on tulnud välja, et tegemist on süsteemse probleemiga kehva teenuspartneri poolt. Seega, tasuks näiteks IT partneri valikul keskenduda sellele, et leida IT ettevõte kes mõtleb firma huvides ning pakub lahendusi, mis vastavad ärivajadustele.

5. Peab olema allkirjastatud leping – Suusõnalised kokkulepped pole suuremad asjad ning kasvõi ülalpool toodud näidete põhjal peaks olema ettevõttel oma IT poliitika (ka väiksematel ettevõtetel võiks see mingis osas olemas olla). See IT poliitika tuleks allkirjastada iga IT töötajaga ning oleks selge märk sellest, et kõik on asjadest ühte moodi aru saanud. See poliitika peaks sisaldama näiteks paroolide ja juurdepääsude poolt, raporteid, teatud koosolekuid ja aruandmist – kõike seda, mis tagaks, et ka juhtkonnal oleks selgem arusaam oma süsteemidest ning parem kontroll ka IT poolel toimuva üle. Ehk siis ootused ja piirangud IT poolele. Kusjuures see ei nõua tõenäoliselt juhtkonnalt ka liigselt aega, kuid samas aitab ennetada väga suuri probleeme.

Kokkuvõtteks: kes valvab IT-administraatoreid?

Enamus IT administraatorite niinimetatud halvale teele minemise probleemidest tulenevad sellest, et nende juhtidel puuduv huvi oma IT süsteemide vastu ning IT administraatoritele antakse liiga vabad käed tegutsemisel. See kõik on ennetatav firmapoolsete selgete IT poliitikatega ja ülemuste poolse asjadel silma peal hoidmisega. Üldiselt tasub siiski lisada, et IT administraatorid on sellised inimesed firmas, kellega tasub hoida häid suhteid ning mitte lasta probleemide korral asjadel nugade peale minna. Tulemused võivad olla päris katastroofilised.

Artikkel on pärit Iteraction.ee blogist

Avafoto: (CC) Ian Allen

- Lahendused
- Turvalisus