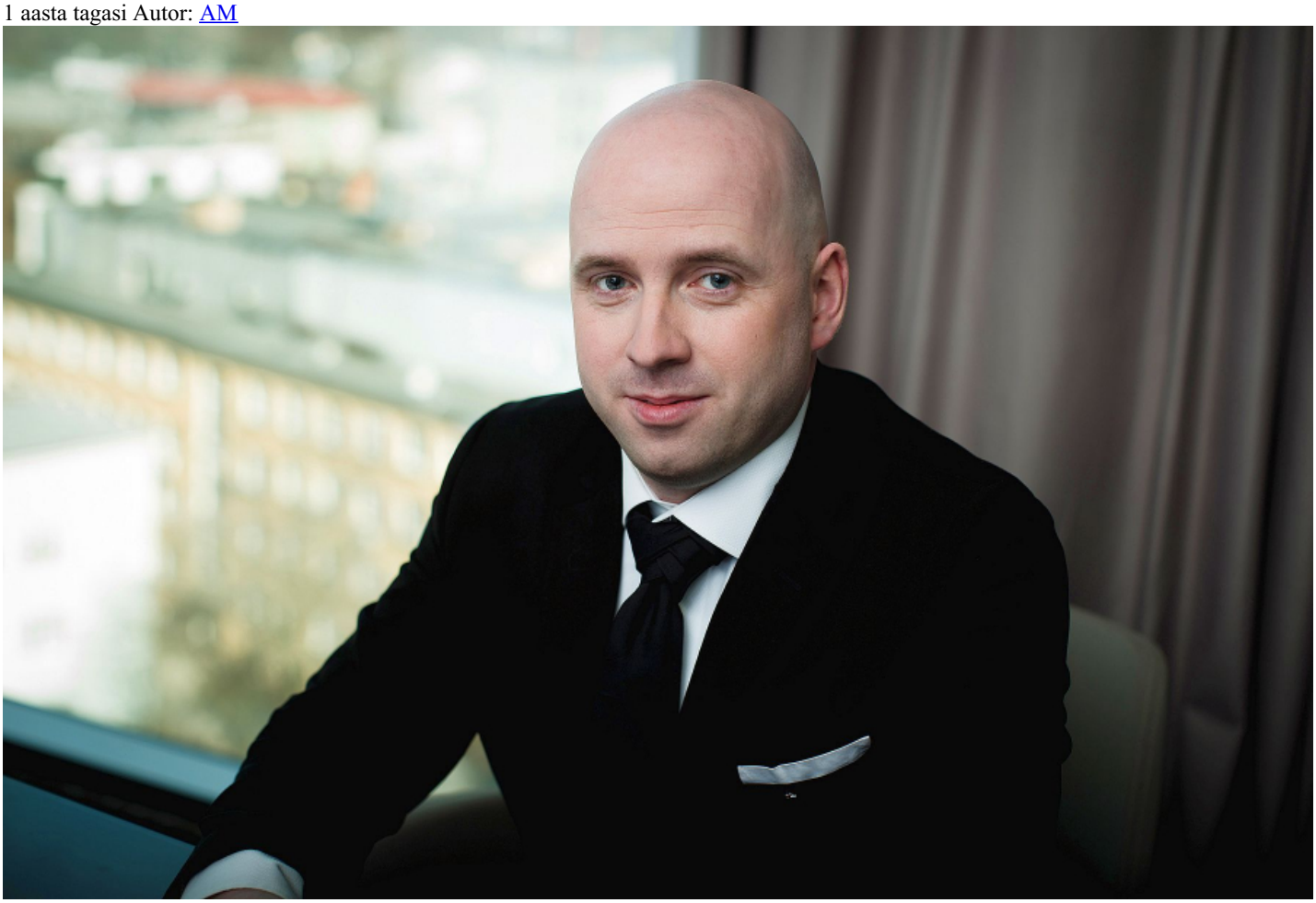
KPMG: ettevõtte ostmine nõuab eelnevat IT-auditit

1 aasta tagasi Autor: AM



Majanduses on käes heitlikud ajad, mis toovad alati kaasa ettevõtete oste ja müüke. Ühtedele annavad need hea võimaluse oma turupositsiooni parandamiseks ning teiste jaoks võib olla ettevõtte müük võimalus oma elutöö realiseerimiseks, ütleb KPMG küberturvalisuse teenuste juht Mihkel Kukk.

„Ilmselgelt ei osta keegi põrsast kotis, nii et iga ühinemise või omandamisega (M&A tehinguga) käib kaasas põhjalik finants- ja juriidiline analüüs. Siia lisandub tänapäeval üha suuremat rolli mängiv tehingueelne IT-audit, mis võtab tükkideks lahti omandatava või müüdava ettevõtte IT-lahendused ning nende haldamise küsimused," märgib Kukk.

90 protsenti ettevõtetest läbi elanud vähemalt ühe küberrünnaku

Infosüsteemide toimimine on ettevõtluses elutähtis, isegi kui on tegu „vana kooli" tüüpi tootmis- või teenindusfirmaga, kus IT-l pigem tugifunktsioon. Samas kasvõi andmeleke või klienditeenindussüsteemi rike halvavad tõsiselt ettevõtte tegevuse ning selliste olukordadega ei taha keegi kokku puutuda.

KPMG rahvusvaheliste uuringute põhjal on 90 protsenti ettevõtetest läbi elanud vähemalt ühe küberrünnaku ning 26 protsenti neist juhtumitest pani firma tegevuse ajutiselt seisma. Intsidendi mõju võib olla ettevõtte tegutsemisele väga ränk.

Kuke sõnul tuleb seega M&A tehingute korral tuleb veenduda, mis seisus on ostetava või ühineva ettevõtte IT köögipool. Täiesti möödapääsmatu on IT-audit tehingutes, kus ostetakse tehnoloogilist toodet või teenust pakkuv ettevõte. Näiteks tarkvaratoode nõuab põhjalikku testimist, et kas see ikka töötab nii, nagu väidetakse. Siia alla käib tarkvaratoote lähtekoodi analüüs, et pärast ei selguks halva üllatusena, et see on auklik nagu Šveitsi juust.

IT-lahendustele keskenduvad idufirmad testivad oma toodet pidevalt, sest neile on ettevõtte müük äriplaani sisse kirjutatud. Kindlaid protsesse järgiv tootearendus loob tugeva vundamendi hilisemale exit'ile ning lubab ettevõtte eest küsida ka kõrgemat hinda. Sellele vaatamata peab ka idufirma omandamisega kaasas käima põhjalik ostueelne analüüs.

Küberturvalisuse kontroll on kriitilise tähtsusega

Tehingupoolte IT-lahendused peavad hästi haakuma ning lisaks toimepidevuse ja turvalisuse tagamisele looma sünergiat, mis on M&A tehingute üks eesmärk. „Näiteks kui leivad ühte kappi panevad ettevõtted kasutavad erinevate tootjate, eri ajast pärit võrgulahendusi, siis nende integreerimisega kaasneb rahaline ja muu ressursikulu, mida peab arvesse võtma. Sama kehtib infoturbe vallas. Näiteks kui käibel on küberkaitse lahendused, mida viimati uuendati 4-5 aastat tagasi, siis võivad need olla lootusetult ajale jalgu jäänud," sõnab Kukk.

Infoturbesüsteemi lähem vaatlus näitab, kuidas on süsteem üles ehitatud ning kas olemasolev süsteem tagab piisava kaitse. Samuti tuleb

veenduda, kuidas käitlevad kolmandad osapooled ettevõtte infot. Ühises pilvedokumentide keskkonnas peavad juurdepääsuvolitused olema selgelt paigas, et ettevõtte võrku ei jõuaks lunavara või kutsumata külalised. Töötajate pädevus peab tagama adekvaatse käitumise küberintsidentide puhul ning IT-auditi käigus tuleb saada ülevaade protsessidest ja juhenditest, kuidas hallatakse võimalikku intsidenti organisatsiooni sees ja vajadusel koos väliste partneritega.

Kokkuvõttes aitab IT-audit müüjatel ja ostjatel mõista ettevõtte tehnoloogilist keskkonda, hinnata riske ja tagada sujuv üleminek uutele omanikele. Audit tagab, et nii müüja kui ka ostja mõistavad täielikult ettevõtte tehnoloogilist keskkonda ja tuvastavad riskid, millega tegeleda. Ostjale annavad punased lipud IT-s aluse nõuda kas nende kõrvaldamist või tingida ettevõtte hinna üle. Müüja saab korralikult sooritatud IT-auditi korral kinnituse, et pakutav kaup on aus ning üllatusi pole oodata kummalegi poolele.