primend

Küberturvalisuse põhiteenused ettevõtte riskide juhtimiseks

Üksikud turvategevused ei anna juhile kindlust, kui ei ole selge, kes vastutab, millised ohud on nähtavad, kus asuvad nõrgad kohad, kas töötajad oskavad riske märgata ning kas kriitilised andmed ja ligipääsud on vajadusel taastatavad.

Primendi IT-turvalisuse põhiteenused aitavad ettevõttel liikuda üksikutelt lahendustelt süsteemse ja juhitud küberturvalisuse poole.

5 põhiteenust, mis aitavad küberriske süsteemselt juhtida

Eesmärk on lihtne: vähendada riske enne, kui neist saavad äritegevust mõjutavad intsidendid.

1 vCISO / CISOaaS - infoturbe juhtimine ilma täiskohaga infoturbejuhita

Primendi vCISO teenus aitab luua ülevaate ettevõtte infoturbe hetkeseisust, määrata prioriteedid ja panna paika praktilise tegevusplaani. Teenus toetab juhtkonda riskide juhtimisel, audititeks valmistumisel, dokumentatsiooni korrastamisel, partneritega seotud turvanõuete täitmisel ja intsidentideks valmisoleku tagamisel.

Kasu ettevõttele: selgem vastutus, parem juhtimisülevaade ja teadlikumad otsused küberturvalisuse arendamisel.

2 Primend Shield - 24/7 automatiseeritud turbejälgimine

Primend Shield aitab jälgida IT-keskkonda ööpäevaringselt, tuvastada kahtlast tegevust ja reageerida enne, kui väikesest ohust saab suur probleem. Teenus aitab märgata näiteks ebatavalisi sisselogimisi, õngitsuskatseid, kahtlaseid kontosid, failide kopeerimist ja lunavararünnakuid. Vajadusel saab süsteem reageerida automaatselt või teavitada vastutajaid.

Kasu ettevõttele: parem nähtavus, kiirem reageerimine ja väiksem risk, et intsident jääb õigel ajal märkamata.

3 Digiturbe seire - leia nõrkused enne ründajaid

Ettevõtte IT-keskkonnas võivad turvanõrkused tekkida märkamatult: uuendamata tarkvara, valesti seadistatud süsteemid, nõrgad kaitsemeetmed või avalikult nähtavad haavatavused. Digiturbe seire aitab regulaarselt kontrollida ettevõtte sise- ja väliskeskkonda, tuvastada nõrgad kohad ning anda soovitused nende maandamiseks. Teenus sisaldab regulaarset skaneerimist, raporteid ja tulemuste tõlgendamist.

Kasu ettevõttele: parem ülevaade tehnilistest riskidest ja võimalus need varakult maandada.

4 Küberteadlikkus Primendiga - turvalisem ettevõte algab teadlikest inimestest

Paljud küberintsidendid saavad alguse inimlikust eksimusest: valest klikist, õngitsuskirjast, nõrgast paroolist või teadmatusest. Primendi küberteadlikkuse teenus aitab töötajatel ohte paremini ära tunda ja turvalisemalt käituda. Veebipõhine platvorm sisaldab lühikesi koolitusi, simuleeritud rünnakuid ja raporteerimist, mis aitab muuta teadlikkuse tõstmise järjepidevaks.

Kasu ettevõttele: töötajad muutuvad teadlikumaks ja inimliku eksimuse riskid vähenevad.

5 Varundus ja taastamine - andmed, ligipääsud ja serverid peavad olema taastatavad

Ettevõtte töö sõltub andmetest, kasutajakontodest, ligipääsudest ja ärikriitilistest süsteemidest. Ekslik kustutamine, pahatahtlik tegevus, konfiguratsioonivead või tehnilised rikked võivad kiiresti põhjustada andmekao või tööseisaku. Primend pakub erinevaid varunduslahendusi Microsoft 365 andmete, Entra ID identiteetide ja ettevõtte serverite taastamiseks.

Kasu ettevõttele: väiksem risk kaotada andmeid, ligipääse ja töövõimet.

Miks Primend?

Primend on Baltikumi IT-partner, kes ühendab Microsofti kompetentsi, igapäevase IT-halduse kogemuse ja praktilised küberturvalisuse teenused.

Meil on **12 aastat kogemust** ettevõtete IT-lahenduste toetamisel, **üle 100 spetsialisti** ja **rohkem kui 500 klienti üle Baltikumi**. Primend on juurutanud **ISO 9001 ja ISO 27001** standardid ning on Eestis pälvinud **7 aastat järjest Microsofti aasta partneri** tiitli.

Soovid teada, millised küberturvalisuse valdkonnad on teie ettevõttes juba kaetud ja millised peaksid olema järgmised sammud?

Küsi personaalset pakkumist primend.sales@primend.com