CLOUD²

Pilvipohjaisen palautumissuunnitelman laatiminen

Parhaat käytänteet, työkalut ja toimintamallit

CLOUDBACKUP SERVICES POWERED BY druva

BUSINESS AS UNUSUAL

CLOUD²
BUSINESS AS UNUSUAL

Contents

Johdanto

Nykyaikana data voidaan säilöä missäpäin maailmaa tahansa riippuen yrityksen operationaalisista tai sääntelyyn liittyvistä tarpeista. Monilla organisaatioilla ei kuitenkaan ole olemassa kattavaa datan palauttamisen suunnitelmaa luonnonkatastrofien, kiristyshaittaohjelmien tai muiden vastaavien poikkeustilanteiden varalle, vaikka data on paremmin liikuteltavissa kuin koskaan ennen.

Cybersecurity Ventures -julkaisu on arvioinut, että verkkorikollisuuden vuodessa aiheuttamat maailmanlaajuiset haitat tulevat nousemaan 6 biljoonaan dollariin vuoteen 2021 mennessä. Vielä vuonna 2015 vastaava luku oli 3 biljoonaa. Verkkorikollisuus on siis jo nyt rahallisesti äärimmäisen kannattavaa ja tulevaisuudessa sen kannattavuus ainoastaan kasvaa. Käytännössä tämä tarkoittaa sitä, että verkkohyökkäykset ovat myös yksittäisten yritysten kohdalla vain ajan kysymyksiä.

Kiristyshaittaohjelmista tai erilaisista katastrofeista selviämisen ja niiden aiheuttamista haitoista palautumisen salaisuus piilee valmistautumisessa. Enää ei riitä, että yrityksen IT-johtajat ristivät sormensa ja toivovat, että yritys ei joudu hyökkäyksen kohteeksi. Johtajien tulee olla aktiivisia ja tehdä tarkoituksenmukaisia toimenpiteitä valmistautuakseen vääjäämättömään. Nykypäivän 24/7-maailmassa selkeän ja eheän palautumissuunnitelman tulee olla keskeinen osa jokaisen yrityksen datahallinnan strategiaa.

Mitä häiriötilanteista palautuminen tarkoittaa?

Heti alkuun on hyvä tehdä selväksi, että **varmuuskopiointi ei tarkoita samaa kuin häiriötilanteista palautuminen tai palautumissuunnitelman laatiminen**. Useat varmuuskopiointiratkaisuja myyvät toimijat väittävät tarjoavansa häiriötilanteista palautumisen keinoja osana heidän ratkaisujaan. Jos nämä ratkaisut eivät ole optimoituja nopeaa yritystietojen ja sovellusten palauttamista varten, eivät ratkaisut ole riittäviä.

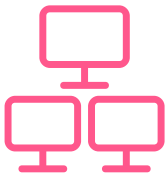
Pelkästään varmuuskopiointiin tarkoitettu sovellus saattaa kopioida tiedot ainoastaan hiljaisempina aikoina, esimerkiksi yöllä, sekä säilöä dataa vanhentunein keinoin, kuten datanauhoille lokaatioihin, joihin on hidasta päästä käsiksi. Onko yrityksellesi varaa siihen, että voi mennä viikkoja ennen kuin pääset dataan käsiksi?

Tehokas varmuuskopiointi- tai palautumisratkaisu säilöö datan useassa eri lokaatiossa.

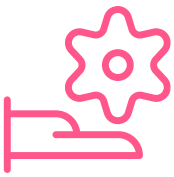
Mikä tärkeintä, yritys voi palauttaa toimintonsa nopeasti ja helposti off-premises -virtuaalikoneiden tai pilvessä toimivien sovellusten avulla. Kattavan palautumissuunnitelman avulla yritykset voivat saavuttaa tavoitellun toipumispisteen (RPO) alle 24 tunnissa sekä vain minuuttien toipumisajan (RTO) palauttaen minkä tahansa määrän dataa aina yksittäisestä tiedostosta kokonaiseen virtuaalikoneeseen.

Yleistyvät tavat palautumissuunnitelman toimeenpanoon

On-premises -infrastruktuuria on historiallisesti käytetty varmuuskopiointiin ja häiriötilanteista palautumiseen. Toteutustavan kallis hinta on kuitenkin rajannut palautumisen ainoastaan kaikkein kriittisimpiin sovelluksiin. Palautumissuunnitelmien perustuessa yhä enemmän pilven tarjoamiin palveluihin on palautumissuunnitelmien hinta pudonnut merkittävästi samalla sallien yhä useampien sovellusten mukaan ottamisen palautumissuunnitelmaan. Tehokas palautumissuunnitelma vaatii kuitenkin osakseen etäkapasiteettia, mikä tyypillisesti hyödyntää pilveä. Tehokkaan häiriötilanteista palautumisen voi järjestää eri tavoin:



Monista ensisijainen datakeskus kokonaan viimeistä kaapelia myöden. Toisen datakeskuksen hallinnointi sujuvan varajärjestelmään siirtymisen takaamiseksi on kuitenkin aikaa vievää ja kallista, etenkin virtuaalikoneympäristöjen kohdalla. Lisäksi jos varajärjestelmäksi tarkoitettu datakeskus sijaitsee lähellä ensisijaista keskusta, voi sitä vahingoittava onnettomuus vaikuttaa myös varajärjestelmän toimintaan.



Hallinnoi itsepalveluperiaatteella toimivaa palautumisjärjestelmää, joka perustuu yrityksen omistamaan tai vuokraamaan pilvessä hostattavaan infrastruktuuriin. Tämä ratkaisu mahdollistaa datan, sovellusten tai molempien palauttamisen.

Hyödynnä palveluntarjoajaa katastrofeista palautumiseen (DRaaS). Tämä muistuttaa itsepalveluperiaatteella toimivaa palautumisjärjestelmää, mutta DRaaS-tarjoaja eliminoi kaikki oman IT:n yleiskustannukset sekä infrastruktuurista aiheutuvat kulut. DRaaS-tarjoaja varmuuskopioi ja palauttaa yrityksen toiminnot pilvipalvelutarjoajan kuten AWS:n avulla.

Pilvinatiivin varmuuskopioinnin ja DRaaS:n edut

Kattava ratkaisu varmuuskopioinnin ja palautumisratkaisun yhdistämisen haasteisiin löytyy kokonaisuudesta, joka on suunniteltu pilvilähtöisesti ja joka hyödyntää julkisen pilven ominaisuuksia välittömän käytettävyyden ja pitkäaikaisen säilyvyyden muodossa. Kokonaisuus tulee olla myös optimoitu kaistan hyödyntämisen suhteen, ja sen tulee minimoida vaikutus loppukäyttäjään. Tehokas DRaaS hyödyntää teknologioita, kuten datan yleistä deduplikointia, mikä varmistaa, että kaikista tiedostoista on ainostaan yksi kopio. Tämä mahdollistaa kaistan säästämisen jopa 80 %, ja varmistaa, että myös syrjässä sijaitsevien toimipisteiden data voidaan suojata, vaikka WAN-nopeudet olisivat matalia.

Hyödyntämällä julkisia palveluntarjoajia kuten AWS:ää, yritykset pääsevät hyödyntämään kerrostettuja datan säilytysmenetelmiä, joissa data on jaoteltu kuumiin, lämpimiin ja kylmiin varastoihin riippuen säilyttämisen ja palauttamisen tarpeista. Tämä mahdollistaa datan pitkäaikaisen säilyttämisen edullisin hinnoin. Valitsemastasi pilvipohjaisesta varmistusratkaisusta olisi hyvä löytyä cache -ominaisuus, joka osaa pitää kuuman ja lämpimän tiedon esimerkiksi paikallisella virtuaalipalvelimella.

Pilvipohjaista palautumissuunnitelmaa laatiessa on huomioitava mahdollisesti heikon yhteyden päässä olevat toimipisteet ja varauduttava siihen, että puhtaasti pilvipohjaisessa varmistusratkaisuissa on oltava myös ratkaisu sille, että minkäänlaista WAN -yhteyttä ei ole.

Välttämättömät vaatimukset tehokkaaseen DRaaS:iin

- SaaS-pohjaisuus
- Pilvinatiivius
- Lähdepuolen deduplikointi
- Datan ja metadatan erottaminen toisistaan
- Yhtenäinen hallintanäkymä
- Salattu arkkitehtuuri

Tehokkaan palautumissuunnitelman laatiminen

Vaikka kattavan palautumissuunnitelman olemassaolo on elintärkeää mille tahansa nykyaikaiselle yritykselle, palautumissuunnitelman laatiminen ei välttämättä ole helppoa tai selkeää. Alla on neljä kohtaa, jotka auttavat sinua yrityksesi palautumissuunnitelman muodostamisessa:

Kohta 1: Tee Business Impact -analyysi (BIA)

Kun alat valmistella yrityksesi varmuuskopiointi- ja häiriötilanteista palautumisen ratkaisua, tulee prosessi aloittaa kattavalla ja täsmällisellä arviolla yrityksesi virtuaalisen ympäristön tilasta. Kuinka paljon dataa on tietyllä hetkellä hallittavana? Missä data sijaitsee? Kuinka kriittistä data on yritystoiminnan kannalta? Kun olet suorittanut tämän vaiheen, seuraa iso kysymys: kuinka paljon häiriö datan käsittelyssä vaikuttaisi yritystoimintaasi? Vaikutuksia tulee ajatella esimerkiksi mahdollisten uusien liiketoimintamahdollisuuksien menetyksinä tai aikana, joka kuluu tiedostojen ja tietokantojen uudelleenrakentamiseen. Tämä vaihe on prosessin kannalta keskeinen, koska se vaikuttaa kaikkiin myöhemmin prosessin aikana tekemiisi päätöksiin, esimerkiksi kuinka paljon varmuuskopiointi- ja palautumisratkaisuun tulee budjetoida resursseja. On päivänselvää, että erityisesti kannattaa panostaa yrityksellesi elintärkeän datan suojeluun.

Kohta 2: Tee riskianalyysi

Business Impact -analyysi on tärkeä työkalu, kun halutaan tarkastella yrityksen sisäisesti liiketoimintakriittistä dataa sekä mahdollisia vaikutuksia liiketoiminnalle, jos tämä data vaarantuu. Riskianalyysi taas tarkastelee mahdollisia ulkoisia tilanteita, jotka voivat vaikuttaa negatiivisesti liiketoimintaasi sekä tällaisten tilanteiden todennäköisyyttä. Tällaiset tilanteet voivat olla sekä luonnonkatastrofeja että ihmisen toiminnasta aiheutuvia tilanteita (laajat sähkökatkot, terroristihyökkäykset jne.). Riskianalyysin avulla voit hahmottaa todennäköisyyttä sille, että palautumissuunnitelma joudutaan jonain päivänä ottamaan

käytäntöön. Kun valmistaudut riskianalyysiin, varmista, että hyödynnät analyysissäsi kaikkia mahdollisia saatavilla olevia tietolähteitä uhkien ja katastrofien arvioinnissa. Tällaisia tietolähteitä ovat esimerkiksi:

- Yrityksen omat tiedot aiemmista häiriötä aiheuttaneista tapahtumista
- Yrityksen työntekijöiden muistikuvat häiriötä aiheuttaneista tapahtumista
- Paikalliset ja maanlaajuiset mediat
- Kirjastot
- Pelastuslaitosten tiedot
- Säätiedot ja -tilastot
- Yrityksen sidosryhmät
- Valtionhallinnon virastot

Kohta 3: Luo riskienhallinnan strategia

Kun olet tunnistanut virtuaalisen ympäristösi kriittiset tekijät, vaikutukset liiketoimintaasi häiriötilanteen sattuessa sekä mahdollisten katastrofien todennäköisyyden, tulee vastattavaksi kysymys: mitä voit tehdä pienentääksesi vahinkoja. Tässä vaiheessa sinun tulee valita tietty ratkaisu liiketoiminnalle kriittisen datan varmuuskopiointia ja häiriötilanteista palautumista varten. Seuraavien osa-alueiden huomioiminen auttaa sinua harkitun päätöksen tekemisessä:

- Recovery Point Objective RPO (kuinka paljon dataa yrityksellläsi on varaa kadottaa)
- Recovery Time Objective RTO (kuinka nopeasti liiketoiminnan tulee voida jatkua normaalisti)
- Datan säilöntään liittyvät lait (missä yrityksesi dataa voi lain mukaan säilyttää)
- Strategian käyttöönoton budjetti

Yllä mainitut osa-alueet auttavat sinua laskemaan ROI:n eri palveluntarjoajien tarjoamille ratkaisuille ja valitsemaan ratkaisun, joka sopii parhaiten juuri sinun yrityksesi tarpeisiin. Kuten aiemmin mainittua, julkisen pilven hyödyntäminen häiriötilanteista palautumiseen voi tarjota säästöjä kaikilla edellä mainituilla osa-alueilla.

Kohta 4: Konfiguroi ja testaa

Yrityksesi varmuuskopiointi- ja häiriötilanteista palautumisen ratkaisun tulee olla toimiva ja säädetty oikein yrityksesi tarpeisiin ennen kuin sitä joudutaan käyttämään aidossa tilanteessa. Ainoa tapa saavuttaa ratkaisun toimintavarmuus on testata järjestelmää säännöllisesti. Pilvinatiivi varmuuskopiointi- ja häiriötilanteista palautumisen järjestelmä mahdollistaa välittömän virtuaalikoneiden ylösajon testausta varten.

Varmista siis, että järjestelmäsi virtuaalikoneet toimivat odotetusti ja että data on varmuuskopioitu asettamasi RPO:n mukaan. Muista myös, että testaus ei ole kertaluontoinen asia. Sen tulee olla säännöllinen ja jatkuva osa työtäsi. Laadi siis yrityksellesi sopiva testausrytmi ja noudata sitä.

Päähuomiot

Katastrofi tulee iskemään

Kattavan häiriötilanteista palautumisen suunnitelman laatiminen on yrityksellesi yhtä tärkeää kuin varmistaa, että yrityksesi tuotantoympäristö on toimiva.

On kiistatonta, että tänä päivänä organisaatiot ovat suuremmassa vaarassa kuin koskaan menettää datansa. Huolimatta parhaista varotoimista on vain ajan kysymys, että tavara lentää tuulettimeen.

Valmistaudu

Vastaus uhkaan reagoimisessa piilee tunnollisessa valmistautumisessa ja suunnittelussa.

Yritykset, jotka ovat tunnistaneet vääjäämättömän, kohdanneet riskit ja suunnitelleet strategian riskien minimoimiseksi, tulevat olemaan paljon sietokykyisempiä ja tuottavampia organisaatioita pitkällä aikavälillä.