Identiteetin- ja pääsynhallinta tuo yrityksille kilpailuetua

INNOFACTOR

Opas identiteetin- ja pääsynhallintaan (IAM)

Identiteetin- ja pääsynhallinta on erottamaton osa 2020-luvun digitaalisessa maailmassa toimivien organisaatioiden toimintaa. Tässä oppaassa havainnollistamme konkreettisten asiakastarinoiden sekä kokeneen IT-asiantuntijan näkemysten kautta, kuinka organisaatiot voivat onnistuneiden IAM-ratkaisuiden avulla parantaa tietoturvaansa, sujuvoittaa työntekijöidensä arkea sekä säästää merkittävästi niin aikaa kuin rahaakin. Lisäksi luomme lyhyen katsauksen tuoreeseen tietoturva-alan trendejä käsittelevään tutkimukseen, jossa esitellään muun muassa kyberturvallisuusalan investointien kehitystä globaalilla tasolla.

Innostavia lukuhetkiä e-kirjamme parissa!

INNOFACTOR

Tietoturva on liiketoimintakriittistä

Tietoturvaa ei nykyisin nähdä enää pelkkänä ylimääräisenä kuluna, vaan yritykset ja organisaatiot ovat huomanneet sen tuottaman arvon. Suhtautuminen kyberhyökkäysiin on viime aikoina muuttunut yhä proaktiivisemmaksi, mutta siitä huolimatta mediassa uutisoidaan säännöllisesti hyökkäysten kohteiksi joutuneista yrityksistä ja organisaatioista, jotka ovat menettäneet kriittisen datan lisäksi myös maineensa.

Tietoturvainvestoinnit tulee osoittaa sinne, missä riskit ovat suurimmat. Identiteetin- ja pääsynhallinnan ratkaisuiden tarkoitus on suojata työntekijöiden identiteetti datan suojaamisen avulla ja siten ehkäistä tietomurtoja, joista jopa yli 80 % johtuu käyttäjän tekemästä virheestä.

Yritykset investoivat tietoturvaan voimakkaasti

Gartner Groupin vuoden 2021 CIO Agenda -selvityksessä tutkittujen yritysten tärkein investointikohde oli kyberturvallisuus. Jopa 61 % IT-johtajista kertoi suunnittelevansa lisäinvestointeja tietoturvallisuuden parantamiseksi, vaikka tietoturvan osuus kattoi jo valmiiksi suurimman osan tutkimuksessa mukana olleiden yritysten yhteenlasketusta 72,5 miljardin dollarin IT-budjetista. Gartnerin selvityksen mukaan automaatiota ja koneoppimista on viime aikoina alettu hyödyntää yhä enemmän, sillä tekoälyn avulla hyökkäyksiä voidaan ehkäistä jo etukäteen.

Parempi turvallisuus ei huononna käyttäjäkokemusta

Koronaviruspandemia heikensi yritysten ja organisaatioiden tulevaisuudennäkymiä ja kasvatti epävarmuutta. Kahden pandemiavuoden jälkeen on kuitenkin helppoa todeta, että identiteetin- ja pääsynhallintaratkaisut ovat merkittävästi helpottaneet organisaatioita siirtymään uudenlaiseen, paikkariippumattomaan työskentelykulttuuriin. Tässä uudessa maailmassa IAM-ratkaisuilla on korvaamaton rooli siinä, kuinka yritykset suojaavat datansa ja resurssinsa.

Oikein tehty IAM ei huononna käyttäjäkokemusta vaan tehostaa tuottavuutta mahdollistamalla saumattoman pääsyn laitteisiin ja yrityssovelluksiin.

Kyse ei ole pelkästään tietoturvasta

Organisaation turvallisuudesta ja riskienhallinnasta vastaaville henkilöille IAM tarjoaa mahdollisuuden tukea liiketoimintaa. Oikein toteutettu IAM-ratkaisu nimittäin parhaimmillaan kasvattaa organisaation kilpailuetua, sillä sen ansiosta työntekijät voivat työskennellä joustavasti ja turvallisesti itselleen sopivimmasta paikasta.

IAM on lisäksi keskeinen työkalu työntekijöiden ja sidosryhmien on- ja offboarding-prosesseissa, sillä se mahdollistaa sekä uusien työntekijöiden pääsyn organisaation resursseihin että lopettavien työntekijöiden pääsyoikeuden mitätöinnin ilman viivästyksiä. Identiteetin- ja pääsynhallinnan avulla voidaan myös varmistaa, että yritys tai organisaatio noudattaa henkilötietojen suojaamiseksi säädettyjä GDPR- ja Schrems II -tietosuoja-asetuksia.

Päättäjien pitää olla proaktiivisia

Proaktiivisuus ja ennakoiminen ovat nousseet yhä keskeisempään rooliin organisaatioiden kokonaisturvallisuuden suunnittelussa ja toimintakyvyn varmistamisessa. Myös Gartnerin tekemässä selvityksessä todetaan, että tietoturva- ja tietohallintojohtajien täytyy keskittyä innovaatioihin sekä suunnitella sellaisia strategioita, jotka ottavat digitaalisen murroksen tuomat haasteet huomioon.

Selvityksen toinen huomionarvoinen seikka liittyy siihen, kuinka organisaatiot voivat käytännössä parantaa tietoturvaansa. Tietomurtojen riskien vähentämisen kannalta olisi tärkeää, että jokainen työntekijä huolehtisi tietoturvasta omalta osaltaan, sillä riskien kasvaessa selkeät käytännöt helpottavat organisaation toimintaa. Kun identiteetin- ja pääsynhallinta on iskostettu syvälle organisaation toimintakulttuuriin, se on paremmin valmistautunut toimintaympäristön mahdollisiin muutoksiin.

Asiakastarinoitamme

INNOFACTOR

Identiteetin- ja pääsynhallinta pähkinänkuoressa

Identiteetin- ja pääsynhallinnan (IAM) tarkoitus on turvata organisaation data, laitteet ja työntekijät, jotta tuottava ja turvallinen työskentely olisi mahdollista ajasta ja paikasta riippumatta. IAM:n tulisi olla erottamaton osa organisaation toimintaa. Oikeanlainen lähestymistapa auttaa sopeutumaan uusin vaatimuksiin, tarpeisiin ja sääntöihin, minkä lisäksi se voi myös helpottaa sopeutumista organisaatiossa tai toimintaympäristössä tapahtuviin yllättäviin muutoksiin.

Laadukkaasti toteutettu IAM tuo sekä turvaa että paremman käyttäjäkokemuksen. Ennen käyttövaltuushallintateknologian (IGA) hankintaa ja käyttöönottoa organisaation täytyy suunnitella eri vaiheet ja käynnistää virallinen IAM-ohjelma.

Turvallinen identiteetinhallinta-ratkaisu Betonmastille

"Innofactor tuntee ympäristömme ja pystyy siksi tarjoamaan meille toimivia ratkaisuja sekä tekemään muutoksia, jotka toimivat juuri meille. Tämä säästää aikaa ja rahaa", sanoo norjalaisella Betonmastilla IT Managerina työskentelevä Øyvind Tørnblad.

Betonmast on yksi Norjan suurimmista rakennusurakoitsijoista, ja sen liiketoimintaan kuuluu monipuolisia rakennushankkeita niin yksityisellä kuin julkisella sektorilla aina suurista asuinrakennusprojekteista toimistokomplekseihin. Yrityksellä on 16 tytäryhtiötä Norjassa ja Ruotsissa, ja yhteensä sen palveluksessa työskentelee noin tuhat työntekijää. Muun muassa näiden syiden vuoksi Betonmast pitää tärkeänä, että se voi tarjota työntekijöilleen helpon pääsyn järjestelmiin riippumatta siitä, tehdäänkö töitä työmaalla, toimistolla vai jossain muualla.

"On erittäin tärkeää, että yrityksellä on mahdollisuus hallita työntekijöiden digitaalista identiteettiä sekä turvata työntekijöiden pääsy heidän tarvitsemiinsa sovelluksiin", sanoo Øyvind Tørnblad.

Keskiössä työntekijöiden käyttäjäkokemus

Innofactor on auttanut Betonmastia implementoimaan Microsoftin IAM- ja Identity Manager (MIM) -ratkaisut käyttäjien identiteettien ja pääsyoikeuksien hallinnoimiseksi. Betonmastille oli erityisen tärkeää varmistaa, että uudet ratkaisut olisivat myös niiden työntekijöiden käytettävissä, jotka eivät työskentele toimistolta käsin.

"Osa työskentelee tietokoneella, kun taas toiset saattavat käyttää ainoastaan henkilökohtaista puhelintaan työmaalla. Olemme halunneet keskittyä erityisesti työntekijöiden käyttäjäkokemukseen sekä siihen, että ratkaisu on kaikkien työntekijöidemme käytettävissä roolista riippumatta", kertoo Tørnblad.

Yhteistyö Innofactorin ratkaisukeskeisten konsulttien kanssa säästi aikaa ja rahaa.

IT-maailmassa nopeat muutokset ovat arkipäivää. Siksi Betonmast halusi varmistaa, että uudet ratkaisut ovat dynaamisia, helposti käyttöönotettavia ja toimintaympäristön muutoksiin sopeutuvia.

"Hankimme Innofactorilta projektipäällikön, jonka kanssa teemme tiivistä yhteistyötä. On suuri etu, että voimme tarpeen vaatiessa konsultoida meidän ratkaisuamme ja tavoitteitamme tuntevia Innofactorin huippuasiantuntijoita."

Yhteistyö Innofactorin kanssa mahdollistaa tarvittaessa nopeatkin muutokset:

"Henkilökohtaisesti pidän tärkeänä sitä, että pieniä muutoksia voidaan toteuttaa joustavasti. Yhteistyö ratkaisukeskeisien konsulttien kanssa säästää sekä aikaa että rahaa."

Harva ajattelee kokonaiskuvaa

Microsoft Identity Managerin ja Innofactorin toteuttamien ratkaisujen avulla Betonmast hallitsee työntekijöidensä identiteettiä useissa eri järjestelmissä saumattomasti. Tietoturvariskien kasvamisen myötä tämä on tärkeämpää kuin koskaan, sillä muiden organisaatioiden tapaan myös Betonmast käyttää monenlaisia tietojärjestelmiä.

"Identiteettien hallitseminen on välttämätöntä, sillä emme mitenkään voi kantaa riskiä siitä, että yrityksestä lähteneelle työntekijälle jäisi edelleen pääsy johonkin järjestelmäämme. Tämän vuoksi haluamme kiinnittää erityistä huomiota SaaS-sovellusten tietoturvaan ja identiteetinhallintaan. Tämä on tärkeää myös GDPR:n kannalta", toteaa Tørnblad.

Tørnbladin mukaan yritykset eivät huomioi tietoturvaa riittävän kokonaisvaltaisesti ottaessaan käyttöön uusia sovelluksia.

"On helpottava tunne, kun kaikessa toiminnassamme huomioidaan identiteetinhallinta ja tietoturva. Haluamme hallita kaikkia järjestelmiämme kokonaisvaltaisesti."

Kun Betonmastista tuli osa AF Gruppen -konsernia vuonna 2019, se sai vastuulleen koko konsernin IT-toiminnot, lisenssit, tietoturvan ja tuen. Konsernilla oli jo entuudestaan vahva tietoturvaosaaminen, mutta siitä huolimatta se päätti hyödyntää Innofactorin osaamista Microsoft Identity Managerin ja sovellusten integroimisessa.

"MIM-identiteettiportaali on nyt linkitetty suoraan AF Gruppenin käyttämiin muihin järjestelmiin, mikä tarkoittaa, että Innofactorin tekemän identiteetinhallintatyön merkitys on kasvanut entistäkin merkittävämmäksi", Tørnblad sanoo.

Tiesitkö, että

- 80 % tietomurroista liittyy identiteettiin ja käyttöoikeuksiin
- 52 % pk-yrityksien tietomurroista havaitaan sattumalta [1]
- kahdeksan kymmenestä tietomurrosta pilvi- ja datapalveluihin johtuu vuotaneista salasanoista
- kiristyshaittaohjelmat ovat yleisin ja kasvavin uhka pk-yrityksille Euroopassa [1]
- hyökkäykset ja tietomurrot käyvät yrityksille erittäin kalliiksi? (Esimerkiksi Norsk Hydro ASA:aan vuonna 2019 kohdistunut hyökkäys aiheutti yritykselle noin 70 miljoonan euron kustannukset.) [2]

1 https://norsis.no/wp-content/uploads/2021/03/NorSIS_Trusler_Trender_2021_Digital.pdf

2 https://www.aftenposten.no/verden/i/8QXzpW/de-er-blitt-mer-hensynsloese-profesjonelle-og-effektive-datakriminelle-har-funnet-seg-et-nytt-favorittmaal

Identiteettiratkaisu antoi Bjørnafjordenin kunnalle hallinnan käyttäjistä kuntaliitoksen jälkeen

Kun norjalaiskunnat Os ja Fusa yhdistyivät Bjørnafjordenin kunnaksi, syntyi tarve kokonaisvaltaiselle identiteettiratkaisulle. Innofactor auttoi ratkaisun käyttöönotossa sekä teetti tietoturvaselvityksen uuden kunnan IT-ratkaisuista.

Norjassa sijaitseva Bjørnafjordenin kunta syntyi tammikuussa 2020 Os- ja Fusa-nimisten kuntien yhdistymisen seurauksena. Uudessa kunnassa on hieman alle 25 000 asukasta ja sen palkkalistoilla noin 1 800 työtekijää.

Bjørnafjordenin kunnan IT-päällikkö **Espen Harald Haga** kertoo, että Os ja Fusa päättivät yhdistymisen jälkeen purkaa entiset palvelinkeskuksensa ja infrastruktuurinsa. Uuden kunnan IT-osastolla on nyt yhteensä 11 työntekijää.

"Fusan ja Osin IT-osastot aloittivat yhteistyön jo vuonna 2018. Viime syksynä aloimme pohtimaan, millainen IT-ratkaisu voisi parhaiten sopia uudelle Bjørnafjordenin kunnalle", Haga kertoo.

Jo alkuvaiheessa entiset kunnat tulivat siihen tulokseen, että kokonaisvaltainen identiteetin- ja pääsynhallintaratkaisu (IAM) olisi tärkeä osa kokonaisuutta.

"Aiemmin emme hallinneet käyttäjien identiteettejä tarpeeksi hyvin, mikä korostui erityisesti uusien työntekijöiden aloittaessa työsuhteensa ja vanhojen lopettaessa. Tiedot työsuhteiden loppumisesta eivät usein kantautuneet IT-osastolle, minkä vuoksi entisillä työntekijöillä saattoi olla pääsy kunnan tietojärjestelmiin. Tämä oli vakava tietoturvaongelma", Haga kertoo.

One Identity -ratkaisu helpotti uusien ja lähtevien työntekijöiden tietojen hallintaa merkittävästi. Tekemiensä havaintojen pohjalta kunnat alkoivat kartoittamaan eri IAM-ratkaisujen ominaisuuksia ja eroavaisuuksia ja päätyivät lopulta Microsoft Identity Manageriin (MIM) perustuvaan One Identity ratkaisuun. Bjørnafjorden otti uuden ratkaisun käyttöön yhdessä Innofactorin asiantuntijoiden kanssa ja siirtyi samassa yhteydessä käyttämään Exchange Onlineen perustuvaa sähköpostiratkaisua.

Identiteetinhallinta oli osa-alue, jossa meillä ei tuohon aikaan ollut asiantuntijuutta. Meillä ei myöskään ollut resursseja toteuttaa ratkaisuja itse, minkä vuoksi Identiteetinhallinta oli osa-alue, jossa meillä ei tuohon aikaan ollut asiantuntijuutta. Meillä ei myöskään ollut resursseja toteuttaa ratkaisuja itse, minkä vuoksi käännyimme Innofactorin puoleen", sanoo Haga.

MIM-ratkaisu on yhdistetty Microsoft Azure AD (Active Directory) -palveluun, jotta työntekijöiden pääsyä tiedostoympäristöihin ja muihin verkkoresursseihin voidaan hallita sen perusteella, mihin AD-ryhmään kukin työntekijä kuuluu. "Nyt meillä on huomattavasti toimivammat on- ja offboarding-prosessit, ja uusien käyttäjien tilien luominen tapahtuu automatisoidusti."

Kunnilla on usein käytössään erilaisia työtehtävissä vaadittuja, joskus vanhentuneitakin sovelluksia, jotka eivät välttämättä integroidu käytössä oleviin IAM-ratkaisuihin. Bjørnafjordeninkin IT joutuukin edelleen poistamaan lopettaneet työntekijät näistä sovelluksista manuaalisesti.

Poistoprosessia on kuitenkin Bjørnafjordenin tapauksessa parannettu niin, että nykyään lopettaneesta työntekijästä lähtee automaattinen hälytys IT-osastolle. Hälytyksen jälkeen lopettaneen työntekijän tiedot poistetaan manuaalisesti niistä sovelluksista, joita ei voi hallita keskitetysti.

Tietoturvaselvitys Innofactorilta

Norjan tietoturvaviranomainen Norwegian National Security Authority (NSM) toteaa vuoden 2021 kansallisia riskejä käsittelevässä raportissaan, että norjalaisten yritysten riski joutua kiristysohjelmien kohteeksi vuoden 2022 aikana on merkittävä. Bjørnafjordenissa kiristysohjelmiin liittyvä uhka on hyvin tiedossa, sillä moni norjalaiskunta on jo joutunut maksamaan kovan hinnan vastaavanlaisista kyberhyökkäyksistä. Myös Maailman Talousfoorumin tekemän selvityksen mukaan kyberturvallisuusjohtajat näkevät kiristyshaittaohjelmat merkittävimpänä uhkana organisaatioiden tietoturvalle. "Kiristyshaittaohjelmiin liittyvän uhkan vuoksi päätimme tukeutua Innofactorin asiantuntemukseen turvallisuuskartoituksen toteuttamisessa. Vaikka moni asia olikin jo valmiiksi kunnossa, kartoitus osoittautui erittäin hyödylliseksi. Saimme nimittäin arvokkaita vinkkejä siitä, miten voimme entisestään parantaa tietoturvavalmiuttamme", toteaa Bjørnafjordenilla IT-konsulttina työskentelevä **Tom Ruben Bratholmen**.

Bratholmen kertoo, että kunnan IT-osasto pitää jokaisena perjantaina tietoturvapäivän, jossa käydään läpi ajankohtaisia tietoturvauhkia, -haavoittuvuuksia ja -suosituksia sekä konkreettisia keinoja kyberturvallisuuden parantamiseksi.

"On tärkeää, että tietoturva huomioidaan kaiken aikaa – eikä vasta siinä vaiheessa, kun vahinko on jo ehtinyt tapahtua."

IT Manager Espen Harald Haga on erittäin tyytyväinen Innofactorin kanssa tehtyyn yhteistyöhön sekä tietoturvaselvityksen ja identiteettiratkaisun tuomiin positiivisiin vaikutuksiin.

"Mielestämme Innofactorilla on todella osaavia ja mukavia asiantuntijoita. Sillä oli meille suuri painoarvo, kun valitsimme ratkaisutoimittajaa", Haga luonnehtii.

5 syytä, miksi IAM tuo kilpailuetua

1. IAM:n avulla käyttäjät pääsevät tarvitsemiinsa resursseihin oikeaan aikaan ja oikealla perusteella.

2. IAM on välttämätön komponentti, kun halutaan taata turvallinen ja tietoturvavaatimusten mukainen pääsy resursseihin monimutkaisissa ympäristöissä.

3. Teknisen osaamisen lisäksi IAM-projekteissa suositellaan myös liiketoimintaosaamista ja -näkemystä, näin mahdollistetaan joustavampi ja tietoturvallisempi työskentely.

4. Kun organisaatiolla on käytössään modernit IAM-työkalut, identiteetinhallinta on nopeampaa ja halvempaa. Ilman IAM-työkaluja organisaatiot joutuvat tekemään automatisoitavissa olevia asioita manuaalisesti, mikä aiheuttaa lisää työtä ja siten myös piileviä kustannuksia. [1]

5. IAM-ratkaisu helpottaa liiketoiminnan laajentamista ja uusien sovellusten käyttöönottoa.

---

1 https://www.gartner.com/en/doc/738620-guide-to-initiating-and-running-an-effective-iam-program

Hyvin suunniteltu IAM voi tuoda merkittäviä säästöjä

Yritys voi ottaa enemmän riskejä nopeammin ja työntekijät voivat työskennellä parhaaksi katsomallaan tavalla. Yksi tärkeä avainsana on automaatio.

Norjassa vuodesta 2002 asti työskennellyt englantilainen **Stephen Isherwood** on tullut tunnetuksi IT-alalla IAM-osaamisestaan. Isherwood loi uraansa energiasektorilla niin pienien startupien kuin suuryritysten palveluksessa, mutta vuonna 2021 hän ilmoitti siirtyvänsä Innofactorin leipiin.

Siirron taustalla oli Isherwoodin halu auttaa asiakkaita tietoturva- ja verkkoteknologioissa sekä erityisesti IAM-ratkaisuissa.

"Oli houkuttelevaa päästä sukeltamaan vielä syvemmälle IAM:ään", hän kertoo. Isherwood uppoutui identiteetin- ja pääsynhallinnan maailmaan alun perin vuonna 2016. Hän työskenteli yrityksessä, jossa oli tuohon aikaan muutamia tuhansia työntekijöitä yli 30 toimipisteessä, aikaansa edellä olevat etätyökäytännöt sekä runsaasti käyttäjiä, joille oli annettava käyttöoikeuksia ja poistettava niitä tarpeen mukaan.

"Meille syntyi tarve kattavampaan käyttäjänhallintaan, minkä vuoksi otimme käyttöön Microsoft Identity Managerin. Hallinnoimalla käyttäjien identiteettejä saimme varmistettua, että ihmiset pystyivät työskentelemään turvallisesti olinpaikastaan riippumatta", Isherwood sanoo.

Miljardihankinta toi merkittäviä säästöjä

Ensimmäinen projekti toi suurta lisäarvoa yritykselle, kun merkittävän yritysoston myötä tuhansia käyttäjiä lisättiin nopealla aikataululla IT-ympäristöön.

"Saimme lisättyä uudet käyttäjät nopeasti omiin järjestelmiimme, sillä hallitsimme identiteettejä ja olimme jo valmiiksi integroineet ratkaisumme HR:n käyttämiin järjestelmiin. IAM:stä olikin yllättäen tullut liiketoiminnan kannalta kriittinen komponentti", Isherwood kertoo.

Oikeaoppinen IAM parantaa organisaation tietoturvaa, mikä mahdollistaa ketterän päätöksenteon ja reagoimisen muutoksiin.

"Olimme täysin valmiina etätyöskentelyyn, kun yhteiskunta sulkeutui ensimmäistä kertaa pandemian seurauksena. Aiempien IAM-investointien ansiosta saimme helposti järjestettyä tarvittavan tuen työntekijöiden kotitoimistoihin yli 30 maahan. Kaikki tämä toteutettiin alle 24 tunnissa."

Onnistumisen reseptinä olivat Microsoft Azure Active Directory, etäyhteydet, identiteetti- ja pääsynhallintaohjelmisto ja toimivat tietoturvariskejä pienentävät prosessit.

Lisäksi GDPR:n ja Schrems II:n kaltaiset uudet vaatimukset satavat Microsoftin laariin, sillä ne asettavat tiukkoja vaatimuksia IT-ympäristön sekä tallennettavan datan hallinnalle.

Tulevaisuus ilman palomuureja

Innofactorilla Isherwood työskentelee sellaisten asiakkuuksien parissa, joiden yhteinen nimittäjä on monimutkaisuus ja korkeat tietosuojavaatimukset. Hän uskoo, että Microsoftin ohjelmistot ovat jo nyt niin kehittyneitä, että muutaman vuoden kuluttua yritykset eivät välttämättä enää tarvitse palomuureja.

"Tulevaisuudessa emme tarvitse kuin päätelaitteen, käyttäjätilin ja internetyhteyden. Pääsy annetaan sitä hallitsevan ohjelmiston kautta, ja tunnistautuminen tapahtuu identiteetin perusteella."

Isherwood korostaa, että Microsoftilla on valtavien resurssiensa ansiosta parhaat edellytykset menestyä IAM-markkinoilla. Yhtiö tunnetaan tietoturvan edelläkävijänä, kyvykkyydestään ottaa käyttöön moderneja ominaisuuksia sekä ennen kaikkea asiantuntijoistaan ja analyytikoistaan.

"Microsoftin IAM-ratkaisuissa on paljon erilaisia ominaisuuksia, mikä tekee siitä mielestäni alan johtavan toimijan. Microsoftin ratkaisut pienentävät todennäköisyyttä joutua hyökkäysten tai kiristysohjelmien kohteeksi."

Tärkeää tuntea toimialan vaatimukset

Isherwood uskoo, että hyvä IAM-asiantuntija on liiketoimintalähtöinen.
"Tässä tarvitaan muutakin kuin teknologian tuntemusta. Digitalisoimme liiketoiminnan prosesseja, joten niiden ja arvoketjun ymmärtäminen on eduksi. Tämä auttaa rakentamaan työskentelytapoja tukevia ratkaisuja."

Isherwood suosittelee työvaiheiden visualisointia liiketoimintaprosessien vaiheiden kartoittamiseksi.

"On tärkeää ymmärtää asiakkaan prosessit perin pohjin. Vasta tämän jälkeen valitaan teknologia ja ominaisuudet sekä toteutetaan riskianalyysi. Näin saamme valmiudet analysoida sitä, tapahtuvatko yksittäisten käyttäjien kirjautumiset niistä paikoista, mistä oletamme niiden tapahtuvan."

Investoinnit tietoturvaan kaksinkertaistuivat

Gartnerin toukokuun 2021 ennusteen mukaan globaalit investoinnit kyberturvallisuuteen ja riskienhallintateknologioihin kasvoivat 12,4 % vuonna 2021, yhteensä 150,4 miljardiin dollariin. Kasvu selittyy pääosin lisääntyneellä etä- ja hybridityöskentelyllä sekä pilvialustojen kasvaneilla tietoturvavaatimuksilla. Identiteetin- ja pääsynhallinnan osuus kasvusta oli peräti 15,6 %.

OTA YHTEYTTÄ

INNOFACTOR