CSO

Microsoft Security

SPONSORERET INDHOLD

Sikkerhed med Nul tillid: **Erfaringer fra brugere, der allerede er godt i gang**

CSO Microsoft Security

Indholdsfortegnelse

CSO Microsoft Security

Introduktion

De sidste to års omvæltninger har rystet op i traditionelle it- og sikkerhedsmodeller. Det har betydet, at Nul tillid-sikkerhed hurtigt har udviklet sig fra at være et interessant koncept til at være grundlaget for moderne sikkerhed til virksomheder.

Ny undersøgelse fra Foundry viser, at 52 % af organisationer har forsøg med eller har installeret en Nul tillid-arkitektur, og yderligere 15 % undersøger Nul tillid-modeller. Disse brugere rapporterer talrige fordele fra deres installationer, herunder bedre beskyttelse af kundedata, mindre kompleksitet og sikker og pålidelig adgang til virksomhedsressourcer.

Denne e-bog udforsker resultaterne af Foundrys undersøgelse, der understreger vigtigheden af en Nul tillid-strategi, så CISO'er kan beskytte deres organisationer mod flere forskellige risici fra talrige angrebsvektorer. For dem, der er ved at tage første skridt på rejsen til Nul tillid, indeholder den også vejledning i, hvordan det implementere.

Om undersøgelsen

Foundry foretog en undersøgelse af amerikanske virksomheder i februar og marts 2022 for at se nærmere på, hvordan det går med brugen af Nul tillid. Respondenterne skulle være it-chef eller højere i en virksomhed med over 500 medarbejdere og spille en rolle i forhold til køb af produkter og tjenester til cybersikkerhed.

Der var i alt 250 respondenter i undersøgelsen, der var på 23 spørgsmål.

CSO Microsoft Security

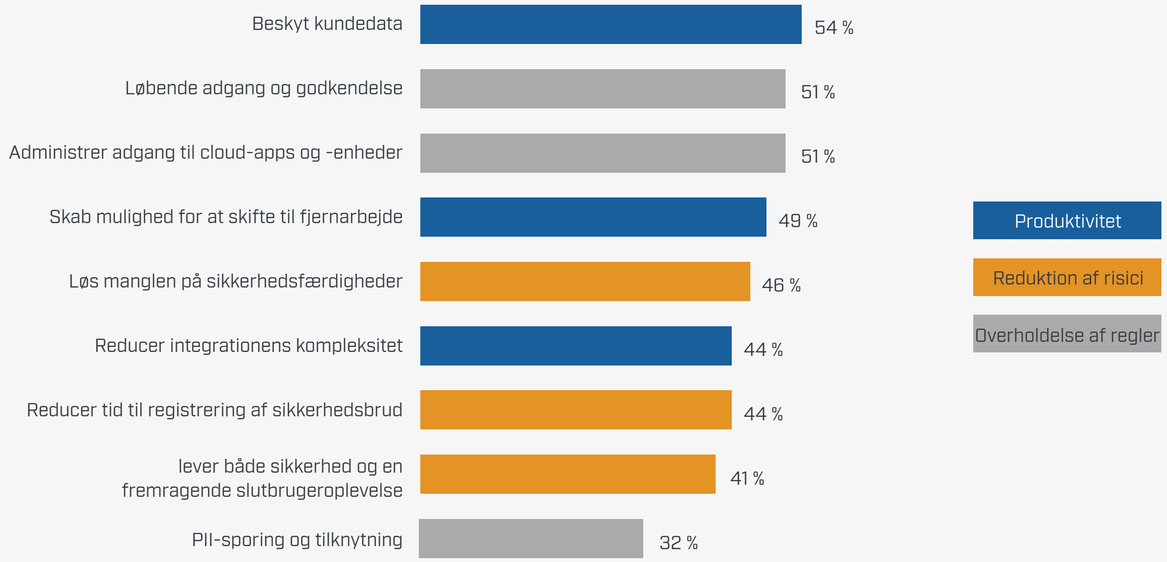
Nul tillid er landet, og det skaber værdi

Undersøgelsens resultater sammen med dybdegående interviews med it- og sikkerhedschefer viser tydeligt, at Nul tillid har en høj prioritet i de fleste organisationer. Og dem, der har installeret forskellige Nul tillid-komponenter, oplever allerede fordelene.

De fleste respondenter, der har implementeret Nul tillid (87 %), siger, at arkitekturen lever op til eller overgår deres oprindelige mål for implementering, brug og integration.

"[Nul tillid] er blevet en standardfremgangsmåde i driften for os. Jeg kan ikke se, at vi nogensinde skulle gå tilbage til der, hvor vi var før", siger en it-direktør fra en global detailvirksomhed. (Respondenter kunne give svar i anonymiseret form mod til gengæld at tale frit om deres sikkerhedsplaner.)

Opnåede fordele efter implementering af Nul tillid



12 % af respondenter sagde, at de opnår *alle* disse fordele

Kilde: Zero Trust Adoption Survey, marts 2022, Foundry. Datagrundlag: 250

CSO Microsoft Security

Ca. 44 % af respondenterne rapporterede også, at Nul tillid havde reduceret den kompleksitet, der følger med implementeringen af en integreret sikkerhedsarkitektur. "Fordi du forholder dig til og arbejder inden for et framework, bliver tingene mindre komplicerede", siger CISO'en for en callcentervirksomhed med 3.500 medarbejdere.

En VP og CISO, der arbejder for en virksomhed inden for finansielle tjenesteydelser med 17.000 medarbejdere, siger, at den multifaktorgodkendelse, som hans virksomhed implementerede som del af Nul tillid, er blevet populær blandt medarbejderne. "Det har faktisk givet større medarbejdertilfredshed, fordi de nu ikke behøver arbejde på virksomhedens udleverede maskine og bruge en VPN-klient. De kan få adgang til ressourcerne overalt", siger han.

Konceptet med minimumsrettigheder for brugere har ligeledes givet været en fordel, bemærker CISO'en. "Vi har haft færre katastrofale fejl af systemadministratorer på grund af implementeringen af systemet med adgang med mimimumsrettigheder", siger han. "De får deres rettigheder til bestemte ting og inden for bestemme tidsrammer, hvilket betyder, at der er mindre risiko for, at de begår en fejl."

På grund af den øgede udbredelse af phishing og andre cyberangreb opsummerer it-direktøren i detailvirksomheden fordelene ved Nul tillid på denne måde: "Hvis vi ikke havde disse typer værktøjer, ville vi sandsynligvis være i en dårlig situation og være nødt til at betale nogen i Bitcoin lige nu."

CSO Microsoft Security

Drivkræfterne bag Nul tillid-installation

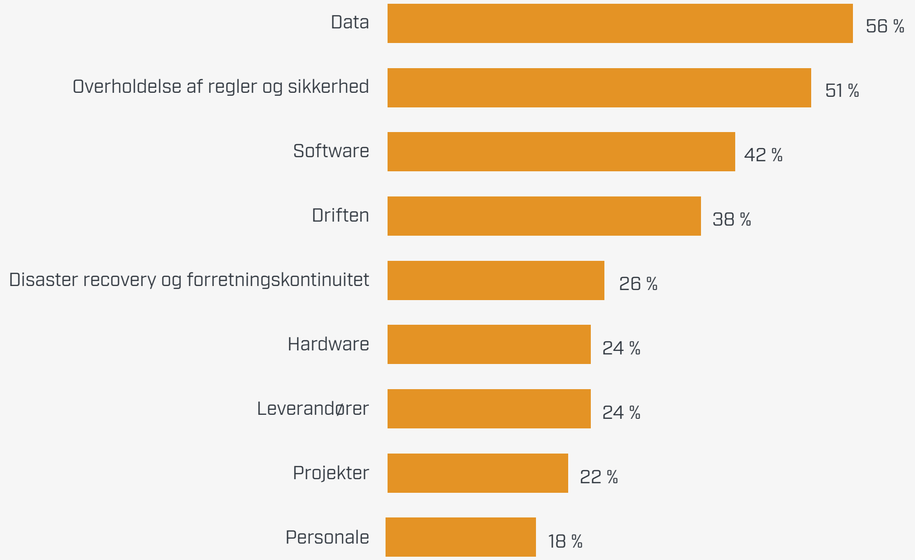
Et sammenfald af begivenheder får virksomheder til som minimum at overveje en Nul tillid-arkitektur. Behovet for at håndtere de risici, som en række ressourcer udsættes for, står øverst på listen. Undersøgelsens respondenter begrundede et års sikkerhedshændelser med en række forskellige årsager, hvor de vigtigste var sikkerhedssårbarheder fra tredjepartspersoner eller -organisationer. Andre årsager omfattede:

- Uventede forretningsrisici
- Forkert konfiguration af tjenester eller systemer
- Ondsindede angreb fra insidere
- Ikke-ondsindede brugerfejl, herunder phishingofre
- Kompromitterede identiteter
- Software uden rettelser
- Stjålne legitimationsoplysninger

Disse hændelser udgør en række forskellige risici med data som det vigtigste.

For mange organisationer har det pludselige skift til fjernarbejde, der blev foranlediget af pandemien, sat skub i planerne om brug af Nul tillid, da traditionelle perimeterbaserede sikkerhedsmodeller blev forældede. Mange organisationer var allerede på vej i den retning, da de flyttede flere applikationer og it-infrastruktur til cloud-løsningen, men pandemien gav et ekstra skub.

De vigtigste kategorier i risikogruppen for trusler mod cybersikkerhed



Kilde: Zero Trust Adoption Survey, marts 2022, Foundry. Datagrundlag: 250

CSO Microsoft Security

CISO'en i en virksomhed inden for medicinsk teknologi med 1.700 medarbejdere sagde f.eks., at cloud-løsningen og pandemien blev de motiverende faktorer for hans brug af Nul tillid, og det giver nu et sikkert fundament, hvad endmodellen for arbejdspladsen måtte være.

"Den forretningsmæssige motivation var den kendsgerning, at vi er en cloud-baseret virksomheder og er nødt til at kunne beskytte vores miljø", siger han. "Vi var også nødt til at have en funktionsdygtig ekstern arbejdsstyrke under pandemien.". [Nul tillid] har gjort, at vi har været i stand til at reducere vores behov for arbejdsplads, og vi vil formentlig forblive med som minimum at drive 60 % af virksomheden virtuelt med fjernadgang."

CSO Microsoft Security

Ingen mangel på trusler

Behov for overholdelse af regler skabte også motivation for mere robuste sikkerhedsmodeller. "Tilsynsmyndighederne holder øje med os, og de forventer, at vi fortsat forbedrer vores sikkerhedsstruktur", siger SVP for global informationssikkerhed i en virksomhed inden for finansielle tjenesteydelser med 290.000 medarbejdere.

Nogle organisationer har proaktivt valgt at se på Nul tillid for at undgå, at et højtprofileret sikkerhedsbrud retter fokus mod dem af de forkerte årsager. "Det handler om at være proaktiv og forsøge ikke at blive en del af nyhedsstrømmen", sagde CIO'en på en institution til videregående uddannelse med 3.500 medarbejdere. "Der er nogle virkelige skrækhistorier om andre institutioner af omtrent vores størrelse, der var nede i lang tid."

Andre har allerede oplevet en alvorlig cybersikkerhedshændelse, hvilket har fået dem til hurtigt at se nærmere på deres sikkerhedsstrategi. Efter at et forsikringsselskab med 6.000 medarbejdere kom ud for et ransomwareangreb, der lukkede virksomhedens netværk ned i to uger, kom mandatet til at tage Nul tillid i brug direkte fra CEO'en. "Vi satte turbo på implementeringen", siger virksomhedens VP of IT development. "Det var helt afgjort bedste praksisser i begyndelsen, og derefter accelererede det kraftigt efter vores ransomwareangreb."

En cloudbaseret katalysator

VP'en og CISO for en større virksomhed inden for finansielle ydelser siger, at hans team indså behovet for en ny sikkerhedsarkitektur for flere år siden, da den begyndte at benytte flere cloud-baserede ressourcer, og brugerne blev mere mobile.

"Vi indså, at den traditionelle sikkerhedsstruktur, hvor vi i overført betydning beskytter os med en ydre mur, som vi havde benyttet tidligere, ikke ville kunne beskytte os mod angribere fremadrettet", siger han.

Den realitet blev mere end tydelig i starten af 2020, hvor virksomheden opdagede, at det på et tidspunkt i det forgangne år var lykkedes for en angriber at trænge igennem dens forsvar af de ydre grænser og have bevæget sig på tværs i miljøet uden at blive opdaget. "Vi havde brug for en ny arkitektur, hvor vi kunne beskytte og godkende brugen af disse ressourcer, uanset hvor de måtte befinde sig, og Nul tillid er en arkitektur, der er designet med netop det formål for øje."

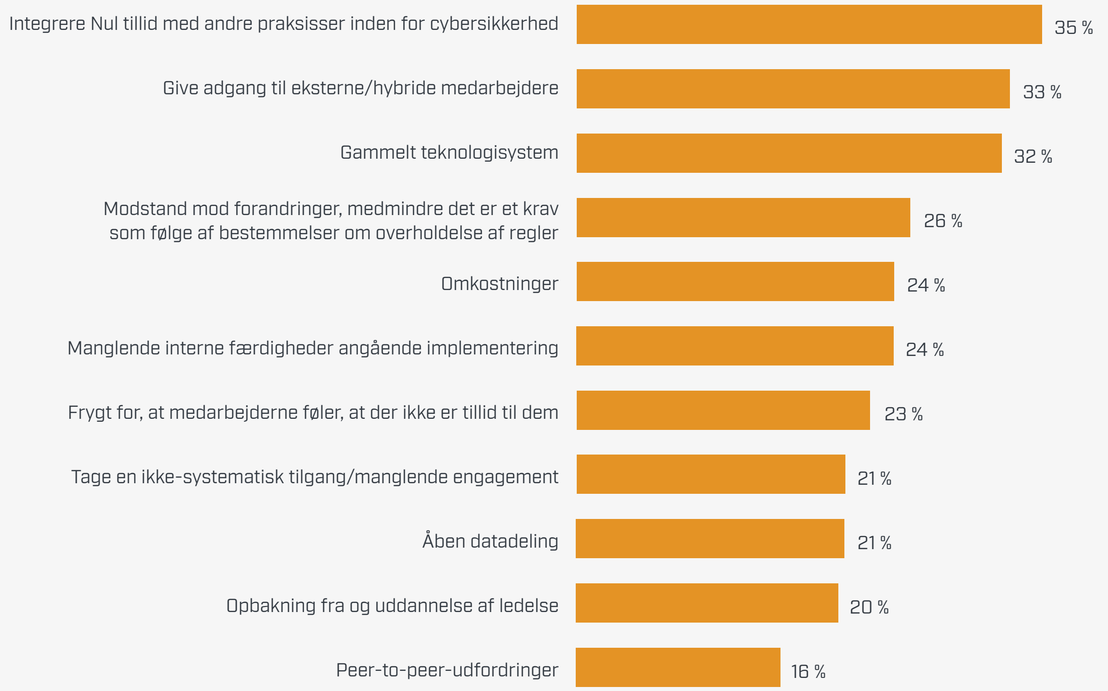
CSO Microsoft Security

Forhindringer i forhold til brug af Nul tillid

For mange organisationer udgør Nul tillid et grundlæggende skift i sikkerhedsstrukturen, -processen og mindsettet, hvilket forklarer nogle af de forhindringer, de skal overkomme for at tage det i brug.

"Der var så mange forskellige siloer, som vi begyndte at støde på i organisationen", bemærkede callcentrets CISO, og forklarede, at server-, netværks- og databaseteams hver især havde deres egen samling af webservere og -værktøjer. "Det låste virkelig situationen fast, fordi alle have en forskellig ide om, hvad det skulle gøres, og hvordan det skulle ske."

Hvad afholder dig fra at bruge Nul tillid?



Kilde: Zero Trust Adoption Survey, marts 2022, Foundry. Datagrundlag: 250

CSO Microsoft Security

Det kan faktisk være en positiv sidegevinst ved Nul tillid, at sådanne problemer kommer frem i dagens lys, ifølge Anthony Mocny, Senior Product Marketing Manager for Nul tillid hos Microsoft. "Som en arkitektur er Nul tillid designet til at nedbryde siloer for sikkerhedsteams, der skal operere inden for teknologiske søjler, og det hjælper teams med at arbejde sammen på en sammenhængende måde", siger han. "Det kan også betyde en kulturel ændring i forhold til den måde, teams, arbejder sammen på."

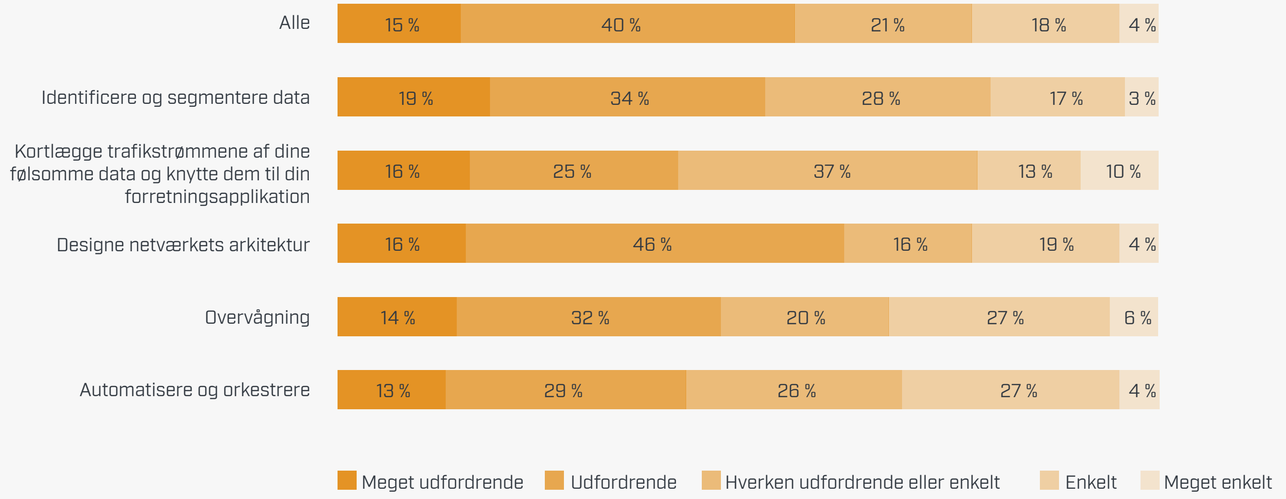
For VP/CISO'en fra finansielle tjenesteydelser blev gamle applikationer en forhindring, der skulle overkommes på vejen til Nul tillid. "De er blevet eftertilpasset med moderne godkendelsesteknologi", siger han. "Afhængigt af, hvor gamle de, er det måske ikke ret nemt at gøre."

CSO Microsoft Security

Installationsudfordringer

Når virksomheder starter på rejsen mod Nul tillid, kan der også dukke en række implementeringsudfordringer op. Mere end halvdelen af undersøgelsens respondenter (56 %) anerkendte, at implementering af Nul tillid var udfordrende eller meget udfordrende. I særdeleshed:

Hvor stor en udfordring er implementering af Nul tillid?



Kilde: Zero Trust Adoption Survey, marts 2022, Foundry. Datagrundlag: 168

CSO Microsoft Security

Udfordringer i forhold til segmentering og mikrosegmentering dukkede tit op i de dybdegående samtaler.

"Du segmenterer dit netværk helt ned til den individuelle vært", siger VP/CISO'en for finansielle tjenesteydelser. "Det er ligesom at sætte en lille firewall mellem hver enkelt vært på det interne netværk, så du kan se al trafikken og styre den helt ned til den enkelte maskine. Det har enorme sikkerhedsmæssige fordele, men det er supersvært at implementere, fordi du dybest er nødt til at administrere titusindvis af firewalls."

Kortlægning af trafikstrømme kan være en proces, der tager flere måneder. Som CTO'en i en forlags- og medievirksomhed på 5.000 medarbejdere formulerede det efter at have defineret de vigtige data-, applikations- og netværkstjenester, de skulle beskytte, "vi kortlagde transaktionsstrømme langs netværket og forsøgte at forstå dem som grupper af oplysninger", siger han. “[Vi] segmenterede derefter dele af disse oplysninger, og hvordan de rent faktisk bevæger sig i netværket, helt ned til de enkelte pakker med oplysninger." På det tidspunkt anvendte virksomheden Nul tillid-politikker på hver enkelt type af trafikstrøm. "Vi byggede også nye funktioner oven på for at overvåge og vedligeholde vores netværk.”

På trods af udfordringerne tror mange respondenter på, at Nul tillid i sidste enden forenkler den daglige drift. Med traditionelle teknologier "tager det flere dage at foretage ændringer, fordi du er nødt til at skubbe dem ud på tværs af alle hardware- og softwarekomponenter, og det bruger vi mange ressourcer på", siger SVP'en for global informationssikkerhed i inden for finansielle tjenesteydelser. "Når vi ser på Nul tillid, så minimerer det virkelig den arkitekturmæssige kompleksitet i det lange løb og reducerer det antal medarbejdere, vi har brug for til at klare den type arbejde."

CSO Microsoft Security

Bedste praksisser for implementering af Nul tillid

I takt med at flere virksomheder implementerer en Nul tillid-arkitektur, udvikler de køreplaner og bedste praksisser, som andre kan følge. Her er fem overvejelser i forbindelse med planlægning af en installation.

Vær ikke for ambitiøs i starten

Det kan være en frygtindgydende opgave at skulle lave en køreplan for en Nul tillid-strategi, hvis du kun ser arbejdet i bredere sammenhæng, hvor det handler om at revidere politikker og beskyttelsesfunktioner på tværs af netværk, data, applikationer, identitet, endpoints og infrastruktur. "I starten handlede det om bare at se på dette kæmpe bjerg, der skulle bestiges, og vi satte spørgsmålstegn ved, om vi virkelig ville gøre det, siger CIO'en fra institutionen for videregående uddannelse. "Du er bare nødt til at tage ét skridt ad gangen."

CIO'en og dennes team var i sidste ende nødt til at vælge en tilgang, hvor de fokuserede på det økonomiske, så de prioriterede segmentering af økonomi- og lønapplikationer på et separat netværk.

Det er en fornuftig tilgang at identificere de vigtigste aktiver, der skal beskyttes, ifølge Mocny. "Vær opmærksom på årsagen til, at du overhovedet implementerer Nul tillid", siger han.

Start med multifaktor i tvivlstilfælde

Når sikkerhedsstakken skal prioriteres, anbefaler mange CISO'er og sikkerhedsleverandører, at der i første omgang fokuseres på godkendelse og anden identitetsbaseret beskyttelse. "Hvis du ikke har et udgangspunkt i tankerne, er multifikatorgodkendelse et godt sted at starte", siger Mocny. Microsoft estimerer, at multifaktorgodkendelse kan forhindre mere end 90 % af identitetsbaserede angreb.

VP/CISO'en fra virksomhed inden for finansielle tjenesteydelser er enig. "Godkendelse er et grundlæggende element i implementering af Nul tillid-arkitektur. Ingen af de andre komponenter fungerer, hvis du ikke kan validere identiteten af slutbrugeren, så vi startede der."

Derefter tacklede VP/CISO inden for finansielle tjenesteydelser netværkskomponenten, hvilket straks gav fordele, fordi det støttede eksterne medarbejdere. Teamet kiggede ikke på mikrosegmentering før senere i forløbet, fordi den ikke er synlig for virksomheden generelt set. "Når du er færdig med den, har du en væsentlig større beskyttelse, men ingen kender forskellen", siger han.

CSO Microsoft Security

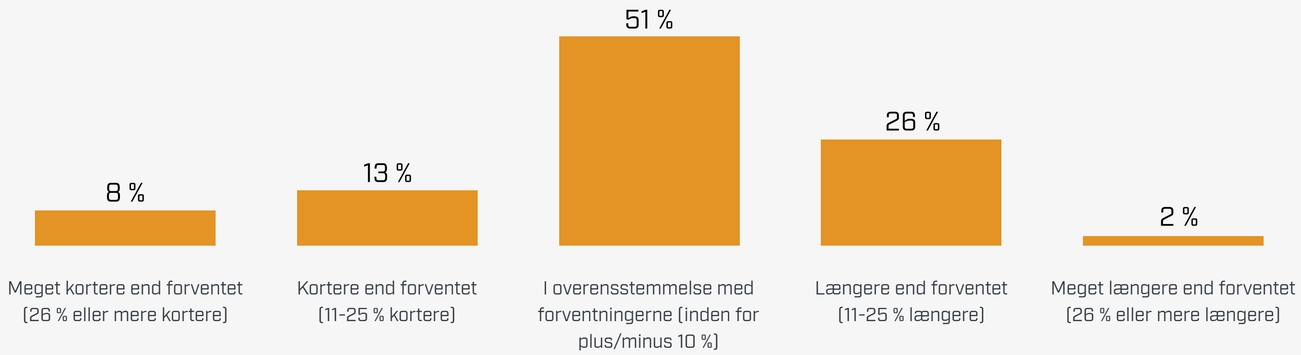
Sæt realistiske tidslinjer

Det er vigtigt, at CISO'er har realistiske forventninger omkring implementering af Nul tillid. "Implementering af en Nul tillid-arkitektur er et program og ikke et projekt", siger VP/CISO'en fra finansielle tjenesteydelser. "Det er en kæmpe stor ændring. Hvis det skal gøres rigtigt, kræver det talrige projekter, og det vil sandsynligvis vare i flere år. Der findes ikke en hurtig og nem implementering af Nul tillid-infrastrukturen."

Det giver hans SVP-kolleger ham ret i. "Jeg tror ikke, at vi nogensinde bliver færdig, fordi der kommer altid en ny teknologi til, der kommer altid ny malware til, og der kommer altid nye trusler til", siger han.

Størstedelen af undersøgelsens respondenter (72 %) siger, at deres installationstidslinjer enten fulgte tidsplanen eller var foran den, mens resten sagde, at implementeringen tog længere tid end forventet.

Overholder Nul tillid dine tidslinjemål?



Kilde: Zero Trust Adoption Survey, marts 2022, Foundry. Datagrundlag: 168

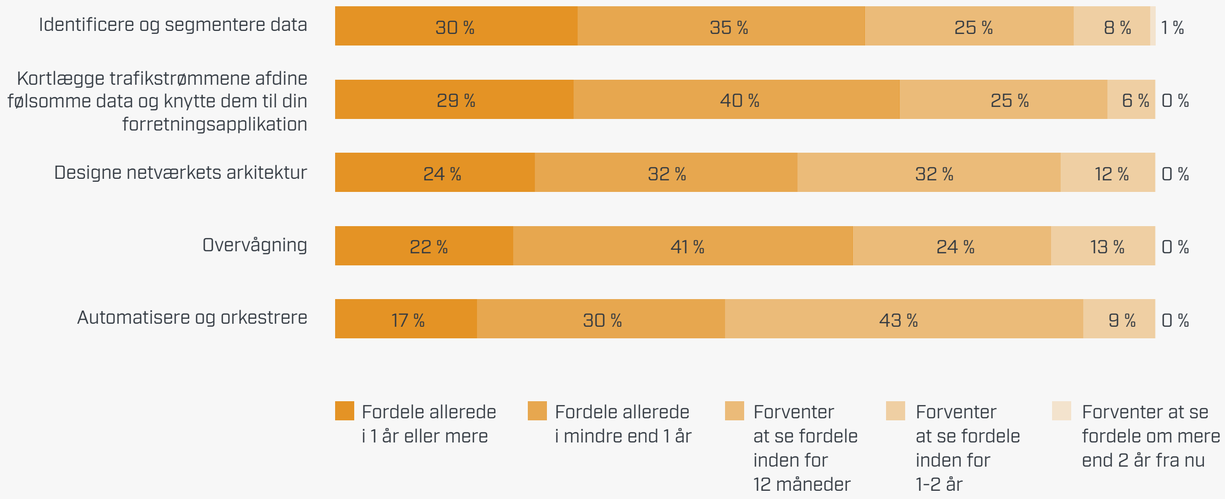
CSO Microsoft Security

Mål undervejs

Mens en Nul tillid-installation er i gang, kan og bør CISO'er opstille milepæle undervejs for at måle fremskridtet. Det er et godt tegn, at ca. 2/3 af undersøgelsens respondenter siger, at de fik fordele fra de fleste aspekter i deres projekter inden for et år, og ca. 1/4 eller mere forventer det inden for 12 måneder, og det på tværs af vigtige aktiviteter, herunder identificere og segmentere data, kortlægge trafikstrømme og designe netværkets arkitektur.

"Nul tillid er en rejse, fordi der er brug for en løbende evaluering for forsvare sig mod angrebene, hvis type ændrer sig", siger Mocny. "Vær altid på udkig efter forbedringer."

Tidslinje for at opnå fordele ved Nul tillid



Kilde: Zero Trust Adoption Survey, marts 2022, Foundry. Datagrundlag: 103

CSO Microsoft Security

Fokuser på mennesker, ikke blot teknologi

Den store rækkevidde af en Nul tillid-sikkerhedsmodel rammer alle medarbejdere, herunder it- og sikkerhedsteams, der har fået til opgave at installere den. Det er grunden til, at det er vigtigt at sikre sig, at installationer er i overensstemmelse med nye processer og praksisser for forandringsledelse, så der opnås en glat og vellykket udrulning. Det er noget, der gælder alle store teknologiprojekter.

"Ud over ændringen i teknologien er der også en ændring i kulturen", siger Mocny. "Hvis du har flere teams, der håndterer sikkerhed, herunder netværksarkitekter eller identitetseksperter, har du også brug for at ændre den måde, disse teams arbejder sammen på. Du er nødt til at nedbryde siloer for at sikre, at al teknologien fungerer på en sammenhængende måde."

Hvis disse siloer skal kunne nedbrydes, betyder det, at teams på tværs af disse discipliner skal tæt involveret i de indledende skridt og POC-projekter (proof of concept). Det var noget, en direktør for it-systemer i et teleselskab med ca. 2.000 medarbejdere lærte efter have kæmpet med flere enkelte fejlsteder under installationen, herunder tjenester, der ikke kunne godkende, og som der pludselig "ikke var tillid til", hvilket gjorde, at de samt visse systemer ikke var tilgængelige.

"Installation af én tjeneste kan have en dominoeffekt og få andre til at gå ned, siger han. Fremadrettet "vil vi være langt mere forsigtige – mere POC-tid, flere gennemgange og flere gennemgange af arkitekturen med fageksperter før installation."

Investeringsafkast på Nul tillid

En undersøgelse fra 2021, som **Forrester Consulting Total Economic Impact™** fik til opgave at udføre, kvantificerer omkostningsbesparelser og forretningsfordele for Microsoft Nul tillid-løsning. Baseret på fem virksomheder, som Forrester interviewede, realiserede en sammensat organisation et afkast på 92 % over tre år ved at implementere en Nul tillid-arkitektur med Microsoft.

Denne sammensatte organisation sparede også i gennemsnit $ 20 pr. medarbejder pr. måned ved at undgå behovet for sikkerhedsværktøjer, der bliver overflødige under Nul tillid, herunder styring af løsninger til endpoints, antivirus og antimalware.

CSO Microsoft Security

Hvor befinder du dig på vejen til Nul tillid?

Som undersøgelsen angiver, opvejer fordelene ved en Nul tillid-sikkerhedsmodel klart nogle af installationsvanskelighederne, som CISO'er og deres sikkerhedsteams står over. Hvis din organisation imødekommer disse udfordringer med en gennemtænkt plan, kan hjælpe den med hurtigt at øge beskyttelsen, reducere risici og begynde at skabe værdi i hele forretningen.

Hvis du gerne vil evaluere din organisations Nul tillid-modenhedsniveau og se flere praktiske installationsressourcer, kan du tage Microsofts **vurdering af Nul tillid-modenhedsmodellen**.