CSO

Microsoft Security

SPONSRAT MATERIAL

Säkerhet med Zero Trust: **Lärdomar från tidiga användare**

CSO Microsoft Security

Innehåll

- Inledning
- Zero Trust är en realitet och skapar värde
- Drivkrafter för att distribuera Zero Trust
- Ingen brist på hot
- Hinder för att införa Zero Trust
- Distributionens utmaningar
- Metodtips för att implementera Zero Trust
- Hur långt har du kommit med Zero Trust?

CSO Microsoft Security

Inledning

Händelserna under de två senaste åren har ställt traditionella IT- och säkerhetsmodeller på huvudet. Zero Trust-säkerhet har därför snabbt utvecklats från att vara ett intressant begrepp till att utgöra grunden för det moderna företagets säkerhet.

En ny undersökning från Foundry visar att 52 procent av organisationerna testar eller har distribuerat en Zero Trust-arkitektur, och ytterligare 15 procent tittar på Zero Trust-modeller. Dessa tidiga användare har upplevt en mängd fördelar med sina distributioner, bland annat bättre skydd av kunddata, mindre krångel samt säker och tillförlitlig åtkomst till företagets resurser.

I den här e-boken tittar på vi resultaten från Foundrys undersökning, som understryker hur viktigt det är med en Zero Trust-strategi för att informationssäkerhetschefer (CISO) ska kunna skydda sina organisationer mot en mängd olika risker och attackvektorer. Den ger också vägledning till hur du kan implementera Zero Trust för din resa mot bättre säkerhet.

Om undersökningen

Foundry undersökte amerikanska företag i februari och mars 2022 för att ta reda på hur långt de kommit med att införa Zero Trust. Respondenterna skulle vara IT-chef eller ha en högre befattning i ett företag med fler än 500 anställda och ansvara för inköp av produkter och tjänster inom cybersäkerhet.

Sammanlagt besvarade 250 personer enkäten som bestod av 23 frågor.

CSO Microsoft Security

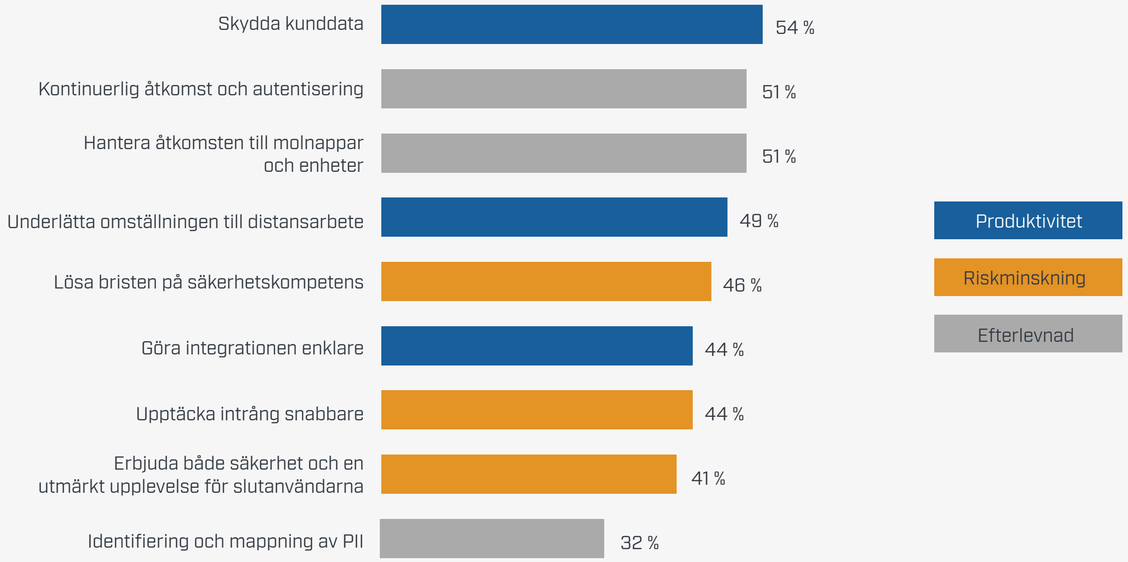
Zero Trust är en realitet och skapar värde

Utifrån undersökningens resultat, och ingående intervjuer med IT- och säkerhetschefer, är det tydligt att Zero Trust är en högt prioriterad fråga för de flesta organisationer. De som redan har distribuerat olika Zero Trust-kcomponenter har redan märkt av dessa fördelar.

De flesta respondenter som har implementerat Zero Trust (87 procent) uppger att arkitekturen motsvarar eller överträffar de ursprungliga målen med implementering, användning och integration.

”[Zero Trust] har blivit en standardrutin för oss. Jag kan inte tänka mig att vi någonsin kommer gå tillbaka till hur vi gjorde tidigare”, säger en IT-chef för en global detaljhandelskedja. (Respondenterna utlovades anonymitet i utbyte mot att kunna tala öppet om sina säkerhetsplaner.)

Upplevda fördelar efter att ha implementerat Zero Trust



12 procent av respondenterna uppgav att de uppnådde *alla* dessa fördelar

Källa: Zero Trust Adoption Survey, mars 2022, Foundry. Bas: 250

CSO Microsoft Security

Hela 44 procent av respondenterna uppgav också att Zero Trust gjorde det enklare att implementera och integrera säkerhetsarkitekturen. ”Eftersom du hanterar och arbetar med ett ramverk blir det mindre komplicerat”, säger en CISO för ett callcenterföretag med 3 500 anställda.

En CISO för ett företag inom finansiella tjänster med 17 000 anställda uppger att den flerfaktorautentisering som hans företag införde inom Zero Trust har blivit en succé bland medarbetarna. ”Medarbetarna har faktiskt blivit nöjdare, eftersom de nu inte behöver använda sina jobbdatorer och använda en VPN-klient. De har tillgång till resurserna oavsett var de arbetar”, säger han.

Begreppet åtkomst med lägsta möjliga privilegier har också gett utdelning, påverkar denna CISO. ”Vi har haft färre katastrofala fel som uppstått på grund av systemadministratörer, tack vare implementeringen av detta åtkomstsystem”, uppger han. ”De får sina privilegier för specifika uppgifter och specifika tidsramar, vilket innebär att sannolikheten för misstag minskar.”

Med tanke på de allt fler nätfiske- och andra cyberattacker summerar en IT-chef fördelarna med Zero Trust på följande sätt: ”Om vi inte hade haft dessa typer av verktyg hade vi förmodligen hamnat i en besvärlig situation där vi fått betala bitcoin till någon.”

CSO Microsoft Security

Drivkrafter för att distribuera Zero Trust

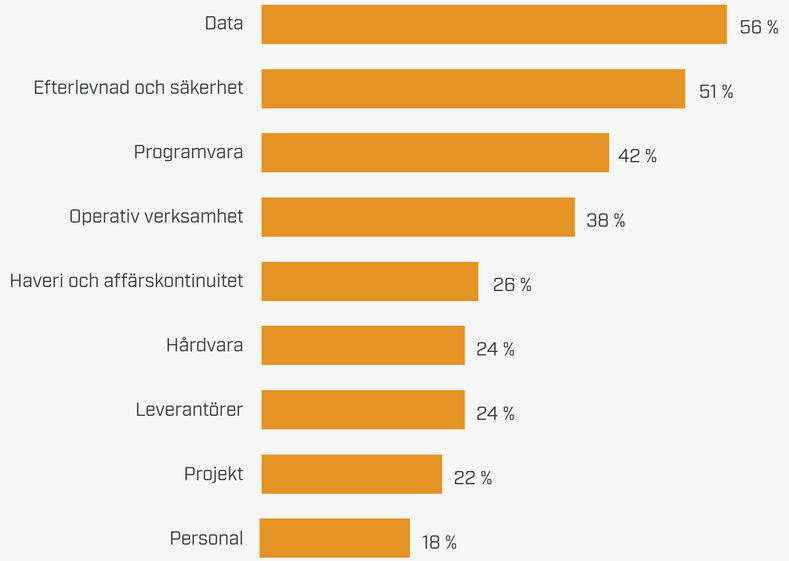
En kombination av händelser har fått företagen att åtminstone överväga en Zero Trust-arkitektur. Högst upp på listan finns behovet att hantera en mängd olika resurser som riskerar att utsättas för en mängd olika hot. Undersökningens respondenter tillskrev årets många säkerhetsincidenter ett antal orsaker, som berodde på sårbarheter hos externa individer eller organisationer. Andra orsaker var bland andra:

- Oväntade affärsrisker
- Felkonfigurerade tjänster eller system
- Skadliga, oavsiktliga insiderangrepp
- Användarfel utan uppsåt, bland annat offer för nätfiske
- Identitetsintrång
- Ej felkorrigerad programvara
- Stulna inloggningsuppgifter

Dessa incidenter utgör en mängd olika risker, som berörde data.

För många organisationer innebar den plötsliga omställningen till distansarbete, som orsakades av pandemin, att man snabbare behövde införa planer på Zero Trust, eftersom traditionella perimeterbaserade säkerhetsmodeller inte var tillräckliga. Många organisationer hade redan börjat gå i den riktningen, och flyttat alltfler appar och även IT-infrastruktur till molnet. Men pandemin gav utvecklingen en extra knuff.

Största riskkategorier för cyberhot



Källa: Zero Trust Adoption Survey, mars 2022, Foundry. Bas: 250

CSO Microsoft Security

En CISO för ett företag inom medicinteknik med 1 700 anställda uppger till exempel att pandemin utgjorde en stark drivkraft för att införa Zero Trust, vilket nu skapat en säker grund för en framtida arbetsplatsmodell.

”Drivkrafterna var det faktum att vi var en molnbaserat företag och behövde kunna skydda vår miljö”, säger han. ”Vår personal behövde också kunna arbeta på distans under pandemin. Med [Zero Trust] har vi dramatiskt kunna minska våra tillgångar, och vi kommer troligen att bli åtminstone ett till 60 procent virtuellt distansarbetande företag.”

CSO Microsoft Security

Ingen brist på hot

Behoven av regelefterlevnad har också drivit fram kraven på mer stabila säkerhetsmodeller. ”Tillsynsmyndigheterna har ögonen på oss, och de förväntar sig att vi fortsätter förbättra vårt ramverk för säkerhet”, säger en säkerhetsdirektör för global informationssäkerhet på ett företag inom finansiella tjänster med 290 000 anställda.

En del organisationer har vidtagit proaktiva åtgärder mot Zero Trust för att undvika att komma i rampljuset på grund av allvarliga intrång. ”Det handlade om att vara proaktiv och försöka undvika att hamna i medierna”, säger en informationschef på en institution för högre utbildning med 3 500 anställda. ”Det förekommer en del skräckhistorier från andra lokala institutioner av vår storlek som haft långa driftavbrott.”

Andra har redan upplevt allvarliga incidenter inom cybersäkerhet, så att de snabbt behövt omvärdera sin säkerhetsstrategi. Efter att ett försäkringsbolag med 6 000 anställda drabbats av en utpressningsattack som stängde ned företagsnätverket i två veckor, kom det en order direkt från vd:n att införa Zero Trust. ”Vi genomförde implementeringen blixtsnabbt”, säger företagets IT-utvecklingsdirektör. ”I början tillämpade vi definitivt bästa praxis, men efter utpressningsattacken tog det verkligen fart.”

En molnbaserad katalysator

En CISO för ett större företag inom finansiella tjänster uppger att hans team insåg behovet av en ny säkerhetsarkitektur för flera år sedan, då man började använda mer molnbaserade resurser och användarna blev mer mobila.

”Vi insåg att den traditionella säkerhetsarkitekturen med att bygga ett fort med vallgravar, som vi förlitat oss på tidigare, inte skulle kunna skydda oss mot framtida angrepp”, säger han.

Verkligheten blev extremt tydlig tidigt under 2020, när företaget upptäckte att en angripare någon gång under föregående år hade trängt in innanför företagets perimeter och flyttat sidled inom miljön utan att upptäckas. ”Vi behövde en ny arkitektur där vi kunde skydda och autentisera användningen av dessa resurser, oavsett var de fanns, och Zero Trust är en arkitektur som gör just detta.”

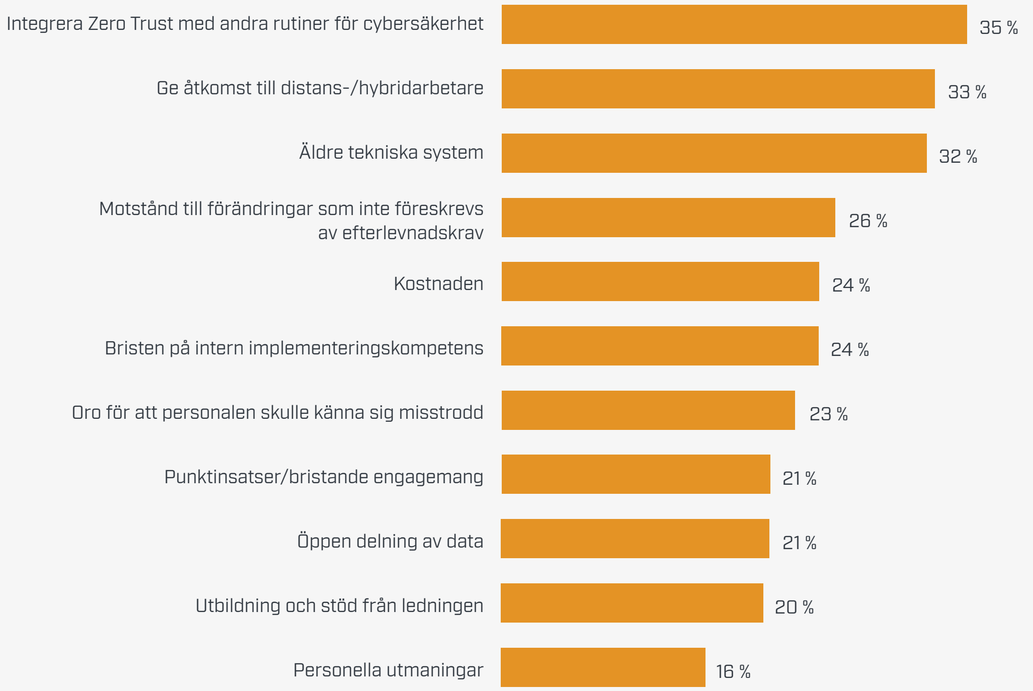
CSO Microsoft Security

Hinder för att införa Zero Trust

För många organisationer representerar Zero Trust en grundläggande omställning av säkerhetsstrukturen och -processerna samt inställningen till säkerhet – vilket förklarar en del hinder som måste övervinnas innan modellen kan införas.

”Vi hittade så många separata system i organisationen”, uppger en CISO för ett callcenter, och förklarar att de team som arbetade med servrar, nätverk och databaser hade sina egna uppsättningar webbservrar och verktyg. ”Detta innebar ett problem eftersom alla hade sin egen uppfattning om vad vi skulle göra och hur vi skulle göra det.”

Vad finns det för förhinder för att införa Zero Trust?



Källa: Zero Trust Adoption Survey, mars 2022, Foundry. Bas: 250

CSO Microsoft Security

Att identifiera sådana problem kan faktiskt ha en positiv sidoeffekt på Zero Trust, enligt Anthony Mocny, ansvarig för produktmarknadsföring av Zero Trust på Microsoft. ”Som arkitektur är Zero Trust utformat för att rasera murarna mellan de säkerhetsteam som arbetat med olika områden, och hjälpa dem att samarbeta”, säger han. ”Det innebär även en kulturell förändring, på så sätt hur teamen arbetar tillsammans.”

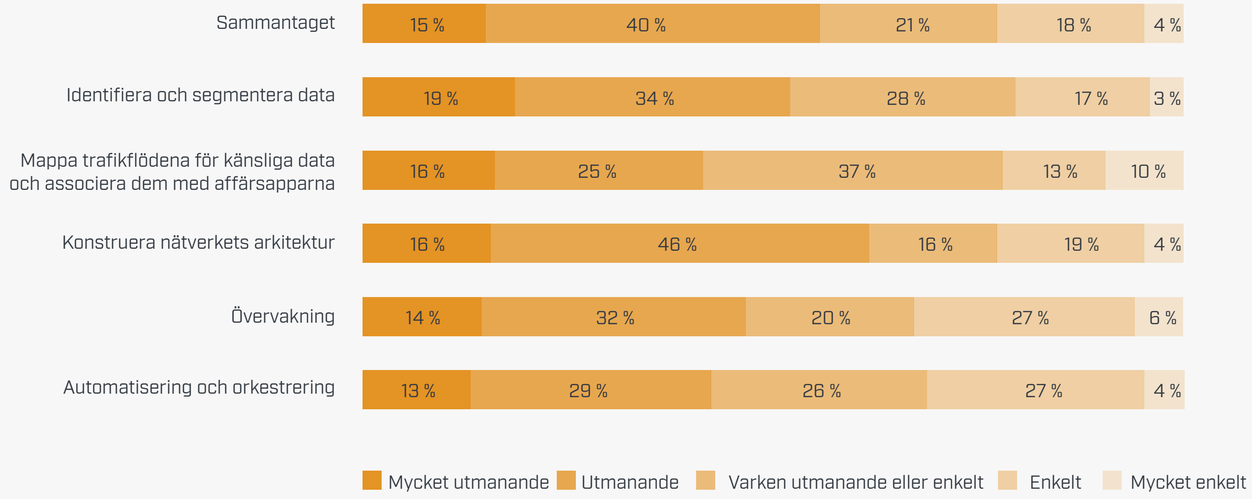
För den CISO som arbetade på företaget inom finansiella tjänster innebar äldre appar ett hinder på vägen för att kunna införa Zero Trust. ”De måste designas om med en modern autentiseringsteknik”, säger han. ”Beroende på hur gamla de var, var det inte alltid helt enkelt.”

CSO Microsoft Security

Distributionens utmaningar

När företag börjar med att implementera Zero Trust kan en del olika utmaningar uppstå. Över hälften av undersökningens respondenter (56 procent) menade att det varit utmanande eller mycket utmanande att implementera Zero Trust. Mer specifikt:

Hur utmanande är en Zero Trust-implementering?



Källa: Zero Trust Adoption Survey, mars 2022, Foundry. Bas: 168

CSO Microsoft Security

Utmaningarna med segmentering och mikrosegmentering var något som ofta togs upp under djupintervjuerna.

”Du segmenterar nätverket ända ned till den enskilda värden”, säger CISO:n för företaget inom finansiella tjänster. ”Det är som att bygga upp en liten brandvägg mellan varje enskild värd i det interna nätverke t, så att du kan se all trafik och kontrollera den ända ned till den individuella datorn. Det innebär enorma fördelar för säkerheten, men är jättesvårt att implementera eftersom du måste hantera tusentals brandväggar.”

Att mappa trafikflöden kan vara en annan process som tar flera månader att utföra. Efter att ha definierat viktiga data-, app- och nätverkstjänster som behövde skyddas ”mappade vi transaktionsflödet längs med nätverket och försöka förstå dem som grupper med information”, säger teknikdirektören på ett förlags- och medieföretag med 5 000 anställda. ”Sedan segmenterade vi delar av den informationen och hur den faktiskt traverserade nätverket, ända ned till enskilda informationspaket.” Vid den punkten tillämpade företaget Zero Trust-policyer på varje typ av trafikflöde. ”Vi tog också fram nya funktioner för att övervaka och underhålla nätverket.”

Trots dessa utmaningar anser många respondenter att Zero Trust i slutänden förenklar den dagliga driften. Med traditionell teknik “tar det dagar att göra ändringar – du måste skicka ut dem till alla hårdvaru- och programvarukomponenter, och det krävde massor av resurser”, säger direktören för global informationssäkerhet på företaget för finansiella tjänster. ”Med Zero Trust blir arkitekturen betydligt mindre komplex på lång sikt, och det krävs färre medarbetare för att utföra samma typ av arbete.”

Metodtips för att implementera Zero Trust

När många företag implementerar en Zero Trust-arkitektur utvecklar de färdplaner och metodtips som andra kan ha nytta av. Här är fem överväganden som kan vara till nytta när man planerar en distribution.

Ta inte i för mycket i början

Att staka ut en Zero Trust-strategi kan tyckas extremt utmanande om du ser detta som ett sätt att förändra policyer och skydda nätverk, data, appar, identiteter, slutpunkter och infrastruktur. ”I början verkade det vara ett oöverstigligt berg att ta sig över, och vi frågade oss själva om vi verkligen mäktade med det”, säger informationsdirektören på utbildningsinstitutionen. ”Men du måste göra det ett steg i taget.”

Informationsdirektören och hens team började tillämpa metoden ”följ pengarna”, och prioriterade segmenteringen av ekonomi- och löneappar i ett separat nätverk.

Enligt Mocny kan det vara ett bra sätt att identifiera vilka tillgångar som är viktigast att skydda. ”Fundera över varför du egentligen implementerar Zero Trust”, säger han.

Om du tvekar, börja med flerfaktorautentisering

Om man prioriterar säkerhetstacken är det många CISO:r och säkerhetsleverantörer som rekommenderar att man till en början fokuserar på autentisering och annat identitetsbaserat skydd. ”Om du inte vet var du ska börja, är flerfaktorautentisering något att titta på”, säger Mocny. Microsoft uppskattar att flerfaktorautentisering kan förhindra mer än 90 procent av de identitetsbaserade angreppen.

CISO:n på företaget inom finansiella tjänster håller med. ”Autentisering är ett grundläggande element när man implementerar en Zero Trust-arkitektur. Ingen annan komponent fungerar om du inte kan validera slutanvändarens identitet, så det var där vi började.”

Därefter tog CISO:n på företaget för finansiella tjänster sig an nätverkskomponenten, vilket direkt innebar fördelar för dem som arbetade på distans. Teamet väntade med mikrosegmenteringen eftersom företaget som helhet inte hade lika stor nytta av detta. ”När du är klar har verksamheten blivit betydligt säkrare, men ingen märker någon skillnad”, säger han.

CSO Microsoft Security

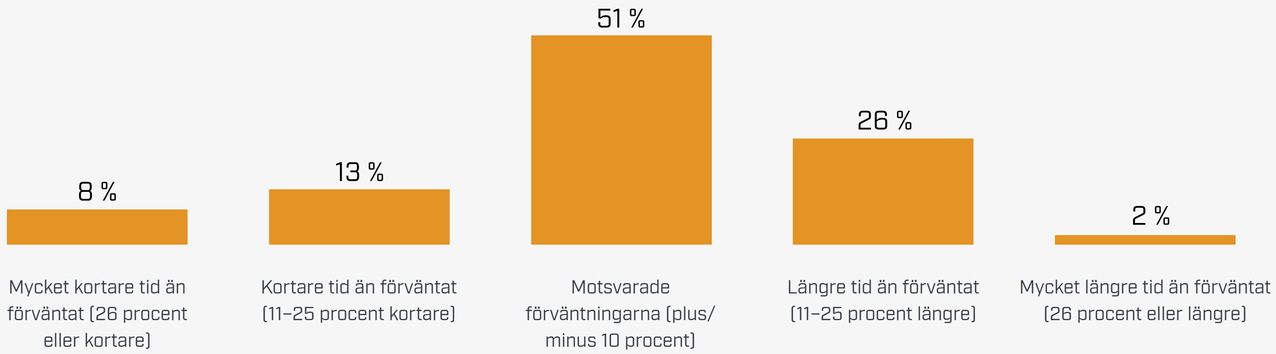
Sätt upp realistiska tidsplaner

Det är viktigt att CISO:orna sätter upp realistiska förväntningar när det gäller Zero Trust-distributioner. ”Att implementera en Zero Trust-arkitektur är ett program och inte ett projekt”, säger CISO:n på företaget för finansiella tjänster. ”Detta var en enorm förändring. För att genomföra detta på rätt sätt krävs en rad projekt, som troligen kommer pågå under flera år. Det finns inget snabbt och enkelt sätt att implementera en Zero Trust-arkitektur.”

Hans kollega ekonomidirektören håller med. ”Jag tror aldrig vi blir klara, eftersom det hela tiden kommer ny teknik, det kommer ständigt ny skadlig kod och det kommer alltid nya hot”, säger han.

Majoriteten av undersökningens respondenter (72 procent) uppger att de kunde hålla tidsplanen eller till och med ligga före den, medan resten uppgav att implementeringen tog längre tid än förväntat.

Höll ni tidsplanen för Zero Trust?



Källa: Zero Trust Adoption Survey, mars 2022, Foundry. Bas: 168

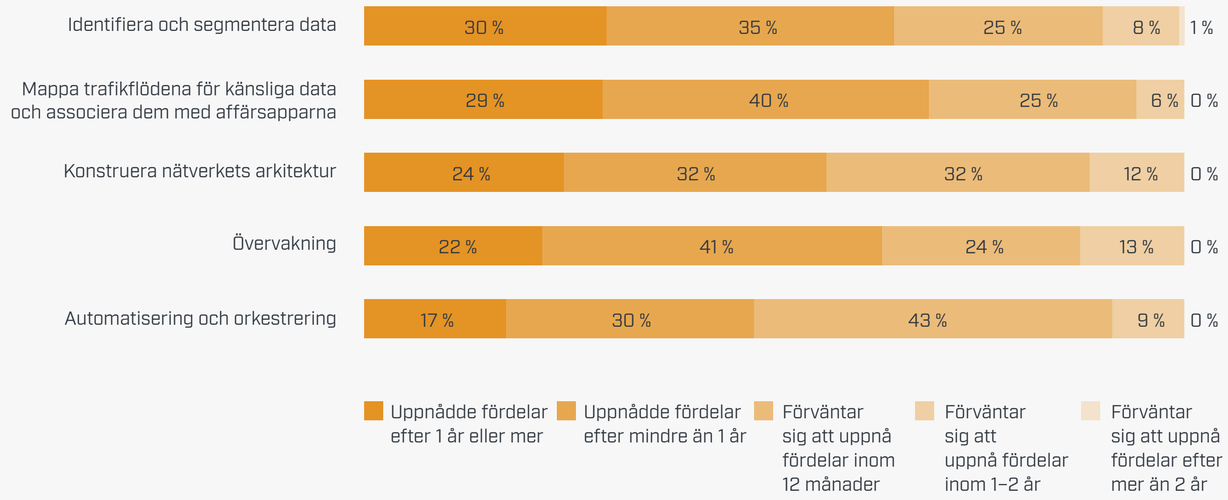
CSO Microsoft Security

Mät under arbetets gång

När en Zero Trust-distribution pågår kan och bör en CISO sätta upp milstolpar utmed vägen för att mäta hur arbetet går. Ett gott tecken är att omkring två tredjedelar av undersökningens respondenter uppgav att de uppnådde fördelar inom de flesta områden i sina projekt inom ett år, och ungefär en fjärdedel eller mer förväntade sig göra det inom 12 månader. Dessa aktiviteter omfattade bland annat områden som att identifiera och segmentera data, mappa trafikflöden och konstruera nätverksarkitekturen.

”Zero Trust är en pågående resa eftersom du hela tiden måste skydda verksamheten mot nya typer angrepp”, säger Mocny. ”Håll alltid utkik efter möjligheter till förbättringar.”

Tidslinje för att uppnå fördelar med Zero Trust



Källa: Zero Trust Adoption Survey, mars 2022, Foundry. Bas: 103

Fokusera på människor, inte bara teknik

Modellen med Zero Trust-säkerhet påverkar alla medarbetare, inklusive de IT- och säkerhetsteamen som distribuerar den. Därför är det, som vid alla större teknikprojekt, viktigt att distributionerna synkroniseras med nya processer och rutiner för förändringshantering så att utrullningen går så smidigt som möjligt.

”Det handlar inte bara om en teknisk förändring, det är även en kulturell förändring”, säger Mocny. ”Om det finns flera team som hanterar säkerheten – inklusive nätverksarkitekter och identitetsexperter – måste du också förändra hur dessa team samarbetar. Du måste riva murarna mellan dem så att all teknik fungerar på ett enhetligt sätt.”

Att riva murar innebär att få alla team inom alla områden engagerade i pilotprojekten och koncepttesten. En IT-systemdirektör på ett telekomföretag med cirka 2 000 anställda lärde sig den läxan efter att ha kämpat med flera problem under distributionen, bland annat tjänster som inte kunde autentiseras och plötslig var ”obetrodda”, så att de inte gick att använda.

”Distributionen av en tjänst kan få en dominoeffekt så att andra stängs av”, säger han. ”Vi har blivit mycket mer försiktiga – med mer tid för koncepttest, fler genomgångar och fler granskningar av arkitekturen tillsammans med ämnesexperter innan vi distribuerar“, fortsätter han.

Avkastning på investeringen i Zero Trust

I uppdragsundersökningen **Forrester Consulting Total Economic Impact™ från 2021** kvantifieras kostnadsbesparingar och affärsfördelar med Microsofts Zero Trust-lösningar. Utifrån de fem företag som Forrester intervjuade uppnådde ett sammansatt företag en treårig avkastning på investeringen på 92 procent genom att implementera en Zero Trust-arkitektur med Microsoft.

Denna sammansatta organisation sparade också i genomsnitt 20 USD per anställd och månad genom att undanröja behovet av säkerhetsverktyg som blivit överflödiga under Zero Trust, inklusive slutpunktshantering, antiviruslösningar och lösningar mot skadlig kod.

CSO Microsoft Security

Hur långt har du kommit med Zero Trust?

Så som framkommer av undersökningen uppvägs de distributionsutmaningar som CISO:er och deras team ställs inför av fördelarna som uppnås med en säkerhetsmodell som bygger på Zero Trust. Genom att hantera dessa utmaningar med en genomtänkt plan kan din organisation snabbt förbättra skyddet, minska riskerna och börja skapa värde i hela verksamheten.

Om du vill utvärdera din organisations mognadsstatus för Zero Trust och se fler praktiska distributionsresurser kan du genomföra Microsofts **modell för Zero Trust-mognadsbedömning**.