Kandidatuppsats

IT-forensik och informationssäkerhet 180hp

IT-världens Paradise Hotel – lita inte på någon!

En kvalitativ studie om Zero Trust inom svenska företag och myndigheter

Digital forensik 15 hp

Halmstad 2023-06-09

Amanda Nordgren, Johan Michel & David Boqvist

HÖGSKOLAN I HALMSTAD

En kvalitativ studie om Zero Trust inom svenska företag och myndigheter

Författare	Amanda Nordgren, Johan Michel & David Boqvist
Program	IT-forensik och informationssäkerhet
Handledare	Eric Järpe
Examinator	Urban Bilstrup
Lärosäte	Högskolan i Halmstad
Datum	2023-06-09

Sammanfattning

Det är idag viktigare än någonsin att skapa och bibehålla adekvat nätverkssäkerhet hos företag och myndigheter. När information och data flyttas ut i molnen och allt fler enheter ansluter till nätverken ökar risken för cyberattacker. Zero Trust är idag ett koncept som utgör ett steg mot en säkrare övergång från interna IT-miljöer till molnlösningar. Denna studie belyser vikten av att ha hög säkerhetsnivå med fokus på Zero Trust och mottot ”lita aldrig, verifiera alltid”.

Studien jämför svenska företags och myndigheters inställning och vilka hinder som måste överkommas för att genomföra övergången till en Zero Trust arkitektur. Studien genomfördes med hjälp av semistrukturerade intervjuer med respondenter som är representativa för en större grupp IT-experter med kunskap inom området. En mindre litteraturstudie har utförts för att koppla samman svaren från intervjuerna till befintlig forskning inom området. Studien visar på flertalet hinder som behöver tas i beaktning vid implementation såsom kostnadsfrågor, bristande kompetens och tidskrävande och uråldriga system som inte kan hantera Zero Trust på en nivå där säkerheten kan garanteras. Inställningen till Zero Trust upplevs som positiv då det kan och har applicerats på delar av nätverkens infrastruktur och är teoretiskt eftersträvansvärt i större utsträckning hos samtliga av respondenterna i studien.

Nyckelord: Zero Trust, nätverkssäkerhet, cybersäkerhet

Abstract

In today's world, network security is of utmost importance for companies and authorities as data and information are increasingly being stored and transmitted through cloud solutions. This has led to a higher risk of cyberattacks. To enhance security during this transition, Zero Trust has emerged as a promising concept, with its direction from an internal IT-environment to a more secure cloud solution. Its main motto "never trust, always verify" emphasizes the importance of a high level of security. This study aims to highlight the significance of Zero Trust and compare the attitudes of Swedish companies and authorities towards its implementation.

The study was conducted using semi-structured interviews with IT experts who possess knowledge in this domain. Additionally, a literature review was conducted to connect the outcomes of the interviews with the existing research in the field of Zero Trust. The results indicate that several barriers must be considered during the implementation phase. These include cost-related issues, lack of expertise, and outdated systems that cannot handle Zero Trust at the required security level. Despite these challenges, the respondents' attitudes towards Zero Trust were positive. They believed that it could be applied to sporadic and isolated parts of the network infrastructure, and that striving towards it at a theoretical level was essential.

Keywords: Zero Trust, network security, cybersecurity

Förord

Vi vill först och främst tacka vår handledare Eric Järpe som varit till stor hjälp under arbetets gång. Vi vill även rikta ett stort tack till respondenterna som gjorde detta arbete möjligt.

Innehållsförteckning

Figurförteckning

Tabellförteckning

1 Introduktion

Cybersäkerhet är ett fundamentalt koncept, vilket fokuserar på att säkerställa konfidentialitet, riktighet och tillgänglighet för data som överförs eller lagras på interna nätverk eller på själva Internet (Van Der Ham, 2021). Det här konceptet blir gradvis viktigare i takt med att komplexiteten mellan den fysiska dimensionen och cyberdimensionen ökar. Den ökade komplexiteten ger möjligheter för angripare att med illvilliga avsikter, dra fördel av fjärrhantering av system. Sådana attacker har blivit allt vanligare och mer sofistikerade, vilket väcker oro hos en rad olika aktörer i samhället, inklusive företag och myndigheter (Falowo, Popoola, Riep, Adewopo, & Koch, 2022).

I ljuset av detta blir cybersäkerhet ett relevant ämne eftersom samhället efterfrågar säkerhet i sin informationsstruktur för att förhindra systemsårbarheter i situationer som cyberterrorism, systemsabotage och informationskrigföring. En ökad medvetenhet om cybersäkerhet är avgörande för att garantera säkerheten i informationssystem och skydda mot potentiella hot (Furstenau, o.a., 2020).

För att hantera dessa hot är det avgörande att utveckla en strategi för cybersäkerhet som kan anpassas efter förändringar i teknologisk utveckling och hotbilder (Furstenau, o.a., 2020). Denna strategi kan innefatta ett brett spektrum av åtgärder, inklusive att säkra nätverk och datasystem, och förvalta behörigheter och använda starka autentiseringsfunktioner. I synnerhet kan företag och myndigheter dra nytta av att ta ett proaktivt tillvägagångssätt för att förhindra cyberattacker. Detta inkluderar att tillämpa bästa praxis för cybersäkerhet, genom att begränsa åtkomst till känslig information och säkerställa att all programvara är uppdaterad med de senaste säkerhetsfunktionerna (FMV, FRA, Försvarsmakten, MSB, Polisen, PTS, Säkerhetspolisen, 2020).

Nätverksinfrastrukturen som organisationer använder idag har blivit för komplex för deras eget bästa. Ett enda företag använder idag flera interna nätverk, flera fjärrkontor och/eller mobila individer samt molntjänster. Denna komplexitet av infrastruktur har överskuggat den perimeterbaserade nätverkssäkerhet som förr eftersträvades. Det har lett till att det inte finns någon lätt identifierbar omkrets på företagets nätverkssäkerhet. Det har även visat sig att om en angripare tar sig igenom omkretsen, är ytterligare sidorörelser inom nätverket obehindrad (Rose, Borchert, Mitchell, & Connelly, 2020).

Enligt statistik från SCB köpte 75% av regionerna i Sverige molntjänster år 2021. För företag med 50–249 anställda var andelen som köpte molntjänster 89%, medan den för företag med mer än 250 anställda var 94% (SCB, 2021). Den allt mer utbredda trenden att använda molntjänster som behöver

tillgång till resurser har gjort det traditionella säkerhetsparadigmet föråldrat. Detta beror på att en extern enhet, som behöver tillgång till vissa företagsresurser för att utföra en nödvändig funktion, kan utgöra en potentiell attackvektor om den beviljas generell åtkomst till alla resurser inom nätverket. Således innebär användningen av molntjänster en ökad risk för säkerhetsincidenter och kräver en mer sofistikerad säkerhetsstrategi för att skydda organisationernas nätverk (Souppaya, Symington, Scarfone, & Barker, 2022).

För att lösa säkerhetsproblemen med den klassiska nätverksarkitekturen och den ökade användningen av molntjänster har Zero Trust (ZT) utvecklats. ZT är ett koncept som baseras på en princip där alla användare och enheter ska betraktas vara obehöriga. ZT är designad för att förhindra dataintrång och hindra angripare att röra sig fritt inom nätverket. ZT metoden är främst tillämpad för att fokusera på data och tjänstskydd, men kan och är rekommenderat att tillämpas på hela företagets tillgångar som enheter, infrastrukturkomponenter samt virtuella- och molnkomponenter (Rose, Borchert, Mitchell, & Connelly, 2020).

Ett exempel på denna modernisering är presidentordern från President Biden från 2021. Målet med denne presidentorder är att förbättra landets cybersäkerhet genom att modernisera synsättet cybersäkerhet, och där regeringen måste börja anta bästa säkerhetspraxis, vilket är helt i linje med ZT:s utveckling. (Biden, 2021).

Med tanke på de framsteg som görs i de Förenta Statera inom cybersäkerhet är det intressant att undersöka ifall även företag och myndigheter i Sverige har börjat skydda sig inför framtiden, samt huruvida Sverige hänger med i den digitala utvecklingen när det gäller att skydda sig ur ett cyber- och informationssäkerhetsperspektiv.

2 Bakgrund

2.1 Klassisk nätverkssäkerhetslösning

En stor majoritet av företag och myndigheter runt om i världen inklusive Sverige, som här är huvudfokus, nyttjar idag en IT- och nätverkssäkerhetsprincip som kallas för “skalskydd”. Det är ett system som funnits med länge och på senare tid har allt fler börjat inse att det inte längre är ett tillräckligt skydd för att mäta sig mot de moderna angriparna enligt (Uctu, Alkan, Alper, & Dörterler, 2019).

Skalskyddet i fråga kan liknas vid en medeltida borg, där allt fokus har lagts vid att hindra fienden från att inta borgen. Borgen skyddas med vallgravar, bryggor, portar och höga, tjocka murar. När dessa hinder väl passerats är resterande delar oskyddade och blir därmed sårbara för de nyfikna ögonen hos inkräktare med illvilliga avsikter. För att jämföra med dagens mest använda säkerhetslösningar är vallgraven en brandvägg och portarna och murarna är antivirusprogram där allt krut har lagts på att stoppa inkräktarna innan de nått systemen. Väl inne i systemen ligger känsliga data oskyddade vilket då leder till oerhörd skada mot de företag eller myndigheter som har fått skalet penetrerat (Nace, 2020).

Nätverksstrukturen är vanligtvis indelad i interna och externa nätverk, och utrustning såsom brandväggar används för att skydda dessa nätverk genom placering runt de interna och externa nätverken. Datatrafiken som flödar i nätverken filtreras genom dessa skyddsåtgärder. Emellertid, på grund av den ökande användningen av molntjänster, har de fysiska gränserna mellan företagens interna och externa nätverk suddats ut, vilket ökar säkerhetsriskerna och minskar brandväggarnas effektivitet (Shore, Zeadally, & Keshariya, 2021). Molnservrar överför data genom offentliga nätverk, vilket utsätter servern för sårbarheter och gör det svårt att sätta en fysisk gräns mellan molnservern, företagets intranät och Internet. Som ett resultat är det omöjligt att distribuera en traditionell skyddsutrustning för nätverkssäkerhet (Rose, 2022)

2.2 Zero Trust (ZT)

Zero Trust är ett säkerhetskoncept som grundar sig i principen att ingen användare, enhet eller applikation automatiskt kan anses vara säker. Detta innebär att all trafik, oavsett om den kommer från interna eller externa nätverket, betraktas som potentiellt hotfull. Som ett resultat måste all trafik verifieras, identifieras och godkännas innan åtkomst till resurser tillåts. Genom att alltid verifiera enheter och användare och kontrollera åtkomst till nätverket går det att minska risken för oönskade intrång (Chuan, Lv, Qi, Xie, & Guo, 2020).

Detta är en betydande förändring från traditionella säkerhetsmodeller som förlitar sig på att interna nätverk är säkra och att användare på dessa nätverk går att lita på. ZT är ett säkerhetskoncept och inte en specifik programvara och därför finns det ett antal tekniska verktyg och tekniker som kan användas för att genomföra det. Exempelvis kan företag använda sig av flera tekniker såsom multifaktorautentisering, identitets- och åtkomsthantering och mikrosegmentering av nätverk. Det sistnämnda innebär att nätverket delas upp i små isolerade segment vilket bidrar till att spridningsrisken vid attacker minskar (Mehraj & Banday, 2020).

Eftersom ZT fokuserar på att förhindra obehörig åtkomst och minskar risken för dataläckage, är det ett alltmer populärt säkerhetskoncept bland organisationer. Dessutom har ZT blivit viktigare i takt med att organisationer alltmer använder molntjänster (SCB, 2021). Detta beror på att traditionella säkerhetslösningar, såsom brandväggar, inte är tillräckliga för att skydda data mot cyberhot i en miljö med molntjänster (Rose, 2022).

ZT är ett relativt nytt säkerhetstänk och många organisationer är inte fullständigt medvetna om dess egenskaper, vilket kan bidra till hinder för implementeringen av Zero Trust-lösningar (Chuan, Lv, Qi, Xie, & Guo, 2020).

2.3 Tidigare relaterade arbeten

ZT:s innovativa tillvägagångssätt för att säkra ett nätverk har lett till en våg av rapporter och konferenspapper som diskuterar ZT:s potentiella roll i framtiden och hur det kan implementeras på olika sätt. (Hosney, Halim, & Yousef, 2022) diskuterar att det höga kravet på kontroll med ZT lägger ett för stort ansvar på IT-avdelningar på företag. I stället kan detta upprätthållas med hjälp av AI som automatiserar kontrollen. En rapport från Ericsson (Olsson, Shorov, Abdelrazek, & Whitefield, 2021) föreslår att börja implementera ZT inom telekom eftersom den nuvarande lösningen inte håller måttet för att skydda nätverksresurserna. (Samaniego & Deters, 2018) resonerar att ZT bör implementeras inom Internet of Things (IoT) eftersom den nuvarande lösningen inte har den skalbarhet som IoT kräver inför framtiden. IoT är samlingsnamnet för smarta enheter vilka är uppkopplade mot internet och har förmågan att kommunicera och dela data sinsemellan för att kunna automatisera och förbättra vardagen.

En kinesisk undersökning av (He, Huang, Chen, Ni, & Ma, 2022) analyserade ZT:s kärnteknologi och dess applikation. De kom fram till att applikationen just nu är i dess första fas, vilket betyder att det inte går att förstå alla fördelar och nackdelar med lösningen än, något som i sin tur hindrar implementationen hos företagen. Detta leder till den informationslucka som denna studie har i syfte att täppa; vad som krävs från företag och myndigheter för att de ska börja implementera ZT och gå ifrån den traditionella metoden, beskriven i 2.1, som används idag.

Det finns ett arbete som riktar in sig på ZT i kombination med svenska företag. Arbetet har syftet att undersöka hur svenska företags inställning är till ZT och vilka hinder som svenska företag upplever med ZT. I arbetet görs ingen skillnad på offentlig sektor och privata företag i arbetet. Resultatet visar att svenska företag har en välvillig inställning till ZT, vilket främst beror på kraven som ställs på företagen från olika aktörer. Hindren som finns är huvudsakligen föråldrade resurser, komplexitet, tid och kostnad (Råsberg & Björkman, 2022). Eftersom den tidigare litteraturen täcker en grundlig undersökning av svenska företag och ZT, kommer detta arbete att fokusera på vidareforskning på samma ämne men med andra inriktningar.

2.4 Problemformulering

De traditionella säkerhetslösningarna som används idag anses inte längre vara tillräckliga för att skydda svenska företag och myndigheter från cyberangrepp (Försvarsmakten, 2022). Zero Trust-modellen har framträtt som en möjlig lösning för att hantera dessa hot, men hur har svenska företag och myndigheter implementerat Zero Trust-modellen, och hur har de hanterat hinder som uppkommit under processen?

2.5 Syfte och frågeställningar

Syftet med studien är att undersöka om det finns skillnader i inställningen till Zero Trust (ZT) mellan svenska myndigheter och svenska företag och hur dessa skillnader eventuellt manifesterar sig. Dessutom syftar studien till att undersöka hur svenska organisationer som redan har implementerat ZT har hanterat eventuella hinder.

För att kunna besvara syftet har följande frågeställningar valts:

- Hur skiljer sig inställningen till Zero Trust mellan svenska myndigheter och svenska företag?
- Hur har svenska organisationer som tillämpat Zero Trust lösningar gått tillväga och hur har eventuella hinder hanterats?

2.6 Problematisering

Hur skiljer sig inställningen till Zero Trust mellan svenska myndigheter och svenska företag?

Det finns ingen tydlig förståelse för hur inställningen till Zero Trust skiljer sig mellan den offentliga sektorn och privata företag. Detta är en relevant fråga eftersom skillnader i inställning kan påverka valet av säkerhetsstrategi och implementeringen av Zero Trust-modellen, samt leda till skillnader i nivån av cybersäkerhet och informationssäkerhet. Därför är det viktigt att undersöka och jämföra inställningen till Zero Trust mellan den offentliga och privata sektorn för att förstå vad som påverkar dessa skillnader.

Trots att det är en viktig fråga är det fördomsfullt att förutsätta att det faktiskt finns skillnader mellan sektorerna. Det gäller att identifiera de faktorer som är avgörande för deras inställning till Zero Trust.

Hur har svenska organisationer som tillämpat Zero Trustlösningar gått tillväga och hur har eventuella hinder hanterats?

Trots sitt fördelaktiga syfte har implementeringen av Zero Trust-modellen visat sig vara en komplex och utmanande process för företag. Denna frågeställning är relevant för att förstå utmaningarna med att implementera Zero Trust-modellen i praktiken, samt identifiera de mest effektiva strategierna för att hantera hinder och säkerställa en framgångsrik implementering. Däremot kan det vara svårt att veta vilka företag som verkligen har implementerat ZT då det inte finns en färdig ZT-modell att använda eller en metod för att mäta graden av implementering. Hindren som finns kan skilja sig markant mellan företag beroende på vilka faktorer som spelar in, som exempelvis kostnad eller kunskap.

3 Metod

Detta kapitel kommer avhandla de olika metodval som har använts för att besvara frågeställningarna. Metoderna kommer att diskuteras för att ge läsaren en tydlig bild av varför dessa metoder valts. En problematisering av metoderna kommer även att diskuteras för att förstå varför alternativa metoder inte valts.

3.1 Val av metod

Med anledning av studiens syfte och frågeställningar valdes en kvalitativ metod. En kvalitativ metod har som syfte att besvara frågan varför ett visst fenomen är, eller inte är, på ett visst sätt. Metoden kan även beskrivas som ”ord hellre än siffror” (Busetto, Wick, & Gumbinger, 2020).

(Creswell & Creswell, 2018) förklarar ytterligare att en kvalitativ metod är lämpligast då området som undersökes är relativt nytt och att det lämnar mer utrymme åt forskaren att vara innovativ och mer kreativ. Detta bidrar till att frågorna som ställs är mer öppna vilket ger möjligheten att av svaren förstå vilka underliggande faktorer som medverkar till ett specifikt problem.

En kvalitativ metod är passande till studien eftersom Zero Trust innebär en förändring i organisationers struktur, processer och tekniska system, vilket kan vara svårt att mäta kvantitativt. De kvalitativa metoder som valts fokuserar på att förstå och beskriva uppfattningar, attityder och erfarenheter från deltagarna, vilket ger en djupgående förståelse kopplat till implementation av Zero Trust och dess effekt på organisationen. Det är också en lämplig metod för att undersöka de faktorer som kan påverka framgången eller misslyckandet av Zero Trust implementeringar, inklusive organisatoriska hinder och tekniska utmaningar.

3.2 Litteraturstudie

En systematisk litteraturstudie är en forskningsprocess som är transparent och möjliggör framtida replikerbarhet, där syftet är att samla in den bästa möjliga kunskapen inom ett visst område för att besvara en eller flera frågeställningar. Det är viktigt att ha ett kritiskt förhållningssätt under processen, både kring litteraturen och forskarens tolkning av den (Lewis-Beck, Bryman, & Liao Futing, 2004).

För att kunna besvara frågeställningarna “*hur skiljer sig inställningen till Zero Trust mellan svenska myndigheter och svenska företag?*” samt “*hur har svenska organisationer som har tillämpat Zero Trustlösningar gått till väga och hur har eventuella hinder hanterats?*” behövde först information samlas in för att få större kunskap kring ämnet Zero Trust. För att datainsamlingen skulle vara relevant för studiens syfte genomfördes en litteratursökning.

Först fastställdes de kriterier som skulle tillämpas för att avgöra vilken litteratur som skulle inkluderas i studien, vilka redovisas i avsnitt 3.3. Därefter gjordes en bestämning av vilka relevanta vetenskapliga databaser som skulle användas för att genomföra systematiska sökningar. Google Scholar ansågs vara mest relevant. Det är en sökmotor för bland annat tidskrifter som är peer-reviewed, artiklar, uppsatser och böcker inom den vetenskapliga världen, vilken ansågs vara mest passande till studien. För att identifiera lämpliga källor användes primärt följande söktermer: *Zero Trust, Zero Trust implementation, cyberattacks, cloud computing* och *network architecture.* Efter att den relevanta litteraturen valts ut, organiserades den i en tabell för att få en överskådlighet och en kvalitetsbedömning utfördes av den inkluderade litteraturen för att bedöma dess tillförlitlighet och relevans. Det sista steget var att sammanställa resultatet från litteraturstudien, vilket redovisas i kapitel 4.

3.3 Avgränsning

Eftersom teorin i studien ska vara så aktuellt som möjligt och Zero Trust är en alltmer populär säkerhetsimplementation, avgränsades litteraturstudien till att endast innehålla litteratur skriven de senaste 5 åren. Artiklarna som valdes ut till granskning och analys handlade om vad Zero Trust är, vilka områden i ett företag som berörs, samt implementation av Zero Trust i företag. Av den anledningen har litteratur som berör övriga områden av Zero Trust inte behandlats.

Vetenskapliga artiklar som var granskade och skrivna på engelska valdes då det inte finns tillräckligt många granskade artiklar på svenska som berör ämnet Zero Trust att tillgå. Vidare sorterades artiklar äldre än 2018 bort för att hålla källorna så aktuella som möjligt.

3.4 Intervjustudie

Den forskningsansats som studien följer är kvalitativ, vilket innebär att det är viktigt att metoden för datainsamling speglar denna ansats. En kvalitativ forskningsansats syftar till att förstå och tolka fenomen ur deltagarnas perspektiv, vilket innebär att det är viktigt att samla in data som tillåter en djupgående och rik förståelse av deltagarnas erfarenheter och uppfattningar. Med grund i studiens frågeställningar framstod en semistrukturerad intervjustudie som det främsta alternativet för datainsamling. Detta på grund av att en semi-strukturerad intervju tillåter intervjun att hållas som en öppen konversation samtidigt som att den data som skapas inte blir oväsentlig. En mer ingående motivering bakom detta val kommer att presenteras nedan.

Enligt (Alsaawi, 2014) kan en semistrukturerad intervjustudie bäst förklaras som en kompromiss mellan en strukturerad intervjustudie och en ostrukturerad intervjustudie.

I en strukturerad intervjustudie skriver forskaren ner frågorna på förhand för att på ett bättre sätt hålla kontroll över vad som diskuteras i intervjun. På så sätt är det ett effektivt sätt att hålla intervjun fokuserad på området samt öppna för jämförelser mellan olika respondenter. Dock saknar denna intervjustudie djup och bredd i den data som ges av respondenterna eftersom variationen av svaren på frågorna är begränsad på grund av den strikta kontrollen. (Alsaawi, 2014) påpekar att denna intervjustudie är främst tillämpbar då forskaren på förhand har kännedom om vilken sorts information som söks.

En ostrukturerad intervjustudie är motsatsen till en strukturerad. Intervjun innehåller endast några få frågor där respondenterna tillåts utveckla sina svar. Intervjun liknar mer en konversation mellan två personer där forskaren försöker avbryta så lite som möjligt för att ge rum till respondenten att fritt kunna förklara sitt svar samt skapa en avslappnad stämning. Dock kan denna sorts intervjustudie leda till att intervjun tappar fokus på huvudområdet eftersom respondenterna är fria att utveckla åt vilket håll de vill. Denna sorts intervjustudie kan leda till att man får tillbaka en enorm mängd data, varav en del inte är relevant för studien, men är tillämpbar för forskare som undersöker ett visst specifikt område på djupet.

Kombinationen av de två intervjustudierna som presenterats är en semistrukturerad intervjustudie. Frågorna är bestämda i förväg men forskaren ger utrymme för respondenten att kunna utveckla sina svar genom att ställa öppna frågor. Denna typ av intervjustudie är främst använd av forskare som har en övergripande förståelse av området men forskar inom det för att få en djupare inblick.

(DeJonckheere & Vaughn, 2019) förklarar vidare att den huvudsakliga anledningen till att använda en semistrukturerad intervjustudie är att samla in information från nyckelpersoner med personliga erfarenheter och uppfattningar relaterade till området. Att använda en semistrukturerad intervjustudie ger även forskaren nya vägar för att samla in tidigare opresenterade data inom området vilket passar denna studie bra.

Urval av respondenter

Som det har förklarats tidigare, lyfter (DeJonckheere & Vaughn, 2019) vikten att ha korrekta respondenter för att kunna uppfylla studiens syfte. De förklarar vidare att de bästa respondenterna är de som är tillgängliga, villiga att bli intervjuade samt att de har egen erfarenhet och kunskap inom området.

Denna studie har tillämpat metoden som beskrivs av (Palinkas, et al., 2015) som ”målmedveten provtagning” (purposeful sampling) vilket innebär att studien identifierar och väljer ut individer som är särskilt kunniga inom området eller har erfarenhet av området. Förutom kunskap och erfarenhet

noterar författarna vikten av tillgänglighet, viljan att delta och förmågan att kommunicera erfarenheter och åsikter på ett uttrycksfullt och reflekterande sätt.

Med det som grund valdes respondenterna utifrån två kriterier.

1. Kunskap om ZT.
2. Arbetar på ett företag som hjälper andra företag att implementera ZT eller på ett företag/myndighet där de har implementerat ZT, alternativt där ZT lyfts som ett lämpligt alternativ.

Kriterierna bedömdes som nödvändiga för att respondenterna skulle kunna ge relevanta svar på intervjufrågorna och i slutändan studiens syfte. Att respondenterna arbetar på företag som hjälper andra företag att implementera ZT var viktigt för att få en förståelse kring hur implementationen går till samt vilka vanliga hinder som finns. Det var även nödvändigt för att få reda på om det finns en skillnad mellan myndigheters och företags inställning till ZT.

Respondenterna i **Tabell 1** som arbetar på ett företag eller myndighet där ZT implementerats eller lyfts som ett lämpligt alternativ hjälpte till att svara på hur de har gått till väga rent praktiskt samt vilka hinder de eventuellt har stött på under implementeringen. Intervjuer hölls även med företag som hjälper företag och myndigheter att implementera Zero Trust-lösningar för att få större insyn i skillnader mellan företag och myndigheter.

Intervjuerna genomfördes på distans via Microsoft Teams, spelades in, transkriberades och raderades därefter. Anonymitet utlovades till respondenterna på grund av den känsliga data som diskuterades i intervjuerna.

Tabell 1

Tabell över respondenter som deltog i intervjuerna.

Respondent	Verksamhet	Roll	Anställda
R1	Myndighet - förvaltning	Utvecklingschef	Ca 40
R2	Myndighet - förvaltning	IT-arkitekt	Ca 400
R3	Företag - konsultverksamhet inom telekom	IT-tekniker	Ca 1350
R4	Företag - fastighetsbolag	IT-chef	Ca 85
R5	Företag - revision- och konsultverksamhet	Chef cybersäkerhet	Ca 2800

En översikt av vilken typ av verksamhet och bransch varje respondent jobbar inom. Kolumnen till vänster representerar respondentens anonymiseringskod, kolumnen efter det representerar respondentens verksamhet samt vilken roll respondentens har inom verksamheten. Sista kolumnen till höger representerar antalet anställda verksamheten har totalt.

Intervjuguide

(DeJonckheere & Vaughn, 2019) förklarar att semistrukturerade intervjuer inkluderar en kort lista med vägledande frågor som kompletteras med uppföljningar och undersökande frågor som bygger på respondentens svar. Alla frågor bör vara öppna, neutrala och tydliga samt undvika att vara ledande. Intervjun börjar med en enkel kontextinställningsfråga innan intervjun går vidare till mer djupare frågor. (DeJonckheere & Vaughn, 2019) beskriver ytterligare att frågorna kan delas upp i fyra olika kategorier; ”*Grand Tour*”, *Kärnfrågor*, *Planerade följdfrågor* och *Oplanerade följdfrågor*.

Den första kategorin, ”*Grand Tour”*, handlar om att ställa allmänna frågor som är relaterade till innehållet som har i syfte att inleda intervjun och hjälpa respondenterna att börja prata om deras erfarenhet. När detta har uppnåtts går man över till *kärnfrågorna.* Kärnfrågorna är fem till tio frågor som är direkt relaterade till informationen man vill få ut. Detta har som syfte att besvara frågeställningarna samt hjälpa respondenten att prata öppet om ämnet på ett förbehållslöst sätt.

Av dessa kärnfrågor kan det uppkomma både planerade och oplanerade följdfrågor. Planerade följdfrågor är specifika frågor som kräver mer detaljer om särskilda aspekter i kärnfrågor. Oplanerade följdfrågor, är frågor som uppstår under intervjun baserade på respondentens svar. Båda dessa kategorier har samma syfte, nämligen att kunna få ett mer utförligt svar om kärnfrågorna samt diskutera eventuella särskilda aspekter som kan antydas av dessa svar.

Tabell 2

Teman och frågor som använts under intervjuerna.

Tema & Frågor	**Intervjufråga**
T1, Q1	*- Beskriv din roll i företaget/myndigheten.*
T1, Q2	*- Hur skulle du definiera termen Zero Trust?*
T2, Q3	*- Hur gick processen till?*
T3, Q4	*- Vilka hinder har ni upplevt i arbetet med implementeringen*
T3, Q5	*- Skulle du kunna beskriva på vilka sätt de har varit hinder?*

En översikt av frågorna som har ställts under intervjuerna, indelade i tre olika teman. T1 motsvarar kategorin ”Grand Tour” där målet är att inleda intervjun och hjälpa respondenten att börja prata om deras erfarenhet. T2 motsvarar kategorin ”kärnfrågorna” där målet är att få svar på de frågeställningarna som ställs i början av studien. T3 motsvarar kategorin ”följdfrågor” där specifika och ospecifika följdfrågor kan ställas till respondenten för att få ut mer information.

Intervjuguiden har byggts upp med hjälp av de fyra kategorierna som har benämnts tidigare vilken i sin tur kan delas in i tre olika teman. I **Tabell 2** beskrivs några kärnfrågor ur varje teman.

Det första temat, T1 i **Tabell 2**, handlar om att få en introduktion av respondenten samt vad deras definition av ZT är. Q1 i samma tabell ger forskaren, som ställer frågorna, en inblick om vilken position respondenten har inom organisationen samt vad för sorts informationen denna intervju kan komma bidra med till studien. Q2 är en mer generell fråga för att få respondenten att börja diskutera och ett smidigt sätt att inleda intervjun. Detta är delen som tidigare i kapitlet har benämnts som *"Grand Tour".*

T2 i **Tabell 2** handlar om att få en överblick över processen av implementation av ZT inom företaget eller myndigheten. För att uppfylla studiens syfte är det viktigt att en röd tråd genomsyrar denna fråga där följdfrågor blir viktiga redskap för att sedan kunna jämföra de olika svaren med varandra.

T3 i **Tabell 2** handlar om hinder. En generell fråga om hur eventuella hinder under processen löses ges till respondenten som på egen hand får utveckla och förklara hinder som uppkommit samt hur dessa hanterades på bästa möjliga sätt.

Utöver frågorna som är ställda med koppling till intervjuguiden, finns det ytterligare en typ av frågor som lagts till, nämligen uppföljningsfrågor. Där har författarna en möjlighet att återuppta en intervju efter den har avslutats ifall nya insikter och tankar kring ämnet har uppstått under processens gång. Det kan komma att spela en vital roll när slutsatser och diskussioner börjar formas. Det ger en flexibilitet för att inte måla in studien i ett hörn, helt i linje med den semistrukturerade intervjuformen.

3.5 Metodpositionering

Metoderna som används i denna studie har valts utifrån förmågan att kunna besvara frågeställningarna så optimalt som möjligt.

I tidigare publicerat material inom ämnet ZT, avsnitt 2.3, har forskarna använt sig av kvalitativa metoder vilket kan bero på att kännedomen kring området och spridningen av kunskapen är och har varit begränsad. De tidigare arbeten har valt att ta sig an området med hjälp av tidigare material för att kunna förstå hur fenomenet fungerar i olika miljöer. Dock finns det en lucka i informationen, där forskare inte har valt att göra några intervjuer med företag för att få större förståelse kring ZT.

Denna lucka kan finnas för att området ZT fortfarande är för instabilt för företag och myndigheter att börja applicera på ett storskaligt nätverk, samt att det kan finnas hinder som ligger bakom detta. Hindren kan vara budget,

avsaknad av expertis inom personalstyrkan, eller att det är ett för stort steg för företag att ta med tanke på den informationskänsliga data som de kan ha.

Litteraturstudie har valts som en av metoderna då det i dagsläget finns en stor mängd öppen information om hur ZT fungerar. Informationen har i syfte att ge läsaren en god förståelse om ZT, hur den hade kunnat vara applicerbar i en mängd olika miljöer samt fördelar och nackdelar med implementeringen.

Semistrukturerad intervjustudie har valts då denna kvalitativa metod har störst potential att kunna besvara frågeställningarna. Målsättningen med intervjun är att undersöka och förstå hur olika företag har eller planerar att applicera ZT som sin nya säkerhetslösning, vilket görs bäst genom att låta respondenten utveckla och prata fritt inom området. En strukturerad intervju hade inte gett studien samma djup då denna form av intervju inte tillåter någon utveckling av respondenten. Å andra sidan hade en ostrukturerad intervju kunnat ge för mycket data, där inte allt är relevant i denna studie.

Ett experiment i studien har valts att inte utföras eftersom syftet med studien är att förstå hur denna process har realiserats i olika nätverks- och IT-miljöer. Att göra ett experiment i en kontrollerad miljö hade inte heller hjälpt att besvara studiens frågeställningar.

3.6 Studiens forskningsbidrag

Denna studie kan potentiellt bidra till ökad medvetenhet om Zero Trust-konceptet och dess fördelar för cybersäkerhet inom både företag och myndigheter. Som ett resultat av denna ökade medvetenhet kan det uppstå en högre efterfrågan av Zero Trust-lösningar och tillämpningar.

Vidare kan, genom identifiering av hinder i implementering av Zero Trust, denna studie underlätta överbryggandet av dessa hinder och därmed bidra till förbättrad cybersäkerhet inom svenska företag och myndigheter. En förbättrad cybersäkerhet kan på sin tur leda till minskade risker för hot mot informations- och cybersäkerheten, exempelvis dataintrång eller sabotage. Vidare kan denna studie även vara till hjälp för att informera policybeslut på både företags- och myndighetsnivå. Resultaten kan även användas för att informera policybeslut på en nationell nivå, vilket i sin tur kan leda till en ökad användning av Zero Trust-lösningar inom hela Sverige.

Denna studie kan också bidra till att fylla ett forskningsgap gällande Zero Trust-tillämpning inom svenska företag och myndigheter. Resultaten från studien kan användas som grund för fortsatt forskning och utveckling av Zero Trust-lösningar som är specifikt anpassade för den svenska kontexten. Således kan denna studie bidra till att utveckla nya Zero Trust-lösningar som kan förbättra cybersäkerheten inom svenska företag och myndigheter.

3.7 Problematisering

Att välja mellan olika forskningsmetoder är en viktig process i utformningen av en studie. Metoderna som valts till denna studie, semistrukturerade intervjuer och systematisk litteraturstudie, har olika fördelar och utmaningar som kan påverka resultatet.

När semistrukturerade intervjuer väljs som forskningsmetod är det viktigt att överväga vilken typ av data som kommer att samlas in. Semistrukturerade intervjuer ger en möjlighet att samla in djupgående information från respondenterna och tillåter även möjligheten att ställa följdfrågor och utforska nya idéer. Samtidigt är det viktigt att understryka att semistrukturerade intervjuer är tidskrävande att genomföra och bearbeta. Dessutom kan resultaten av intervjuerna påverkas av forskarens personliga åsikter och tolkningar av data, vilket kan leda till bristande objektivitet och tillförlitlighet.

En systematisk litteraturstudie ger en möjlighet att sammanställa stora mängder information från olika källor och undersöka tidigare forskning inom ett specifikt ämnesområde. Detta gör det möjligt att undersöka existerande kunskap och identifiera luckor som kan utforskas vidare i en studie. Det är samtidigt viktigt att notera att en systematisk litteraturstudie, likt semistrukturerade intervjuer, är en tidskrävande process och kräver en noggrann och systematisk metod för att säkerställa att all relevant information samlas in. Däremot kan resultaten av en systematisk litteraturstudie påverkas av vilka källor som väljs och hur informationen analyseras.

Att enbart utföra en litteraturstudie kan vara ett alternativ till metodval för studien, där undersökningar av tidigare arbeten analyseras och bearbetas för att kunna besvara frågeställningarna. Hindren som finns i att enbart utföra en litteraturstudie är att delar av frågeställningarna är dåligt dokumenterad i dagsläget. Som nämnts i avsnitt 2.3, finns det endast ett arbete som behandlar ZT i svenska företag.

Ytterligare en metod som kan vara passande till studien är att använda fokusgrupper, där en grupp av deltagare samlas för att diskutera ett ämne och delar sina åsikter och kunskaper. För att besvara en del av studiens syfte är det möjligt att bjuda in deltagare som arbetar inom IT-säkerhet för att diskutera konceptet ZT. Däremot kan det vara problematiskt att samla ihop deltagare som ska diskutera säkerhetslösningar i sina företag då det är ett känsligt ämne.

Sammanfattningsvis är det viktigt att välja forskningsmetoder som passar det specifika ämnet och forskningsfrågorna som undersöks i studien. Anledningen till att semistrukturerade intervjuer och systematisk litteraturstudie används i kombination i denna studie är för att öka validiteten och tillförlitligheten. Genom att samla in djupgående information

från respondenter och sammanställa stora mängder information från olika källor fås en mer omfattande förståelse av ämnet och på så sätt kan validiteten stärkas genom att bekräfta eller utmana resultaten från en metod med resultaten från en annan metod.

3.8 Etiska aspekter

I denna studie är det av högsta vikt att säkerställa att den genomförs på ett etiskt sätt, särskilt med hänsyn till den potentiellt känsliga information som kan komma att avslöjas. Forskningen som utförs i studien kan eventuellt innebära att information som rör företags eller myndigheters IT-säkerhet uppenbaras, vilket kan avskräcka vissa individer från att delta i intervjuerna.

För att garantera att studien uppnår sitt syfte, var det avgörande att intervjurespondenterna kände sig bekväma att dela med sig av denna känsliga information. Därför var det nödvändigt att framhålla att deltagandet i en intervju var på respondenternas villkor, och att de inte var skyldiga att svara på några frågor som ansågs vara olämpliga eller känsliga. Det var också av största vikt att poängtera att informationen som delades i intervjuerna skulle behandlas konfidentiellt och att respondenterna skulle förbli anonyma i sina roller som företrädare för sina respektive organisationer.

Genom att klart kommunicera de etiska riktlinjerna och säkerhetsåtgärderna, var förhoppningen att de noggrant utvalda respondenterna skulle känna sig trygga att delta i intervjuerna, och att studien kunde utföras på ett ansvarsfullt och respektfullt sätt. Det är av högsta betydelse att skydda integriteten och säkerheten för de organisationer och individer som berörs av denna forskning, och detta kommer förbli en genomgående prioritet i studien.

4 Litteraturstudie

För att ge läsaren en ökad förståelse för Zero Trust och dess påverkan inom företag behövs ett beskrivande kapitel. All information som presenteras i kapitlet har samlats in genom litteratursökningen och innefattar arbetets litteraturstudie. Kapitlet kommer att delas upp i två olika delar, 4.1 kommer att behandla tekniken och hur ZT är uppbyggt samt dess implementering i system och 4.2 kommer att ta upp hinder från tidigare litteratur gällande implementering av ZT.

4.1 Zero Trust

ZT är ett säkerhetskoncept som utvecklats för att hantera hoten mot nätverk och datasystem. Idén bakom ZT är att alla enheter och användare ska behandlas som potentiella hot tills de verifierats på ett tillförlitligt sätt. Termen ”Zero Trust” kommer från John Kindervag som i en rapport från 2010, utvecklade ett nytt säkerhetssystem för att komma ifrån den moderna idén (Kindervag, 2010). Hans idé var enkel; säkerhetsansvariga ska sluta lita på datapaket som om de vore användare. De måste eliminera idén om ett pålitligt nätverk (interna nätverket) och ett opålitligt nätverk (externa nätverket). Detta ligger till grund för ZT:s motto "lita aldrig, verifiera alltid".

För att säkerställa en stark säkerhet enligt ZT krävs det strikta kontroller av åtkomst och verifikation av allt som försöker få åtkomst till nätverket. Detta kan innebära användning av tekniker som multifaktorautentisering, åtkomstkontroll baserad på roll och användarbehörighet samt kontinuerlig övervakning av nätverksaktivitet för att upptäcka och hantera misstänkta aktiviteter.

Uppbyggnadsstrukturer

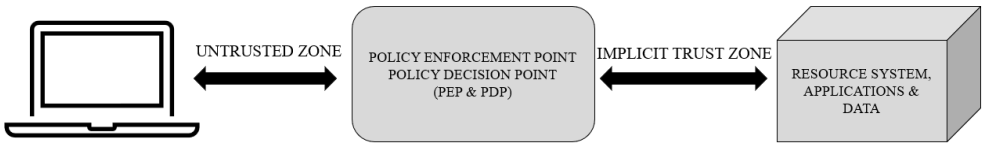
Det absolut viktigaste för att system med ZT arkitektur ska fungera är att det finns en policy eller riktlinjer som beskriver hur organisationen ska förhålla sig till nätverkssäkerheten. För att riktlinjerna ska kunna gälla bör fokus ligga på att hindra obehöriga att få tillgång till systemen och tjänsterna som erbjuds av och inom organisationerna. När det kommer till ZT arkitekturen i praktiken, bygger den på en cybersäkerhetsplan där flera olika koncept samverkar för att minimera osäkerheten i kommunikationen mellan de olika ingående delarna. Många av IT-miljöerna idag är stora och komplexa att hantera och administrera. För att ZT ska kunna användas effektivt måste ansvariga individer vara uppdaterade kring och, över tiden, analysera risker samt vidta lämpliga åtgärder för att hindra attacker gentemot kritiska funktioner, tillgångar och andra resurser på nätverket (Rose, Borchert, Mitchell, & Connelly, 2020).

När det talas om att skydda tillgångarna och resurserna i ett nätverk med ZT handlar det främst om att i största möjliga mån begränsa användares möjligheter att komma åt data och tjänster. En person bör endast ha tillgång till systemet på den nivå som är nödvändig för att utföra sitt arbete (Shore, Zeadally, & Keshariya, 2021).

I **Figur 1** nedan beskrivs på enklaste sätt hur en användare får tillgång till eller blir nekad access till en applikation eller nätverk. Initialt finns det inget som bekräftar att datorn tillhör nätverket och den måste autentiseras. Autentiseringen sker mot organisationens fördefinierade riktlinjer Policy Enforcement Point (PEP) och Policy Decision Point (PDP) och utifrån dessa accepteras eller nekas tillträde. PEP och PDP utgör efter första autentisering sedan grunden för hur mycket i nätverket en användare ska kunna få tillgång till (Rose, Borchert, Mitchell, & Connelly, 2020). Riktlinjerna administreras av någon eller några individer som tillsammans utgör en slags bas för vad varje enskild användare ska få tillgång i sin personliga tillitzon (Shore, Zeadally, & Keshariya, 2021). Om en individ befinner sig i en icke tillförlitlig zon och sedan vill komma åt resurser eller applikationer måste det genomföras en kontroll mot hur autentisk identiteten på personen i fråga är. Fortgår verifieringen som den ska och personen har den identitet som den uppger, kontrollerar systemet huruvida personen har rätt behörighet för att tillåta access. Processen genomförs i en så kallad ”implicit trust zone” som kan liknas vid ett väntrum eller en lobby. Accessuppgifterna finns att hämta från PEP och PDP som spelar en central roll i organisationens säkerhetsuppbyggnad (Rose, Borchert, Mitchell, & Connelly, 2020).

Figur 1

Zero Trust - Autentiserings- och accessprocedur



Datorn föreställer en enhet som försöker ansluta till ett nätverk. I den initiala fasen är enheten ett direkt hot mot nätverket och behandlas utifrån de premisserna. Enheten jämförs med en fastställd policy (PEP) varav den kan beviljas eller nekas tillträde med hjälp av (PDP). När enheten är verifierad befinner den sig i väntrummet (Implicit Trust Zone) och behöver autentiseras återigen gentemot enhetens privilegier enligt PEP för att få tillgång till olika applikationer och data i nätverket.

Zero Trusts grundstenar

I NIST:s rapport från 2020 finns ingen exakt definition av Zero Trust, men de flesta tolkningar involverar ett antal gemensamma implementeringspunkter. Fokus ligger på vad som borde finnas i stället för vad som inte existerar eller vad som borde plockas bort ur de gamla systemen. I rapporten görs ett försök att summera och pussla ihop grundsatserna för att uppnå en målbild av implementeringens ingående delar (Rose, Borchert, Mitchell, & Connelly, 2020).

Arkitekturen är uppbyggd enligt **Figur 1** med en inledande inställning till att alla enheter på nätverket, oavsett var de kommer ifrån, ska likställas med resurser och tillgångar. Efter anslutningen klassificeras de av organisationen och får minsta möjliga access för att genomföra sina uppgifter. Om en individ eller enhet vill komma åt organisationstillgångar måste det finnas säkerhetskrav som uppfylls och vid varje ny åtkomst till en applikation eller uppkoppling måste det ske en autentisering som direkt är kopplad till säkerhetskraven (Rose, Borchert, Mitchell, & Connelly, 2020).

Fortsättningsvis behöver kommunikationen ske säkert, oavsett om det sker inifrån organisationens datacentra eller om uppkoppling sker från extern plats. Säkerheten ska inte garanteras bara genom att enheten eller resursen finns på samma fysiska plats som organisationen. All kommunikation behöver konfidentialitet- och integritetsskyddas och för att det ska kunna ske måste förfrågningar utvärderas innan maskinen eller individen som skickar förfrågan tillåts att komma åt önskat innehåll (Rose, 2022).

PDP och PEP måste vara skapade för att dynamiskt kunna vara föränderliga. Allt eftersom nya enheter ansluts till nätverken och individer tillsätts eller förändrar sin roll inom organisationen, måste riktlinjerna också möjliggöra transparens. Organisationen måste skydda sina resurser, och bästa sätt att göra det, är att definiera och övervaka vad som är resurser, vad varje resurs ska ha tillgång till och över tiden uppdatera vad varje resurs verkligen behöver ha tillgång till (Rose, 2022).

Zero Trust definierar övervakning som en vital del ur ett säkerhetsperspektiv. Konceptet att övervaka alla resurser på enheten motiveras genom att man inte litar på någon. Systemet ska inte göra skillnad på en elakartad anslutning eller en förväntad anslutning. För att det ska fungera i praktiken behöver övervakningen ske i olika delar, från autentiseringen in till systemet, ut i hur enheten inne i systemet uppträder beteendemässigt utifrån tidigare inlärda mönster. Dessa mönster hämtas från den definierade policyn i PEP och PDP. Exempel på detta kan vara tidsbestämda anslutningar, var man brukar befinna sig när man ansluter och vilka patchar och versioner som finns installerade på enheterna. Tidpunkter för anslutningar spelar också en stor roll i huruvida en anslutning accepteras eller nekas (Rose, 2022).

En organisation som brukar Zero Trust-lösningar ska också ha egenskapen att kunna sätta specifika resurser i total karantän. Om det finns sårbarheter att utnyttja i exempelvis en version av operativsystem som används inuti nätverket kan man stänga ute de som har den versionen installerad. Först när enheterna uppdaterats och inte längre ses som ett hot kan de återgå till normalförfarande igen. Det krävs kompetent personal som kan upprätthålla ett sådant system tillsammans med flertalet automatiserade verktyg som hjälpmedel när det gäller att upptäcka och bekämpa nya hot (Rose, Borchert, Mitchell, & Connelly, 2020).

Implementeringsprocedurer

När ett företag eller en myndighet väljer att implementera Zero Trust finns det sju steg som organisationen borde följa för att implementera det på bästa sätt enligt (Rose, 2022).

Det första steget kallas "*Prepare"* och kan ses som byggstenen vilket allt kommer att byggas runt, se **Figur 2** I detta steg ska organisationen göra en inventering av alla resurser, nätverksidentiteter och roller inom företaget. Ansvariga chefer över olika sektioner kan även ge sin input till hur resurserna används i arbetsflöden för att få en omfattning om vilka säkerhetskrav som kommer att behövas. Sammanfattningsvis är det första steget till för att förbereda organisationen att hantera sina säkerhets- och integritetsrisker (Rose, 2022).

Nästa steg i implementeringsprocessen är "*Categorize".* Detta steg används för att placera de olika resurserna i olika riskkategorier; "Låg", "Måttlig" eller "Hög", baserat på resursens konfidentialitet, integritet och tillgänglighetskrav i arbetsflöden. Uppgiften går ut på att dokumentera egenskaperna hos ett system, både resursen och dess relevanta arbetsflöden. Det har inte nödvändigtvis något med själva Zero Trust-implementationen att göra, men det krävs för att få en överblick och förståelse kring organisationens tillgångar och resurser (Rose, 2022).

Vidare behöver organisationen välja ut någon slags utgångsdata för att hantera de olika resurserna nämnda ovan. Det sker i kategorin *"Select"*. Detta steg är inte Zero Trust-specifikt, utan ses som en grundläggande del i det stora IT-säkerhetsperspektivet. Att känna till och välja vilka kontroller som ska genomföras i förhållande till kända attackytor och var potentiellt känslig information finns är kritisk (Rose, 2022). Den här kategorin förblir dynamisk under hela implementeringens gång och ändras kontinuerligt i takt med att risken och hoten mot tillgångarna ändras. Här läggs också grunden för PEP och PDP som är en vital del i Zero Trusts uppbyggnad (He, Huang, Chen, Ni, & Ma, 2022).

"*Implement"*-steget är inte heller bundet till Zero Trust. Administratörer bör undvika lösningar som innebär frekventa mänskliga handlingar och i stället fokusera på automatisering för dynamiska svar på säkerhetsproblem som återkommer i olika former (Rose, 2022).

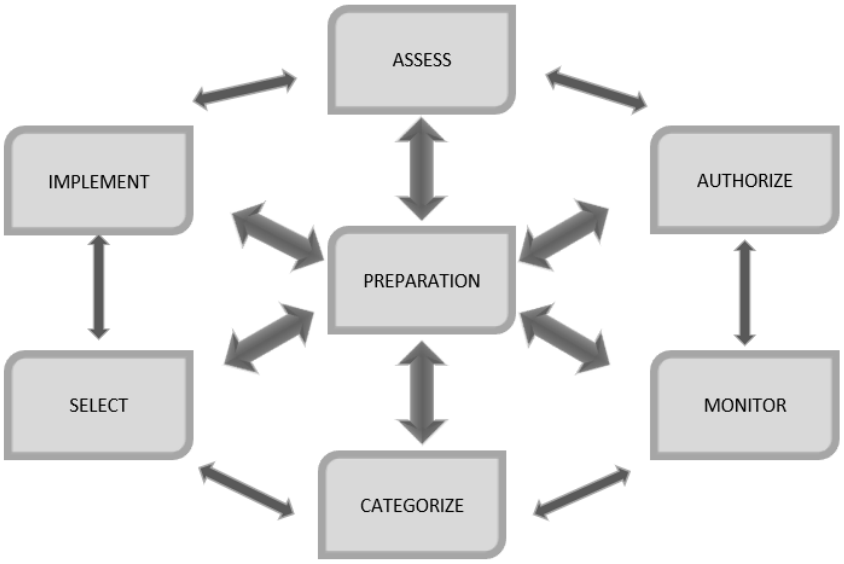
Det femte steget inom implementeringsprocessen är "*Assess"* och understryker vikten av kontinuerlig bedömning av kontroller inom Zero Trust på grund av det ständigt växlande IT-miljön och dess trender. Assess-steget innebär att bedöma både systemet och de processer som används för att hantera det vilket kan ses som att kompromissa två bedömningsprocesser (Rose, 2022). Ledningsprocessen bör kontinuerligt utvärderas på grund av Zero Trusts dynamiska natur, vilket innebär att systemet i sig sannolikt kommer att förändras snabbt. Bedömningen bör även innehålla aktiva processer som ”red team-testning” av systemet som input till bedömningarna. Det innebär simulering av angrepp från ett motståndarperspektiv (Shore, Zeadally, & Keshariya, 2021).

Det näst sista steget handlar om att systemet ska kunna vara dynamiskt i hur det förhåller sig till förändringar i nätverkskonfigurationen. Steget som benämns ”A*uthorize*” ska inte ses som statiskt då de ska kunna hantera nya anslutningar, nya processer och nya resurser. Det ska inte heller vara låst till specifika versioner när nya uppdateringar blir tillgängliga (Rose, 2022).

Sista steget betecknas "*Monitor"* och innebär att Zero Trust kräver att organisationen ska övervaka resurserna som krävs för att verksamheten ska bedriva primära uppdrag. Detta omfattar att övervaka enheter, användarbeteenden samt nätverkstrafik (Rose, 2022). Exakt hur detta görs är beroende på vilka tekniska lösningar som finns i företaget sedan tidigare. Oavsett vilken teknik som nyttjas och administreras bör företaget eller organisationen ha policys på plats för att utlösa åtgärder baserat på beteenden som observeras genom övervakning (He, Huang, Chen, Ni, & Ma, 2022).

Figur 2

Zero Trust – Implementeringsprocedur



Preparation är det centrala i implementeringen av ZT där allt kretsar kring hur väl grunden har lagts för att lyckas. Sedan ska tillgängliga resurser kategoriseras och väljas ut i ett slags rankingsystem där en policy börjar formas (PEP & PDP). Vidare bör automatik implementeras för att minska mänsklig interaktion i onödiga delar av systemet. När allt är genomfört ska systemen i stegen assess, authorize och monitor övervakas, utvärderas och dynamiskt förändras över tiden.
Att pilarna går åt alla håll och riktningar symboliserar att stegen inte är statiska utan att de är föränderliga i takt med att hoten ändras och utvecklas.

Zero Trust i praktiken

Splunk är ett amerikanskt mjukvaruföretag som är ett av flera företag som hjälper andra företag och organisationer att implementera ZT. I deras artikel, en guide, presenterar de sina sex steg på hur ett företag går från ett legacy-arkitektur till en ZT-arkitektur.

Första steget i guiden är att samla in relevant data. Genom att göra en inventering av organisationens resurser blir det tydligt vilka resurser som är mest kritiska för arbetsflödet och som kräver mest säkerhet och övervakning. Några exempel på kritiska resurser är nätverket, vilket inkluderar organisationens datacenter samt molnnätverksarkitektur såsom switchar och routrar samt lagringsutrymmet och administrativa delen som kan inkludera bland annat system och programvaror som hjälper till med administrativa funktioner inom organisationen. I **Figur 2** presenteras detta steg under kategorin *”preparation”* och liknas vid allt arbete som genomförs innan den praktiska implementationen (Splunk, 2022).

Nästa steg i implementationsresan är att förstå och effektivisera organisationens data. Inom en organisation kan ett flertal olika produkter användas av olika leverantörer som alla ger data på olika sätt. Ett exempel är att alla brandväggsleverantörer använder olika loggformat och

datastruktur. För att kunna stödja en centraliserad övervakning måste all data som kommer in vara normaliserad på ett konsekvent format. Också detta är ett steg i fasen *”preparation”* (Splunk, 2022).

Det tredje steget i guiden är att expandera organisationens data. Oftare än inte kommer den kontinuerliga övervakningen av säkerhetskontroller att misslyckas upptäcka avancerade säkerhetshot. För att undvika detta bör säkerhetsövervakningen även övervaka hur auktoriserad användning ser ut. Genom att övervaka auktoriserade användare kan man få insikt i vad som skiljer anomalier från normala data. Detta medför att man på ett bättre sätt kan upptäcka skadlig åtkomst. Detta kan göras med hjälp av nätverksloggar som korrelerar med användares applikations- och process-loggar (Splunk, 2022).

Fjärde steget handlar om att förstärka organisationens data. Detta görs genom att samla information från datakällor som ger ännu mer sammanhang. Dessa datakällor kan vara “Threat Intelligence” vilket innebär inhämtning och analys av information om cyberhot, information från sårbarhetsanalyser samt patchanalys. Dessa datakällor ger organisationen ett sätt att förstå den nuvarande hotbilden mot användare och system. Inte heller detta steg finns enskilt representerat i **Figur 2** utan får mer ses som en kombination av *”monitor”* och *”assess”* (Splunk, 2022)**.**

I femte steget börjar organisationen att kolla på hur deras incidenthantering ser ut. Efter att ha utfört alla tidigare steg bör organisationen ha en stark grund för övervakning och säkerhet med hjälp av normaliserade och berikade data. Detta leder till att organisationen kan börja gå vidare och implementera hur de utreder ett eventuellt skadligt intrång och hur deras respons ser ut till en incident. Även detta steg finns representerat steget i **Figur 2** som tillsammans med steg fyra utgör ”*Assess”*.

Sista steget inom implementering av Zero Trust handlar om att organisationen ska sätta upp ett säkerhetsdetekteringssystem med riskbaserad varning. Genom att introducera tidigare incident-fall till Zero Trust-systemet kan det börja lära sig hur en incident ser ut och kan därmed detektera misstänkt aktivitet inom systemet och varna för detta. Detta steg representerar det sista steget ”*Monitor”* i **Figur 2** och innebär att organisationen nu ska övervaka resurserna för att kunna bedriva verksamheten optimalt (Splunk, 2022).

4.2 Hinder vid implementering av Zero Trust

(Teerakanok, Uehara, & Inomata, 2021) förklarar att det finns återkommande hinder för organisationer som har valt eller ska implementera ZT, eftersom ZT fortfarande är i sin utvecklingsfas. Dessa hinder kan enkelt

delas upp i två olika kategorier, hinder som försvårar för organisationen internt, och hinder som försvårar för organisationen externt.

Interna hinder

PDP, eller *policy data point,* har ansvaret inom ZT att ta beslut. Denna process kräver information från olika källor för att ta det slutgiltiga beslutet om huruvida systemet beviljar eller nekar åtkomst till företagets resurser. Däremot finns det ingen gemensam standard mellan aktörer gällande utbytet av cybersäkerhetsinformation mellan olika system. Detta betyder att om en leverantör har tekniska problem eller lider av en säkerhetsbrist och företaget väljer att byta leverantör är det inte garanterat att standarden av säkerhetsinformationen är detsamma som förut (Shore, Zeadally, & Keshariya, 2021).

Vidare förklarar (Teerakanok, Uehara, & Inomata, 2021) att det finns hinder gällande tillitsnivån inom ZT system. När en användare eller en enhet skickar en förfrågan om att få tillgång till företagets resurser så behöver ZT systemet beräkna enhetens eller användares tillitsnivå och sedan jämföra den med gränsen som är satt inom systemet. Att beräkna tillitsnivån är en otroligt resurskrävande process då en för hög tröskel kopplat till just tillitsnivån på systemet kan leda till att det påverkar företagets arbetsflöde negativt. Å andra sidan kan en för låg tröskel vad gäller tillitsnivån leda till att enheter och användare som egentligen inte ska ha tillgång till den resursen kan få tag i den och leder till att systemet anses som universellt och mindre säkert.

Gemensamt för dessa hinder är att grunden, själva tillitsalgoritmen (TA) behöver filtreras, normaliseras och korreleras på ett bättre sätt för att förbättra algoritmen. TA innehåller information från olika källor som nätverkstrafik, geolokalisering och användares identitet. Det är emellertid viktigt att notera att varje del av information inte är lika betydelsefull. Vid bedömning av tillitsnivå på en begäran är användarinformation mer värdefull än information om nätverkstrafik. För närvarande finns det ingen optimal lösning eller strategi för att väga dessa attributet mot varandra. I stället är det upp till företaget att kontinuerligt observera och justera denna parameter över tid för att säkerställa att systemet är korrekt kalibrerat (Teerakanok, Uehara, & Inomata, 2021).

TA kan även bestå av statiska regler som företaget angivit och som kan ses som universella regler, till exempel att neka all åtkomst från en utsatt eller skadad enhet. Det kan även bestå av dynamiska regler som skattar sannolikheten för att en användare är potentiellt farlig baserat på tidigare nämnda parametrar och involverar oftast maskininlärning. (Homeland Department of Security, K.D, Uttecht, 2020) tar upp en viktig poäng gällande information från opålitliga källor. En underrättelsemyndighet som

har implementerat ZT kan behöva ta emot information från källor som inte går att autentisera och som då ligger i konflikt med ZT-policys att neka allting som inte kan autentiseras.

Ansvaret som ligger på TA betyder att en standardiserad strategi behövs inom ZT-system då felaktiga beslut av TA i allra högsta grad kan påverka systemet PDP:s slutgiltiga beslut vilket i sin tur kan leda till att otillåtna användare och enheter får tillgång till systemet.

Externa hinder

Externa hinder kan ses som hinder som påverkar företagets arbetsflöde genom att antingen försvåra för användarna inom företaget att använda system, eller försvårar för företaget i allmänhet.

(Teerakanok, Uehara, & Inomata, 2021) tar upp ett hinder som inte är låst till ZT utan kan påverka alla sorters olika företag inom olika sektorer, nämligen *Vendors Lock-In and Interoperability.* Med detta menas att företag blir låsta till ett visst företag därför att lösningar från andra företag inte kommunicerar eller är kompatibla med varandras enheter. Eftersom att implementera ZT är en utdragen och dyr lösning, kan företag som hjälper till med implementeringen välja att använda API:s eller lösningar som är låsta till den leverantören. Med tanke på att ZT fortfarande befinner sig i sin utvecklingsfas har detta problem inte uppkommit än rent praktiskt. Om man emellertid inspekterar tidigare “nya” lösningar såsom moln-lösningar och IoT, uppstår detta problem. En standardiserad lösning inom ZT för hur systemet ska vara uppbyggt och fungera skulle sätta stopp för detta.

Ett annat hinder som måste prioriteras inom ZT är att arbetsflödet för användarna av systemet inte får rubbas. När ett företag väljer att implementera ZT i sina system pågår detta i flera steg för att till slut kunna byta ut det äldre systemet mot ZT. Detta kan göras genom att införa tekniska restriktioner på det gamla systemet samtidigt som man uppmuntrar användarna att börja nyttja ZT. När allt fler börjat använda det nya systemet utan problem kan företaget välja att flytta arbetsflödet från det gamla systemet till det nya. I detta ligger det ett stort ansvar på företaget för att se till att övergången blir så smidig som möjlig för användarna. Det finns även ett ansvar på användarna att ge kontinuerlig feedback på systemet till de ansvariga vilket i sin tur kan ta tid och föranleda onödig frustration som kan påverka arbetet. (Teerakanok, Uehara, & Inomata, 2021).

Slutligen finns det även ett potentiellt hinder gällande enheter som användarna själva tar med utifrån, även kallat BYOD (*Bring Your Own Device*). I ett ZT nätverk är det viktigt att kunna kontrollera risken hos alla enheter som är anslutna till nätverket. Om användarna däremot börjar ta med sig egna enheter uppkommer det ett hinder då en policy inom företaget kan vara att man inte får installera företagets applikationer på privata

enheter. Detta leder till att det kan finnas enheter som inte går att kontrollera på ett nätverk som kräver att få tillgång till allt för att kontrollera säkerhetsrisken inom företaget (Teerakanok, Uehara, & Inomata, 2021).

5 Resultat

5.1 Empiri

Empirikapitlet är indelat i tre delar som presenterar intervjusvaren kopplade till studiens frågeställningar, inställning till och implementation av ZT samt hinder som upplevts. Respondenterna som förekommer i denna empiri finns representerade i **Tabell 1**.

Inställning

Studiens första frågeställning berör svenska företags och myndigheters inställning till Zero Trust och om det finns någon skillnad mellan dem. Under intervjuerna fick respondenterna frågor om hur de ställer sig till konceptet Zero Trust.

Några av frågorna och svaren från respondenter från företag var följande:

Hur skulle du vilja beskriva termen Zero Trust?

> *Det finns en teoretisk och en praktisk sida med att säga Zero Trust. I teorin är det en väldigt bra grej att ha att sträva emot, för då får jag i min roll en mycket enklare vardag egentligen […] Men det kan bli för mycket att kräva det av medarbetare, eller sådana som agerar i nätverket som behöver bandbredden eller behöver nyttja den. Så det är en balansgång, att ligga på rätt säkerhetsnivå så att folk ändå kan jobba effektivt om man kan säga så.*
>
> Respondent 4

> *[...] På grund av COVID-19, har företagskontoren, tredje parter, kunder och mobila enheter tillgång till företagsnätverket via ett opålitligt internet och allt inom nätverkets omkrets är också opålitligt. Så i princip ska du aldrig lita på och alltid verifiera. Zero Trust säkerhetsarkitekturen är det nya perspektivet och i grunden inspirationen för ledare att hantera cyberhotslandskapet.*
>
> Respondent 5

Inom vilka användningsområden tycker du att Zero Trust är mest lämplig att implementera?

> *Jag tycker att, för användningen inom molnet och dess kringgående Software As A Service eller vad det kan bygga på, där är liksom Zero Trust ett bra koncept. Som jag tycker att man ska implementera. […] Sen kan det också vara en grej att man BÖR lita på sina anställda i tillräcklig mån kan jag tycka, sen kan jag också tycka att det är bättre att ha serverdrift och on-premise i vissa avseenden om man själv äger datan. Då kan man styra hur man vill.*
>
> Respondent 3

Några av frågorna och svaren från respondenter från myndigheter var följande:

Hur skulle ni vilja beskriva termen Zero Trust?

> *För vår del handlar Zero Trust egentligen om att varje mikrotjänst oavsett vad den gör för något, om det handlar om inloggningslådan eller om det handlar om något annat, så handlar det om att när kommunikation sker mellan mikrotjänster, eller mot externa tjänster som vi använder oss utav så ska vi i varje steg kontrollera att 1: den användare oavsett om det är en person eller tjänst som initierat anropsbegäran ska kontrolleras om den har tjänsten eller den som anropat har rätt att begära den här informationen, och om det sker under rätt former. På samma sätt handlar det om transferering av data.*
>
> Respondent 1

> *[…] nu med omvärldens krav och även med läget med säkerheten i världen så inser vi ju att den gamla modellen måste avvecklas och ersättas av någonting som är lite mer robust och lite mer vad kan man säga, tålig i den här förflyttningen då vi har allt fler användare som vill jobba mobilt och kanske vill komma åt information från andra platser än deras vanliga kontor och det normala nätverket.*
>
> Respondent 2

För mig innebär det en förflyttning där vi traditionellt sett har haft mer fokus på brandväggar och vägen in till datacenter och sådana saker och åtkomsttjänsten och från vilken enhet vi kommer åt tjänsten. Och nu med Zero Trust som är framtiden med en modell som är lite friare där man börjar autentisera användare på ett helt annat sätt och hur vi litar på tjänsterna på ett helt annat sätt som gör att vi även kan tillgängliggöra dom på ett annat sätt...

Respondent 2

På ett teoretiskt plan tycker jag att det är jättebra.

Respondent 1

Företaget som hjälper andra företag och myndigheter att implementera Zero Trust-lösningar fick i sin tur svara på frågor om de sett vilken typ av företag, privata eller offentliga, som är intresserade av sådana lösningar samt om de sett en märkbar skillnad mellan företag och myndigheter.

Några av svaren och frågorna var följande:

Upplever ni att det mest är myndigheter eller företaget som går mot Zero Trust-lösningar?

Baserat på min erfarenhet tror jag att det främst är företag som jobbar mer i molnet.

Jag har mer synlighet i den privata sektorn. Så jag kan inte göra en bra jämförelse mellan privat och offentlig...

Vi har diskuterat mer med de privata företagen kring detta ämne...

Från min erfarenhet av att arbeta med den offentliga sektorn har jag faktiskt aldrig stött på Zero Trust-frågan så mycket. Det handlar mer om säkerhet och du vet, att skydda data och inte just Zero Trust-frågan. Men det verkar vara ett alltmer populärt ämne, så fler och fler personer kommer att tänka på det.

Respondent 5

Implementation

Studiens andra frågeställning berör implementation av Zero Trust-lösningar i svenska företag och myndigheter. Därmed fick respondenterna svara på frågor huruvida de har implementerat sådana lösningar och i vilken grad de i sådana fall gjort det.

Exempel på fråga och svar från myndigheter var följande:

Har ni implementerat Zero Trust eller har ni funderat på att göra det?

> *Alltså, ja och nej. Vi är som de allra flesta. Vi har lite ambitionen och har principiellt beslutat att gå mot Zero Trust men sen har vi ett enormt arv av system i vår infrastruktur som är skapat och bygger på andra föråldrade premisser. Den övergången kommer att ta tid, men vår inriktning är att försöka implementera nya saker utifrån Zero Trust modeller och Zero Trust principer. Med det sagt kommer vi troligtvis inte orka med att göra om allt det gamla, men inriktningen är att det kommer att avvecklas stegvis.*
>
> Respondent 2

> *Det är en helhetslösning hos oss, det är byggt med konceptet security first. Det är väldigt vanligt att man annars bygger ett system eller kommer med en lösning på något och sen kommer på, juste vi måste göra det säkert också. […] att vi inte utvecklar nya system utan att ha security first tankesättet vid uppstarten. Nu är jag supernöjd att vi har ett modernt system implementerat och att vi inte har kvar några legacy-system alls.*
>
> Respondent 1

Några av frågorna och svaren från företag:

Har ni implementerat Zero Trust eller har ni funderat på att göra det?

> *Ja, det har vi men absolut inte fullt ut överallt. Det är något vi får fortsätta jobba med på lång sikt. Vi jobbar med tvåfaktorsautentisering i ungefär 90% av accessen från människa till nätverk eller system. Men vi har lite till där kvar att jobba med just i den frågan. Och den är vi kanske i vissa lägen att vi har långa spann mellan att vi frågar efter en verifiering igen.*
>
> Respondent 4

Vi har kommit ganska långt på den administrativa sidan, där våra medarbetare där dom jobbar dagligen, oavsett vad man har för medel, om man jobbar med telefoner eller laptops, eller andra skärmar.

Respondent 4

Vi har på viss basis, när vi köper in så har vi sett till att det finns inträdesavtal, att data-processing-agreements är på plats för den typen av data som ska hanteras i systemet […] Det är saker vi tänker på och analyserar och har med i data-processing-agreements och ser till att det stämmer överens.

Respondent 3

[…] där har vi styrt så att, eller för att, man ska kunna ändra något i eller administrera en server eller hantera den på något vis, då ska det vara styrt via en metod som man signerar med sig själv och en identifierbar metod. Sen kollar även servrarna att det här är en av de godkända identifierarna också när koden körs in till servern.

Respondent 3

Strävar ni åt Zero Trust som en helhetslösning?

Vi ser det inte som en helhetslösning, det är inte applicerbart i alla fall att implementera Zero Trust till 100%. Man kan såklart göra det så gott det går, men med det kommer sådana enorma kostnader så för att upprätthålla viss eller vissa säkerhetskrav då går det inte längre.

Respondent 3

[…] det är definitivt styrt på projektnivå, om vi får in en beställning så kör vi Zero Trust för ett visst projekt […] Det är med andra ord implementerat där det är smidigt och det är snabbt och där det går att implementera. Där gör vi det och försöker hela tiden tänka utifrån det perspektivet.

Respondent 3

Hinder

För att kunna besvara studiens andra frågeställning ytterligare fick respondenterna svara på vilka hinder de möjligtvis har upplevt med implementation av Zero Trust.

Några frågor och svar från myndigheter:

Vilka hinder har ni upplevt i arbetet med implementeringen?

> *För att kunna köra Zero Trust hela vägen måste man designa hela sin infrastruktur och sina applikationer på ett visst sätt. Har man inte det har man legacy-system, och då är det svårt och kräver otroligt mycket arbete. Det är helt enkelt bara att göra om och göra rätt från början i så fall. Jag tror det kommer bli en process där de allra flesta kommer gå stegvis alltmer mot en Zero Trust, men att vi kommer fortsatt ha kvar de gamla klassiska perimeterskydden kvar i vår infrastruktur över en överskådlig tid framöver i alla fall.*
>
> Respondent 2

> *Man är alltid beroende av externa parter som man inte har kontroll över. […] där har vi som köpare enbart kunna ställa krav som att det ska vara bra. Där faller ju själva Zero Trust grejen lite grann. När vi säger Zero Trust måste vi på något sätt ändå lita på att det funkar när någon loggar in […] Så någonstans handlar det om balansen mellan säkerhet och tillgänglighet eller konfidentialitet, riktighet och tillgänglighet. Har jag säkrat konfidentialiteten, då är jag nog rätt person hoppas vi, men vi kan inte vara för säkra för då minskar tillgängligheten för mycket.*
>
> Respondent 1

> *När det gäller IT-projekt så… den klassiska projekt-triangeln med kalendertid, resurser och pengar, funktioner. Vad ska man satsa på, satser man på det ena krymper det andra osv. Här har vi suttit i en situation med kriterier som man nästan aldrig har i projekt av den här formen, dvs. en tidpunkt då vi måste vara klara.*
>
> Respondent 1

Några frågor och svar från företag:

Vilka hinder har ni upplevt i arbetet med implementeringen?

> *Det är kostnadsbilden. Det finns aldrig outgrundligt med pengar eller en stor spargris att plocka pengar ur. Många vill sälja verktyg och produkter, och det är klart att man kan bunkra sig till tänderna, men det blir också en avvägande roll där just nu att det är fortfarande ganska kostsamt då […] Det är klart att jag inte är säker på att vår miljö är 100% skyddad men vi har gjort vad vi kan. med vår kunskap, vår budget där vi övervakar och vi gör det ena med det andra. Vi kan aldrig vara helt hundra. Nackdelen kan ju också vara att man väljer ett spår… sen bara ett halvår senare finns det ny metodik och nya möjligheter att skydda sig på nya sätt.*
>
> Respondent 4

> *[…] så har ju verkligen inte alla system eller leverantörer varit mogna att vara mottagliga för det heller.*
>
> Respondent 4

Skulle du kunna beskriva på vilka sätt de har varit hinder?

> *Vi har som mål att försöka jobba ett steg före och med verifiering från särskilt externa aktörer men det krävs ju också av egna medarbetare. Leverantörerna är också ett skäl, de är inte riktigt med på banan. Sen rent, den mänskliga faktorn, att människan också i grunden är lat. Vi vill ju bara att allt ska fungera och allt sådant här som jag vill lägga på eller förnya hur du identifiera dig, hur och vad som läses av och så där.*
>
> Respondent 4

> *Det absolut största problemet som jag upplever med att implementera Zero Trust det ligger helt klart på organisationsnivå. Det kan vara svårt att liksom, eller i vissa fall kan det krävas med Zero Trust, om man ska kunna implementera det krävs det stor teknisk kompetens av dels den anställde […] men sen kan det vara så att det är kostnadsfrågor där man kan ha svårt att motivera för en chef om chefen i sig inte är kunnig. Det är mycket pengar inblandat och det finns viss osäkerhet i själva besluten.*
>
> Respondent 3

Om data då färdas mellan molnet, on-premise servrarna och kanske även lokala enheter också för att få ihop ett helhetskoncept med Zero Trust för att täcka upp hela den här gruppen av data blir det inte direkt applicerbart för att det kan finnas osäkerheter och man kan inte från ledningens håll förstå sig på hur det fungerar och därför vill man inte kliva in på det tåget liksom.

Respondent 3

Företag som hjälper andra företag och myndigheter att implementera Zero Trust-lösningar fick svara på frågan vilka hinder, om några, som kan uppkomma under processen.

Vilka är de vanligaste hindren som ni stöter på vid implementationer av Zero Trust?

Den största utmaningen är att ha en bred och bra täckning, det är därför du behöver ha en prioritering på vad som behöver implementeras.

Lätt Zero Trust-tänkesätt kan du implementera enkelt, låt oss säga endast för dina kunder eller bara från jobbet, från jobbet till hemanvändare. Men när du vill täcka varje ruta som du ser, jag menar varje interaktion som pågår i din organisation, det är förmodligen inte möjligt. Du kan inte uppnå det ens på tre-fyra år. Det handlar om bra planering och bra prioriteringar.

Respondent 5

5.2 Analys

Inställning till ZT

Detta underkapitel kommer att analysera svaren som respondenter givit gällande studiens första frågeställning. Avsnittet kommer att delas upp i tre delar där de första två styckena kommer att analysera myndigheternas och företagens svar och sedan jämförs svaren i det tredje stycket.

Företag

Företagens inställning till ZT var delad. De är överens om att ZT är ett koncept som bör implementeras men att det är svårt, om inte omöjligt, att implementera det fullt ut. I teorin är det en bra säkerhetslösning men i det praktiska avseendet kan det vara en alldeles för krävande lösning. En respondent höjde vikten av att lita på sina anställda och att ha en bättre serverdrift snarare än ZT lösningar. En annan respondent tog upp att en sådan lösning kan bli ineffektiv för de som agerar i nätverket.

Myndighet

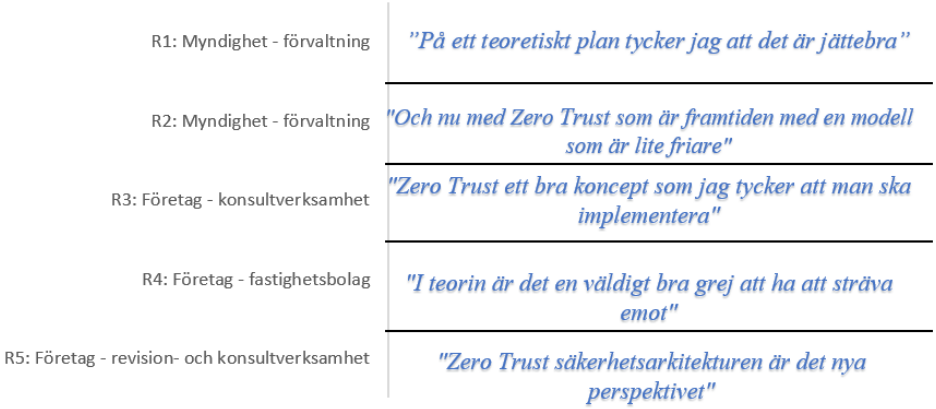
Myndigheternas inställning till ZT är välvillig till viss grad. De inser att vägen framåt inom nätverkssäkerhet är Zero Trust och förstår dess fördelar på ett teoretiskt plan. Respondenterna svarar att med tanke på säkerhetsläget i omvärlden måste deras legacy-system börja avvecklas och ersättas av någonting som är mer robust. I samband med detta har coronapandemin ändrat om kontors-landskapet där allt fler användare vill arbeta hemifrån. För detta behövs det ett nytt system som tillåter användare att komma åt myndighetens information och resurser från andra platser än kontoret och som kan både tillåta detta samtidigt som det håller säkerhetskraven som myndigheten begär.

Jämförelse av inställning

Både företag och myndigheter inser fördelarna med ZT som koncept för nätverkssäkerhet. Företagen verkar dock mer delade i sin inställning till att implementera det fullt ut på grund av dess komplexitet och svårigheterna som tillkommer för användarna av systemet. Å andra sidan verkar myndigheter vara mer positiva till ZT och inser att äldre system måste ersättas.

Figur 3

Inställning till Zero Trust



Sammanställning av svar som efter analys och jämförelse tyder på att det finns en positiv inställning till att implementera Zero Trust lösningar ur ett säkerhetsperspektiv.

Implementering av ZT och eventuella hinder

Detta stycke kommer att sammanställa respondenternas svar gällande studiens andra frågeställning. Stycket kommer att delas upp i tre delar där de första två delarna kommer att analysera svaren från företagen respektive myndigheterna och sedan jämförs de i det sista delen.

Företag

Inget av företagen har implementerat ZT som en helhetslösning. De använder det som lösning där det anses vara smidigt, snabbt och enkelt applicerbart. En respondent förklarade att det inte är möjligt att implementera ZT till 100% då det tillkommer enorma kostnader för att upprätthålla vissa av säkerhetskraven, men att de styr det på projektnivå. En annan respondent beskriver det som en effekt av pandemin, då det sedan dess inte har känts bra att ha enkla inloggningar, eller vissa passager öppna direkt in till kontoren. Av den anledningen har de implementerat ZT huvudsakligen på den administrativa sidan av företaget.

De två primära hindren som beskrivs är kostnadsbilden och avsaknad av kunskap på högre nivå i företagen. Det krävs en stor teknisk kompetens för att kunna implementera ZT-lösningar. Det kan vara svårt att motivera för en chef som inte är kunnig inom området att bekosta en dyr säkerhetslösning som är svår att förstå. De förklarar det som att man får göra det man kan med den kunskapen och budgeten som finns.

Ytterligare ett problem som nämns är externa aktörer som inte är framme i sin verksamhet att gå fullt ut ZT, vilket leder till att företagen själva inte kan applicera sådana lösningar i de delar där de externa aktörerna är viktiga.

Myndighet

Myndigheternas implementering av ZT särskiljs eftersom det finns skillnader i var de befinner sig i respektive genomförandeprocess. En myndighet svarade att de inte hade några legacy-system kvar i deras organisation. Denna utveckling gjordes då det gamla systemet, likt den klassiska lösningen som beskrivits i avsnitt 2.1, skötte allt. Det fanns ingen kontroll på vilka funktioner som gjorde vad och vilka API:er som anropade varandra. Detta system övergavs och i stället har de gått över till en mikrotjänst-arkitektur. Respondenten förklarade att ur deras perspektiv handlar ZT om att varje mikrotjänst ska kontrollera att användaren som skickar en begäran faktiskt har rätt att begära informationen och att detta sker under rätt former. Samma kontroll utförs vid transferering av data och begäran av data. Sammanfattningsvis används ZT som en helhetslösning i myndigheten.

Myndigheten har märkt av prestandaproblem efter implementeringen av ZT. Användare av systemet upplever att systemet känns "segt" och inte riktigt så bra som de hade hoppats på att det skulle vara. De är däremot inte helt säkra på ifall det är en bieffekt av ZT-lösningen eller något annat i systemet. De tryckte också på svårigheten med att implementera ett system som ZT med tanke på att de är beroende av externa parter. BankID togs upp som ett exempel som var integrerat i deras system. Respondenten tog upp problematiken med att ha ett system som inte litar på något, samtidigt som myndigheten i sig måste lita på en extern partner som man inte har någon kontroll över.

Den andra myndigheten har tidigare haft ett perimeterskydd men har börjat bygga förutsättningar för att kunna autentisera inom datacentret, autentisera API:er och tjänster som tidigare har varit oskyddade. De har tagit ett principiellt beslut att gå mot ZT men har ett enormt arv av system i infrastrukturen som bygger på föråldrade premisser. Detta innebär att övergången kommer att ta en längre tid men målet är att implementera nya funktioner utifrån ZT-modellen och dess principer. Sedan ska det gamla systemet stegvis avvecklas. Däremot kompletterade respondenten med att de troligtvis inte har orken med att göra om alla de gamla lösningarna.

Myndigheten har, traditionellt sett, haft mer fokus på brandväggar och vägen in till datacentret och åtkomsttjänster. Detta innebär att deras huvudsakliga hinder är att förflytta sig från en perimeter-baserad lösning till ZT, vilket blir ett för stort steg då det kräver att organisationen gör alla resurser och all information tillgänglig för alla oavsett plats, jämfört med att bara säkra upp nätverket inom kontoret. Gällande infrastrukturen inom nätverkssäkerheten svarade respondenten att det krävs mycket fokus på autentisering, single sign-on och certifikathantering, av vilka den kan ses som grundmekanismerna i autentiseringen.

Jämförelse

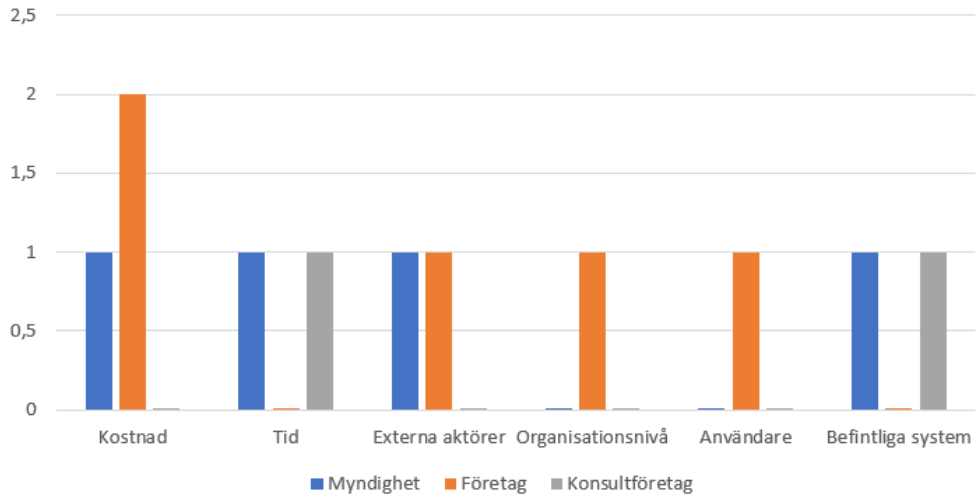
När det kommer till jämförelsen av hinder företagen och myndigheterna har upplevt, finns det många likheter. Ingen av dem upplever att Zero Trust är ett enkelt koncept eller att det går att överge de traditionella lösningarna över en natt. Zero Trust upplevs som en målbild att sträva mot i det långa loppet och är en process som fortgår under en längre period. Idag har delar av företagen och myndigheterna implementerat Zero Trustlösningar på ställen där det anses vara mer smidigt och lättare applicerbart.

De främsta hindren som är gemensamma för alla organisationer är kostnadsfrågan och de enorma tekniska kunskaperna som krävs för att lägga en bra grund för att kunna komma i gång med ZT. Det har även påpekats att hårdvaran som de använder i sina system ofta är ålderstigen och därför inte kompatibel med Zero Trust.

Sammanfattningsvis kan implementeringen av ZT-lösningar vara en tuff utmaning för både företag och myndigheter, och det finns olika strategier som kan användas beroende på säkerhetskrav och nuvarande system som används inom organisationen. Att implementera ZT som en helhetslösning kan anses vara den mest effektiva metoden för att uppnå hög säkerhet, men det kan också vara kostsamt och tekniskt utmanande. Att använda ZT på vissa delar i verksamheten kan vara en mer realistisk strategi. För myndigheter kan implementeringen av ZT vara mer komplex på grund av befintliga system och integration med andra teknologier.

Figur 4

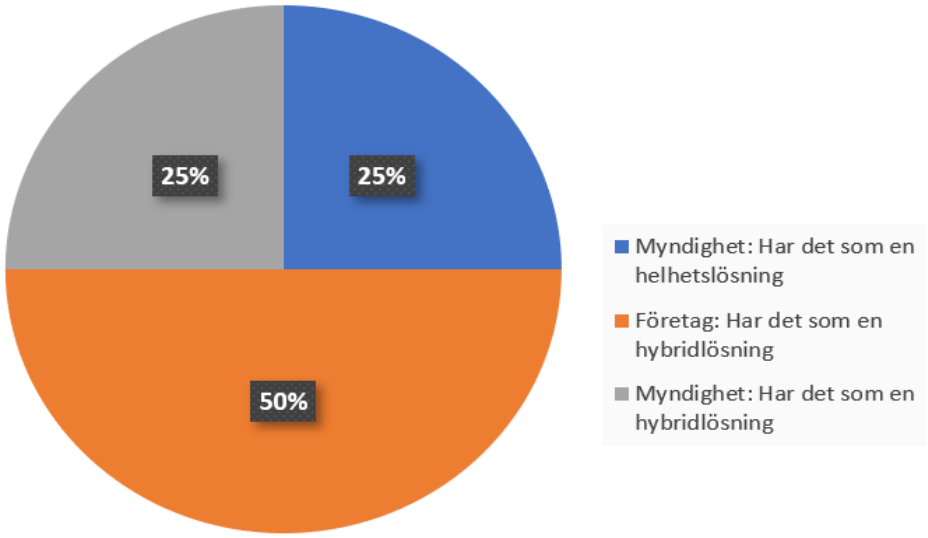
Hinder vid implementation



Diagrammet representerar en överblick vad gäller vilka hinder som upplevs när det kommer att implementera Zero Trust-lösningar i organisationerna. ”Myndighet” representeras av två myndigheter, ”företag” representeras av två företag, och ”konsultföretag” representeras av ett företag som hjälper andra organisationer att implementera ZT-lösningar.

Figur 5

Hur organisationen har implementerat Zero Trust



Diagrammet presenterar hur organisationerna implementerat Zero Trust i sina respektive verksamheter. De tre fälten representerar huruvida ett företag eller en myndighet har det som en helhetslösning eller om det bara har implementerats till viss del i en typ av hybridlösning med gamla system som jobbar i symbios med nya ZT-lösningar. Notera att konsultföretag som hjälper andra företag med ZT inte är med i diagrammet.

6 Diskussion

I detta kapitel behandlas empirin och dess respektive analys inom studien. Empirin och analysen av studien kommer att knytas samman med teorin. Därefter följer en diskussion om metoden där studiens metodik granskas och utvärderas.

6.1 Resultatdiskussion

Genom att applicera Zero Trust-lösningar kan man uppnå en imponerande skyddsnivå. Trots detta uppfattas det som en utmanande säkerhetslösning att använda som en helhetslösning. I detta avsnitt kommer inställningen till ZT, dess implementering samt hinder som förekommer i relation till ZT att diskuteras. Målet är att belysa svenska företags och myndigheters förhållningssätt till ZT.

Inställning

Resultatet av analysen kring insamlade data har visat att själva inställningen till Zero Trust inte skiljer sig nämnvärt beträffande jämförelsen mellan företagen och myndigheterna. I grund och botten finns det ingenting i respondenternas svar som tyder på annat än en positiv inställning till Zero Trust som koncept på det teoretiska planet. Samtliga respondenter som finns representerade i empirin, ser fördelarna med Zero Trust och inser att det är en lösning att eftersträva för att uppnå adekvat nätverks- och applikationssäkerhet. Efter analysen upplevs däremot viss skillnad vad gäller inställning till Zero Trust i praktiken. Myndigheten som implementerat Zero Trust fullt ut står stadigt i sin åsikt vad gäller att omställningen till Zero Trust är och kommer fortsätta vara rätt väg att ta.

Flera av respondenterna, oavsett om de är representanter från ett företag eller myndighet vittnar om att Zero Trust är en förflyttning från gamla system. För att minska risken att bli utsatta för attacker på företagets eller myndighetens nätverk behöver systemen uppdateras. Att företagen i sig var positiva till Zero Trust i grund och botten kom (Råsberg & Björkman, 2022) fram till i sin studie. Slutsatserna från den studien blev här bekräftade och kompletterade med att även myndigheterna är positivt inställda efter analysen av svaren från intervjuerna i den här studien.

Det finns, som tidigare nämnts, inga svenska studier kopplat till jämförelsen svenska företags och myndigheters inställning till Zero Trust. Konceptet som i USA har fått så pass stort genomslag att Vita Huset kommit ut med en order att Zero Trust ska införas för bästa möjliga säkerhet (Biden, 2021) är också eftersträvansvärt i Sverige. Den här studien bevisar att det finns en välvilja bland både företag och myndigheter kopplat till konceptets implementation. Det som däremot skiljer sig åt är huruvida det är applicerbart fullt ut eller bara applicerbart på enstaka delar av

nätverkssystemen beroende på diverse hinder som förklaras nedan under rubriken ”Hinder”.

Implementering

Resultatet av insamlad data gällande implementation av ZT visar att det verkar finnas en viss skillnad mellan hur företag och myndigheter har valt att implementera ZT. Inget av företagen har implementerat ZT som en helhetslösning, då kostnaden för att bygga om nätverksarkitekturen till en ZT-arkitektur, samt upprätthålla nätverket ökar till nivåer som företagen inte har råd att med. En annan faktor har varit pandemin. På grund av att allt fler har börjat jobbat hemifrån har man insett att enkla inloggningar och direkta portar in till kontoret inte är adekvata lösningar längre. I stället implementerar företagen ZT i den utsträckning det anses vara en smidig och enkel lösning jämfört med tidigare system men som fortfarande stärker företagets säkerhet.

På myndigheternas sida fanns det en skillnad mellan de olika myndigheternas strävan att implementera ZT till 100%. Det finns flera faktorer som ligger bakom detta, men den faktor som har störst påverkan är hur mycket av myndigheternas system som fortfarande körs med legacy-nätverk. Ena myndigheten har valt att bygga om sitt nätverk från ett legacy-nätverk till ett ZT-nätverk, medan den andra myndigheten har valt att applicera ZT-lösningar på det existerande nätverket och i framtiden ha en hybridlösning.

Generellt visar svaren att det överensstämmer med det (Rose, Borchert, Mitchell, & Connelly, 2020) tar upp i sin studie om att en övergång till ZT är en välkalkylerad resa jämfört med en enkel ersättning av hård- och mjukvara på en storskalig nivå. Vidare bekräftar även företagens och ena myndighetens val att inte implementera ZT fullt ut med det som (Rose, Borchert, Mitchell, & Connelly, 2020) skriver i sin studie, nämligen att organisationer ibland väljer att inte implementera ZT fullt ut, utan fortsätter att köra med en hybridlösning mellan ZT och en perimeterbaserad lösning, då det tillåter organisationen att fortsätta investera i framtida IT-moderniseringsinitiativ.

Det som är anmärkningsvärt gällande dessa resultat är skillnaden i viljan att implementera ZT som helhetslösning mellan företag och myndigheter. Företagen lutar mer åt (Rose, Borchert, Mitchell, & Connelly, 2020) rekommendationer att implementera en hybridlösning för att fortfarande ha tillgångar att investera i framtida säkerhetslösningar. Myndigheterna å sin sida är splittrade, där ena myndigheten har implementerat ZT fullt ut i sin nätverksarkitektur och den andra myndigheten har utvecklat en hybridlösning. Enligt (Rose, Borchert, Mitchell, & Connelly, 2020) anses en implementation av ZT till 100% inte vara hållbart för myndigheter och företag med ett befintligt nätverk. (Rose, Borchert, Mitchell, & Connelly,

2020) förklarar dock vidare att det finns tillfällen då en organisation blir ombedd att uppfylla ett nytt ansvar som i sin tur kräver att man bygger den egna infrastrukturen från grunden igen. I dessa fall kan det vara möjligt att implementera ZT i den nya infrastrukturen. Detta motsvarar de resultat som myndigheter givit under studien och som tidigare har sagt att de har behövt byta ut sina legacy-system mot en ny infrastruktur som kommer att hålla länge samt att detta kommer uppfylla de säkerhetskrav som nu ställs på organisationer jämfört med tidigare.

Ett av studiens syften är att undersöka hur svenska organisationer har tillämpat ZT-lösningar samt hur de har gått tillväga. Med hjälp av intervjuerna samt teorin bakom, kan det konstateras att företagen har tillämpat hybridlösningar. Detta innebär att företagen och myndigheten både kan åtnjuta det senaste inom säkerhetsvärlden, samtidigt som man inte helt kastar ut det tidigare, vilket medför att företagen fortfarande kan investera i nya möjligheter och anta ett nytt säkerhetssystem i framtiden. Myndigheten som implementerat ZT fullt ut kan antas ha fått ett direktiv att bygga en ny nätverksarkitektur som klarar av de förhöjda säkerhetskraven som ställs på organisationer runt om i världen. På grund av de legacy-system som fanns tidigare hos myndigheten kan man dra slutsatsen att nybyggnad var att föredra framför ombyggnad.

Hinder

I studiens teoretiska utgångspunkt presenteras interna och externa hinder. De interna hinder som presenteras är utbytet av cybersäkerhetsinformation mellan olika aktörer och tillitsnivån inom ZT-system. De externa hinder som presenteras är kostnad, arbetsflöde för användare och BYOD.

Med hjälp av studiens empiri identifierades också, utöver de som identifierades i teorin, teknisk kunskap och tid som möjliga hinder. Hindren som har identifierats kommer presenteras och diskuteras under respektive rubrik.

Kostnads- och tidsutmaningar

En betydande utmaning som identifierats i samband med införandet av ZT-arkitekturen är dess höga kostnad. Denna utmaning beror inte endast på ekonomiska faktorer för organisationer, utan även på en brist i tillgängliga resurser i form av tid och arbetskraft. Kostnaden i form av tid avspeglar den diskussionen som presenteras av (Teerakanok, Uehara, & Inomata, 2021) i deras artikel om övergången till ZT-arkitektur, där de noterar att ZT-implementeringen är en utdragen och kostsam process. Författarna påpekar också att, på grund av den utdragna och kostsamma lösningen, har företag valt att anlita hjälp från tredjepartsleverantörer för implementering av ZT-lösningar, vilket ibland leder till att organisationen blir låst till leverantören som tillhandhåller lösningen.

Respondenterna som ingår i denna studie har inte sökt hjälp från tredjepartsleverantörer och därför kan inte denna studie påvisa att det är något som organisationer ser som ett hinder. Däremot håller respondenterna med om att en övergång till ZT som en helhetslösning utgör en kostsam och krävande process. Respondenterna visar att en betydande respekt och medvetenhet om att det finns många delar i deras system som behöver bytas ut att detta medför betydande kostnader. Majoriteten av respondenterna understryker att de har fattat beslut om att anta ZT. De har dock en betydande mängd befintliga system, vilket medför att övergången till ZT kommer att ta tid samt resurser och de implementerar därför ZT endast där det är mest lämpligt. Tillsammans med den finansiella tröskeln utgör dessa faktorer därmed hinder för de flesta organisationer att fullständigt införa ZT som helhetslösning.

Teknisk expertis och användarvänlighet

Det andra hindret som uppmärksammats med införandet av ZT är bristande teknisk kompetens och användarvänlighet. Två av respondenterna påpekade organisatoriska problem som anses vara utmanande. Det krävs en hög teknisk kompetens från både anställda och ledningen. Motivationen för ledningen att införa ZT anses vara problematisk på grund av bristande kunskap om ämnet och de höga kostnaderna som är involverade. Även om studiens respondenter inte angav avsaknad av teknisk kompetens bland anställda som ett hinder är de medvetna om att kompetens ör ett måste.

I avsnitt 4.1 diskuteras olika typer av implementeringsprocedurer i samband med ZT. Eftersom det finns olika teoretiska tillvägagångsätt behöver det finnas tydliga ramverk för att under lätta för IT-ansvariga som vill genomföra en fullständig ZT-implementering. (Rose, 2022) påpekar att implementeringen och underhållet av en fullständig ZT-lösning är ett pågående projekt som aldrig upphör. Det kräver därför stort tålamod och en ständig uppdatering av IT-personalen för att säkerställa säkerheten i företaget eller myndigheten. Enligt rapporterna från både (Rose, 2022) och (Splunk, 2022) kan man observera att det fortfarande finns ett gap mellan den teoretiska implementeringen och det praktiska genomförandet av ZT. Detta kan skrämma flera organisationer från att implementera ZT, då det fortfarande finns flera stora frågetecken som behöver besvaras innan ZT kan anses tillräckligt användarvänligt för att kunna implementeras fullt ut hos organisationer.

(Teerakanok, Uehara, & Inomata, 2021) förklarar i sin artikel att när en användare eller enhet skickar en förfrågan om att få tillgång till organisationens resurser, behöver ZT-systemet beräkna enhetens tillitsnivå och jämföra den med gränsen som är satt inom systemet. Att beräkna tillitsnivån är en resurskrävande process, och en för hög tillitsnivå kan påverka organisationens arbetsflöde. Detta kan knytas an till en av

respondenterna som implementerat ZT som en helhetslösning i sin organisation, och som påpekade att systemet upplevs som långsamt. Respondenten menar att problemen som uppstod efter implementationen och troligtvis beror på att systemet behöver verifiera alla enheter som försöker nå resurser. En annan respondent såg det som ett hinder för att implementera ZT som en helhetslösning då det kan vara krävande för medarbetare eller andra användare som agerar i nätverket.

Externa aktörer

(Rose, 2022) betonar i sin rapport vikten av säker kommunikation både inom organisationens datacenter och vid anslutning från externa platser. Endast närvaron av en enhet eller resurs på organisationens fysiska plats ska inte garantera dess säkerhet. I stället måste all kommunikation skyddas med åtgärder för konfidentialitet och integritet. Detta kan dock skapa problem om organisationen är beroende av externa aktörer som de inte har kontroll över. Respondenter från både myndigheter och företag uttryckte att de är beroende av externa aktörer, såsom mjukvara eller leverantörer, och att dessa inte alltid är mottagliga för ZT, vilket i sin tur kan påverka organisationens säkerhet.

6.2 Metoddiskussion

Studien har fokuserat på ett litet urval av svenska myndigheter och företag som presenterats i avsnitt 3.4. Ståndpunkten är att urvalet av respondenter med ämneskompetens inom Zero Trust är en nyckelfaktor för att intervjuerna skulle vara relevant för studien. Syftet med undersökningen har varit att få en bild av Zero Trust i Sverige.

Ett mindre antal respondenter har möjliggjort en mer djupgående analys av resultaten från varje enskild intervju. Inom ramen för den semistrukturerade intervjuguiden, som beskrivs i avsnitt 3.4, har intervjufrågorna kunnat varieras något. Detta har öppnat upp möjligheten för mer personliga och interaktiva samtal med utrymme för flexibilitet. Frågorna i undersökningen har utformats så att de inte har påverkat respondenternas svar. Respondenterna har haft möjlighet att ge svar som inte endast har varit enkla och tydligt positiva eller negativa inställningar till Zero Trust. Det har varit möjligt att generalisera svaren till en viss grad, vilket gör att de kan anses tillämpliga och representativa för svenska företag och myndigheter.

Det kan diskuteras om det faktum att antalet respondenter var lågt ledde till att svaren gavs med liknande inriktningar, och medvetenheten om att detta kan påverka studiens validitet finns i åtanke. Om studien hade fortsatt under en längre tid, hade förhoppningarna varit att fler respondenter hade ställt upp, och andra typer av undersökningar, såsom paneldiskussioner, hade genomförts för att stärka slutsatserna.

Andra metoder som var tillgängliga men aktivt valdes bort som beskrivs i avsnitt 3.1, var kvantitativa undersökningar, till exempel enkäter. Beslutet grundades på en oro för att respondenter utan tillräcklig kunskap om Zero Trust skulle påverka resultaten negativt ur en trovärdighetssynvinkel. För att en sådan metod skulle vara tillämplig skulle det krävts stora mängder data. Med tanke på att Zero Trust-arkitekturen är en relativt okänd lösning på ett aktuellt och komplext problem, finns det en överhängande risk att svarsfrekvensen skulle varit för låg.

7 Slutsats

Hur skiljer sig inställningen till Zero Trust mellan svenska myndigheter och svenska företag?

Baserat på teorin och empiriska data i studien, finns det ingen indikation på någon skillnad i inställningen gentemot Zero Trust mellan myndigheter och företag i Sverige. Trots att det existerar vissa åsiktsskillnader rörande lämpligheten och möjligheten att implementera Zero Trust som en helhetslösning eller endast på delar av befintliga system, är både myndigheter och företag positivt inställda till konceptet Zero Trust.

Hur har svenska organisationer som tillämpat Zero Trustlösningar gått tillväga och hur har eventuella hinder hanterats?

Svenska organisationer har valt att tillämpa Zero Trust på olika sätt, beroende på om organisationen är ett företag eller en myndighet. Samtliga företag och en av myndigheterna har valt hybridlösningar, vilket innebär att de har infört Zero Trust-lösningar men samtidigt behållit sin tidigare perimeterbaserade säkerhetslösning. Detta tillvägagångssätt gör det möjligt för dem att fortsätta investera i Zero Trust-baserade säkerhetslösningar i framtiden. Den andra myndigheten har valt att implementera Zero Trust som en integrerad lösning genom att gå ifrån deras äldre nätverksarkitektur till en helt ny arkitektur som bygger helt och hållet på ZT-teknologi.

7.1 Framtida forskning

Med studien finns det en förhoppning att fler väljer att bryta ned Zero Trust och forska mer djupgående inom området. Eftersom det är ett relativt nytt koncept är det fortfarande ett stort outforskat fält som behöver nya rön. I takt med att studien framskridit, har ytterligare frågor uppstått vilka kan betraktas som områden med hög potential för framtida forskning.

Denna studie fokuserar på svenska företag och myndigheter men har teoridelar med nästan enbart publikationer och artiklar som är från övriga delar av världen. Det finns alltså anledning att jämföra Sverige med det som sker utanför Sveriges landsgränser. Det vill säga att förslagsvis jämföra Europa med Nordamerika eller Asien för att sedan eventuellt smalna av området till enstaka länder, exempelvis att jämföra inställningen i USA med Sverige.

En viktig, del kopplat till hinder vid implementering av Zero Trust, var gamla system och kostnadsfrågan vad gäller att byta ut dem till nya. Att fortsätta forska kring området, hur man implementerar Zero Trust i gamla system eller vilka system som behöver bytas ut för att ta steget till att implementera Zero Trustlösningar är något som skulle kunna hjälpa företag och myndigheter att ta steget vidare.

För att få fler företag och myndigheter att bli uppmärksamma på Zero Trust och få dem att överväga att implementera sådana lösningar finns det behov av mer konkreta jämförelser. Exempelvis går det att genomföra experiment med personer som besitter expertis inom området för att göra en jämförelse kring hur svårt eller enkelt det är att ta sig in i system med Zero Trust respektive traditionella nätverkslösningarna.

Referenser

Alsaawi, A. (2014). A Critical Review of Qualitative Interviews. *European Journal of Business and Social Sciences, Vol. 3, No. 4*.

Biden, J. R. (den 12 Maj 2021). Executive Order on Improving the Nation's Cybersecurity. Washington DC, USA. Hämtat från https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/ den 15 Februari 2023

Busetto, L., Wick, W., & Gumbinger, C. (2020). How to use and assess qualitative research methods. *Neurological Research and Practice*. doi:10.1186/s42466-020-00059-z

Chuan, T., Lv, Y., Qi, Z., Xie, L., & Guo, W. (Ausgusti 2020). An Implementation Method of Zero-trust Architecture. *International Conference on Artificial Intelligence Technologies and Application (ICAITA). 1651*. Dalian: IOP Publishing Ltd. doi:10.1088/1742-6596/1651/1/012010

Creswell, J. W., & Creswell, J. D. (2018). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches* (5 uppl.). Los Angeles: SAGE Publications.

DeJonckheere, M., & Vaughn, L. M. (2019). *Semistructured interviewing in primary care research: a balance of relationship and rigour*. Family medicine and community health. doi:10.1136

Falowo, O. I., Popoola, S., Riep, J., Adewopo, V. A., & Koch, J. (2022). Threat Actors' Tenacity to Disrupt: Examination of Major Cybersecurity Incidents. *IEEE Access, 10*. doi:10.1109/ACCESS.2022.3231847

FMV, FRA, Försvarsmakten, MSB, Polisen, PTS, Säkerhetspolisen. (2020). *Cybersäkerhet i Sverige 2020 - Rekommenderade säkerhetsåtgärder*. Post- och telestyrelsen (PTS).

Försvarsmakten. (2022). *Cyberangrepp största hotet just nu*. Försvarsmakten. Hämtat från https://www.forsvarsmakten.se/sv/aktuellt/2022/03/cyberangrepp-storsta-hotet-just-nu/ den 11 Mars 2023

Furstenau, L. B., Sott, M. K., Homrich, A. J., Kipper, L. M., Aziz Al Abri, A., Cardoso Flores, T., . . . Cobo, M. J. (2020). 20 Years of Scientific Evolution of Cyber Security: a Science Mapping. *International Conference on Industrial Engineering and Operations Management*, (pp. 2-8). Dubai.

He, Y., Huang, D., Chen, L., Ni, Y., & Ma, X. (2022). A Survey on Zero Trust Architecture: Challenges and Future Trends. *Hindawi*. doi:10.1155/2022/6476274

Homeland Department of Security, K.D, Uttecht. (2020). *Zero Trust Concepts for Federal Government Architectures.* Lexington, MASS: Massachusetts Institute of Technology. Hämtat från https://apps.dtic.mil/sti/pdfs/AD1106904.pdf den 13 03 2023

Hosney, E. S., Halim, I. T., & Yousef, A. H. (2022). An Artificial Intelligence Approach for Deploying Zero Trust Architecture (ZTA). *5th International Conference on Computing and Informatics (ICCI).* Cairo.

Kindervag, J. (2010). *Build Security Into Your Networks DNA: The Zero Trust Network.* Cambridge: Forrester.

Lewis-Beck, M. S., Bryman, A., & Liao Futing, T. (2004). *The SAGE Encyclopedia of Social Science Research Methods.* Sage Publications. doi:10.4135/9781412950589

Mehraj, S., & Banday, M. T. (2020). Establishing a Zero Trust Strategy in Cloud Computing Environment. *International Conference on Computer Communication and Informatics (ICCCI)* (p. 6). Coimbatore, Indien: IEEE. doi:10.1109/ICCCI48352.2020.9104214

Nace, L. (2020). Securing Trajectory based Operations Through a Zero Trust Framework in the NAS. *2020 Integrated Communications Navigation and Surveillance Conference (ICNS).* doi:10.1109/ICNS50378.2020.9222912

Olsson, J., Shorov, A., Abdelrazek, L., & Whitefield, J. (2021). *5G Zero Trust - A Zero-Trust Architecture for Telecom.* Ericsson Technology Review.

Palinkas, L. A., Horwitz, S. M., Green, C. A., Wisdom, J. P., Duan, N., & Hoagwood, K. (2015). Purposeful Sampling for Qualitative Data Collection and Analysis in Mixed Method Implementation Research. *Administration and policy in mental health, 42(5)*.

Råsberg, F., & Björkman, J. (2022). *Inställningen till Zero Trust på svenska företag.* Jönköping: Tekniska Högskolan i Jönköping inom informatik.

Rose, S. (2022). *Planning for a Zero Trust Architecture: A Planning Guide for Federal Administrators.* NIST. doi:doi.org/10.6028/NIST.CSWP.20

Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero Trust Architecture. Retrieved 02 12, 2023, from https://doi.org/10.6028/NIST.SP.800-207.

Samaniego, M., & Deters, R. (2018). Zero-Trust Hierarchical Management in IoT. *IEEE International Congress on Internet of Things (ICIOT).* San Francisco.

SCB. (2021). Köp av molntjänster efter typ av tjänst. Andel företag. År 2021. Retrieved April 17, 2023, from https://www.statistikdatabasen.scb.se/pxweb/sv/ssd/START__NV__NV0116__NV0116D/KopMolnTjanst/

Shore, M., Zeadally, S., & Keshariya, A. (2021, Oktober 25). Zero Trust: The What, How, Why, and When. *Computer, 54*(11). doi:10.1109/MC.2021.3090018

Souppaya, A. K., Symington, S., Scarfone, K., & Barker, W. (2022, December). Implementing a Zero Trust Architecture. *E*. Retrieved April 17, 2023

Splunk. (2022). *The Essential Guide to Zero Trust.* Splunk.

Teerakanok, S., Uehara, T., & Inomata, A. (2021). Migrating to Zero Trust Architecture: Reviews and Challenges. *Security and Communication Networks.* doi:doi.org/10.1155/2021/9947347

Uctu, G., Alkan, M., Alper, D. İ., & Dörterler, M. (2019). *Perimeter Network Security Solutions: A survey.* IEEE. doi:10.1109/ISMSIT.2019.8932821

Van Der Ham, J. (2021). Toward a Better Understanding of "Cybersecurity". *Digital Threats: Research and Practice, 2*(3), 1-3. doi:10.1145/3442445