Guide

6 trin til implementering af Zero Trust-principperne

En guide til CISO'er og IT-chefer i Danske virksomheder

wingmen

part of springboardnetwork

Powering your secure digital future

Indhold

Kenneth Thorsted

Senior Security Advisor

Kenneth er ekspert i at forene teknologi og forretningsudvikling, og mestrer spændingsfeltet mellem teknologisk fremskridt og forretningsmæssige prioriteter. Med solid baggrund inden for IT-sikkerhed og dybdegående ekspertise inden for cybersikkerhedsrådgivning, især med fokus på Cisco-sikkerhedsløsninger, bidrager han med unikke kompetencer.

Trin 1: Identity & People - kontinuerlig validering

Grundstenen i Zero Trust-principperne ligger begrebet ”least privilege access,” hvilket sikrer, at brugerne kun har adgang til de ressourcer, der er nødvendige for deres roller. Identity and People fokuserer på at validere og løbende verificere identiteten af personer, der får adgang til netværket, tjenesterne eller dataene. Dette opnås gennem multifaktorautentificering (MFA) og etablering af bruger-trust. Ved at bevæge sig væk fra traditionel adgangskodebaseret godkendelse og vedtage MFA kan virksomheder beskytte mod kompromitterede legitimationsoplysninger, phishing-angreb og andre password-relaterede trusler.

Fordele

Forbedret sikkerhed

MFA reducerer risikoen for uautoriseret adgang og databrud betydeligt.

Omkostnings-effektivitet

Implementering af MFA giver it-afdelinger mulighed for at allokere ressourcer til andre kritiske områder.

Brugeren i centrum

Passive metoder som biometri og softwaretokens tilbyder enklere og friktionsfri logins til brugerne.

Identity and People er afgørende i din sikkerhedsstrategi for at opbygge et robust Zero Trust-miljø. Ved at sikre, at kun autoriserede brugere med pålidelige enheder kan få adgang til kritiske ressourcer, skaber du et stærkt fundament for din modstandsdygtighed over for sikkerhed.

Trin 2: Device -
Kontrol af enheders "trust" og "hygiejne"

I dette trin bevæger Zero Trust sig fra et fokus på brugerne til de enheder, de bruger til adgang, uanset om de er virksomhedsejede eller personlige. Sikring af disse enheders integritet og opretholdelse af compliance, inden der gives adgang, er en afgørende part i jeres sikkerhedsværn. Organisationer bør registrere og vurdere alle enheder, der opretter forbindelse til deres netværk, og validere, at de opfylder sikkerhedskravene. En compliant enhed er mindre tilbøjelig til at blive kompromitteret, hvilket reducerer de samlede sikkerhedsrisici.

Fordele

Proaktiv beskyttelse

Kontrol af device-integritet hjælper med at identificere og afværge potentielle trusler, før de eskalere

Avanceret Endpoint Detection & Response (EDR)

Moderne løsninger går ud over traditionel antivirusscanning og giver mere robust sikkerhed, da de kan ser anomali, og rapportere ind til fælles "source of truth" data-lake.

Cloud-native sikkerhed

Cloud-baserede sikkerhedsløsninger som SASE tilbyder forbedret beskyttelse til fjernadgangsscenarier.

Sikring af enheder er ikke en mulighed; Det er en nødvendighed. Ved at implementere foranstaltninger til kontinuerligt at bekræfte enhedstilstanden, styrker du dit forsvar mod en lang række cybertrusler.

Trin 3: Network - centralnervesystemet

Et sikkert netværk er et grundlæggende element i Zero Trust. Det indebærer at analysere og kontrollere alle forbindelser over netværket, identificere potentielle trusler og opretholde synligheden af brugere og enheder. Segmentering, trafikanalyse og applikationsydeevne er nøglekomponenter i netværksinfrastrukturen, der sikrer, at der gives adgang baseret på verificeret identitet og enhedstillid.

Fordele

Central netværks-administration

Et centralt styret og programerbart netværk giver mulighed for nem implementering og overvågning af politikker.

Telemetri og håndhævelse

Netværket kan fungere som telemetrikilde for dataindsamling og håndhævelse for sikkerheds-foranstaltninger

Registrering af adgangs-overtrædelse

Anomalier i trafik, adgangsforsøg og datamængder kan fremhæve kompromitterede enheder og potentielle trusler.

Investering og udvikling af et sikkert netværk, der håndhæver politikker baseret på identitet- og enhedsverifikation, er afgørende for at opretholde et robust Zero Trust-økosystem.

Trin 4: Workload -
sikring af applikationer og systemer

Workload sikkerhed fokuserer på at beskytte applikationer og systemer, uanset om de er placeret i datacentre eller cloudmiljøer. Synlighed i services, applikationsmoduler og trafikmønstre gør det muligt for organisationer at anvende effektiv segmentering og beskytte workloads mod potentielle trusler. Mikrosegmentering og hostbeskyttelseskontroller spiller en afgørende rolle i sikringen af hele stakken af programniveauer.

Fordele

Ensartet beskyttelse

Opnå lige så robust beskyttelse i Cloud-baserede løsninger som i lokale datacentre.

Data dependency Insights

Forståelse af dataflow hjælper med at træffe informerede beslutninger og styrker databeskyttelsen.

Trusselsdetektion i applikationer

Indikatorer for kompromittering kan detekteres på forskellige lag, hvilke forbedrer sikkerheden.

Beskyttelse af dine workloads, uanset deres placering i Kubernetes, Docker eller VMware, er afgørende i dagens dynamiske trusselslandskab. Fokus på workload sikkerhed sikrer, at dine programmer og systemer forbliver beskyttet mod potentielle sårbarheder.

Trin 5: Data -
beskyttelse af organisationens livsnerve

Data er livsnerven i enhver organisation, og beskyttelse af dem bør være en topprioritet. Datasikkerhed omfatter kategorisering, mærkning og beskyttelse af data på enheder, i applikationer og under overførsel. Implementering af foranstaltninger til at forebygge datatab og detektering af eksfiltreringsforsøg er væsentlige aspekter i at sikre følsomme oplysninger.

Fordele

Omfattende databeskyttelse

Klassificering og kategorisering af data gør det muligt effektiv at sikrer korrekt beskyttelse uanset deres placering.

Datasynlighed

Forståelse af datalagring og adgangs-foranstaltninger til at opdage uregelmæssigheder og potentielle trusler.

Kryptering & forebyggelse af datatab

Beskyttelse af data under transit og detektering af uautoriserede forsøg beskytter følsomme oplysninger.

Datasikkerhed er afgørende for at sikre fortroligheden og integriteten af din organisations aktiver. En datacentrisk tilgang udgør en vigtig del af din Zero Trust-strategi.

Trin 6: Security Operations - grundlaget for Zero Trust

Endelig er robust Security Operations dit cockpit i et Zero Trust-miljø. En omfattende sikkerhedsdrift integrerer synlighed fra flere kilder, hvilket muliggør risikobevidste beslutninger og automatiserer detektions- og responshandlinger. Ved at prioritere trusler, forbedre arbejdsgangen og reducere den gennemsnitlige tid til at reagere, spiller operation for jeres sikkerhed en afgørende rolle i at opretholde en robust sikkerværn.

Fordele

Historiske logs/events

Logning og rapporterings-hjælp i forensics og undersøgelser.

Automatiseret respons

Integration af detektionsteknologier med forebyggelses-funktioner minimerer responstiden.

Playbook design

At have foruddefinerede responsprotokoller sikrer effektiv trusselsstyring.

Robust Security Operations er afgørende for at implementere og vedligeholde en effektiv Zero Trust-strategi, hvilket sikrer, at din organisation er klædt på til at forsvare sig mod avancerede trusler.

Zero Trust
vejen til sikkerhed

Adoption af Zero Trust er en nødvendighed i dagens cyberlandskab. Ved at følge de seks trin i denne guide kan din virksomhed mindske risici og reagere effektivt på skiftende trusler. Husk, at nøglen til en succesfuld Zero Trust-implementering ligger i kontinuerlig validering, overvågning og proaktiv sikkerhed. Med Zero Trust kan sikkerhedsarbejdet afgrænses, og organisationer kan beskytte deres digitale fremtid.

Er din organisation klar til at beskytte sig mod avancerede angreb?

Hos Wingmen er vi specialiserede i at implementere og vedligeholde avancerede cybersikkerhedsløsninger. Vores ekspertise strækker sig over endpoint-sikkerhed, netværkssikkerhed, cloud-sikkerhed og mere. Vi tilbyder managed security services døgnet rundt, der sikrer hurtig detektion, menneskelig analyse og ekspertrespons. Vores mål er at forbedre din organisations cybersikkerhed ved at implementere de rette teknologier, etablere sikkerhedspolitikker og træne dit personale.

Kontakt mig for at styrke din organisations cybersikkerhed og beskytte din digitale forretning.

Kenneth Thorsted
Senior Security Advisor

Email: kth@wingmen.dk

Tlf: +45 30385531

wingmen
part of springboardnetwork

Cisco Partner