DELL Technologies

5 Rekommendationer för hantering av nollförtroendebehov

1	2	3	4	5
Planera för paradigmskiftet till att ”lite aldrig på något, verifiera alltid”	**Bestäm önskad väg**	**Organisationen driver nollförtro-endemiljön, inte tvärtom**	**Fokusera på data**	**Implementera ”lita aldrig på något, verifiera alltid” i hela IT-ekosystemet**
Fastställ en acceptabel kompromiss mellan riskreducering och affärspåverkan	Inkrementell säkerhetsförbättring	Skapa kontroller utifrån verksamhetens behov	Se till att all nätverks-, enhets- och användaraktivitet loggas kontinuerligt	Nollförtroendeaktivi-teter såsom flerfaktor-sautentisering och identitetshantering måste tillämpas universellt för att undvika kritiska luckor
Ta hänsyn till kostnader, inverkan på drift och intressenter samt överensstämmelse-krav och lagstadgade krav	Hyperskala	Dokumentera processer, roller, ansvarsområden och dataklassificeringar	Använd AI och ML för att analysera data och identifiera avvikelser som kan indikera hot	Inkludera fysiska och digitala leverantör-skedjor från tredje part i nollförtroender-amverket
Gå från perimeterbaserad säkerhet till en mikrosegmenterad, datacentrerad modell	Dedikerad miljö	Användarupplevelsen är fortfarande avgörande	Tänk på att skydd av data och program är nyckeln i en nollförtro-endearkitektur	
Ta hjälp utifrån om det behövs	Identitet är den nya perimetern	Säkerhetsförbättringar som nollförtroende får inte ske på bekostnad av användbarheten		
		Organisatoriska mål som tillväxt och innovation är fortfarande av största vikt		

Nollförtroende anses generellt sett vara den bästa sortens säkerhetsarkitektur.

Data visar att de flesta organisationer har börjat fundera på eller håller på att implementera nollförtroende[1]. Även om övergången till nollförtroende är omfattande finns det några praktiska överväganden som kan hjälpa dig på vägen.

Dell Technologies ämnesexperter Tracy Emmersen, Director of Solution Adoption for Project Fort Zero, och Justin Vogt, Principal Security Engineer, delade med sig av sina rekommendationer och insikter till Ash Lakshmanan, Security Services Product Manager. Deras viktigaste förslag sammanfattas nedan, eller så kan du se hela deras konversation på dell.com/cybersecuritymonth.

> När vi tittar på nollförtroende ur en holistisk synvinkel och tar ett steg tillbaka handlar allt verkligen bara om data.”
>
> ***Tracy Emmersen***
> *Director of Solution Adoption for Project Fort Zero, Dell Technologies*

Planera för det (stora) paradigmskiftet till att ”lite aldrig på något, verifiera alltid”

I sin mest grundläggande form innebär övergången till en nollförtroendemiljö ett omfattande skifte från historiska säkerhetsmodeller till en som baseras på principerna om att ”lita aldrig på något, verifiera alltid” och åtkomst med lägsta behörighet. ”Vi måste se på vår säkerhetsställning på ett annat sätt än tidigare, komma bort från traditionella perimeterbaserade nätverkssäkerhetslösningar och röra oss mer mot en mikrosegmenterad, datacentrerad arkitektur”, konstaterar Emmersen.

Bestäm önskad väg

Emmersen förklarade tre olika sätt att uppnå fördelarna med nollförtroende:

- **Inkrementell:** En iterativ metod som tar in viktiga nollförtroendeprinciper i den aktuella miljön
- **Hyperskalare:** Utnyttjar nollförtroendefunktionerna hos de stora molnleverantörerna
- **Dedikerad, helt kompatibel miljö:** Privat miljö på plats som är byggd från grunden, strikt i enlighet med nollförtroendestandarder

Utöver dessa tre vägar kan virtualiserade små och medelstora företag också använda en metod som kallas ”Identitet är den nya perimetern”. Den här metoden fokuserar på identitets- och åtkomsthantering och använder SaaS-verktyg för att uppnå nollförtroendebaserat skydd. En viktig komponent i den här metoden är att implementera flerfaktorautentisering (MFA) överallt, vilket illustrerar effekten av just den här nollförtroendefunktionen.

Hyperskalnings- och identitetsmetoderna är vanligtvis billigare, medan de inkrementella och dedikerade miljöerna kräver större investeringar.

Det är organisationen som driver implementeringen av nollförtroende, inte tvärtom

I grunden är en nollförtroendearkitektur utformad för att administrera och skydda en organisations arbetsflöden, användarroller och relaterade behörigheter, enheter, data, program och nätverk. Den första delen av en implementering kräver robust dokumentation av dessa aspekter, och sedan är kontrollplanet och infrastrukturen utformade för att verkställa de principer som styr dem.

Om nollförtroendemiljön hämmar eller avsevärt ändrar affärsverksamheten till skada för organisationen är den förbättrade säkerhet som uppnås sannolikt inte värt det. Som Vogt påpekar: ”Om [säkerhet] … står i vägen för organisationens kärnuppdrag … är vi egentligen inte bättre än de motståndare som vi försöker hindra. Vi ordnade bara vår egen överbelastning.”

Fokusera på data

Emmersen konstaterar: ”När vi tittar på nollförtroende ur en holistisk synvinkel och tar ett steg tillbaka handlar det verkligen bara om data.” Att skydda organisationens data är en av de mest värdefulla fördelarna med en övergång till nollförtroende, och principer som kontinuerlig verifiering och segmentering skyddar data och program genom att förhindra att hot rör sig i sidled inom nätverket.

Loggning och kontinuerlig övervakning är viktiga komponenter i nollförtroende, och dessa data och denna telemetri analyseras för att identifiera avvikelser som kan tyda på en risk eller ett hot. En ändring i dataanvändningsmönster kan till exempel identifiera potentiell exfiltrering eller en utpressningsvirusattack.

1. Från en studie som beställts av Dell av Enterprise Strategy Group, ”Assessing Organizations' Security Journeys: Insights Spanning the Attack Surface, Threat Detection and Response, Attack Recovery, and Zero Trust”, november, 2023

DELL Technologies

Med tanke på den enorma mängd data som genereras genom att logga all aktivitet måste moderna analysverktyg använda AI och maskininlärning för att vara effektiva.

”Lita aldrig på något, verifiera alltid” måste gälla hela vägen

Även om mycket fokus på data, program, användare och enheter är internt måste den granskning som en arkitektur med nollförtroende innebär gälla under hela IT-livscykeln. Om den inte gör det kan det uppstå allvarliga säkerhetsluckor.

Leverantörskedjan är ett bra exempel, och Vogt föreslår att du ställer viktiga frågor om hårdvara och mjukvara från tredje part:

- ”Vilka andra hade tillgång till den?
- Vad är den gjord av?
- Vad finns under ytan?
- Hur kan vi ta dessa principer om att inte lita på [och] ha någon form av verifieringsprocess och någon form av hållning med lägsta behörighet till den teknik som vi använder? Även om det är uppströms i teknikens leverantörskedja?”

Att gå mot en nollförtroendearkitektur eller implementera dess principer representerar nuvarande bästa praxis för att främja cybersäkerhetsmognad. Flera vägar representerar olika kompromisser mellan kostnad, risk och nivån på säkerhetsförbättringen. Det första steget bör vara att fastställa organisationens unika position och låta den vägleda de tekniska besluten.

Lär dig att hantera några av dagens främsta cybersäkerhetsutmaningar på **dell.com/cybersecuritymonth**

DELL Technologies