RESOURCE CENTER

Vad betyder noll förtroende? Hur man implementerar Zero Trust Architecture

Get the full interactive view at https://bitwarden.com/sv-se/resources/how-to-implement-zero-trust-architecture/

bitwarden

Översikt

Traditionella säkerhetsmodeller, som bygger på perimeterbaserade försvar, gör ofta organisationer sårbara för interna och externa hot. Zero trust-arkitekturen presenterar ett modernt tillvägagångssätt som tar itu med teknikledares kärnkamp: balansera stränga säkerhetsbehov med operativ effektivitet. Den här guiden kommer att förklara vad noll förtroende betyder, gå igenom dess kärnkomponenter och tillhandahålla en färdplan för att anta en noll förtroende-säkerhetsmodell.

Vad är noll förtroende?

Noll förtroende är ett arkitektoniskt tillvägagångssätt som antar att alla användare, enheter och data är potentiella hot tills motsatsen bevisats. Konceptet har utvecklats, men dess kärnidé förblir densamma: verifiera identiteten för varje användare, enhet eller process innan du beviljar åtkomst till känsliga resurser.

Tanken bakom noll förtroende är att alla användare, oavsett om de är inom eller utanför en organisation, autentiseras, auktoriseras och kontinuerligt valideras innan de beviljas (eller behåller) åtkomst till applikationer och data.

Fördelarna med att anta noll förtroende inkluderar:

- Mycket förbättrad säkerhet: Noll förtroende minskar attackytan för din organisation genom att begränsa åtkomsten till känsliga resurser.
- Minskad risk: Noll förtroende minimerar risken från insiderhot, sidorörelser eller externa attacker.
- Efterlevnad och regulatoriska krav: Zero trust överensstämmer med regulatoriska krav för dataskydd och konfidentialitet.

Några av de vanliga användningsfallen för noll förtroende är:

- Molntjänster: Används för att säkra molnbaserade applikationer och data.
- IoT-enheter: Skydda dina IoT-enheter och nätverk från obehörig åtkomst.
- Fjärrpersonal: Säkerställer organisatorisk säkerhet när anställda arbetar på distans eller använder offentligt Wi-Fi.
- Datacenter: Förbättrar nätverkssegmentering och isolering för känsliga resurser.

Naturligtvis kommer noll förtroende med sin del av utmaningarna. För det första kräver noll förtroende komplex infrastruktur, policyer och procedurer för att hantera identitetsverifiering, åtkomstkontroll och övervakning. Det finns också det faktum att noll förtroende kan vara ganska resurskrävande, vilket kräver avancerade säkerhetsverktyg och expertis. Slutligen finns det användaradoption, vilket kan innebära att din organisations användare måste anta olika processer för autentisering.

Zero trust använder också följande koncept:

- **Mikrosegmentering** är en nätverkssegmenteringsteknik som används för att isolera känsliga resurser från LAN genom att dela upp dem i mindre zoner (eller segment). Detta minskar attackytan och begränsar sidorörelsen.

- **Minsta behörighetsåtkomst** är ett sätt att ge användare och applikationer endast de nödvändiga behörigheterna som behövs för att utföra deras uppgifter. Denna princip syftar till att minimera risken för obehörig åtkomst, dataintrång och andra säkerhetsincidenter.

Så här fungerar zero trust:

- Steg 1 - Autentisering: Användare eller enheter försöker autentisera sig genom en säker kanal (t.ex. VPN).
- Steg 2 - Auktorisering: Systemet verifierar användarens eller enhetens identitet mot kända referenser.
- Steg 3 - Åtkomstkontroll: Om autentiseringen lyckas beviljas åtkomst baserat på fördefinierade policyer och principer för lägsta behörighet.
- Steg 4 - Övervakning och tillämpning: Nätverksaktivitet övervakas kontinuerligt och säkerhetsregler tillämpas för att förhindra obehörig åtkomst.

Exempel på noll förtroende

- Exempel 1: En anställd som arbetar på distans kräver åtkomst till känslig kunddata. Under en modell med noll förtroende verifieras deras identitet genom MFA, deras enhets säkerhetsställning kontrolleras och deras åtkomst begränsas endast till nödvändig data, oavsett deras fysiska plats.
- Exempel 2: Molnleverantörer som AWS, Azure och Google Cloud använder nollförtroendeprinciper i sina säkerhetsmodeller.
- Exempel 3: Företag segmenterar sina nätverk i mindre zoner baserat på användarnas plats och åtkomsträttigheter.
- Exempel 4: Implementering av identitetsdrivna säkerhetslösningar som verifierar användarnas identiteter innan de ger dem åtkomst till känsliga resurser.
- Exempel 5: Tillämpa principer om noll förtroende på slutpunktsenheter som bärbara datorer, stationära datorer och mobila enheter.

Nyckelkomponenter i en Zero Trust-arkitektur

Det finns fem primära komponenter i Zero Trust Architecture.

Read more:
Additional enterprise options for least privilege access control

Identitetshantering

Den här komponenten ansvarar för att verifiera användaridentiteter och se till att alla användare är autentiserade och auktoriserade innan de får åtkomst till känsliga resurser.

Åtkomstkontrollpolicyer

Åtkomstkontrollpolicyer fastställer regelbaserade åtkomstkontroller för att säkerställa att endast betrodda användare kan komma åt specifika resurser.

Kryptering och nyckelhantering

Detta säkerställer kryptering av både data under överföring och vila, med hjälp av säker nyckelhantering.

Nätverkssegmentering (mikrosegmentering)

Nätverkssegmentering delar upp nätverket i mindre, isolerade segment baserat på användarroller eller känsliga datatyper.

Slutpunktssäkerhet

Den här komponenten skyddar slutpunktsenheter, som bärbara datorer, stationära datorer och mobila enheter med robusta säkerhetsåtgärder för att förhindra sidorörelseattacker.

Övervakning och incidenthantering

För att uppnå noll förtroende måste teamen kontinuerligt övervaka systemaktivitet för misstänkt beteende, samt ha en incidentresponsplan på plats för att begränsa och åtgärda intrång.

Multifaktorautentisering (MFA)

Att lägga till MFA ger organisationer ett extra lager av säkerhet genom att kräva flera former av verifiering, vilket ytterligare minskar risken för obehörig åtkomst, en kärnkomponent i noll förtroende.

Noll-kunskap kryptering

Noll-kunskapskryptering säkerställer att endast användaren har tillgång till sina data.

Förslag: Noll-kunskapskryptering håller data privat så att endast de avsedda användarna/systemet kan se eller använda dem, utan att exponera själva datan vid något tillfälle. Det kan vara en viktig komponent i ett nollförtroendesystem.

> Läs hur end-to-end-kryptering banar väg för noll kunskap i denna vitbok.

Minst privilegierad åtkomst

Åtkomst med minsta privilegier ger användarna endast den minsta åtkomst som krävs för att utföra sina uppgifter, vilket begränsar den potentiella skadan från ett inträngt konto.

Implementera en säkerhetsmodell med noll förtroende: En steg-för-steg-färdplan

Att implementera noll förtroende är en strategisk resa, inte en enkel programvaruinstallation/-konfiguration, och det här avsnittet kommer att vägleda teknikledare i att planera ett stegvis tillvägagångssätt. Redan innan du bestämmer dig för att använda noll förtroendesäkerhet är det viktigt att ha en färdplan för framgång. Den färdplanen bör bestå av minst fem steg, inklusive följande.

Read more:

The credential lifecycle: Stay ahead to strengthen your security and access management

Steg 1: Bedömning och planering

Under denna fas är det viktigt att identifiera intressenter, inklusive IT-team, ledning och användare, för att säkerställa inköp och stöd för den nya modellen.

Steg 2: Implementering av identitets- och åtkomsthantering

Distribuera en identitetshanteringsplattform som tillhandahåller användarprofilering och hotintelligens i realtid, som Okta Identity Cloud, CyberArk Idaptive, ForgeRock Identity Platform, SailPoint IdentityIQ eller IBM Identity and Access Management.

Steg 3: Nätverksmikrosegmentering

Implementera nätverkssegmentering med VLAN, subnät eller andra tekniker för att isolera känslig data och/eller resurser.

Steg 4: Kontinuerlig övervakning och hotrespons

Implementera ett SIEM-system (Security Information Events Management) för att övervaka säkerhetsrelaterade händelser och tillhandahålla hotanalys och intelligens i realtid.

Steg 5: Iteration och optimering

Det är viktigt att förstå att varje iteration av en nollförtroende-distribution ständigt kommer att utvecklas för att fungera med ett ständigt föränderligt landskap. Med varje ny iteration bör plattformen optimeras ytterligare genom analys och övervakning.

När dessa steg är klara, bestäm hur ditt team ska hantera utbildning och testning, underhåll och slutpunktssäkerhet.

Dos av noll förtroende

- **Implementera multi-factor authentication (MFA)**: Kräv alltid att användare tillhandahåller flera former av autentisering, såsom lösenord, 2FA-koder, tokens eller biometriska data.
- **Använd kryptering**: Kryptering av känsliga data både under överföring och i vila bör anses vara ett måste för att förhindra obehörig åtkomst.
- **Segmentera nätverkstrafik**: Dela upp nätverket i mindre segment baserat på användarroller eller känslighetsnivåer för att minska organisationens attackyta.
- **Implementera åtkomstkontroller**: Upprätta regelbaserade åtkomstkontroller för att säkerställa att endast auktoriserade användare kan komma åt specifika resurser inom din organisation.
- **Övervaka systemaktivitet**: Övervaka kontinuerligt systemaktivitet för misstänkt beteende och se till att de nödvändiga teamen kan reagera snabbt på alla potentiella säkerhetsincidenter.
- **Använd artificiell intelligens (AI) och maskininlärning (ML)**: Använd AI/ML-drivna säkerhetsverktyg för att upptäcka anomalier i systemaktivitet och förhindra potentiella

intrång, eftersom dessa typer av system kan upptäcka problem snabbare än sina mänskliga motsvarigheter.

- **Genomför regelbundna säkerhetsrevisioner**: Utför regelbundna säkerhetsrevisioner för att identifiera sårbarheter och säkerställa efterlevnad av organisationens policyer. Dessa är också en nödvändighet för iteration och optimering.

Don'ts av noll förtroende

- Begränsa **inte åtkomsten** överdrivet: Undvik alltför restriktiva åtkomstkontroller som hindrar legitima användaraktiviteter, som e-post eller fildelning, eftersom detta kan leda till en störtflod av problem.
- Försumma **inte slutpunktssäkerhet**: Säkerhetsfel i slutpunkten kan leda till laterala rörelseattacker över ditt LAN såväl som dataintrång. Implementera robusta säkerhetsåtgärder till alla slutpunkter.
- Ignorera **inte identitetshantering**: Identitetshantering är nyckeln till noll förtroende, och att misslyckas med att hantera identiteter korrekt kan leda till obehörig åtkomst till känsliga resurser.
- Lita **inte bara** på brandväggar: Brandväggar är en bra källa till grundläggande enhets- och nätverkssäkerhet, men när de används ensamma kanske de inte är tillräckliga för att förhindra avancerade hot.
- Missa **inte att kontinuerligt övervaka organisationens säkerhetsställning**: Noll förtroende är ett koncept som ständigt utvecklas. Övervaka kontinuerligt säkerhetsställningen för att hålla organisationen före ständigt föränderliga hot.
- Ignorera **inte incidentresponsplaner:** Det är viktigt att ha planer för när incidenter inträffar. Om det inte finns en åtgärdsplan för incidenter kan organisationen vara för långsam i sin reaktion på en händelse.
- **Försumma inte användarutbildning**: Noll förtroende kan vara ett helt nytt koncept för användare, så det är viktigt att utbilda dem om den här nya policyn för att främja och underlätta användarnas antagande.

Bitwarden stöder nollförtroendetransformationer

Zero Trust Architecture erbjuder en grundläggande förändring i hur organisationer närmar sig cybersäkerhet, och går från en perimetercentrerad vy till en datacentrerad. Tekniledare kan avsevärt stärka sin säkerhetsställning genom att förstå dess kärnprinciper och implementera funktioner som multifaktorautentisering och nollkunskapskryptering.

Zero trust-säkerhetsmodellen hjälper till att leverera ökad säkerhet, förbättrad incidentrespons, förbättrad efterlevnad, minskad risk från hot från utomstående, minskade kostnader för säkerhetsoperationer, förbättrad användarupplevelse, bättre skydd mot avancerade hot, förebyggande av dataförlust och framtidssäker säkerhet.

Börja din resa med noll förtroende idag genom att se över din nuvarande säkerhetsinfrastruktur och identifiera områden där Bitwarden omedelbart kan förbättra din säkerhetsställning.