WALLIX
CYBERSECURITY SIMPLIFIED

Beginnershandleiding
voor toegangsbeveiliging

Beginnershandleiding voor toegangsbeveiliging

SAMENVATTING

Dit is een uitgebreide beginnershandleiding voor iedereen die de basisprincipes over toegangsbeveiliging wil leren begrijpen.

Toegangsbeveiliging is een kader waarin beleid en technologie samenkomen, met als doel om gebruikers toegang te geven tot sensitieve IT-systemen. Een goed opgezet toegangsbeveiligingssysteem brengt een aantal voordelen met zich mee, waaronder bescherming tegen cyber-aanvallen, een betere naleving van wet- en regelgeving en meer controle over externe apparaten die toegang hebben tot het netwerk en de gegevens van een bedrijf.

Een bedrijf dat up to date wil zijn moet zichzelf beschermen tegen bedreigingen die van binnen en buiten de muren komen. Een goed doordachte toegangsbeveiliging geeft bedrijven meer controle over de toegangsrechten van gebruikers en bevoegdhedenniveaus. Drie processen staan hierbij centraal: identificatie, authenticatie, en machtigingen.

Het zero trust principe en het least privilege principe zijn belangrijk in een sterke netwerkbeveiliging. Er zijn een aantal specifieke systemen die bedrijven kunnen gebruiken om deze concepten toe te passen in hun IT-infrastructuur: Identity Management, Privileged Access Management and Endpoint Privileged Management.

Introductie van toegangsbeveiliging

Wat is toegangsbeveiliging?

Een gebouw wordt meestal goed beveiligd. Bedrijven hebben veiligheidsprocedures om te voorkomen dat buitenstaanders zomaar binnendringen. Gebouwen worden, aan de hand van veiligheidsprocedures, dagelijks gecontroleerd en geactualiseerd om ervoor te zorgen dat de juiste mensen toegang hebben tot juiste plaatsen. Pasjes, fysieke controleposten, wachtwoorden en gezichtsherkenningstechnologieën kunnen hier onderdeel van uitmaken.

Belangrijke data, zoals data over klanten, wordt meestal opgeslagen in databases. Het is logisch dat bedrijfsgevoelige informatie moet worden beschermd. Zou een netwerk van een bedrijf niet net zo goed moeten worden beveiligd als een gebouw?

Iedereen heeft een fysieke identiteit. En tegenwoordig hebben we ook allemaal een digitale identiteit. Het kan gemakkelijk zijn om een indringer te herkennen op basis van een fysieke identiteit. Digitale indringers daarentegen, zijn moeilijker te traceren aan de hand van een digitale identiteit. Daarom is het belangrijk om te weten wie precies toegang wil tot de IT-Infrastructuur en tot op welk niveau. Gebruikers moeten het juiste toegangsniveau hebben om toegang te krijgen tot de informatie die zij nodig hebben. Zij hoeven geen toegang te hebben tot bronnen en applicaties die niet voor hen bedoeld zijn. De IT-Infrastructuur lijkt wat dat betreft op een gebouw, waar de toegang tot ruimtes eveneens gereguleerd is.

Elk persoon die toegang heeft tot het netwerk beschikt idealiter over één digitale identiteit. Deze identiteit moet worden beheerd. Als er veranderingen in de 'levenscyclus' van een gebruiker optreden (bijvoorbeeld verandering van een functie), dan zullen de bevoegdheden (zoals toegangsrechten) moeten worden aangepast. In het geval dat een medewerker het bedrijf verlaat zal de toegang waarschijnlijk tijdelijk of geheel worden stopgezet.

Toegangsbeveiliging kan worden gezien als een kader waar beleid en technologie samenkomen. Het doel is dat de juiste mensen toegang hebben tot de juiste informatie in de IT-infrastructuur. Dit betekent dat van iedereen gekend moet zijn welke bevoegdheden en restricties zij hebben. Wanneer honderden gebruikers toegang krijgen tot een netwerk, dan is het belangrijk dat er kan worden achterhaald wie wie is en wat ze deden op het netwerk, en wanneer ze dat de deden. Drie op elkaar afgestemde processen zorgen dat dit mogelijk is: identificeren, authentiseren en machtigen.


“Toegangsbeveiliging
en -beheer is een kader waar
beleid en technologie
samenkomen. Het zorgt
ervoor zorgt dat de juiste
mensen toegang hebben tot
de juiste informatie in de
IT-infrastructuur. ”

Identificeren, authentiseren en machtigen

Deze processen werken samen om te verifiëren wie de gebruikers zijn en welke toegangsrechten zij hebben. Op het eerste gezicht lijken deze processen op elkaar. Echter, er zijn belangrijke verschillen die van belang zijn voor een goede toegangsbeveiliging

Identificatie

Identificatie is de eerste stap in het proces om toegang te verlenen. Allereerst moeten we weten wie toegang wil. Elke gebruiker is onderdeel van het IT-netwerk en heeft een digitale identiteit. Deze digitale identiteit is gekoppeld aan een uniek persoon in de echte wereld en heeft een unieke gebruikersnaam of een uniek e-mailadres nodig.

Het verlenen van toegang (en daaraan gekoppelde rechten) tot het IT-netwerk gebeurt op basis van deze unieke gegevens. Medewerkers krijgen op die manier digitaal toegang tot de organisatie en dit is noodzakelijk om hun werk te kunnen doen. Dat is de reden waarom bedrijven investeren in deze software.

Een gebruikersnaam is niet voldoende om iemands identiteit vast te stellen. Iemand anders zou de gebruikersnaam gemakkelijk kunnen intikken en daarmee documenten raadplegen die toegankelijk zijn voor dat account. Dit is waarom het belangrijk is om te authentiseren.

Authentiseren

In het authenticatie proces wordt gecontroleerd of de inloggegevens van de gebruiker overeenkomen met de identiteit van de gebruiker. Hiervoor is het volgende nodig: iets wat alleen jij weet, iets wat alleen jij hebt of iets wat onderdeel van jou is.

- **Iets wat alleen jij weet:** Het meest bekende voorbeeld is een wachtwoord. Als de gebruikersnaam de identificeerder is, dan is het wachtwoord de authenticatie. Een wachtwoord is de meest simpele vorm van toegangsbeheer en brengt risico's met zich mee. Wachtwoorden zijn gemakkelijk te delen of te stelen.
- **Iets wat alleen jij hebt:** Dit kan een fysiek item zijn, zoals een kaart of een RSA token dat een tijdelijk wachtwoord genereert.
- **Iets wat onderdeel van jou is:** Dit betreft de biometrische authenticatie methodes. De identiteit wordt vastgesteld aan de hand van een onderdeel van het lichaam, zoals het iris van een oog, een gezicht of een vinger. Gedragsindicatoren kunnen ook worden gebruikt, zoals typgedrag, stem of handtekening erkenning.

De digitale identiteit en één van de bovenstaande authenticatie methodes, creëren een toegangspoort tot het netwerk.

De toegangsbeveiliging van het netwerk wordt beter als er meerdere authenticatie methodes worden ingezet. Zodoende wordt het moeilijker gemaakt voor hackers, aangezien zij meer van de reeds genoemde gegevens moeten stelen.

Het gebruik van twee of meerdere authenticatie methodes wordt multi-factor authenticatie genoemd (MFA). MFA verhoogt de geloofwaardigheid in de beveiliging van sensitieve IT-systemen.

Machtigen

Machtigen is het proces waarin iemand toestemming krijgt om iets te doen of te krijgen. Deze stap is heel belangrijk als het netwerk veel gebruikers heeft. Als een gebruiker is ingelogd, wat kan een gebruiker daarna? In het machtiging proces worden niveaus van bevoegdheden toegekend en gevoelige data beschermd, aangezien alleen individuelen die toestemming hebben, toegang krijgen.

Als elke gebruiker apart kan worden geïdentificeerd, kan worden gecontroleerd of de identiteit van de gebruiker klopt en kunnen IT-beheerders de juiste toegangsrechten daaraan koppelen. Hierdoor krijgt elke gebruiker toegang tot bronnen die passen bij zijn of haar functie.

Machtigen is een belangrijke stap, want elke gebruiker heeft iets anders nodig op het netwerk. De ene gebruiker heeft alleen toegang nodig tot enkele applicaties terwijl andere gebruikers servers en databases moeten kunnen aanpassen. Het zou niet logisch zijn dat alle gebruikers dus dezelfde toegangsrechten krijgen.

Het toegangsbeheer zal in staat moeten zijn om gebruikers te identificeren, vervolgens te bevestigen dat het om de correcte identiteit gaat (authentiseren) om daarna de toegang te geven (machtigen). Bedrijven die de toegangsbeveiliging op orde hebben, profiteren van vele voordelen.

De voordelen van een sterke toegangsbeveiliging

Beheren van privilege niveaus

Het is niet goed als accountgegevens, zoals gebruikersnamen en wachtwoorden, gestolen worden. Echter, de daadwerkelijke schade hangt af van het toegansniveau dat is gekoppeld aan dat account.

Wanneer het netwerk goed beveiligd is, dan kunnen er gemakkelijk aanpassingen worden gedaan in de instellingen van de toegangsniveaus en daarmee de zichtbaarheid die de gebruiker heeft.

Niet iedereen heeft dezelfde toegangsrechten nodig om zijn taken uit te voeren. Er zal goed moeten worden nagedacht wie toegang nodig heeft en tot welke data en applicaties. Zodoende wordt vermeden dat gebruikers teveel rechten hebben, die in verkeerde handen kunnen vallen, met datalekken als gevolg.

Door een goed uitgedacht beleid te hebben, kunnen toegangsrechten gemakkelijk gestroomlijnd worden. IT-beheerders werken bij voorkeur met een gecentraliseerde hub, waar aan elke groep gebruikers specifieke toegangsrechten worden toegewezen. Hierdoor blijft het overzicht behouden en zijn IT-beheerders in de mogelijkheid om gemakkelijk aanpassingen te doen.

Beveiliging tegen cyberaanvallen

Gartner voorspelt dat er wereldwijd $133.7 miljard wordt uitgegeven aan cybersecurity in 2022.

Toegangs-beveiliging

Bedrijven en organisaties proberen zichzelf te beschermen tegen cyberaanvallen. Toegangsbeveiliging is daar een cruciaal onderdeel van. Privileged Access Management (PAM) is door Gartner in 2019 als de belangrijkste prioriteit genoemd voor de beveiliging van netwerken van bedrijven.

Aangezien een bedrijf van binnen en buiten kan worden aangevallen, is het erg belangrijk om te weten:

- Wie heeft er toegang tot jouw systeem?
- Welke bevoegdheden hebben zij?
- Wat doen zij met hun toegang?
- Wanneer hebben zij toegang tot het systeem?

Deze vragen zijn relevant om te stellen over insiders, zoals medewerkers, maar ook over "outsiders" zoals partners en bedrijven waarmee wordt samengewerkt of thuiswerkende medewerkers. Het zijn de gebruikersnamen en wachtwoorden, die de gebruikers toegang tot een systeem geven. Het zijn de gebruikers die (onbedoeld) phising, ransomware en malware binnenhalen. Daarom is het erg belangrijk om de juiste vragen te stellen over degenen die toegang krijgen tot het systeem

Beveiliging van je interne IT-omgeving

Een lokaal IT-netwerk dat binnen de muren van een bedrijf blijft, behoort tot het verleden. Bedrijven hebben tegenwoordig 'eindpunten' over de gehele wereld. Medewerkers en onderaannemers kunnen inloggen op afstand van het bedrijf en op hun eigen toestellen.

Internet of Things (IoT), dus het internet der dingen, wordt steeds vaker ingezet en dit opent weer nieuwe mogelijkheden om tot het netwerk toegang te krijgen. IoT breidt zich uit, en opent meer wegen dan ooit naar een netwerk. Deze mogelijkhedenwaren er nog niet, aangezien de eindpunten afgeschermd waren van het wereldwijde internet. Tegenwoordig, zijn de eindpunten buiten het netwerk van het bedrijf niet standaard beschermd door de traditionele IT-omgeving beveiliging. Bedrijven hebben daarom behoefte aan een extra beveiligingslaag voor endpoints die overal toegang hebben tot gevoelige bedrijfsmiddelen.

Een toegangsmanagement oplossing kan ingezet worden om gebruikers te authentiseren op verschillende eindpunten. Dit betekent dat gebruikers hun identiteit kunnen verifiëren op afstand zonder impact te hebben op hun productiviteit.

Naleven van de wet- en regelgeving

Het is belangrijk om exact te weten wie een netwerk betreedt en wie het netwerk verlaat, en welke bevoegdheden zij hebben. Het is niet een 'nice to have', het is een verplichting. In ISO 27001 en GDPR is dit gereguleerd. Zij stellen een verplichting op het hebben van controlemechanismes en het transparant bijhouden van sessies van gebruikers. Door een goede regulatie van deze processen in een bedrijf, kunnen boetes worden voorkomen.

Bedrijven moeten niet wachten met het beveiligen van het netwerk, totdat ze hun eerste data-lek hebben. De juiste oplossingen stellen IT-teams in staat om de naleving van de wet- en regelgeving te ondersteunen zonder overbelasting van cybersecurity-middelen of het te ingewikkeld maken van zakelijke taken.

Door goed na te denken over het beveiligen van het IT-netwerk, worden ook andere processen van het bedrijf gestroomlijnd.

Een goed beveiligd netwerk brengt voordelen voor een bedrijf. Het is belangrijk om een aantal concepten van toegangsbeveiliging daarvoor te begrijpen, zoals insider threat, zero trust en least privilege.

Begrijpen van Toegangsbeveiliging

Insider Threat

Een insider kan worden gedefinieerd als iemand die toegang heeft tot interne gevoelige bedrijfsinformatie. Dit kunnen medewerkers zijn die fulltime werken, maar net zo goed medewerkers die parttime in dienst zijn of iemand die via een contract van een extern bedrijf (third party) verbonden is aan het netwerk. Deze gebruikers hebben allen toegang tot de infrastructuur van het bedrijf en op verschillende tijdstippen. In deze tijden van cybercriminaliteit, kan elke insider een potentiële toegang zijn voor hackers.
Het is misschien raar om te denken dat gewaardeerde collega's ook een potentieel gevaar kunnen vormen. De realiteit is echter, dat een significant deel van de datalekken in verband kan worden gebracht met accountgegevens van insiders. Dit betekent niet dat medewerkers opzettelijk het bedrijf in gevaar brengen. Insiders hebben vaak niet eens door dat hun accountgegevens worden gebruikt. Het maakt dus niet uit hoe goed een medewerker te vertrouwen is. Hoewel de meerderheid het bedrijf nooit opzettelijk in gevaar zou brengen, kunnen de accountgegevens van elke gebruiker van het netwerk worden gestolen, verloren raken of (onbewust) worden gedeeld met iemand met slechte intenties.

Volgens een onderzoek uit 2020 door The Ponemon Institute, is het aantal incidenten dat gerelateerd is aan insiders en Toegangsbeveiliging, met 47% toegenomen sinds 2018. Dit rapport geeft aan dat 62% van de incidenten werd veroorzaakt door het onzorgvuldig omgaan

Hoe groot is het gevaar voor een aanval van binnenuit?

Insider threat is de belangrijkste oorzaak van een cyberaanval. Volgens een onderzoek uit 2020 door The Ponemon Institute, is het aantal incidenten dat gerelateerd is aan insiders en Toegangsbeveiliging, met 47% toegenomen sinds 2018. Dit rapport geeft aan dat 62% van de incidenten werd veroorzaakt door het onzorgvuldig omgaan met accounts.

Insider threat vormt een risico omdat alle medewerkers, inclusief de meest betrouwbare medewerkers, data kunnen lekken, door phising emails, delen van gebruikersnamen en wachtwoorden of doordat ze vanuit een eindpunt, dat buiten het bedrijfsnetwerk ligt, inloggen.

Toegangs-beveiliging

In het onderzoek dat door Ponemon Institute is uitgevoerd, wordt vermeld dat bedrijven gemiddeld 60% van het budget meer uitgeven om bewustwording bij insiders te creëren in vergelijking met drie jaar geleden. Steeds meer bedrijven nemen maatregelen tegen deze kwetsbaarheden.

Hoe beschermen we ons tegen deze kwetsbaarheden?

Mensen zullen altijd toegang nodig hebben tot IT-bronnen om hun werk te kunnen doen. Bedrijven moeten daarom zorgen dat deze IT-bronnen beschermd zijn tegen misbruik en kwetsbaarheden. Hoe meer open het netwerk is, hoe kwetsbaarder een netwerk wordt, hoe groter de kans op een succesvolle aanval toe zal nemen.

We verkennen twee principes die een bedrijf kan toepassen om zich te beschermen tegen datalekken. Het eerste principe is het Zero trust principe dat zich richt op de identificatie en authenticatie van gebruikers. Het tweede principe betreft het principe van least privilege, het principe van de minste bevoegdheden, waar de toegangsrechten van gebruikers tot een minimum worden beperkt.

Het zero trust principe

Iedereen met toegang tot het netwerk vormt mogelijk een risico voor cyberaanvallen. Dit betreft dus ook de meest loyale medewerkers van een bedrijf. Daarom is het logisch om het zero trust principe toe te passen voor gebruikers die toegang willen tot het netwerk. Het is niet de bedoeling dat iedereen met wantrouwen moet worden behandeld en er moet worden gewacht totdat er iets fout gaat.

Het betekent simpelweg dat niemand impliciet kan worden vertrouwd die toegang wil tot de data van het bedrijf. Door het zero trust principe toe te passen wordt proactief naar bewijs gevraagd van de identiteit, voordat toegang wordt gegeven. De gebruikers moeten voorafgaand aan het verkrijgen van de toegang, bewijzen dat zij iets nodig hebben en dat het verzoek legitiem is.

Hoe kunnen we gebruikers vertrouwen?

Door het zero trust principe te hanteren, wordt het risico op een aanval van binnenuit verminderd, maar nog niet volledig geëlimineerd. Als toegang wordt verleend op basis van gebruikersnamen en wachtwoorden, is er een kans dat deze gegevens worden gestolen en gebruikt door iemand anders.

Multi-Factor Authentication (MFA) biedt mogelijkheden om de betrouwbaarheid van het toegangsproces te verhogen. Het verhoogt de kans dat de identiteit van de gebruiker klopt, aangezien er meerdere keren en vormen van verificatie plaatsvinden. Hoe complexer het verificatieproces, hoe moeilijker (maar niet onmogelijk) het voor een hacker is om alle informatie te stelen. Het is bijvoorbeeld moeilijker om een wachtwoord en een beveiliging token te stelen, dan alleen een wachtwoord. Hoe meer authenticatie factors, hoe groter het vertrouwen dat de identiteit van de gebruiker klopt.

Is multi-factor authenticatie genoeg?

Medewerkers worden doorgaans vertrouwd, en dat is iets goeds. Maar wanneer het gaat over de toegang die wordt verleend tot bedrijfsgevoelige informatie, dan is het een slecht idee om zomaar iedereen te vertrouwen. Iedereen kan een data-lek veroorzaken en daarom is het beter om niet iedereen "zomaar" te vertrouwen.

Zero trust is de eerste defensieve lijn tegen aanvallen en diefstal van inloggegevens. Een belangrijk onderdeel van zero trust is het principe van de least privilege, oftewel het principe van de minste privileges. Dit houdt in dat gebruikers zo min mogelijk bevoegdheden krijgen. In het geval een hacker erin slaagt om in het systeem te komen door middel van inloggegevens van een bestaande gebruiker, dan zal de schade beperkt zijn.

Het principe van de least privilege

Het principe van de least privilege betekent dat de privileges van gebruikers tot een minimum worden beperkt, dus tot de noodzakelijke privileges die gebruikers in staat stellen om hun werk uit te voeren. Het limiteren van de bevoegdheden zorgt ervoor dat de schade beperkt blijft. Alle bevoegdheden die de gebruiker heeft, zullen ook door de hacker gebruikt kunnen worden. Een hacker weet hoe hij grote schade aan kan richten. Het principe van de least privileges kan, naast het limiteren van de toegang, ook worden toegepast op het aantal keren dat toegang wordt verleend, of tot de locatie van de gebruiker. Een medewerker zou bijvoorbeeld alleen toegang kunnen krijgen tijdens de werkuren of als hij/zij inlogt van een bepaalde locatie.

Is er een goed doordacht beleid is rond het principe van de least privileges, dan wordt de potentiële 'attack surface', oftewel de ruimte die überhaupt kan worden aangevallen, verminderd.

Denk aan een hotel, waarin een gast een toegangskaart krijgt waarmee alle ruimtes te openen zijn, op elk gewenst tijdstip. Dit is niet de bedoeling en niet nodig. De gast moet alleen toegang krijgen tot de gereserveerde kamer en de gemeenschappelijke ruimtes. Bovendien moet de toegang beperkt worden tot de duur van de reservatie.

Waarom is het principe van least privilege zo belangrijk?

Het principe van least privileges, limiteert de toegangsmogelijkheden van de gebruiker. De gebruiker hoeft of kan zich niet machtigen om tot bepaalde gedeeltes toegang van het netwerk te krijgen. In het geval de hacker zou inloggen, zou de hacker dus ook tot een klein aantal bronnen toegang krijgen en dit vermindert te kans op schade. Door de toegang te limiteren van de gebruikers, beperken we de kans op schade in het geval de inloggegevens niet legitiem worden gebruikt.

Het hoofd van IT heeft andere toegangsrechten nodig dan een extern bedrijf (third party) dat bijvoorbeeld onderhoud moet uitvoeren op een specifiek apparaat. Hij/zij heeft toegang nodig tot een specifiek gedeelte van het netwerk om taken te kunnen uitvoeren. In het geval dat hij/zij meer toegang zou krijgen dan nodig, en hij/zij per ongeluk malware binnenhaalt (bijvoorbeeld door te klikken op een link in een email), dan zou er veel schade veroorzaakt worden.

Dit kan worden voorkomen. Mocht een (externe) medewerker meer rechten nodig hebben tot bronnen waarin hij/zij geen rechten heeft, dan kan dit verzoek altijd worden ingewilligd, per taak.

Hoe kunnen we het principe van de least privilege implementeren?

Het principe klinkt eenvoudig in theorie. Het toepassen van dit principe is echter moeilijker, en zeker als er honderden of zelfs duizenden gebruikers zijn in een bedrijf. Deze gebruikers hebben allemaal andere rollen en daardoor andere bevoegdheden nodig, die van tijd tot tijd kunnen veranderen. Ook zullen vele gebruikers het netwerk betreden of juist verlaten. Om het least privilege principe toe te passen, moeten bedrijven het volgende weten:

- Welke bronnen bevatten gevoelige informatie?
- Wie heeft daadwerkelijk toegang nodig tot deze informatie?
- Aan welke wet- en regelgeving moet het bedrijf voldoen?

Een combinatie van least privilege en een aanpak waarin niemand wordt vertrouwd, zero trust, versterkt de toegangsbeveiliging van het netwerk. Een centrale toegangsmethode past het beste hierbij, aangezien het dan gemakkelijker wordt om gebruikers te identificeren en de bevoegdheden toe te kennen. In de volgende paragraaf wordt meer uitleg gegeven over deze management systemen, die ervoor zorgen dat zero trust en least privilege principe in actie komen.

Beheer van Toegangsbeveiliging

Identiteit- en toegangsmanagement (IAM)

Cloud omgeving, werken op afstand, 'bring your own device' beleid (BYOD) en Industrial Internet of Things (IIoT) hebben IT-netwerken meer dan ooit complexer gemaakt. Dit zorgt voor uitdagingen in het beheer van digitale identiteiten. Een centraal systeem waarin gebruikers kunnen worden gemonitord, beschermt het bedrijf tegen het nemen van onnodige risico's.

Er is reeds uitgelegd hoe het verificatie proces verloopt. Het verificatie proces moet een integraal onderdeel zijn van de beveiliging van het netwerk. Identity and Access Management (IAM), oftewel Identiteit- en toegangsmanagement, geeft een waaier aan oplossingen om gebruikers te identificeren en authentiseren. Deze systemen stellen bedrijven in staat om elke gebruiker te definiëren en de toegangsrechten tot het netwerk toe te kennen.

Wat zijn de belangrijkste kenmerken van IAM?

Identiteit- en toegangsmanagementsystemen richten zich in de basis op drie fundamenten: identificatie, authenticatie en machtiging van gebruikers. De juiste selectie van oplossingen, zorgt ervoor dat een organisatie een robuuste beveiliging heeft en daarmee de gebruikers en bedrijfsdata beschermt.

Toegangs-beveiliging

Wat wordt er gevraagd van de oplossingen die deel uitmaken van het IAM-ecosysteem? Identiteit- en toegangsmanagementsystemen moeten gebruikers kunnen verifiëren en bij voorkeur door middel van multi-factor authenticatie (MFA). Door de juiste toepassing hiervan, kunnen bedrijven het zero trust principe toepassen wanneer iemand het netwerk wil betreden.

De functies van medewerkers, en hun bijkomende toegangsrechten in de infrastructuur van een bedrijf, kunnen veranderen in de loop der tijd. Een systeem waarin gebruikersrechten gemakkelijk kunnen worden aangepast, verwijderd of toegevoegd, is belangrijk voor een effectieve toegangsbeveiliging. Effectief toegangsbeheer stelt super-beheerders in staat om accounts te activeren en te deactiveren, maar ook om rechten aan te passen en om informatie over gebruikers in een database op te slaan. Zo'n systeem moet gemakkelijk in het gebruik zijn. Als zo'n systeem te gecompliceerd is of op uiteenlopende bronnen berust, dan zal het de effectiviteit van het systeem teniet doen.

De meest effectieve beveiligingssystemen zijn voor alle gebruikers toegankelijk op eenvoudige wijze. Als het raadplegen van bronnen lastig wordt gemaakt door een te gecompliceerd inlogproces, dan zullen gebruikers naar alternatieve methoden zoeken. Dit brengt het bedrijf in gevaar. Een simpele authenticatie methode (Single sign-on (SSO)), en een centrale toegang op één platform, stroomlijnt de inlogervaring, waardoor gebruikers deze weg zullen blijven gebruiken. Dit bevordert de juiste beveiligingsprocessen.
IAM is een overkoepelende term voor alles wat met identiteit- en toegangsmanagement software te maken heeft. Onderdeel van een sterk IAM beleid is Privileged Access Management (PAM). Letterlijk vertaald is dit geprivilegieerd toegang management, oftewel het managen van processen rond toekenning van bevoegdheden van gebruikers. PAM oplossingen zorgen voor een verbeterde beveiliging, als de principes rond Least Privilege en Zero trust geïntegreerd zijn.

Privileged Access Management

Door de inzet van Privileged Access Management (PAM) kunnen bedrijven hun gebruikers beter monitoren en controleren. Identiteit oplossingen en MFA authentiseren en autoriseren elke gebruiker die toegang tot een systeem nodig heeft, waarna PAM is gericht op het stroomlijnen van beheer en toezicht op de toegangsrechten van geprivilegieerde gebruikers, zodat organisaties beschermd worden tegen het per ongeluk of opzettelijk misbruik van geprivilegieerde toegang.

De gevaren die schuil gaan achter het blind vertrouwen van gebruikers, zijn duidelijk. Een zero trust principe hebben is de juiste oplossing. Hiervoor moet een systeem voldoen aan de mogelijkheid om elke toegangspoging te valideren en te monitoren. Zelfs super-beheerders zijn in staat om (onbedoeld) het systeem te misbruiken. Er is een mogelijkheid dat inloggegevens (per ongeluk) worden verwijderd, verloren of gestolen. Een gebruiker met slechte intenties én met beheerder rechten, zou gemakkelijk vergaande veranderingen in het systeem kunnen aanbrengen, en deze acties uit het zicht kunnen houden (door sporen te wissen). Eveneens kunnen gebruikers fouten maken.

Als ze te veel gebruikersrechten hebben, kan dit grote gevolgen hebben.

PAM vermindert dit risico en faciliteert de controle over toegangsrechten en mogelijkheden, inclusief die van beheerders. Het monitort de acties van medewerkers en geeft inzicht in wanneer en wat ze raadplegen. Indien zich een data-lek voordoet, kan gemakkelijk een controlespoor (ook wel 'audit trail') worden bekeken, waarin de sporen van gebruikers te vinden zijn. De meest effectieve PAM systemen valideren de pogingen tot toegang, tegen de volgende criteria:

1. Kan een gebruiker bewijzen wie hij/zij is?

2. Heeft de gebruiker de noodzakelijke privileges om toegang te krijgen tot de bron?

3. Zijn er beperkingen waarmee rekening moet worden gehouden in het verlenen van toegang?

4. Worden de activiteiten van de gebruiker gemonitord, opgeslagen, met als doel de gebruiker te traceren en controleren?

5. Kan de sessie worden gestopt (automatisch of manueel), als de activiteit niet geautoriseerd of verdacht is?

PAM varieert qua opbouw, maar kent doorgaans drie hoofdcomponenten:

- **Toegangsmanager**
- **Wachtwoordmanager**
- **Sessiemanager**

Deze modules werken gezamenlijk om ervoor te zorgen dat de bovenstaande vragen worden beantwoord, voordat de toegang wordt toegekend.

Toegangsmanager

Een toegangsmanager kent de privileges van accounts toe vanuit één dashboard. Het IT-team van het bedrijf kan hierdoor een systeem opzetten van rollen en functies, en hieraan gebruikers verbinden. Dit vergemakkelijkt het om op grote schaal en op individueel niveau bevoegdheden te beheren. Er kan onderscheid worden gemaakt in verschillende soorten rollen, zoals interne, externe en derde partijen, die telkens andere bevoegdheden hebben. In dit systeem hebben super-beheerders de mogelijkheid om machtigingen te managen en gebruikers te traceren.

De toegangsmanager centraliseert de toegang tot bronnen, zonder dat gebruikers verschillende keren moeten inloggen of van systeem moeten veranderen. De gebruikers zien alleen de bronnen, waarvoor zij rechten hebben gekregen. Niet meer en niet minder. Ze kunnen geen andere bronnen of applicaties van IT zien, ook al weet iedereen dat deze er wel zijn.

De toegangsmanager geeft de beheerders een duidelijk beeld over wie toegang heeft en wie welke bronnen raadpleegt. De toegangsmanager maakt het bovendien gemakkelijk om bronnen te connecteren met interne en externe gebruikers, doordat de toegang naar bronnen gestroomlijnd wordt.

Toegangs-beveiliging

De toegangsmanager is in het bijzonder belangrijk voor grote organisaties die toegang verlenen aan externe locaties en gebruikers, zoals medewerkers die op afstand werken of onderaannemers en bedrijven die een bepaalde service verlenen. De toegangsmanager geeft een extra laag aan beveiliging aan “insiders” die buiten het netwerk inloggen.

Wachtwoordmanager

Het doel van een effectief PAM beleid is ervoor te zorgen dat gebruikers geen wachtwoorden kennen die toegang geven tot bedrijfsgevoelige data of systemen. De wachtwoordmanager bewaart alle wachtwoorden door middel van SSH sleutels in een beveiligde kluis. Dit betekent dat gebruikers nooit hun root - wachtwoorden moeten weten of hoeven te delen. Deze methode verlaagt significant het risico niveau op diefstal van wachtwoorden. In het geval de wachtwoorden in de verkeerde handen vallen, kunnen ze ongeldig worden gemaakt. Wachtwoorden worden gecontroleerd op complexiteit en worden automatisch geroteerd, wat betekent dat referenties ongeldig worden, zelfs als ze worden geschonden.

Een wachtwoordmanager is meer dan een kluis alleen. Een wachtwoordmanager bewaart en versleutelt wachtwoorden, maar stimuleert ook een robuust wachtwoorden beleid en best practises in een organisatie. De wachtwoordmanager is een belangrijk onderdeel van PAM, en vermindert het risico op blootstelling aan risico’s.

Sessiemanager

De sessiemanager is de kern van een robuust PAM systeem. De sessiemanager monitort continu wie waarvoor toegang heeft, en of deze acties van gebruikers gelegitimeerd en geautoriseerd zijn. De manager houdt automatisch een logboek bij van de sessies. Het is niet mogelijk om de data manueel aan te passen. Het is wel mogelijk om de data te doorzoeken. Wanneer een gebruiker een poging doet om toegang te krijgen tot sensitieve data, dan kan het systeem dit automatisch stopzetten. Dit is het zero trust principe in actie: ‘better safe than sorry’.

De sessiemanager geeft zicht op de acties van gebruikers, waardoor het risico op (onbedoeld) misbruik van de toegekende rechten wordt verminderd. Het brengt een aantal gegevens in kaart, waaronder hoeveel en wat er wordt geklikt en getypt. Zodoende krijgen bedrijven inzicht in de sessies van gebruikers. Ook registreert de software niet legitieme acties, zoals acties die een gebruiker kan proberen te verbergen, hetzij op een ander scherm of met toetscommando's.

De opnames van sessies zijn handig bij het opsporen van ongelukken in real-time, waardoor de actie gemakkelijk ongedaan kan worden gemaakt. Opnames kunnen bovendien goed van te pas komen voor trainings- of auditdoeleinden. Een uitgebreide PAM-oplossing is de best mogelijke manier om de beveiliging tegen de potentiële risico's van bevoorrechte gebruikers te optimaliseren.

Endpoint Privilege Management

In het verlengde van PAM, kan Endpoint Privilege Management (EPM) gezien worden als een kritische component in de IAM-strategie, om gebruikers veilig te laten inloggen op het bedrijfsnetwerk vanuit allerhande apparaten en locaties, waaronder "terminal" apparatuur. EPM past het concept van least privilege toe op de eindpunten, waardoor het mogelijk wordt om de toegang tot applicaties of processen op afstand van de gebruiker toe te staan of te blokkeren. Dit beschermt het netwerk tegen gevaren als ransomware en malware. Of het nu een telefoon, computer of een ander toestel is, elk toestel moet aan een aantal voorwaarden voldoen om toegang te krijgen tot het netwerk.

Waarom zouden we eindpunten moeten beveiligen?

De dagen dat medewerkers op het netwerk gingen van een vaste computer in een bedrijf, zijn voorbij. Moderne organisaties hebben honderdduizenden eindpunten. En dit aantal zal alleen nog maar toenemen door de opkomst van Industrial Internet of Things (IIoT). Een gemiddelde medewerker heeft toegang tot een netwerk van een bedrijf via een desktop PC, een werklaptop, een werktelefoon en persoonlijke toestellen, vanaf welke locatie dan ook. Hoe meer eindpunten er zijn, hoe meer potentiële routes hackers zullen vinden om te infiltreren in de IT-infrastructuur.

Het is belangrijk om een goed toegangsbeleid te hebben, waardoor vermeden wordt dat ongeautoriseerde apparaten toegang krijgen. Echter, het is onmogelijk om maatregelen per persoon toe te passen. Endpoint Privilege Management geeft de controle en is in lijn met de regelgeving GDPR, NIS en PCI-DSS, zonder dat dit ten koste gaat van de productiviteit van gebruikers.

Hoe werkt Eindpunt Privilege Management?

Endpoint Privilege Management (EPM) geeft beheerders de mogelijkheid om met een gecentraliseerde aanpak gebruikers te identificeren en de toegang tot het bedrijfsnetwerk te beheren. EPM vermindert het risico op het toekennen van te veel bevoegdheden, aangezien er wordt gestimuleerd om op applicatie- en procesniveau na te denken over het toekennen van bevoegdheden in plaats van op gebruikersniveau. Beheerders kunnen toegangsmachtigingen instellen, zodat zelfs persoonlijke apparaten buiten de eigen netwerkomgeving geen risico kunnen vormen voor bedrijfsmiddelen.

Als IT-beheerders het principe van least privilege ook toepassen op bepaalde IIoT eindpunten, dan zal de IT-infrastructuur extra beschermd zijn, en dan komt dit de productiviteit van gebruikers ten goede.

Een eenduidig beleid rond het toekennen van rechten, rollen en controles op procesniveau, geeft het IT-team de mogelijkheid om met labels, zoals black list, grey list of white list voor applicaties en acties werken. De dagelijkse taken van gebruikers worden niet verstoord. Gebruikers hoeven niet met IT te bellen om een tool te downloaden die belangrijk is voor het werk. De eindpunten blijven beveiligd en de toegang beperkt tot een minimum, zelfs voor gebruikers met verhoogde bevoegdheden.

Conclusie

Beeld u in hoe de voorbeelden uit deze handleiding samenkomen. Een onderaannemer heeft toegang nodig tot een database van het bedrijf om haar taken te kunnen uitvoeren. Ze logt in op het bedrijfsnetwerk via een persoonlijke tablet. Het bedrijf heeft een IAM-procedure, waardoor haar identiteit geauthentiseerd kan worden met MFA: ze krijgt een tijdelijk wachtwoord en een code die gegenereerd is door een RSA-token.

Het PAM systeem autoriseert de toegang tot de server en de bronnen die ze nodig heeft. Vervolgens wordt haar sessie opgenomen en gemonitord terwijl ze aan het werk is binnen het netwerk. Wanneer ze toegang nodig heeft tot meer bronnen, dan kan ze deze tijdelijke extra bevoegdheden aanvragen bij het IT-team. EPM geeft de onderaannemer de mogelijkheid om met haar toestel apps te downloaden en hiermee te werken, maar met de criteria van het bedrijf. Aan het einde van de taak, als haar werk is voltooid, zal het PAM-systeem door een automatische controle, het bronwachtwoord afwisselen, en trekt het haar verhoogde privileges in. Het PAM systeem verwijdert haar toegangsprivileges van het netwerk van het bedrijf wanneer de taak voldaan is.

Dit voorbeeld geeft inzicht in hoe PAM en EPM kunnen bijdragen tot een goed beveiligd toegangsbeheer, als onderdeel van een overkoepelende IAM-strategie.

Over WALLIX

WALLIX beschermt identiteiten en toegang tot IT-infrastructuur, applicaties en gegevens. WALLIX-oplossingen, specifiek op het gebied van Privileged Access Management, zorgen voor naleving van de nieuwste IT-beveiligingsstandaarden en beschermen systemen tegen cyberaanvallen, diefstal en datalekken als gevolg van gestolen toegangsgegevens en verhoogde toegangsprivileges tot gevoelige bedrijfsmiddelen.

WWW.WALLIX.COM

WALLIX
CYBERSECURITY SIMPLIFIED