De Asset Centric en User Centric Benaderingen van Security

Samenvatting

In de haast om aan regelgeving of klanteisen te voldoen, hebben organisaties miljoenen uitgegeven aan het implementeren van security en compliance maatregelen, hetzij per situatie hetzij per maatregel. Dit heeft geresulteerd in een asset-centric security benadering, waarbij we focussen op de IT infrastructuur en zorgen dat deze veilig is.

In de huidige veelzijdige gebruikers gemeenschap is een gebruiker echter niet langer gebonden aan één enkel apparaat. Dus, hoewel het nog steeds nodig is om de assets te beveiligen, ontstaat er nu behoefte aan een user-centric benadering van security waarbij de security regels in lijn zijn met het gebruik van deze assets.

Deze whitepaper geeft een overzicht van zowel de asset-centric als de user-centric aanpak van security. Deze invalshoeken zullen worden gerelateerd aan de standaard voor Informatie Security: ISO 27001.

Security

Waarom is Security belangrijk?

Informatie is een belangrijke asset in onze huidige markt. Daarom willen bedrijven informatie beheren als zijnde een asset, tegelijkertijd ontwikkelen zij steeds meer samenwerkingsverbanden met andere bedrijven om sneller aan de wensen van een klant tegemoet te kunnen komen. Dit heeft de druk op IT afdelingen aanzienlijk verhoogd. Enerzijds moeten ze informatie beschikbaar maken voor meer gebruikers. Anderzijds moeten ze zorgen dat deze informatie veilig blijft en alleen wordt gedeeld met de juiste individuen en organisaties.

Security is dus belangrijk en iedere benadering zal op twee onderwerpen moeten focussen:

- Beschikbaarheid: ervoor zorgen dat informatie beschikbaar is voor gebruik.
- Veiligheid: ervoor zorgen dat alleen geautoriseerde personen er toegang tot hebben.

Beschikbaarheid

Op dit moment is een belangrijke taak van veel beheerders ervoor zorgen dat geautoriseerde gebruikers wanneer nodig toegang hebben tot informatie en de bijbehorende assets.

Focus op assets

Vandaag de dag is de meest gebruikte aanpak het focussen op assets. Deze benadering komt voort uit een risk management strategie:

In een Microsoft Windows omgeving betekent dit dat de volgende taken op regelmatige basis moeten worden uitgevoerd:

- Het scannen van machines op kwetsbaarheden, dat wil zeggen zoekopdrachten naar geïnstalleerde besturingssysteem patches en geïnstalleerde software, querying NTFS en share right assignments, querying service properties en het draaien van MBSA queries.
- Het nemen van tegenmaatregelen voor bepaalde risico's, dat wil zeggen het installeren van patches, het veranderen van service parameters, het veranderen van NTFS en share rights assignments.

Deze standaard en regelmatig terugkerende taken kunnen eenvoudig worden geautomatiseerd met een oplossing voor automation voor Windows, zoals RES Automation Manager.

Gebruikers zijn niet langer gebonden aan één enkel apparaat.

De vraag is of deze asset-centric benadering, die bedreigingen als externe krachten definieert, genoeg is. Zorgt deze aanpak voor

beschikbaarheid van de service? In de huidige gebruikersomgeving is Bring Your Own Device (BYOD) eerder regel dan uitzondering. Een gebruiker brengt zijn persoonlijke tablet, smart phone of laptop (asset) naar kantoor omdat ze de gebruiksvriendelijkheid en snelheid van applicatie levering prettig vinden. Dit resulteert in nieuwe uitdagingen voor IT afdelingen, omdat de prioriteit ligt bij de beschikbaarheid van de services voor een gebruiker.

Gebruikers willen dat hun services (applicaties plus hun instellingen) beschikbaar zijn, ongeacht de delivery methode, en zij willen wijzigingen, die zij in de ene omgeving maken, automatisch terug zien in alle andere. Dit resulteert in de volgende benadering van beschikbaarheid: the user-centric benadering, die wordt bereikt door middel van user workspace management. In deze aanpak worden alle gebruikersinstellingen losgekoppeld van de onderliggende applicatie delivery oplossing, en worden toegepast zodra een gebruiker een applicatie start. Dit geeft de gebruiker een uniforme workspace, onafhankelijk van een applicatie delivery oplossing.

Nieuwe Uitdagingen: Vertrouwelijkheid

Door te focussen op de beschikbaarheid van services voor gebruikers, zowel binnen als buiten kantoor, worden de gebruikersproductiviteit en de business performance verbeterd.

Echter, deze benadering brengt wel nieuwe uitdagingen met zich mee voor de IT afdeling, en deze uitdagingen moeten geadresseerd worden. Een gebruiker heeft nu ook buiten het kantoor toegang tot het bedrijfsnetwerk, maar sommige services en bijbehorende resources zouden niet buiten het kantoor beschikbaar moeten zijn.

Wanneer u de beschikbaarheid van een service voor een gebruiker hebt gerealiseerd dient u ervoor te zorgen dat deze service alleen beschikbaar is voor hen die geautoriseerd zijn. Dit is vertrouwelijkheid, de focus van het volgende deel van deze whitepaper.

Vertrouwelijkheid

Er voor zorgen dat informatie alleen toegankelijk is voor diegenen die geautoriseerd zijn voor toegang is een uitdagende taak in de huidige omgeving. Als een gebruiker niet gebonden is aan één enkel werkstation is het niet langer mogelijk om toegang op basis van het werkstation (asset) toe te staan of te verbieden. De asset-centric benadering, hoe belangrijk ook, is niet voldoende. Een user-centric benadering is ook nodig, zodat een gebruiker toegang kan krijgen tot de services, maar alleen na de volgende checks:

- Wie is de gebruiker? Deze vraag wordt beantwoord door het gebruik van authenticatie op basis van username en password.
- Waar is de gebruiker? Dit is belangrijk omdat de locatie waarvan een gebruiker een service start kan bepalen of deze service (zoals de applicatie plus de instellingen en resources) beschikbaar zou moeten zijn.
- Hoe laat is het? Sommige services kunnen geplande tijdsvensters voor onderhoudswerkzaamheden hebben en gedurende deze tijd niet beschikbaar zijn.
- Heeft een gebruiker de benodigde geloofsbrieven? In sommige gevallen wilt u de toegang tot een service wellicht baseren op aanvullende authenticatie niveaus omdat de applicatie te veel gevoelige informatie bevat.

Naast de interne gebruiker werken bedrijven steeds meer samen met andere bedrijven. Deze samenwerkingsverbanden zullen informatie moeten delen en dus moeten ze worden ondersteund door IT. De aanpak die gebaseerd is op assets probeert ervoor te zorgen dat externe bedreigingen niet binnen kunnen komen. Dit is niet mogelijk in een organisatie met samenwerkingsverbanden omdat mensen van andere bedrijven in uw netwerk moeten kunnen komen. U wilt ze echter alleen toegang geven tot de services die zij nodig hebben. Dit vereist een andere benadering - één die van binnenuit naar buiten werkt in plaats van andersom. Dit is wat u kunt geven met een user-centric security benadering.

U geeft een gebruiker toegang tot een service, namelijk de applicatie met de instellingen. Op basis van deze toegang kunt u daarna de gebruiker toegang geven tot gerelateerde:

- Files en folders
- Lokale storage
- Removable storage
- Netwerk resources
- Apparaten

Conclusie

De ISO 17799 standaard is gerelateerd aan informatie security. Deze standaard definieert informatie als een asset die in vele vormen kan voorkomen en waarde heeft voor een organisatie. Het doel van informatie security is deze asset naar behoren te beschermen zodat business continuïteit kan worden gegarandeerd, schade aan het bedrijf wordt geminimaliseerd en return on investment wordt gemaximaliseerd. Volgens ISO 17799, wordt informatie security gekarakteriseerd als het behoud van:

- Integriteit: het indekken van de juistheid en volledigheid van informatie en van beveiligingsmethoden.
- Beschikbaarheid: ervoor zorgen dat geautoriseerde gebruikers, wanneer nodig, toegang hebben tot informatie en bijbehorende assets.
- Vertrouwelijkheid: zorgen dat informatie alleen toegankelijk is voor diegenen die daartoe geautoriseerd zijn.

Zoals besproken in de voorgaande paragrafen, zijn er twee benaderingen van Informatie Security: asset-centric en user-centric. De asset-centric benadering zorgt ervoor dat de infrastructuur beschikbaar is en helpt deze te beschermen tegen externe bedreigingen. In de huidige veelzijdige gebruikersomgeving echter, is deze benadering op zichzelf niet voldoende om services beschikbaar te maken voor gebruikers. Omdat de gebruiker werkt vanaf meerdere desktops, zowel binnen als buiten het bedrijfsnetwerk, is tevens een user-centric benadering noodzakelijk. Het combineren van deze twee methoden zal resulteren in een betere beschikbaarheid maar belangrijker nog, zal de vertrouwelijkheid zoals beschreven in ISO 27001, aanzienlijk verbeteren. De user-centric security aanpak wordt geleverd door middel van user workspace management. Dit geeft de gewenste beschikbaarheid van de services aan eindgebruikers, zonder het noodzakelijke security beleid in gevaar te brengen.

RES Software levert oplossingen voor zowel de asset- als user-centric security benadering.

Over RES Software

RES Software stelt IT-afdelingen in staat om de belangrijkste elementen van de computerervaring van een gebruiker centraal te leveren, beheren en beveiligen, onafhankelijk van werkstijlen en apparaten. Door de manier waarop IT-services aan virtuele werkplekken worden geleverd te automatiseren en door het verstrekken van een gebruiksvriendelijke 'IT Store', helpt RES Software IT-professionals de gevolgen van IT Consumerization, steeds meer vooruitstrevende zakelijke gebruikers, Bring Your Own Device-initiatieven en Cloudtechnologieën te beheersen. De gepatenteerde technologieën van RES Software worden wereldwijd gebruikt en worden ondersteund door een hoogwaardige klantenservice. Volg updates op Twitter @RESsoftware_NL en ga naar www.ressoftware.nl voor meer informatie.