advenica

Säker övervakning med Zabbix

Zabbix är en mjukvara baserad på öppen källkod som används för att övervaka IT-utrustning som servrar, nätverksutrustning, virtuella maskiner, etc. I en installation med Zabbix har man Zabbix proxies med uppgiften att samla in information från den närliggande utrustningen för att sen skicka vidare denna information till en centralt placerad Zabbix-server. Zabbix-servern sammanställer informationen och gör den tillgänglig för en operatör. Operatören kan i Zabbix server definiera vyer, grafer, larmvillkor, m.m. för att underlätta och effektivisera sitt arbete.

Utmaning

Spridning av skadlig kod i känsliga system

I en segmenterad nätverksinfrastruktur där Zabbix proxy och Zabbix server placeras i olika zoner behöver kommunikationen mellan dessa zoner övervakas och monitoreras. Övervakningszonen där Zabbix server är placerad kommunicerar med de zoner som har system som övervakas. Därför är det viktigt att säkerställa att en attack i någon av zonerna inte kan sprida sig vidare till övriga zoner och system via denna kommunikations-möjlighet. Zabbix server i övervakningszonen ska heller inte få åtkomst till fler tjänster eller applikationer i de andra zonerna än vad som tillåts via Zabbix.

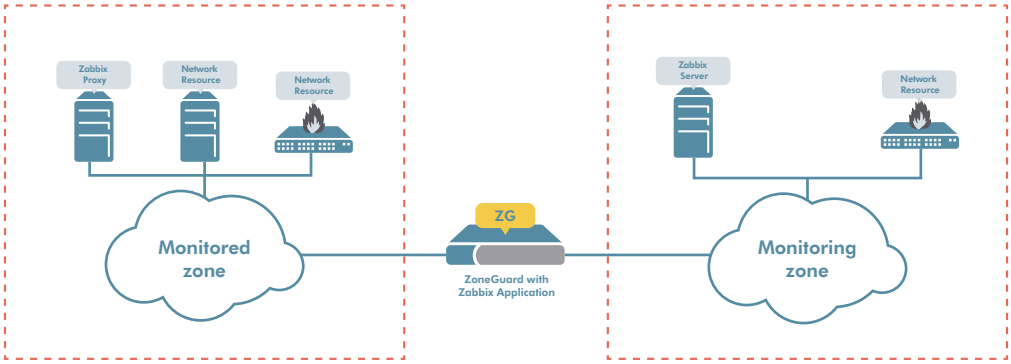
En attack mot Zabbix där en attackerare fjärrmässigt lyckas exekvera godtycklig kod i Zabbix server eller Zabbix proxy skulle vara katastrofal, eftersom den skulle kunna sprida sig till samtliga sammankopplade system. Även en enklare attack som tillfälligt stör tillgängligheten i övervakade system skulle även den med stor sannolikhet orsaka signifikanta problem med stora kostnader. Därför är det viktigt att noggrant övervaka kommunikationen och på så sätt minska attackvektorerna mot servrarna.

Lösning

Strikt kommunikation mellan Zabbix proxy och server

Det protokoll som används mellan Zabbix server och Zabbix proxy är baserat på JSON och denna lösning kontrollerar att kommunikationen uppfyller Zabbix protokollspecifikation som talar om exakt hur kommunikationen ska se ut. Lösningen bygger på Advenicas ZoneGuard, på vilken det installeras och konfigureras en applikation speciellt utvecklad för Zabbix.

Nuvarande version av lösningen stödjer version 4 av Zabbix i ”passive mode”, som innebär att det alltid är Zabbix server som initierar kommunikationen med Zabbix proxy och inte tvärtom. Zabbix kan kommunicera både komprimerat och krypterat mellan server och proxy och lösningen stödjer komprimerad kommunikation men inte krypterad kommunikation.



Figur 1. ZoneGuard med Zabbix applikation för monitorering av kommunikationen mellan zonerna.

Fördelar

Strikt kommunikation som förhindrar attacker

Till skillnad från en vanlig brandvägg vet alltså denna lösning exakt hur Zabbix proxy och Zabbix server kommunicerar med varandra och kontrollerar att kommunikationen håller sig inom vad som är tillåtet. Detta hindrar en attackerare från att gå utanför specifikation för att utnyttja svagheter eller buggar i Zabbix implementation eller konfiguration. Dessa svagheter kan i värsta fall leda till att attackeraren tar över Zabbix server eller proxies för att i nästa steg attackera övriga system i zonen.

advenica

Advenica tillhandahåller expertis, hög assurans och cybersäkerhetslösningar i världsklass för kritisk data-inmotion upp till Top Secret-klassning. Med oss stärker länder, myndigheter och företag informationssäkerheten och digitaliserar ansvarsfullt. Bolaget grundades 1993 och har EU-godkännande på högsta säkerhetsnivå. Våra unika produkter designas, utvecklas och tillverkas i Sverige.

Läs mer på advenica.com

ISO 9001 CERTIFIED
ISO 14001 CERTIFIED