Syslog en fysieke beveiliging

Voor veel beveiligingssystemen is de beschikbaarheid en integriteit van cruciaal belang. Om de beschikbaarheid en integriteit van deze systemen te bewaken kan gebruik worden gemaakt van logging en monitoring van systeemgedrag en -activiteiten. Het spreekt voor zich dat de eisen en diepgang aan logging zwaarder worden naarmate de afhankelijkheid en het risico toenemen.

Het verzamelen en analyseren van systeemlogging uit beveiligingssystemen zoals toegangscontrole, inbraaksignalering, CCTV, camera's en niet te vergeten besturings PLC's wordt steeds vaker een 'must have' voor klanten. Logisch, in deze systemen wil je geen hackers hebben. Door met een zogenaamde SIEM oplossing continue de syslog berichten te monitoren kan veel proactiever worden gehandeld op mogelijke aanvallen door hackers.

SIEM Security Information & Event Monitoring (SIEM) is binnen de ICT-security ondertussen een geworteld begrip. Een SIEM geeft grip en inzicht in alle mogelijke risico's en bedreigingen voor het systeem en de netwerkbeveiliging. SIEM maakt het geautomatiseerd monitoren en controleren van het beveiligingsbeleid van een organisatie mogelijk. Een SIEM doet dit door real-time informatie te verzamelen uit logfiles van netwerkcomponenten, tools, securitycomponenten, servers, camera's, PLC's, applicaties en databases en deze vervolgens te correleren, analyseren en presenteren en om security threats te detecteren. Een belangrijk aspect hierbij is de correlatie, waarbij verbanden tussen logs gezocht worden. Hierdoor geeft een SIEM een overzichtelijk beeld van de actuele status van de cyber security.

Syslog In 1980 bedacht de Amerikaanse computerprogrammeur Eric Paul Allman het syslog protocol als onderdeel van Sendmail. Ondanks zijn leeftijd is het syslog protocol tot op de dag van vandaag hét mechanisme om systeemlogging te verzamelen en te versturen naar (bijvoorbeeld) een SIEM. In de internetstandaard RFC 3164 (later vervangen door RFC 5424) wordt het mechanisme waarmee syslog berichten worden verstuurd uitvoerig beschreven. Zo beschrijft de RFC dat syslog niet versleuteld wordt verstuurd en meestal gebruik maakt van UDP. Daarnaast kent het geen beperking van zogenaamde control characters (denk aan een backspace), waardoor een hacker berichten kan wijzigen. Een ander probleem met syslog is dat er geen replay-mogelijkheid beschikbaar is. Hierdoor kunnen berichten tijdens het transport van server naar SIEM voorgoed verloren gaan. Allman heeft tijdens het ontwerpen van syslog gekozen voor eenvoud en snelheid en heeft daardoor concessies moeten doen aan de security. Daarom moet syslog-verkeer altijd in een aparte en beveiligde VLAN worden afgehandeld. Daarnaast zijn er enkele onduidelijkheden in de beide RFC's waardoor er dialecten van het syslog protocol zijn ontstaan die zijn gebonden aan verschillende leveranciers. Bij deze dialecten komt het vaak voor dat headers niet conform RFC zijn of een eigen logformaat aanhouden en dat heeft weer gevolgen voor het correct inlezen in een SIEM.

Waarom geen SNMP? Ondanks de nadelen ten aanzien van de beveiliging en betrouwbaarheid van syslog blijven veel organisaties nog steeds gebruik maken van de stokoude en onveilige syslog methodiek. Waarom dan geen gebruik maken van SNMP zult u zich afvragen? Simple Network Management Protocol (SNMP) is een protocol dat in een TCP/IP netwerk wordt gebruikt om managementinformatie te kunnen uitwisselen. Deze managementinformatie maakt het mogelijk om de prestaties van het netwerk bij te houden, fouten op te sporen en netwerk capaciteitsplanning te doen. SNMP definieert ook SNMP-traps, die net als syslog, door de apparaten worden gestuurd wanneer het nodig wordt geacht om het optreden van een bepaalde gebeurtenis te melden. De belangrijkste reden hiervoor is de beperking van het aantal SNMP-berichten ten opzichte van het aantal syslog berichten. Sterker nog, voor een goede diepe en zwaardere monitoring met een SIEM zijn heel veel syslog-event berichten nodig, in sommige gevallen tot tienduizend syslog berichten per seconde. Zo kan één grote Cisco switch (Catalyst 6500) meer dan zesduizend verschillende Syslog-event berichten omvatten, terwijl de specifieke SNMP MIB voor dit apparaat ongeveer negentig trapmeldingen ondersteunt.

Fysieke beveiliging Veel technieken die gebruikt worden binnen de fysieke beveiliging zijn op IT-technologie gebaseerd. De integratie tussen fysieke beveiligingssystemen en IT neemt de komende jaren alleen maar toe. Denk aan IP-camera's of intercoms met daarop een app. Maar ook nu al zijn veel toegangscontrolesystemen uitgerust met een server met daarop een applicatie die onder andere de deurcontroles aanstuurt. Ook camerasystemen zijn vaak een server met daarop een applicatie en daaraan een IP-netwerk met IP-camera's. Omdat er een samensmelting ontstaat tussen fysieke beveiligingssystemen met IT-systemen worden er in de Programma's van Eisen voor beveiligingsinstallaties steeds vaker eisen gesteld aan de beschikbaarheid van syslog. Op dit ogenblik is slechts een handjevol systemen voorzien van syslog en zelfs de grote marktleiders laten het op dit punt afweten. Ook installateurs grijpen, teveel, naar SNMP en laten syslog links liggen, waardoor het SIEM niet goed kan werken en de cyber securityweerstand van de beveiligingsinstallaties tekort wordt gedaan.

■ Ronald Eygendaal

Ronald Eygendaal schrijft sinds 1990 over informatiebeveiliging, elektronische en technische beveiliging, fraudedetectie en -bestrijding en bewaking en beveiliging.

Bronnen:

https://tools.ietf.org/html/rfc5424

http://www.ciscopress.com/articles/article.asp?p=426638

http://www.cisco.com/c/en/us/td/docs/security/fwsm/fwsm41/system/message/syslog/logmsgs.html