Syslog en fysieke beveiliging

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

Het verzamelen en analyseren van systeem logging 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 men geen hackers. Door met een zogenaamde SIEM-oplossing voortdurend de Syslog berichten te monitoren kan men veel proactiever handelen 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 systeem- en netwerkbeveiligingsrisico's en bedreigingen. 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 en te analyseren en te 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 als onderdeel van Sendmail het Syslog protocol. Ondanks zijn leeftijd is Syslog tot op de dag van vandaag hét mechanisme om systeem logging 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 gebruikmaakt 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 replaymogelijkheid 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 apart beveiligd V-LAN worden afgehandeld. Daarnaast zijn er toch wat onduidelijkheden in de beide RFC's waardoor

er leveranciergebonden dialecten van het Syslog protocol zijn ontstaan. 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.

Omdat er een samensmelting ontstaat tussen fysieke beveiligingssystemen met IT-systemen worden er in de Programma's van Eisen voor beveiligingsinstallatie steeds vaker eisen gesteld aan de beschikbaarheid van Syslog.

Waarom geen SNMP?

Ondanks de nadelen ten aanzien van de beveiliging en betrouwbaarheid van Syslog blijven veel organisaties nog steeds gebruikmaken van de stokoude, onveilige Syslog methodiek. Waarom dan geen gebruikmaken 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 netwerkcapaciteitsplanning te doen. SNMP definieert ook SNMP-traps die, net als Syslog, door de apparaten kan worden gestuurd wanneer ze het nodig achten 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. (1 SNMP <> 60 Syslog) Sterker nog, voor een goede diepe en zwaardere monitoring met een SIEM zijn heel veel Syslog event berichten nodig. In sommige gevallen gaat dat tot 10.000 Syslog berichten per seconde. Een voorbeeld: zo kan één grote Cisco switch (Catalyst 6500) meer dan 6.000 verschillende Syslog event berichten omvatten en de specifieke SNMP MIB voor het apparaat ondersteunt ongeveer 90 trap meldingen.

Syslog en fysieke beveiliging

Veel technieken die gebuikt 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 bijvoorbeeld aan IP-camera's of intercoms met daarop een app. Maar ook nu al zijn veel toegangscontrole systemen uitgerust met een server met daarop een applicatie die onder andere de deurcontroles aanstuurt. Ook camera systemen zijn vaak gewoon 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 beveiligingsinstallatie steeds vaker eisen gesteld aan de beschikbaarheid van Syslog. Op dit ogenblik is slechts een handvol 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 security weerstand van de beveiligingsinstallaties te kort wordt gedaan.

Door Ronald Eygendaal

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

RFC 5424 The Syslog Protocol March 2009

6. Syslog Message Format

The syslog message has the following ABNF [RFC5234] definition:

```
SYSLOG-MSG      = HEADER SP STRUCTURED-DATA [SP MSG]

HEADER          = PRI VERSION SP TIMESTAMP SP HOSTNAME
                  SP APP-NAME SP PROCID SP MSGID
PRI             = "<" PRIVAL ">"
PRIVAL          = 1*3DIGIT ; range 0 .. 191
VERSION         = NONZERO-DIGIT 0*2DIGIT
HOSTNAME        = NILVALUE / 1*255PRINTUSASCII

APP-NAME        = NILVALUE / 1*48PRINTUSASCII
PROCID          = NILVALUE / 1*128PRINTUSASCII
MSGID           = NILVALUE / 1*32PRINTUSASCII

TIMESTAMP       = NILVALUE / FULL-DATE "T" FULL-TIME
FULL-DATE       = DATE-FULLYEAR "-" DATE-MONTH "-" DATE-MDAY
DATE-FULLYEAR   = 4DIGIT
DATE-MONTH      = 2DIGIT  ; 01-12
DATE-MDAY       = 2DIGIT  ; 01-28, 01-29, 01-30, 01-31 based on
                          ; month/year
FULL-TIME       = PARTIAL-TIME TIME-OFFSET
PARTIAL-TIME    = TIME-HOUR ":" TIME-MINUTE ":" TIME-SECOND
                  [TIME-SECFRAC]
TIME-HOUR       = 2DIGIT  ; 00-23
TIME-MINUTE     = 2DIGIT  ; 00-59
TIME-SECOND     = 2DIGIT  ; 00-59
TIME-SECFRAC    = "." 1*6DIGIT
TIME-OFFSET     = "Z" / TIME-NUMOFFSET
TIME-NUMOFFSET  = ("+" / "-") TIME-HOUR ":" TIME-MINUTE


STRUCTURED-DATA = NILVALUE / 1*SD-ELEMENT
SD-ELEMENT      = "[" SD-ID *(SP SD-PARAM) "]"
SD-PARAM        = PARAM-NAME "=" %d34 PARAM-VALUE %d34
SD-ID           = SD-NAME
PARAM-NAME      = SD-NAME
PARAM-VALUE     = UTF-8-STRING ; characters '"', '\' and
                               ; ']' MUST be escaped.
SD-NAME         = 1*32PRINTUSASCII
                  ; except '=', SP, ']', %d34 (")

MSG             = MSG-ANY / MSG-UTF8
MSG-ANY         = *OCTET ; not starting with BOM
MSG-UTF8        = BOM UTF-8-STRING
BOM             = %xEF.BB.BF
```