Syslog et protection physique

Pour de nombreux systèmes de protection, la disponibilité et l'intégrité revêtent une importance cruciale. Le logging ou enregistrement et le monitoring du comportement et des activités du système permettent de surveiller l'une et l'autre. Il est évident que les exigences et la profondeur de l'enregistrement s'alourdissent en fonction de la dépendance et du risque.

De plus en plus souvent, la collecte et l'analyse du système d'enregistrement (logging) de protection (contrôle des accès, alerte anti-intrusion, vidéosurveillance, caméras, sans oublier les PLC) constituent un impératif incontournable pour les clients. C'est logique, car dans ces systèmes, les hackers ne sont pas les bienvenus. Le monitoring permanent des messages Syslog à l'aide d'une solution SIEM permet d'agir de manière beaucoup plus proactive face aux piratages potentiels.

SIEM

Le concept de Security Information & Event Monitoring (SIEM) est désormais bien connu au sein de l'univers de la sécurité IT. Un SIEM permet de maîtriser et de visualiser la totalité des risques et menaces possibles dans un système ou un réseau. Il permet de suivre et de contrôler la politique de protection d'une organisation, en collectant des informations en temps réel dans les fichiers log des composants réseau ou sécurité , outils, serveurs, caméras, PLC, applications et base de données, puis en les corrélant, en les analysant et en les présentant, et afin de détecter les menaces. La corrélation, qui consiste à chercher des liens entre les logs, est un élément important du processus dans la mesure où elle permet à un SIEM de fournir une image claire du statut actuel de la cybersécurité.

Syslog

C'est en 1980 que le programmeur américain Eric Paul Allman a conçu le protocole Syslog en tant qu'élément de Sendmail. Bien qu'ancien, Syslog reste encore, à l'heure actuelle, le mécanisme par excellence permettant de collecter les systèmes d'enregistrement et les envoyer, par exemple, à un SIEM. La norme Internet RFC 3164 (remplacée ultérieurement par RFC 5424) décrit dans le détail le mécanisme d'envoi des messages Syslog. Elle stipule par exemple que Syslog n'est pas envoyé sous forme cryptée, et utilise généralement l'UDP. Le protocole n'est pas non plus limité au niveau des « caractères de contrôle » (comme le retour arrière), ce qui permet à un hacker de modifier des messages. Autre problème : Syslog ne dispose d'aucune possibilité de relecture, et il est donc possible que des messages se perdent définitivement lors du transfert du serveur vers le SIEM. En concevant Syslog, Allman a privilégié la simplicité et la rapidité, au détriment parfois de la sécurité.

C'est pourquoi le trafic Syslog doit toujours passer par un V-LAN sécurisé spécifique. De plus, les deux normes RFC contiennent un certain nombre d'imprécisions qui ont entraîné la naissance, au sein du protocole Syslog, de « dialectes » chez les fournisseurs. Ainsi, il arrive souvent que les entêtes ne respectent pas les RFC ou qu'ils contiennent un format de log propriétaire, ce qui n'est pas sans conséquences pour la lecture dans le SIEM.

Dans la mesure où les systèmes de protection physique fusionnent avec les systèmes informatiques, les cahiers des charges d'une installation de protection incluent de plus en plus souvent des exigences liées à la disponibilité de Syslog.

Pourquoi pas un SNMP ?

En dépit des inconvénients de Syslog au niveau de la protection et de la fiabilité, de nombreuses organisations continuent à utiliser ce protocole archaïque et peu sûr. Mais pourquoi, vous demandez-vous, ne pas passer à un SNMP ? *Le Simple Network Management Protocol* (SNMP) est utilisé dans un réseau TCP/IP pour échanger des informations d'administration. Ces informations permettent de tenir les performances du réseau à l'œil, de traquer les erreurs et de planifier la capacité du réseau. Le SNMP définit aussi des « traps » qui, tout comme Syslog, peuvent être envoyées par les appareils lorsqu'ils estiment nécessaire de signaler un évènement donné. La principale raison en est la limitation du nombre de messages SNMP par rapport à ceux que permet Syslog. (1 SNMP <> 60 Syslog). Mieux encore, pour un bon monitoring plus approfondi et plus lourd avec un SIEM, il faut une multitude de messages évènement Syslog, jusqu'à 10.000 par seconde dans certains cas. Exemple : un seul grand commutateur Sysco (Catalyst 6500) est capable d'inclure plus de 6000 messages évènement Syslog, tandis que le MIB SNMP spécifique de l'appareil supporte environ 90 traps.

Syslog et protection physique

De nombreuses techniques utilisées en matière de protection physique sont basées sur la technologie IT. L'intégration entre systèmes physiques et informatiques ne fera que se renforcer au cours des prochaines années, par exemple au niveau des caméras IP ou des intercoms reliés à une appli. Mais de nombreux systèmes de contrôle des accès sont déjà équipés d'un serveur relié à une application qui commande notamment les contrôles des portes. Les systèmes de caméras consistent souvent, eux aussi, en un serveur avec application et réseau IP de caméras IP. Pour fusionner les systèmes physiques et informatiques, les cahiers des charges d'une installation de protection incluent de plus en plus souvent des exigences liées à la disponibilité de Syslog. Actuellement, seuls quelques systèmes sont équipés de Syslog, et même les grands leaders du marché restent sur leur quant-à-soi. Les installateurs, eux aussi, ont (trop) tendance à se rabattre sur les SNMP et négligent Syslog, ce qui empêche le SIEM de fonctionner correctement et fragilise la cybersécurité des installations de protection.

Par Ronald Eygendaal

Sources :
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
```