Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité des systèmes d'information
CERT-FR

Paris, le 13 juin 2016
N° CERTFR-2016-ACT-024

Affaire suivie par :
CERT-FR

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTFR-2016-ACT-024

1 - Sonde de détection d'intrusions réseau - Comment implémenter les points de mesure ?

Une sonde de détection d'intrusions réseau est un équipement passif, elle ne s'insère donc pas en coupure sur un flux de production. Il est donc nécessaire, pour implémenter les points de mesure définis, d'assurer une duplication en temps réel de l'activité réseau à analyser.

Deux techniques différentes existent pour dupliquer un trafic réseau : la première, généralement appelée « port miroir », est logicielle, et s'appuie sur les équipements réseau déjà en place ; la seconde, généralement appelée « tap », s'appuie sur des boîtiers matériels dédiés à cette fonction. Nous allons voir les avantages et les inconvénients de ces deux solutions.

Port miroir

La majorité des commutateurs du marché permettent de configurer une recopie logicielle de tout ou partie du trafic sur un ou plusieurs ports physiques dédiés. Le port miroir peut être un choix peu coûteux, si les équipements existants d'un réseau disposent déjà de cette fonctionnalité.

Toutefois, la recopie logicielle du trafic n'est pas sans risque. En effet, si l'équipement atteint sa limite de capacité sur ses fonctions « principales » (comme par exemple : la commutation de paquets, le routage, etc.), des fonctions annexes comme la recopie de paquets peuvent être dégradées, entraînant dans un tel cas des pertes sur l'activité à superviser.

La recopie logicielle peut également altérer le signal, car les couches basses réseau sont analysées et traitées par les commutateurs. Cette technique ne garantit donc pas la recopie de l'intégralité du trafic commuté sur le réseau de production. Étant donné qu'un seul paquet perdu sur un flux volumineux peut empêcher l'analyse par la sonde ou l'évader, il est primordial de considérer ce problème et de superviser la charge des commutateurs, si cette technique est mise en place.

La mise en place d'un port miroir sur un équipement du réseau augmente aussi la consommation de ressources : cela peut donc également dégrader le réseau de production. Une attention particulière doit être apportée au fond de panier, car le débit total commuté par l'équipement est décuplé.

D'autre part, il est important d'intégrer les ports miroirs dans les procédures d'exploitation : lors du remplacement d'un équipement ou d'un changement de configuration, il faut s'assurer que la recopie est toujours opérationnelle et qu'il n'y a pas de perte d'une partie des flux.

Une erreur de configuration peut également autoriser des communications depuis le réseau de duplication, voire même entre la sonde et le réseau de production.

Par contre, la mise en oeuvre d'un port miroir peut se faire sans interruption du réseau en production à superviser, à condition de disposer de suffisamment de ports physiques libres au niveau des commutateurs où les points de mesure sont effectués.

TAP

Un TAP garantit la recopie stricte du signal reçu : aucune analyse des couches au-delà de celle physique n'est réalisée. Le signal est régénéré électriquement pour des TAP cuivre, et la lumière est divisée sur deux chemins pour les TAP fibre. La mise en oeuvre d'une duplication de trafic sur un réseau en production nécessite une brève interruption du lien à superviser : celle-ci correspond au temps nécessaire pour placer le boîtier TAP en « coupure », c'est-à-dire sur le chemin de câble.

Pour les TAP alimentés, un défaut d'alimentation arrête la duplication, mais le TAP reste passant pour le lien coupé, moyennant généralement une microcoupure de quelques millisecondes.

Pour les TAP fibre, une partie de la lumière incidente étant réfléchie et l'autre réfractée, le signal est affaibli en fonction de proportions précisées dans la documentation du TAP.

Contrairement au port miroir, le TAP garantit également l'isolation entre le réseau de production et le réseau de détection.

Le prix d'un boîtier de duplication de trafic (TAP) varie entre une centaine d'euros et un millier, en fonction du type de média à dupliquer.

Conclusion

En conclusion, bien que ces deux méthodes permettent la duplication du trafic, il est conseillé de privilégier l'utilisation d'équipement dédié afin de garantir la séparation entre le réseau de production et le réseau de détection, ainsi qu'une recopie à l'identique des flux réseau.

2 - Rappel des avis émis

Dans la période du 06 au 12 juin 2016, le CERT-FR a émis les publications suivantes :

- CERTFR-2016-AVI-190 : Vulnérabilité dans VLC Media Player
- CERTFR-2016-AVI-191 : Multiples vulnérabilités dans Google Android (Nexus)
- CERTFR-2016-AVI-192 : Multiples vulnérabilités dans Wireshark
- CERTFR-2016-AVI-193 : Multiples vulnérabilités dans Mozilla Firefox
- CERTFR-2016-AVI-194 : Multiples vulnérabilités dans les produits Symantec
- CERTFR-2016-AVI-195 : Multiples vulnérabilités dans PHP
- CERTFR-2016-AVI-196 : Multiples vulnérabilités dans SCADA les produits Siemens
- CERTFR-2016-AVI-197 : Vulnérabilité dans Citrix Xenserver
- CERTFR-2016-AVI-198 : Multiples vulnérabilités dans les produits VMware
- CERTFR-2016-AVI-199 : Multiples vulnérabilités dans le noyau Linux d'Ubuntu

Gestion détaillée du document

13 juin 2016 version initiale.