Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

X.1216

(09/2020)

SÉRIE X: RÉSEAUX DE DONNÉES, COMMUNICATION ENTRE SYSTÈMES OUVERTS ET SÉCURITÉ

Sécurité du cyberespace – Cybersécurité

Exigences en matière de collecte et de conservation de preuves relatives aux incidents de cybersécurité

Recommandation UIT-T X.1216

Union internationale des télécommunications

RECOMMANDATIONS UIT-T DE LA SÉRIE X

RÉSEAUX DE DONNÉES, COMMUNICATION ENTRE SYSTÈMES OUVERTS ET SÉCURITÉ

RÉSEAUX PUBLICS DE DONNÉES	X.1–X.199
INTERCONNEXION DES SYSTÈMES OUVERTS	X.200–X.299
INTERFONCTIONNEMENT DES RÉSEAUX	X.300–X.399
SYSTÈMES DE MESSAGERIE	X.400–X.499
ANNUAIRE	X.500–X.599
RÉSEAUTAGE OSI ET ASPECTS SYSTÈMES	X.600–X.699
GESTION OSI	X.700–X.799
SÉCURITÉ	X.800–X.849
APPLICATIONS OSI	X.850–X.899
TRAITEMENT RÉPARTI OUVERT	X.900–X.999
SÉCURITÉ DE L'INFORMATION ET DES RÉSEAUX	
Aspects généraux de la sécurité	X.1000–X.1029
Sécurité des réseaux	X.1030–X.1049
Gestion de la sécurité	X.1050–X.1069
Télébiométrie	X.1080–X.1099
APPLICATIONS ET SERVICES SÉCURISÉS (1)	
Sécurité en multidiffusion	X.1100–X.1109
Sécurité des réseaux domestiques	X.1110–X.1119
Sécurité des télécommunications mobiles	X.1120–X.1139
Sécurité de la toile	X.1140–X.1149
Protocoles de sécurité (1)	X.1150–X.1159
Sécurité d'homologue à homologue	X.1160–X.1169
Sécurité des identificateurs en réseau	X.1170–X.1179
Sécurité de la télévision par réseau IP	X.1180–X.1199
SÉCURITÉ DU CYBERESPACE	
Cybersécurité	**X.1200–X.1229**
Lutte contre le spam	X.1230–X.1249
Gestion des identités	X.1250–X.1279
APPLICATIONS ET SERVICES SÉCURISÉS (2)	
Communications d'urgence	X.1300–X.1309
Sécurité des réseaux de capteurs ubiquitaires	X.1310–X.1319
Sécurité des réseaux électriques intelligents	X.1330–X.1339
Courrier certifié	X.1340–X.1349
Sécurité de l'Internet des objets (IoT)	X.1360–X.1369
Sécurité des systèmes de transport intelligents	X.1370–X.1389
Sécurité de la technologie des registres distribués	X.1400–X.1449
Protocoles de sécurité (2)	X.1450–X.1459
ÉCHANGE D'INFORMATIONS SUR LA CYBERSÉCURITÉ	
Aperçu général de la cybersécurité	X.1500–X.1519
Échange concernant les vulnérabilités/les états	X.1520–X.1539
Échange concernant les événements/les incidents/l'heuristique	X.1540–X.1549
Échange de politiques	X.1550–X.1559
Heuristique et demande d'informations	X.1560–X.1569
Identification et découverte	X.1570–X.1579
Échange garanti	X.1580–X.1589
SÉCURITÉ DE L'INFORMATIQUE EN NUAGE	
Aperçu de la sécurité de l'informatique en nuage	X.1600–X.1601
Conception de la sécurité de l'informatique en nuage	X.1602–X.1639
Bonnes pratiques et lignes directrices concernant la sécurité de l'informatique en nuage	X.1640–X.1659
Mise en œuvre de la sécurité de l'informatique en nuage	X.1660–X.1679
Sécurité de l'informatique en nuage (autres)	X.1680–X.1699
COMMUNICATIONS QUANTIQUES	
Terminologie	X.1700–X.1701
Générateur quantique de nombres aléatoires	X.1702–X.1709
Cadre de sécurité pour les réseaux QKDN	X.1710–X.1711
Conception de la sécurité pour les réseaux QKDN	X.1712–X.1719
Techniques de sécurité pour les réseaux QKDN	X.1720–X.1729
SÉCURITÉ DES DONNÉES	
Sécurité des mégadonnées	X.1750–X.1759
SÉCURITÉ DE LA 5G	X.1800–X.1819

Pour plus de détails, voir la Liste des Recommandations de l'UIT-T.

Recommandation UIT-T X.1216

Exigences en matière de collecte et de conservation de preuves relatives aux incidents de cybersécurité

Résumé

La Recommandation UIT-T X.1216 décrit une procédure générale pour les interventions et les enquêtes en cas d'incident de cybersécurité. Elle contient une analyse des sources des preuves relatives aux incidents de cybersécurité et précise les exigences relatives aux capacités des outils utilisés pour collecter et conserver ces preuves dans le cadre d'une procédure d'enquête. La présente Recommandation précise en outre les exigences relatives à la garantie de fiabilité des outils, qui serviront de lignes directrices aux développeurs qui conçoivent des outils de ce type.

Historique

Édition	Recommandation	Approbation	Commission d'études	Identifiant unique*
1.0	UIT-T X.1216	03-09-2020	17	11.1002/1000/14259

Mots clés

Cybersécurité, preuve relative à un incident de cybersécurité, intervention et enquête en cas d'incident.

* Pour accéder à la Recommandation, reporter cet URL http://handle.itu.int/ dans votre navigateur Web, suivi de l'identifiant unique, par exemple http://handle.itu.int/11.1002/1000/11830-en.

AVANT-PROPOS

L'Union internationale des télécommunications (UIT) est une institution spécialisée des Nations Unies dans le domaine des télécommunications et des technologies de l'information et de la communication (ICT). Le Secteur de la normalisation des télécommunications (UIT-T) est un organe permanent de l'UIT. Il est chargé de l'étude des questions techniques, d'exploitation et de tarification, et émet à ce sujet des Recommandations en vue de la normalisation des télécommunications à l'échelle mondiale.

L'Assemblée mondiale de normalisation des télécommunications (AMNT), qui se réunit tous les quatre ans, détermine les thèmes d'étude à traiter par les Commissions d'études de l'UIT-T, lesquelles élaborent en retour des Recommandations sur ces thèmes.

L'approbation des Recommandations par les Membres de l'UIT-T s'effectue selon la procédure définie dans la Résolution 1 de l'AMNT.

Dans certains secteurs des technologies de l'information qui correspondent à la sphère de compétence de l'UIT-T, les normes nécessaires se préparent en collaboration avec l'ISO et la CEI.

NOTE

Dans la présente Recommandation, l'expression "Administration" est utilisée pour désigner de façon abrégée aussi bien une administration de télécommunications qu'une exploitation reconnue.

Le respect de cette Recommandation se fait à titre volontaire. Cependant, il se peut que la Recommandation contienne certaines dispositions obligatoires (pour assurer, par exemple, l'interopérabilité et l'applicabilité) et on considère que la Recommandation est respectée lorsque toutes ces dispositions sont observées. Le futur d'obligation et les autres moyens d'expression de l'obligation comme le verbe "devoir" ainsi que leurs formes négatives servent à énoncer des prescriptions. L'utilisation de ces formes ne signifie pas qu'il est obligatoire de respecter la Recommandation.

DROITS DE PROPRIÉTÉ INTELLECTUELLE

L'UIT attire l'attention sur la possibilité que l'application ou la mise en œuvre de la présente Recommandation puisse donner lieu à l'utilisation d'un droit de propriété intellectuelle. L'UIT ne prend pas position en ce qui concerne l'existence, la validité ou l'applicabilité des droits de propriété intellectuelle, qu'ils soient revendiqués par un membre de l'UIT ou par une tierce partie étrangère à la procédure d'élaboration des Recommandations.

A la date d'approbation de la présente Recommandation, l'UIT n'avait pas été avisée de l'existence d'une propriété intellectuelle protégée par des brevets à acquérir pour mettre en œuvre la présente Recommandation. Toutefois, comme il ne s'agit peut-être pas de renseignements les plus récents, il est vivement recommandé aux développeurs de consulter la base de données des brevets du TSB sous http://www.itu.int/ITU-T/ipr/.

Table des matières

Recommandation UIT-T X.1216

Exigences en matière de collecte et de conservation de preuves relatives aux incidents de cybersécurité

1 Domaine d'application

La présente Recommandation décrit une procédure générale pour les interventions et les enquêtes en cas d'incident de cybersécurité. Elle contient une analyse des sources des preuves relatives aux incidents de cybersécurité et précise les exigences relatives aux capacités des outils utilisés pour collecter et conserver ces preuves dans le cadre d'une procédure d'enquête. La présente Recommandation précise en outre les exigences relatives à la garantie de fiabilité de ces outils, qui serviront de lignes directrices aux développeurs qui conçoivent des outils de ce type.

La présente Recommandation ne porte pas sur les questions de confidentialité ni les réglementations relatives à l'obtention de données sur les incidents de sécurité, aux poursuites judiciaires, aux procédures disciplinaires et à d'autres mesures connexes liées au traitement des possibles preuves relatives à un incident de cybersécurité. Il est considéré que ces éléments ne relèvent pas des activités "de collecte et de conservation".

2 Références

Les Recommandations UIT-T et autres références suivantes contiennent des dispositions qui, par suite de la référence qui y est faite, constituent des dispositions de la présente Recommandation. Au moment de la publication, les éditions indiquées étaient en vigueur. Les Recommandations et autres références étant sujettes à révision, les utilisateurs de la présente Recommandation sont invités à rechercher la possibilité d'appliquer les éditions les plus récentes des Recommandations et autres références énumérées ci-dessous. Une liste des Recommandations UIT-T en vigueur est publiée périodiquement. La référence à un document figurant dans la présente Recommandation ne donne pas à ce document en tant que tel le statut de Recommandation.

Aucune.

3 Définitions

3.1 Termes définis ailleurs

La présente Recommandation emploie les termes suivants définis ailleurs:

3.1.1 collecte [b-ISO/CEI 27037]: processus consistant à rassembler des éléments physiques contenant des preuves numériques éventuelles.

3.1.2 preuve [b-UIT-T X.813]: information qui, par elle-même ou par association avec d'autres informations, peut être utilisée pour résoudre un litige.

3.1.3 investigation [b-ISO/CEI 27042]: application d'examens, d'analyses et d'interprétations destinés à favoriser la compréhension d'un incident.

3.1.4 conservation [b-UIT-R BR.1351]: opérations de maintenance à effectuer pour assurer une bonne conservation du contenu archivé, par exemple vérification régulière de l'état de détérioration du support et copie du contenu sur de nouveaux supports, lorsque cela est nécessaire.

3.1.5 atteinte à la sécurité [b-UIT-T E.409], **[b-IETF RFC 2828]**: tout événement préjudiciable pouvant menacer certains aspects de la sécurité.

3.1.6 timbre horodateur [b-ISO/CEI 27037]: paramètre variant dans le temps, qui désigne un point sur l'axe des temps par rapport à une référence commune.

3.2 Termes définis dans la présente Recommandation

La présente Recommandation définit les termes suivants:

3.2.1 preuve relative à un incident de cybersécurité: information ou donnée, stockée ou transmise sous forme binaire, pour laquelle il a été établi, dans le cadre du processus d'analyse, qu'elle était utile aux fins de l'enquête sur un incident de cybersécurité.

NOTE – Cette définition repose sur la définition des "preuves numériques" donnée dans la norme [b-ISO/CEI 27037].

3.2.2 défense par cible mouvante: mécanismes qui modifient automatiquement un ou plusieurs attributs du système, afin de rendre la surface vulnérable d'un système impossible à prévoir pour des pirates informatiques.

NOTE – Cette définition repose sur [b-Jajodia14].

4 Abréviations et acronymes

La présente Recommandation utilise les abréviations et acronymes suivants:

ARP protocole de résolution d'adresse (*address resolution protocol*)

BYOD apporter son propre dispositif (*bring your own device*)

DLL bibliothèque de liens dynamiques (*dynamic linked library*)

Fichier PE fichier exécutable portable (*portable executable file*)

IP protocole Internet (*Internet Protocol*)

MAC commande d'accès au support physique (*media access control*)

MTD défense par cible mouvante (*moving target defence*)

PII information d'identification personnelle (*personally identifiable information*)

WORM à écriture unique et à lecture multiple (*write once read many*)

5 Conventions

Dans la présente Recommandation:

L'expression "il est obligatoire" indique une exigence qui doit être strictement suivie et par rapport à laquelle aucun écart n'est permis pour pouvoir déclarer la conformité au présent document.

Le terme "devrait" indique une exigence qui est recommandée mais qui n'est pas absolument nécessaire. Cette exigence n'est donc pas indispensable pour déclarer la conformité.

6 Vue d'ensemble des preuves relatives aux incidents de cybersécurité

6.1 Procédure générale pour les interventions et les enquêtes en cas d'incident

Lorsqu'on analyse la cause d'un incident de cybersécurité, la collecte et la conservation des preuves relatives à l'incident en question sont un élément essentiel des interventions et de l'enquête correspondantes, car les données analysées concernant l'incidents de cybersécurité pourraient servir de preuves si le cas est porté en justice. En outre, les preuves rassemblées peuvent être utilisées pour examiner les vulnérabilités et ainsi améliorer la cybersécurité au sein d'une organisation.

La procédure d'enquête sur un incident, illustrée dans la Figure 1, comprend les phases successives suivantes:

− Préparation: cette phase correspond aux activités de préparation qui devraient être menées en amont en vue de pouvoir mener une enquête sur un incident.

– Détection: durant cette phase, un événement non autorisé, c'est-à-dire un incident, est observé. Selon la gravité de l'incident, une décision devrait être prise concernant la manière de procéder face à cet incident, en plus de collecter des données.
– Collecte: les données devraient être obtenues auprès des outils utilisés pour recueillir les données sur le trafic. Cette phase est très importante. Étant donné que les données sur le trafic sont échangées rapidement, il n'est pas possible de générer les mêmes données sur le trafic de réseau ultérieurement.
– Conservation: les données originales sur le trafic de réseau qui ont été obtenues devraient être stockées sur un dispositif de sauvegarde et un hachage de toutes les données devrait également être conservé.
– Enquête: durant cette phase, toutes les traces recueillies devraient être prises en compte. Les preuves sont analysées afin d'identifier les artéfacts liés à l'attaque. Les indicateurs sont classés et corrélés afin de déduire des observations importantes, à l'aide des schémas d'attaque existants. Le trajet utilisé pour l'attaque sera peut-être reconstruit et l'attribution permettra peut-être d'établir l'identité de l'auteur de l'attaque au moyen d'une analyse itérative effectuée durant cette phase, en vue de parvenir à une conclusion.
– Établissement de rapports: les observations et explications découlant de l'enquête devraient être présentées dans un langage compréhensible pour les acteurs juridiques.

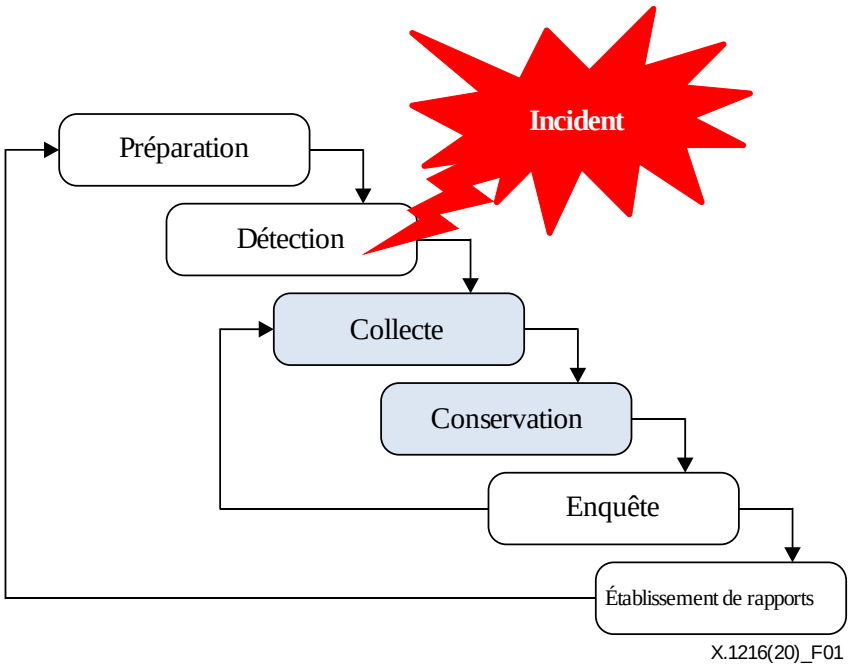

Figure 1 – Procédure générale d'enquête sur un incident

Diverses lignes directrices élaborées par l'ISO/CEI relatives aux enquêtes numériques et aux interventions en cas d'incident sont normalisées dans [b-ISO/CEI 27035-3], [b-ISO/CEI 27037], [b-ISO/CEI 27041], [b-ISO/CEI 27042] et [b-ISO/CEI 27043]. Ces lignes directrices visent avant tout à mettre à disposition des bonnes pratiques et à permettre le traitement des preuves numériques tout au long de la procédure d'enquête sur un incident. [b-IETF RFC 3227] fournit également des lignes directrices pour la collecte et l'archivage de preuves, par exemple pour les activités préparatoires et les considérations liées aux étapes de la collecte; la sélection des supports d'archive et des documents pour la chaîne de conservation; et l'ensemble des outils qui seront requis pour la collecte et l'archivage de preuves. Toutefois, les lignes directrices relatives à la sélection ou à la mise au point des outils d'enquête ne sont pas clairement décrites.

6.2 Sources des données relatives aux incidents de cybersécurité

Généralement, les sources des données relatives aux incidents de cybersécurité sont les dispositifs hôtes, les dispositifs de sécurité du réseau, les dispositifs de réseau et les réseaux. La Figure 2 illustre les informations par catégorie disponibles pouvant être obtenues auprès des sources de données.

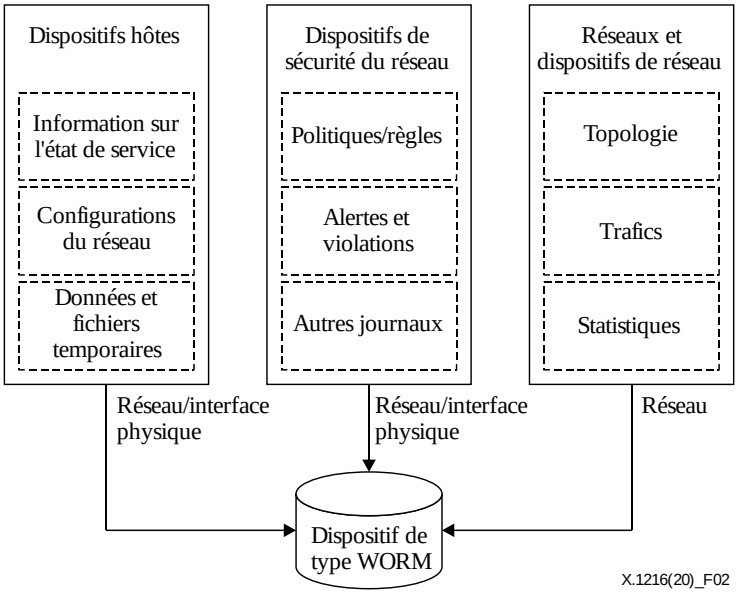

Figure 2 – Diverses sources permettant d'obtenir des données relatives aux incidents de cybersécurité

6.2.1 Dispositifs hôtes

En règle générale, un dispositif hôte fournit différents types de données relatives aux incidents de cybersécurité. Les outils de collecte de données devraient recueillir ces données avec prudence, étant donné que certaines données sont volatiles et peuvent être facilement détruites. Les types de données qui peuvent être recueillies depuis un dispositif hôte concernent:

1) L'état du système:
   - Informations générales (nom de l'hôte, informations sur le compte de l'utilisateur, date et heure associées au système, heure du dernier redémarrage, fuseau horaire actuel et périphérique de démarrage).
   - Informations sur le système d'exploitation (fabricant, nom, architecture, version, numéro de série et date d'installation).
   - Programmes d'application (programmes installés, état des correctifs et variables d'environnement).
   - Processus (table de processus, processus d'exécution automatique et services programmés).
   - Session de connexion.
   - Autres données des registres.
2) Le stockage des données:
   - Données en mémoire.
   - Systèmes de fichiers temporaires (fichiers récemment utilisés ou exécutés, y compris bibliothèque de liens dynamiques (DLL) et descripteurs).
   - Fichiers cachés, fichiers exécutables, fichiers ouverts, fichiers supprimés et zone non utilisée.

- Support d'archivage.
- Données partagées (dossiers partagés et dispositifs de réseau).

3) Les réseaux:
   - Table de routage, cache ARP (protocole de résolution d'adresse) et statistiques de type noyau.
   - Configurations du réseau (adresses IP, adresses MAC (commande d'accès au support physique), ports ouverts et interfaces de réseau).
   - Informations relatives au navigateur Internet (historique du navigateur Internet, objets Internet récemment consultés et cookies).

6.2.2 Dispositifs de sécurité du réseau

Les données relatives aux attaques devraient être recueillies auprès des dispositifs de sécurité du réseau, tels que des systèmes de détection des intrusions et des pare-feu:

- Politiques de sécurité (commande d'accès et règles de détection).
- Événements et journaux de sécurité (alertes, alarmes, avertissements et erreurs).
- Informations statistiques.

6.2.3 Réseaux et dispositifs de réseau

Lorsque l'on effectue une enquête sur une cyberattaque, il est important de rassembler des données auprès des réseaux. À titre d'exemple, les informations relatives à la topologie du réseau peuvent aider les personnes enquêtant sur un cyberincident à comprendre les composantes et les configurations du réseau d'une entreprise, à reconstruire les trajets utilisés pour une attaque, et à évaluer l'étendue des dégâts, et ce, en particulier lorsque la configuration du réseau change de manière dynamique, comme c'est le cas actuellement, avec le déploiement de l'informatique en nuage, de machines virtuelles et de technologies de sécurité MTD, et l'utilisation de dispositifs personnels dans un contexte professionnel (BYOD). On trouvera ci-dessous des exemples types de données fournies par les réseaux et les équipements de réseau:

- Configuration de la topologie du réseau.
- Journaux du routeur.
- Services en réseau.
- Informations relatives à l'hôte en réseau (ports ouverts, services exploités au niveau interne et état).
- Traces réseau (y compris un en-tête et des données).
- Données sur les flux de session (adresse IP/numéro de port d'origine, adresse IP/numéro de port de destination, protocole et autres informations d'en-tête TCP).
- Fichiers transférés via le réseau.
- Statistiques sur le trafic de réseau.

7 Exigences en matière de collecte de données relatives aux incidents de cybersécurité

De la même manière qu'il est important de décider quelles données doivent être recueillies en cas d'incident de cybersécurité, il est important de décider comment collecter, conserver et analyser ces données. La présente section décrit les capacités pour collecter des données relatives aux incidents de cybersécurité auprès des trois types de sources de données présentées dans le § 6.

Les données d'enregistrement et d'autres données relatives aux incidents qui sont recueillies auprès des sources de données peuvent contenir des informations d'identification personnelle (PII). Les personnes responsables de la mise en œuvre devraient limiter la collecte des informations PII à celles qui sont strictement nécessaires pour signaler et traiter un incident, et protéger les informations PII conformément aux lois et aux réglementations pertinentes et applicables.

7.1 Collecte de données relatives aux incidents de cybersécurité auprès des dispositifs hôtes

Les dispositifs hôtes sont généralement la principale source de données pour l'analyse des incidents de cybersécurité. Ils fournissent des données relatives aux registres, aux journaux et aux fichiers qui sont chargés par le système. Lorsqu'une analyse plus précise est requise, il convient de vider la mémoire du dispositif hôte pour en collecter les données.

Pour ce faire, l'outil de collecte doit être doté de capacités qui lui permettent d'effectuer notamment les opérations suivantes:

- examiner les processus et collecter les informations relatives aux processus;
- déterminer l'état du système;
- faire des copies bit par bit;
- générer des images du noyau;
- automatiser un processus de collecte;
- importer et exporter les données recueillies;
- prendre en charge différents systèmes d'exploitation des dispositifs hôtes;
- fournir les bibliothèques nécessaires pour la collecte de données et ne pas utiliser les bibliothèques des dispositifs hôtes;
- collecter des données volatiles pendant que le système fonctionne; et
- déterminer l'état réseau de la connexion en cours et du connecteur ouvert.

7.2 Collecte des données relatives aux incidents de cybersécurité auprès des dispositifs de sécurité du réseau

De nombreuses données utiles pour analyser un incident de cybersécurité devraient être recueillies auprès des dispositifs de sécurité du réseau, tels que les systèmes de protection contre les intrusions, les systèmes de détection des intrusions, les systèmes de prévention des intrusions, les systèmes de pare-feu et les systèmes de gestion des événements et des informations de sécurité.

Pour ce faire, l'outil de collecte doit être doté de capacités qui lui permettent d'effectuer notamment les opérations suivantes:

- recueillir les journaux d'événements auprès des dispositifs de sécurité du réseau;
- recueillir les alertes et les journaux de violation auprès des dispositifs de sécurité du réseau;
- recueillir les journaux d'authentification des utilisateurs auprès des dispositifs de sécurité du réseau;
- rassembler les politiques et les règles de sécurité des dispositifs de sécurité du réseau.

7.3 Collecte des données relatives aux incidents de cybersécurité depuis des réseaux et des dispositifs de réseau

L'organisation recueille des preuves et effectue une surveillance du réseau afin de détecter des points susceptibles de faire l'objet d'attaques au niveau interne. Si la surveillance du dispositif hôte ne s'avère pas efficace, la surveillance du réseau peut permettre d'étayer les preuves. La surveillance du réseau n'a pas pour objet de prévenir les attaques, mais plutôt de recueillir des informations utiles en cas d'incident et elle fournit par ailleurs beaucoup plus d'éléments à analyser. Afin de recueillir des données relatives aux incidents de sécurité auprès des réseaux ou des dispositifs de réseau, les outils de collecte de données doivent offrir les capacités suivantes:

- recueillir des informations sur le trafic du réseau sans perte;
- extraire le flux de session de la trace réseau et rassembler des informations sur le flux de session (telles que: adresse IP et numéro de port d'origine, adresse IP et numéro de port de destination, informations relatives au protocole IP et au service, heure de début/fin de la session, nombre et taille des paquets entrants, nombre et taille des paquets sortants);
- recueillir les fichiers exécutables portables (PE) transférés via le réseau et extraire des informations sur ces fichiers (telles que: nom du fichier, taille du fichier, heure de collecte du fichier, adresse IP et numéro de port d'origine de la session contenant le fichier PE, adresse IP et numéro de port de destination de la session contenant le fichier PE et protocole IP); et
- recueillir les journaux des dispositifs de réseau, tels que les routeurs, les commutateurs et les systèmes de surveillance du réseau.

8 Exigences en matière de conservation des données relatives aux incidents de cybersécurité

Afin d'analyser les causes des incidents de cybersécurité, il est nécessaire de conserver les données d'origine qui ont été recueillies et d'éviter qu'elles ne soient détériorées. En particulier, dans le cas d'une procédure judiciaire, il est nécessaire de conserver les données recueillies afin de préserver l'intégrité et la légitimité des preuves. Pour ce faire, les outils de conservation devraient prendre en charge les capacités suivantes:

- générer des sommes de contrôle et des signatures numériques;
- confirmer que les données recueillies sont conservées sans perte;
- générer des timbres horodateurs (en ms) pour l'heure de collecte et de conservation des données;
- enregistrer les données recueillies sur un dispositif de type "à écriture unique et à lecture multiple" (WORM);
- fournir un profil des politiques de conservation des données qui devrait être mis à jour en conséquence;
- s'assurer que les données recueillies sont conservées tant que la politique est en vigueur;
- conserver les données et les métadonnées recueillies dans une forme normalisée (différents éléments à prendre en considération en la matière sont précisés dans [b-UIT-T X.1215] et [b-UIT-T X.1541]).

9 Exigences relatives à la garantie de fiabilité des outils de collecte et de préservation

Les données recueillies et conservées par un outil de collecte et de conservation peuvent être utilisées en vue d'enquêter sur la cause des incidents de cybersécurité et comme preuves afin d'identifier les responsables.

Par conséquent, l'outil de collecte et de conservation des données pour l'analyse des incidents de cybersécurité doit être doté des capacités suivantes pour garantir la fiabilité en termes de gestion des utilisateurs et de gestion des données:

- L'outil devrait fournir un moyen de limiter et de contrôler l'accès des utilisateurs à l'outil lui-même et aux données stockées.
- L'outil ne devrait pas permettre les tentatives de remplacement, à modification ou de suppression des données conservées sans autorisation adéquate.
- L'outil devrait fournir des fonctions de gestion de la sécurité que les administrateurs autorisés peuvent configurer et utiliser pour gérer les fonctions de sécurité, les politiques de sécurité et les données importantes.
- Lors de la transmission des données recueillies entre des dispositifs physiquement séparés, les données doivent être chiffrées afin de garantir leur confidentialité et leur intégrité.
- Tous les moyens de communication associés à l'outil devraient utiliser un protocole de communication chiffrée.
- L'outil devrait fournir une fonction de sauvegarde des données conservées.
- L'outil devrait fournir des capacités permettant de tenir des journaux, de signaler les erreurs et d'effectuer des audits.
- L'outil devrait fournir des capacités permettant de traiter les métadonnées et le contenu formalisé et d'en assurer le partage conformément aux politiques existantes (comme précisé dans [b-UIT-T X.1550] et [b-UIT-T X.1582]).

Bibliographie

[b-UIT-T E.409] Recommandation UIT-T E.409 (2004), *Organisation en cas d'incident et prise en charge des incidents relatifs à la sécurité: lignes directrices destinées aux organisations de télécommunication*.

[b-UIT-T X.813] Recommandation UIT-T X.813 (1996), *Technologies de l'information – Interconnexion des systèmes ouverts – Cadres de sécurité pour les systèmes ouverts: non-répudiation*.

[b-UIT-T X.1215] Recommandation UIT-T X.1215 (2019), *Cas d'utilisation pour l'expression structurée d'informations sur les menaces*.

[b-UIT-T X.1541] Recommandation UIT-T X.1541 (2017), *Format d'échange de description d'objet incident version 2*.

[b-UIT-T X.1550] Recommandation UIT-T X.1550 (2017), *Modèles de contrôle d'accès applicables aux réseaux d'échange d'informations sur les incidents*.

[b-UIT-T X.1582] Recommandation UIT-T X.1582 (2014), *Protocoles de transport prenant en charge l'échange d'informations sur la cybersécurité*.

[b-UIT-R BR.1351] Recommandation UIT-R BR.1351 (1998), *Conditions à remplir pour utiliser la technologie du numérique dans les systèmes d'archivage audio en radiodiffusion.*

[b-IETF RFC 2828] IETF RFC 2828 (2000), *Internet Security Glossary*.

[b-IETF RFC 3227] IETF RFC 3227 (2002), *Guidelines for Evidence Collection and Archiving.*

[b-ISO/CEI 27035-3] ISO/CEI 27035-3, *Technologies de l'information − Techniques de sécurité – Gestion des incidents de sécurité de l'information − Partie 3: Lignes directrices relatives aux interventions en cas d'incident.*

[b-ISO/CEI 27037] ISO/CEI 27037:2012, *Technologies de l'information – Techniques de sécurité – Lignes directrices pour l'identification, la collecte, l'acquisition et la préservation de preuves numériques.*

[b-ISO/CEI 27041] ISO/CEI 27041:2015, *Technologies de l'information – Techniques de sécurité – Préconisations concernant la garantie d'aptitude à l'emploi et d'adéquation des méthodes d'investigation sur incident.*

[b-ISO/CEI 27042] ISO/CEI 27042:2015 *Technologies de l'information – Techniques de sécurité – Lignes directrices pour l'analyse et l'interprétation des preuves numériques.*

[b-ISO/CEI 27043] ISO/CEI 27043: 2015, *Technologies de l'information – Techniques de sécurité – Principes et processus d'investigation sur incident.*

[b-Jajodia14] Jajodia, Sushil, et Kun Sun. "MTD 2014: First ACM workshop on moving target defense". Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security. 2014.

SÉRIES DES RECOMMANDATIONS UIT-T

Série A	Organisation du travail de l'UIT-T
Série D	Principes de tarification et de comptabilité et questions de politique générale et d'économie relatives aux télécommunications internationales/TIC
Série E	Exploitation générale du réseau, service téléphonique, exploitation des services et facteurs humains
Série F	Services de télécommunication non téléphoniques
Série G	Systèmes et supports de transmission, systèmes et réseaux numériques
Série H	Systèmes audiovisuels et multimédias
Série I	Réseau numérique à intégration de services
Série J	Réseaux câblés et transmission des signaux radiophoniques, télévisuels et autres signaux multimédias
Série K	Protection contre les perturbations
Série L	Environnement et TIC, changement climatique, déchets d'équipements électriques et électroniques, efficacité énergétique; construction, installation et protection des câbles et autres éléments des installations extérieures
Série M	Gestion des télécommunications y compris le RGT et maintenance des réseaux
Série N	Maintenance: circuits internationaux de transmission radiophonique et télévisuelle
Série O	Spécifications des appareils de mesure
Série P	Qualité de transmission téléphonique, installations téléphoniques et réseaux locaux
Série Q	Commutation et signalisation et mesures et tests associés
Série R	Transmission télégraphique
Série S	Équipements terminaux de télégraphie
Série T	Terminaux des services télématiques
Série U	Commutation télégraphique
Série V	Communications de données sur le réseau téléphonique
Série X	**Réseaux de données, communication entre systèmes ouverts et sécurité**
Série Y	Infrastructure mondiale de l'information, protocole Internet, réseaux de prochaine génération, Internet des objets et villes intelligentes
Série Z	Langages et aspects généraux logiciels des systèmes de télécommunication

Imprimé en Suisse
Genève, 2020