Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

X.1214

(03/2018)

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

Sécurité du cyberespace – Cybersécurité

Techniques d'évaluation de la sécurité dans les réseaux de télécommunication/technologies de l'information et de la communication

Recommandation UIT-T X.1214

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.1429
Protocoles de sécurité (2)	X.1450–X.1459
ECHANGE D'INFORMATIONS SUR LA CYBERSÉCURITÉ	
Aperçu général de la cybersécurité	X.1500–X.1519
Echange concernant les vulnérabilités/les états	X.1520–X.1539
Echange concernant les événements/les incidents/l'heuristique	X.1540–X.1549
Echange de politiques	X.1550–X.1559
Heuristique et demande d'informations	X.1560–X.1569
Identification et découverte	X.1570–X.1579
Echange 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 oeuvre de la sécurité de l'informatique en nuage	X.1660–X.1679
Sécurité de l'informatique en nuage (autres)	X.1680–X.1699

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

Recommandation UIT-T X.1214

Techniques d'évaluation de la sécurité dans les réseaux de télécommunication/ technologies de l'information et de la communication

Résumé

La Recommandation UIT-T X.1214 décrit une méthode d'évaluation de la sécurité pour les éléments logiciels des réseaux de télécommunication/technologies de l'information et de la communication (TIC), ainsi que les bonnes pratiques en la matière à l'intention des développeurs, des fabricants, des opérateurs et des spécialistes de la sécurité exerçant dans le domaine des télécommunications, en vue de l'examen de la sécurité de leurs éléments logiciels. Les réseaux traditionnels à commutation de circuits et les réseaux en mode paquet sont exposés à différentes menaces et attaques, internes et externes, qui ciblent les divers éléments des réseaux de télécommunication/TIC. Dans ces réseaux, la présente Recommandation porte sur:

– la détection des vulnérabilités;

– la méthode d'évaluation de la sécurité.

Historique

Edition	Recommandation	Approbation	Commission d'études	Identifiant unique*
1.0	UIT-T X.1214	29-03-2018	17	11.1002/1000/13404

Mots clés

Analyse binaire, test à données aléatoires, test d'intrusion, évaluation de la sécurité, test de sécurité, examen du code source, recherche de vulnérabilités.

* 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 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

Introduction

Les réseaux de télécommunication/TIC jouent un rôle essentiel dans la croissance économique de la plupart des pays, ce qui a amené les pouvoirs publics à adopter, pour le secteur des télécommunications, une réglementation prévoyant des exigences visant à assurer la sécurité des équipements et des réseaux de télécommunication. Les opérateurs de télécommunication devraient adopter un programme de sécurité fiable et géré, afin de faire en sorte que les éléments logiciels de leurs réseaux soient protégés contre les attaques malveillantes, qu'elles viennent de l'extérieur ou de l'intérieur, tout en garantissant le respect des dispositions réglementaires au niveau local. Pour ce faire, un mécanisme d'évaluation de la sécurité très efficace fondé sur des normes et des bonnes pratiques en matière de sécurité acceptées partout dans le monde doit être en place pour ces éléments logiciels.

La mise en oeuvre constante d'un dispositif de sécurité cohérent dans l'ensemble du réseau d'une organisation face à des menaces qui évoluent en permanence est une tâche complexe et de longue haleine. Les organisations devront peut-être supporter des dépenses importantes pour se remettre d'une atteinte à la sécurité. Ces coûts sont liés aux mesures de correction, aux programmes de protection et de fidélisation des clients, aux activités juridiques, aux partenaires commerciaux découragés, à la baisse de la productivité des employés et à la diminution des recettes. Une méthode d'évaluation de la sécurité efficace aide les organisations à éviter ces écueils financiers en permettant d'identifier et de traiter en amont les risques pour leurs actifs et leurs capacités en matière de logiciels, avant même que ces organisations soient confrontées à une attaque ou à une atteinte à la sécurité. Les marchés (par exemple pouvoirs publics, secteur de la finance et télécommunications) exigent de plus en plus souvent une évaluation indépendante du point de vue de la sécurité.

La présente Recommandation porte essentiellement sur les techniques d'évaluation de la sécurité que les opérateurs de réseau de télécommunication/TIC et les fournisseurs de services devraient adopter pour identifier et évaluer en amont les vulnérabilités au niveau de leurs éléments logiciels.

Recommandation UIT-T X.1214

Techniques d'évaluation de la sécurité dans les réseaux de télécommunication/ technologies de l'information et de la communication

1 Domaine d'application

La présente Recommandation traite des techniques d'évaluation de la sécurité pouvant être utilisées pour les éléments logiciels des réseaux de télécommunication/technologies de l'information et de la communication (TIC). Les réseaux traditionnels à commutation de circuits et les réseaux de prochaine génération en mode paquet sont exposés à différentes menaces et attaques, internes et externes, qui ciblent les diverses parties des éléments logiciels d'un réseau de télécommunication/TIC. L'évaluation de la sécurité des éléments logiciels avant leur déploiement dans ces réseaux peut aider les opérateurs et les fournisseurs de services à renforcer considérablement la fiabilité des réseaux. En conséquence, ce domaine doit faire l'objet d'une normalisation, afin que des normes et des bonnes pratiques en matière d'évaluation globale de la sécurité des éléments logiciels puissent être mises à la disposition des développeurs, des fabricants, des opérateurs et des spécialistes de la sécurité.

Ces techniques peuvent être utilisées séparément ou de manière combinée, selon les souhaits ou les besoins.

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 d'une Recommandation.

[UIT-T X.1520] Recommandation UIT-T X.1520 (2014), *Vulnérabilités et expositions courantes*.

[UIT-T X.1524] Recommandation UIT-T X.1524 (2012), *Enumération des failles courantes*.

[UIT-T X.1544] Recommandation UIT-T X.1544 (2013), *Enumération et classification des schémas d'attaque courants.*

3 Définitions

3.1 Termes définis ailleurs

La présente Recommandation utilise les termes suivants définis ailleurs:

3.1.1 répertoire [UIT-T X.1524]: ensemble implicite ou explicite d'éléments sur les failles de sécurité dans les logiciels pris en charge par une capacité, par exemple une base de données des failles de sécurité, l'ensemble des configurations dans un analyseur de codes ou un site web.

3.1.2 vulnérabilité [UIT-T X.1520]: toute faille dans un logiciel susceptible d'être exploitée pour porter atteinte à un système ou aux informations qu'il contient.

3.1.3 faille [UIT-T X.1524]: lacune ou imperfection dans le code logiciel, la conception, l'architecture ou le déploiement, qui peut, à un moment donné, devenir une vulnérabilité ou peut contribuer à l'introduction d'autres vulnérabilités.

3.2 Termes définis dans la présente Recommandation

La présente Recommandation définit les termes suivants:

3.2.1 analyse binaire: technique d'identification des failles dans les fichiers exécutables en langage machine.

3.2.2 test à données aléatoires: technique permettant de découvrir des vulnérabilités inconnues ou nouvelles dans un logiciel en insérant dans le logiciel des données d'entrée inattendues et en observant les éventuelles anomalies.

3.2.3 mutation: manipulation d'octets, de mots ou de chaînes dans un paquet de données d'entrée.

3.2.4 test d'intrusion: technique permettant d'évaluer les incidences de l'exploitation de vulnérabilités identifiées.

3.2.5 évaluation de la sécurité: étude explicite visant à localiser les vulnérabilités et les risques en matière de sécurité.

3.2.6 recherche de vulnérabilités fondée sur les signatures: technique de recherche qui compare les contenus d'une cible à sa base de données de signatures connues afin d'identifier les vulnérabilités.

Si une signature donnée est repérée, le scanner identifie la vulnérabilité et propose également la mesure corrective.

3.2.7 examen du code source: technique d'identification des failles dans les segments de code logiciel écrits dans des langages de haut niveau.

3.2.8 outil: application logicielle ou dispositif qui examine un serveur, un réseau, un logiciel, un logiciel en binaire, une application logicielle ou un dispositif ou autre artefact, et produit des informations se rapportant aux vulnérabilités, aux failles ou aux expositions, par exemple un scanner de vulnérabilité, un outil de test à données aléatoires, un outil d'examen de code source, un analyseur binaire ou un outil de test d'intrusion.

3.2.9 recherche de vulnérabilités: technique d'identification des vulnérabilités connues ou répertoriées dans une cible.

4 Abréviations et acronymes

La présente Recommandation utilise les abréviations et acronymes suivants:

CAPEC énumération et classification des schémas d'attaque courants (*common attack pattern enumeration and classification*)

CVE vulnérabilités et expositions courantes (*common vulnerabilities and exposures*)

CWE énumération des failles courantes (*common weakness enumeration*)

DUT dispositif testé (*device under test*)

OS système d'exploitation (*operating system*)

SQL langage de requête structuré (*structured query language*)

TIC technologies de l'information et de la communication

5 Conventions

Néant.

6 Notion de base – Tests de sécurité

Les réseaux de télécommunication/TIC sont souvent une association hétérogène d'équipements provenant de différents fournisseurs. Un programme de certification par des tiers de confiance jouissant d'une grande crédibilité doit être en place en vue d'effectuer une évaluation visant à identifier et à évaluer les failles et les vulnérabilités en matière de sécurité contenues dans les mises en oeuvre logicielles, micrologicielles et matérielles des équipements. L'évaluation de la sécurité d'un produit porte principalement sur la détection et la validation des vulnérabilités que présente ce produit. La détection des vulnérabilités peut être divisée en deux grandes catégories (voir les § 6.1 et 6.2).

6.1 Détection des vulnérabilités connues ou répertoriées

On trouve des vulnérabilités logicielles dans les produits logiciels couramment utilisés au quotidien. Ces vulnérabilités, par exemple les vulnérabilités et expositions courantes (CVE), sont répertoriées dans la National Vulnerability Database (base de données nationale des vulnérabilités des Etats-Unis) et dans plusieurs autres bases de données. La gestion efficace des vulnérabilités répertoriées est ainsi un élément important des activités menées par les entreprises modernes dans le domaine de la sécurité. La surveillance manuelle de toutes les vulnérabilités présentes dans les systèmes et leur traitement adéquat sont des tâches gigantesques. Il existe des outils automatisés qui effectuent des recherches fondées sur les signatures afin de détecter ces vulnérabilités et de les identifier sur la base de la liste [b-CVE].

6.2 Détection des vulnérabilités inconnues ou nouvelles

Ce type de détection concerne la découverte de vulnérabilités qui n'ont encore jamais été répertoriées. Il existe pour ce faire différentes approches ayant chacune ses avantages et inconvénients. Il n'existe pas d'approche exhaustive et aucune méthode ne permet à elle seule de découvrir toutes les vulnérabilités possibles pour une cible donnée. Les outils et techniques utilisés pour détecter les vulnérabilités inconnues ou nouvelles sont par exemple les outils de test à données aléatoires, les outils d'examen du code source et les outils d'analyse binaire. Des précisions concernant ces outils figurent aux § 7.2 à 7.5.

7 Techniques de test de sécurité

Comme indiqué ci-dessus, il existe différentes approches pour détecter les vulnérabilités au niveau des éléments logiciels, ayant chacune ses avantages et inconvénients. Aucune méthode ne permet à elle seule de découvrir toutes les vulnérabilités possibles pour une cible donnée. En conséquence, un mécanisme d'évaluation efficace supposera nécessairement de recourir aux différentes approches présentées dans les § 7.1 à 7.5

7.1 Recherche de vulnérabilités

Un scanner de vulnérabilités de réseau est un appareil ou un logiciel utilisé pour inspecter l'architecture d'un réseau et signaler les éventuelles vulnérabilités identifiées au niveau des éléments logiciels du réseau. Pendant cette opération, on effectue une comparaison entre une base de données des signatures des vulnérabilités et les informations obtenues lors de l'inspection du réseau afin d'établir une liste des vulnérabilités dont on peut supposer qu'elles sont présentes dans le réseau. Le scanner de vulnérabilités est parfois doté d'un outil de test d'intrusion intégré, qui donne la possibilité d'exploiter effectivement les vulnérabilités identifiées pour vérifier si elles sont réellement présentes. L'analyse des vulnérabilités est le processus consistant à vérifier la gravité des vulnérabilités identifiées. L'environnement opérationnel des organisations comprend généralement de nombreuses vulnérabilités, dont certaines aboutissent à des risques plus graves que d'autres sur le plan de la sécurité. Par exemple, certaines vulnérabilités logicielles ont des conséquences désastreuses si elles sont exploitées. Il est par conséquent important d'évaluer les problèmes les plus graves et d'y remédier en premier.

La recherche de vulnérabilités peut généralement être effectuée sur les systèmes connectés à l'Internet, ainsi que sur les réseaux internes non connectés à l'Internet, afin d'évaluer les vulnérabilités logicielles.

Les outils, répertoires et services utilisés pour la recherche de vulnérabilités doivent être compatibles avec la liste CVE conformément aux exigences et fonctionnalités spécifiées dans [UIT-T X.1520].

7.2 Test à données aléatoires

Les tests à données aléatoires sont une méthode permettant de découvrir des vulnérabilités inconnues ou nouvelles dans un logiciel en insérant dans le logiciel des données d'entrée inattendues et en observant les éventuelles anomalies. Il s'agit généralement d'un processus automatisé ou semi-automatisé qui suppose de manipuler et de fournir de manière répétée des données au logiciel cible pour qu'il traite ces données. Selon que le logiciel cible est une pile de protocoles, une application ou des fichiers, on utilisera un outil de test à données aléatoires pour protocole, pour application ou pour fichier. Etant donné que le chercheur ou le testeur n'a pas besoin de connaître le fonctionnement interne de la cible, cette méthode est parfois également appelée méthode de test par boîte noire.

Il existe deux grands types de méthodes de test à données aléatoires, à savoir celles reposant sur la génération de données et celles reposant sur la mutation de données, qui sont décrites dans les § 7.2.1 et 7.2.2, respectivement.

7.2.1 Test à données aléatoires reposant sur la génération

Selon cette méthode, la mise au point du test commence par l'étude d'une spécification donnée pour comprendre toutes les structures de données prises en charge et les intervalles de valeurs acceptables pour chacune d'entre elles. On génère ensuite les données d'entrée pour les cibles, qui permettent de tester les conditions limites ou d'enfreindre complètement la spécification. Bien que sa mise au point puisse exiger un travail considérable en amont, ce type de test présente l'avantage de pouvoir être réutilisé pour tester de multiples mises en oeuvre d'un même protocole ou format de fichier.

7.2.2 Test à données aléatoires reposant sur la mutation

Les outils de test à données aléatoires reposant sur la mutation appliquent des mutations à des échantillons de données existantes sous la forme d'une capture de paquets liée à la cible pour mettre au point les tests. Chaque octet, mot ou chaîne contenu dans ces échantillons est manipulé et envoyé à la cible. Cette méthode ne nécessite que très peu de recherches au préalable et peut être mise en place en peu de temps. En revanche, elle n'est pas très efficace dans la mesure où elle peut nécessiter de rassembler de nombreux échantillons de données pour obtenir une couverture satisfaisante du protocole cible.

Les outils de test à données aléatoires sont efficaces pour les problèmes pouvant entraîner le blocage d'un programme; par exemple les débordements de la mémoire tampon, l'exécution de scripts intersites, les attaques par déni de service, les erreurs de format et l'injection de codes en langage de requête structuré (SQL). Les tests à données aléatoires sont moins efficaces pour faire face aux menaces de sécurité n'entraînant pas le blocage d'un programme, comme les logiciels espions ainsi que certains virus, vers informatiques, chevaux de Troie et enregistreurs de frappe.

Les outils, répertoires et services utilisés pour les tests à données aléatoires doivent être compatibles avec l'énumération des failles courantes (CWE) conformément aux exigences et fonctionnalités spécifiées dans [UIT-T X.1524].

7.3 Examen du code source

L'examen du code source est une méthode utilisée couramment par les développeurs de logiciels pour trouver les failles ou les points faibles, qui est également appelée méthode de test par boîte blanche. Il peut être effectué manuellement ou à l'aide d'outils automatisés. Etant donné que les programmes

logiciels sont souvent composés de millions de lignes de code, un examen uniquement manuel est généralement impossible. Les outils automatisés sont des ressources précieuses qui facilitent cette opération, mais permettent uniquement d'identifier des segments de code potentiellement vulnérables ou suspects. Il faut parfois faire appel à l'analyse humaine pour déterminer si les problèmes repérés sont réels, cet outil pouvant également donner de faux résultats positifs. La réticence des fournisseurs ou des fabricants à partager les codes sources constitue la principale limite de cette méthode.

Les outils, répertoires et services utilisés pour l'examen du code source doivent être compatibles avec l'énumération CWE conformément aux exigences et fonctionnalités spécifiées dans [UIT-T X.1524].

7.4 Analyse binaire

L'évaluation de la sécurité moyennant l'utilisation d'instructions en langage machine au lieu du code source est généralement appelée analyse binaire. L'analyse binaire crée un modèle de comportement en analysant le flux de commande et de données d'une application grâce à un code machine exécutable – comme le voit l'auteur d'une attaque. Contrairement aux outils utilisant le code source, cette méthode détecte de manière fiable les problèmes dans l'application principale et couvre également les vulnérabilités se trouvant dans les bibliothèques tierces, dans les éléments prêts à l'emploi et dans le code inséré par un compilateur ou utilisé par un interprète propre à la plate-forme.

Le développement de logiciels est un processus à plusieurs niveaux, dans le cadre duquel de plus en plus de menaces différentes – par exemple celles découlant de codes malveillants ou de l'existence de portes dérobées – sont impossibles à repérer avec des outils d'examen du code source, car elles ne sont pas visibles dans le code source. Il est possible de détecter ces menaces en utilisant l'analyse binaire statique sur l'application dans sa version finale.

Les outils, répertoires et services utilisés pour l'analyse binaire doivent être compatibles avec l'énumération CWE conformément aux exigences et fonctionnalités spécifiées dans [UIT-T X.1524].

7.5 Test d'intrusion

Un test d'intrusion est une tentative à but préventif autorisée visant à évaluer la sécurité d'une infrastructure en essayant de manière sécurisée d'exploiter les vulnérabilités des systèmes, y compris du système d'exploitation (OS), les failles des protocoles et des applications, les erreurs de configuration et les comportements imprudents des utilisateurs finals. Son objectif est avant tout d'évaluer dans quelle mesure il est possible de compromettre les systèmes ou l'utilisateur final, et d'évaluer toutes les conséquences que ces incidents pourraient avoir sur les ressources ou les opérations concernées. Pour effectuer ce type de test, on utilise généralement des technologies manuelles ou automatisées afin de compromettre de manière systématique les serveurs, les extrémités, les applications web, les réseaux hertziens, les dispositifs de réseau, les dispositifs mobiles et d'autres points d'exposition potentiels. Un test d'intrusion peut viser une boîte blanche (qui donne des informations sur le contexte ou sur le système) ou une boîte noire (qui ne donne que des informations sans importance voire aucune information).

En effectuant un test d'intrusion, les vulnérabilités les plus graves, les vulnérabilités les moins importantes ou les fausses vulnérabilités peuvent être identifiées en amont, ce qui permet à une organisation de définir de manière plus judicieuse les mesures à prendre en priorité pour y remédier et d'appliquer les correctifs de sécurité nécessaires.

Les outils, répertoires et services utilisés pour les tests d'intrusion doivent être compatibles avec l'énumération et la classification des schémas d'attaque courants (CAPEC) conformément aux exigences et fonctionnalités spécifiées dans [UIT-T X.1544].

Appendice I

Organigramme

(Cet Appendice ne fait pas partie intégrante de la présente Recommandation.)

L'organisation des techniques d'évaluation de la sécurité en organigramme est une façon judicieuse de commencer l'évaluation de la sécurité. Pour élaborer cet organigramme, on peut envisager un modèle selon lequel l'évaluation commence par la partie la plus élémentaire du réseau et s'étend vers les systèmes intégrés déployés dans le réseau. La sécurité est en premier lieu assuré pour le code source des éléments logiciels, puis dans les applications et les bibliothèques du système, puis dans les systèmes du réseau et, enfin, dans l'ensemble du réseau déployé.

Par conséquent, l'évaluation de la sécurité dans sa totalité peut être organisée en deux grandes étapes:

i) La première étape est celle précédant le déploiement, lors de laquelle la cible peut faire l'objet d'une vérification approfondie faisant appel à toutes les techniques d'évaluation de la sécurité examinées et les conclusions de cette évaluation devraient servir à atténuer les vulnérabilités repérées.

ii) La seconde étape est celle postérieure au déploiement, lors de laquelle la cible est déjà opérationnelle dans le réseau. A cette étape, il ne sera peut-être pas possible de soumettre la cible à toutes les techniques d'évaluation. Par conséquent, les responsables des analyses de sécurité pourront effectuer des recherches périodiques de vulnérabilités, afin de faire en sorte qu'il soit remédié à intervalles réguliers aux vulnérabilités identifiées après le déploiement du produit moyennant l'installation de correctifs, etc.

Lors de l'étape précédant le déploiement, une première mesure pourrait consister à analyser les codes sources des éléments logiciels pour pouvoir corriger les failles détectées. Par la suite, les applications et bibliothèques utilisées par ces applications font l'objet d'une analyse binaire. A l'issue de cette analyse binaire, on effectue des tests à données aléatoires puis, en dernier lieu, une recherche des vulnérabilités et des tests d'intrusion pour les systèmes. Les conclusions et les observations découlant de cette évaluation globale devraient être transmises aux développeurs concernés pour qu'ils puissent prendre des mesures de correction afin d'atténuer toutes les vulnérabilités détectées.

Lors de l'étape postérieure au déploiement, le réseau tout entier pourra faire l'objet de recherches périodiques de vulnérabilités. Dès lors qu'une vulnérabilité quelle qu'elle soit est détectée, elle doit être corrigée.

La Figure I.1 est un organigramme illustrant le déroulement de l'évaluation.

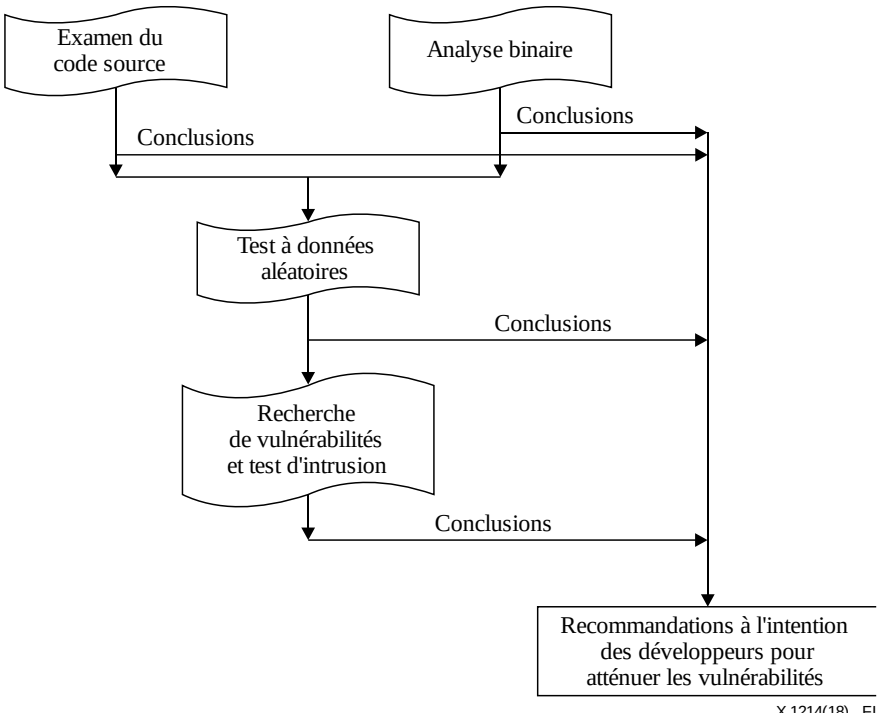

Figure I.1 – Organigramme des techniques d'évaluation de la sécurité

Appendice II

Autres techniques complémentaires pour renforcer la sécurité d'un réseau TIC

(Cet Appendice ne fait pas partie intégrante de la présente Recommandation.)

Le présent Appendice présente des techniques permettant de renforcer encore la sécurité d'un réseau de télécommunication/TIC.

II.1 Evaluation de la solidité du mot de passe

L'authentification par mot de passe est couramment utilisée dans les réseaux de télécommunication/TIC à différentes fins, par exemple, pour la configuration, la gestion, l'exploitation et la maintenance, et la fourniture de services. Les administrateurs des systèmes devraient évaluer la solidité de ces mots de passe, afin de veiller à ce qu'ils ne puissent pas être piratés facilement. Pour ce faire, il est possible d'utiliser le cassage de mots de passe. Il existe différents mécanismes pour casser les mots de passe, comme l'attaque par dictionnaire, l'attaque en force brute et les "rainbow tables".

II.2 Evaluation de la confidentialité sociale

Dans certains cas, il est possible d'exercer une manipulation psychologique sur des employés d'une organisation pour les amener à divulguer des informations confidentielles. Il s'agit d'un type d'abus de confiance visant à obtenir des informations, à frauder ou à accéder à un système. On pourra faire appel à l'ingénierie sociale pour évaluer la crédibilité de ces personnes ou groupes dans une organisation. Des cibles particulières seront peut-être identifiées lorsque l'organisation a connaissance d'une menace ou pense que la divulgation d'informations par une personne ou un groupe donné de personnes pourrait avoir des incidences considérables.

II.3 Evaluation de la sécurité fonctionnelle

Même s'il se peut qu'aucun outil particulier ne soit utilisé pour tester la sécurité fonctionnelle, cette méthode complète les techniques de détection des vulnérabilités présentées aux § II.1 et II.2.

Les exigences de sécurité fonctionnelle pour un dispositif ou un élément de réseau quelconque utilisé dans des réseaux de télécommunication/TIC sont les suivantes:

i) authentification locale d'un utilisateur pour la configuration et la gestion d'un dispositif;

ii) authentification à distance d'un utilisateur pour la configuration et la gestion d'un dispositif;

iii) stockage sécurisé du mot de passe dans un dispositif;

iv) vérification sécurisée de la gestion de la clé cryptographique;

v) mécanisme de protection du dispositif contre l'installation illégale de correctifs logiciels;

vi) protection du trafic de gestion à distance d'un dispositif;

vii) classification des utilisateurs des dispositifs ayant des droits de gestion en fonction des privilèges ou des permissions;

viii) synchronisation temporelle sécurisée;

ix) création d'événements d'audit (journaux) par le dispositif testé (DUT);

x) exportation sécurisée des journaux d'audit par le dispositif DUT.

II.4 Balayage des dispositifs hertziens

Le balayage des dispositifs hertziens peut aider les organisations à prendre des mesures correctives afin d'atténuer les risques que représentent les technologies hertziennes en matière de sécurité. Un

outil de balayage hertzien devrait être capable d'inspecter tous les dispositifs hertziens IEEE 802.11 [b-IEEE Std. 8802-11], au niveau national ou international. Le balayage hertzien peut permettre d'identifier des dispositifs hertziens non autorisés situés dans le rayon d'action des scanners, de découvrir des signaux hertziens à l'extérieur du périmètre d'une organisation et de détecter d'éventuelles portes dérobées et atteintes à la sécurité.

II.5 Utilisation de mises en oeuvre de modules et d'algorithmes cryptographiques sécurisés

Des algorithmes cryptographiques sont utilisés pour le chiffrement et le déchiffrement des données d'authentification ou des données d'utilisateur pour le transfert sécurisé des données dans des réseaux de télécommunication/TIC. Bien que les algorithmes cryptographiques soient correctement conçus, les erreurs de mise en oeuvre sont courantes. Si des algorithmes non sécurisés ayant des failles dans leur mise en oeuvre sont déployés dans des réseaux de télécommunication/TIC, ils peuvent être exploités par l'auteur d'une attaque, ce qui pourrait entraîner d'importantes pertes de données et des intrusions frauduleuses. Par conséquent, des modules et algorithmes cryptographiques hautement sécurisés pourront être utilisés dans les réseaux de télécommunication/TIC.

II.6 Reniflage de réseau

Le reniflage de réseau est une technique passive qui surveille les communications dans le réseau, décode les protocoles et examine les en-têtes afin de signaler les informations présentant un intérêt. Cette technique, également appelée surveillance ou analyse du réseau, peut être utilisée de manière légitime par un administrateur de réseau ou de système pour surveiller et rétablir le trafic dans le réseau.

Grâce aux informations rassemblées par le renifleur de réseau, un administrateur ou un spécialiste de la sécurité peut identifier des paquets erronés et utiliser les données pour repérer les goulets d'étranglement et aider à maintenir la transmission sécurisée et efficace des données dans le réseau.

Bibliographie

[b-IEEE Std. 8802-11] ISO/IEC/IEEE 8802-11:2018(E) – *ISO/IEC/IEEE – Norme internationale – Technologies de l'information – Télécommunications et échange d'information entre systèmes – Réseaux locaux et métropolitains – Exigences spécifiques – Partie 11: Spécifications du contrôle d'accès du milieu sans fil (MAC) et de la couche physique (PHY)*

[b-CVE] CVE Numbering Authorities (1999-2018*). Common vulnerabilities and exposures list.* Mitre Corporation. https://cve.mitre.org/cve/

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	Equipements 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, 2019