Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

X.1157

(09/2015)

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

Applications et services sécurisés – Protocoles de sécurité

Capacités techniques de détection des fraudes et de réponse pour les services exigeant un niveau de garantie élevé

Recommandation UIT-T X.1157

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	
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	**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 pollupostage	X.1230–X.1249
Gestion des identités	X.1250–X.1279
APPLICATIONS ET SERVICES SÉCURISÉS	
Communications d'urgence	X.1300–X.1309
Sécurité des réseaux de capteurs ubiquitaires	X.1310–X.1339
Recommandations relatives aux infrastructures de clé publique	X.1340–X.1349
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.1157

Capacités techniques de détection des fraudes et de réponse pour les services exigeant un niveau de garantie élevé

Résumé

La Recommandation UIT-T X.1157 définit les capacités nécessaires pour assurer une détection des fraudes et une réponse pour les applications des technologies de l'information et de la communication (TIC) sensibles sur le plan de la sécurité. Le service de détection des fraudes et de réponse assure la détection, l'analyse et la gestion des fraudes parmi les utilisateurs, les comptes, les produits, les processus et les canaux. Il surveille et analyse les activités et les comportements des utilisateurs au niveau des applications (et non au niveau des systèmes, des bases de données ou des réseaux) et observe ce qui se passe à l'intérieur des comptes et parmi les comptes, via tout canal dont disposent les utilisateurs. Il analyse aussi les comportements entre des utilisateurs, des comptes ou d'autres entités en lien les uns avec les autres, à la recherche d'activités anormales, de corruptions ou d'utilisations abusives. Il est très couramment utilisé dans des secteurs d'activité gérant l'argent de clients, comme les services financiers, l'accès à distance aux entreprises, etc., mais est également couramment utilisé pour détecter des fraudes internes et d'autres types d'activités non autorisées.

Historique

Edition	Recommandation	Approbation	Commission d'études	ID unique*
1.0	ITU-T X.1157	2015-09-17	17	11.1002/1000/12353

Mots clés

Système de détection des fraudes, gestion des fraudes.

* 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

Recommandation UIT-T X.1157

Capacités techniques de détection des fraudes et de réponse pour les services exigeant un niveau de garantie élevé

1 Domaine d'application

La présente Recommandation fournit des lignes directrices sur les capacités techniques à utiliser pour la gestion des fraudes dans les services exigeant un niveau de garantie élevé. Elle a pour objectif de définir un système capable de détecter les activités frauduleuses. De nombreuses entités commerciales et entreprises utilisant des applications des technologies de l'information et de la communication (TIC) sensibles sur le plan de la sécurité pourront appliquer la présente Recommandation pour déployer un système de détection des fraudes et de réponse. La présente Recommandation est également applicable à la gestion des fraudes à l'intérieur d'une organisation ainsi que des fraudes externes via un accès distant ou un service commercial. La présente Recommandation porte sur:

– les capacités du service de détection des fraudes et de réponse;

– les opérations et les composants du système de détection des fraudes et de réponse; et

– des considérations relatives au service de défense et de réponse en cas d'incident.

2 Références

Aucune.

3 Définitions

3.1 Termes définis ailleurs

La présente Recommandation utilise les termes suivants définis ailleurs:

3.1.1 niveau de garantie [b-UIT-T X.1252]: niveau de confiance dans le lien entre une entité et l'information d'identité présentée.

3.1.2 authentification (d'entité) [b-UIT-T X.1252]: processus utilisé pour obtenir une confiance suffisante dans le lien entre l'entité et l'identité présentée.

NOTE – Dans un contexte de gestion d'identité (IdM), le terme authentification désigne l'authentification d'entité.

3.1.3 garantie d'authentification [b-UIT-T X.1252]: degré de confiance obtenu au cours du processus d'authentification, dans le fait que le partenaire de communication est bien l'entité qu'il déclare être ou qu'il est censé être.

NOTE – La confiance repose sur le degré de confiance dans le lien entre l'entité communicante et l'identité présentée.

3.1.4 utilisateur final [b-UIT-T X.1141]: une personne physique qui emploie des ressources pour les besoins d'une application.

3.1.5 identité [b-UIT-T X.1252]: représentation d'une entité sous la forme d'un ou de plusieurs attributs qui sont suffisants pour pouvoir distinguer les entités dans un contexte. Aux fins de la gestion des identités (IdM), le terme identité désigne l'identité contextuelle (sous-ensemble d'attributs), c'est-à-dire que la diversité des attributs est limitée par un cadre avec des frontières définies (le contexte) dans lequel l'entité existe et interagit.

NOTE − Chaque entité est représentée par une identité holistique, qui comprend tous les éléments d'information possibles caractérisant cette entité (les attributs). Toutefois, l'identité holistique est théorique et échappe à toute description et utilisation pratique, car le nombre de tous les attributs possibles est indéfini.

3.1.6 garantie d'identité [b-UIT-T X.1252]: degré de confiance dans le processus de validation et de vérification d'identité utilisé pour établir l'identité de l'entité à laquelle le justificatif a été délivré, et degré de confiance dans le fait que l'entité qui utilise le justificatif est cette entité ou l'entité à laquelle le justificatif a été délivré ou attribué.

3.1.7 contrôle d'identité [b-UIT-T X.1252]: processus permettant de valider et de vérifier suffisamment d'informations pour confirmer l'identité déclarée de l'entité.

3.1.8 vérification d'identité [b-UIT-T X.1252]: processus consistant à confirmer qu'une identité déclarée est correcte sur la base de la comparaison des déclarations d'identité offertes avec les informations précédemment avérées.

3.1.9 fournisseur de services [b-UIT-T X.1141]: rôle joué par une entité du système, consistant à fournir des services aux entités principales ou à d'autres entités du système.

3.2 Termes définis dans la présente Recommandation

La présente Recommandation utilise les termes suivants:

3.2.1 système de détection des fraudes: logiciel en tant qu'application qui assure la surveillance, la détection et la gestion des fraudes ou d'autres utilisations abusives parmi les utilisateurs (par exemple les clients), les comptes, les canaux, les produits et d'autres entités (par exemple les kiosques).

NOTE – Pour déployer le système de détection des fraudes, les applications des entreprises pourraient intégrer un moteur de détection des fraudes pour une transaction évalue le risque de fraude pour une transaction liée aussi bien à la navigation des utilisateurs et à l'accès aux applications qu'à tout type d'activité, par exemple une modification d'adresse, un paiement ou l'accès à des informations sensibles.

3.2.2 gestion des fraudes: ensemble complet d'activités, reposant sur des systèmes d'alerte avancée, des signes et des schémas pour les différents types de fraude, des profils des utilisateurs et de leurs activités, une réponse aux incidents, etc., afin d'atténuer le risque en matière de sécurité au moyen d'un système de détection des fraudes.

NOTE – Un certain nombre de problèmes rendent nécessaire la mise au point de systèmes de gestion des fraudes: le volume considérable des données, la nécessité d'une détection rapide et précise des fraudes sans gêner les activités opérationnelles, l'apparition en permanence de nouvelles fraudes pour échapper au contrôle des techniques existantes, le risque de fausses alarmes, etc.

3.2.3 application des technologies de l'information et de la communication (TIC) sensible sur le plan de la sécurité: application qui exige un niveau de garantie de sécurité très élevé en termes de protection des informations personnelles ou des informations confidentielles d'une organisation et/ou d'une entreprise.

NOTE – Lorsque des applications TIC sensibles sur le plan de la sécurité sont compromises et contrôlées par un attaquant, l'exposition d'informations sensibles, à savoir d'informations personnelles ou financières, est extrêmement préjudiciable pour les utilisateurs, les organisations, l'infrastructure des télécommunications et les services, qui peuvent comprendre des services financiers en ligne, des services médicaux en ligne et des services d'accès à distance aux entreprises.

4 Abréviations et acronymes

La présente Recommandation utilise les abréviations et acronymes suivants:

API interface de programmation d'application (*application programming interface*)

ATM distributeur automatique (*automated teller machine*)

DLP prévention de la perte de données (*data loss prevention*)

DNS système de noms de domaine (*domain name system*)

DSL ligne d'abonné numérique (*digital subscriber line*)

GSM système mondial de communications mobiles (*global system for mobile communications*)

HTTP protocole de transfert hypertexte (*hypertext transfer protocol*)

ID identité, identification

IP protocole Internet (*internet protocol*)

IPS système de prévention des intrusions (*intrusion prevention system*)

ISP fournisseur d'accès Internet, fournisseur de services Internet (*internet service provider*)

IT technologies de l'information, informatique (*information technology*)

MITM "homme du milieu", intercepteur (*man-in-the-middle*)

NAC contrôle d'accès au réseau (*network access control*)

OS système d'exploitation (*operating system*)

PC ordinateur personnel (*personal computer*)

PIN numéro d'identification personnel (*personal identity number*)

SMS service de messages courts (*short message service*)

SP fournisseur de services (*service provider*)

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

SSL couche de connecteurs sécurisés (*secure socket layer*)

TAN numéro d'authentification de transaction (*transaction authentication number*)

TIC technologies de l'information et de la communication

WiMAX interopérabilité mondiale pour l'accès hyperfréquence (*worldwide interoperability for microwave access*)

5 Conventions

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

L'expression "il est recommandé" indique une disposition qui est recommandée mais qui n'est pas absolument nécessaire. Cette disposition n'est donc pas indispensable pour déclarer la conformité.

L'expression "il est interdit" indique une disposition qui doit être strictement suivie et par rapport à laquelle aucun écart n'est permis pour pouvoir déclarer la conformité à la présente Recommandation.

L'expression "peut, à titre d'option" indique une disposition optionnelle qui est admissible, sans pour autant être en quoi que ce soit recommandée. Elle ne doit pas être interprétée comme l'obligation pour le fabricant de mettre en oeuvre l'option et la possibilité pour l'opérateur de réseau ou le fournisseur de service de l'activer ou non, mais comme la possibilité pour le fabricant de fournir ou non cette option, sans que cela n'ait d'incidence sur la déclaration de conformité à la présente Recommandation.

6 Aspects généraux relatifs à la détection des fraudes et à la réponse

6.1 Problématique

Des attaques par logiciels malveillants ont ciblé des services applicatifs basés sur les télécommunications dans de nombreux types d'entreprises et de secteurs d'activité (par exemple les services en ligne dans les secteurs du transport, des hôpitaux, etc.). Ces attaques deviennent une préoccupation majeure et sont de plus en plus perpétrées au moyen de courriels de harponnage ciblés et d'objets infectés de logiciels malveillants, par exemple des publicités, sur lesquels cliquent les utilisateurs inexpérimentés. Ces méthodes ont été utilisées pour infecter les systèmes informatiques de nombreuses organisations.

De nombreuses entités commerciales et entreprises sont exposées à des risques importants de perte de données, d'accès inapproprié aux comptes et de transactions inappropriées, provenant de sources externes ou internes. Il arrive souvent que des logiciels malveillants ciblés contournent les systèmes de protection existants, et que les atteintes à la confidentialité des données résultantes ne soient détectées qu'après une longue période et la survenue d'une importante exfiltration de données. La preuve d'une activité malveillante est souvent cachée au vu et au su de tous, et n'est pas détectée faute de capacité de surveillance ou en raison de l'incapacité de faire la distinction entre un cas anormal d'utilisation d'une application ou d'un accès à des données et une activité normale. Par exemple, il se peut qu'un client d'une banque ne s'aperçoive qu'une fraude a été commise que lorsqu'il constatera l'absence de confirmation d'un compte dans son rapport de crédit, ou lorsqu'un agent de recouvrement lui réclamera un paiement.

Les attaques par logiciels malveillants perpétrées contre des clients financiers et des employés d'entreprises entraînent pour les victimes de graves atteintes à la réputation ou de graves préjudices financiers. Elles sont de plus en plus couramment utilisées à l'encontre de comptes de particuliers ou d'entreprises, afin de dérober des informations sensibles ou des fonds. Par conséquent, si les processus opérationnels et les organisations ne sont pas structurés correctement pour gérer efficacement la détection des fraudes, des alarmes ou des alertes importantes pourraient être ignorées. Enfin, les attaques par logiciels malveillants peuvent être utilisées pour prendre le contrôle de comptes d'utilisateurs, ou pour commettre une fraude ou dérober des ressources basées sur un serveur.

6.2 Rôle de la gestion des fraudes

Un système de gestion des fraudes pourra s'appliquer dans trois grands cas de fraude:

- Détection de la prise de contrôle d'un compte, qui a lieu en général lorsque les identifiants d'un compte d'utilisateur sont dérobés, ou au moyen de logiciels malveillants. Les logiciels malveillants infectent le système informatique d'une entreprise non seulement au moyen de documents infectés joints à un courriel mais aussi simplement lors de la visite d'un site web infecté.
- Détection de l'ouverture frauduleuse d'un compte, qui a lieu en général lorsque les identifiants d'un compte d'utilisateur sont dérobés, ou au moyen de logiciels malveillants.
- Détection de l'utilisation d'un compte dérobé (ou d'un autre utilisateur), par exemple, une carte de crédit dérobée, lorsqu'un utilisateur fait un achat, ou prétend être l'utilisateur normal.

Un système de gestion des fraudes est très couramment utilisé pour un ou plusieurs cas de fraude, par exemple la prise de contrôle d'un compte, la détection d'une fraude interne, la détection d'une fraude à la carte de paiement en temps réel et le blocage d'une transaction, ainsi qu'en tant que système spécifique de gestion des fraudes ou des utilisations abusives pour l'entreprise. Dans chacun de ces scénarios, il est essentiel pour l'entreprise qui assure une transaction de vérifier la légitimité de la personne à l'origine de la transaction.

6.3 Principales capacités pour la gestion des fraudes

Pour faire face à toute fraude d'identité, un système de détection des fraudes doit prendre en charge trois capacités: surveillance, détection et réponse. Ces capacités visent à rechercher toute activité suspecte dans diverses données d'événement, à détecter les fraudes le plus tôt possible après leur survenue et à mettre fin aux fraudes en cas de détection d'activités suspectes.

Surveillance: Un système de détection des fraudes surveille les fraudes en recherchant les activités et comportements anormaux des utilisateurs au niveau des applications, ainsi qu'au niveau des systèmes, des bases de données ou des réseaux, et observe ce qui se passe à l'intérieur des comptes et parmi les comptes, via tout canal dont disposent les utilisateurs. En outre, il surveille et analyse les comportements des comptes ou des utilisateurs et les transactions associées, et identifie les comportements anormaux, au moyen de règles ou de modèles statistiques. Il peut aussi (dans l'idéal) utiliser des profils d'utilisateur et de compte mis à jour en permanence, ainsi que des groupes d'homologues pour comparer les transactions et identifier celles qui sont suspectes. En particulier, pour une surveillance systématique des fraudes internes, il faut surveiller les utilisateurs des systèmes informatiques disposant de privilèges leur permettant de modifier directement les fichiers et les données, sans passer par des applications d'utilisateur clé en main.

Détection: Un système de détection des fraudes peut explorer, éplucher et analyser de grands volumes de données en utilisant un filtrage complexe basé sur des relations et des règles, défini par l'entreprise, pour prévenir les fraudes. Il peut être utilisé pour détecter les fraudes internes (à savoir commises par un employé) et les fraudes externes (à savoir commises par un client ou un partenaire commercial). Pour la prise en charge de la capacité de détection des fraudes, il peut et doit disposer de profils pour diverses entités – utilisateurs, comptes, foyers, ordinateurs personnels, téléphones portables, kiosques, etc. – pour pouvoir repérer tout comportement anormal de la part de cette entité pour une transaction donnée. La détection des fraudes utilise des politiques basées sur des règles reposant sur le jugement humain et le savoir et/ou sur des modèles mathématiques prédictifs pour évaluer la probabilité de fraude pour une transaction donnée.

Réponse: Après la détection d'une activité suspecte, un système de gestion des fraudes devrait appliquer diverses mesures de précaution comme un blocage de compte ou un partage d'informations. Diverses techniques complémentaires de surveillance et de détection peuvent aider les entreprises à mieux détecter les activités suspectes des utilisateurs, reconnaître les cas d'accès inapproprié aux ressources ou d'activité frauduleuse sur un compte, et enquêter sur les incidents et répondre par des alertes en temps réel, une gestion des incidents, un blocage de compte ou une intervention au niveau de la transaction. Par conséquent, les organisations doivent déterminer quel est l'ensemble de techniques de surveillance et d'analyse le plus adapté au niveau de risque auquel elles sont exposées, et déterminer aussi quelles sont les techniques de sécurité qu'elles mettront en oeuvre et prendront en charge.

7 Architecture du système de détection des fraudes et de réponse

7.1 Fonctionnement et composants

Les applications TIC peuvent intégrer des composants de détection des fraudes afin de pouvoir gérer le risque de fraude pour une transaction liée aussi bien à un accès utilisateur qu'à tout type d'activité. Le fonctionnement du système de détection des fraudes ne devrait être transparent ni pour les pirates ni pour les utilisateurs, d'une part afin que les pirates ne puissent pas apprendre les règles du système et d'autre part afin d'éviter tout désagrément pour les utilisateurs légitimes. Les transactions suspectes des utilisateurs sont revérifiées par le système de détection des fraudes en temps réel pour déterminer si elles sont légitimes, ou sont suspendues en attendant que le système de détection des fraudes dispose de suffisamment de temps pour déterminer si elles sont légitimes.

Le système de détection des fraudes comprend plusieurs composants qui traitent, stockent et transfèrent des données dans le but de détecter les activités anormales. Le fonctionnement de ce système fait intervenir le traitement de données entre les composants. Les opérations et les composants du système de détection des fraudes sont décrits en détail dans la Figure 1. Idéalement, le système de détection des fraudes commence à surveiller l'intégralité de la session après la connexion initiale et, pour ce faire, il exécute les opérations suivantes pour la gestion des fraudes (de la capacité de surveillance à la capacité de réponse).

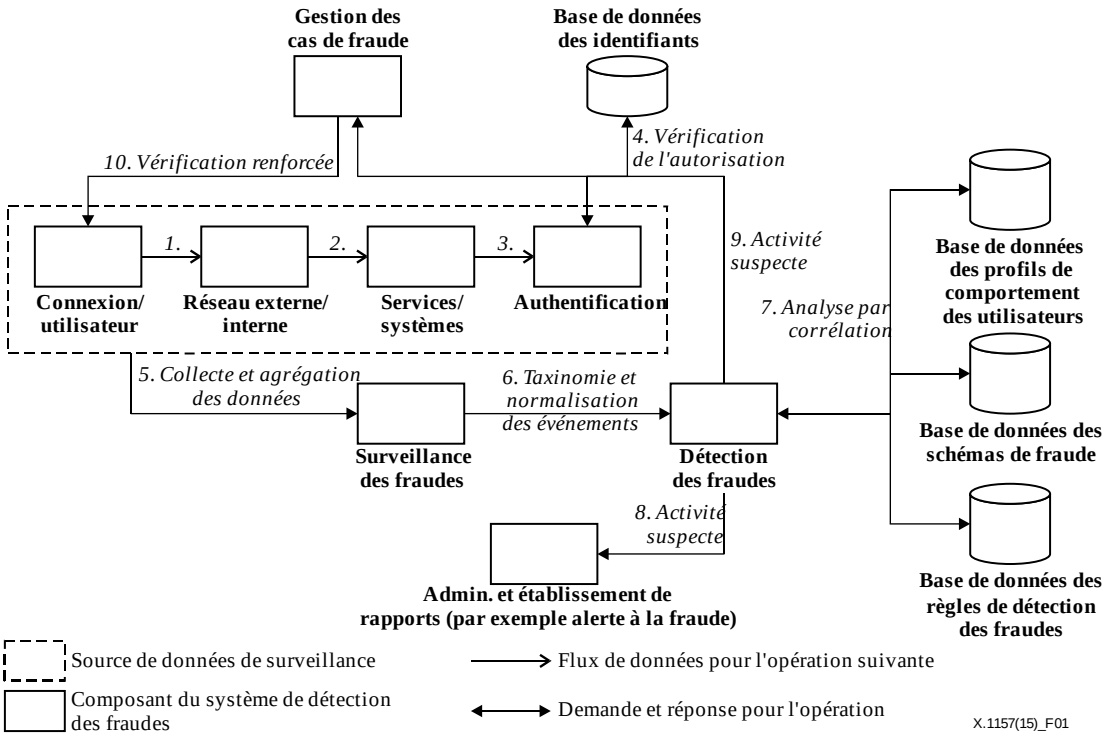

Figure 1 – Opérations et composants d'un système de détection des fraudes

Opérations de connexion, d'authentification et de vérification de l'autorisation (flux de données 1, 2, 3 et 4)

Dans les conditions normales, la connexion initiale est analysée et une note de risque lui est attribuée après comparaison des identifiants collectés pendant la connexion avec les données figurant dans la base de données des identifiants des utilisateurs (nom d'utilisateur et mot de passe), le protocole IP, la base de données des profils de comportement des utilisateurs, etc. La vérification de l'autorisation est basée sur les règles d'authentification définies dans la base de données des identifiants, qui est en principe configurable par l'établissement et est extensible (de nouvelles règles peuvent être ajoutées).

Opération de surveillance et de détection des fraudes et de gestion des cas de fraude (flux de données 5, 6, 7, 9 et 10)

Le système de détection des fraudes collecte des données émanant de diverses sources (réseaux, services/systèmes, et fonction d'authentification) après la connexion de l'utilisateur. Il analyse les données collectées par le composant de surveillance des fraudes. Par exemple, si la fonction d'authentification identifie une activité douteuse, le système de détection des fraudes envoie les informations relatives à la fraude présumée au composant de détection des fraudes, lequel interroge alors les bases de données se rapportant aux fraudes (données relatives aux profils de comportement des utilisateurs, données relatives aux schémas de fraude, et données relatives aux règles de détection des fraudes) en vue d'une analyse par corrélation. Les cas de fraude sont priorisés en

fonction du niveau de risque déterminé par le composant de détection des fraudes et donnent une image complète du risque associé aux interactions présentant une note de risque élevée. Dans le cas d'une fraude présentant un niveau de risque élevé, le composant de gestion des cas de fraude demande une vérification renforcée de la connexion de l'utilisateur. Les résultats de la résolution des cas de fraude peuvent et doivent être communiqués aux bases de données, créant ainsi une boucle d'auto-apprentissage pour améliorer la performance future.

Opération d'administration et d'établissement de rapports (flux de données 8)

Le composant d'administration et d'établissement de rapports devrait aussi être présent afin de permettre à l'établissement de mieux comprendre et contrôler le système de détection des fraudes. Ce composant permet aux utilisateurs du système d'analyser facilement la performance du système et de faire rapport sur cette performance, d'identifier les incohérences concernant les notes ou l'accès et de déterminer les améliorations possibles, et de suivre les opérations des utilisateurs du système. En outre, les outils d'établissement de rapports permettent de présenter facilement des informations détaillées sur la performance à la haute direction et aux analystes des fraudes.

7.2 Considérations relatives à l'architecture

Lors de la mise en oeuvre du système de détection des fraudes pour les applications TIC, l'une des trois architectures suivantes devrait être envisagée: module de détection des fraudes intégré dans le serveur d'applications (par exemple le web), écoute et/ou surveillance de l'application en ligne, et interfaces de programmation dans l'application existante. Les règles et processus de l'entreprise sont des facteurs importants pour la performance d'une application.

Un module de détection des fraudes placé à l'intérieur du serveur d'applications

Les règles établies par l'entreprise sont appliquées par le filtre à toute demande HTTP (protocole de transfert hypertexte) (par exemple, connexion ou paiement) avant que la transaction ne parvienne à l'application. Les transactions peuvent être stoppées et/ou redirigées vers une routine de vérification des transactions en temps réel dans le cadre de l'exécution des règles de détection des fraudes du module. Plusieurs fournisseurs proposent des modules d'extension pour les serveurs d'applications qui intègrent directement un préprocesseur.

Ecoute et/ou surveillance de l'application TIC (mode écoute)

Dans ce mode, l'application écoute ou "renifle" les fichiers d'entrée ou le trafic de réseau HTTP (par exemple, connexion), ou lit les données à l'aide de modules d'extension des serveurs d'applications installés sur chaque serveur. Les données sont lues en temps réel (approche "renifleur" – réseau) ou presqu'en temps réel (approche écouteur – serveur d'applications) et soit sont transmises à une autre application de gestion des fraudes soit sont mises dans un format permettant d'appliquer les règles de détection des fraudes. Dans ce dernier cas, les transactions suspectes sont mises en file d'attente en attendant un suivi par les analystes des fraudes. Des interfaces de programmation d'application (API) personnalisées peuvent être intégrées afin de rediriger les transactions vers une vérification de type question/réponse.

Interfaces de programmation dans l'application existante (mode intégration en ligne)

Dans ce cas, des interfaces API sont utilisées pour faire passer toutes les transactions par le système de détection des fraudes avant leur traitement. Le flux de transactions est contrôlé, et un utilisateur peut être questionné en temps réel si une transaction suspecte est détectée. Toute modification des règles de l'entreprise nécessite de modifier l'application centrale. Les interfaces API sont principalement basées sur des services web. De plus, avec les interfaces API, il est plus difficile de remplacer une solution propre à un fournisseur par une autre.

D'une manière générale, l'utilisation d'interfaces API pour la détection des fraudes permet aux entreprises/organisations de contrôler directement le flux de transactions, mais des efforts

considérables d'intégration sont nécessaires, et une mise à jour systématique est obligatoire lors de toute modification de l'application centrale. Pour les serveurs d'applications qui ne nécessitent pas d'intervention en temps réel concernant les transactions des utilisateurs, on préférera la deuxième approche, qui est la plus simple à retirer et remplacer.

8 Capacités techniques de détection des fraudes et de réponse

8.1 Capacités de surveillance

La capacité de surveillance établit le contexte pour les utilisateurs et les données qui est nécessaire à une détection précoce des attaques et des atteintes à la sécurité, et permet d'accéder aux données et de surveiller les activités. La surveillance de l'accès par les utilisateurs disposant de privilèges et de l'accès aux données sensibles constitue également une exigence courante pour l'établissement des rapports de conformité.

Le système de détection des fraudes doit mettre en oeuvre une capacité de gestion des informations et des événements de sécurité pour assurer une large surveillance des activités des utilisateurs et de l'accès aux ressources à travers le réseau, les systèmes, les bases de données et les applications. Le système de détection des fraudes doit aussi compléter les données relatives aux événements avec des données de contexte concernant les utilisateurs, les actifs, les menaces et les vulnérabilités afin d'améliorer l'efficacité de la surveillance de la sécurité aux fins de détection des atteintes à la sécurité. En outre, il doit compléter sélectivement la surveillance générale de la sécurité avec des capacités supplémentaires, par exemple la surveillance des menaces avancées, basée sur le niveau de risque, et la capacité de mettre en oeuvre et d'exploiter efficacement le système de détection des fraudes et de réponse.

Le système de détection des fraudes collecte par ailleurs des données relatives aux événements presqu'en temps réel d'une manière qui permet de les analyser immédiatement. La capacité de surveillance en temps réel est importante pour la gestion des menaces pour pouvoir suivre et analyser la progression d'une attaque à travers les composants et les systèmes, et pour la surveillance des activités des utilisateurs pour pouvoir suivre et analyser les activités d'un utilisateur à travers les applications, ou pour pouvoir suivre et analyser une série de transactions connexes ou événements connexes d'accès à des données. Enfin, la capacité de surveillance en temps réel devrait pouvoir assurer une collecte de données par lots pour les cas où la collecte en temps réel n'est pas pratique ou n'est pas nécessaire.

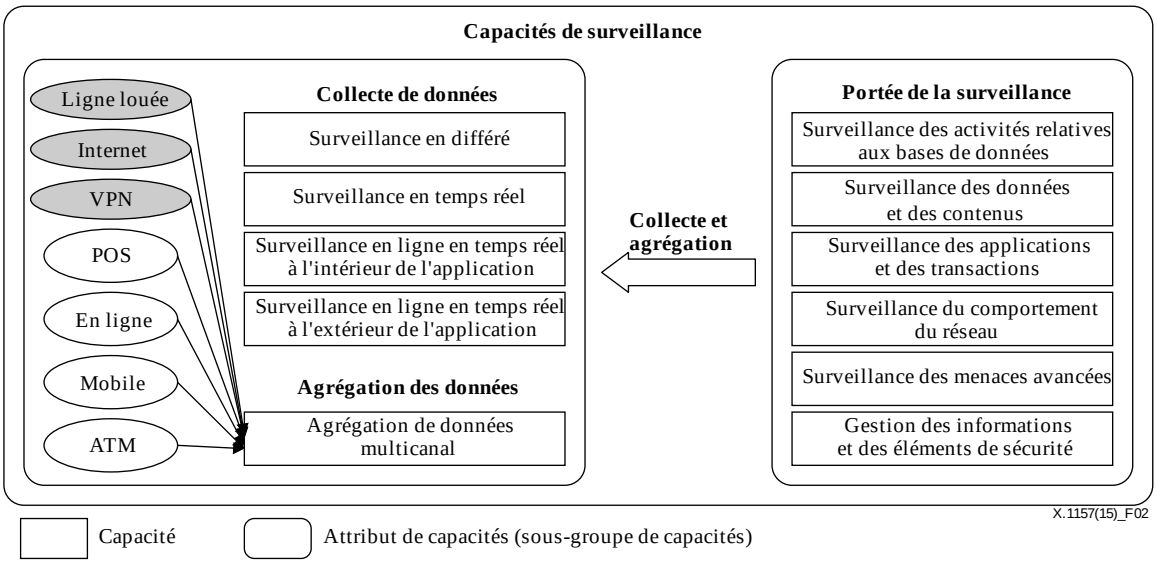

Figure 2 – Capacités de surveillance d'un système de détection des fraudes

8.1.1 Agrégation et collecte de données

L'agrégation et la collecte de données sont assurées pour des sources de données de journaux très diverses: dispositifs de réseau et de sécurité, journaux de serveur, de base de données et d'application, données fournies par des applications liées à la sécurité, par exemple des applications d'évaluation des vulnérabilités et de surveillance des activités relatives aux bases de données, et données fournies par des systèmes de gestion d'identité et d'accès, par exemple les annuaires d'entreprise ou les systèmes de gestion de configuration et d'accès pour les utilisateurs.

Surveillance en différé

La surveillance en différé nécessite un examen manuel ou automatique des fichiers journaux. Elle peut être déployée rapidement en vue d'une analyse post-transaction avec des périodes de résolution relativement longues et permet d'éviter de stopper les transactions au moment de l'exécution. Elle devrait pouvoir assurer une collecte de données par lots pour les cas où la collecte en temps réel n'est pas pratique ou n'est pas nécessaire.

Surveillance en temps réel

La surveillance en temps réel consiste à surveiller toutes les transactions (par exemple HTTP) en temps réel à l'aide d'un filtre de serveur web. Cette fonction peut assurer la surveillance sans matériel supplémentaire en utilisant un filtre de serveur web à faible impact. L'application n'a pas besoin d'être modifiée pour pouvoir observer les données de transaction en temps réel.

Surveillance en ligne en temps réel à l'intérieur de l'application

La surveillance en ligne en temps réel à l'intérieur de l'application consiste à surveiller toutes les transactions web HTTP en temps réel via une intégration à l'intérieur de l'application. Le déploiement et le maintien de cette fonction peuvent demander du temps et de l'argent car des modifications importantes de l'application sont nécessaires pour pouvoir surveiller les points de transaction spécifiques.

Surveillance en ligne en temps réel à l'extérieur de l'application

La surveillance en ligne en temps réel à l'extérieur de l'application consiste à surveiller toutes les transactions web HTTP en temps réel via un filtre à l'extérieur de l'application. Cette fonction n'a aucune incidence sur l'application pour les approches de reniflage et de filtrage web mais le filtre à l'extérieur de l'application est en ligne avec l'application, ce qui peut introduire un risque au niveau de la fiabilité de l'application. L'application n'a pas besoin d'être modifiée pour pouvoir observer les données de transaction en temps réel.

Agrégation de données multicanal

Avec l'agrégation de données multicanal, les données de transaction provenant d'autres canaux peuvent être entièrement incorporées dans les processus de surveillance et de détection des fraudes. De plus, l'agrégation de données multicanal recherche tout comportement suspect concernant les utilisateurs ou les comptes et, dans le même temps, permet d'observer ce qui passe dans les canaux et les produits et de corréler les alertes et les activités pour chaque utilisateur, compte ou entité. L'agrégation de données multicanal permet d'analyser les relations entre les entités internes et/ou externes et leurs attributs (par exemple, utilisateurs, comptes, attributs de compte, machines et attributs de machine) afin de détecter les activités anormales ou les utilisations abusives.

8.1.2 Source de données surveillée

Le système de détection des fraudes détecte les activités malveillantes dans un flux constant d'événements discrets qui sont généralement associés à un utilisateur autorisé et qui proviennent de plusieurs sources: réseaux, systèmes et applications. Les capacités de surveillance reposent sur l'intégration de plusieurs sources pour obtenir les événements suspects et les incidents.

Surveillance des activités relatives aux bases de données

La surveillance des activités relatives aux bases de données aide à maintenir la séparation des tâches pour les utilisateurs disposant d'un accès privilégié aux bases de données en surveillant les activités des administrateurs. Cette capacité permet en outre d'améliorer la sécurité des bases de données en détectant les violations des règles et les activités inhabituelles. L'agrégation et la corrélation des événements relatifs aux bases de données et l'établissement de rapports concernant ces événements permettent de disposer d'une capacité d'audit sur les bases de données sans qu'il soit nécessaire de mettre en oeuvre des fonctions natives d'audit sur ces bases de données.

Cette capacité permet de détecter les modifications concernant la structure et le contenu des bases de données, et l'accès aux données par les utilisateurs disposant de privilèges via des modules d'extension locaux ou distants. Étant donné qu'elle opère au niveau des bases de données et des fichiers, elle ne dispose pas d'informations contextuelles sur l'accès et la navigation qui ne sont pas liées aux bases de données ou aux fichiers associés. On peut utiliser des composants de surveillance de réseau (en ligne ou hors bande) pour surveiller les requêtes SQL (langage de requête structurée) et les accès en tant qu'administrateur depuis le réseau.

Surveillance des données et des contenus

La capacité de surveillance des données et des contenus est souvent utilisée pour limiter les fuites d'informations, par exemple les numéros de carte de crédit, les informations d'identification personnelle, et les informations de propriété intellectuelle contenues dans des documents ou des bases de données, à l'aide de fonctions assurant la surveillance des contenus, le filtrage et la prévention de perte de données (DLP). Cette capacité a pour objet de permettre aux entreprises de surveiller leurs contenus internes afin de détecter les activités suspectes. La surveillance des contenus et le filtrage sont utilisés pour protéger les contenus en déplacement (via une surveillance ou un filtrage dans le réseau), au repos (via un balayage des mémoires) et en cours d'utilisation (via des agents de point d'extrémité). La plupart des fonctions permettent aussi de balayer les contenus stockés sur le réseau afin de repérer les violations des règles (par exemple, un numéro de carte de crédit sur un serveur non approuvé) et de détecter les violations des règles de l'entreprise concernant l'utilisation appropriée des contenus et des données.

Les outils DLP permettent de découvrir, surveiller et bloquer activement le déplacement de données sensibles ou l'accès à des données sensibles à l'aide de techniques d'inspection des contenus et d'analyse contextuelle, avec l'application d'une ou de plusieurs règles au moment de l'utilisation. La DLP est limitée par la capacité de l'organisation considérée à définir les contenus sensibles, leurs structures ou d'autres caractéristiques d'identification.

Ces fonctions sont extrêmement utiles pour ce qui est de limiter les expositions accidentelles ou celles dues à des processus incorrects de l'entreprise, mais il existe de nombreuses pratiques non surveillées auxquelles un attaquant ou un initié peut recourir à des fins malveillantes (par exemple l'utilisation d'un téléphone avec appareil photo, d'une messagerie vocale, d'un papier et d'un stylo) pour contourner les solutions prenant en compte les contenus.

Surveillance des applications et des transactions

La capacité de surveillance des applications et des transactions comprend une surveillance des applications car les failles dans les applications sont fréquemment exploitées dans des attaques ciblées, et il se peut qu'une activité anormale concernant une application soit le seul signal d'une activité frauduleuse ou d'une atteinte à la sécurité. La capacité d'analyser les flux d'activités pour un groupe d'applications permet aux différents composants d'être surveillés au niveau application; en outre, la capacité de définir et d'analyser les flux d'activités pour les applications personnalisées permet aux applications développées en interne d'être surveillées au niveau application.

La capacité de surveillance est également attentive aux activités suspectes des utilisateurs pour une application via un canal d'accès donné (par exemple, sur le web, par téléphone, en personne), ou

pour différentes applications et différents canaux d'accès, ou encore pour différentes organisations en cas de partage entre elles de listes noires d'adresses IP. Elle consiste à détecter aussi bien un accès anormal (par exemple, un accès simultané par un même dispositif depuis deux emplacements géographiques distincts) qu'une séquence de transactions suspecte (par exemple, la modification d'une adresse suivie d'un transfert d'argent d'un montant élevé). Par défaut, elle peut aussi repérer les activités non autorisées des employés si elle est mise en oeuvre dans une application qui est surveillée par l'application de détection des fraudes.

Surveillance du comportement du réseau

La capacité de surveillance du comportement du réseau permet de mettre en évidence les opérations dans le réseau sur la base des flux de trafic entre les systèmes, en particulier de la source, de la destination, du port, du protocole, du volume de données échangées et de l'identité des utilisateurs. Cette capacité permet d'analyser la sécurité ainsi que les opérations. De plus, grâce à une combinaison alliant signature et détection d'anomalie, elle permet de mettre en évidence l'état du réseau et d'identifier les écarts par rapport à la situation de référence, susceptibles de correspondre à un comportement anormal ou suspect. L'objet de cette capacité est que les entreprises puissent surveiller le comportement de leur réseau interne afin de détecter les activités suspectes.

En ce qui concerne la sécurité, les cas d'utilisation comprennent la surveillance afin de détecter la propagation des vers, l'installation non autorisée d'applications et les activités suspectes d'accès aux systèmes. En ce qui concerne les opérations, les cas d'utilisation comprennent la planification de capacité et l'analyse du trafic, notamment la capacité de relier une identité d'utilisateur à un flux de trafic, ou de répondre aux exigences d'un auditeur demandant de suivre l'accès des utilisateurs aux systèmes essentiels. Cette capacité offre peu de visibilité au-delà de la couche 3, et ne permet donc pas de détecter directement les problèmes d'accès aux systèmes, bases de données, contenus, systèmes de fichiers, etc.

Surveillance des menaces avancées

Des logiciels malveillants ciblés contournent la génération actuelle de systèmes de prévention des intrusions (IPS) et de pare-feu dans le réseau et de passerelles de sécurité sur le web. Certains petits fournisseurs spécialisés proposent des produits basés sur le réseau permettant de détecter les menaces avancées. Ces outils consistent généralement à analyser les exécutables afin de détecter les capacités malveillantes (utilisant souvent des environnements virtuels), à surveiller les communications (y compris les requêtes DNS (système de noms de domaines)) à destination ou en provenance des centres de commande et de contrôle de botnets connus ou présumés, ou à appliquer les deux techniques. Ces capacités permettent d'identifier rapidement un risque de compromission par une menace avancée (par exemple une menace avancée persistante), mais un grand nombre de capacités identiques sont actuellement ajoutées aux pare-feu, systèmes de prévention des intrusions (IPS) et passerelles de sécurité sur le web de prochaine génération.

D'autres fonctions sont spécialisées dans la détection des menaces contre une entreprise dans l'environnement externe, y compris le "darknet", dans les canaux de messagerie instantanée, dans les forums de discussion, dans les réseaux sociaux, etc. Ces fonctions visent à détecter les activités relatives à un domaine, à un ensemble d'adresses IP ou à des mots clés.

Gestion des informations et des événements de sécurité

La capacité de gestion des informations et des événements de sécurité consiste à assurer une large collecte d'événements parmi différentes sources d'informations et à les corréler pour assurer une détection précoce des atteintes à la sécurité. Elle améliore la gestion des menaces et la réponse aux incidents de sécurité moyennant la collecte et l'analyse d'événements de sécurité émanant de sources de données très diverses en temps réel. Ces sources sont les suivantes: dispositifs de réseau et de sécurité, journaux de serveur, de base de données et d'application, données fournies par des applications liées à la sécurité, par exemple des applications de gestion de la sécurité et de

surveillance des activités relatives aux bases de données, et données fournies par des systèmes de gestion d'identité et d'accès, par exemple les annuaires d'entreprise ou les systèmes de gestion de configuration et d'accès pour les utilisateurs. En outre, cette capacité surveille le respect des règles de sécurité et enquête sur les incidents en procédant à une analyse des données passées émanant de ces sources et en établissant des rapports sur ces données.

Aux fins de détection des fraudes, la capacité agrège et analyse les données relatives aux événements qui sont produites par les dispositifs, les systèmes et les applications. La principale source de données est constituée par les données des journaux, mais la capacité traite aussi d'autres formes de données. Les données sont normalisées afin que les événements émanant de sources distinctes puissent être corrélés et analysés en fonction des ensembles de règles qui sont conçus à des fins spécifiques, par exemple la surveillance des événements de sécurité dans le réseau ou la surveillance des activités des utilisateurs, car la surveillance et l'analyse dépendent entièrement des données relatives aux événements qui sont produites par d'autres sources. Toute activité qui n'est pas prise en compte en tant qu'événement ou dans un journal d'activités est invisible pour la capacité.

8.2 Capacités de détection

Pour la détection des fraudes, on utilise des processus basés sur des serveurs en arrière-plan (transparents pour les utilisateurs) qui examinent les accès et les comportements des utilisateurs. Ces informations sont ensuite comparées à un profil de ce qui est attendu et considéré comme "normal". Parallèlement, une combinaison de facteurs de risque est évaluée afin de mettre en évidence les vraies fraudes et de maintenir le taux de fausses détections à un faible niveau. Les transactions suspectes des utilisateurs sont revérifiées en temps réel pour déterminer si elles sont légitimes, ou elles sont suspendues en attendant que les analystes des fraudes disposent de suffisamment de temps pour déterminer si elles sont légitimes.

Etant donné que la détection des fraudes a lieu dans le contexte d'une application, elle ne permet pas de détecter les processus indésirables et potentiellement frauduleux qui sont extérieurs à l'application. Elle ne permet pas non plus de détecter un comportement suspect qui n'est pas défini dans son moteur car les règles n'intègrent pas le schéma d'activité, le modèle n'a pas suffisamment appris pour pouvoir le repérer ou l'application ne fournit pas assez de données pertinentes au moteur d'évaluation du risque de fraude. Pour que la détection soit efficace, le système d'analyse doit disposer de connaissances intégrées pour différents cas d'utilisation, ou le client doit fournir ces connaissances sous la forme de règles et de rapports de corrélation personnalisés. Le système de détection des fraudes a donc besoin de capacités permettant en particulier de mettre à jour les schémas de fraude, de prendre en charge une bibliothèque de règles prédéfinies, et d'appliquer les règles en temps réel.

La plupart des capacités nécessitent des efforts considérables d'ajustement des modèles, d'ajustement des profils et d'élaboration des règles de détection avant que les applications soient entièrement fonctionnelles. Ces capacités sont les suivantes: surveillance de toutes les transactions, analyse et évaluation automatiques des risques, établissement des profils de comportement des utilisateurs et apprentissage, détection de fraude intelligente ou propre à un service applicatif, et évaluation des risques multicanal.

Saisie de transaction

La saisie de transaction désigne les capacités qui repèrent et extraient les principaux attributs des transactions et qui nécessitent l'établissement automatique d'un profil détaillé du comportement de chaque utilisateur lors du premier accès.

Normalisation et taxinomie des événements

Les données relatives aux événements doivent être normalisées afin que les événements émanant de sources distinctes puissent être corrélés et analysés en fonction des ensembles de règles qui sont

conçus à des fins spécifiques, par exemple la surveillance des événements de sécurité dans le réseau ou la surveillance des activités des utilisateurs. Les informations provenant de sources hétérogènes sont alignées sur un modèle commun de classification des événements. La taxinomie aide à reconnaître les schémas, et permet aussi d'améliorer la portée et la stabilité des règles de corrélation. La normalisation des événements provenant de sources hétérogènes permet de les analyser au moyen d'un nombre plus petit de règles de corrélation, ce qui réduit les efforts de déploiement et de support. En outre, les événements normalisés sont plus faciles à manipuler lorsqu'il s'agit d'élaborer des rapports et des tableaux de bord.

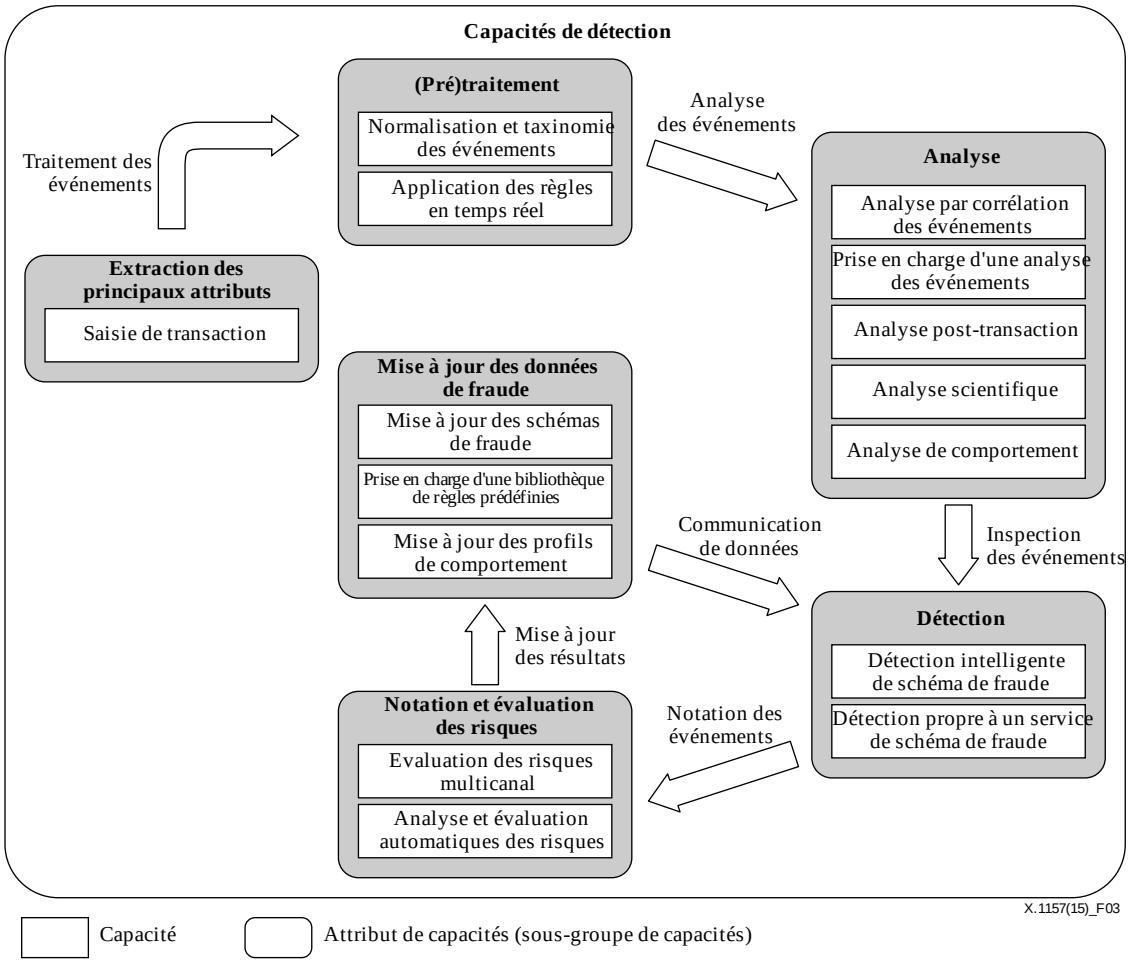

Figure 3 – Capacités de détection d'un système de détection des fraudes

Mise à jour des schémas de fraude

Une mise à jour des schémas de fraude est une mise à jour automatique des données sur les cas de fraude depuis le réseau. Ces données sur les cas de fraude comprennent des données IP géographiques pour pouvoir analyser l'emplacement de la source des transactions – ville, pays et fournisseur d'accès Internet (ISP) – ainsi que des données sur la réputation des serveurs hôtes pour pouvoir identifier les transactions provenant de sources suspectes connues, et des données sur les anonymiseurs pour les transactions provenant de quelqu'un qui cherche à cacher le point d'origine. La mise à jour des schémas de fraude devrait permettre d'appliquer le système de détection des fraudes à d'autres scénarios de fraude dans l'entreprise et de le personnaliser pour répondre aux exigences opérationnelles précises des entreprises. Par exemple, le système de détection des fraudes pourrait intégrer les résultats provenant de systèmes de détection des fraudes externes, d'évaluation du crédit et d'échange de renseignements, par exemple les listes noires.

Pour le déploiement d'une mise à jour des schémas de fraude, les renseignements sur l'environnement actuel des menaces existent dans diverses sources, en particulier dans des listes ouvertes à tous, dans les contenus sur les menaces et la réputation élaborés et tenus à jour par des équipes de recherche en sécurité des fournisseurs de solutions de sécurité, et dans les données compilées par les fournisseurs de services de gestion de la sécurité ou d'autres services. Les renseignements sur les menaces peuvent être intégrés dans un système de détection des fraudes sous la forme de listes de surveillance, de règles de corrélation et d'interrogations de manière à accroître le taux de détection précoce des atteintes à la sécurité.

Des informations à jour sur les menaces et les schémas d'attaque aident les organisations à reconnaître les activités anormales. Par exemple, un faible volume d'activités vers une adresse IP externe pourrait sembler normal et être tout simplement négligé. Il en va tout autrement s'il existe un système de renseignement sur les menaces qui indique que la destination est sous le contrôle d'un botnet. Cette information peut être passée au crible des algorithmes d'apprentissage automatique du comportement attendu, ou des règles plus génériques permettant de déterminer ce qui constitue un comportement "normal", afin de détecter les fraudes.

Prise en charge d'une bibliothèque de règles prédéfinies

La prise en charge d'une bibliothèque de règles prédéfinies signifie que le système de détection des fraudes prend en charge les règles disponibles qui ont fait leurs preuves pour neutraliser les fraudes. En général, cette fonction du système de détection des fraudes inclut un ensemble de règles éprouvées pour le déploiement et devrait aussi permettre de procéder facilement à la création de nouvelles règles et à la modification des règles existantes. En outre, cette fonction peut permettre d'échanger des règles avec d'autres organisations. Elle permet au système de détection des fraudes de mettre à jour et d'évaluer rapidement les règles et de nouveaux scénarios de fraude, et de visualiser et d'analyser facilement les données et les résultats de détection des fraudes. Elle peut aussi définir un ensemble spécifique de règles pour gérer les fraudes ou les utilisations abusives au niveau d'un client, au niveau d'un groupe de clients, ou pour tout autre utilisateur.

La plupart des systèmes de détection des fraudes à la carte de crédit permettent aux entreprises de gérer les règles applicables à chacune de leurs transactions, afin de pouvoir détecter les schémas de fraude propres à leurs situations.

Cette bibliothèque de règles pourrait définir un ensemble de règles sur la base d'informations contextuelles:

- Contexte concernant l'utilisateur: les rôles opérationnels d'un utilisateur.
- Contexte concernant les actifs: propriété, applications associées ou processus opérationnels.
- Contexte concernant la sécurité de l'information: vulnérabilités présentes au niveau du système d'exploitation, des applications, du web ou des bases de données, et état de la configuration.
- Contexte concernant les menaces externes: acteurs malveillants et schémas d'attaque connus.
- Contexte concernant les données: exigences critiques pour l'entreprise ou exigences juridiques et réglementaires.
- Contexte concernant l'application: utilisation de l'application dans l'entreprise et limites de l'accès normal aux données.

Analyse par corrélation des événements

La corrélation des événements établit des relations entre les messages ou les événements qui sont générés par les dispositifs, les systèmes ou les applications, sur la base de caractéristiques comme la source, la cible, et le protocole ou le type d'événement. Il faudrait aussi disposer d'une bibliothèque de règles de corrélation prédéfinies et pouvoir personnaliser facilement ces règles. A l'aide d'une

analyse par corrélation des événements, une console d'affichage des événements de sécurité devrait pouvoir présenter en temps réel les incidents et événements de sécurité.

Prise en charge d'une analyse des événements

Une analyse des événements est basée sur une corrélation des événements en temps réel, et sur une analyse des événements passés sur la base de requêtes. L'analyse des événements de sécurité repose sur des instantanés de tableau de bord, des rapports et des fonctions d'interrogation ad hoc pour faciliter l'examen des activités des utilisateurs et des accès aux ressources afin d'identifier les menaces, les atteintes à la sécurité ou les utilisations abusives des droits d'accès. Lorsqu'une activité suspecte est mise en évidence par la surveillance de la sécurité ou les rapports d'activité, il est important de pouvoir analyser les activités des utilisateurs et les accès aux ressources. Pour ce faire, on peut employer une approche itérative consistant à commencer par une interrogation générale au sujet de la source d'un événement, d'un utilisateur ou d'une cible, puis à lancer des interrogations de plus en plus ciblées pour identifier la source du problème. L'analyse des événements utilise des fonctions d'analyse de comportement pour compléter la corrélation basée sur des règles.

Application des règles en temps réel

L'application des règles en temps réel consiste à appliquer les règles de détection des fraudes au flux de transactions en temps réel pour générer des notes de risque pour les utilisateurs/sessions et des alertes détaillées en cas d'incident. Cette fonction doit prendre en considération les comportements inhabituels des utilisateurs, les schémas de fraude courants, les listes noires/blanches et les données sur les cas de fraude. Cette fonction peut prendre en charge une syntaxe de règles telle que des comportements inhabituels des utilisateurs avec des délais de grâce, une identité de dispositif client, des schémas de fraude courants, des listes noires/blanches, des données IP géographiques, et des données sur la réputation des serveurs hôte. De plus, le système de détection des fraudes peut générer une note de risque pour chaque session et une note de risque cumulative pour chaque utilisateur; il peut aussi activer une authentification basée sur le risque, qui fournit les notes de risque pour les utilisateurs et les sessions en temps réel au système d'authentification afin de déterminer si une authentification supplémentaire est nécessaire.

Prise en charge d'un outil de gestion

La fonction de prise en charge d'un outil de gestion assure le stockage et l'analyse efficaces d'une grande quantité d'informations, y compris la collecte, l'indexage et le stockage de toutes les données des journaux et de toutes les données relatives aux événements provenant de toutes les sources, ainsi que la capacité de mener des recherches et d'établir des rapports sur ces données. Les capacités d'établissement de rapport devraient aussi intégrer des rapports prédéfinis, et permettre de définir des rapports ad hoc ou d'utiliser des outils d'établissement de rapport de tiers. La fonction d'outil de gestion intègre généralement des rapports prédéfinis et modifiables pour les activités des utilisateurs et les accès aux ressources et des rapports types à des fins spécifiques et pour la gestion périodique. En général, l'outil de gestion est disponible sur le web et prend en charge l'attribution des cas et les processus associés, y compris la présentation de vues propres à un utilisateur, par exemple la situation sur les cas de fraude connus, les activités en cours et les nouveaux éléments marqués, et des mécanismes d'alerte configurables, y compris des notifications par courriel et sur le web.

Analyse post-transaction

L'analyse post-transaction permet de saisir et de stocker tous les éléments de données en vue d'une analyse future. L'entrepôt de données contient alors un historique complet des transactions pour tous les utilisateurs pour une période donnée. Cette fonction nécessite des processus sophistiqués de saisie et de formatage des données pour pouvoir stocker les données en temps réel et les extraire et les évaluer rapidement. Le système de détection des fraudes utilise le profil de comportement de chaque utilisateur individuel pour l'analyse post-transaction et peut stocker les transactions en les classant par session, par utilisateur et par date aux fins de l'extraction et de l'analyse.

Analyse scientifique

La fonction d'analyse scientifique consiste à faire des recherches, procéder à un filtrage et faire une analyse en profondeur dans l'entrepôt des données relatives aux transactions. Elle permet de filtrer, de rechercher et d'analyser en détail des transactions et des schémas d'accès. Elle permet d'identifier de nouveaux schémas de fraude pour lesquels il conviendrait de disposer de règles de détection en temps réel.

Analyse de comportement

Le système de détection des fraudes a besoin des transactions avec les profils de comportement pour tous les utilisateurs et prend en charge des systèmes plus sophistiqués pour suivre le comportement des différents utilisateurs. Il élabore un profil d'activités normales et utilise une fonction d'analyse de comportement afin de signaler les écarts par l'envoi d'alertes. L'établissement des profils de comportement comporte une phase d'apprentissage qui élabore les profils d'activités normales pour les données relatives aux événements émanant de sources discrètes collectées par les capacités de surveillance.

Le système de détection des fraudes commence automatiquement à établir le profil de comportement d'un utilisateur dès qu'il voit cet utilisateur. Il peut ensuite élaborer un profil de ce qui est considéré comme un comportement "normal" pour cet utilisateur puis repérer tout comportement "inhabituel". La phase de détection signale par une alerte les écarts par rapport au comportement normal. Lorsque les conditions anormales sont bien définies, il est possible de définir des règles de corrélation qui recherchent un ensemble précis de conditions. La capacité doit détecter, suivre, traduire et comprendre automatiquement les schémas et les anomalies qui peuvent être préjudiciables tout en évitant d'interrompre les activités des clients légitimes. Enfin, l'établissement des profils de comportement permet de déterminer le risque sur la base de l'écart par rapport au comportement normal.

Après l'établissement d'un profil initial, le système a besoin de plus de temps pour apprendre ce qui constitue un comportement anormal ou les entreprises ont besoin de plus de temps pour mettre en oeuvre les bonnes règles qui permettront de détecter un comportement ou une session anormal. Cette approche permet d'améliorer la capacité de découverte d'une attaque ciblée mais des efforts d'ajustement considérables devront encore être déployés par les experts du domaine pour limiter les faux positifs.

Détection intelligente de schéma de fraude

Les fraudes ne peuvent pas toutes être détectées au moyen des journaux de réseau et d'application et des différents champs de données. Il faut prévoir une analyse de données non structurées reposant sur l'utilisation de diverses logiques d'exploration des données qui permettent d'évaluer si les informations saisies sont appropriées.

Les entreprises devraient opter pour des logiques d'exploration des données qui apprennent par elles-mêmes, avec peu de données, et pour des systèmes leur permettant de mettre à jour les règles facilement et rapidement compte tenu des paramètres de fraude connus ou nouvellement découverts. L'identité d'un nouvel utilisateur en ligne peut être vérifiée à l'aide d'un service de notation d'identité, fourni directement par des fournisseurs de systèmes de notation d'identité. Ces notes établissent la probabilité qu'un utilisateur en ligne soit un fraudeur.

Détection propre à un service de schéma de fraude

Un système de détection des fraudes doit pouvoir définir des règles permettant de rechercher des schémas de transactions qui correspondent à des schémas de fraude connus et à des schémas de fraude propres à un service. En d'autres termes, le système recherche une séquence spécifique de transactions et de conditions qui sont suspectes conformément à la logique opérationnelle du service

applicatif. Un tel schéma pourrait concerner une seule session, ou bien plusieurs sessions et plusieurs utilisateurs en fonction du service applicatif considéré.

Enfin, en cas de mauvais réglage, les systèmes de détection des fraudes peuvent générer un trop grand nombre de faux positifs. Dans des environnements tels que celui du commerce électronique, où une exécution en temps réel est impérative, un taux élevé de faux positifs est clairement inacceptable.

Evaluation des risques multicanal

Les systèmes de détection des fraudes opèrent uniquement dans une application donnée et dans un canal donné, et non pas sur plusieurs canaux (par exemple, téléphone, web ou en personne) ou types de compte (par exemple, compte de dépôt ou compte de crédit). En outre, les systèmes de détection des fraudes ne sont pas au courant des activités frauduleuses en dehors de l'application, et ils ne sont pas intégrés dans les systèmes qui sont au courant de ces activités (par exemple, détection des fraudes dans un réseau et dans un système). Par conséquent, ils ne permettent pas de détecter les processus indésirables et potentiellement frauduleux qui sont extérieurs à l'application.

Cela étant, pour détecter les fraudes, il faut être attentif aux activités suspectes des utilisateurs pour une application via un canal d'accès donné (par exemple, sur le web, par téléphone ou en personne), ou pour différentes applications et différents canaux d'accès, ou encore pour différentes organisations (par exemple lorsqu'elles partagent des listes noires d'adresses IP). Il s'agit de détecter aussi bien un accès anormal (par exemple, un accès simultané par un même dispositif depuis deux emplacements géographiques distincts) qu'une séquence de transactions suspecte (par exemple, la modification d'une adresse suivie d'un transfert d'argent d'un montant élevé).

Pour détecter davantage de fraudes, le système de détection des fraudes doit intégrer les notes provenant des modules de détection des fraudes dans des modules de notation des risques multicanal qui prennent en compte l'ensemble des canaux des utilisateurs (par exemple, centres d'appel ou distributeurs automatiques (ATM)).

Analyse et évaluation automatiques des risques

Cette fonction nécessite de pouvoir évaluer et estimer automatiquement les risques de sécurité. La détection des fraudes et la notation du risque pour une transaction reposent sur des modèles ou des règles, ou une combinaison des deux. Pour détecter des activités suspectes à partir de diverses données collectées, on peut utiliser diverses techniques de modélisation – réseaux bayésiens, réseaux neuronaux, etc. – et d'autres techniques d'exploration des données, qui ont besoin de données pour calculer les probabilités de fraude.

Les réseaux neuronaux qui fonctionnent bien dans l'espace actuel des cartes de crédit ne donnent pas satisfaction dans l'espace Internet car ils ont besoin de grandes quantités de données pour détecter les schémas frauduleux. Par conséquent, pour les transactions sur le web, le système de détection des fraudes utilise d'autres techniques de modélisation, par exemple les réseaux bayésiens, qui ont besoin de moins de données pour calculer les probabilités de fraude, ou simplement une détection basée sur des règles. Les modèles de détection des fraudes génèrent des notes de risque, qui peuvent être intégrées dans les ensembles de règles des applications puis conservées et mises à jour par l'entreprise ou l'organisation.

8.3 Capacités de réponse

Le système de détection des fraudes nécessite un déclenchement automatique d'alertes à la fraude, le blocage de comptes, et une vérification renforcée du demandeur d'une transaction particulière qui a été étiquetée comme suspecte aux fins de la réponse aux incidents. Toutes les demandes d'ouverture de compte en ligne ou les transactions anonymes présentant un risque élevé devraient passer par un ensemble de procédures de filtrage initiales, à commencer par les événements d'authentification résultant de la procédure initiale de contrôle d'identité ainsi que l'utilisation des

applications et les journaux des applications. La procédure initiale de filtrage inclut une procédure élémentaire de détection des fraudes, par exemple l'identification du dispositif du client et la vérification des données d'identité de base, comme le nom, l'adresse de courrier électronique, l'analyse de l'emplacement géographique, la validation du numéro de téléphone, la détection des fraudes à la carte de crédit, la validation des rapports du bureau de crédit et/ou la notation de l'identité.

Les transactions suspectes qui ne passent pas les étapes initiales de contrôle d'identité devraient être transmises à une équipe d'enquête sur les fraudes, et mises en file d'attente en attendant un filtrage supplémentaire manuel ou automatique. Le système de détection des fraudes peut ensuite utiliser une approche stratifiée de contrôle d'identité basée sur le risque, qui renforce la vérification d'identité si un filtrage supplémentaire est demandé pour des utilisateurs suspects et des transactions présentant un risque élevé.

Vérification renforcée du demandeur

Le système de détection des fraudes peut intégrer le mécanisme d'authentification de manière à ce que la note de risque générée par le système de détection des fraudes détermine la force de l'authentification de l'utilisateur ou de la vérification des transactions de l'utilisateur. Il présente les mesures qui peuvent être prises pour éliminer les transactions suspectes ou autres transactions présentant un risque élevé qui nécessitent un contrôle d'identité. Dans un souci de réduction des coûts et de commodité pour les clients, les entreprises peuvent utiliser une approche basée sur le risque, dans laquelle la force de la solution de contrôle d'identité est proportionnée au risque de la transaction. Pour cela, le système de détection des fraudes peut utiliser conjointement plusieurs applications de contrôle d'identité (voir [b-UIT-T X.1154]).

D'une manière générale, on ne trouve pas sur le marché une seule application de contrôle d'identité universelle, mais plusieurs mécanismes de contrôle d'identité qui peuvent être associés afin de dissuader efficacement les fraudeurs.

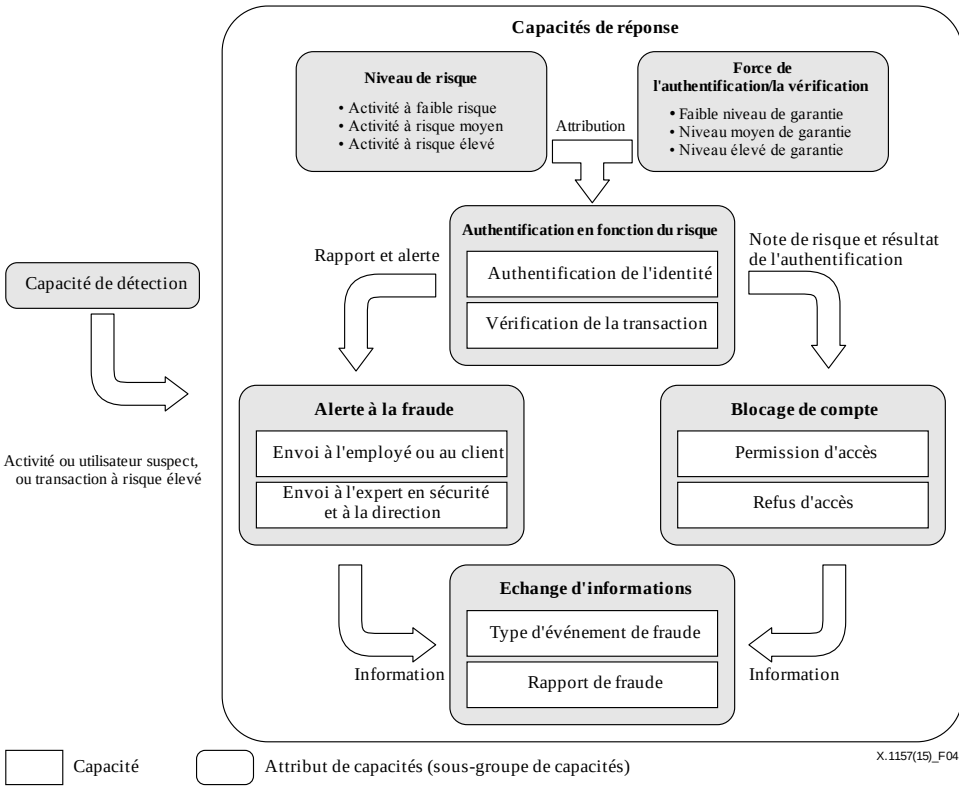

Figure 4 – Capacités de réponse d'un système de détection des fraudes

Authentification en fonction du risque

Plus le risque, déterminé par exemple par un système de détection des fraudes, est élevé, plus les mesures de contrôle d'identité nécessaires sont coûteuses et gênantes pour le client. On dispose de plusieurs approches lorsqu'une authentification plus forte est nécessaire, par exemple:

- L'accès initial au compte est configuré de manière à autoriser les activités à faible risque, par exemple l'accès en lecture seule aux informations publiques, nécessitant un contrôle d'identité très élémentaire. Par exemple, le mécanisme de contrôle d'identité peut vérifier le nom et l'adresse postale de l'utilisateur par rapport à une source secondaire.
- Les activités à risque plus élevé, par exemple la mise à jour d'une adresse postale, sont retardées en attendant que soit effectué un contrôle d'identité plus fort (voir [b-UIT-T X.1254]) avec détection des fraudes, notamment une authentification fournissant un niveau de garantie plus élevé.
  - Le mécanisme de contrôle d'identité peut vérifier les informations personnelles par rapport à une base de données publiques en utilisant une authentification basée sur des connaissances. Cette vérification combine des informations accessibles au public, par exemple des données démographiques, des listes de titulaires de permis de conduire et des données des bureaux de crédit.
  - Le mécanisme de contrôle d'identité peut exiger que l'utilisateur réponde à une ou plusieurs questions pour lesquelles une réponse a été fournie au préalable et stockée dans le profil de l'utilisateur ou qui sont basées sur des informations que le vrai titulaire du compte devrait connaître.
  - Le mécanisme de contrôle d'identité peut employer des méthodes d'authentification utilisant d'autres canaux, par exemple la téléphonie mobile ou le courrier électronique, pour contacter le titulaire du compte. Il peut aussi envoyer un mot de passe à usage unique à un nouvel utilisateur en ligne par appel téléphonique ou SMS (message du

service de messages courts) à un numéro de téléphone qui est déjà enregistré au niveau de l'entreprise ou qui a été saisi par l'utilisateur sur une page de demande d'ouverture d'un nouveau compte ou de paiement.

- Les activités les plus risquées, comme les transferts d'argent vers un compte bancaire externe, sont interdites en attendant que l'utilisateur puisse être contacté pour validation; toutefois, comme de nombreuses transactions sont exécutées par lots (et non en temps réel), cette approche ne modifiera peut-être pas le calendrier d'exécution des transactions.

Alertes à la fraude

Les alertes à la fraude consistent à générer automatiquement ou manuellement des alertes lorsque des activités suspectes sont détectées. En général, une alerte à la fraude résulte de l'association d'une note de risque et de règles appliquées en fonction de cette note. Les alertes détaillées comprennent une description des attributs des transactions et des activités et peuvent être notifiées par courrier électronique ou par téléavertisseur et être configurées en fonction de la règle, de la gravité et des droits de l'utilisateur. Les alertes à la fraude peuvent être envoyées à un expert en sécurité ou à un client/utilisateur en fonction du niveau de risque mesuré. L'expert en sécurité peut ensuite examiner de manière plus détaillée le risque perçu, tandis que l'envoi de l'alerte à la fraude au client/à l'utilisateur permet d'alerter les prêteurs potentiels du fait que leur identité a pu être dérobée.

Blocage de compte

Le blocage d'un compte d'utilisateur a lieu lorsqu'une activité suspecte est détectée. L'accès de l'utilisateur est autorisé ou refusé en fonction de la note attribuée et des limites de tolérance de l'établissement. Les utilisateurs qui ont une note insuffisante pour pouvoir obtenir un accès sans restriction obtiendront un accès limité ou seront obligés de passer par une authentification plus forte pour obtenir un accès sans restriction ou être autorisés à effectuer certaines transactions à risque élevé. Si les utilisateurs ne respectent pas cette obligation, ils pourront recommencer la procédure de vérification renforcée ou seront bloqués rapidement.

Echange d'informations

Les systèmes de détection des fraudes devraient garantir une coordination efficace des activités de réponse aux incidents avec les partenaires compétents de l'organisation.

L'aspect le plus important de la coordination en matière de réponse aux incidents est l'échange d'informations sur les menaces, les attaques et les vulnérabilités entre différentes organisations de manière à ce que chacune puisse tirer parti des connaissances dont disposent les autres. Un échange d'informations peut aussi avoir lieu directement entre l'entreprise et les clients ou entre l'organisation et les employés car il est fréquent que les mêmes menaces et attaques touchent simultanément plusieurs organisations ou services. L'objet de l'échange d'informations est de permettre à toute organisation qui a détecté une fraude de communiquer cette information, en interne ou avec les autres organisations risquant d'en être victimes.

Les organisations qui reçoivent ce type d'information peuvent par exemple entreprendre un examen manuel des transactions lancées depuis les adresses IP suspectes. Un rapport de fraude pourra décrire une transaction particulière dont on sait ou dont on pense qu'elle est frauduleuse, ou pourra décrire un schéma de comportement dont on pense qu'il est le signe d'une fraude.

Appendice I

Services applicatifs TIC sensibles

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

I.1 Services financiers en ligne

I.1.1 Services bancaires en ligne et problèmes de sécurité

Les services bancaires en ligne permettent aux clients d'un établissement financier de mener des transactions financières sur un site Internet sécurisé exploité par l'établissement, qui peut être une banque de détail ou virtuelle, une coopérative de crédit ou une société de crédit immobilier. Pour bénéficier des services bancaires en ligne d'un établissement financier, un client ayant un accès Internet personnel doit adresser une demande à l'établissement, et établir un mot de passe (sous divers noms) aux fins de vérification. Pour accéder aux services bancaires en ligne, le client va sur le site Internet de l'établissement financier, et saisit son numéro de client et son mot de passe. Certains établissements financiers ont mis en place d'autres mesures de sécurité pour l'accès, mais l'approche adoptée est différente d'un établissement à l'autre.

L'authentification au moyen d'un mot de passe unique est toujours employée, mais certains pays considèrent qu'à elle seule, elle n'est pas assez sûre pour les services bancaires en ligne. Deux méthodes différentes sont utilisées pour la sécurité des services bancaires en ligne.

- Le système de numéro d'identification personnel/numéro d'authentification de transaction (PIN/TAN) dans lequel le numéro PIN représente un mot de passe utilisé pour la connexion et les numéros TAN représentent des mots de passe à usage unique utilisées pour authentifier les transactions. Les numéros TAN peuvent être distribués de différentes manières, la plus courante consistant à envoyer une liste de numéros TAN à l'utilisateur des services bancaires en ligne par lettre postale. Le moyen d'utilisation le plus sûr des numéros TAN consiste à les générer lorsqu'on en a besoin au moyen d'un jeton de sécurité. Les numéros TAN générés de cette façon sont fonction de l'heure et d'un secret unique, stocké dans le jeton de sécurité (authentification à deux facteurs). Les services bancaires en ligne avec PIN/TAN sont généralement offerts via un navigateur web utilisant des connexions sécurisées SSL (couche de connecteurs sécurisés), de sorte qu'aucun chiffrement supplémentaire n'est nécessaire.
- Pour fournir les numéros TAN à un utilisateur de services bancaires en ligne, un autre moyen consiste à envoyer le numéro TAN de la transaction bancaire en cours sur le téléphone mobile GSM (système mondial de communications mobiles) de l'utilisateur par SMS. En général, le SMS indique le montant et les détails de la transaction; la validité du numéro TAN n'est que de courte durée. Ce service de "numéro TAN par SMS" a été adopté par des banques dans un grand nombre de pays, en particulier en Allemagne, en Autriche et aux Pays-Bas, car il est considéré comme très sûr.
- Les services bancaires en ligne basés sur une signature, pour lesquels toutes les transactions sont signées et chiffrées numériquement. Les clés pour la génération de la signature et le chiffrement peuvent être stockées sur des cartes à puce ou sur un support de mémoire, en fonction de la mise en oeuvre concrète.

I.1.2 Paiement en ligne et problèmes de sécurité

Un paiement en ligne est un transfert électronique d'argent d'un compte à un compte, au sein d'un même établissement financier ou faisant intervenir plusieurs établissements, au moyen de systèmes informatiques.

Les utilisateurs ne feront pas confiance à un système de paiement en ligne non sécurisé. Il est absolument indispensable que le système soit fiable pour que les utilisateurs l'adoptent. Les applications de paiement en ligne représentent un défi pour la sécurité, du fait qu'elles s'appuient largement sur les systèmes TIC essentiels, ce qui crée des vulnérabilités dans les établissements financiers et les entreprises et peut entraîner des préjudices pour les clients. Pour qu'une transaction financière électronique soit sûre, les exigences suivantes doivent être respectées:

- Intégrité et autorisation: l'intégrité signifie que les informations sont exactes, complètes et valables conformément aux valeurs et aux attentes de l'entreprise. L'intégrité pour un système de paiement signifie qu'une somme d'argent n'est retirée à un utilisateur que si celui-ci autorise le paiement. De plus, les utilisateurs pourraient demander à un établissement financier de ne pas effectuer de paiement à leur intention sans leur accord explicite.
- Confidentialité: la confidentialité est définie comme la protection des informations sensibles ou privées contre toute divulgation non autorisée. Certaines parties concernées voudront peut-être que les transactions soient confidentielles. La confidentialité dans ce contexte signifie que diverses informations relatives à une transaction, par exemple l'identité du payeur/bénéficiaire, l'objet de l'achat, la somme, etc., ne doivent pas être divulguées. Dans la plupart des cas, les participants concernés voudront que les communications soient privées.
- Disponibilité et fiabilité: la disponibilité vise à garantir que les systèmes d'information et les données sont prêts à être utilisés lorsqu'on en a besoin. Elle est souvent exprimée par le pourcentage de temps pendant lequel un système peut être utilisé pour un travail productif. Toutes les parties souhaitent pouvoir effectuer ou recevoir des paiements chaque fois qu'elles en ont besoin.

I.2 Services médicaux en ligne

Les services médicaux en ligne, destinés à assurer une gestion électronique de toutes les activités dans les grands établissements médicaux, sont très prometteurs pour ce qui est d'accélérer les tâches administratives dans les centres médicaux et les hôpitaux. Toutefois, la mise en oeuvre concrète de services médicaux en ligne pose de nombreux problèmes de sécurité. Pour que les hôpitaux adoptent largement les services médicaux en ligne, il est essentiel d'examiner en détail les problèmes de sécurité et de jeter les bases de la normalisation de divers composants afin de mettre en oeuvre correctement des services médicaux en ligne. Un système médical en ligne type peut être constitué de nombreux composants et sous-systèmes: prise de rendez-vous; admission, sortie et transfert; saisie des ordonnances; régimes alimentaires; notes cliniques de routine; demandes analyses et de radios; archivage des images, et inscription par carte à puce. Chacun de ces sous-systèmes est vulnérable aux menaces contre la sécurité.

I.2.1 Problèmes de sécurité liés aux services médicaux en ligne

- Menaces contre la confidentialité et la sécurité des informations: la base de connaissances existante sur les risques pour la sécurité des informations identifie différents types de menaces contre la confidentialité et la sécurité des informations médicales. Toutefois, la taxinomie ad hoc actuelle ne peut pas, à elle seule, être utile dans la pratique.
- Inquiétudes des patients concernant la confidentialité: avec l'utilisation croissante de systèmes sur le web pour la gestion des informations médicales et le déploiement de banques de données médicales personnelles, les inquiétudes des patients concernant la confidentialité sont passées au premier plan.
- Interopérabilité des données et sécurité des informations: le principe de base de l'interopérabilité des données est d'assurer un échange de données précis et transparent dans

une même organisation et entre plusieurs organisations pour favoriser l'administration des soins de santé dans les meilleurs délais.

- Problèmes de sécurité des informations médicales: le secteur médical a connu une augmentation considérable de l'utilisation de dispositifs mobiles et d'applications sur le web. Dans le même temps, les travaux de recherche en sécurité de l'information ont été ciblés sur l'élaboration de cadres et de protocoles afin de remédier aux problèmes de sécurité dans le secteur médical.

I.3 Services d'accès à distance aux entreprises

De nombreux employés des organisations et intervenants extérieurs utilisent des systèmes d'accès à distance aux entreprises pour effectuer un travail à distance. La plupart des télétravailleurs utilisent des systèmes d'accès à distance aux entreprises pour interagir avec les ressources informatiques non publiques d'une organisation. La nature de ces systèmes d'accès à distance – permettant d'accéder à des ressources protégées depuis des réseaux externes et souvent aussi depuis des serveurs hôtes externes – fait que ces systèmes sont généralement exposés à un risque plus élevé que les systèmes analogues avec accès uniquement depuis l'intérieur de l'organisation, et le risque associé aux ressources internes mises à la disposition des télétravailleurs via l'accès à distance est accru.

I.3.1 Problèmes de sécurité liés à l'accès à distance aux entreprises

Les objectifs de sécurité les plus courants pour les systèmes d'accès à distance aux entreprises sont les suivants:

- Confidentialité: garantir que les communications via l'accès à distance et les données d'utilisateur stockées ne puissent pas être lues par des parties non autorisées.
- Intégrité: détecter toute modification apportée volontairement ou non aux communications via l'accès à distance.
- Disponibilité: garantir que les utilisateurs puissent accéder aux ressources depuis un point d'accès distant chaque fois qu'ils en ont besoin.

Pour atteindre ces objectifs, tous les composants des solutions d'accès à distance aux entreprises – dispositifs client, serveurs d'accès à distance et serveurs internes accessibles depuis un point d'accès distant – doivent être protégés contre diverses menaces. Les systèmes d'accès à distance ont souvent besoin d'une protection supplémentaire car, du fait de leur nature, ils sont généralement plus exposés aux menaces externes que les systèmes avec accès uniquement depuis l'intérieur de l'organisation.

Les principaux problèmes de sécurité concernant l'accès à distance aux entreprises sont les suivants:

- Insuffisance des contrôles en matière de sécurité physique: les dispositifs client avec accès à distance sont utilisés en divers lieux hors du contrôle de l'organisation, par exemple au domicile des employés, dans des cafés, dans des hôtels ou dans des salles de conférence. Du fait qu'ils sont mobiles, ces dispositifs peuvent facilement être perdus ou dérobés, d'où un risque de compromission élevé pour les données contenues dans ces dispositifs. Même si le propriétaire d'un dispositif client l'a toujours en sa possession, il existe d'autres risques pour la sécurité physique, par exemple un attaquant qui regarde par-dessus l'épaule d'un télétravailleur dans un café et voit des données sensibles sur l'écran du dispositif client.
- Réseaux non sécurisés: étant donné que l'accès à distance se fait pratiquement toujours sur l'Internet, les organisations n'ont en principe aucun contrôle sur la sécurité des réseaux externes utilisés par les clients. Les systèmes de communication utilisés pour l'accès à distance sont notamment les suivants: téléphones et modems DSL (ligne d'abonné numérique), réseaux large bande câblés ou hertziens (voir [b-IEEE 802.11]), WiMAX (interopérabilité mondiale pour l'accès hyperfréquence), et réseaux cellulaires. Ces systèmes de communication sont susceptibles de faire l'objet d'écoutes clandestines, d'où un

risque de compromission pour les informations sensibles transmises via l'accès à distance. Des attaques par intercepteur (MITM) peuvent aussi être perpétrées pour intercepter et modifier des communications. Le risque lié à l'utilisation de réseaux non sécurisés peut être atténué, mais pas éliminé, par l'utilisation de techniques de chiffrement pour protéger la confidentialité et l'intégrité des communications, ainsi que par l'utilisation de mécanismes d'authentification mutuelle pour vérifier les identités des deux points d'extrémité.

- Dispositifs infectés sur les réseaux internes: les dispositifs client, en particulier les ordinateurs portables, sont souvent utilisés sur des réseaux externes, puis apportés dans l'organisation et connectés directement au réseau interne de l'organisation. Un attaquant disposant d'un accès physique à un dispositif client peut installer des logiciels malveillants sur le dispositif pour collecter des données contenues dans ledit dispositif et dans les réseaux et systèmes auxquels il est connecté. Si un dispositif client est infecté par un logiciel malveillant, celui-ci peut se propager dans toute l'organisation une fois que le dispositif client est connecté au réseau interne. Outre l'utilisation de techniques appropriées de protection contre les logiciels malveillants dans la configuration de sécurité de base de l'organisation, par exemple des logiciels de protection contre les logiciels malveillants sur les dispositifs client, les organisations devraient envisager d'utiliser des solutions de contrôle d'accès au réseau (NAC) qui vérifient le niveau de sécurité d'un dispositif client avant de l'autoriser à utiliser un réseau interne. Les organisations devraient aussi envisager d'utiliser un réseau distinct pour les dispositifs client des télétravailleurs, au lieu de les autoriser à se connecter directement au réseau interne.
- Accès de l'extérieur à des ressources internes: l'accès à distance aux entreprises permet à des serveurs hôtes externes d'accéder à des ressources internes, par exemple des serveurs. Si ces ressources internes n'étaient pas auparavant accessibles depuis les réseaux externes, le fait de les rendre accessibles via l'accès à distance va les exposer à de nouvelles menaces, en particulier dans le cas de dispositifs client et de réseaux non sécurisés, et va accroître considérablement la probabilité de compromission de ces ressources. Chaque type d'accès à distance qui peut être utilisé pour accéder à une ressource interne accroît le risque de compromission de cette ressource.

Bibliographie

[b-UIT-T X.1141] Recommandation UIT-T X.1141 (2006), *Langage de balisage d'assertion de sécurité (SAML 2.0).*

[b-UIT-T X.1154] Recommandation UIT-T X.1154 (2013), *Cadre général de l'authentification combinée dans des environnements à plusieurs fournisseurs de service d'identité.*

[b-UIT-T X.1252] Recommandation UIT-T X.1252 (2010), *Termes et définitions de base relatifs à la gestion d'identité.*

[b-UIT-T X.1254] Recommandation UIT-T X.1254 (2012), *Cadre de garantie d'authentification d'entité.*

[b-IEEE 802.11] IEEE 802.11, *IEEE Standard for Information technology – Telecommunications and information exchange between systems, Local and metropolitan area network – Specific requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications.*

SÉRIES DES RECOMMANDATIONS UIT-T

Série A	Organisation du travail de l'UIT-T
Série D	Principes généraux de tarification
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	Terminaux et méthodes d'évaluation subjectives et objectives
Série Q	Commutation et signalisation
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 et réseaux de prochaine génération
Série Z	Langages et aspects généraux logiciels des systèmes de télécommunication

Imprimé en Suisse
Genève, 2016