Unión Internacional de Telecomunicaciones

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

X.1157

(09/2015)

SERIE X: REDES DE DATOS, COMUNICACIONES DE SISTEMAS ABIERTOS Y SEGURIDAD

Aplicaciones y servicios con seguridad – Protocolos de seguridad

Capacidades técnicas de detección y respuesta al fraude para servicios con requisitos de alto nivel de seguridad

Recomendación UIT-T X.1157

Unión Internacional de Telecomunicaciones

RECOMENDACIONES UIT-T DE LA SERIE X

REDES DE DATOS, COMUNICACIONES DE SISTEMAS ABIERTOS Y SEGURIDAD

REDES PÚBLICAS DE DATOS	X.1–X.199
INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.200–X.299
INTERFUNCIONAMIENTO ENTRE REDES	X.300–X.399
SISTEMAS DE TRATAMIENTO DE MENSAJES	X.400–X.499
DIRECTORIO	X.500–X.599
GESTIÓN DE REDES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS Y ASPECTOS DE SISTEMAS	X.600–X.699
GESTIÓN DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.700–X.799
SEGURIDAD	X.800–X.849
APLICACIONES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.850–X.899
PROCESAMIENTO DISTRIBUIDO ABIERTO	X.900–X.999
SEGURIDAD DE LA INFORMACIÓN Y DE LAS REDES	
Aspectos generales de la seguridad	X.1000–X.1029
Seguridad de las redes	X.1030–X.1049
Gestión de la seguridad	X.1050–X.1069
Telebiometría	X.1080–X.1099
APLICACIONES Y SERVICIOS CON SEGURIDAD	
Seguridad en la multidifusión	X.1100–X.1109
Seguridad en la red residencial	X.1110–X.1119
Seguridad en las redes móviles	X.1120–X.1139
Seguridad en la web	X.1140–X.1149
Protocolos de seguridad	**X.1150–X.1159**
Seguridad en las comunicaciones punto a punto	X.1160–X.1169
Seguridad de la identidad en las redes	X.1170–X.1179
Seguridad en la TVIP	X.1180–X.1199
SEGURIDAD EN EL CIBERESPACIO	
Ciberseguridad	X.1200–X.1229
Lucha contra el correo basura	X.1230–X.1249
Gestión de identidades	X.1250–X.1279
APLICACIONES Y SERVICIOS CON SEGURIDAD	
Comunicaciones de emergencia	X.1300–X.1309
Seguridad en las redes de sensores ubicuos	X.1310–X.1339
Recomendaciones relacionadas con la PKI	X.1340–X.1349
INTERCAMBIO DE INFORMACIÓN DE CIBERSEGURIDAD	
Aspectos generales de la ciberseguridad	X.1500–X.1519
Intercambio de estados/vulnerabilidad	X.1520–X.1539
Intercambio de eventos/incidentes/heurística	X.1540–X.1549
Intercambio de políticas	X.1550–X.1559
Petición de heurística e información	X.1560–X.1569
Identificación y descubrimiento	X.1570–X.1579
Intercambio asegurado	X.1580–X.1589
SEGURIDAD DE LA COMPUTACIÓN EN NUBE	
Visión general de la seguridad de la computación en nube	X.1600–X.1601
Diseño de la seguridad de la computación en nube	X.1602–X.1639
Prácticas óptimas y directrices en materia de seguridad de la computación en nube	X.1640–X.1659
Aplicación práctica de la seguridad de la computación en nube	X.1660–X.1679
Otras cuestiones de seguridad de la computación en nube	X.1680–X.1699

Para más información, véase la Lista de Recomendaciones del UIT-T.

Recomendación UIT-T X.1157

Capacidades técnicas de detección y respuesta al fraude para servicios con requisitos de alto nivel de seguridad

Resumen

La Recomendación UIT-T X.1157 describe las capacidades necesarias para el servicio de detección y respuesta al fraude de servicios basados en aplicaciones de tecnologías de la información y la comunicación (TIC) sensibles a la seguridad. El servicio de detección y respuesta al fraude permite la detección, el análisis y la gestión del fraude entre usuarios, cuentas, productos, procesos y canales. Supervisa y analiza la actividad y el comportamiento del usuario a nivel de aplicación (en lugar de hacerlo a nivel de sistema, de base de datos o de red) y observa lo que ocurre en las cuentas a través de cualquier canal disponible para el usuario. También analiza el comportamiento entre usuarios, cuentas u otras entidades relacionadas, y trata de detectar actividades anormales, corrupción o usos indebidos. Se utiliza por lo general en áreas verticales de gestión económica del cliente, como ciberfinanzas, acceso a distancia en la empresa, etc., pero también se utiliza a menudo para detectar fraudes internos y otros tipos de actividades no autorizadas.

Historia

Edición	Recomendación	Aprobación	Comisión de Estudio	ID único*
1.0	ITU-T X.1157	2015-09-17	17	11.1002/1000/12353

Palabras clave

Gestión del fraude, sistema de detección del fraude.

* Para acceder a la Recomendación, sírvase digitar el URL http://handle.itu.int/ en el campo de dirección del navegador, seguido por el identificador único de la Recomendación. Por ejemplo, http://handle.itu.int/11.1002/1000/11830-en.

PREFACIO

La Unión Internacional de Telecomunicaciones (UIT) es el organismo especializado de las Naciones Unidas en el campo de las telecomunicaciones y de las tecnologías de la información y la comunicación. El Sector de Normalización de las Telecomunicaciones de la UIT (UIT-T) es un órgano permanente de la UIT. Este órgano estudia los aspectos técnicos, de explotación y tarifarios y publica Recomendaciones sobre los mismos, con miras a la normalización de las telecomunicaciones en el plano mundial.

La Asamblea Mundial de Normalización de las Telecomunicaciones (AMNT), que se celebra cada cuatro años, establece los temas que han de estudiar las Comisiones de Estudio del UIT-T, que a su vez producen Recomendaciones sobre dichos temas.

La aprobación de Recomendaciones por los Miembros del UIT-T es el objeto del procedimiento establecido en la Resolución 1 de la AMNT.

En ciertos sectores de la tecnología de la información que corresponden a la esfera de competencia del UIT-T, se preparan las normas necesarias en colaboración con la ISO y la CEI.

NOTA

En esta Recomendación, la expresión "Administración" se utiliza para designar, en forma abreviada, tanto una administración de telecomunicaciones como una empresa de explotación reconocida de telecomunicaciones.

La observancia de esta Recomendación es voluntaria. Ahora bien, la Recomendación puede contener ciertas disposiciones obligatorias (para asegurar, por ejemplo, la aplicabilidad o la interoperabilidad), por lo que la observancia se consigue con el cumplimiento exacto y puntual de todas las disposiciones obligatorias. La obligatoriedad de un elemento preceptivo o requisito se expresa mediante las frases "tener que, haber de, hay que + infinitivo" o el verbo principal en tiempo futuro simple de mandato, en modo afirmativo o negativo. El hecho de que se utilice esta formulación no entraña que la observancia se imponga a ninguna de las partes.

PROPIEDAD INTELECTUAL

La UIT señala a la atención la posibilidad de que la utilización o aplicación de la presente Recomendación suponga el empleo de un derecho de propiedad intelectual reivindicado. La UIT no adopta ninguna posición en cuanto a la demostración, validez o aplicabilidad de los derechos de propiedad intelectual reivindicados, ya sea por los miembros de la UIT o por terceros ajenos al proceso de elaboración de Recomendaciones.

En la fecha de aprobación de la presente Recomendación, la UIT no ha recibido notificación de propiedad intelectual, protegida por patente, que puede ser necesaria para aplicar esta Recomendación. Sin embargo, debe señalarse a los usuarios que puede que esta información no se encuentre totalmente actualizada al respecto, por lo que se les insta encarecidamente a consultar la base de datos sobre patentes de la TSB en la dirección http://www.itu.int/ITU-T/ipr/.

ÍNDICE

Recomendación UIT-T X.1157

Capacidades técnicas de detección y respuesta al fraude para servicios con requisitos de alto nivel de seguridad

1 Alcance

Esta Recomendación ofrece directrices sobre las capacidades técnicas para la gestión del fraude en servicios con requisitos de garantías de seguridad de un nivel elevado. El objetivo de la Recomendación es proporcionar un sistema capaz de realizar actividades de detección del fraude. La Recomendación es aplicable a numerosos sectores comerciales y empresariales que utilizan aplicaciones de las tecnologías de la información y la comunicación (TIC) sensibles a la seguridad mediante el despliegue de un sistema de detección y respuesta al fraude. También es aplicable a la gestión del fraude interno en una organización así como del fraude externo realizado a través de accesos a distancia o de servicios comerciales. La recomendación abarca las áreas siguientes:

– capacidades para los servicios de detección y respuesta al fraude;

– operaciones y componentes del sistema de detección y respuesta al fraude; y

– consideraciones sobre el servicio de defensa y respuesta a incidentes.

2 Referencias

Ninguna.

3 Definiciones

3.1 Términos definidos en otros documentos

En esta Recomendación se utilizan los términos siguientes que se definen en otros documentos.

3.1.1 nivel de garantía *(assurance level)* [b-ITU-T X.1252]: nivel de confianza en la vinculación entre una entidad y la información de identidad presentada.

3.1.2 autentificación (de entidad) *((entity) authentication)* [b-ITU-T X.1252]: proceso utilizado para obtener una confianza suficiente en la vinculación entre la entidad y la identidad presentada.

NOTA – En el contexto de la gestión de identidad (IdM) se entiende que el término autentificación se refiere a la autentificación de una entidad.

3.1.3 garantía de autentificación (*authentication assurance*) [b-ITU-T X.1252]: grado de confianza a la que se llega en el proceso de autentificación de que el asociado de la comunicación es la entidad que declara ser o se espera que sea.

NOTA – La confianza se basa en el grado de confianza en el vínculo entre la entidad que comunica y la entidad a la que se presenta.

3.1.4 usuario final *(end user)* [b-ITU-T X.1141]: persona natural que aplica los recursos.

3.1.5 identidad *(identity)* [b-ITU-T X.1252]: representación de una entidad bajo la forma de uno o varios atributos que permiten distinguir suficientemente a la entidad o entidades dentro del contexto. A los efectos de la gestión de identidad (IdM), se entiende que este término constituye una identidad contextual (subconjunto de atributos), es decir que la diversidad de atributos está limitada por un marco con fronteras definidas (el contexto) en el cual existe e interactúa la entidad.

NOTA − Cada entidad está representada por una identidad holística que comprende todos los posibles elementos de información que caracterizan a dicha entidad (atributos). Sin embargo, la identidad holística es una cuestión teórica y elude cualquier descripción y utilización práctica, dado que el número de todos los atributos posibles es indefinido.

3.1.6 garantía de identidad (*identity assurance*) [b-ITU-T X.1252]: grado de confianza en el proceso de validación y verificación de la identidad utilizado para determinar la identidad de la entidad para la cual se expide la credencial, y el grado de confianza en que la entidad que utiliza la credencial es dicha entidad o la entidad a la cual se le expidió o asignó la credencial.

3.1.7 demostración de identidad *(identity proofing)* [b-ITU-T X.1252]: proceso mediante el cual se valida y verifica información suficiente como para confirmar la identidad alegada por la entidad.

3.1.8 verificación de identidad *(identity verification)* [b-ITU-T X.1252]: proceso a tenor del cual se confirma que la identidad declarada es correcta mediante la comparación de las declaraciones de identidad ofrecidas con información previamente demostrada.

3.1.9 proveedor de servicio *(service provider)* [b-ITU-T X.1141]: cometido que asume una entidad del sistema para proporcionar servicios a los principales u otras entidades del sistema.

3.2 Términos definidos en esta Recomendación

En esta Recomendación se utilizan los términos siguientes:

3.2.1 sistema de detección del fraude *(fraud detection system)*: software de aplicación para la supervisión, detección y gestión del fraude u otros usos indebidos de usuarios (por ejemplo, clientes), cuentas, canales, productos y otras entidades (por ejemplo, quioscos).

NOTA – Para desplegar un sistema de detección del fraude las aplicaciones de empresa pueden integrar un motor de detección del fraude con el fin de evaluar el riesgo de fraude en una transacción, desde la navegación del usuario y el acceso a la aplicación hasta cualquier tipo de actividad, como un cambio de dirección, la realización de pagos o la captura de información sensible.

3.2.2 gestión del fraude *(fraud management)*: gama completa de actividades que incluye sistemas de alerta temprana, signos y modelos de distintos tipos de fraude, perfiles de usuarios y sus actividades, respuesta a incidentes, etc. para mitigar el riesgo de la seguridad mediante un sistema de detección del fraude.

NOTA – Existen una serie de aspectos necesarios en el desarrollo de sistemas de gestión del fraude, incluido el enorme volumen de datos involucrados, el requisito de una detección del fraude rápida y precisa que no perturbe el funcionamiento del negocio, el desarrollo continuado de nuevos fraudes para eludir las técnicas existentes y el riesgo de falsas alarmas.

3.2.3 aplicaciones de las tecnologías de la información y la comunicación (TIC) sensibles a la seguridad (*security sensitive information and communication technology application*): aplicación que requiere un nivel muy elevado de garantías de seguridad para la protección de un activo de información de individuos, información secreta de la organización y/o la empresa.

NOTA – Cuando un atacante pone en peligro y controla aplicaciones TIC sensibles a la seguridad, la exposición de información sensible, es decir, información personal o financiera, tiene un efecto dañino masivo sobre usuarios, organizaciones, servicios e infraestructura de telecomunicaciones, que pueden incluir aplicaciones de ciberfinanzas, cibersalud y acceso a distancia de la empresa.

4 Abreviaturas y acrónimos

En esta Recomendación se utilizan las abreviaturas y acrónimos siguientes:

API Interfaz de programación de aplicaciones (*application programming interface*)

ATM Cajero automático (*automated teller machine*)

DLP Prevención de pérdida de datos (*data loss prevention*)

DNS Sistema de nombres de dominio (*domain name system*)

DSL Línea de abonado digital (*digital subscriber line*)

GSM Sistema mundial para comunicaciones móviles (*global system for mobile communications*)

HTTP Protocolo de transferencia de hipertexto (*hypertext transfer protocol*)

ID Identidad

IP Protocolo Internet (*internet protocol*)

IPS Sistema de prevención de la intrusión (*intrusion prevention system*)

IT Tecnología de la información (*information technology*)

MITM Ataque por intromisión (*man-in-the-middle*)

NAC Control de acceso a la red (*network access control*)

OS Sistema operativo (*operating system*)

PC Computadora personal (*personal computer*)

PSI Proveedor de servicios de Internet

PIN Número de identidad personal (*personal identity number*)

PS Proveedor de servicio

SMS Servicio de mensajes cortos (*short message service*)

SQL Lenguaje de consulta estructurado (*structured query language*)

SSL Capa de conexión segura (*secure socket layer*)

TIC Tecnología de la información y la comunicación

TAN Número de transacción (*transaction number*)

WiMAX Interoperabilidad mundial para acceso por microondas (*worldwide interoperability for microwave access*)

5 Convenios

La expresión "es necesario/requisito para" indica un requisito que debe cumplirse estrictamente y en relación con el que no está permitida desviación alguna si se declara la conformidad con esta Recomendación.

La expresión "se recomienda" indica un requisito recomendado pero [...] que no es un requerimiento absoluto. Por tanto, este tipo de requisito no es necesario cuando se declara la conformidad.

La expresión "está prohibido" indica un requisito que debe cumplirse estrictamente y en relación con el que no está permitida desviación alguna si se declara la conformidad con esta Recomendación.

La expresión "puede opcionalmente" indican un requisito opcional, que está permitido pero que no es una recomendación. El término no establece que la implementación del suministrador deba incluir una opción que pueda ser habilitada opcionalmente por el operador de red/proveedor de servicios. Significa que el suministrador puede ofrecer de forma opcional la característica en cuestión y aun así declarar la conformidad con esta Recomendación.

6 Aspectos generales de la detección y respuesta al fraude

6.1 Exposición del problema

En los servicios de aplicaciones basados en las telecomunicaciones, los ataques mediante software malicioso han sido responsables de ataques dirigidos a objetivos concretos en muchos tipos de empresas y de industrias verticales (por ejemplo, en el ámbito del cibertransporte, los ciberhospitales, y otros tipos de ciberindustrias). Dichos ataques se están convirtiendo en una preocupación importante y se realizan cada vez más a través de correos electrónicos que pretenden "peskar" datos de grupos específicos ("*spear-phishing*") a través de objetos infectados con software malicioso, como es el caso de anuncios sobre cuyos enlaces usuarios inexpertos hacen clic. Estos métodos han sido utilizados para infectar a numerosas organizaciones.

Las organizaciones de muchos sectores comerciales deben hacer frente a importantes riesgos derivados de la pérdida de datos, del acceso indebido a cuentas y de actividades transaccionales desde orígenes externos e internos. El software malicioso dirigido puede a menudo superar las protecciones de la tecnología existente y permitir un acceso ilícito a datos que no se detecta hasta transcurrido un plazo de tiempo largo y una vez que los datos han sido robados y extraídos de la organización ("exfiltración"). Normalmente, las pruebas de actividad maliciosa permanecen ocultas a simple vista y no se detectan por falta de capacidades de supervisión y por la incapacidad de discernir entre un patrón de actividad anormal de las aplicaciones y patrones de actividad normales del acceso a datos. Por ejemplo, los clientes de los bancos pueden desconocer que han sufrido un fraude hasta que ven en un extracto de su cuenta un cargo no confirmado o hasta que un acreedor les requiere un pago.

Los ataques que utilizan software malicioso contra clientes de entidades financieras y empleados de empresas causan un daño grave a la reputación y las finanzas de sus víctimas. Se están convirtiendo rápidamente en herramientas muy utilizadas para atacar a clientes y a cuentas corporativas y para el robo de información sensible o de fondos. Por tanto, salvo que los procesos de negocio y las organizaciones se estructuren adecuadamente para gestionar eficazmente la detección del fraude, pueden pasarse por alto alarmas y alertas importantes. Finalmente, los ataques basados en software malicioso pueden utilizarse para acceder a cuentas de usuarios, perpetrar fraude o robar activos gestionados desde un servidor.

6.2 Cometido de la gestión del fraude

Un sistema de gestión del fraude puede aplicarse a tres casos típicos de fraude:

- Detección de la toma de control de una cuenta, que por lo general ocurre cuando se roban las credenciales de un usuario o a través de software malicioso ("malware"). El software malicioso infecta las computadoras de una empresa no sólo a través de documentos adjuntos a correos electrónicos, sino también cuando se visita una página web infectada.
- Detección de un nuevo fraude sobre una cuenta que por lo general ocurre cuando se roban las credenciales de un usuario o a través de software malicioso.
- Detección del uso de una cuenta robada (u otro medio financiero), por ejemplo, una tarjeta de crédito robada, cuando se realiza una compra o se pretende actuar como un usuario normal.

Un sistema de gestión del fraude se utiliza por lo general contra uno o más casos de fraude, como la toma de control de una cuenta, la detección de fraude interno, la detección en tiempo real de fraude por el pago mediante tarjeta y el bloqueo de transacciones, y como sistema de gestión del fraude o de usos indebidos específicos de la empresa. En cada uno de esos escenarios, es esencial que la empresa que ofrece el servicio basado en transacciones verifique la legitimidad de las personas que las realizan.

6.3 Principales capacidades para la gestión del fraude

Para luchar de forma integral contra el fraude asociado a la identidad, el sistema de detección del fraude debe disponer de tres capacidades básicas: supervisión, detección y respuesta a incidentes. Estas capacidades incluyen los pasos que deben darse para, en primer lugar, detectar una actividad sospechosa a partir de datos de diversos eventos, tomar las acciones necesarias para detectar el fraude en una fase temprana del mismo y adoptar las medidas necesarias para resolver el fraude si se detectan actividades sospechosas.

Supervisión: un sistema de detección del fraude puede realizar la supervisión mediante la detección de anomalías en la actividad de los usuarios y en el comportamiento a nivel de la aplicación, del sistema, de la base de datos o de la red, y mediante la observación de lo que sucede en las cuentas y entre ellas utilizando cualquiera de los canales disponibles para el usuario. También se supervisa y analiza el comportamiento del usuario o de las cuentas y de las transacciones asociadas, e identifica comportamientos anómalos mediante la aplicación de reglas o modelos estadísticos. También pueden utilizarse (de forma óptima) perfiles de usuarios y de cuentas que se actualizan continuamente, así como grupos de pares de los mismos para comparar transacciones e identificar las que son sospechosas. En particular, el seguimiento integral del fraude interno requiere la supervisión de usuarios privilegiados de las tecnologías de la información capaces de modificar archivos y datos directamente, en lugar de utilizar aplicaciones de usuario prediseñadas.

Detección: un sistema de detección del fraude tiene la capacidad de recuperar, diseccionar y analizar grandes volúmenes de datos utilizando un cribado complejo de relaciones y de reglas definidas por la empresa para prevenir el fraude. Puede utilizarse para la detección del fraude de origen interno (empleados) y externo (clientes y socios). Para aplicar la capacidad de detección del fraude deben establecerse perfiles de diversas entidades como usuarios, cuentas, hogares, computadoras personales, terminales móviles y quioscos a fin de detectar un comportamiento transaccional anormal de alguna de ellas. La detección del fraude utiliza políticas basadas en reglas que, a su vez, se apoyan en el juicio y conocimiento humanos y/o en modelos matemáticos predictivos con el fin de cuantificar la probabilidad de fraude de una transacción dada.

Respuesta: después de detectar una actividad sospechosa, el sistema de gestión del fraude debe responder a la misma adoptando medidas precautorias tales como el bloqueo de cuentas o el intercambio de información. La utilización de tecnologías complementarias de supervisión y detección puede ayudar a las empresas a detectar de forma más adecuada actividades de usuarios sospechosos, reconocer patrones de acceso a los recursos inadecuados o la actividad fraudulenta de una cuenta, e investigar y responder a los incidentes con alertas en tiempo real, gestión de incidentes, bloqueo de cuentas o incluso interviniendo en la transacción. Por tanto, las organizaciones deben determinar la combinación de tecnologías de supervisión y análisis más apropiada para su nivel de riesgo, así como las capacidades para el soporte e implementación de la tecnología de seguridad.

7 Arquitectura del sistema de detección y respuesta al fraude

7.1 Funcionamiento y componentes

Las aplicaciones de las TIC pueden estar integradas con componentes de detección del fraude para soportar las capacidades más importantes de gestión del riesgo de fraude de una transacción desde un acceso de usuario a cualquier tipo de actividad. El funcionamiento del sistema de detección del fraude no debe ser transparente a los piratas informáticos ni a los usuarios, de tal forma que los primeros no puedan aprender las reglas del sistema y, en consecuencia, no se generen perjuicios a los usuarios legítimos. En el caso de transacciones de usuarios sospechosos, el sistema de detección del fraude repite su verificación en tiempo real para evaluar su legitimidad o bien las transacciones permanecen suspendidas durante el tiempo necesario para que el sistema de detección del fraude analice su legitimidad.

El sistema de detección del fraude está formado de varios componentes que procesan, almacenan y transfieren datos para detectar cualquier actividad anormal. El funcionamiento del sistema de detección del fraude, es decir, sus capacidades, se basa en el procesamiento de datos entre los componentes. Las operaciones y los componentes del sistema de detección del fraude se describen en detalle en la Figura 1. Idealmente, el sistema de detección del fraude comienza la supervisión de la sesión tras su registro de inicio. En consecuencia, el sistema de detección del fraude realiza las funciones de gestión del fraude, desde la capacidad de supervisión hasta la capacidad de respuesta, de la forma siguiente:

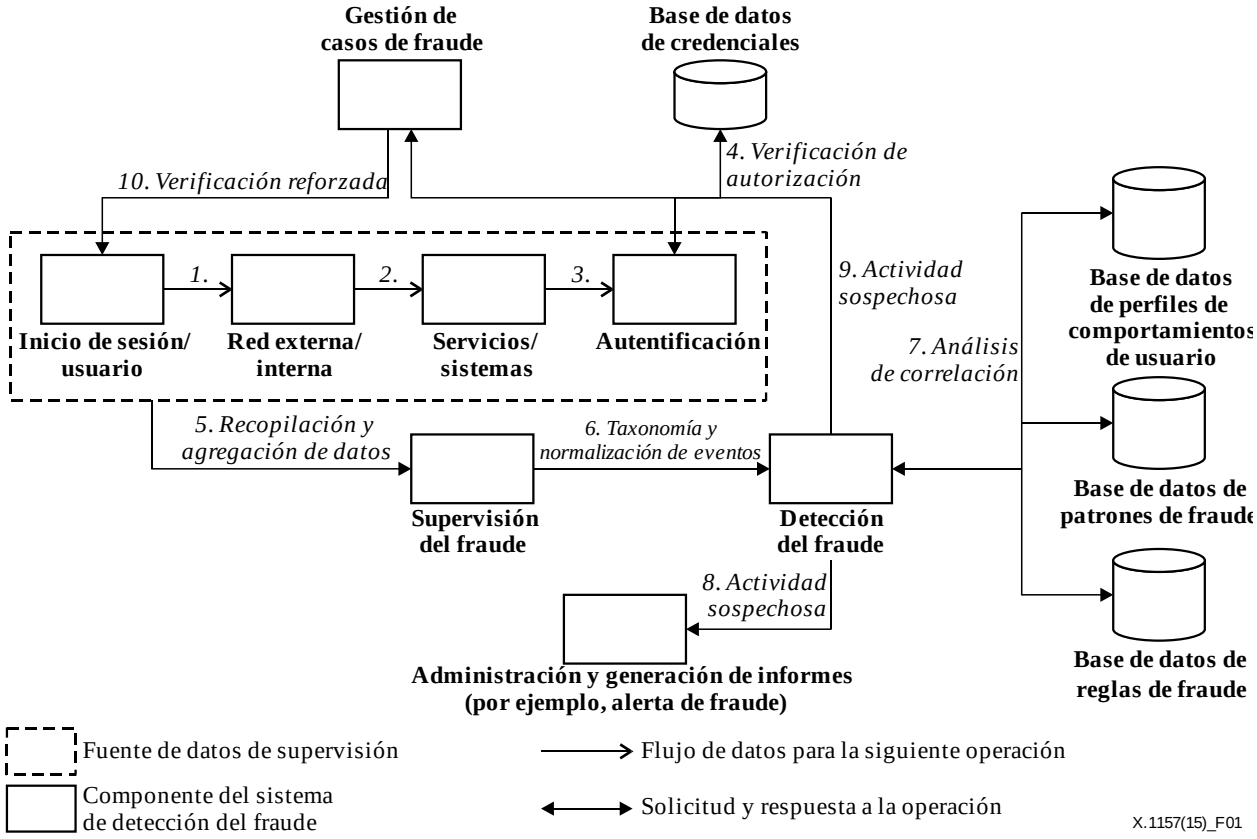

Figura 1 – Operaciones y componentes del sistema de detección del fraude

Operación de inicio de sesión, autentificación y autorización de verificación (flujos de datos 1, 2 y 3)

En circunstancias normales, se analiza el registro de inicio de sesión y se le asigna una puntuación de riesgo cuando se comparan las credenciales recopiladas durante el mismo con los datos que residen en la base de datos de credenciales de usuario (usuario y contraseña), el protocolo Internet (IP) y la base de datos de perfiles de comportamientos de usuario, etc. La autorización de verificación se rige por las normas de autentificación definidas en la base de datos de credenciales, que suele ser configurable por la institución y que es extensible para permitir nuevas reglas.

Operación de supervisión, detección y gestión de casos de fraude (flujos de datos 5, 6, 7, 9 y 10)

El sistema de detección del fraude recopila datos de diversas fuentes (a saber, redes, servicios/ sistemas, y autentificación) tras el inicio de sesión del usuario. El sistema de detección del fraude analiza los datos recogidos del componente de supervisión del fraude. Por ejemplo, si hay alguna actividad dudosa identificada por la autentificación, el sistema de detección del fraude envía la información sospechosa de fraude al componente de detección del fraude. A continuación, dicho componente envía una solicitud de consulta de datos para el análisis de correlación en las bases de datos relacionadas con el fraude (es decir, datos del perfil de comportamiento del usuario, datos de

patrones de fraude y datos de reglas de fraude). Los casos de fraude se priorizan en función del nivel de riesgo que refleja el componente de detección del fraude y muestran una imagen completa de los riesgos asociados a interacciones con puntación de alto riesgo. En caso de fraude con un alto nivel de riesgo, el componente de gestión del fraude solicita una verificación reforzada al componente de inicio de sesión del usuario. La resolución de casos puede y debe alimentar las bases de datos para reforzar un mecanismo de autoaprendizaje que mejore la calidad de la gestión futura.

Operación de administración y generación de informes (flujo de datos 8)

El componente de administración y generación de informes está a disposición de la institución para mejorar la comprensión y el control del sistema de detección del fraude. Este componente permite que los usuarios del sistema analicen e informen con facilidad sobre la calidad de funcionamiento del sistema, identificar la valoración e inconsistencias del acceso y las áreas de mejora, y realizar el seguimiento de las actuaciones de los usuarios del sistema y de la calidad de funcionamiento. Además, las herramientas de generación de informes son una manera sencilla de presentar información detallada sobre la calidad del servicio a gestores y analistas de alto nivel responsables del fraude.

7.2 Consideraciones sobre la arquitectura

La implementación de un sistema de detección del fraude para aplicaciones de las TIC puede utilizar una de las tres arquitecturas siguientes: Módulos de detección del fraude integrados en el servidor de aplicaciones (por ejemplo, en la web), escucha y/o supervisión de aplicaciones en línea e interfaces programáticas incluidas en aplicaciones preexistentes. Las reglas y los procesos de negocio son los aspectos determinantes más importantes para la eficacia de una aplicación.

Módulo de detección del fraude integrado en el servidor de aplicaciones

Las reglas de la empresa se aplican mediante el filtrado de todas las solicitudes realizadas a través del protocolo de transferencia de hipertexto (HTTP) (por ejemplo, el inicio de sesión o un pago) antes de que la transacción interactúe con la aplicación. Las transacciones pueden ser detenidas y/o redirigidas a una rutina de verificación de transacciones en tiempo real mediante la ejecución de las reglas antifraude del módulo. Varios vendedores ofrecen conectores ("plug-in") a servidores de aplicaciones que están integrados con un preprocesador.

Escucha y/o supervisión de la aplicación TIC (modo escucha)

En este modo, la aplicación escucha o "inspecciona" archivos de entrada o tráfico de red HTTP (por ejemplo, registros de inicio de sesión), o bien, lee datos utilizando conectores de servidores de aplicaciones instalados en cada servidor. Los datos se leen en tiempo real (enfoque de inspección de la red) o en tiempo casi real (enfoque de escucha del servidor de aplicaciones), o bien alimentan a otra aplicación de gestión del fraude o se reconstruyen con un formato al que pueden aplicarse las reglas de gestión del fraude. En este último caso, las transacciones sospechosas se ponen en cola para un análisis ulterior del fraude. Las interfaces de programación de aplicaciones (API) personalizadas pueden integrarse de forma que las transacciones sean redirigidas a una verificación del tipo impugnación/respuesta.

Interfaces programáticas en aplicaciones preexistentes (modo de integración en línea)

En este caso, las API se utilizan para que todas las transacciones pasen a través del sistema de detección del fraude antes de su procesamiento. Se controla el flujo de transacciones y puede impugnarse a un usuario en tiempo real si se detecta una transacción sospechosa. Los cambios en las reglas de negocio requieren modificar la aplicación principal. Las API se basan principalmente en servicios web. Además, las API hacen que sea más costoso sustituir la solución de un proveedor por la de otro.

En general, la utilización de APIs para la detección del fraude permite a empresas y organizaciones tener un control directo sobre el flujo de transacciones, pero requiere un importante trabajo de integración y deben actualizarse siempre que se modifique la aplicación principal. En el caso de servidores de aplicaciones que no requieran intervenir en tiempo real en las transacciones de usuario es preferible el segundo enfoque, que es la más fácil de retirar y sustituir.

8 Capacidades técnicas de detección y respuesta al fraude

8.1 Capacidades de supervisión

La capacidad de supervisión establece el contexto de usuario y de datos necesario para la detección precoz de ataques y de incumplimientos, y asimismo permite el acceso a los datos y el seguimiento de la actividad. La supervisión de los usuarios privilegiados y del acceso a datos sensibles es también un requisito común para la generación de informes sobre cumplimiento.

El sistema de detección del fraude tiene que aplicar la capacidad de información de seguridad y de gestión de eventos para lograr una supervisión de amplio alcance de la actividad del usuario y del acceso a los recursos a través de la red, sistemas, bases de datos y aplicaciones. El sistema de detección del fraude también tiene que enriquecer los datos relativos a los eventos con el contexto de los usuarios, activos, amenazas y vulnerabilidades a fin de mejorar la eficacia de la supervisión de la seguridad para la detección de incumplimientos. Además, necesita enriquecer selectivamente la supervisión de la seguridad con capacidades adicionales, tales como la supervisión de amenazas avanzadas basada en el nivel de riesgo y la capacidad de implementar y explotar eficazmente el sistema de detección y respuesta al fraude.

El sistema de detección del fraude también recopila datos de eventos en tiempo real para permitir su análisis inmediato. La capacidad de supervisión en tiempo real es importante para gestionar las amenazas con el fin de rastrear y analizar los avances de un ataque a través de los componentes y sistemas, y supervisar la actividad del usuario a fin de rastrear y analizar su actividad a través de las distintas aplicaciones, o con el objetivo de rastrear y analizar eventos de transacciones relacionadas o de acceso a datos. Por último, la capacidad de supervisión en tiempo real debe permitir la recopilación de datos por lotes cuando la recopilación en tiempo real no es práctica o necesaria.

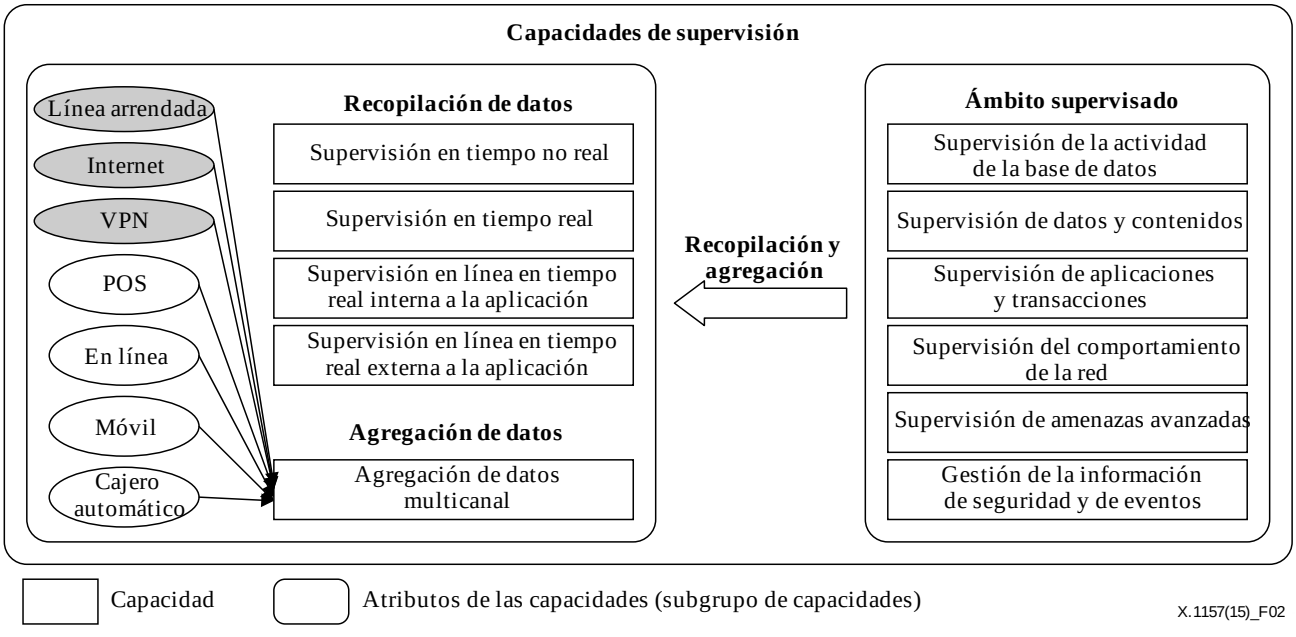

Figura 2 – Capacidades de supervisión del sistema de detección del fraude

8.1.1 Agregación y recopilación de datos

La agregación y recopilación de datos se realizan para una amplia variedad de fuentes de datos de registro, incluidos dispositivos de red y de seguridad, servidores, registros en bases de datos y en aplicaciones, resultados de las aplicaciones de seguridad, como la evaluación de la vulnerabilidad y los supervisores de la actividad de bases de datos, y resultados de las tecnologías de gestión de la identidad y del acceso, como directorios de empresas y sistemas de aprovisionamiento de usuarios y de gestión de accesos.

Supervisión en tiempo no real

La supervisión en tiempo no real requiere el examen manual o automático de los ficheros de registros de inicio de sesión. Puede proporcionar una alternativa de despliegue rápido para un análisis posterior a las transacciones con periodos de despacho más largos y puede prescindir de la capacidad de detener las transacciones en el momento de su compleción. Debe permitir la recopilación de datos por lotes cuando la recopilación en tiempo real no es práctica o necesaria.

Supervisión en tiempo real

La supervisión en tiempo real permite supervisar todas las transacciones (por ejemplo, HTTP) en tiempo real utilizando un filtro de servidor web. Esta función puede realizar la supervisión sin utilizar hardware adicional mediante un filtro de servidor web de bajo impacto. Para visualizar los datos de transacciones en tiempo real no son necesarios cambios en las aplicaciones.

Supervisión en línea en tiempo real interna a la aplicación

Permite supervisar todas las transacciones web HTTP en tiempo real mediante la integración en una aplicación interna. El despliegue y mantenimiento de esta función puede ser costoso y requerir un largo periodo de tiempo ya que son necesarias numerosas modificaciones en la aplicación para supervisar los puntos de transacción específicos.

Supervisión en línea en tiempo real externa a la aplicación

Permite supervisar todas las transacciones web HTTP en tiempo real mediante un filtro de la aplicación externa. Esta función no afecta a la aplicación para realizar los enfoques de inspección y filtrado web ya que el filtro de la aplicación externa está en línea con la aplicación, lo que puede introducir un cierto riesgo en la fiabilidad de la misma. Para visualizar datos de transacciones en tiempo real no son necesarios cambios en la aplicación.

Agregación de datos multicanal

En este caso, los datos de transacciones procedentes de otros canales pueden incorporarse completamente en los procesos de supervisión y de detección del fraude. Además, la agregación de datos multicanal trata de identificar comportamientos sospechosos de usuarios o de cuentas y, al mismo tiempo, tiene la ventaja de observar varios canales y productos y de correlacionar alertas y actividades de cada usuario, cuenta o entidad. La agregación de datos multicanal permite analizar las relaciones entre entidades internas y/o externas y sus atributos (por ejemplo, usuarios, cuentas, atributos de cuentas, máquinas y atributos de máquinas) para detectar actividades anormales o usos indebidos.

8.1.2 Fuentes de datos supervisadas

El sistema de detección del fraude puede detectar una actividad maliciosa en un flujo continuo de eventos discretos asociados por lo general a un usuario autorizado y que se generan en múltiples redes, sistemas y aplicaciones. Las capacidades de supervisión incluyen la integración con varios orígenes para detectar eventos sospechosos e incidentes.

Supervisión de la actividad de las bases de datos

La supervisión de la actividad de las bases de datos permite mantener la separación de obligaciones de usuarios con acceso privilegiado a la base de datos mediante la supervisión de la actividad del administrador. Esta capacidad también mejora la seguridad de la base de datos al detectar violaciones de la política y actividades inusuales. La agregación, correlación y generación de informes sobre eventos de la base de datos proporciona una capacidad de auditoría de la base de datos sin necesidad de funciones nativas de auditoría de bases de datos.

La capacidad permite identificar cambios en la estructura y el contenido de la base de datos así como en el acceso a datos de usuarios privilegiados a través de los registros de inicio de sesión a distancia o locales. Debido a que actúa en la capa de base de datos y de archivos, carece del contexto de cualquier acceso a la información y navegación no ligado a la base de datos o a archivos asociados. Los componentes de supervisión de red (en línea o fuera de banda) pueden utilizarse para supervisar consultas realizadas en lenguaje SQL (lenguaje estructurado de consultas) y el acceso administrativo desde la red.

Supervisión de datos y de contenidos

Las capacidades de supervisión y de contenidos se utilizan a menudo para limitar fugas de información, como números de tarjetas de crédito, información de identificación personal y propiedad intelectual basada en documentos y bases de datos, con funciones de apoyo a la supervisión, filtrado y prevención de pérdida de datos (DLP, *data loss prevention*) de contenidos. El propósito de esta capacidad es permitir que la empresa supervise sus contenidos internos para detectar actividades sospechosas. La supervisión y filtrado de contenidos se utilizan para proteger los contenidos en movimiento (mediante supervisión de red o filtrado), los contenidos en reposo (mediante la exploración del almacenamiento) y los contenidos en uso (mediante agentes que actúan en los puntos extremos). La mayoría de las funciones también incluyen capacidades para explorar el contenido almacenado en la red en busca de violaciones a la política (por ejemplo, la existencia de un número de tarjeta de crédito en un servidor no aprobado) y detectar violaciones de las políticas corporativas sobre el uso apropiado de datos y contenidos.

Las herramientas para la prevención de pérdida de datos (DLP) pueden descubrir, supervisar y bloquear activamente el movimiento o acceso a datos sensibles mediante la inspección de contenidos y técnicas de análisis contextual para aplicar una o más políticas cuando se utilicen. La prevención de pérdida de datos está limitada por la capacidad de una organización para definir el contenido sensible, sus estructuras u otras características identificativas.

Aunque estas funciones son muy útiles para limitar una exposición accidental o causada por procesos de negocio deficientes, hay muchas actividades no supervisadas (como teléfonos con cámara incorporada, correo de voz, papel y lápiz) que un atacante malicioso o alguien interno puede utilizar para eludir soluciones que tienen en cuenta el contenido.

Supervisión de la aplicación y las transacciones

La capacidad de supervisión de la aplicación y las transacciones incluye la supervisión de la aplicación dado que los ataques dirigidos explotan con frecuencia debilidades de la aplicación, y la actividad anormal de una aplicación puede ser la única señal de violación efectiva del sistema o de una actividad fraudulenta. La capacidad de analizar flujos de actividad de aplicaciones empaquetadas permite la supervisión a nivel de aplicación de esos componentes; además, la capacidad de definir y analizar flujos de actividades de aplicaciones personalizadas permite la supervisión a nivel de capa de aplicación de aplicaciones desarrolladas en la propia institución.

La capacidad de supervisión también trata de detectar la actividad de usuarios sospechosos en una aplicación sobre un canal de acceso dado (por ejemplo, web, teléfono o en persona, o a través de aplicaciones y de canales de acceso) o incluso organizaciones que comparten ente sí listas negras de direcciones IP. Abarca desde la detección de un acceso anormal (por ejemplo, el acceso simultáneo

a un dispositivo desde dos ubicaciones geográficas distintas) a una secuencia de transacciones sospechosas (por ejemplo, un cambio de una dirección seguida por una transferencia de dinero de alto valor). Por defecto, esta capacidad también puede detectar actividades no autorizadas de empleados en una aplicación supervisada por la aplicación de detección del fraude.

Supervisión del comportamiento de la red

Esta capacidad proporciona visibilidad de las operaciones en la red en base a flujos de tráfico entre sistemas, incluyendo origen, destino, puerto, protocolo, volumen de datos intercambiados e identidad del usuario. La capacidad puede aplicarse al análisis de la seguridad y de las operaciones conexas. Además, utiliza una combinación de firma y detección de anomalías para tener visibilidad sobre el estado de la red e identificar desviaciones respecto a las referencias que puedan reflejar comportamientos anormales o sospechosos. El propósito de esta capacidad es que la empresa pueda supervisar el comportamiento de su red interna para detectar actividades sospechosas.

Los casos de uso sobre la seguridad incluyen la supervisión para detectar la propagación de gusanos, la instalación no autorizada de aplicaciones y actividades sospechosas de acceso al sistema. Entre los casos de uso sobre el funcionamiento se encuentra la planificación de capacidades y el análisis del tráfico, incluyendo la capacidad de vincular una identidad de usuario (ID) al flujo de tráfico o aplicar requisitos de auditoría para rastrear el acceso de usuarios a sistemas críticos. La capacidad tiene poca visibilidad más allá de la capa 3, por lo que no pueden detectar directamente aspectos relacionados con el acceso al sistema, base de datos, contenidos, sistema de archivos u otros.

Supervisión de amenazas avanzadas

El software malicioso dirigido a objetivos concretos evita pasar a través de sistemas dotados de la actual generación de sistemas de prevención de intrusiones (IPS, *intrusion prevention systems*), cortafuegos de red y pasarelas de seguridad web. Algunos proveedores pequeños y especializados tienen productos de red para detectar amenazas avanzadas. Estas herramientas trabajan generalmente mediante el análisis de programas ejecutables para la detección de capacidades maliciosas (a menudo utilizando entornos virtuales), mediante la supervisión de las comunicaciones (incluyendo consultas a sistemas de nombres de dominio (DNS)) hacia y desde centros de mando y control conocidos o sospechosos por generar botnets, o una combinación de ambas técnicas. Las capacidades pueden identificar rápidamente el peligro potencial de una amenaza avanzada (por ejemplo, una amenaza persistente avanzada), aunque muchas de dichas capacidades están siendo actualmente añadidas a cortafuegos, sistemas de prevención de intrusiones (IPS) y pasarelas de seguridad web de próxima generación.

Otras funciones están especializadas en la detección de amenazas para la empresa desde el exterior, incluidas las "redes oscuras" (*darknet*), los canales de charla interactiva en Internet (IRC, *Internet relay chat*), las salas de charla, las redes sociales, etc. Estas funciones pueden realizarse mediante la detección de actividades dirigidas contra un dominio, un conjunto de direcciones IP o palabras clave.

Gestión de la información de seguridad y de eventos

Las capacidades de gestión de la información de seguridad de eventos tienen un amplio alcance que abarca la recopilación de eventos y la posibilidad de correlacionar eventos procedentes de fuentes de información dispares con el fin de conseguir la detección precoz de incumplimientos. Esta capacidad mejora la gestión de las amenazas y la respuesta a incidentes de seguridad gracias a la recopilación y análisis en tiempo real de eventos de seguridad procedentes de una amplia variedad de fuentes de datos. Dichas fuentes incluyen dispositivos de red y de seguridad, servidores, bases de datos y registros de inicio de sesión en las aplicaciones, los productos de aplicaciones pertinentes de seguridad, como los supervisores de la gestión de seguridad y de la actividad de las bases de datos, y los productos pertinentes de tecnologías de gestión de la identidad y del acceso, como los sistemas

de directorios empresariales, de aprovisionamiento de usuarios y de gestión de accesos. Además, esta capacidad permite supervisar el cumplimiento de la política de seguridad y la investigación de incidentes mediante el análisis y elaboración de informes sobre datos históricos de dichas fuentes.

Para la detección del fraude, la capacidad agrega y analiza datos de eventos producidos por dispositivos, sistemas y aplicaciones. La fuente de datos primaria son los datos de registro de inicio de sesión, pero la capacidad también puede procesar otros datos. Los datos se normalizan de manera que se puedan correlacionar y analizar eventos de distintas fuentes de acuerdo con un conjunto de reglas diseñadas para fines específicos, como la supervisión de eventos de seguridad de la red o la supervisión de la actividad de usuarios, ya que la supervisión y el análisis dependen completamente de los datos de eventos producidos por otras fuentes. Una actividad que no se externalice como un evento o en un registro de actividad, no es visible para esta capacidad.

8.2 Capacidades de detección

La detección del fraude utiliza procesos de fondo (es decir, transparentes para los usuarios) basados en servidores que examinan el acceso del usuario y su comportamiento. Esta información se compara con un perfil esperado que se considera "normal". Simultáneamente evalúa una combinación de factores de riesgo para detectar fraude real y mantener una tasa reducida de detecciones erróneas. Las transacciones de usuarios sospechosos se vuelven a verificar en tiempo real para evaluar su legitimidad o dejarlas en suspenso hasta que los analistas de fraude hayan investigado su legitimidad.

Dado que la detección del fraude funciona en el contexto de una aplicación, no puede detectar procesos falseados y potencialmente fraudulentos externos a la aplicación. La detección del fraude no puede identificar comportamientos sospechosos no incluidos en su motor de evaluación porque las reglas no incluyen el patrón de actividad detectado, el modelo no ha aprendido lo suficiente para identificarlo o la integración de la aplicación no proporciona suficientes datos relevantes para el motor de evaluación del riesgo de fraude. Para que la detección sea eficaz, el análisis debe incluir el conocimiento de casos de uso específicos, o bien, el cliente debe proporcionar esta información en forma de reglas de correlación e informes personalizados. Por tanto, el sistema de detección del fraude necesita capacidades como la actualización del patrón de fraude, una biblioteca de reglas predefinidas y el procesamiento en tiempo real de las reglas.

Con anterioridad a que las aplicaciones estén plenamente operativas, la mayoría de las capacidades requieren un amplio refinamiento de los modelos, un refinamiento del perfil o el desarrollo de reglas de detección. Estas capacidades incluyen la supervisión de todas las transacciones, el análisis y clasificación automática de riesgos, la creación y aprendizaje de perfiles de comportamiento del usuario, criterios de decisión sobre patrones de fraude específicos del servicio de la aplicación y patrones de fraude inteligentes, así como una evaluación de los riesgos debidos a conjunto de canales existentes.

Captura de transacciones

La captura de transacciones son capacidades que identifican y extraen atributos clave de las transacciones y que requieren la creación de perfiles detallados de comportamiento para cada usuario automáticamente cuando se produce el primer acceso.

Normalización y taxonomía de eventos

Los datos de los eventos deben normalizarse para poder correlacionar y analizar eventos de distintas fuentes de acuerdo con un conjunto de reglas diseñadas para fines específicos, como la supervisión de eventos de seguridad de la red o de eventos de la actividad del usuario. Ello supone establecer una correspondencia entre información procedente de fuentes heterogéneas y un esquema común de clasificación de eventos. La taxonomía ayuda al reconocimiento de patrones y a la mejora del alcance y estabilidad de las reglas de correlación. Cuando se normalizan eventos de fuentes heterogéneas, éstos pueden analizarse utilizando un menor número de reglas de correlación, lo que

simplifica las tareas de despliegue y apoyo. Además, para elaborar informes y cuadros de mando resulta más fácil trabajar con eventos normalizados.

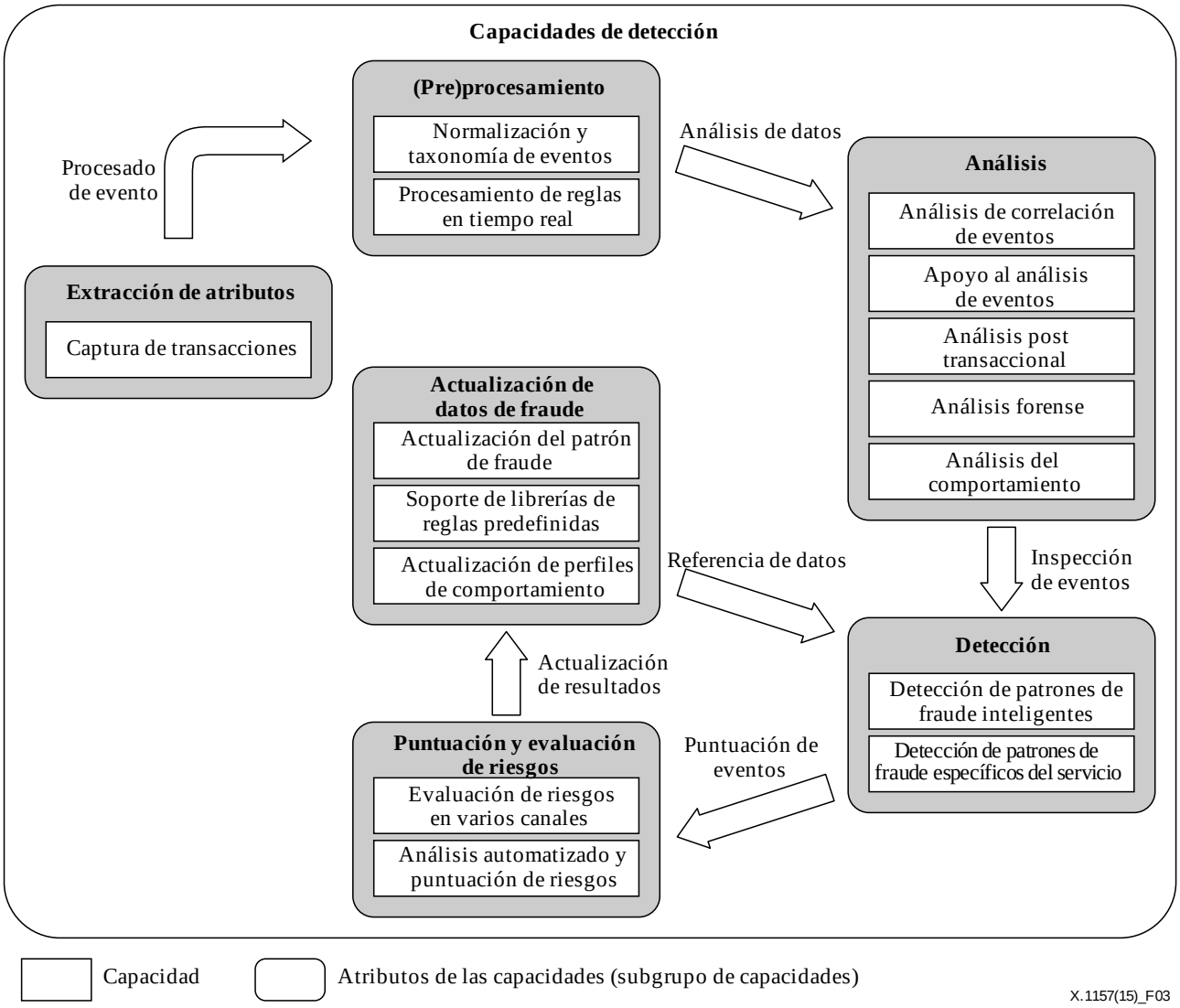

Figura 3 – Capacidades de detección del sistema de detección del fraude

Actualización del patrón de fraude

Esta capacidad permite la actualización automática de datos de incidentes de fraude de la red. Los datos de incidentes de fraude incluyen datos geográficos de la dirección IP para la localización del origen de cada transacción, incluyendo ciudad, país y proveedor de Internet, así como datos de reputación del computador anfitrión para identificar transacciones de fuentes sospechosas ya conocidas y datos del anonimizador para transacciones de alguien que trate de ocultar el punto de origen. La actualización del patrón del fraude debe poder aplicar el sistema de detección del fraude a otros casos de uso de fraude en la empresa y personalizarlo a fin de satisfacer requisitos de negocio específicos. Por ejemplo, el sistema de detección del fraude podría integrar los resultados de la detección del fraude externo, la puntuación de la confianza y los sistemas de información compartida, como por ejemplo, listas negras.

Para facilitar la actualización del patrón del fraude existe información sobre el contexto de la amenaza de interés en diversas fuentes, incluyendo listas de fuentes abiertas, contenidos sobre la amenaza y la reputación que desarrollan y mantienen equipos de investigación de proveedores de seguridad, y datos elaborados por proveedores de seguridad gestionada y de otros servicios. Los datos con información sobre la amenaza pueden integrarse en un sistema de detección del fraude en

forma de listas de vigilancia, reglas de correlación y consultas, de manera que aumente la tasa de éxito de la detección precoz de incumplimientos.

La información actualizada sobre amenazas y patrones de ataque puede ayudar a una organización a reconocer actividades anormales. Por ejemplo, una actividad reducida dirigida a una dirección IP externa puede parecer normal y pasar desapercibida fácilmente. Sin embargo, todo cambia si existe un sistema de información de amenazas que indique que el destino está asociado con el control de botnets. Esta información puede compararse con los algoritmos de aprendizaje de las máquinas sobre comportamientos esperados o con normas más genéricas sobre lo que es un comportamiento "normal" a fin de detectar el fraude.

Soporte de librerías de reglas predefinidas

Esta función indica que el sistema de detección del fraude soporta reglas previamente probadas y que están disponibles para luchar contra el fraude. Por lo general, esta función del sistema de detección del fraude incluye el despliegue de reglas probadas y también debe permitir la creación/modificación de nuevas reglas de forma sencilla. Además, esta función puede incluir la posibilidad de compartir reglas con otras organizaciones. Permite que el sistema de detección del fraude actualice de forma rápida las reglas de prueba así como nuevos escenarios de fraude y observar y analizar fácilmente datos y resultados de la detección del fraude. También puede incluir un conjunto específico de reglas para la gestión del fraude o del uso indebido a nivel de cliente, a nivel de grupo de clientes o de cualquier otro usuario.

La mayoría de los sistemas de detección del fraude asociado a tarjetas de crédito permiten a las empresas gestionar las reglas de negocio que determinan cómo se ejecutan sus transacciones, por lo que cada empresa puede identificar patrones de fraude específicos.

Esta biblioteca de reglas puede definir un conjunto de reglas basadas en información de seguridad e información contextual:

- contexto de usuario: funciones de negocio de un usuario;
- contexto de activos: propiedad, aplicaciones conexas o procesos de negocio;
- contexto de seguridad de la información: vulnerabilidades del sistema operativo, la situación de la aplicación, la capa web o la base de datos y la configuración;
- contexto de amenaza externa: agentes maliciosos conocidos y patrones de ataque;
- contexto de datos: criticidad para el negocio o requisitos jurídicos y regulatorios;
- contexto de aplicación: uso de la aplicación en el negocio y límites del acceso normal a los datos.

Análisis de la correlación de eventos

La correlación de eventos establece relaciones entre mensajes o eventos generados por dispositivos, sistemas o aplicaciones, en base a características como origen, destino y protocolo o tipo de evento. También debe existir una biblioteca de reglas de correlación predefinidas y la posibilidad de personalizar fácilmente dichas reglas. A partir del análisis de la correlación de eventos, una consola de eventos de seguridad debe presentar en tiempo real incidentes y eventos relacionados con la seguridad.

Soporte de la analítica de eventos

La analítica de eventos se realiza mediante la correlación de eventos en tiempo real y el análisis en base a consultas de eventos históricos. La analítica de eventos de seguridad se compone de vistas de un panel de control, informes y funciones de consulta ad hoc para la investigación de la actividad del usuario y del acceso a recursos a fin de identificar una amenaza, un incumplimiento o un uso indebido de los derechos de acceso. Cuando una actividad sospechosa se pone de manifiesto gracias a la supervisión de seguridad o a los informes de actividad, es importante poder analizar el acceso

del usuario y el acceso a los recursos. El proceso puede aplicar un enfoque iterativo que empiece con una consulta amplia sobre la fuente, usuario o destino de un evento y, a continuación, realizar una serie de consultas cada vez más enfocadas para identificar la causa del problema. La analítica de eventos utiliza funciones de análisis del comportamiento para lograr una mayor correlación basada en reglas.

Procesamiento de reglas en tiempo real

Esta función permite el procesamiento en tiempo real de las reglas de fraude respecto a la corriente de transacciones para generar puntuaciones del riesgo del usuario/sesión y alertas detalladas de incidentes. Debe tener en cuenta comportamientos inusuales de usuarios, patrones de fraude comunes, listas negras y blancas y datos de incidentes de fraude. Puede soportar sintaxis de normas como el comportamiento inusual de un usuario con períodos de gracia, ID de dispositivos de cliente, patrones de fraude comunes, listas negras/blancas, datos geográficos de direcciones IP y datos de reputación del anfitrión. Además, el sistema de detección del fraude permite calcular una puntuación asociada al riesgo de cada sesión y una puntuación acumulada del riesgo de cada usuario; también puede permitir una autentificación basada en el riesgo al proporcionar en tiempo real al sistema de autentificación las puntuaciones de riesgo del usuario y de la sesión para determinar si es necesaria una autentificación adicional.

Soporte de la herramienta de gestión

Esta función permite el almacenamiento y análisis económico de grandes volúmenes de información, incluida la recopilación, indexación y almacenamiento de todos los datos de registro y de eventos de cualquier origen, así como la capacidad de búsqueda e información sobre los datos. Las capacidades de generación de informes también deben incluir informes predefinidos y la definición de informes ad hoc o la utilización de herramientas de terceros para la generación de informes. La función de la herramienta de gestión incluye por lo general informes predefinidos y modificables sobre la actividad de los usuarios, informes sobre el acceso a los recursos y sobre modelos para fines de gestión específicos y recurrentes. Por lo general, la herramienta de gestión está disponible a través de la web y soporta la asignación y flujos de trabajo de casos, incluyendo vistas de usuarios específicos, tales como una situación conocida de incidente de fraude, actividades en curso y nuevos elementos marcados, así como mecanismos de alerta configurables, incluidas las notificaciones mediante correo electrónico y servicios web.

Análisis posterior a la transacción

Es la capacidad de capturar y almacenar todos los elementos de datos para un análisis ulterior. El almacén de datos contiene finalmente un historial completo de las transacciones de todos los usuarios durante un periodo de tiempo. Esta función requiere la captura y el formateo sofisticados de los datos para su almacenamiento en tiempo real y su recuperación y evaluación rápida. El sistema de detección del fraude utiliza el perfil de comportamiento de cada usuario para un análisis posterior a la transacción y puede tener la capacidad de almacenar transacciones clasificadas según la sesión, el usuario y el sello de tiempo para su posterior recuperación y análisis.

Análisis forense

Esta función permite buscar, filtrar y profundizar en los detalles del almacenamiento de datos de las transacciones. Incluye la capacidad de filtrado, búsqueda, y análisis detallado de las transacciones y los patrones de acceso. También permite la identificación de patrones de fraude emergentes que justifican la utilización de reglas de detección en tiempo real.

Análisis del comportamiento

El sistema de detección del fraude requiere transacciones con perfiles de comportamiento aplicables a todos los usuarios y el soporte de sistemas más sofisticados para el seguimiento del comportamiento de cada usuario. Mediante una función de análisis del comportamiento, el sistema

construye un perfil de actividad normal y alerta de las desviaciones que puedan producirse. La creación de perfiles de comportamiento consta de una fase de aprendizaje que crea perfiles de actividad normal para fuentes discretas de eventos recopilados mediante las capacidades de supervisión.

El sistema de detección del fraude inicia automáticamente la creación del perfil de un usuario en la primera ocasión en la que lo detecta. El sistema puede construir entonces un perfil de lo considerado como comportamiento "normal" del usuario y comprobar posteriormente si se producen comportamientos "inusuales". La fase de detección alerta de las desviaciones respecto a la conducta normal. Cuando están bien definidas las condiciones anormales, es posible definir reglas de correlación para identificar un conjunto específico de condiciones. La capacidad debe detectar, seguir, traducir y comprender automáticamente patrones y anomalías que puedan ser perjudiciales y, sin embargo, no interrumpir la experiencia de un cliente legítimo. Por último, la creación de perfiles de comportamiento puede permitir la toma de decisiones sobre el riesgo en base a desviaciones con respecto al comportamiento normal.

Tras la creación inicial del perfil, el sistema necesita más tiempo para aprender lo que es un comportamiento anormal o para que las empresas implementen normas para detectar un comportamiento o una sesión anormal. Este enfoque puede mejorar la capacidad de descubrir un ataque dirigido, pero todavía requiere un extenso refinamiento realizado por expertos a fin de controlar falsos positivos.

Detección de patrones de fraude inteligentes

No todos los fraudes pueden detectarse a través de registros de inicio de sesión en la red y en las aplicaciones y campos de datos discretos. El análisis de datos no estructurados debe incluirse mediante lógicas de minería de datos que evalúen la idoneidad de la información introducida.

Las empresas deben identificar lógicas de minería de datos que aprendan por sí mismas, con un mínimo de datos, así como sistemas en los que puedan actualizarse de forma fácil y rápida reglas aplicables a parámetros de fraude conocidos o recién descubiertos. Ello permite verificar una nueva identidad de usuario en línea con respecto a un servicio de puntuación de la identidad proporcionado por proveedores de sistemas de puntuación de la identidad. Estas puntuaciones estiman la probabilidad de que un usuario en línea sea un defraudador.

Detección de patrones de fraude específicos del servicio

Un sistema de detección del fraude requiere la capacidad de definir reglas que busquen patrones de transacciones que se correspondan con patrones de fraude conocidos y patrones de fraude específicos del servicio. En otras palabras, el sistema busca secuencias específicas de transacciones y condiciones sospechosas de acuerdo con la lógica del negocio o la actividad del servicio de la aplicación. Este patrón podría presentarse en una única sesión o extenderse a lo largo de varias sesiones y para varios usuarios de acuerdo con el servicio de aplicación específico.

Por último, si el servicio no ha sido refinado adecuadamente, los sistemas de detección del fraude pueden generar demasiados falsos positivos. En entornos como el comercio electrónico, donde la ejecución en tiempo real es imprescindible, una elevada tasa de falsos positivos es claramente inaceptable.

Evaluación del riesgo en varios canales

Los sistemas de detección del fraude sólo funcionan para una aplicación determinada y un canal dado, y no se aplican a varios canales (por ejemplo, teléfono, web o en persona) o a varios tipos de cuentas (por ejemplo, depósito o cuenta de crédito). Además, los sistemas de detección del fraude desconocen todo sobre actividades fraudulentas fuera de la aplicación, y no están integrados en sistemas que conozcan dicha actividad (por ejemplo, detección del fraude basada en la red y basada en los sistemas). Por tanto, no pueden detectar procesos falseados y potencialmente fraudulentos externos a la aplicación.

En consecuencia, la detección del fraude requiere observar alguna actividad sospechosa del usuario en una aplicación y sobre un canal de acceso dado (por ejemplo, web, teléfono o en persona), o en distintas aplicaciones, canales de acceso o incluso organizaciones (por ejemplo, donde las organizaciones comparten una "lista negra" de direcciones IP). Ello abarca desde la detección de un acceso anormal (por ejemplo, el acceso simultáneo de un dispositivo desde dos ubicaciones geográficas) hasta una secuencia de transacciones sospechosas (por ejemplo, un cambio de la dirección seguida por una transferencia de una gran cantidad de dinero).

Para detectar fraudes adicionales, el sistema de detección del fraude debe integrar las puntuaciones de los módulos de detección del fraude en módulos de puntuación de riesgos de varios canales que observan dichos canales de usuario (por ejemplo, centros de llamadas o cajeros automáticos).

Análisis y clasificación automática del riesgo

Esta función requiere la capacidad de valorar, evaluar y clasificar automáticamente los riesgos de la seguridad. La detección del fraude y la puntuación del riesgo de una transacción están regidos por modelos o reglas, o por una combinación de ambos. Para encontrar alguna actividad sospechosa en un conjunto de datos recopilados pueden utilizarse diversas técnicas de modelado como la bayesiana, las redes neuronales y otras tecnologías de minería de datos que necesitan datos para calcular las probabilidades de fraude.

Las redes neuronales, que funcionan bien en el espacio actual de tarjetas de crédito, no funcionan sin embargo adecuadamente en el espacio de Internet, ya que necesitan grandes cantidades de datos para detectar patrones fraudulentos. Por tanto, en el caso de transacciones en la web el sistema de detección del fraude utiliza técnicas de modelado alternativos, como la bayesiana, que necesita un menor volumen de datos para calcular las probabilidades de fraude, o bien, exclusivamente la detección basada en reglas. Los modelos de detección del fraude puntúan el riesgo con valores que pueden introducirse en los conjuntos de reglas de la aplicación y ser mantenidas y actualizadas por la empresa/organización.

8.3 Capacidades de respuesta

El sistema de detección del fraude requiere la generación automática de alertas de fraude, el bloqueo de cuentas y la verificación reforzada del solicitante de cualquier transacción considerada sospechosa para aplicar la capacidad de respuesta a incidentes. Todas las aplicaciones de cuentas en línea y todas las transacciones anónimas de alto riesgo deben someterse a un conjunto de procedimientos iniciales de cribado que comienzan con eventos de autenticación resultado del procedimiento inicial de demostración de identidad aplicado a la utilización de la aplicación y a los registros de inicio de sesión de la aplicación. El procedimiento inicial de cribado incluye actividades básicas de detección del fraude, como la identificación de dispositivos de cliente y la verificación de datos básicos de la identidad como nombre, dirección de correo electrónico, análisis de geolocalización, validación del número telefónico, detección del fraude de tarjetas de crédito, validación del informe de la oficina de créditos y/o la puntuación de la identidad.

Las transacciones sospechosas que no superan las etapas iniciales de demostración de identidad deben enviarse a un equipo de investigación del fraude para un cribado adicional manual o automático. Para el cribado adicional, el sistema de detección del fraude puede utilizar un enfoque basado en el riesgo y la demostración de la identidad por capas que refuerce el análisis de identidad si aparecen usuarios sospechosos y transacciones de alto riesgo.

Verificación reforzada del solicitante

El sistema de detección del fraude puede integrar el mecanismo de autentificación de forma que la puntuación de riesgo del sistema de fraude determine la fortaleza de la autentificación del usuario o la verificación de las transacciones del usuario. Incluye los pasos necesarios para descartar transacciones sospechosas u otras transacciones de alto riesgo que requieran demostración de la identidad. Con el fin de minimizar los costos y maximizar la comodidad del cliente, las empresas

pueden adoptar un enfoque basado en el riesgo, en el que la fortaleza de la verificación de la identidad es proporcional al riesgo de la transacción. A tal fin, el sistema de detección del fraude puede utilizar aplicaciones de demostración de múltiples identidades combinadas que se describen en [b-ITU-T X.1154].

En general, no existe en el mercado una aplicación de demostración de identidad que abarque por sí misma todos los casos. No obstante, hay comercialmente disponibles mecanismos de demostración de identidad que pueden combinarse para constituir una medida de disuasión eficaz frente a defraudadores.

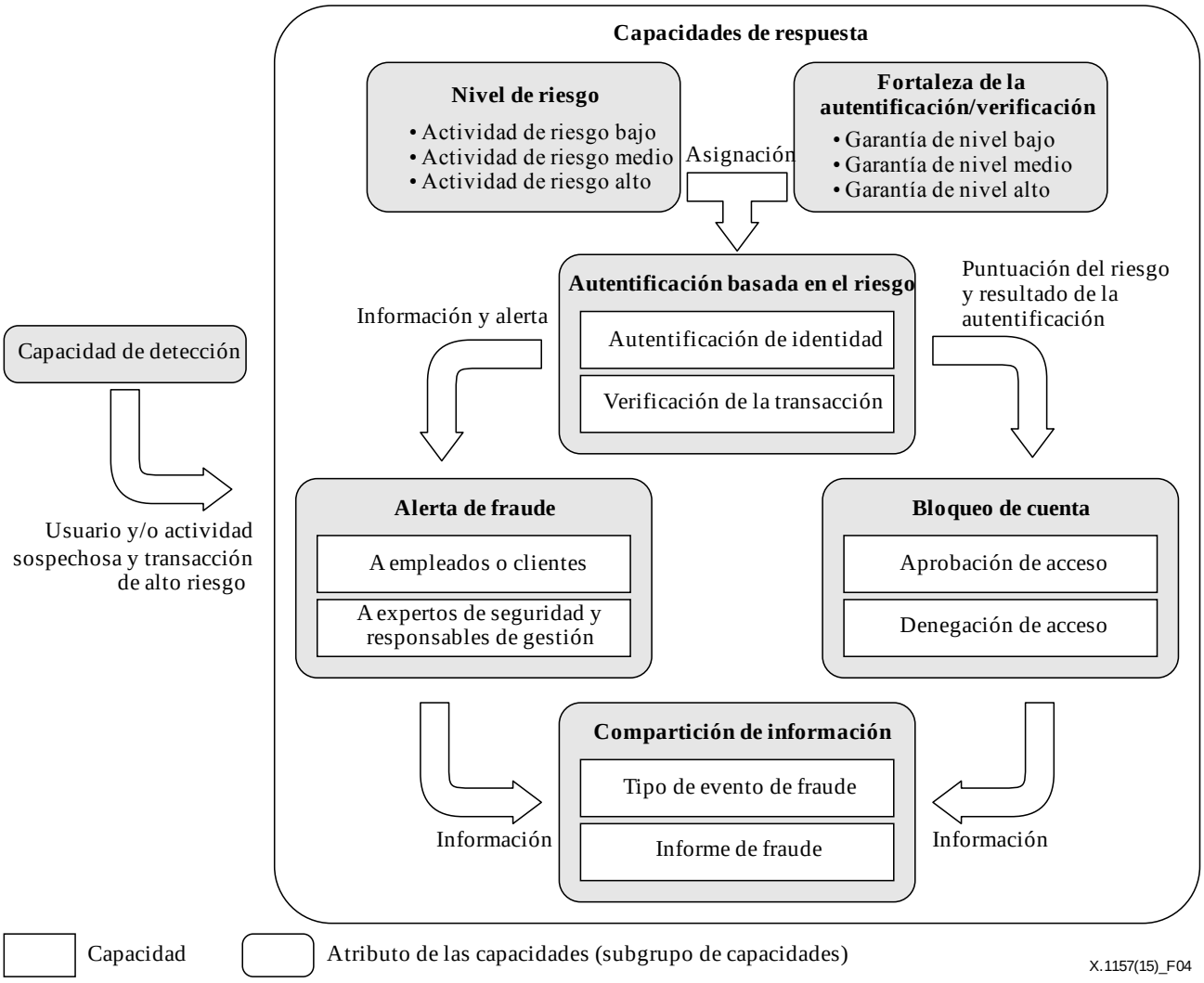

Figura 4 – Capacidades de respuesta del sistema de detección del fraude

Autentificación basada en el riesgo

Cuanto mayor sea el riesgo que determine, por ejemplo, un sistema de detección del fraude, mayores serán el coste y las molestias para el cliente de las medidas de demostración de identidad necesarias. Para los casos en los que sea necesaria una autentificación más robusta existen varios enfoques posibles, como por ejemplo:

- El acceso inicial a la cuenta se configura para permitir una actividad de bajo riesgo, como el acceso de sólo lectura a información pública que requiere una demostración de identidad muy básica. Por ejemplo, el mecanismo de demostración de identidad puede comprobar el nombre y correo electrónico del usuario por comparación con una fuente secundaria.

- Una actividad de mayor riesgo, como la actualización de una dirección de correo, se pospone hasta que se haga una demostración de identidad más robusta (ver [b-ITU-T X.1254]), junto con la detección del fraude. Esto incluye una autentificación con un nivel de garantía más elevado:
  - el mecanismo de demostración de identidad puede verificar la información personal con respecto a una base de datos pública mediante autenticación basada en el conocimiento. Esta verificación combina información disponible públicamente, como datos demográficos, de permisos de conducción de automóviles y de oficinas de riesgo;
  - el mecanismo de demostración de identidad puede requerir que el usuario responda a una o más preguntas complejas que han sido contestadas previamente y se han almacenados en el perfil de usuario o están basadas en información que el titular genuino de la cuenta debería conocer;
  - el mecanismo de demostración de identidad puede utilizar métodos de autentificación por canales alternativos, como el teléfono móvil o el correo electrónico, para contactar con el titular de la cuenta. El mecanismo de demostración de identidad puede enviar una contraseña de un solo uso al usuario en línea a través de una llamada de voz o un mensaje SMS dirigido a un número de teléfono registrado en la empresa o que el usuario introdujo en su solicitud de nueva cuenta o en la página de pago.
- Las actividades de mayor riesgo, como las transferencias de dinero a una cuenta bancaria externa vinculada, permanecen prohibidas hasta que se haya establecido contacto de validación con el usuario; sin embargo, debido a que muchas transacciones se ejecutan en modo por lotes (en lugar de en tiempo real), este enfoque puede no alterar el momento de ejecución de la transacción.

Alertas de fraude

Consiste en la generación automática o manual de alertas cuando se detecta una actividad sospechosa. La alerta de fraude suele ser el resultado de combinar la puntuación del riesgo y algunas reglas que actúan en función de dicha puntuación. Las alertas con información detallada incluyen atributos de la transacción y una descripción de la actividad y pueden notificarse por correo electrónico o radiobúsqueda configurable por una regla, indicando la gravedad de la transacción y el usuario de administración. Las alertas de fraude pueden enviarse a un experto en seguridad o a un cliente/usuario de acuerdo con el nivel de riesgo medido. El experto en seguridad puede entonces investigar el riesgo percibido con más detalle, mientras que la alerta de fraude enviada al cliente/usuario puede utilizarse para alertar a los prestatarios potenciales de que su identidad ha podido ser robada.

Bloqueo de una cuenta

El bloqueo de cuentas de usuario se aplica cuando se detecta alguna actividad sospechosa. El acceso del usuario puede ser autorizado o denegado en base a la puntuación asignada y los límites de tolerancia de la institución. Los usuarios que no reciben una puntuación adecuada para garantizar un acceso total, pueden recibir un permiso de acceso limitado o estar obligados a proporcionar una autentificación más robusta para tener acceso total, o bien, se les puede permitir algunas transacciones de alto riesgo. Si los usuarios no cumplen estos requisitos, pueden volver a iniciar el procedimiento de verificación reforzado o, en caso contrario, quedan bloqueados de inmediato.

Intercambio de información

Los sistemas de detección del fraude deben garantizar que los sistemas coordinan de manera efectiva parte de sus actividades de respuesta a incidentes con los miembros adecuados de la organización.

El aspecto más importante de la coordinación de la respuesta a incidentes es el intercambio de información, que permite que varias organizaciones compartan información sobre amenazas, ataques y vulnerabilidades para beneficiarse del conocimiento colectivo. Además, el intercambio de información puede tener lugar directamente entre la empresa y sus clientes o entre la organización y sus empleados ya que las mismas amenazas y ataques a menudo afectan de forma simultánea a múltiples organizaciones o servicios. El propósito del intercambio de información es que cualquier organización que haya detectado un fraude comparta dicha información, ya sea internamente o con otras organizaciones que son potenciales víctimas.

La organización receptora puede utilizar esta información, por ejemplo, para implantar una revisión manual de las transacciones iniciadas desde direcciones IP sospechosas. El informe del fraude puede calificar una transacción concreta como fraudulenta, o que potencialmente fraudulenta, o bien puede describir un patrón de comportamiento considerado indicativo de fraude.

Apéndice I

Servicios de aplicaciones TIC sensibles

(Este apéndice no forma parte integrante de esta Recomendación.)

I.1 Servicios financieros digitales

I.1.1 Banca electrónica y aspectos de seguridad

La banca en línea (o banca por Internet o banca electrónica) permite a los clientes de una institución financiera realizar transacciones financieras en un sitio web seguro operado por la institución, que puede ser un banco minorista o un banco virtual, una cooperativa de crédito o una sociedad de crédito hipotecario. Para acceder a las instalaciones de banca en línea de una institución financiera, un cliente con acceso personal a través de Internet debe registrase en la institución para el servicio y crear una contraseña (con nombres que pueden variar) para la verificación del cliente. Para acceder a la banca en línea, el cliente debe ir a la página web de la entidad financiera y entrar en el servicio de banca en línea utilizando su nombre y contraseña. Algunas instituciones financieras han establecido medidas de seguridad adicionales para el acceso, pero en general el enfoque adoptado por distintas instituciones suele ser diferente.

Aunque todavía se utiliza la autenticación mediante una contraseña única, se trata de un mecanismo que algunos países no consideran suficientemente seguro para la banca en línea. Existen dos métodos diferentes de seguridad en el uso de la banca en línea:

- El sistema basado en un número de identificación personal/número de autentificación de transacción (PIN/TAN), donde el número de identificación personal (PIN) es una contraseña utilizada para el inicio de sesión y el número de transacción (TAN) es una contraseña de un solo uso para autenticar transacciones. Los TAN pueden distribuirse de diferentes maneras; la más común es enviar al usuario de la banca en línea una lista de TAN en una tarjeta. La manera más segura de usar un TAN es generarlo mediante un testigo de seguridad. Los TAN generados mediante testigo varían con el tiempo y constituyen un valor secreto único que se almacena en el testigo de seguridad (autenticación mediante dos factores). La banca en línea con PIN/TAN se utiliza por lo general cuando se usa un navegador web con conexiones seguras mediante capa de conexión segura (SSL), por lo que no es necesario un cifrado adicional.
- Otra manera de proporcionar los TAN a un usuario de la banca en línea es enviar el TAN de cada transacción bancaria al teléfono móvil GSM del usuario mediante un mensaje SMS. El texto SMS generalmente cita el monto de la transacción y los detalles; el TAN sólo es válido durante un breve período de tiempo. Bancos de muchos países han adoptado el servicio "SMS TAN", por ejemplo en Alemania, Austria y los Países Bajos, ya que se considera un procedimiento muy seguro.
- Banca en línea basada en la firma electrónica, con todas las transacciones firmadas y cifradas digitalmente. Las claves para la generación de la firma y el cifrado se pueden almacenar en tarjetas inteligentes o en cualquier medio de almacenamiento, en función de cada aplicación concreta.

I.1.2 Pagos electrónicos y aspectos de seguridad

El pago electrónico es el intercambio electrónico o transferencia de dinero entre dos cuentas de una misma o distintas instituciones financieras a través de sistemas informáticos.

Un sistema de pago electrónico no seguro puede no ofrecer confianza a sus potenciales usuarios. La confianza es muy importante para asegurar la aceptación de los usuarios. Las aplicaciones de pago electrónico constituyen un desafío para la seguridad, por su elevada dependencia de sistemas TIC críticos, lo que crea vulnerabilidades en las instituciones financieras y empresas, y potencialmente puede perjudicar a los clientes. Una transacción financiera electrónica segura tiene que cumplir con los requisitos siguientes:

- Integridad y autorización: la integridad se define como la precisión, completitud y validez de la información de acuerdo con valores y expectativas empresariales. La integridad del sistema de pago significa que no se toma dinero de un usuario salvo que el pago esté autorizado por el mismo. Además, los usuarios pueden requerir a una institución financiera que no les remita ningún pago sin su consentimiento explícito.
- Confidencialidad: la confidencialidad se define como la protección frente a una divulgación no autorizada de información sensible o privada. Algunas de las partes involucradas pueden desear la confidencialidad de las transacciones. La confidencialidad en este contexto significa la restricción del conocimiento sobre diversas partes de la información relacionada con una transacción, como la identidad del pagador/beneficiario, el contenido de la compra, la cantidad pagada, etc. En la mayoría de los casos, los participantes involucrados desean garantizar la privacidad de las comunicaciones.
- Disponibilidad y fiabilidad: la disponibilidad tiene por objetivo asegurar que los sistemas de información y los datos están listos para su uso cuando se necesitan. Esto a menudo se expresa como el porcentaje de tiempo en el que un sistema puede utilizarse satisfactoriamente. Todas las partes exigen tener la posibilidad de realizar o recibir pagos siempre que sea necesario.

I.2 Servicios de cibersalud

Los cuidados sanitarios electrónicos, o cibersalud, aplicados a la gestión sin papeles de las actividades de grandes establecimientos sanitarios constituyen una actividad muy prometedora para acelerar las tareas burocráticas de la asistencia sanitaria en centros médicos y hospitales. No obstante, una adecuada implementación de la cibersalud debe hacer frente a numerosos aspectos relacionados con la seguridad. Para la adopción generalizada de la cibersalud en los hospitales es esencial llevar a cabo una evaluación detallada de los aspectos de seguridad a fin de sentar las bases de la normalización de sus diversos componentes para una implementación adecuada. Un típico sistema de cibersalud puede constar de numerosos componentes y subsistemas, tales como un sistema de programación de tareas y citas; de admisión, descarga y transferencia; de entrada de prescripciones; de planificación dietética; de notas clínicas de rutina; de órdenes de laboratorio y radiología; de archivo de imágenes, y de firma con tarjeta inteligente. Cada uno de estos subsistemas es vulnerable a amenazas de seguridad.

I.2.1 Aspectos de seguridad de los servicios de cibersalud

- Amenazas a la privacidad y seguridad de la información: la base de conocimiento existente sobre riesgos de seguridad de la información identifica diferentes tipos de amenazas a la privacidad y la seguridad de la información sobre la salud. No obstante, la actual taxonomía ad hoc puede no ser útil en la práctica;
- Preocupaciones sobre la privacidad entre usuarios de cuidados sanitarios: con la creciente dependencia de sistemas basados en la web para la gestión de información sobre la salud y la proliferación de bancos de datos de salud personal, la preocupación sobre la privacidad de los usuarios de la sanidad ha pasado a un primer plano;
- Interoperabilidad de datos y seguridad de la información: la premisa básica de la interoperabilidad de los datos es facilitar un intercambio de datos preciso y sin solución de continuidad dentro de una organización y entre organizaciones para lograr una asistencia sanitaria oportuna;

- Aspectos de seguridad de la información sobre cibersalud: el uso de dispositivos móviles y de aplicaciones basadas en la web ha experimentado un crecimiento significativo en el sector de la salud. Actualmente, la investigación sobre la seguridad de la información está centrada en el desarrollo de marcos y protocolos para abordar los problemas de seguridad en el ámbito de la cibersalud.

I.3 Servicios de acceso a distancia en la empresa

Empleados y contratistas de numerosas organizaciones utilizan tecnologías de acceso a distancia a fin de realizar su trabajo para la empresa desde ubicaciones externas. La mayoría de los teletrabajadores utilizan tecnologías de acceso a distancia para interactuar con recursos informáticos no públicos de la empresa. La naturaleza de las tecnologías de acceso a distancia en la empresa, que permiten el acceso a recursos protegidos desde redes externas y a menudo también desde anfitriones externos, pone a dichos elementos en una situación de riesgo mayor que tecnologías similares accesibles sólo desde el interior de la organización, e igualmente, hace que aumente el riesgo al que se exponen los recursos internos de la empresa puestos a disposición de los teletrabajadores a través de accesos a distancia.

I.3.1 Aspectos de seguridad del acceso a distancia en la empresa

Los objetivos de seguridad más comunes para las tecnologías de acceso a distancia en la empresa son los siguientes:

- Confidencialidad: garantizar que las comunicaciones de acceso a distancia y los datos de usuario almacenados no puedan ser leídos por personas no autorizadas.
- Integridad: detectar los cambios intencionados o no intencionados en las comunicaciones de acceso a distancia que se producen en tránsito.
- Disponibilidad: garantizar que los usuarios puedan acceder a los recursos a través del acceso a distancia siempre que sea necesario.

Para lograr estos objetivos, todos los componentes de las soluciones de acceso a distancia en la empresa, incluidos los dispositivos de cliente, servidores externos de acceso y servidores internos a los que se accede a través del acceso a distancia, deben estar protegidos frente una amplia variedad de amenazas. Las tecnologías de acceso a distancia en la empresa a menudo necesitan protección adicional dado que por su naturaleza generalmente están más expuestas a amenazas externas que las tecnologías a las que sólo se accede desde el interior de la organización.

Las principales preocupaciones en relación con la seguridad del acceso a distancia en la empresa son las siguientes:

- Falta de controles de seguridad física: los dispositivos de cliente de acceso a distancia en la empresa se utilizan en lugares fuera del control de la organización, tales como hogares de empleados, cafeterías, hoteles y salas de conferencias. La naturaleza móvil de los dispositivos hace que sean susceptibles de pérdida o robo, por lo que los datos en ellos contenidos están en situación de mayor riesgo. Incluso si un dispositivo de cliente está siempre en manos de su dueño, existen otros riesgos de seguridad física, como un atacante que mire por encima del hombro de un trabajador con acceso remoto a la empresa en una cafetería y visualice datos sensibles en la pantalla del dispositivo del cliente.
- Redes inseguras: debido a que casi todos los accesos remotos en la empresa se producen a través de Internet, las organizaciones normalmente no tienen control sobre la seguridad de las redes externas utilizadas por los clientes. Los sistemas de comunicación utilizados para el acceso remoto en la empresa incluyen el teléfono y los módems de línea de abonado digital (DSL), redes de banda ancha, como el cable y sistemas inalámbricos (véase [b-IEEE 802.11]), sistemas de interoperabilidad mundial para acceso por microondas (WiMAX) y redes móviles celulares. Estos sistemas de comunicación pueden ser objeto de espionaje, lo que pone en riesgo la información confidencial transmitida durante el acceso a

distancia. También pueden producirse ataques por intromisión (MITM, *man-in-the-middle*) para interceptar y modificar las comunicaciones. Los riesgos derivados del uso de redes no seguras pueden mitigarse, aunque no eliminarse, mediante el uso de tecnologías de cifrado que protegen la confidencialidad e integridad de las comunicaciones, y mecanismos de autentificación mutua para verificar las identidades de los dos puntos extremos.

- Dispositivos infectados en redes internas: los dispositivos de cliente, particularmente las computadoras portátiles, se utilizan a menudo en redes externas y posteriormente se introducen en la organización y se conectan directamente a sus redes internas. Un atacante con acceso físico a un dispositivo de cliente puede instalar software maligno en el dispositivo para recoger datos del mismo y de las redes y sistemas a los que se conecta. Si un dispositivo de cliente está infectado con software malicioso, dicho software puede extenderse a través de la organización cuando el dispositivo de cliente se conecta a la red interna. Además de utilizar las tecnologías apropiadas contra el software malicioso de la configuración de seguridad de referencia de la organización, como el software de protección instalado en los dispositivos de cliente, las organizaciones deben considerar la utilización de soluciones de control del acceso a la red (NAC, *network access control*) que verifiquen la situación de seguridad de un dispositivo de cliente antes de permitirle utilizar una red interna. Las organizaciones también deberían considerar la utilización de una red diferente para los dispositivos de cliente de teletrabajadores, en lugar de permitirles conectarse directamente a la red interna.
- Acceso externo a recursos internos: el acceso a distancia en la empresa permite la conexión de anfitriones externos a recursos internos, como por ejemplo servidores. Si recursos internos que no eran previamente accesibles desde redes externas, cuando se ponen a disposición a través de accesos a distancia quedan expuestos a nuevas amenazas, especialmente debido a los dispositivos de cliente y a redes que no son de confianza, y se incrementa significativamente la probabilidad de verse afectados. Cada forma de acceso a distancia en la empresa que pueda utilizarse para acceder a un recurso interno aumenta el riesgo de que dicho recurso se vea comprometido.

Bibliografía

[b-ITU-T X.1141] Recomendación UIT-T X.1141 (2006), *Lenguaje de marcaje de aserción de seguridad (SAML 2.0).*

[b-ITU-T X.1154] Recomendación UIT-T X.1154 (2013), *Marco general para la autentificación combinada en entornos con múltiples proveedores de servicio de identidad.*

[b-ITU-T X.1252] Recomendación UIT-T X.1252 (2010), *Términos y definiciones de referencia para la gestión de la identidad*.

[b-ITU-T X.1 254] Recomendación UIT-T X.1254 (2012), *Marco de garantía de autentificación de entidad.*

[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*.

SERIES DE RECOMENDACIONES DEL UIT-T

Serie A	Organización del trabajo del UIT-T
Serie D	Principios generales de tarificación
Serie E	Explotación general de la red, servicio telefónico, explotación del servicio y factores humanos
Serie F	Servicios de telecomunicación no telefónicos
Serie G	Sistemas y medios de transmisión, sistemas y redes digitales
Serie H	Sistemas audiovisuales y multimedia
Serie I	Red digital de servicios integrados
Serie J	Redes de cable y transmisión de programas radiofónicos y televisivos, y de otras señales multimedia
Serie K	Protección contra las interferencias
Serie L	Medio ambiente y TIC, cambio climático, ciberdesechos, eficiencia energética, construcción, instalación y protección de los cables y demás elementos de planta exterior
Serie M	Gestión de las telecomunicaciones, incluida la RGT y el mantenimiento de redes
Serie N	Mantenimiento: circuitos internacionales para transmisiones radiofónicas y de televisión
Serie O	Especificaciones de los aparatos de medida
Serie P	Terminales y métodos de evaluación subjetivos y objetivos
Serie Q	Conmutación y señalización
Serie R	Transmisión telegráfica
Serie S	Equipos terminales para servicios de telegrafía
Serie T	Terminales para servicios de telemática
Serie U	Conmutación telegráfica
Serie V	Comunicación de datos por la red telefónica
Serie X	**Redes de datos, comunicaciones de sistemas abiertos y seguridad**
Serie Y	Infraestructura mundial de la información, aspectos del protocolo Internet y redes de la próxima generación
Serie Z	Lenguajes y aspectos generales de soporte lógico para sistemas de telecomunicación

Impreso en Suiza
Ginebra, 2016