الاتحاد الدولي للاتصالات

ITU-T

قطاع تقييس الاتصالات
في الاتحاد الدولي للاتصالات

X.1157

(2015/09)

السلسلة X: شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

تطبيقات وخدمات آمنة – بروتوكولات الأمن

القدرات التقنية لكشف الاحتيال والتصدي له في الخدمات ذات المتطلبات العالية من مستوى الضمان

التوصية ITU-T X.1157

الاتحاد الدولي للاتصالات

توصيات السلسلة X الصادرة عن قطاع تقييس الاتصالات

شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

الشبكات العمومية للبيانات	X.199–X.1
التوصيل البيني للأنظمة المفتوحة	X.299–X.200
التشغيل البيني للشبكات	X.399–X.300
أنظمة معالجة الرسائل	X.499–X.400
الدليل	X.599–X.500
التشغيل البيني لأنظمة التوصيل OSI ومظاهر النظام	X.699–X.600
إدارة التوصيل البيني للأنظمة المفتوحة (OSI)	X.799–X.700
الأمن	X.849–X.800
تطبيقات التوصيل البيني للأنظمة المفتوحة (OSI)	X.899–X.850
المعالجة الموزعة المفتوحة	X.999–X.900
أمن المعلومات والشبكات	
الجوانب العامة للأمن	X.1029–X.1000
أمن الشبكة	X.1049–X.1030
إدارة الأمن	X.1069–X.1050
الخصائص البيومترية	X.1099–X.1080
تطبيقات وخدمات آمنة	
أمن البث المتعدد	X.1109–X.1100
أمن الشبكة المحلية	X.1119–X.1110
أمن الخدمات المتنقلة	X.1139–X.1120
أمن الويب	X.1149–X.1140
بروتوكولات الأمن	**X.1159–X.1150**
الأمن بين جهتين نظيرتين	X.1169–X.1160
أمن معرفات الهوية عبر الشبكات	X.1179–X.1170
أمن التلفزيون القائم على بروتوكول الإنترنت	X.1199–X.1180
أمن الفضاء السيبراني	
الأمن السيبراني	X.1229–X.1200
مكافحة الرسائل الاقتحامية	X.1249–X.1230
إدارة الهوية	X.1279–X.1250
تطبيقات وخدمات آمنة	
اتصالات الطوارئ	X.1309-X.1300
أمن شبكات المحاسيس واسعة الانتشار	X.1339–X.1310
التوصيات المتعلقة بالبنية التحتية للمفاتيح العمومية	X.1349–X.1340
تبادل معلومات الأمن السيبراني	
نظرة عامة عن الأمن السيبراني	X.1519–X.1500
تبادل مواطن الضعف/الحالة	X.1539–X.1520
تبادل الأحداث/الأحداث العارضة/المعلومات الحدسية	X.1549–X.1540
تبادل السياسات	X.1559–X.1550
طلب المعلومات الحدسية والمعلومات الأخرى	X.1569–X.1560
تعرف الهوية والاكتشاف	X.1579–X.1570
التبادل المضمون	X.1589–X.1580
أمن الحوسبة السحابية	
نظرة عامة على أمن الحوسبة السحابية	X.1601–X.1600
تصميم أمن الحوسبة السحابية	X.1639–X.1602
أفضل الممارسات ومبادئ توجيهية بشأن أمن الحوسبة السحابية	X.1659–X.1640
تنفيذ أمن الحوسبة السحابية	X.1679–X.1660
أمن أشكال أخرى للحوسبة السحابية	X.1699–X.1680

لمزيد من التفاصيل، يرجى الرجوع إلى قائمة التوصيات الصادرة عن قطاع تقييس الاتصالات.

التوصية ITU-T X.1157

القدرات التقنية لكشف الاحتيال والتصدي له في الخدمات ذات المتطلبات العالية من مستوى الضمان

ملخص

تقدم التوصية ITU-T X.1157 القدرات اللازمة لدعم خدمة كشف الاحتيال والتصدي له في خدمات تطبيقات تكنولوجيا المعلومات والاتصالات (ICT) الحساسة من حيث المتطلبات الأمنية. وتدعم خدمات كشف الاحتيال والتصدي له كشف الاحتيال وتحليله وإدارته عبر المستعملين والحسابات والمنتجات والعمليات والقنوات. وتقوم برصد وتحليل نشاط المستعمل وسلوكه على مستوى التطبيق (بدلاً من مستوى النظام أو قاعدة البيانات أو الشبكة) ومراقبة ما يجري داخل الحسابات وعبرها باستخدام أي قناة متاحة لدى المستعمل. وتقوم أيضاً بتحليل السلوك بين المستعملين والحسابات والكيانات الأخرى ذات الصلة، مع البحث عن النشاط غير العادي وجوانب الفساد وسوء الاستعمال. وتُستخدم بشكل عام في قطاعات إدارة أموال العملاء مثل التمويل الإلكتروني والنفاذ عن بُعد إلى المؤسسات وما إلى ذلك، ولكن يشيع استخدامها أيضاً للكشف عن الاحتيال الداخلي وأنواع أخرى من الأنشطة غير المرخصة.

التسلسل التاريخي

الطبعة	التوصية	تاريخ الموافقة	لجنة الدراسات	معرف الهوية الفريد*
1.0	ITU-T X.1157	2015-09-17	17	11.1002/1000/12353

الكلمات الأساسية

نظام كشف الاحتيال، إدارة الاحتيال.

* للنفاذ إلى التوصية، اطبع العنوان الإلكتروني: http://handle.itu.int/ في حقل العنوان من متصفح الويب الذي تستعمله، متبوعاً بحرف الهوية الفريد للتوصية. ومثال على ذلك http://handle.itu.int/11.1002/1000/11830-en.

تمهيد

الاتحاد الدولي للاتصالات وكالة متخصصة للأمم المتحدة في ميدان الاتصالات وتكنولوجيات المعلومات والاتصالات (ICT). وقطاع تقييس الاتصالات (ITU-T) هو هيئة دائمة في الاتحاد الدولي للاتصالات. وهو مسؤول عن دراسة المسائل التقنية والمسائل المتعلقة بالتشغيل والتعريفة، وإصدار التوصيات بشأنها بغرض تقييس الاتصالات على الصعيد العالمي.

وتحدد الجمعية العالمية لتقييس الاتصالات (WTSA) التي تجتمع مرة كل أربع سنوات المواضيع التي يجب أن تدرسها لجان الدراسات التابعة لقطاع تقييس الاتصالات وأن تُصدر توصيات بشأنها.

وتتم الموافقة على هذه التوصيات وفقاً للإجراء الموضح في القرار رقم 1 الصادر عن الجمعية العالمية لتقييس الاتصالات.

وفي بعض مجالات تكنولوجيا المعلومات التي تقع ضمن اختصاص قطاع تقييس الاتصالات، تعد المعايير اللازمة على أساس التعاون مع المنظمة الدولية للتوحيد القياسي (ISO) واللجنة الكهرتقنية الدولية (IEC).

ملاحظة

تستخدم كلمة "الإدارة" في هذه التوصية لتدل بصورة موجزة سواء على إدارة اتصالات أو على وكالة تشغيل معترف بها.

والتقيد بهذه التوصية اختياري. غير أنها قد تضم بعض الأحكام الإلزامية (بهدف تأمين قابلية التشغيل البيني والتطبيق مثلاً). ويعتبر التقيّد بهذه التوصية حاصلاً عندما يتم التقيّد بجميع هذه الأحكام الإلزامية. ويستخدم فعل "يجب" وصيغ ملزمة أخرى مثل فعل "ينبغي" وصيغها النافية للتعبير عن متطلبات معينة، ولا يعني استعمال هذه الصيغ أن التقيّد بهذه التوصية إلزامي.

حقوق الملكية الفكرية

يسترعي الاتحاد الانتباه إلى أن تطبيق هذه التوصية أو تنفيذها قد يستلزم استعمال حق من حقوق الملكية الفكرية. ولا يتخذ الاتحاد أي موقف من القرائن المتعلقة بحقوق الملكية الفكرية أو صلاحيتها أو نطاق تطبيقها سواء طالب بها عضو من أعضاء الاتحاد أو طرف آخر لا تشمله عملية إعداد التوصيات.

وعند الموافقة على هذه التوصية، لم يكن الاتحاد قد تلقى إخطاراً بملكية فكرية تحميها براءات الاختراع يمكن المطالبة بها لتنفيذ هذه التوصية. ومع ذلك، ونظراً إلى أن هذه المعلومات قد لا تكون هي الأحدث، يوصى المسؤولون عن تنفيذ هذه التوصية بالاطلاع على قاعدة المعطيات الخاصة ببراءات الاختراع في مكتب تقييس الاتصالات (TSB) في الموقع http://www.itu.int/ITU-T/ipr/.

المحتويات

الصفحة

التوصية ITU-T X.1157

القدرات التقنية لكشف الاحتيال والتصدي له في الخدمات ذات المتطلبات العالية من مستوى الضمان

1 مجال التطبيق

توفر هذه التوصية المبادئ التوجيهية المتعلقة بالقدرات التقنية لإدارة الاحتيال في الخدمات ذات المتطلبات العالية من مستوى الضمان. وتهدف هذه التوصية إلى توفير نظام قادر على كشف أنشطة الاحتيال. وتطبق في عدد كبير من القطاعات التجارية والمؤسسات التي تستخدم تطبيقات تكنولوجيا المعلومات والاتصالات (ICT) الحساسة من حيث المتطلبات الأمنية، وذلك عبر نشر نظام كشف الاحتيال والتصدي له. كما تطبق هذه التوصية في إدارة الاحتيال الداخلي في منظمة وفضلاً عن الاحتيال الخارجي عن طريق النفاذ عن بُعد أو عبر خدمة تجارية. وتغطي هذه التوصية المجالات التالية:

- قدرات خدمة كشف الاحتيال والتصدي له؛
- عمليات ومكونات نظام كشف الاحتيال والتصدي له؛
- الاعتبارات المتعلقة بخدمة مكافحة الحوادث والتصدي لها.

2 المراجع

لا يوجد.

3 التعاريف

1.3 مصطلحات معرفة في أماكن أخرى

تستخدم هذه التوصية المصطلحات التالية المعرَّفة في وثائق أخرى:

1.1.3 مستوى الضمان (assurance level) [b-ITU-T X.1252]: مستوى الثقة في الربط بين كيان والمعلومات عن الهوية المقدمة.

2.1.3 الاستيقان من كيان (entity authentication) [b-ITU-T X.1252]: عملية تستعمل لتحقيق قدر كاف من الثقة في الربط بين الكيان والهوية المقدّمة.

ملاحظة – يؤخذ استعمال مصطلح استيقان في سياق إدارة الهوية (IdM) على أنه يعني استيقان من كيان.

3.1.3 ضمان الاستيقان (authentication assurance) [b-ITU-T X.1252]: درجة الثقة التي تم التوصل إليها في عملية الاستيقان بأن الشريك في الاتصال هو نفسه الكيان الذي يدعيه أو المتوقع.

ملاحظة – تقوم الثقة على درجة الثقة في الربط بين الكيان المتصل والهوية المقدّمة.

4.1.3 المستعمل النهائي (end user) [b-ITU-T X.1141]: شخص طبيعي يستخدم الموارد لأغراض تطبيقية.

5.1.3 الهوية (identity) [b-ITU-T X.1252]: تمثيل كيان في شكل واحد أو أكثر من النعوت التي تتيح تمييز الكيان أو الكيانات بالقدر الكافي ضمن سياق. ولأغراض إدارة الهوية (IdM)، يُفهم المصطلح هوية كهوية سياقية (مجموعة فرعية من النعوت)، أي تتحدّد المجموعة المتنوعة من النعوت بإطار ذي ظروف حدّية محددة (السياق) يوجد فيه الكيان ويتفاعل.

ملاحظة – يُمثَّل كل كيان بهوية واحدة شاملة تضم جميع عناصر المعلومات المحتملة التي تميز ذلك الكيان (النعوت). بيد أن هذه الهوية الشاملة هي قضية نظرية عصية على أي وصف واستعمال عملي لأن العدد الكلي لجميع النعوت المحتملة لا حصر له.

6.1.3 ضمان الهوية (identity assurance) [b-ITU-T X.1252]: درجة الثقة في عملية تدقيق الهوية والتحقق منها التي يُلجأ إليها للتثبّت من هوية الكيان الذي تصدر أوراق الاعتماد له، ودرجة الثقة بأن الكيان الذي يستعمل أوراق الاعتماد هو الكيان الذي أُصدرت أو خُصصت أوراق الاعتماد له.

7.1.3 تدقيق الهوية (identity proofing) [b-ITU-T X.1252]: عملية التثبت والتحقق من صحة معلومات كافية للتأكد من الهوية التي يدعيها الكيان.

8.1.3 التحقّق من الهوية (identity verification) [b-ITU-T X.1252]: عملية التأكد من صحة هوية مزعومة بمقارنة الادعاءات المقدمة عن الهوية بمعلومات مثْبَتة سابقاً.

9.1.3 مقدّم الخدمة (service provider) [b-ITU-T X.1141]: دور يؤديه كيان في نظام بأن يقدّم خدمات إلى أطراف رئيسية أو إلى كيانات في أنظمة أخرى.

2.3 مصطلحات معرفة في هذه التوصية

تستخدم هذه التوصية المصطلحات التالية:

1.2.3 نظام كشف الاحتيال (fraud detection system): برمجيات بشكل تطبيق يدعم رصد وكشف وإدارة الاحتيال أو أي سوء استعمال آخر عبر المستعملين (مثل الزبائن) والحسابات والقنوات والمنتجات والكيانات الأخرى (مثل أكشاك الإنترنت).

ملاحظة – لنشر نظام كشف الاحتيال، يمكن دمج تطبيقات المؤسسة مع محرك كشف الاحتيال الذي يقيّم مخاطر الاحتيال في معاملة، بدءاً من تصفح المستعمل والنفاذ إلى التطبيق إلى أي نوع من النشاط، من قبيل تغيير العنوان أو الدفع أو استرجاع معلومات حساسة.

2.2.3 إدارة الاحتيال (fraud management): مجموعة كاملة من الأنشطة تتضمن أنظمة الإنذار المبكر، وعلامات وأنماط مختلف أنواع الاحتيال، وبيانات عامة عن المستعملين وأنشطتهم، والتصدي للحوادث وما إلى ذلك، من أجل التخفيف من المخاطر الأمنية باستخدام نظام كشف الاحتيال.

ملاحظة – يوجد عدد من المسائل التي تستلزم تطوير أنظمة إدارة الاحتيال، بما في ذلك الحجم الهائل للبيانات ذات الصلة، ومتطلبات الكشف السريع والدقيق للاحتيال من دون إعاقة المعاملات التجارية، والتطور المستمر لوسائل احتيال جديدة للتملص من التقنيات القائمة، وخطر الإنذارات الكاذبة.

3.2.3 تطبيق تكنولوجيا المعلومات والاتصالات (ICT) الحساسة من حيث المتطلبات الأمنية (security sensitive information and communication technology (ICT) application): تطبيق يتطلب مستوى عال جداً من ضمان الأمن لحماية أحد الأصول المعلوماتية للأفراد وسرية معلومات منظمة و/أو مؤسسة.

ملاحظة – عندما تتعرض تطبيقات تكنولوجيا المعلومات والاتصالات الحساسة من حيث المتطلبات الأمنية للاختراق ويتحكم فيها المهاجم، يتسبب كشف المعلومات الحساسة، أي المعلومات الشخصية أو المالية، بإلحاق ضرر كبير بالمستعملين والمنظمات والبنية التحتية للاتصالات وخدماتها، التي قد تتضمن تطبيقات للتمويل الإلكتروني والرعاية الصحية الإلكترونية والنفاذ عن بُعد إلى المؤسسات.

4 المختصرات والأسماء المختصرة

تستعمل هذه التوصية المختصرات والأسماء المختصرة التالية:

API السطح البيني لبرمجة التطبيقات *(Application Programming Interface)*

ATM ماكينة الصرف الآلي *(Automated Teller Machine)*

DLP منع فقدان البيانات *(Data Loss Prevention)*

DNS نظام أسماء الميادين *(Domain Name System)*

DSL الخط الرقمي للمشترك *(Digital Subscriber Line)*

HTTP بروتوكول نقل النصوص المترابطة *(HyperText Transfer Protocol)*

ICT تكنولوجيا المعلومات والاتصالات *(Information and Communication Technology)*

ID هوية *(Identity)*

IP بروتوكول الإنترنت *(Internet Protocol)*

IPS نظام منع التسلّل *(Intrusion Prevention System)*

ISP مقدّم خدمة الإنترنت *(Internet Service Provider)*

IT تكنولوجيا المعلومات *(Information Technology)*

MITM متطفّل *(Man-in-the-Middle)*

NAC التحكم في النفاذ إلى الشبكة *(Network Access Control)*

OS نظام التشغيل *(Operating System)*

PC حاسوب شخصي *(Personal Computer)*

PIN رقم الهوية الشخصي *(Personal Identity Number)*

SMS خدمة الرسائل القصيرة *(Short Message Service)*

SP مقدّم الخدمة *(Service Provider)*

SQL لغة استعلام بِنْيَوية *(Structured Query Language)*

SSL طبقة مقبس آمن *(Secure Socket Layer)*

TAN رقم الاستيقان من معاملة *(Transaction Authentication Number)*

WiMAX قابلية التشغيل البيني العالمي للنفاذ إلى الموجة الصغرية *(Worldwide Interoperability for Microwave Access)*

5 الاصطلاحات

في هذه التوصية كلمة "مطلوب" تدل على متطلب إلزامي يجب التقيد به بصرامة ولا يسمح بأي انحراف عنه في حال زعم المطابقة مع هذه الوثيقة.

وكلمة "يُوصَى" تدل على متطلب يوصى به لكنه غير إلزامي بالمطلق. وبالتالي لا حاجة تدعو لتوفر هذا المتطلب لزعم المطابقة.

وعبارة "يحظر من" تدل على متطلب إلزامي يجب التقيد به بصرامة ولا يسمح بأي انحراف عنه في حال زعم المطابقة مع هذه الوثيقة.

وكلمة "يمكن اختيارياً" تدل على مطلب اختياري مسموح به دون أن ينطوي على أي توصية به. ولا يرمي هذا المصطلح إلى إلزام التطبيق بتوفير هذا الخيار الذي يمكن أن يوفره مشغل الشبكة/مقدم الخدمة بشكل اختياري. بل إن المصنّع يمكنه إدراج هذا الخيار وزعم المطابقة مع هذه التوصية في نفس الوقت.

6 الجوانب العامة لكشف الاحتيال والتصدي له

1.6 بيان المشاكل

في خدمات التطبيقات القائمة على الاتصالات، كانت الهجمات القائمة على البرمجيات الضارة مسؤولة عن الهجمات الموجهة التي تستهدف أنواعاً كثيرة من الشركات والصناعات العمودية (مثل النقل الإلكتروني والمستشفيات الإلكترونية والأنواع الأخرى من الصناعات الإلكترونية). وهذه الهجمات في سبيلها لأن تصبح مصدر قلق كبير ويتزايد تقديمها عبر الرسائل الإلكترونية للتصيد الاحتيالي ومن خلال أشياء مصابة بالبرمجيات الضارة مثل الإعلانات التي يقوم المستعملون عديمو الخبرة بالنقر عليها. وقد استعملت هذه الطرق، ولا تزال تُستعمل، لإصابة عدة منظمات بالعدوى.

وتواجه المنظمات في الكثير من القطاعات التجارية والمؤسسات مخاطر كبيرة تتمثل في فقدان البيانات والنفاذ غير الملائم للحسابات والنشاط المتعلق بالمعاملات الذي تقوم به مصادر خارجية وداخلية. وتستطيع البرامج الضارة الموجهة الالتفاف في الغالب على تكنولوجيات الحماية القائمة، ولا يتم الكشف عن الحالات الناجمة لخرق البيانات إلا بعد فترة طويلة وبعد أن يتم استخلاص مقدار كبير من البيانات. وعادةً ما يكون الدليل على نشاط البرمجيات الضارة أمام مرأى الجميع ولكن عدم كشفه يعود إلى غياب قدرة المراقبة (الرصد) وعدم القدرة على تبيّن نمط لنشاط تطبيق غير عادي أو للنفاذ إلى البيانات من أنماط النشاط العادية. وعلى سبيل المثال، قد لا يعلم زبائن المصارف بأن هناك عملية احتيال قد ارتُكبت إلا بعد رؤيتهم حساباً لم يتم تأكيده في كشف حسابهم الائتماني، أو بعد أن يتصل بهم محصل الدين مطالباً إياهم بالدفع.

والهجمات القائمة على البرمجيات الضارة والموجهة للعملاء الماليين وموظفي الشركات تسبب لضحاياها أضراراً كبيرة تتعلق بسمعتهم وأخرى مالية. وهي تتحول بشكل سريع إلى أداة شائعة لمهاجمة حسابات العملاء والمؤسسات وسرقة المعلومات الحساسة أو الأموال. وبناءً عليه، بات من غير الممكن تجاهل الإنذارات والتنبيهات الهامة ما لم يتم تنظيم العمليات التجارية والمنظمات بشكل مناسب من أجل إدارة كشف الاحتيال بفعالية. وأخيراً، يمكن استخدام الهجمات القائمة على البرمجيات الضارة من أجل الاستيلاء على حسابات المستعملين أو تنفيذ عمليات احتيال أو سرقة للأصول القائمة على المخدّمات.

2.6 دور إدارة الاحتيال

يمكن تطبيق إدارة الاحتيال في ثلاث حالات احتيال نموذجية:

- كشف عملية الاستيلاء على حساب، ويحدث ذلك عادة عند سرقة أوراق اعتماد حساب المستعمل، أو من خلال البرمجيات الضارة. والبرمجيات الضارة تصيب نظام حواسيب الشركة ليس فقط بواسطة وثائق مصابة مرفقة ببريد إلكتروني وإنما أيضاً بمجرد زيارة موقع إلكتروني مصاب؛
- كشف الاحتيال على حساب جديد، ويحدث عادة عند سرقة أوراق اعتماد حساب المستعمل أو من خلال برمجيات ضارة؛
- كشف استعمال حساب مسروق (أو حساب شخص آخر)، كبطاقة ائتمان مسروقة مثلاً، عند القيام بعملية شراء أو عندما يدعي الشخص بأنه مستعمل طبيعي.

ويشيع استخدام كشف الاحتيال في حالة أو أكثر من حالات الاحتيال، من قبيل الاستيلاء على حساب، وكشف عملية احتيال داخلية، وكشف بطاقة دفع مزيفة في الوقت الفعلي وإلغاء المعاملة، وكنظام خاص بالمؤسسة لإدارة الاحتيال أو سوء الاستعمال. وفي كل واحد من هذه التصورات، من الضروري أن تتحقق المؤسسة التي تنفّذ المعاملة من شرعية الشخص الذي يجري المعاملة.

3.6 القدرات الرئيسية لإدارة الاحتيال

عندما يتعلق الأمر بالتصدي بشكل شامل لعملية احتيال تستهدف كشف الهوية، يتطلب نظام كشف الاحتيال الالتزام بثلاث قدرات لمعالجة هذه المشكلة: الرصد أو المراقبة، والكشف، والتصدي للحوادث. وتشمل هذه القدرات في المقام الأول الخطوات

التي ينبغي اتخاذها للبحث عن نشاط مشبوه من بيانات الأحداث المختلفة، والإجراءات اللازمة لكشف الاحتيال في مرحلة مبكرة من العملية عند حدوثه، والإجراءات التي ينبغي القيام بها لحل مشكلة الاحتيال فيما لو تم الكشف عن أنشطة مشبوهة.

المراقبة: يستطيع نظام كشف الاحتيال أن يرصد حالات الاحتيال بالبحث عن الحالات الشاذة في نشاط المستعمل وسلوكه على مستوى التطبيق، وكذلك داخل النظام وعلى مستوى قاعدة البيانات أو الشبكة، وأن يراقب ما يرشح من ذلك داخل الحسابات وعبرها باستخدام أي قناة متاحة لدى المستعمل. كما يقوم بمراقبة وتحليل سلوك المستعمل أو الحساب والعمليات المرتبطة به ويحدد السلوك الشاذ باستخدام قواعد أو نماذج إحصائية. وقد يستخدم أيضاً (على أمثل وجه) البيانات العامة للمستعملين والحسابات التي يجري تحديثها باستمرار، وكذلك لمجموعات النظراء من أجل مقارنة المعاملات والتعرّف إلى المعاملات المشبوهة من بينها. ويتطلب الرصد الشامل للاحتيال الداخلي بوجه خاص مراقبة المستعملين المميزين لتكنولوجيا المعلومات (IT) القادرين على تعديل الملفات والبيانات بشكل مباشر، بدلاً من الاضطرار للجوء إلى تطبيقات الاستعمال الجاهزة مسبقاً.

الكشف: يتمتع نظام كشف الاحتيال بالقدرة على استخراج كميات كبيرة من البيانات وتشريحها وتحليلها لمنع الاحتيال، وذلك باستخدام عملية فرز معقدة للعلاقات والقواعد يحددها العمل التجاري. ويمكن استعمال هذه القدرة لكشف الاحتيال الداخلي المصدر (أي الموظفون) والخارجي (أي العملاء والشركاء التجاريون). ولدعم القدرة على كشف الاحتيال، في استطاعة النظام كما يتعين عليه أن يضع بيانات عامة للكيانات المختلفة، كالمستعملين والحسابات والأسر والحواسيب الشخصية (PC) والهواتف المتنقلة وأكشاك الإنترنت، من أجل تحديد السلوك الشاذ للمعاملات التي يقوم بها ذلك الكيان. ويستخدم نظام كشف الاحتيال سياسات قائمة على القواعد تستند إلى الحكم البشري والمعرفة و/أو إلى نماذج رياضية تنبؤية لتحديد درجة احتمال تعرض معاملة معينة للاحتيال.

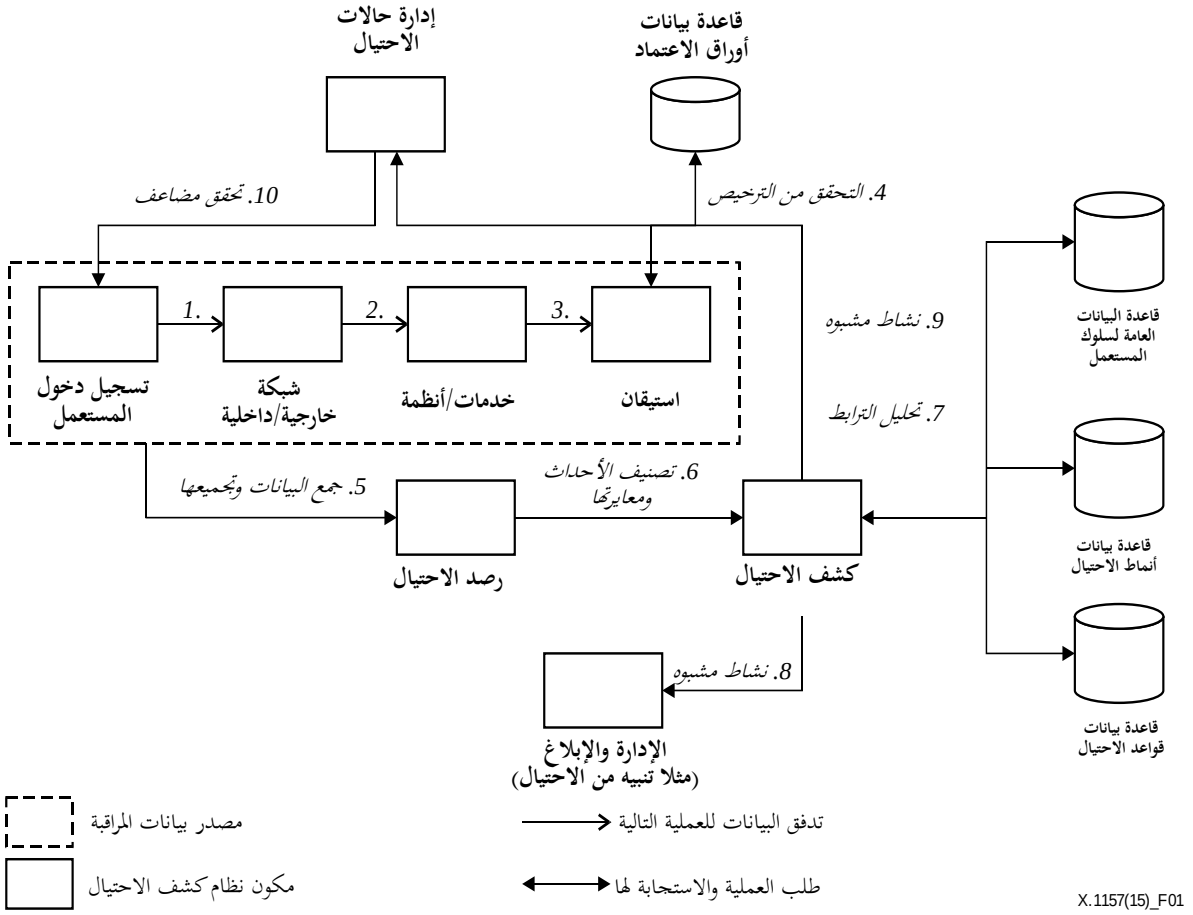
التصدي: بعد الكشف عن نشاط مشبوه، يتعين على نظام إدارة الاحتيال أن يتصدى للنشاط المشبوه باعتماد تدابير تحوطية متنوعة مثل إلغاء الحساب أو تبادل المعلومات. ويمكن لمجموعة متنوعة من تكنولوجيات الرصد والكشف التكميلية أن تساعد المؤسسات على الكشف بشكل أفضل عن النشاط المشبوه للمستعمل، والتعرف إلى أنماط النفاذ غير المناسب إلى الموارد أو نشاط الحساب الاحتيالي، والتحقيق في الحوادث والتصدي لها والتنبيه بشأنها في الوقت الفعلي، وإدارة الحوادث، وإلغاء الحسابات أو التدخل في المعاملات. وبالتالي يتعين على المنظمات أن تحدد أنسب مجموعة من تكنولوجيات الرصد والتحليل من حيث مستوى المخاطر الخاصة بها، وأن تحدد أيضاً قدراتها الأمنية المتعلقة بتنفيذ التكنولوجيا ودعمها.

7 معمارية نظام كشف الاحتيال والتصدي له

1.7 التشغيل والمكونات

يمكن دمج تطبيقات تكنولوجيا المعلومات والاتصالات مع مكونات كشف الاحتيال لدعم القدرات الرئيسية لإدارة مخاطر الاحتيال في معاملة بدءاً من نفاذ المستعمل وانتهاء بأي نوع من أنواع النشاط. وينبغي ألا يكون عمل نظام كشف الاحتيال شفافاً لا للقراصنة ولا للمستعملين لكي لا يتمكن القراصنة من تعلم قواعد النظام، وبالتالي لكي لا يواجه المستعملون الشرعيون أي عقبات. ويعاد التحقق من المعاملات المشبوهة التي يجريها المستعمل، بواسطة نظام كشف الاحتيال في الوقت الفعلي من أجل تقييم شرعيتها أو يتم تعليقها إلى أن يتاح الوقت لنظام كشف الاحتيال للبحث في مدى شرعيتها.

ويتألف نظام كشف الاحتيال من عدة مكونات تقوم بمعالجة البيانات وخزنها ونقلها من أجل كشف نشاط غير عادي. ويتمثل عمل نظام كشف الاحتيال، أي قدرته، في معالجة البيانات بين المكونات. ويرد في الشكل 1 وصف مفصل للعمليات التي يقوم بها نظام كشف الاحتيال ومكوناته. ومن الناحية النظرية، من المفترض أن يبدأ نظام كشف الاحتيال برصد كامل الدورة بعد تسجيل الدخول الأولي. وبناءً على ذلك يقوم نظام كشف الاحتيال بالعمليات اللازمة لإدارة الاحتيال، أي العمليات التي تتراوح بين قدرة الرصد وقدرة التصدي، وذلك على النحو التالي:



الشكل 1 – عمليات نظام كشف الاحتيال ومكوّناته

عملية تسجيل الدخول والاستيقان والتحقق من الترخيص (تدفقات البيانات 1 و2 و3 و4)

في ظل الظروف العادية، يتم تحليل تسجيل الدخول الأولي ويخصص له درجة تقييم للمخاطر عند مقارنة أوراق الاعتماد المجمّعة أثناء تسجيل الدخول بالبيانات الكامنة في قاعدة بيانات أوراق اعتماد المستعمل (اسم المستعمل وكلمة المرور) وبروتوكول الإنترنت (IP) وقاعدة البيانات العامة لسلوك المستعمل وما إلى ذلك. وتستند عملية التحقق من الترخيص إلى قواعد الاستيقان المحددة في قاعدة بيانات أوراق الاعتماد والتي تكون عادة قابلة للتشكيل بواسطة المؤسسة وقابلة للتوسع لإفساح المجال أمام وضع قواعد جديدة.

عملية رصد حالات الاحتيال وكشفها وإدارتها (تدفقات البيانات 5 و6 و7 و9 و10)

بعد تسجيل الدخول الذي يقوم به المستعمل، يجمع نظام كشف الاحتيال البيانات من مصادر متنوعة (أي الشبكات، والخدمات/الأنظمة، والاستيقان). ويقوم بتحليل البيانات التي جُمعت من مكوّن رصد الاحتيال. فإذا حددت عملية الاستيقان أي نشاط مشكوك به مثلاً، يرسل نظام كشف الاحتيال معلومات عن حالة الاحتيال المشتبه بها إلى مكوّن كشف الاحتيال. ومن ثَم يرسل مكون كشف الاحتيال طلب استعلام عن البيانات لتحليل الترابط في قواعد البيانات المتصلة بالاحتيال (أي البيانات العامة لسلوك المستعمل، وبيانات أنماط الاحتيال، وبيانات قواعد الاحتيال). وتُرتَّب حالات الاحتيال بحسب الأولوية بناءً على مستوى الخطر المأخوذ من مكون كشف الاحتيال وتعطي صورة كاملة عن المخاطر المرتبطة بالمعاملات التي تنطوي على درجات عالية من الخطر. وفي حالة الاحتيال ذات المستوى العالي من الخطر، يطلب مكون إدارة حالة الاحتيال مضاعفة التحقق من تسجيل دخول

المستعمل. وفي سبيل الارتقاء بمستوى الأداء في المستقبل، يمكن ولا بدّ من إعادة تلقيم تسوية الحالات في قواعد البيانات لإنشاء حلقة تعلم ذاتي.

عملية الإدارة والإبلاغ (تدفق البيانات 8)

ينبغي أن يكون مكون الإدارة والإبلاغ متاحاً أيضاً للمؤسسة لفهم نظام كشف الاحتيال والتحكم به على نحو أفضل. ويتيح هذا المكون لمستعملي النظام القيام بسهولة بتحليل أداء النظام والإبلاغ عنه، وتحديد حالات عدم الاتساق في تحديد الدرجات أو النفاذ ومجالات تحسينها، وتتبّع أفعال مستعملي النظام وأدائهم. وعلاوة على ذلك، توفر أدوات الإبلاغ طريقة سهلة لتقديم معلومات مفصلة عن الأداء إلى الإدارة العليا ومحلّلي حالات الاحتيال.

2.7 اعتبارات تتعلق بالمعمارية

عند تنفيذ نظام كشف الاحتيال المتعلق بتطبيقات تكنولوجيا المعلومات والاتصالات، ينبغي النظر في استخدام إحدى المعماريات الثلاث التالية: تركيب وحدات كشف الاحتيال داخل مخدّم التطبيق (مثلاً الويب)، والاستماع إلى التطبيق الإلكتروني و/أو مراقبته، ووضع سطوح بينية برنامجية داخل التطبيق التقليدي. وتعتبر القواعد والعمليات التجارية العناصر الأكثر أهمية لفعالية تطبيق معين.

تركيب وحدة كشف الاحتيال داخل مخدّم التطبيق

تُطبق القواعد التي تفرضها المؤسسة بواسطة المرشاح على أي طلب يخضع لبروتوكول نقل النصوص المترابطة (HTTP) (مثلاً تسجيل الدخول أو الدفع) قبل أن تصل المعاملة إلى التطبيق. ويمكن إيقاف المعاملات و/أو إعادة توجيهها نحو برنامج روتيني للتحقق من المعاملات في الوقت الفعلي من خلال تنفيذ قواعد الاحتيال الخاصة بالوحدة. ويوفر عدد من الصانعين إضافات مساعدة لمخدمات التطبيقات يتم دمجها مباشرة في معالج أولي.

الاستماع إلى تطبيق تكنولوجيا المعلومات والاتصالات و/أو مراقبته (أسلوب الاستماع)

في هذا الأسلوب، يستمع التطبيق إلى ملفات الدخل أو حركة شبكة البروتوكول HTTP (مثلاً تسجيل الدخول) أو "يستشفّها"، أو يقرأ البيانات باستخدام الإضافات المساعدة لمخدم التطبيق المركبة في كل مخدم. وتُقرأ البيانات في الوقت الفعلي (نهج "استشفاف" الشبكة) أو في الوقت الفعلي تقريباً (نهج الاستماع إلى مخدم التطبيق) وتلقّم في تطبيق آخر لإدارة الاحتيال أو يعاد تنظيمها في نسق يمكن أن تطبق عليه القواعد المتعلقة بالاحتيال. وفي الحالة الأخيرة توضع المعاملات المشبوهة في صف انتظار لمتابعتها من قبل محلل حالات الاحتيال. ويمكن إدماج السطوح البينية لبرمجة التطبيقات (API) المصمّمة حسب الطلب بحيث يعاد توجيه المعاملات لعملية التحقق بأسلوب التحدي والردّ.

وضع سطوح بينية برنامجية داخل التطبيق التقليدي (أسلوب الدمج المعزّز)

تستعمل في هذه الحالة السطوح البينية لبرمجة التطبيقات (API) لتمرير جميع المعاملات عبر نظام كشف الاحتيال قبل أن تتم معالجة المعاملة. ويتم في هذا الأسلوب التحكم بتدفق المعاملات مع إمكانية تحدي المستعمل في الوقت الفعلي إذا تم الكشف عن معاملة مشبوهة. ويستدعي تغيير القواعد التجارية تغييراً في التطبيق الأساسي. وتقوم السطوح البينية لبرمجة التطبيقات أساساً على خدمات الويب. وبالإضافة إلى ذلك، فإن السطوح البينية لبرمجة التطبيقات تزيد من صعوبة التحول من حلّ إلى آخر بين الحلول الخاصة بالجهات الصانعة.

وعموماً فإن استعمال السطوح البينية لبرمجة التطبيقات لكشف الاحتيال يوفر للمؤسسات/المنظمات تحكماً مباشراً في تدفق المعاملات ولكنه يتطلب عملاً تكاملياً ملحوظاً، ولا بد من تحديثه باستمرار عند تغيّر التطبيق الأساسي. أما مخدّمات التطبيق التي لا تتطلب تدخلاً في معاملات المستعملين في الوقت الفعلي فتفضل اتباع النهج الثاني الذي يعتبر الأسهل من حيث نزع الوحدات واستبدالها.

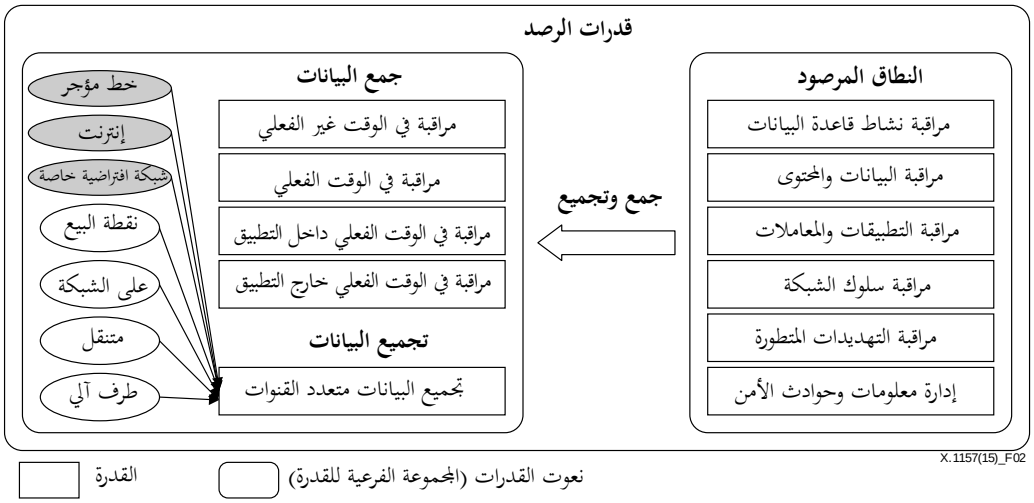
8 القدرات التقنية لكشف الاحتيال والتصدي له

1.8 قدرات الرصد

تُنشئ قدرة الرصد سياقاً خاصاً بالمستعمل والبيانات، يعتبر ضرورياً لكشف الهجمات والخروقات المبكرة ويتيح النفاذ إلى البيانات ورصد الأنشطة. وتعتبر مراقبة المستعمل المميز والنفاذ إلى البيانات الحساسة من المتطلبات الشائعة أيضاً للإبلاغ بشأن الامتثال.

ويتعين على نظام كشف الاحتيال أن ينفّذ القدرة المتعلقة بإدارة المعلومات والحوادث الأمنية بغية رصد نشاط المستعمل على نطاق واسع والنفاذ إلى الموارد عبر الشبكة والأنظمة وقواعد البيانات والتطبيقات. كما يتعين على نظام كشف الاحتيال أن يعزز البيانات المتعلقة بالأحداث بسياق خاص بالمستعملين والأصول والتهديدات ومواطن الضعف لتحسين فعالية المراقبة الأمنية اللازمة لكشف الخروقات. وعلاوة على ذلك، يتعين عليه أن يزود بشكل انتقائي المراقبة الأمنية العامة بقدرات إضافية من قبيل رصد التهديدات المتطورة استناداً إلى مستوى الخطر وبالقدرة على تنفيذ نظام كشف الاحتيال والتصدي له وتشغيله بشكل فعال.

كذلك يقوم نظام كشف الاحتيال بجمع البيانات المتعلقة بالأحداث في الوقت الفعلي تقريباً بطريقة تسمح بإجراء تحليل فوري. ويتسم الرصد في الوقت الفعلي بالأهمية بالنسبة لإدارة التهديدات من أجل تتبع وتحليل تطور هجمة معينة عبر المكونات والأنظمة، أو مراقبة نشاط مستعمل معين بهدف تتبع وتحليل نشاطه عبر التطبيقات، أو تتبع وتحليل سلسلة من المعاملات المتصلة ببعضها البعض أو من الأحداث المتصلة بالنفاذ إلى البيانات. وأخيراً ينبغي لقدرة الرصد في الوقت الفعلي أن تسمح بجمع البيانات على دفعات في الحالات التي يكون فيها الجمع في الوقت الفعلي غير عملي أو غير ضروري.



الشكل 2 – قدرات الرصد في نظام كشف الاحتيال

1.1.8 تجميع البيانات وجمعها

يتوفر تجميع البيانات وجمعها في مجموعة كبيرة من مصادر بيانات السجلات، بما في ذلك الشبكة وأجهزة الأمن، والمخدّم، وقاعدة البيانات وسجلات التطبيق، وخرج التطبيقات المتصلة بالأمن مثل تقييم مواطن الضعف وأجهزة رصد نشاط قاعدة البيانات، وخرج التكنولوجيات المتصلة بإدارة الهوية والنفاذ مثل أدلة المؤسسات وأنظمة تزويد المستعملين وإدارة النفاذ.

الرصد في الوقت غير الفعلي

يتطلب الرصد في الوقت غير الفعلي استعراض ملفات السجلات بشكل يدوي أو آلي. وباستطاعته توفير خيار النشر السريع من أجل التحليل اللاحق للمعاملات بفترات تأخير أطول، وإلغاء القدرة على إيقاف المعاملات عند إتمامها. وينبغي أن يدعم جمع البيانات على دفعات في الحالات التي يكون فيها الجمع في الوقت الفعلي غير عملي أو غير ضروري.

الرصد في الوقت الفعلي

يقوم الرصد في الوقت الفعلي بمراقبة جميع المعاملات (البروتوكول HTTP مثلاً) في الوقت الفعلي بواسطة مرشح مخدّم الويب. وفي وسع هذه الوظيفة أن تؤدي عملية المراقبة من دون معدات إضافية باستخدام مرشح قليل التأثير في مخدّم الويب. ولا حاجة لإجراء أي تغييرات في التطبيق تعتبر ضرورية من أجل التعرف إلى بيانات المعاملات في الوقت الفعلي.

الرصد الإلكتروني في الوقت الفعلي داخل وظيفة التطبيق

يعمل هذا الرصد الإلكتروني في الوقت الفعلي داخل وظيفة التطبيق على مراقبة جميع معاملات الويب المتعلقة بالبروتوكول HTTP في الوقت الفعلي عن طريق الدمج داخل التطبيق. وقد ينطوي نشر هذه الوظيفة والمحافظة عليها على تكلفة عالية ومدة طويلة لأنها تتطلب إجراء تعديلات واسعة على التطبيق لمراقبة النقاط الخاصة بالمعاملات.

الرصد الإلكتروني في الوقت الفعلي خارج وظيفة التطبيق

يعمل هذا الرصد الإلكتروني في الوقت الفعلي خارج وظيفة التطبيق على مراقبة جميع معاملات الويب المتعلقة بالبروتوكول HTTP في الوقت الفعلي عن طريق مرشاح خارجي للتطبيق. وليس لهذه الوظيفة تأثير على التطبيق في نهج الاستشفاف ونهج مرشاح الويب ولكن المرشاح الخارجي للتطبيق يكون متوافقاً مع التطبيق، مما قد يشكل خطراً على موثوقية التطبيق. ولا حاجة لإجراء أي تغييرات في التطبيق تعتبر ضرورية لرؤية بيانات المعاملات في الوقت الفعلي.

تجميع البيانات المتعدد القنوات

يعني تجميع البيانات المتعدد القنوات أنه يمكن إدراج بيانات المعاملات الواردة من قنوات أخرى بشكل كامل في عمليات رصد الاحتيال وكشفه. بالإضافة إلى ذلك، يبحث تجميع البيانات المتعدد القنوات عن سلوك مستعمل أو حساب مشبوه ويفيد في الوقت نفسه في البحث عبر القنوات والمنتجات ويربط بين التنبيهات والأنشطة التي يقوم بها كل مستعمل أو حساب أو كيان. ويتيح تجميع البيانات المتعدد القنوات تحليل العلاقات بين الكيانات الداخلية و/أو الخارجية ونعوتها (مثلاً المستعملون والحسابات ونعوت الحسابات والآلات ونعوت الآلات) من أجل الكشف عن أنشطة غير عادية أو سوء استعمال.

2.1.8 مصدر البيانات المراقبة

يستطيع نظام كشف الاحتيال أن يكشف النشاط الضار في مسار ثابت من أحداث متفرقة تكون عادة مرتبطة بمستعمل مصرّح له وتتأتى من شبكات وأنظمة ومصادر تطبيقات متعددة. وتشمل قدرات الرصد الدمج مع مصادر عدة للحصول على أحداث ووقائع مشبوهة.

رصد نشاط قاعدة البيانات

يساعد رصد نشاط قاعدة البيانات في الحفاظ على الفصل بين واجبات المستعملين الذين يتمتعون بنفاذ مميز إلى قاعدة البيانات عن طريق مراقبة نشاط المدير الإداري. كما تعزز هذه القدرة أمن قاعدة البيانات من خلال كشف الانتهاكات المتعلقة بالسياسة العامة والنشاط غير العادي. ويوفر تجميع الأحداث المتعلقة بقاعدة البيانات وترابطها والإبلاغ عنها القدرة على مراجعة قاعدة البيانات دون الحاجة إلى تفعيل الوظائف الأصلية لمراجعة قاعدة البيانات.

وتدعم هذه القدرة التمكن من العثور على التغييرات في بنية قاعدة البيانات ومحتواها، ونفاذ المستعملين المميزين إلى البيانات من خلال عمليات تسجيل دخول محلية أو عن بُعد. وبما أنها تعمل في طبقة قاعدة البيانات والملفات، فإنها تفتقر إلى سياق أي نفاذ أو تصفح للمعلومات لا يكون مرتبطاً بقاعدة البيانات أو بالملفات. ويمكن استعمال مكونات مراقبة الشبكة (المتعاقبة أو خارج النطاق) لمراقبة الاستفسارات البنيوية للغة الاستعلام البنيوية (SQL) والنفاذ الإداري من الشبكة.

رصد البيانات والمحتوى

تُستعمل قدرات رصد البيانات والمحتوى غالباً للحد من حالات تسرب المعلومات مثل أرقام بطاقات الائتمان والمعلومات المحدّدة لهوية شخص والملكية الفكرية القائمة على الوثائق أو قواعد البيانات، إلى جانب وظائف دعم رصد المحتوى والترشيح ومنع فقدان البيانات (DLP). والغرض من هذه القدرة هو أن تمكِّن المؤسسة من مراقبة محتواها الداخلي من أجل كشف الأنشطة المشبوهة. وتستعمل مراقبة المحتوى وترشيحه لحماية المحتوى أثناء تحركه (من خلال مراقبة الشبكة وترشيحها)، وأثناء توقفه (عن طريق مسح المحتوى المخزون)، وأثناء استعماله (من خلال العملاء الطرفيين). كما تتضمن معظم الوظائف قدرات لمسح المحتوى المخزون على الشبكة لمعرفة الانتهاكات المتعلقة بالسياسة العامة (مثلاً رقم بطاقة ائتمان على مخدّم غير معتمد)، والعثور على الانتهاكات المتعلقة بسياسة المؤسسة بشأن الاستعمال المناسب للمحتوى والبيانات.

وتستطيع أدوات منع فقدان البيانات اكتشاف الحركة أو النفاذ إلى البيانات الحساسة ومراقبتها وإيقافها على نحو ناشط باستعمال تقنيات فحص المحتوى والتحليل السياقي لتطبيق سياسة واحدة أو أكثر وقت الاستعمال. ويكون منع فقدان البيانات محدوداً بقدرة المنظمة على تعريف المحتوى الحساس أو بنيته أو خصائصه المميزة الأخرى.

ومع أن هذه الوظائف مفيدة للغاية في الحد من التعرّض العرضي أو الناجم عن عمليات تجارية سيئة، فثمة العديد من الأنشطة غير المراقبة التي يمكن أن يستخدمها مهاجم ضار أو مهاجم ضار من الداخل (مثل الهواتف المزودة بكاميرا والرسائل الصوتية وباستخدام الورق والحبر) للالتفاف على الحلول المواكبة للمحتوى.

رصد التطبيقات والمعاملات

تشتمل قدرة رصد التطبيقات والمعاملات على مراقبة التطبيقات لأن مواطن ضعف التطبيق تستغل عادة في الهجمات الموجهة، ولأن نشاط التطبيق الشاذ قد يكون الإشارة الوحيدة لنشاط احتيالي أو لعملية خرق ناجحة. وتمكّن القدرة على تحليل مسارات الأنشطة في التطبيقات المرزمة من مراقبة طبقة التطبيق الخاصة بتلك المكونات؛ يضاف إلى ذلك أن القدرة على تحديد وتحليل مسارات الأنشطة في تطبيقات العملاء تمكّن من مراقبة طبقة التطبيق في التطبيقات التي يجري تطويرها داخلياً.

وتقوم قدرة المراقبة أيضاً برصد النشاط المشبوه للمستعمل في تطبيق داخل قناة نفاذ معينة (مثل الويب أو الهاتف أو بسبل شخصية، أو عبر قنوات التطبيق والنفاذ) أو حتى في المنظمات التي يتم فيها تبادل عناوين بروتوكول الإنترنت المسجلة في القائمة السوداء. وقد يتراوح ذلك من كشف النفاذ الشاذ (مثل النفاذ المتزامن لجهاز واحد من مكانين متباينين جغرافياً) وحتى تسلسلٍ لمعاملات مشبوهة (مثل تغيير عنوان يليه تحويل مبلغ كبير من المال). ويمكنها أيضاً من حيث المبدأ أن تحدد أنشطة الموظفين غير المصرح لهم إذا كانت تنفذ في تطبيقٍ تتم مراقبته من قبل تطبيق كشف الاحتيال.

مراقبة سلوك الشبكة

إن القدرة على مراقبة سلوك الشبكة تبرز للعيان عمليات الشبكة استناداً إلى تدفقات الحركة بين الأنظمة، بما في ذلك المصدر والوجهة والمنْفَذ والبروتوكول وحجم البيانات المتبادلة وهوية المستعمل. ولهذه القدرة إمكانية تطبيق في التحليل القائم على الأمن أو العمليات. بالإضافة إلى ذلك تستخدم هذه القدرة مزيجاً من كشف البصمة والشذوذ لإبراز حالة الشبكة وتحديد الانحرافات عن الخطوط الأساسية، التي قد تشير إلى السلوك المشبوه أو الشاذ. والغرض من هذه القدرة هو تمكين المؤسسة من مراقبة سلوك شبكتها الداخلية من أجل كشف الأنشطة المشبوهة.

ويستخدم الأمن حالات تشمل الرصد لكشف انتشار الديدان والتركيب غير المصرح به للتطبيقات والنشاط المشبوه للنفاذ إلى النظام. ويستخدم التشغيل حالات تشمل التخطيط للسعة وتحليل الحركة، بما في ذلك القدرة على ربط هوية المستعمل (ID) بتدفق الحركة، أو تلبية متطلبات المراجِع لتتبع نفاذ المستعمل إلى الأنظمة الحساسة. ولهذه القدرة إمكانية ضعيفة للرؤية بعد الطبقة 3، ولذلك يتعذر عليها القيام مباشرةً بكشف المسائل المتعلقة بالنظام أو قاعدة البيانات أو المحتوى أو نظام الملفات أو المسائل الأخرى المتعلقة بالنفاذ.

مراقبة التهديدات المتطورة

تلتف البرمجيات الضارة الموجهة حول الجيل الحالي من مقدمي خدمة الإنترنت (IPS) وجدران حماية الشبكة وتكنولوجيات بوابة الأمن لخدمة الويب. ولدى بعض الصانعين المتخصصين الصغار منتجات قائمة على الشبكات لكشف التهديدات المتطورة. وهذه الأدوات تقوم عموماً بتحليل الأمور القابلة للتنفيذ لكشف القدرات الضارة (غالباً باستخدام بيئات افتراضية)، أو بمراقبة الاتصالات (بما في ذلك الاستعلامات عن نظام أسماء الميادين (DNS)) الصادرة من مراكز قيادة وسيطرة الشبكات الروبوتية المعروفة أو المشبوهة والواردة إليها، أو بمزيج من التقنيتين. وباستطاعة هذه القدرات أن تحدد بسرعة أي خلل محتمل قد ينجم عن تهديد متطور (مثل تهديد متطور مستمر)، لكن العديد من القدرات نفسها يجري إضافتها إلى الجيل التالي من جدران الحماية وأنظمة منع التسلل وبوابات الأمن لخدمة الويب.

وهناك وظائف أخرى متخصصة في كشف التهديدات الموجهة ضد مؤسسة في البيئة الخارجية بما في ذلك في "الشبكة العصية" (darknet)، وفي قنوات التحادث عبر الإنترنت، وفي غرف المحادثة، وفي شبكات التواصل الاجتماعي وما إلى ذلك. ويمكن تأدية هذه الوظائف من خلال كشف نشاط ضد ميدان أو مجموعة من عناوين بروتوكول الإنترنت أو الكلمات الأساسية.

إدارة معلومات الأمن وأحداثه

تمثل قدرات إدارة معلومات الأمن وأحداثه المجال الواسع النطاق لجمع الأحداث والقدرة على ربطها من خلال مصادر معلومات متباينة بهدف الكشف المبكر عن الخروقات. وتحسن هذه القدرة من إدارة التهديدات والتصدي لحوادث الأمن من خلال جمع وتحليل أحداث الأمن الواردة من مجموعة واسعة من مصادر البيانات في الوقت الفعلي. وتشمل هذه المصادر الشبكة، وأجهزة الأمن، والمخدّم، وقاعدة البيانات، وسجلات التطبيق، وخرج التطبيقات المتصلة بالأمن من قبيل أجهزة رصد إدارة الأمن ونشاط قاعدة البيانات، وكذلك خرج التكنولوجيات ذات الصلة بإدارة الهوية والنفاذ مثل أدلة المؤسسات وأنظمة تزويد المستعملين وإدارة النفاذ. وعلاوة على ذلك فإن هذه القدرة تدعم مراقبة الامتثال لسياسة الشركة والتحقيق في الحوادث من خلال تحليل البيانات السابقة الواردة من هذه المصادر والإبلاغ عنها.

وفيما يتعلق بكشف الاحتيال، تجمّع هذه القدرة البيانات المتعلقة بالأحداث التي أنتجتها الأجهزة والأنظمة والتطبيقات وتقوم بتحليلها. ومع أن بيانات السجلات تشكل المصدر الأولي للبيانات، فإن باستطاعة هذه القدرة أن تعالج أيضاً أشكالاً أخرى من البيانات. وتقيّس البيانات بحيث يمكن ربط الأحداث الواردة من مصادر متباينة وتحليلها وفقاً لمجموعات القواعد التي تصمم لأغراض محددة، مثل مراقبة أحداث أمن الشبكة أو مراقبة نشاط المستعمل لأن المراقبة والتحليل يعتمدان كلياً على بيانات الأحداث المتولدة من مصادر أخرى. أما النشاط الذي لم يستخرج باعتباره حدثاً أو من سجل نشاط ما فلا يكون مرئياً من قبل القدرة.

2.8 قدرات الكشف

يستخدم كشف الاحتيال عمليات أساسية قائمة على المخدم (تكون شفافة للمستعملين) تعاين نفاذ المستعمل وسلوكه. ومن ثم يقارن كشف الاحتيال هذه المعلومات بالبيانات العامة لما هو متوقع ويعتبر "اعتيادياً". وهو يعمل في آن معاً على تقييم مجموعة من عوامل الخطر لإظهار حالات الاحتيال الحقيقية وجعل معدلات الكشف الزائف متدنية. ويعاد التحقّق من المعاملات المشبوهة للمستعمل في الوقت الفعلي من أجل تقييم شرعيتها أو يتم تعليقها إلى أن يتاح الوقت لمحللي الاحتيال للبحث في مدى شرعيتها.

وبما أن كشف الاحتيال يعمل في سياق تطبيق معين، فهو غير قادر على الكشف عن العمليات الخبيثة والعمليات الاحتيالية المحتملة التي تكون خارج التطبيق. ولا يمكن لكشف الاحتيال أن يكشف سلوكاً أو يشتبه فيه إن لم يكن هذا السلوك معرّفاً لدى محركه لأن القواعد ليست مدركة لنمط النشاط، ولأن النموذج لم يتعلم بما يكفي لفضح هذا السلوك أو لأن دمج التطبيق لا يوفر لمحرك تقييم مخاطر الاحتيال ما يكفي من البيانات ذات الصلة. وتحقيقاً لفعالية الكشف، يتطلب التحليل معرفة مدمجة لحالات استعمال معينة، أو يتعين على العميل أن يوفر هذه المعرفة على شكل قواعد وتقارير مترابطة ومكيفة حسب الطلب. وعليه، يحتاج نظام كشف الاحتيال إلى قدرات من قبيل تحديث أنماط الاحتيال، وتوفير مكتبة للقواعد محددة مسبقاً، ومعالجة قواعد في الوقت الفعلي.

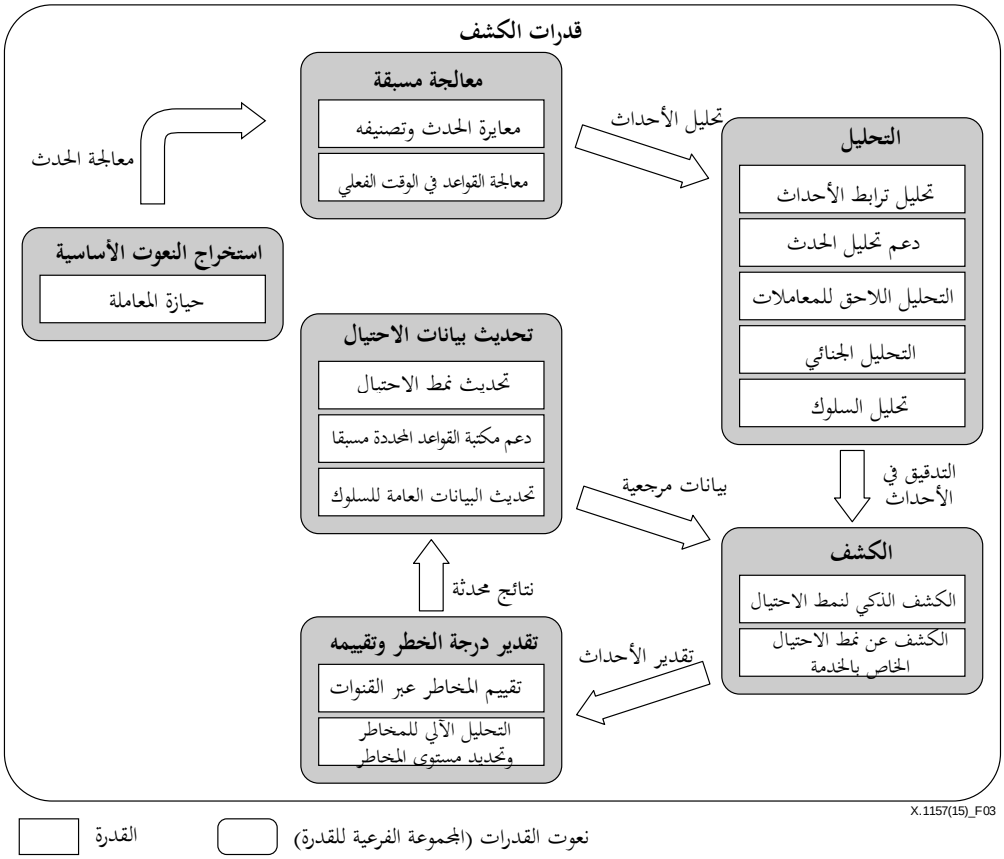
وتتطلب معظم القدرات معالجة مستفيضة للنماذج أو صقلاً للبيانات العامة أو تطويراً لقواعد الكشف قبل أن تصبح التطبيقات تامة التشغيل. ومن بين هذه القدرات مراقبة جميع المعاملات، والتحليل المؤتمت للمخاطر وتقدير مستوى المخاطر، ووضع بيانات عامة لسلوك المستعمل وتعلُّمها، والكشف عن الاحتيال الخاص بالخدمة والكشف الذكي للاحتيال، وتقييم المخاطر عبر القنوات.

حيازة المعاملات

تمثل حيازة المعاملات القدرات التي تتماشى مع النعوت الأساسية وتستخرجها من المعاملات، والتي تتطلب وضع بيانات عامة مفصلة لسلوك كل مستعمل بشكل آلي وعند أول نفاذ يقوم به.

معايرة الأحداث وتصنيفها

ينبغي معايرة البيانات المتعلقة بالحدث لكي يتسنى الربط بين الأحداث الواردة من مصادر متباينة وتحليلها وفقاً لمجموعات القواعد المعدة خصيصاً لأغراض محددة مثل مراقبة الأحداث الأمنية في الشبكات أو مراقبة نشاط المستعمل. ويمثل ذلك تقابلاً للمعلومات المستقاة من مصادر غير متجانسة مع نظام مشترك لتصنيف الأحداث. ويفيد التصنيف في التعرف إلى النمط، كما يعمل على تحسين نطاق قواعد الترابط واستقرارها. وعند معايرة الأحداث الواردة من مصادر غير متجانسة، يصبح من الممكن تحليلها باعتماد عدد أقل من قواعد الترابط مما يقلل من أعمال النشر وأنشطة الدعم. وبالإضافة إلى ذلك، يكون من الأسهل التعامل مع الأحداث المعايرة لدى وضع التقارير ولوحات التحكم.



الشكل 3 – قدرات الكشف في نظام كشف الاحتيال

تحديث نمط الاحتيال

إن حديث نمط الاحتيال يعني التحديث الآلي للبيانات المأخوذة من الشبكة والمتعلقة بحادثة احتيال. وتضم البيانات المتعلقة بحادثة الاحتيال بيانات بروتوكول الإنترنت الجغرافية لتحليل موقع مصدر المعاملات بما في ذلك المدينة والبلد ومقدّم خدمة الإنترنت فضلاً عن بيانات تتعلق بسمعة المضيف لتحديد المعاملات الواردة من مصادر مشبوهة معروفة، والبيانات المتعلقة بإغفال الاسم والهوية للمعاملات التي ترد من شخص يحاول إخفاء نقطة المنشأ. وينبغي أن يكون لتحديث نمط الاحتيال القدرة على تطبيق نظام كشف الاحتيال على الحالات الأخرى لاستخدام الاحتيال على امتداد المؤسسة وتكييفها لتلبية المتطلبات المحددة لأعمال المؤسسة. فعلى سبيل المثال، يمكن لنظام كشف الاحتيال أن يدمج النتائج الناجمة كشف احتيال خارجي وتقدير درجة الائتمان وأنظمة تبادل المعلومات مثل القوائم السوداء.

ومن أجل نشر تحديث نمط الاحتيال، تتوفر في مصادر متنوعة معلومات حول بيئة التهديد القائمة، بما في ذلك القوائم مفتوحة المصدر، ومحتوى التهديد والمضمون المتعلق بالسمعة الذي تعده وتحتفظ به أفرقة البحوث الأمنية داخل مقدمي الخدمات الأمنية، والبيانات التي يعدها مقدمو الخدمات الأمنية المدارة وغيرها من الخدمات الأمنية. ويمكن إدماج البيانات المتعلقة بالتهديدات في نظام كشف الاحتيال على شكل قوائم مراقبة وقواعد للترابط واستفسارات بطرق تكفل زيادة معدل النجاح في الكشف المبكر عن الخروقات.

ويمكن لأحدث المعلومات عن أنماط التهديدات والهجمات أن تساعد المنظمة في التعرف على نشاط شاذ. فيمكن على سبيل المثال لعدد قليل من الأنشطة الصادرة إلى عنوان IP خارجي أن تبدو طبيعية ويمكن إغفالها بسهولة. لكن ذلك يتغير عند وجود نظام معلومات يتعلق بالتهديدات يشير إلى أن الوجهة المقصودة ترتبط بتحكم شبكات روبوتية (برامج تسلل). ولكشف الاحتيال، يمكن مقارنة هذه المعلومات بخوارزميات التعلم الآلي للسلوك المتوقّع أو بالقواعد الأكثر عمومية فيما يتعلق بما يعتبر سلوكاً "اعتيادياً".

دعم مكتبة القواعد المحددة مسبقاً

ينطبق دعم مكتبة القواعد المحددة مسبقاً على الحالة التي يدعم فيها نظام كشف الاحتيال القواعد المثبتة المتاحة للتصدي للاحتيال. وعادة تشمل وظيفة نظام كشف الاحتيال مجموعة من القواعد المثبتة لنشرها، كما ينبغي إدراجها من أجل استحداث/تعديل قواعد جديدة بسهولة. وبالإضافة إلى ذلك، قد تتضمن هذه الوظيفة القدرة على تقاسم القواعد مع منظمات أخرى. وتتيح هذه الوظيفة لنظام كشف الاحتيال سرعة تحديث واختبار القواعد فضلاً عن تصورات الاحتيال الجديدة، والقيام بسهولة برؤية وتحليل البيانات ونتائج كشف الاحتيال. كما يمكنها وضع مجموعة محددة من القواعد لإدارة الاحتيال أو سوء الاستعمال على مستوى العملاء، وعلى مستوى مجموعات العملاء، أو بالنسبة لأي من المستعملين الآخرين.

وتعمل معظم أنظمة كشف الاحتيال المتعلق ببطاقات الائتمان على تمكين المؤسسات من إدارة قواعد الأعمال التجارية التي تتعارض معها كل معاملة من معاملاتها، وذلك لكي يتسنى للأعمال التجارية الكشف عن أنماط الاحتيال الخاصة بتلك الأوضاع.

ويمكن لمكتبة القواعد هذه أن تحدد مجموعة من القواعد على أساس المعلومات الأمنية والمعلومات السياقية:

- سياق المستعمل: أدوار العمل التي يؤديها المستعمل؛
- سياق الأصول: الملكية، والتطبيقات أو العلميات التجارية ذات الصلة؛
- سياق أمن المعلومات: مواطن الضعف القائمة في نظام التشغيل (OS)، والتطبيق، وطبقة الشبكة أو قاعدة البيانات، وحالة التشكيل؛
- سياق التهديد الخارجي: الجهات الفاعلة الخبيثة المعروفة وأنماط الهجمات؛
- سياق البيانات: حراجتها بالنسبة إلى الأعمال أو المتطلبات القانونية والتنظيمية للامتثال؛
- سياق التطبيق: الاستخدامات التجارية للتطبيق وحدود النفاذ الطبيعي إلى البيانات.

تحليل الترابط بين الأحداث

يُقيم تحليل الترابط بين الأحداث العلاقات بين الرسائل أو الأحداث التي تولدها الأجهزة أو الأنظمة أو التطبيقات، بالاستناد إلى خصائص من قبيل المصدر والهدف والبروتوكول أو نوع الحدث. كما يتعين وجود مكتبة تضم قواعد للترابط محددة مسبقاً والقدرة على سهولة تكييف تلك القواعد حسب الطلب. ومن خلال تحليل الترابط بين الأحداث، يتعين على وحدة التحكم بالحدث الأمني توفير عرض في الوقت الفعلي للحوادث والأحداث الأمنية.

دعم تحليل الأحداث

يُنجَز تحليل الأحداث من خلال ترابط الأحداث في الوقت الفعلي، وعن طريق تحليل الأحداث السابقة القائم على الاستعلام. ويتكون تحليل الأحداث الأمنية من عروض لوحة التحكم وتقارير ووظائف مخصصة لدعم التحقيق في نشاط المستعمل والنفاذ إلى الموارد من أجل التعرف على تهديد أو خرق أو سوء استعمال لحقوق النفاذ. ولدى ظهور نشاط مشبوه عن طريق المراقبة الأمنية أو الإبلاغ عن الأنشطة، من المهم بمكان التمكن من تحليل نفاذ المستعمل والنفاذ إلى الموارد. ويمكن تحقيق هذه العملية باتباع نهج تكراري يبدأ باستعلام واسع النطاق عن مصدر الحدث أو المستعمل أو الهدف، ومن ثمّ المباشرة باستعلامات مركزة بصورة متزايدة لتبيّن مصدر المشكلة. ويستخدم تحليل الأحداث وظائف التحليل السلوكي من أجل إثراء عملية الترابط القائمة على القواعد.

معالجة القواعد في الوقت الفعلي

تمثل معالجة القواعد في الوقت الفعلي القدرة على معالجة قواعد الاحتيال المتعارضة مع مسار المعاملات في الوقت الفعلي لتوليد درجات تقييم المخاطر المتعلقة بالمستعمل/الدورة وتنبيهات مفصّلة من الحوادث. وينبغي أن يتم في إطار هذه الوظيفة النظر في السلوك غير الاعتيادي للمستعمل، وأنماط الاحتيال الشائعة، والقوائم السوداء/البيضاء، والبيانات المتعلقة بحوادث الاحتيال. ويمكن أن تدعم هذه الوظيفة قواعد تركيب القواعد مثل السلوك غير الاعتيادي للمستعمل مع وجود فترات سماح، وهوية جهاز العميل، وأنماط الاحتيال الشائعة، والقوائم السوداء/البيضاء، وبيانات بروتوكول الإنترنت الجغرافية، والبيانات المتعلقة بسمعة المضيف. وبالإضافة إلى ذلك، يمكن لنظام كشف الاحتيال إجراء تقييم لدرجة المخاطر لكل دورة وتقييم لدرجة المخاطر المتراكمة لكل مستعمل؛ وباستطاعته أيضاً أن يمكّن الاستيقان القائم على المخاطر الذي يزود نظام الاستيقان في الوقت الفعلي بدرجات تقييم المخاطر التي ينطوي عليها المستعمل والدورة، لتقرير ما إذا كان الاستيقان الإضافي ضرورياً.

دعم أداة الإدارة

تدعم وظيفة دعم أداة الإدارة التخزين الفعال من حيث التكاليف وتحليل كمية كبيرة من المعلومات التي تتضمن جمع وفهرسة وتخزين جميع بيانات السجل والأحداث من كل مصدر من المصادر فضلاً عن القدرة على البحث عن تلك البيانات والإبلاغ عنها. كما يتعين على قدرات الإبلاغ أن تشمل تقارير محددة مسبقاً إلى جانب القدرة على تحديد التقارير المخصصة أو استخدام أدوات الإبلاغ الخاصة بطرف ثالث. وعموماً تضم وظيفة أداة الإدارة تقارير محددة مسبقاً وقابلة للتعديل لنشاط المستعمل والنفاذ إلى الموارد وتقارير نموذجية لأغراض الإدارة المحددة والدورية. وتتوفر أداة الإدارة عادة من خلال تخصيص حالة دعم الشبكة وتدفق العمل بما في ذلك الآراء الخاصة بالمستعمل مثل حالة الوقائع الاحتيالية المعروفة والأنشطة الجارية والبنود المصنفة الجديدة وآليات التنبيه القابلة للتشكيل بما في ذلك البريد الإلكتروني وإخطارات خدمة الويب.

التحليل اللاحق للمعاملات

التحليل اللاحق للمعاملات هو القدرة على حيازة وخزن جميع عناصر البيانات بغية إجراء تحليل في المستقبل. وبعد ذلك يضم مستودع البيانات التاريخ الكامل للمعاملات المتعلقة بجميع المستعملين لفترة زمنية معينة. وتتطلب هذه الوظيفة حيازة متطورة للبيانات وتنسيقها من أجل تخزينها وسرعة استرجاعها وتقييمها في الوقت الفعلي. ويستخدم نظام كشف الاحتيال البيانات العامة المتعلقة بسلوك كل فرد من المستعملين لأغراض التحليل اللاحق للمعاملات، ويمكنه تخزين المعاملات مصنفة بحسب الدورة والمستعمل وختم الوقت من أجل استرجاعها وتحليلها.

التحليل الجنائي

ترمي وظيفة التحليل الجنائي إلى البحث عن تفاصيل مستودع بيانات المعاملات وترشيحها والتنقيب فيها. وتشمل الإمكانية القدرة على الترشيح والبحث والتحليل المسهب للمعاملات وأنماط النفاذ. وهي توفر تحديد أنماط الاحتيال الجديدة التي تستحق وضع قواعد للكشف عنها في الوقت الفعلي.

تحليل السلوك

يتطلب نظام كشف الاحتيال معاملات مزودة ببيانات عامة تتعلق بسلوك جميع المستعملين ويدعم النظم الأكثر تطوراً لتتبع سلوك فرادى المستعملين. فهو يقيم بيانات عامة لنشاط اعتيادي ويستخدم وظيفة تحليل السلوك لإرسال تنبيهات بشأن وقوع انحرافات. وتستخدم عملية وضع البيانات العامة للسلوك مرحلة للتعلّم تنشئ بيانات عامة للنشاط الاعتيادي لمصادر أحداث متفرقة جمُعت بفضل قدرات المراقبة.

يبدأ نظام كشف الاحتيال بصورة آلية بوضع البيانات العامة لمستعمل معين منذ المرة الأولى التي يرى فيها النظام تلك البيانات. ومن ثَم يمكن للنظام أن ينشئ بيانات عامة لما يعتبر سلوكاً "اعتيادياً" لذلك المستعمل ومن ثم يدقق في السلوك "غير الاعتيادي" عند حدوثه. وتنبّه مرحلة الكشف إلى ما يحدث من انحرافات عن السلوك الطبيعي. وحين تكون الأوضاع الشاذة محددة بدقة، يمكن تحديد قواعد للترابط تبحث عن مجموعة محددة من الظروف. وينبغي للقدرة أن تقوم بشكل آلي بالكشف عن الأنماط والحالات الشاذة التي يمكن أن تكون ضارة، وتتبّعها وتأويلها وفهمها، على أن يتم تفادي التسبب بانقطاع الممارسة المشروعة للعميل. وأخيراً، يمكن لوضع البيانات العامة المتعلقة بالسلوك المساعدة في اتخاذ قرارات متعلقة بالمخاطر بالاستناد الى الانحراف عن السلوك الاعتيادي.

وفي أعقاب التحديد الأولي للبيانات العامة، يلزم المزيد من الوقت لكي يتعلّم النظام الأمور التي يتشكل منها السلوك الشاذ أو لكي تتمكن المؤسسات من تطبيق القواعد الصحيحة للكشف عن السلوك الشاذ أو الدورات الشاذة. وبإمكان هذا النهج أن يحسن القدرة على اكتشاف هجمة موجهة لكنه بحاجة إلى قدر أكبر من الصقل من جانب الخبراء في الميدان للتحكم بالإيجابيات الزائفة.

الكشف الذكي لنمط الاحتيال

لا يمكن الكشف عن جميع حالات الاحتيال من خلال الشبكات وسجلات التطبيقات ومجالات البيانات المنفصلة. ولا بد من إدراج تحليل البيانات غير المنظمة عن طريق استخدام منطق استخراج البيانات على اختلافها الذي يمكنه تقييم مدى ملاءمة المعلومات التي تم ادخالها.

ويتعين على المؤسسات البحث عن السبل المنطقية لاستخراج البيانات التي تتعلم كيفية العمل بشكل مستقل، بالحد الأدنى من البيانات، والبحث عن الأنظمة التي يمكنها من خلالها القيام بسرعة وسهولة بتحديث القواعد المتعلقة بمعلمات الاحتيال المعروفة أو التي اكتشفت حديثاً. وفي وسعها التدقيق في الهوية الإلكترونية لمستعمل جديد مقابل خدمة تقدير الهوية، التي يقدمها مباشرة بائعو خدمة تقدير الهوية. ومن شأن هذه التقديرات أن تؤكد احتمال أن يكون المستعمل على الشبكة مستعملاً محتالاً.

كشف أنماط الاحتيال الخاصة بالخدمة

يتطلب نظام كشف الاحتيال القدرة على تحديد القواعد التي تبحث عن أنماط المعاملات التي تقابل أنماط الاحتيال المعروفة وأنماط الاحتيال الخاصة بالخدمة. وبعبارة أخرى، يبحث النظام في خدمة التطبيق عن تسلسل محدد من المعاملات والأحوال المشبوهة وفقاً للمنطق المتبع في الأعمال التجارية/العمل. ويمكن تنفيذ هذا النمط في غضون دورة واحدة، أو قد يشمل دورات متعددة وعدة مستعملين وفقاً لخدمة التطبيق المحددة.

وأخيراً، إذا لم تكن أنظمة كشف الاحتيال متلائمة بشكل مناسب، فقد يتولد عنها الكثير من الإيجابيات الزائفة. ففي بيئات من قبيل التجارة الإلكترونية، حيث يكون التنفيذ في الوقت الفعلي ضرورياً، من الواضح أن لا يكون المعدل الإيجابي المزيف والمرتفع مقبولاً.

تقييم المخاطر عبر القنوات المشتركة

لا تعمل أنظمة كشف الاحتيال إلا في تطبيقات معينة وقنوات معينة، ولا يتم التدقيق فيها عبر القنوات (مثل الهاتف أو الويب أو بسبل شخصية) أو أنواع الحسابات (مثل الإيداعات أو الاعتمادات). بالإضافة إلى ذلك، لا تكون أنظمة كشف الاحتيال مُلمّة بنشاط احتيالي يجري خارج التطبيق، كما أنها ليست مدمجة في أنظمة مُلمّة بمثل هذا النشاط (مثلاً، كشف الاحتيال القائم على الشبكات والأنظمة). وبناءً على ذلك، لا يمكنها الكشف عن العمليات الخبيثة والعمليات الاحتيالية المحتملة التي تكون خارج التطبيق.

وبالتالي فإن الكشف عن الاحتيال يقتضي رصد نشاط المستخدم المشبوه في تطبيق ضمن قناة نفاذ معينة (مثل الشبكة أو الهاتف أو بسبل شخصية)، أو عبر التطبيقات أو قنوات النفاذ أو حتى المنظمات (حيث يتم، على سبيل المثال، تبادل عناوين بروتوكول الإنترنت المدرجة في "القائمة السوداء" فيما بين المنظمات). وقد يتراوح ذلك من كشف النفاذ الشاذ (مثلاً، النفاذ المتزامن من قبل جهاز واحد من موقعين جغرافيين متباينين) وحتى تسلسلٍ لمعاملات مشبوهة (مثلاً، تغيير في العنوان يليه تحويل مبلغ كبير من المال).

وللكشف عن المزيد من الاحتيال، يتطلب نظام كشف الاحتيال إدراج التقديرات المأخوذة من وحدات كشف الاحتيال في وحدات تقييم درجات المخاطر عبر القنوات المشتركة التي تبحث في قنوات الاستعمال (مثل مراكز النداء أو المهاتفة أو ماكينات الصرف الآلي (ATM)).

التحليل الأوتوماتي للمخاطر وتقدير مستوى المخاطر

ويتطلب ذلك القدرة على القيام آلياً بتقييم المخاطر الأمنية وتقديرها وتحديد مستواها. ويعزى الكشف عن الاحتيال وتقييم درجات مخاطر المعاملات إلى النماذج أو القواعد أو كليهما. ومن أجل العثور على نشاط مشبوه من بيانات مجمّعة متنوعة، يمكن استخدام مختلف تقنيات النمذجة وترشيح بايز (Bayesian) والشبكات العصبية والتكنولوجيات الأخرى المتعلقة باستخراج البيانات، وهذا الأمر يحتاج إلى البيانات لحساب احتمالات الاحتيال.

والشبكات العصبية التي تعمل بصورة جيدة في البطاقات الائتمانية الحالية قد لا تعمل بشكل جيد في فضاء الإنترنت نظراً لحاجتها إلى كميات كبيرة من البيانات لتتمكن من كشف أنماط الاحتيال. وبالتالي، ففيما يتعلق بالمعاملات القائمة على الويب، يستخدم نظام كشف الاحتيال تقنيات نمذجة بديلة، مثل ترشيح بايز، تحتاج إلى قدر أقل من البيانات لحساب احتمالات الاحتيال أو الكشف القائم على القواعد فحسب. وتولد نماذج كشف الاحتيال تقديرات للمخاطر يمكن تلقيمها في مجموعات قواعد التطبيقات ومن ثم حفظها وتحديثها من قبل المؤسسة/المنظمة.

3.8 قدرات الاستجابة

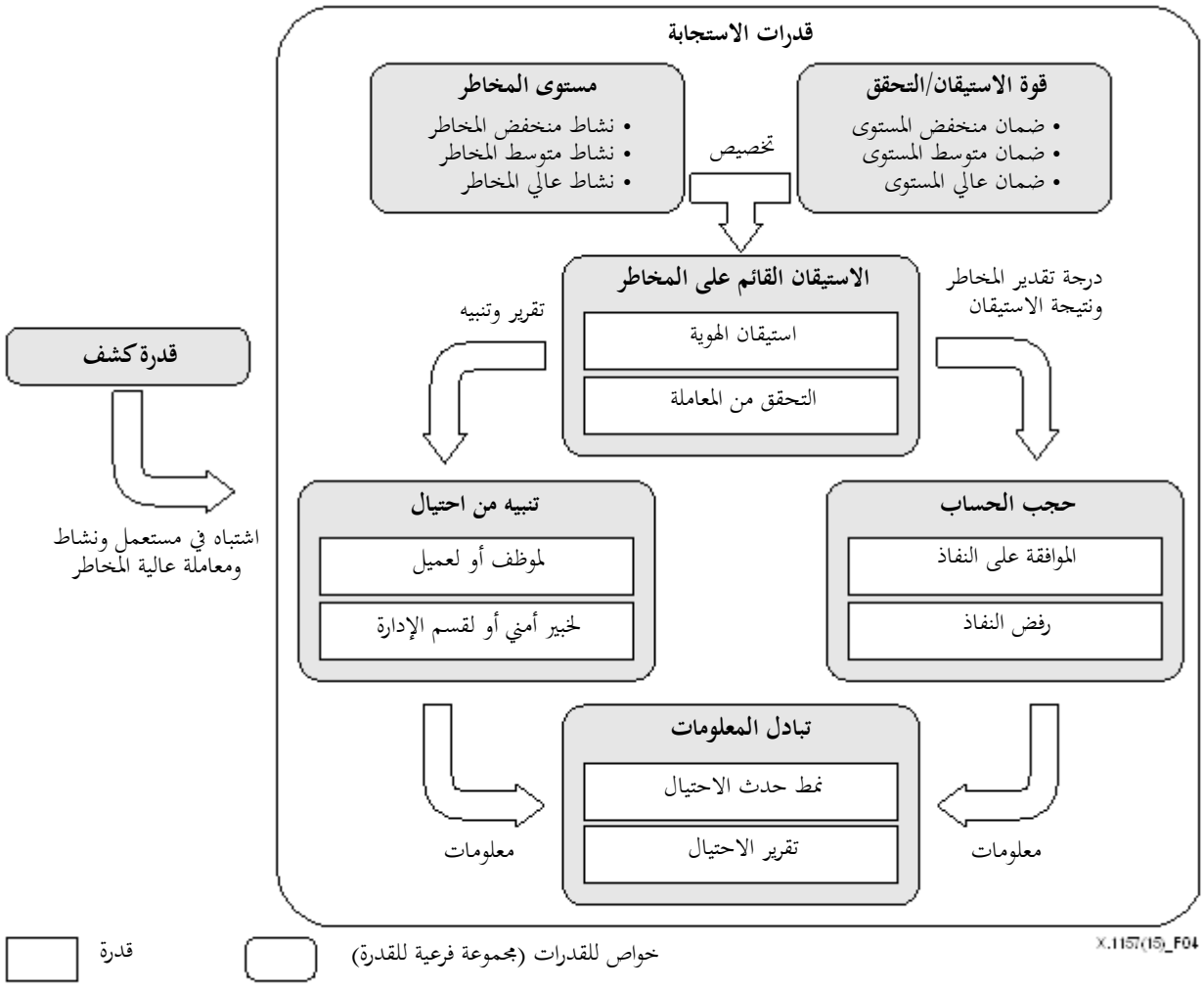
يتطلب نظام كشف الاحتيال إطلاق تنبيهات تتعلق بالاحتيال بشكل أوتوماتي، وإلغاء حسابات، ومضاعفة التحقق من مقدم الطلب لمعاملة معينة تمّ وسمها بأنها مشبوهة وينبغي التصدي لها. ويتعين على جميع طلبات الحسابات الإلكترونية أو المعاملات المجهولة الهوية المعرّضة لخطر عالٍ أن تجتاز مجموعة من إجراءات الفرز الأولية، بدءاً من أحداث تتعلق بالاستيقان نتيجة إجراء تدقيق الهوية الأولي وحتى استخدام التطبيق وسجلات التطبيق. ويتضمن إجراء الفرز الأولي الكشف الأساسي عن الاحتيال من قبيل تحديد هوية جهاز العميل والتحقق من بيانات الهوية الأساسية مثل الاسم والبريد الإلكتروني وتحليل الموقع الجغرافي، والتحقق من صلاحية رقم الهاتف، والكشف على زيف بطاقة الائتمان، والتحقق من تقرير مكتب الائتمانات و/أو تقدير الهوية.

ويتعين تحويل المعاملات المشبوهة التي لا تجتاز الخطوات الأولية من عملية تدقيق الهوية الى فريق التحقيق في الاحتيال، ووضعها في صف انتظار من أجل إجراء فرز إضافي يدوي أو آلي لها. وبعد ذلك، يمكن لنظام كشف الاحتيال أن يستخدم النهج القائم على المخاطر ونهج الطبقات لتدقيق الهوية الذي من شأنه تعزيز التعرف الدقيق على الهوية إذا ما طُلب من المستعملين المشبوهين والمعاملات المشبوهة عالية الخطورة اجتياز عملية الفرز الإضافية.

التحقق المضاعف من مقدمي الطلبات

يستطيع نظام كشف الاحتيال أن يدمج آلية الاستيقان بحيث تتمكن درجة تقدير المخاطر التي تولدت عن نظام الاحتيال من تحديد مدى قوة الاستيقان من المستعمل أو التحقق من معاملات المستعملين. وهو يعرض الخطوات التي يمكن اتخاذها للتخلص من المعاملات المشبوهة أو غيرها من المعاملات عالية الخطورة التي تحتاج الى تدقيق الهوية. ومن أجل التقليل إلى الحد الأدنى من التكاليف وتعظيم التسهيلات للزبائن، يمكن أن تتبع الشركات نهجاً قائماً على المخاطر تكون فيه قوة الحلول المتعلقة بتدقيق الهوية متماشية مع الخطر الكامن في المعاملة. ولهذا الغرض، يمكن لنظام كشف الاحتيال أن يستخدم تطبيقات متعددة مجمعة لتدقيق الهوية يرد وصفها في التوصية [ITU-T X.1154].

وعموماً، لا يتوفر في الأسواق تطبيق فريد وشامل لتدقيق الهوية. ومع ذلك، ثمة عدد من آليات تدقيق الهوية المتاحة للتداول التجاري التي يمكن الجمع بينها لتوفير وسيلة ردعٍ فعالة للمحتالين.



الشكل 4 – قدرات الاستجابة في نظام كشف الاحتيال

الاستيقان القائم على المخاطر

كلما ازداد الخطر، كما يحدد ذلك على سبيل المثال نظام كشف الاحتيال، ارتفعت تكاليف تدابير تدقيق الهوية بالنسبة للعملاء وأصبحت أكثر إزعاجاً. وهناك عدة نهج متاحة يكون فيها الاستيقان الأقوى ضرورياً، فعلى سبيل المثال:

- يتم إنشاء النفاذ الأولي للحساب لتفعيل نشاط متدني الخطورة، مثل النفاذ إلى معلومات عامة مخصصة للقراءة فقط، الأمر الذي يتطلب تدقيقاً أساسياً جداً في الهوية. فيمكن لآلية تدقيق الهوية مثلاً أن تدقّق في اسم المستعمل وعنوانه البريدي في مصدر ثانوي؛
- يتم تأخير نشاط أعلى خطورة، مثل تحديث عنوان بريدي، إلى أن يتم تدقيق الهوية بشكل أقوى (انظر التوصية [b-ITU-T X.1254]) إلى جانب إجراء الكشف عن الاحتيال. ويتضمن ذلك الاستيقان الذي يوفر مستوى أعلى من الضمان؛
  - يمكن لآلية تدقيق الهوية أن تتحقق من معلومات شخصية في قاعدة بيانات مصدر عام باعتماد الاستيقان القائم على المعرفة. ويضم هذا النوع من التحقّق المعلومات المتاحة للجمهور من قبيل البيانات الديمغرافية وسجلات رُخَص القيادة، وبيانات الائتمانات؛
  - قد تطلب آلية تدقيق الهوية من المستعمل أن يجيب على سؤال أو أكثر من أسئلة التحدي التي إما أن تكون قد تمت الإجابة عنها مسبقاً أو مخزونة في البيانات العامة للمستعمل أو مستندة إلى معلومات يعرفها صاحب الحساب الأصلي؛
  - يمكن لآلية تدقيق الهوية أن تستخدم أساليب استيقان في قنوات بديلة من قبيل الهاتف الخلوي أو البريد الإلكتروني للاتصال بصاحب الحساب. وفي وسع آلية تدقيق الهوية أيضاً إرسال كلمة مرور لمرة واحدة إلى مستعمل جديد على الشبكة عن طريق المهاتفة الصوتية أو رسالة نصية قصيرة (SMS) إلى رقم الهاتف المسجل بالفعل في سجل المؤسسة أو الذي يكون قد شكل أحد المدخلات التي يضعها المستعمل في طلب حساب جديد أو في صفحة المدفوعات؛
- الأنشطة الأشد خطورة، من قبيل تحويل الأموال إلى حساب مصرفي خارجي موصول، تعتبر محظورة إلى أن يتم الاتصال بالمستعمل للتحقق من الأمر؛ ومع ذلك، بما أن الكثير من المعاملات تنفّذ على دفعات (بدلاً من الوقت الفعلي)، فقد لا يؤدي هذا النهج إلى تغيير موعد تنفيذ المعاملة.

التنبيه من الاحتيال

إن التنبيه من الاحتيال يعني توليد تنبيه آلي/يدوي لدى الكشف عن نشاط مشكوك فيه. ويكون التنبيه من الاحتيال عادة ناتجاً عن الجمع بين درجة تقييم المخاطر وبعض القواعد التي تعمل على أساس هذه الدرجة. وتتضمن التنبيهات المفصلة نعوت المعاملات وأوصاف النشاط ويمكن الإبلاغ عنها بواسطة البريد الإلكتروني وجهاز استدعاء يمكن تشكيله بحسب القاعدة والخطورة وإدارة المستعملين. ويمكن إرسال التنبيهات المتعلقة بالاحتيال إلى خبير أمني أو إلى عميل/مستعمل وفقاً للمستوى المقيس للخطورة. ومن ثَم يستطيع الخبير الأمني التحقيق في الخطر المتصور بمزيد من الإسهاب، في حين يمكن استخدام التنبيه الموجه الى العميل/المستعمل من أجل تنبيه المقرضين المحتملين بأن الهوية التي تخصهم يحتمل أن تكون قد تعرضت للسرقة.

إلغاء الحسابات

يطبّق إلغاء الحسابات على حسابات المستعملين لدى الكشف عن نشاطات مشبوهة. ويمكن السماح للمستعمل بالنفاذ أو منعه من ذلك على أساس الدرجة المخصصة وحدود تساهل المؤسسة. فالمستعلمون الذين لا يحرزون درجات كافية تخولهم النفاذ التام يمكن السماح لهم بالنفاذ المحدود أو يطلب منهم توفير استيقان أقوى من أجل الحصول على نفاذ تام أو السماح لهم بتنفيذ معاملات معينة عالية الخطورة. فإن لم يفِ المستعملون بهذه المتطلبات، يمكنهم البدء من جديد بإجراء التحقّق المضاعف أو يتم حذفهم فوراً.

تبادل المعلومات

ينبغي لأنظمة كشف الاحتيال أن تضمن قيام النظام بفعالية بتنظيم أجزاء من أنشطته المتعلقة بالتصدي للحوادث مع الشركاء المناسبين في المنظمة.

ويتمثل الجانب الأهم لتنسيق التصدي للحوادث في تبادل المعلومات، حيث تتبادل منظمات مختلفة التهديدات والهجمات والمعلومات المتعلقة بمواطن الضعف فيما بينها بحيث تستفيد كل منظمة من المعارف التي تملكها المنظمة الأخرى. كما يمكن أن يجري تبادل المعلومات مباشرة بين المؤسسات والعملاء أو بين المنظمات والموظفين، وذلك لأن التهديدات والهجمات ذاتها تؤثر في الغالب في منظمات أو خدمات متعددة بشكل متزامن. والغرض من تبادل المعلومات هو تمكين المنظمة التي كشفت حالة احتيال معينة من تبادل هذه المعلومة، إما على نطاق داخلي أو مع المنظمات التي يحتمل أن تقع ضحية للاحتيال.

وفي استطاعة المنظمة المتلقية استخدام هذه المعلومات، مثلاً لإرساء استعراض يدوي للمعاملات المستحدثة من عناوين بروتوكول الإنترنت المشبوهة. ويمكن أن يصف التقرير عن الاحتيال معاملات معينة يُعرف أنها أو يعتقد بأنها مزيفة، أو قد يصف نمطاً من السلوك يوحي بأنه يحمل طابعاً احتيالياً.

التذييل I

خدمات تطبيقات تكنولوجيا المعلومات والاتصالات الحسّاسة

(لا يشكل هذا التذييل جزءاً أساسياً من التوصية)

1.I خدمات التمويل الإلكتروني

1.1.I الأعمال المصرفية الإلكترونية والمسائل الأمنية

تسمح الأعمال المصرفية الإلكترونية أو المعاملات المصرفية عبر الإنترنت (e-banking) لعملاء مؤسسة مالية بإجراء المعاملات المالية على موقع إلكتروني آمن تشغله المؤسسة التي قد تكون مصرفاً يتعامل مع الزبائن أو مصرفاً إلكترونياً أو اتحاداً ائتمانياً أو جمعية للخدمات المالية. وللنفاذ إلى مرفق الأعمال المصرفية الإلكترونية لمؤسسة مالية، يجب على العميل الذي لديه إمكانية النفاذ الشخصي إلى الإنترنت أن يسجل نفسه لدى المؤسسة لهذه الخدمة وأن يستحدث كلمة مرور (تحت مسمّيات مختلفة) للتحقق من هوية العميل. ومن أجل النفاذ إلى الخدمة المصرفية الإلكترونية، ينتقل العميل إلى الموقع الإلكتروني للمؤسسة المالية والدخول إلى مرفق المعاملات المصرفية الإلكترونية باستخدام رقم العميل وكلمة المرور. وقد أعدت بعض المؤسسات المالية خطوات أمنية إضافية للنفاذ، ولكن لا يوجد اتساق حيال النهج المعتمد.

ومع أن الاستيقان الواحد من كلمة المرور لا يزال مستعملاً، بيد أنه لا يعتبر بحد ذاته آمناً بشكل كاف للعمليات المصرفية الإلكترونية في بعض البلدان. وتُستعمل طريقتان مختلفتان لضمان الأمن في العمليات المصرفية الإلكترونية.

- نظام رقم الهوية الشخصي/رقم الاستيقان من المعاملة (PIN/TAN) حيث يمثل الرقم PIN كلمة المرور المستخدمة لتسجيل الدخول وتمثل أرقام الاستيقان من المعاملات (TAN) كلمات مرور لمرة واحدة للاستيقان من المعاملات. ويمكن توزيع الأرقام TAN بطرق مختلفة، أكثرها شيوعاً يتمثل بإرسال رسالة بريدية إلى مستعمل العمليات المصرفية الإلكترونية تتضمن قائمة بأرقام TAN. والطريقة الأكثر أمناً لاستعمال أرقام TAN تنفذ بتوليدها حسب الحاجة باستعمال إذنة (تأشيرة) الأمن. وتعتمد أرقام المعاملات المولدة بإذنات على الوقت وعلى سرّ واحد يُخزن في إذنة الأمن (استيقان بعاملين). وعادة ما تتم المعاملات المصرفية الإلكترونية بواسطة نظام PIN/TAN عن طريق متصفح إنترنت يستخدم الوصلات الآمنة لطبقة مقبس آمن (SSL) بحيث تنتفي الحاجة إلى تجفير إضافي؛
- والطريقة الثانية لتوفير أرقام الاستيقان من المعاملات (TAN) إلى مستعمل العمليات المصرفية الإلكترونية هي بإرسال رقم المعاملة المصرفية الحالية إلى الهاتف المتنقل للمستعمل، الذي يعمل في نظام GSM، عن طريق رسالة نصية قصيرة (SMS). ويُورد نص الرسالة في العادة اقتباساً لقيمة المعاملة وتفاصيلها، ولا يكون الرقم TAN صالحاً إلا لفترة زمنية قصيرة. وقد اعتمدت مصارف في الكثير من البلدان، ولا سيما في ألمانيا والنمسا وهولندا، خدمة "SMS TAN" هذه لأنها تعتبر طريقة آمنة للغاية؛
- الأعمال المصرفية الإلكترونية القائمة على التوقيع حيث توقّع جميع المعاملات ويتم تجفيرها رقمياً. ويمكن تخزين مفاتيح توليد التواقيع وتجفيرها على بطاقات ذكية أو في أي وسط للخزن تبعاً للتنفيذ الفعلي.

2.1.I الدفع الإلكتروني والمسائل الأمنية

الدفع الإلكتروني هو تبادل إلكتروني للأموال أو تحويلها من حساب إلى آخر، إما ضمن مؤسسة مالية واحدة أو عبر عدة مؤسسات، وذلك من خلال أنظمة قائمة على الحواسيب.

وقد لا يحظى نظام الدفع الإلكتروني غير المأمون بثقة المستعملين. وتعتبر الثقة أمراً حاسم الأهمية لضمان قبول المستعملين. وتمثل تطبيقات الدفع الإلكتروني تحدياً أمنياً لأنها تعتمد بشكل كبير على أنظمة أساسية في تكنولوجيا المعلومات والاتصالات تخلق أوجه قصور تخل بالمؤسسات المالية والأعمال التجارية ويحتمل أن تلحق ضرراً بالعملاء. ويتعين على النظام الآمن للمعاملات المالية أن يفي بالمتطلبات التالية:

- السلامة والترخيص/التخويل: تُعرّف السلامة بأنها دقة واكتمال وصلاحية المعلومات وفقاً للقيم والتوقعات التجارية. وتعني سلامة أنظمة الدفع عدم أخذ مبالغ نقدية من المستعمل إلا بعد الحصول على إذن بالدفع منه. وإضافة إلى ذلك قد يطلب المستعملون من مؤسسة مالية عدم استلام أي مدفوعات منهم دون موافقة معلنة من جانبهم؛
- السرّية: تُعرّف السرية على أنها توفير الحماية للمعلومات الحساسة أو الشخصية من الكشف غير المصرح به. وقد يرغب بعض الأطراف المعنيين في ضمان سرية ما يجرونه من معاملات. وتعني السرية في هذا السياق حصر المعرفة بشأن أجزاء مختلفة من المعلومات المتصلة بمعاملة معينة من قبيل هوية الدافع/المدفوع له، ومحتوى الشراء، والمبلغ ونحو ذلك. وفي معظم الحالات، يبدي المشاركون المعنيون رغبة في التأكد من بقاء اتصالاتهم خاصة؛
- التوافر والموثوقية: التوافر هو ضمان أن تكون أنظمة المعلومات والبيانات جاهزة للاستعمال عند الحاجة إليها. وغالباً ما يتم التعبير عن ذلك بوصفه النسبة المئوية من الوقت الذي يمكن فيه استخدام النظام من أجل تأدية عمل منتج. ويتطلب جميع الأطراف القدرة على الدفع أو استلام المدفوعات كلما دعت الحاجة إلى ذلك.

2.I خدمات الرعاية الصحية الإلكترونية

تقدم الرعاية الصحية الإلكترونية (e-healthcare)، التي تهدف إلى إدارة جميع الأنشطة في مؤسسات الرعاية الصحية دون استخدام الورق، الكثير من الوعود بشأن تسريع البيروقراطية النمطية السائدة في الرعاية الصحية في المراكز الطبية والمستشفيات. ومع ذلك، فإن الواقع الذي يواجهه التنفيذ السليم للرعاية الصحية الإلكترونية يتضمن الكثير من القضايا الأمنية. فمن أجل اعتماد المستشفيات للرعاية الصحية الإلكترونية على نطاق واسع، من الضروري إجراء تقييم مفصّل لقضايا الأمن، وتهيئة الظروف لتقييس مختلف المكونات من أجل سلامة تنفيذ الرعاية الصحية الإلكترونية. وقد يتألف نظام نموذجي للرعاية الصحية الإلكترونية من الكثير من العناصر والأنظمة الفرعية، من قبيل المواعيد وبرمجة المواعيد، وإدخال المرضى إلى المستشفى وخروجهم ونقلهم، وملء نماذج الوصفات الطبية، وتخطيط النظام الغذائي، والملاحظات السريرية الروتينية، والنماذج المتعلقة بالمختبرات والتصوير الشعاعي، وأرشفة الصور، والتسجيل للدخول باعتماد البطاقات الذكية. ويعتبر كل من هذه الأنظمة الفرعية معرضاً للتهديدات الأمنية.

1.2.I القضايا الأمنية في مجال خدمات الرعاية الصحية الإلكترونية

- التهديدات التي تتعرض لها خصوصية المعلومات وأمنها: تحدد قاعدة المعارف القائمة بشأن المخاطر الأمنية الأنواع المختلفة من التهديدات التي تواجه خصوصية المعلومات الصحية وأمنها. بيد أن عمليات التصنيف المخصصة الحالية وحدها قد لا تعود بالفائدة على هذا العرف؛
- الشواغل المتعلقة بالخصوصية فيما بين مستهلكي خدمات الرعاية الصحية: مع تزايد الاعتماد على الأنظمة القائمة على الشبكات من أجل إدارة المعلومات الصحية ونشر البنوك الصحية الشخصية، أخذت الشواغل المتعلقة بالخصوصية لدى مستهلكي خدمات الرعاية الصحة تحتل مرتبة الصدارة؛
- قابلية التشغيل البيني للبيانات وأمن المعلومات: تتمثل الفرضية الأساسية لقابلية التشغيل البيني للبيانات في تيسير التبادل الدقيق والسلس للبيانات داخل المنظمات وفيما بينها دعماً لتأمين الرعاية الصحية في الوقت المناسب؛
- قضايا أمن المعلومات الخاصة بالصحة الإلكترونية: لقد شهد قطاع الرعاية الصحية قدراً كبيراً من النمو في استخدام الأجهزة المتنقلة والتطبيقات القائمة على الشبكات. وبصورة متزامنة، تركزت البحوث المتعلقة بأمن المعلومات على تطوير أطر وبروتوكولات لمعالجة القضايا الأمنية في مجال الصحة الإلكترونية.

3.I خدمات النفاذ عن بُعد إلى المؤسسات

يعمل الكثير من موظفي المنظمات والمتعاقدين على استخدام تكنولوجيات النفاذ عن بُعد من أجل تأدية العمل من مواقع خارجية. ويستخدم معظم العاملين الموصولين حاسوبياً تكنولوجيات النفاذ عن بُعد إلى المؤسسات للتواصل مع موارد الحوسبة غير العامة للمنظمة. كما أن طبيعة تكنولوجيات النفاذ عن بُعد إلى المؤسسات – التي تسمح بالنفاذ إلى موارد محمية من شبكات خارجية وكذلك من جهات مضيفة خارجية في الغالب – تضعها عموماً في مواجهة مخاطر تفوق تلك التي تواجه تكنولوجيات مماثلة لا يتم النفاذ إليها إلا من داخل المنظمة، فضلاً عن زيادة الخطر الواقع على الموارد الداخلية التي تتاح للموصولين حاسوبياً من خلال النفاذ عن بُعد للمؤسسة.

1.3.I القضايا الأمنية في النفاذ عن بُعد إلى المؤسسات

إن أكثر الأهداف الأمنية شيوعاً لتكنولوجيات النفاذ عن بُعد إلى المؤسسات هي على النحو الآتي:

- السرية: ضمان عدم تمكن الأطراف غير المرخص لهم من النفاذ عن بُعد للاتصالات والاطلاع على بيانات المستعملين المخزونة؛
- السلامة: الكشف عن أية تغييرات متعمّدة أو غير متعمّدة تطرأ على الاتصالات بالنفاذ عن بُعد أثناء العبور؛
- التوافر: ضمان تمكن المستعملين من النفاذ إلى الموارد من خلال النفاذ عن بُعد كلما دعت الضرورة لذلك.

وتحقيقاً لهذه الأهداف، فإن جميع مكونات حلول النفاذ عن بُعد إلى المؤسسات، بما ذلك أجهزة العملاء، ومخدمات النفاذ عن بُعد، والمخدمات الداخلية التي يتم الوصول إليها عن طريق النفاذ عن بُعد، ينبغي أن تكون مؤمنة ضد مجموعة من التهديدات. وغالباً ما تكون تكنولوجيات النفاذ عن بُعد إلى المؤسسات بحاجة إلى حماية إضافية لأن الطبيعة التي تتسم بها هذه التكنولوجيات تجعلها أكثر عرضة للتهديدات الخارجية من التكنولوجيات التي لا يمكن النفاذ إليها إلا من داخل المنظمات.

ترد الشواغل الأمنية الرئيسية للنفاذ عن بُعد إلى المؤسسات على النحو التالي:

- الافتقار إلى الضوابط الأمنية المادية: تُستخدم أجهزة العملاء للنفاذ عن بُعد إلى لمؤسسات في مجموعة منوعة من المواقع الموجودة خارج حيز سيطرة المنظمة، مثل منازل الموظفين، والمقاهي، والفنادق، وقاعات المؤتمرات. ويزيد الطابع المتنقل الذي تتسم به هذه الأجهزة من احتمال تعرضها للضياع والسرقة، ما يزيد من مخاطر إلحاق الضرر بالبيانات الموجودة في تلك الأجهزة. وحتى وإن كان جهاز العميل في حوزة مالكه بصورة دائمة، فثمة مخاطر أمنية مادية أخرى تتضح في قيام المهاجم باستراق النظر من فوق كتفي العامل الذي ينفذ إلى المؤسسة عن بُعد في مقهى ورؤية بيانات حساسة تظهر على شاشة جهاز العميل؛
- الشبكات غير الآمنة: نظراً لحدوث جميع عمليات النفاذ عن بُعد تقريباً عبر الإنترنت، لا يكون لدى المنظمات في العادة سيطرة على أمن الشبكات الخارجية التي يستخدمها العملاء. وتشمل أنظمة الاتصالات المستخدمة للنفاذ عن بُعد إلى المؤسسات وخطوط الهاتف، وأجهزة المودم DSL، وشبكات النطاق العريض من قبيل الآليات الكبلية واللاسلكية (انظر [b-IEEE 802.11])، وقابلية التشغيل البيني العالمي للنفاذ إلى الموجة الصغرية (WiMAX)، والشبكات الخلوية. وتكون أنظمة الاتصالات هذه عرضة للتنصت مما قد يعرِّض المعلومات الحساسة التي يتم إرسالها أثناء عملية النفاذ عن بُعد إلى المؤسسات للضرر. كما يمكن أن تُشنّ هجمات المتطفلين (MITM) بهدف اعتراض الاتصالات وتعديلها. ومن الممكن التخفيف من حدة مخاطر استخدام الشبكات غير الآمنة، وليس إزالتها، باعتماد تكنولوجيات التجفير لحماية سرية الاتصالات وسلامتها، فضلاً عن استخدام آليات الاستيقان المتبادل للتحقق من هوييتي النقطتين الطرفيتين كلتيهما؛
- الأجهزة المصابة على شبكات داخلية: يتم في الغالب استخدام أجهزة العملاء، ولا سيما الحواسيب المحمولة، على شبكات خارجية ومن ثم تُحضر إلى المنظمة وتُربط مباشرة بالشبكات الداخلية للمنظمة. ويستطيع مهاجم لديه سبل النفاذ المادي إلى جهاز العميل القيام بتركيب برمجيات ضارة على الجهاز لتجميع البيانات منه ومن الشبكات والأنظمة

الموصول بها. فإن كان جهاز العميل مصاباً ببرمجيات ضارة، فقد تعمل البرمجيات الضارة هذه على الانتشار في كامل المنظمة فور توصيل جهاز العميل بالشبكة الداخلية. وإضافة إلى استخدام تكنولوجيات مكافحة البرمجيات الضارة المناسبة انطلاقاً من التشكيلة الأساسية الآمنة للمنظمة، مثل برمجيات مكافحة البرمجيات الضارة على أجهزة العميل، يتعين على المنظمات أن تنظر في استخدام حلول التحكم في النفاذ إلى الشبكة (NAC) التي تتحقق من الوضع الأمني لجهاز العميل قبل السماح له باستخدام شبكة داخلية. وينبغي للمنظمات أيضاً أن تنظر في استخدام شبكة منفصلة لأجهزة العملاء الموصولين حاسوبياً بدلاً من السماح لهم بالتوصيل المباشر بالشبكة الداخلية؛

- النفاذ الخارجي إلى الموارد الداخلية: يوفر النفاذ عن بُعد إلى المؤسسات إمكانية نفاذ جهات خارجية مضيفة إلى موارد داخلية مثل المخدّمات. فإذا لم يكن النفاذ إلى هذه الموارد الداخلية من شبكات خارجية ممكناً من قبل، فإن إتاحتها عن طريق النفاذ عن بُعد سوف يعرضها لتهديدات جديدة، وبوجه خاص من أجهزة وشبكات العملاء غير الموثوقة، مما يؤدي بالتالي إلى زيادة احتمال تضرّرها إلى حد كبير. ومن شأن كل شكل من أشكال النفاذ عن بُعد إلى المؤسسات الذي يمكن استخدامه للنفاذ إلى موارد داخلية أن يعمل على زيادة إلحاق الضرر بتلك الموارد.

بيبليوغرافيا

[b-ITU-T X.1141] التوصية ITU-T X.1141 (2006)، *اللغة التأشيرية للتدعيم الأمني (SAML 2.0)*.

[b-ITU-T X.1154] التوصية ITU-T X.1154 (2013)، *الإطار العام للاستيقان المجمع في بيئات موردي خدمة الهوية المتعددين*.

[b-ITU-T X.1252] التوصية ITU-T X.1252 (2010)، *مصطلحات وتعاريف أساسية تتعلق بإدارة الهوية*.

[b-ITU-T X.1254] التوصية ITU-T X.1254 (2012)، *إطار ضمان استيقان الكيان*.

[b-IEEE 802.11] المعيار IEEE 802.11، *لتكنولوجيا المعلومات – تبادل الاتصالات والمعلومات بين الأنظمة – الشبكات المحلية والحضرية – متطلبات محددة – الجزء 11: مواصفات التحكم في النفاذ إلى الوسط (MAC) والطبقة المادية (PHY) في الشبكات المحلية اللاسلكية*.

سلاسل التوصيات الصادرة عن قطاع تقييس الاتصالات

السلسلة A	تنظيم العمل في قطاع تقييس الاتصالات
السلسلة D	المبادئ العامة للتعريفة
السلسلة E	التشغيل العام للشبكة والخدمة الهاتفية وتشغيل الخدمات والعوامل البشرية
السلسلة F	خدمات الاتصالات غير الهاتفية
السلسلة G	أنظمة الإرسال ووسائطه والأنظمة والشبكات الرقمية
السلسلة H	الأنظمة السمعية المرئية والأنظمة متعددة الوسائط
السلسلة I	الشبكة الرقمية متكاملة الخدمات
السلسلة J	الشبكات الكبلية وإرسال إشارات تلفزيونية وبرامج صوتية وإشارات أخرى متعددة الوسائط
السلسلة K	الحماية من التداخلات
السلسلة L	البيئة وتكنولوجيا المعلومات والاتصالات، تغير المناخ، المخلفات الإلكترونية، كفاءة الطاقة، إنشاء الكبلات وغيرها من عناصر المنشآت الخارجية وتركيبها وحمايتها
السلسلة M	إدارة الاتصالات بما في ذلك شبكة إدارة الاتصالات (TMN) وصيانة الشبكات
السلسلة N	الصيانة: الدارات الدولية لإرسال البرامج الإذاعية الصوتية والتلفزيونية
السلسلة O	مواصفات تجهيزات القياس
السلسلة P	المطاريف وطرائق التقييم الذاتية والموضوعية
السلسلة Q	التبديل والتشوير
السلسلة R	الإرسال البرقي
السلسلة S	التجهيزات المطرافية للخدمات البرقية
السلسلة T	المطاريف الخاصة بالخدمات التليماتية
السلسلة U	التبديل البرقي
السلسلة V	اتصالات البيانات على الشبكة الهاتفية
السلسلة X	**شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن**
السلسلة Y	البنية التحتية العالمية للمعلومات وجوانب بروتوكول الإنترنت وشبكات الجيل التالي
السلسلة Z	اللغات والجوانب العامة للبرمجيات في أنظمة الاتصالات

طُبعت في سويسرا
جنيف، 2016