جامعة دمشق
كلية الاقتصاد
قسم المصارف والتأمين

نظم المعلومات المصرفية

د. ليدا بركات

2023/2022

جدول المحتويات

الفصل الأول: المفاهيم الأساسية في نظم المعلومات..... 2

الفصل الثاني: تقنيات توثيق النظم..... 7

الفصل الثالث: الشبكات..... 13

الفصل الرابع: الصيرفة الإلكترونية..... 20

الفصل الخامس: المخاطر التشغيلية في ظل الصيرفة الإلكترونية..... 33

الفصل السادس: إدارة المخاطر الأمنية..... 42

الفصل السابع: نظم قواعد البيانات 86

الفصل الثامن: تصميم قواعد البيانات 92

الفصل الأول

المفاهيم الأساسية في نظم المعلومات

1-1- مقدمة

الهدف الرئيسي من أي نظام للمعلومات هو تزويد المستخدمين بالمعلومات والبيانات اللازمة لاتخاذ القرارات بمختلف أنواعها وتسيير أنظمة العمليات وإنجازها. تلعب نظم المعلومات دوراً أساسياً في نجاح المصارف وغيرها من المؤسسات والمنظمات من خلال تزويد الإدارة والموظفين بالمعلومات وزيادة سرعة إنجاز العمليات.

يُعرف نظام المعلومات بشكل مبسط على أنه مجموعة من المكونات المترابطة مع بعضها البعض تعمل على جمع البيانات وتحويلها إلى معلومات وإيصال هذه المعلومات إلى المستخدمين.

1-2- مكونات نظام المعلومات

يتضمن نظام المعلومات المكونات التالية:

- المكونات المادية (Hardware)
- البرمجيات (Software)
- البيانات (Data)
- الأفراد (People)

المكونات المادية : الحواسيب والأجهزة الملحقة بها، محطات العمل، وحدات التخزين، شبكات الاتصال وغيرها من التجهيزات المادية.

البرمجيات: مجموعة من التعليمات التي تتولى تشغيل المكونات المادية للنظام والسيطرة عليها، تشمل برمجيات النظم (مثل نظام التشغيل Windows) وبرمجيات التطبيقات (مثل برنامج Microsoft Word).

البيانات: مجموعة من الحقائق أو المشاهدات أو التقديرات غير المنظمة، قد تكون أرقام أو كلمات أو أحرف أو رموز (المادة الخام التي تخضع للمعالجة ونحصل منها على المعلومات).

الأفراد : تتضمن نظم المعلومات نوعين من العاملين:

- المستفدون أو المستخدمون للنظم (مثل العملاء، المحاسبين، موظفي المبيعات)
- المتخصصون في نظم المعلومات (مثل محلل النظم، مبرمج التطبيقات، مدير قاعدة البيانات)

3-1- فعاليات نظام المعلومات (Information System Activities)

يتضمن نظام المعلومات مجموعة من الأنشطة التي يجب القيام بها من أجل الحصول على المعلومات المطلوبة، وهذه الأنشطة هي:

- المدخلات (Input)
- المعالجة (Processing)
- المخرجات (Output)
- تخزين البيانات (Data Storage)
- الرقابة
- التغذية العكسية (Feedback)

المدخلات: تجميع البيانات حول وظائف المصرف الأساسية ومختلف الوثائق والمستندات التي تصور عمليات المصرف مع العملاء والبيئة المحيطة، وإدخال تلك البيانات إلى النظام لتتم معالجتها لاحقاً (على سبيل المثال، تسجيل حركات السحب والايداع التي تمت على حساب العميل) .

المعالجة: القيام بمجموعة من العمليات الحسابية والمقارنة المنطقية وعمليات الفرز والتصنيف على البيانات المدخلة لتحويلها إلى معلومات مفيدة للمستخدم النهائي.

المخرجات: إيصال المعلومات إلى المستخدم النهائي وفق أشكال مختلفة (تقارير، جداول، أشكال بيانية، الخ).

تخزين البيانات: الاحتفاظ بالبيانات والمعلومات وفق طريق منتظمة بما يضمن سهولة استرجاعها (من خلال الاعتماد على نظم قواعد البيانات التي سنتناولها لاحقاً).

الرقابة: وضع مجموعة من الإجراءات والقواعد الرقابية على عمليات الادخال والمعالجة ومقارنة مخرجات النظام بمعايير أداء محددة للتحقق من أن النظام ينتج المعلومات المفترضة عند تصميمه.

التغذية العكسية: قياس رد فعل المستفيدين من عمل النظام لتقويم عمل النظام (قد يقدم النظام المعلومات المفترضة عند تصميمه ولكن بعض المعلومات التي يقدمها لا تلائم حاجات المستفيدين).

1-4- أنواع نظم المعلومات

تقسم النظم في المصرف أو في أي منظمة أخرى إلى عدة أنواع (لا يمكن لنظام واحد أن يوفر كل المعلومات التي تحتاجها المنظمة):

- **نظم دعم العمليات (Operations Support Systems):** الهدف منها مساعدة العمليات اليومية المتعلقة بفعاليات تقديم الخدمات المصرفية المختلفة (على سبيل المثال، توفير البيانات والمعلومات اللازمة لموظف الائتمان لدراسة طلب الحصول على قرض) إلى جانب دعم الوظائف الأساسية الأخرى مثل التسويق، المحاسبة، التمويل، الموارد البشرية
- **نظم دعم الإدارة (Management Support Systems):** الهدف منها مساعدة الاداريين والقياديين من مختلف المستويات على اتخاذ القرارات المناسبة. توجد عدة أنواع من نظم دعم الإدارة (حسب متطلبات كل مستوى إداري):

- نظم المعلومات الإدارية (Management Information Systems)
- نظم دعم القرار (Decision Support Systems)
- نظم المعلومات التنفيذية (Executive Information Systems)

1-4-1- نظم المعلومات الإدارية :الهدف منها تقديم المعلومات (غالباً على شكل تقارير) التي تساعد الإدارة الوسطى في دعم القرارات المتكررة والرقابة وتقويم الأداء (على سبيل المثال، تقديم تقرير توزيع القروض الممنوحة حسب القطاعات الاقتصادية والمناطق الجغرافية) .تعتمد على البيانات الناتجة عن نظم دعم العمليات في إعداد التقارير.

1-4-2- نظم دعم القرار: نظم تفاعلية الهدف منها تقديم المعلومات التي تساعد الإدارة الوسطى والعليا على تقويم بدئل الحل المختلفة لمشكلة فريدة غير متكررة لاختيار الحل الأمثل لها (على سبيل المثال، تحديد موازنة المبيعات) .تعتمد في إنتاج المعلومات على البيانات الداخلية الناتجة عن نظم دعم العمليات ونظم المعلومات الإدارية إلى جانب المصادر الخارجية (على سبيل المثال، أسعار الأسهم في الأسواق المالية، أسعار المنافسين).

1-4-3- نظم المعلومات التنفيذية: الهدف منها دعم الإدارة العليا في اتخاذ القرارات الاستراتيجية (على سبيل المثال، قرارات الاندماج، التنبؤ). تعتمد في إنتاج المعلومات على البيانات الداخلية (البيانات الناتجة عن نظم المعلومات الإدارية ونظم دعم القرار) إلى جانب البيانات الخارجية، وتعرضها على عدة مستويات من الدمج والتلخيص. تتميز بسهولة التعامل المباشر من قبل المديرين مع النظام من خلال واجهة تطبيق (User Interface) مصممة لعرض المعلومات حسب حاجة كل مستخدم من الإدارة العليا (على سبيل المثال، الاستعلامات الفورية عن البيانات التاريخية، عرض التقارير المختلفة على شكل رسوم بيانية).

5-1- مزايا نظم المعلومات في المصارف

- تقديم الخدمات المصرفية على مدار الساعة (أجهزة الصراف الآلي، الصيرفة عبر الهاتف، الصيرفة عبر الإنترنت، الخ)
- التوسع والتنوع في الخدمات المصرفية الحالية
- تحسين نوعية الخدمات المصرفية (تخفيض الزمن اللازم لانجاز الخدمة المصرفية)
- تحسين الإنتاجية في العمل المصرفي (تخفيض التكاليف المرتبطة بانجاز العمليات المصرفية وتحسين كفاءة تقديم الخدمات للعملاء)
- تحسين علاقات العميل مع المصرف (الراحة والسرعة في التعامل مع المصرف)

الفصل الثاني

تقنيات توثيق النظم

Systems Documentation Techniques

2-1- مقدمة

تلعب مراحل توثيق النظم في تحديد كفاءة النظام وفعالية استخدامه وتعديله في فترات لاحقة. تعرف تقنيات تطوير وتوثيق النظم بأنها مجموعة من الأدوات المستخدمة بعملية تحليل وتصميم وتوثيق نظم المعلومات التي تساعد في فهم وتقويم النظام الحالي والمقترح.

2-2- نماذج تقنيات توثيق النظم

- مخطط تدفق البيانات (Data Flow Diagram)
- مخطط سير النظام (System Flowchart)
- مخطط تدفق البرنامج (Program Flowchart)
- مخطط تدفق المستندات (Document Flowchart)

2-2-1- مخططات تدفق البيانات

توصيف بياني لتدفق البيانات ضمن المنظمة: توصيف لمصدر نشوء البيانات و المعالجة التي تتم على البيانات وتخزين البيانات ومقصد نتائج المعالجة .تستخدم أربعة عناصر أساسية:

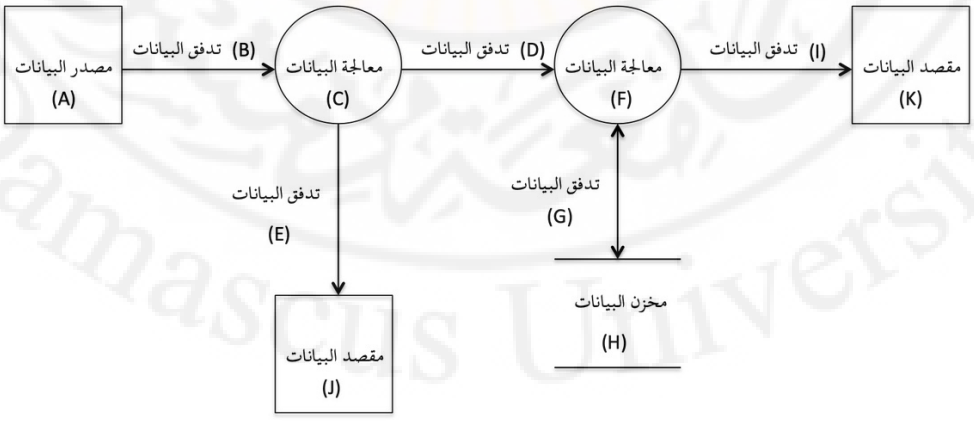
- مصدر البيانات ومقصدها: الكيانات التي ترسل بيانات للنظام أو تستخدم البيانات التي ينتجها النظام

- خط سير البيانات: انتقال البيانات بين المصادر وإجراءات المعالجة والتخزين والمقاصد
- المعالجة: العمليات التي تجري على البيانات أثناء تدفقها خلال النظام
- مخزن البيانات: مستودع لتخزين البيانات (دون الاهتمام بوسيلة التخزين)

2-2-1-1-الرموز المستخدمة في إعداد مخططات تدفق البيانات



2-2-1-2-العناصر الأساسية لمخطط تدفق البيانات



2-2-1-3-مستويات مخطط تدفق البيانات

مخطط تدفق البيانات الدلالي (Context Diagram): الهدف منه معرفة عمل نظام المعلومات بشكل عام، حيث يتضمن كل مصادر البيانات ومقاصدها وعملية معالجة واحدة (يصف النظام مع جميع أنشطته كعملية واحدة). يتم تجزئة المخطط الدلالي إلى عدة مستويات لزيادة التفاصيل المتعلقة بعمليات المعالجة.

مخطط تدفق البيانات المنطقي (Logical Data Flow Diagram): الهدف منه عرض أنشطة النظام دون التعرض إلى التفصيل المادي لبنية النظام (لا يُظهر العاملين أو البرامج المسؤولة عن عملية المعالجة أو أي تفاصيل عن وسائط التخزين).

مخطط تدفق البيانات المادي (Physical Data Flow Diagram): الهدف منه عرض البنية التحتية للنظام (مكان تنفيذ عملية المعالجة، الشخص أو البرنامج الذي ينفذ عملية المعالجة، كيفية تنفيذ المعالجة، مكان تخزين البيانات، التقارير والمستندات التي تتحرك ضمن النظام). يلعب مخطط تدفق البيانات المادي دوراً هاماً عند تحليل وتطوير النظم الحالية.

2-2-2- المخططات التدفقية التحليلية (Flowcharts)

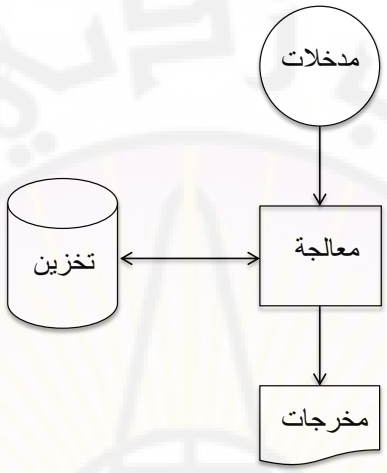
تُستخدم لتوصيف وتحليل بعض عناصر نظام المعلومات بشكل واضح ومختصر ومنطقي .تعتمد على مجموعة من الرموز المعيارية: رموز الإدخال والإخراج، رموز المعالجة، رموز التخزين، رموز سير البيانات ورموز وصل العمليات والمستندات.

2-2-2-1-نماذج المخططات التدفقية التحليلية

- مخططات سير النظام
- مخططات تدفق البرامج

- مخططات تدفق المستندات

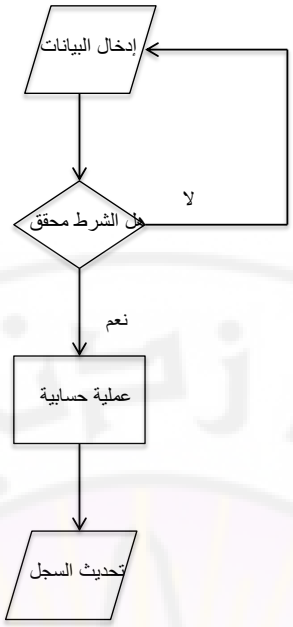
مخططات سير النظام الحاسوبي (Computer Systems Flowcharts**):** تعرض حركة البيانات المعالجة في النظام وتستخدم ثلاثة مكونات: المدخلات، المعالجة والمخرجات. تُستخدم في تصميم وتحليل وتقويم النظم.



الشكل ٢-١: مثال عن مخطط سير النظام الحاسوبي

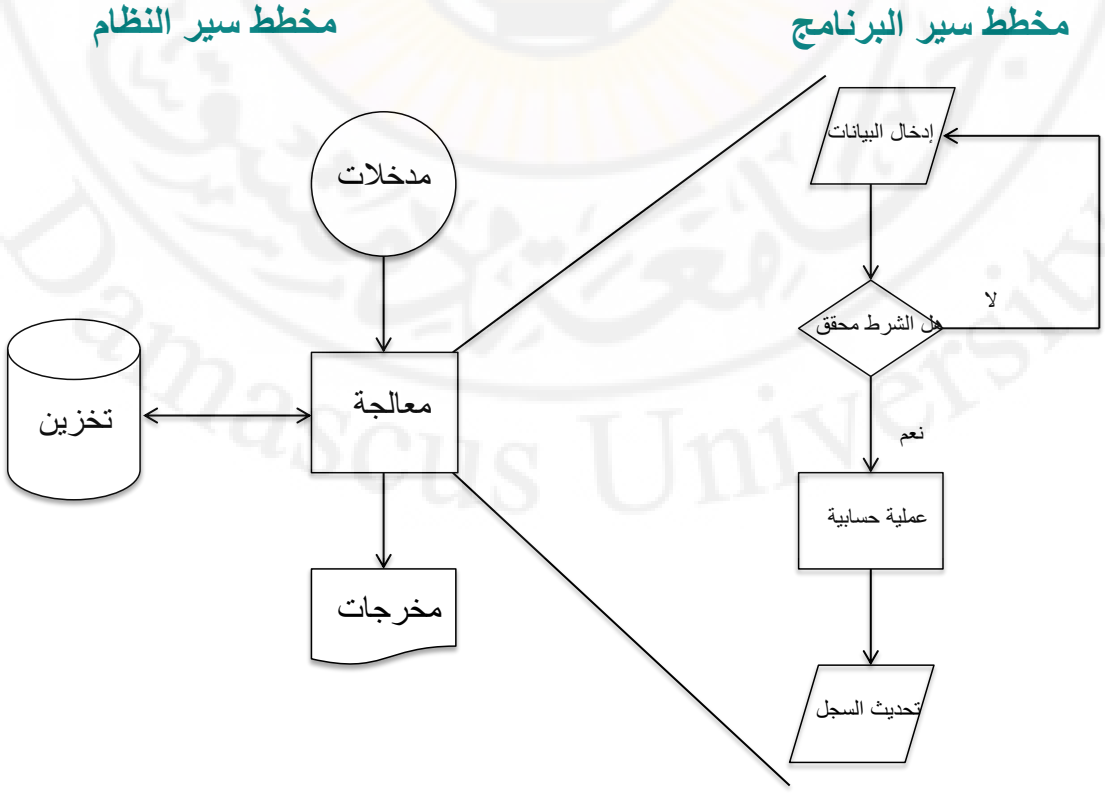
مخططات سير البرنامج (Program Flowcharts): تعرض التتابع المنطقي للعمليات التي يجب أن تنفذ من قبل الحاسب أثناء تنفيذ برنامج معين حيث تستخدم أربعة مكونات:

- الإدخال: لتمثيل أي عملية قراءة للمدخلات
- الإخراج: لتمثيل أي عملية طباعة للمخرجات
- المعالجة: لتمثيل عمليات نقل البيانات والعمليات الحسابية
- القرار وخطوط سير العمليات: لتمثيل المقارنة المنطقية بين متغير أو أكثر التي تحدد اتجاه سير خطوات المعالجة



الشكل ٢-٢: مخطط سير البرنامج لعملية معالجة طلب عميل

العلاقة بين مخطط سير النظام ومخطط سير البرنامج: يقوم مخطط سير البرنامج بتوصيف الخطوات المنطقية لعملية المعالجة المذكورة ضمن مخطط سير النظام



مخططات سير المستندات (Document Flowcharts): تمثل تدفق المستندات والمعلومات بين مواقع المسؤولية داخل المنظمة حيث تعرض مكان إعداد المستندات وتوزيعها والغرض من استخدامها والتصرف النهائي بها. تساعد في تحليل وتقويم إجراءات الرقابة الداخلية للنظام.

الفصل الثالث

الشبكات

Networks

3-1- مفهوم الشبكات

تعرف الشبكات بأنها مجموعة من الحواسيب والتجهيزات المرتبطة مع بعضها من خلال خطوط الاتصال، تسمح بتبادل البيانات والمعلومات بين مستخدمي الشبكة ومشاركة الموارد المختلفة (الطابعات، البرامج التطبيقية، قواعد البيانات، وسائط التخزين، الخ). تشمل المكونات الأساسية للشبكات المكونات المادية و برمجيات الاتصالات.

3-2-المكونات المادية للشبكات

الملقم (Server): حاسب في الشبكة مزود بمجموعة من البرامج مهمتها تقديم البيانات والبرامج المخزنة في الملقم إلى بقية الحواسب ضمن الشبكة

الأجهزة المستضافة (Clients): مجموعة الحواسيب والبرامج التي تدخل إلى البياناتوالبرامج المخزنة داخل الجهاز الملقم

المودم (Modem): جهاز يحول الإشارات الرقمية إلى إشارا تناظرية وبالعكس عند تبادل المعطيات ضمن الشبكة بواسطالهاتف

المحولات (Switches): تعمل على إنشاء ربط ثانوي بين عقدتين (Nodes) ضمن الشبكة ترسل من خلاله كافة المعطيات

الموجهات (Routers): تصل بين شبكتين أو أكثر حيث تقوم بتوجيه حزم البيانات التي تمر من خلالها إلى الشبكة المناسبة باتجاه مقصدها

خطوط الاتصال: الكابلات والخطوط السلكية واللاسلكية التي يتم من خلالها وصل مكونات الشبكة.

3-2-1-وظائف برمجيات الاتصالات

١- الرقابة على الدخول إلى الشبكة

- الرقابة على صلاحيات المستخدم في الدخول إلى الشبكة
- السيطرة على الاتصال مع الشبكة وقطع الاتصال عن الشبكة لمختلف أنواع الأجهزةالمربوطة بها
- إنشاءمؤشرات مختلفة مثل السرعة واتجاه تحويل البيانات

٢- إدارة الشبكة

- استكشاف جاهزية الأجهزة الملحقة بالشبكة لإرسال واستقبال البيانات
- تنظيم صفوف الإنتظار أثناء عمليات الإدخال والإخراج
- تسجيل كل العمليات التي تمت مع الشبكة

٣- السيطرة على نقل البيانات والملفات بين مختلف أجزاء الشبكة

٤- اكتشاف الأخطاء

٥- حماية البيانات أثناء عملية النقل من الدخول غير المصرح به

3-3-نماذج الشبكات

يمكن تصنيف الشبكات حسب السعة والملكية و المسافة التي يمكن أن تغطيها الشبكة جغرافياً والبنية المادية إلى النماذج التالية:

- الشبكة المحلية (Local Area Network)
- الشبكة العريضة (Wide Area Network)
- الشبكة المضيفة للقيمة (Value-Added Network)
- الإنترنت (Internet)
- الإنترانت (Intranet)
- الإكسترانت (Extranet)

الشبكة المحلية: مجموعة من الحواسيب والتجهيزات الأخرى التي تتوضع بالقرب من بعضها بحيث يكون الاتصال مغلقاً بين حواسيب الشبكة. تتمتع الشبكة المحلية بمجموعة من المزايا:

- السرعة في نقل البيانات والدخول إلى الشبكة
- فعالية السيطرة على الدخول إلى الشبكة
- سهولة ربط عدد كبير من الحواسب والمستخدمين
- تكاليف التشغيل والصيانة منخفضة نسبياً

الشبكة العريضة: تغطي منطقة جغرافية كبيرة مثل مدينة أو دولة أو عدة دول

الشبكة المضيفة للقيمة: شبكات للاتصال بين المسافات البعيدة التي تمكن الشركات من تبادل الشبكات الخاصة بالشركات المختلفة

الإنترنت: نظام من الشبكات الحاسوبية (حكومية، تجارية، عامة، خاصة) المرتبطة مع بعضها التي تستخدم بروتوكول TCP/IP لخدمة المستخدمين عالمياً

الإنترانت: يتم تشغيله ضمن شبكات الحاسب الداخلية للشركات وهو عبارة عن إنترنت آمن ومصغر مؤسس على معايير الشبكالعامة

الإكسترانت: شبكة آمنة تسمح للأطراف الخارجية بالوصول إلى شبكة الإنترانت الخاصة بشركة معينة

3-4-التراكيب البنيوية للشبكات (Network Topologies)

تحدد آلية ربط مكونات الشبكة مع بعضها للاستفادة من موارد الشبكة بكفاءة وفعالية .

يتأثر تحديد التراكيب البنيوية للشبكة بالعوامل التالية:

- الحماية عند توقف الشبكة أو أحمكوناتها عن العمل
- إمكانية إضافة مكونات جديدة إلالشبكة
- سرعة نقل المعطيات بين مكونات الشبكة
- طريقة الوصول إلىالشبكة
- تكاليف بناء الشبكة

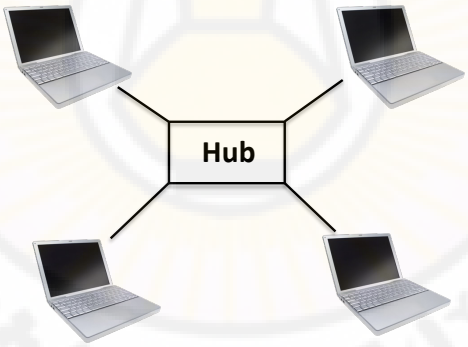
3-4-1-نماذج التراكيب البنيوية للشبكات

- هيئة النجمة (Star Topology)
- هيئة الحلقة (Ring Topology)
- هيئة الحافلة (Bus Topology)
- هيئة الشجرة (Tree Topology)
- هيئة الشبكة (Mesh Topology)
- الهيئة الهجينة (Hybrid Topology)

هيئة النجمة: يتم ربط كل حواسيب الشبكة من خلال عقدة مركزية (الموزع (Hub) أو المحول) وتعتبر من أسهل الهيئات في التصميم وأكثرها استخداماً.

المزايا: سهولة الصيانة - سرعة نقل البيانات - سهولة الرقابة والتشغيل والصيانة.

العيوب : تكاليف التأسيس عالية - تحتاج إلى كميات كبيرة من الأسلاك.

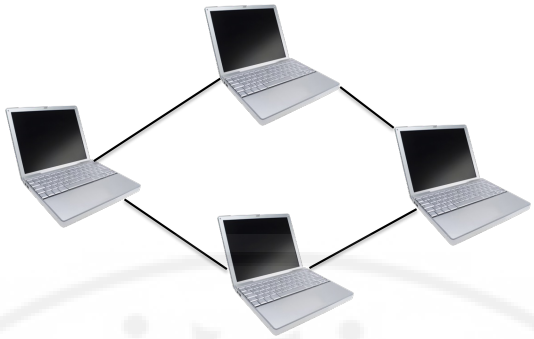


الشكل ٣-١: هيئة النجمة

هيئة الحلقة: ترتبط كل عقدة (المخدم، الجهاز المستضاف، الخ) من عقد الشبكة مع العقد الأخرى حيث تمر البيانات من خلال كل عقد الشبكة.

المزايا: استمرار عمل النظام عند تعطل أحد العقد.

العيوب: تكاليف الصيانة والسيطرة عالية نسبياً.



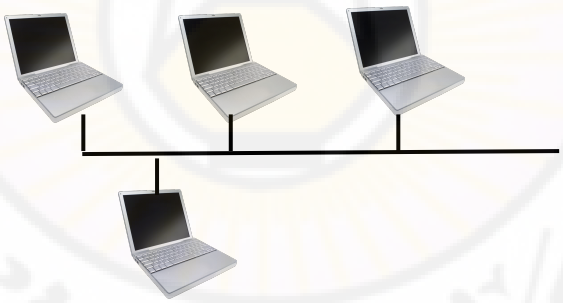
الشكل ٣-٢: هيئة الحلقة

هيئة الحافلة: ترتبط أجهزة الشبكة من خلال خط واحد مركزي

المزايا:

- التكلفة المنخفضة عند إضافة جهاز جديد إلى الشبكة
- تكاليف تأسيسها منخفضة بالنسبة للهيئات الأخرى

العيوب: ضعف الأداء مع توسع الشبكة



الشكل ٣-٣: هيئة الحافلة

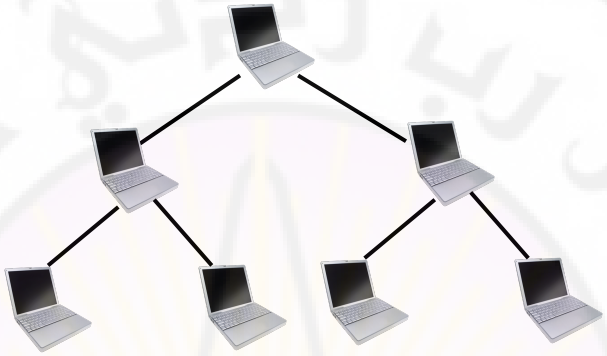
هيئة الشجرة: تتكون من عقدة مركزية ترتبط بها باقي مكونات الشبكة بشكل هرمي.

المزايا:

- سهولة إضافة مكونات جديدة إلى الشبكة
- سهولة إدارة وصيانة الشبكة
- سهولة اكتشاف الأخطاء

العيوب:

- تحتاج إلى كميات كبيرة من الأسلاك
- ارتفاع تكاليف الصيانة مع توسع الشبكة
- توقف الشبكة عند تعطل العقدة المركزية



الشكل ٣-٤: هيئة الشجرة

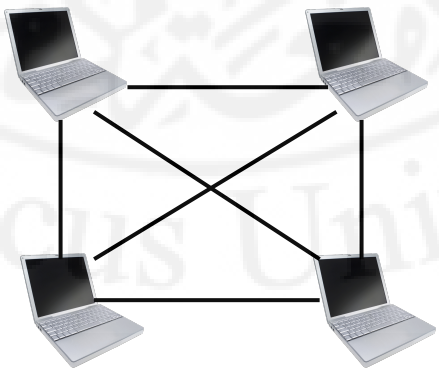
هيئة الشبكة: ترتبط كل عقدة في الشبكة بالعقد الأخرى.

المزايا:

- سهولة اكتشاف الأخطاء
- توفر الأمن والخصوصية(Privacy)

العيوب :

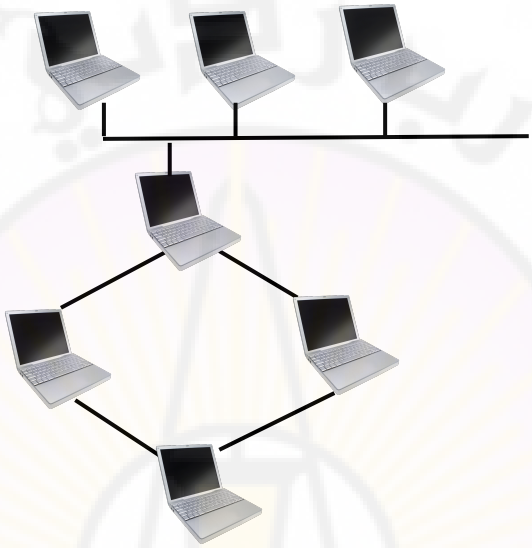
- تكاليف التأسيس عالية
- تحتاج إلى كميات كبيرة من الأسلاك



الشكل ٣-٥: هيئة الشبكة

الهيئة الهجينة: تجمع بين عدة هيئات في شبكة واحدة (مثال: الجمع بين هيئة الباص وهيئة الحلقة).

المزايا: سهولة اكتشاف الأخطاء ومعالجتها - المرونة وسهولة توسيع الشبكة



الشكل ٣-٦: الهيئة الهجينة

الفصل الرابع

الصيرفة الإلكترونية

4-1- مقدمة

تأثرت الصناعة المصرفية خلال العقود القليلة الماضية بالتطور المستمر الحاصل في تكنولوجيا المعلومات والاتصالات، حيث اعتمدت المصارف في تقديم منتجاتها وخدماتها على قنوات اتصال الكترونية تفاعلية مثل أجهزة الصرف الآلي (ATMs)، والحواسيب الشخصية (PC's)، والهواتف النقالة، الخ، استطاعت المصارف من خلالها تقديم المنتجات والخدمات المصرفية التقليدية (الوصول إلى المعلومات المالية، الحصول على القروض، فتح الحسابات الايداعية، الخ)، إلى جانب منتجات وخدمات جديدة نسبياً مثل خدمات دفع الفواتير الالكترونية. ساعد ذلك المصارف على تمييز منتجاتها وخدماتها في البيئة التنافسية العالية التي تواجهها.

4-2- تعريف الصيرفة الإلكترونية

تُعتبر الصيرفة الإلكترونية (E-banking) من أحدث الوسائل في تقديم الخدمات والمنتجات المصرفية، وهي تتكون من الأنظمة التي تسمح لعملاء المصرف (سواء الأفراد أو المؤسسات) بالوصول إلى حساباتهم المصرفية، وتنفيذ المعاملات المالية، والحصول على المعلومات المتعلقة بالخدمات والمنتجات المصرفية عبر شبكة عامة أو خاصة ومن ضمنها شبكة الإنترنت.

تجدر الإشارة إلى أنّ مصطلح الصيرفة الإلكترونية ليس مرادفاً لمفهوم الصيرفة عبر الإنترنت، بالرغم من أنّ الأخير هو النوع الأكثر انتشاراً للصيرفة الإلكترونية، حيث تتضمن الصيرفة الإلكترونية العديد من قنوات الوصول المختلفة التي سيتم تناولها لاحقاً من خلال بيان أنواع الأعمال المصرفية الإلكترونية.

يمكن تعريف الصيرفة الإلكترونية على أنّها التسليم الآلي المباشر للخدمات والمنتجات المصرفية التقليدية والمبتكرة عبر قنوات اتصال إلكترونية تفاعلية، حيث

يتمكن العملاء الوصـــول إلى الخدمات المصـــرفية الإلكترونية باســـتخدام وســـيلة إلكترونية ذكية مثل الحاسب الشخصـي أو الهاتف الخليوي أو جهاز الصـرف الآلي (Automated Teller Machine ATM) أو الهاتف الخليوي أو غيرها من الوسائل.

3-4- أهمية الأعمال المصرفية الإلكترونية

في الواقع، فإن التغيير الذي حدث في الصـناعة المصـرفية على الصـعيد العالمي في ظل التوسـع الملحوظ في اسـتخدام التكنولوجيا الحديثة قد حقق للمصـرف ولعملائه مزايا عديدة أبرزها:

- ارتفاع كفاءة إدارة المصرف وزيادة ربحيته نظراً للانخفاض الكبير الحاصل في تكاليف التشـــغيل، فقد تحول فرع المصـــرف التقليدي إلى قناة نشـــيطة تُستخدم في تسويق وبيع جميع منتجات وخدمات المصرف المتنوعة وبالتالي تقل الحاجة إلى الفروع والموظفين.
- تقديم خدمات مصـرفية جديدة مثل خدمة تجميع الحسـاب للعميل وخدمة دفع الفواتير الإلكترونية.
- حواجز أقل لدخول الصـــناعة المصـــرفية، نظراً لأنّ الحاجة لفروع فعلية تصبح أقل، كما تتضاءل الحاجة للمصروفات الرأسمالية الضخمة لإقامة هذه الفروع.
- إمكانية تســـويق المنتجات المصـــرفية خارج حدود الدولة الأم، لأنّ العمل المصـــرفي الإلكتروني لا يعرف الحدود الجغرافية للدول وبالتالي إمكانية الوصـــول إلى قاعدة أعرض من العملاء المودعين والمقترضـــين وطالبي الخدمات المصرفية.
- خيارات أكثر بالنسبة للعملاء، لأنّ العمل المصـرفي الإلكتروني يتيح للعملاء إمكانية المقارنة بين المصـــارف وخدماتها ومنتجاتها ومعدلات العائد على استثمار أموالهم بشكل أفضل وأسرع.
- الوصـول السـريع للخدمات على مدار السـاعة ومن أي موقع وبالتالي ارتفاع الراحة والملاءمة بالنسبة للعملاء.

4-4- أنواع الأعمال المصرفية الإلكترونية

بشكل عام يمكن أن يتم تصنيف الأعمال المصرفية الإلكترونية وفقاً لقنوات الوصول إلى الخدمات المصرفية إلى ثلاثة أنواع رئيسية هي: الصيرفة عبر الحواسيب الشخصية المربوطة بالنظام المصرفي من خلال الشبكات الداخلية والخارجية، والصيرفة عبر الهاتف، والصيرفة عبر أجهزة الصرف الآلي.

4-4-1- الصيرفة عبر الحواسيب الشخصية (PC Banking)

يمكن تقسيمها إلى الصيرفة عبر الإنترنت (Internet Banking)، والصيرفة عبر الحاسب المنزلي (Home Banking).

الصيرفة عبر الإنترنت

تُشير الصيرفة عبر الإنترنت إلى أنّ الخدمات المصرفية مثل التعريف عن الخدمات والحصول على القروض والاستعلام عن رصيد الحساب وتحويل الأموال وغيرها يتم توفيرها من قِبل المصرف عبر شبكة الإنترنت.

هناك نوعان أساسيان لمواقع المصرف الإلكترونية، هما الموقع المعلوماتي والموقع التعاملي.

1- الموقع المعلوماتي (Informational Website): يّقدم هذا الموقع معلومات عامة عن المصرف وعن المنتجات والخدمات التي يقدمها، حيث يقوم المصرف عن طريقه بتسويق هذه المعلومات عن طريق مخدّم مستقل (Server) لا يملك منفذاً إلى الشبكة الداخلية للمصرف، وبالتالي يمكن أن يتم تقديم هذا المستوى من الصيرفة عن طريق المصرف أو من مصدر خارجي.

يُعتبر الموقع المعلوماتي للمصرف شكلاً من أشكال الدعاية الإعلامية، وبالتالي لا يمكن للمصرف أن يقوم بتقديم أي نوع من الخدمات لعملائه عن طريقه.

2- الموقع التعاملي /التفاعلي (Transactional Website): يتيح هذا المستوى للعملاء إمكانية إنجاز العمليات المصرفية والتي يمكن أن تتضمن مختلف أنواع العمليات بدءاً من أبسط العمليات مثل الاستعلام عن الرصيد إلى عمليات التحويل المالية الكبرى التي تتم لأهداف تجارية.

الصيرفة عبر الحاسب المنزلي

تمكّن الصيرفة عبر الحاسب المنزلي (Home Banking) العميل المصرفي من إدارة حسابه من حاسبه الشخصي من مكان محدد مسبقاً من المنزل أو من مكتب العمل، وهي تُتيح مختلف أنواع الخدمات مثل الاستعلام عن الرصيد وتحويل الأموال من حساب إلى آخر والكشف عن الحساب وغيرها من الخدمات المشابهة للخدمات المتاحة للصيرفة عبر الإنترنت التي تُعتبر تطويراً لهذا النوع من الصيرفة.

يتكون هذا النظام من قسمين: برنامج في حاسب العميل وبرنامج في الحاسب المصرفي الذي يعمل كمخدّم للتواصل، حيث يستقبل الاتصالات من العملاء ويتأكد من هويتهم الشخصية ويتلقى منهم المعطيات ويصدّق على التواقيع الرقمية ويولّد إيصالات رقمية ويرسل المعطيات للعملاء.

يتطلب هذا النوع من الصيرفة أن يقوم العملاء بتحميل حزمة البرمجيات المحددة من قِبل المصرف على حواسبهم الشخصية، بحيث يتمكنون من تنفيذ عملياتهم المصرفية فقط على الحواسيب الشخصية التي تحتوي على حزمة البرمجيات المحددة، ومن أمثلة تلك البرمجيات Intuit و Inc's Quicken. بينما الصيرفة عبر الإنترنت تعتمد فقط على المتصفح (Browser)، مثل MS Explorer و Netscape Navigator، وبالتالي فهي لا تتطلب من العملاء تحميل أي برمجيات بما يمكّن العميل من الوصول إلى الخدمات المصرفية عبر أي حاسب يملك منفذاً إلى شبكة الإنترنت.

4-4-2-الصيرفة عبر الهاتف

يمكن تقسيمها إلى الصيرفة عبر الهاتف الثابت والصيرفة عبر الهاتف الجوال.

الصيرفة عبر الهاتف الثابت

تمكّن الصيرفة عبر الهاتف الثابت (Phone Banking) العملاء من الحصول على المعلومات المتعلقة بالمنتجات المصرفية التفاعلية (عمليات السحب والإيداع) وغير التفاعلية (الاستعلام عن الرصيد، التحويلات من حساب لآخر، إصدار دفتر الشيكات، الخ)، إلى جانب إمكانية استخدام نظام الدفع المصرفي مثل تحرير أمر السداد أو أمر التحصيل، فتح أو إلغاء الوديعة لأجل أو الحساب الجاري، طلب الحصول على قرض، شراء الاستثمارات المالية وبيعها وغيرها من الخدمات التقليدية التي كانت متاحة عن طريق الفرع فقط، حيث يعمل الفاكس المتصل بالهاتف كمخرج لقناة التواصل.

إن الميزة المرتبطة بهذه الخدمة هي أنها لا تتطلب أي أدوات تقنية إضافية سوى الهاتف، حيث يتصل العميل باستخدام الخط الهاتفي الكلاسيكي برقم محدد مسبقاً ويتبع إما تعليمات المجيب الآلي أو موظف في المصرف يدعى مستشار العميل (Client Advisor) المؤهل بإمداد العميل بالمعلومات المتعلقة بالمنتجات والخدمات المصرفية الذي يقوم (أي مستشار العميل) بعد عملية التحقق (Verification) والتأكد من هوية الشخص الذي يتحدث معه بتنفيذ أي عملية تفاعلية وغير تفاعلية، إلى جانب قدرته على تقديم الاستشارة للعميل، وعرض منتجات مصرفية إضافية.

نظراً لحصول المستشار على أجر من المصرف، فإنّ التكاليف والرسوم المرتبطة بهذه الخدمة تكون مرتفعة عادةً، ولذلك، قد تقوم المصارف أحياناً بإنشاء نظام الهاتف المؤتمت (Automated Telephone System) الذي يعمل على أساس قائمة يمكن للعميل التحرك خلالها باستخدام الأزرار الموجودة على هاتفه. هذه القائمة التي يقدمها النظام تكون مصممة بشكل مبسط بحيث لا يستغرق تنفيذ الخيار وقتاً طويلاً، وعندما يحتاج العميل إلى كمية كبيرة من المعلومات يقوم النظام بإرسالها عبر

الفاكس. تُقدم بعض البنوك هذه الخدمة مجاناً لعملائها لأنها خدمات ذات تكاليف زهيدة وتوفر جهداً كبيراً على العملاء.

الصيرفة عبر الهاتف الجوال

يمكن الوصول إلى الخدمات المرتبطة بالصيرفة عبر الهاتف الجوال (Mobile Banking) عبر الرسائل القصيرة (SMS Banking) أو الإنترنت الخليوي إضافة إلى إمكانية استخدام برامج خاصة يتم تحميلها على الهاتف الجوال.

تتضمن الحزمة المعيارية من الأنشطة التي تغطيها الصيرفة عبر الهاتف الجوال ما يلي: كشوفات الحساب المصغرة، عمليات الإنذار عن نشاط معين على الحساب أو تجاوز السقف المحدد، الكشف عن القرض، طلب دفتر الشيكات، إلغاء البطاقات التي تمت سرقتها أو ضياعها، تحويل الأموال محلياً ودولياً، إيقاف دفع الشيكات، الاستعلام عن الرصيد، متابعة الودائع لأجل، كشف حساب صناديق الاستثمار وغيرها من الخدمات الأخرى.

4 -4-3- الصيرفة عبر أجهزة الصرف الآلي (ATMs)

وهي عبارة عن الوحدات الطرفية الإلكترونية التي تمكن العملاء من الوصول على مدار الساعة إلى الخدمات المصرفية المختلفة والتي يمكن أن تتضمن: سحب النقدية، قبول الودائع، تحويل الأموال، الحصول على المعلومات المتعلقة برصيد الحساب وغيرها من الخدمات. يتحقق ذلك عبر إدخال بطاقة بلاستيكية خاصة إلى الصراف الآلي التي تمتلك شريطاً مغناطيسياً (Magnetic Strip) يحوي رمز إثبات الهوية (Identification Code) لصاحب البطاقة الذي يتم إرساله مع رقم إثبات الشخصية (PIN) الذي يقوم العميل بإدخاله عبر لوحة المفاتيح الرقمية الموجودة لدى أجهزة الصرف الآلي إلى الحاسب المركزي للمصرف، وبعد التأكد من هوية صاحب البطاقة يوافق الحاسب المركزي للمصرف على تنفيذ العمليات المطلوبة.

إلى جانب ذلك، فإنه يمكن لعميل مصـرف معين أن يقوم بسـحب النقدية من جهاز الصـرف الآلي التابع لمصـرف آخر، وذلك لوجود الشـبكات المشـتركة التي يتم إنشاؤها بين المصارف الواقعة على نطاق دولة واحدة.

4-5- المخاطر المرتبطة بالأعمال المصرفية الإلكترونية

4-5-1-تعريف الخطر

عرفت الأدبيات المصـرفية المخاطر بأنها عبارة عن احتمال تعرض المصـرف لخسائر غير متوقعة وغير مخطط لها و/أو تذبذب في الإيراد المتوقع من استثمار أو نشـاط معين، وذلك نتيجة للأحداث المسـتقبلية المحتملة الوقوع التي لها قدرة على التأثير على تحقيق أهداف المصرف المعتمدة لتنفيذ استراتيجياته بنجاح.

4-5-2- خصائص الأعمال المصرفية الإلكترونية

تتمتع الأعمال المصرفية الإلكترونية بمجموعة من الخصائص التي يمكن تلخيصها بما يلي:

- التطور السـريع جداً نظراً لارتباطها بالتطور التكنولوجي المسـتمر، وتلبية توقعات العملاء المتغيرة بشكل دائم؛
- الانتشار الجغرافي الواسع والعريض؛
- التكامل بين تطبيقات الصـيرفة الإلكترونية ونظم عمليات البنوك المحوسـبة (Core Banking Systems)؛
- الاعتماد المتزايد للمصارف على حزم برمجية (نظم مصرفية) جاهزة؛
- تغير شكل العلاقة التقليدية بين المصرف والعميل.

لم تخلق هذه الخصـائص مخاطر إضـافية، وإنما زادت من أهمية بعض المخاطر التقليدية المرتبطة بالأنشطة المصرفية، وهي المخاطر التالية [BCBS 2003][1]:

[1] Basel Committee On Banking Supervision, "Risk Management Principles for Electronic Banking", 2003.

- المخاطر الإستراتيجية (Strategic Risks)؛
- المخاطر التشغيلية (Operational Risks)؛
- مخاطر السمعة (Reputational Risks)؛
- المخاطر القانونية (Legal Risks).

4-5-3- المخاطر الإستراتيجية

تُعد المخاطر الإستراتيجية (Strategic Risks) من بين أهم المخاطر التي تصاحب الأعمال المصرفية الإلكترونية، وترتبط هذه المخاطر بالقرارات والسياسات والتوجهات التي تتخذها الإدارة العليا للمصرف، وتختلف بذلك عن بقية المخاطر المصرفية في كونها أكثر عمومية واتساعاً، كما أنها تؤثر على كافة المخاطر الأخرى.

ينشأ الخطر الإستراتيجي عادة نتيجة عدم انسجام الأهداف الإستراتيجية للمصرف مع الإستراتيجيات التي تمّ تطويرها والموارد التي تمّ توظيفها لتحقيق تلك الأهداف. لذلك يترتب على المصرف قبل قيامه بتقديم خدمات الصيرفة الإلكترونية، أن يقوم أولاً بتقدير تكاليف إدارة المخاطر المرافقة لها مقابل العائد المتوقع تحققه منها، والتأكد من انسجام هذه الخدمات مع الأهداف الملموسة في الخطة الإستراتيجية للمصرف، إلى جانب وجود الخبرة والمصادر المناسبة لتحديد ومتابعة ومراقبة المخاطر المصاحبة لعمليات الصيرفة الإلكترونية. بالتالي، يجب أن تركز عملية التخطيط واتخاذ القرار على كيفية مقابلة الصيرفة الإلكترونية لحاجة محددة لا أن يتم التركيز عليها كهدف مستقل، ولذلك يتوجب على خبراء التكنولوجيا ومدراء التنفيذ والتسويق المشاركة في عملية التخطيط واتخاذ القرار للتأكد من أنّ خطة العمل منسجمة مع الأهداف الكلية للمصرف، وأنها ضمن مستوى المخاطر التي يستطيع المصرف أن يتحملها.

يمكن أن تنشأ المخاطر الإستراتيجية أيضاً عن الأخطاء التي قد تقع بها الإدارة العليا أو الخلل الذي قد يحدث عند تبني استراتيجيات وخطط تقديم هذه الخدمات

وتنفيذها، وذلك في ضوء الحاجة الملحة لتقديم مثل هذه الخدمات تحت تأثير التطور التكنولوجي المستمر ونمو الطلب عليها من جهة، واشتداد المنافسة من قِبل المؤسسات المصرفية وغير المصرفية من جهة أخرى. بالتالي ترتبط المخاطر الإستراتيجية للصيرفة الإلكترونية بجزء كبير منها بقضايا التوقيت، فقد تنشأ مخاطر إستراتيجية كبيرة في حال توجه إدارة المصرف لأخذ زمام الريادة في استخدام تقنيات حديثة دون القيام بتحليل مناسب للتكلفة والعائد، حيث ينعكس ذلك بتكاليف أعلى وتزداد درجة التعقيد في عملياتهم. أو على العكس تماماً، قد تنشأ هذه المخاطر في حال تباطؤ إدارة المصرف في إدخال التقنيات المصرفية الحديثة، فعلى الرغم من أنّ ذلك قد يمكن المصرف من تجنب التكاليف العالية، غير أنّ ذلك يعرضه لخطر عدم إقبال العملاء على تلك الخدمات والمنتجات.

عند إدارة المخاطر الإستراتيجية المرافقة لخدمات الصيرفة الإلكترونية، فإنه يتوجب على المؤسسة المالية أن تقوم بتطوير أهداف واضحة للصيرفة الإلكترونية لتتمكن من خلالها تقييم نجاح إستراتيجيتها المتعلقة بالصيرفة الإلكترونية، وبالتحديد على المصارف أن تراعي ما يلي:

- مدى كفاءة نظام معلومات الإدارة MIS (Management Information System) لمتابعة معدل استخدام وربحية الصيرفة الإلكترونية؛
- التكاليف المصاحبة لمتابعة ومراقبة أنشطة الصيرفة الإلكترونية إلى جانب تكاليف الإشراف على موردي الخدمة التقنية؛
- تصميم وتسليم وتسعير الخدمات بالشكل الذي يولد طلباً كافياً عليها من قِبل العملاء؛
- درجة المنافسة من قِبل الأطراف الأخرى المقدمة لخدمات الصيرفة الإلكترونية؛
- مدى توافر الدعم التقني والتشغيلي والتسويقي لخدمات ومنتجات الصيرفة الإلكترونية.

إلى جانب هذه المتطلبات والترتيبات العديدة التي يستلزمها تقديم الخدمات المصرفية الإلكترونية، فإنه يتوجب على الإدارة العليا النظر في اعتبارات تتعلق بالربحية والوضع التنافسي للمصرف والانعكاسات على المخاطر الأخرى بالشكل الذي يساهم في تبني الخيارات الملائمة عند وضع إستراتيجية تقديم هذه الخدمات.

4-5-4- المخاطر التشغيلية

المخاطر التشغيلية (Operational Risks) هي المخاطر المرتبطة باستخدام التقنيات والأنظمة، الأمر الذي يجعل هذه المخاطر الأكثر أهمية بالنسبة للخدمات المصرفية الإلكترونية وذلك نظراً للاعتماد الكبير على التقنيات في كافة أوجه تقديم هذه الخدمات.

تُعد المخاطر الأمنية وانتظام تقديم الخدمة هي المخاطر التشغيلية الأساسية في بيئة الأعمال المصرفية الإلكترونية، فقد خلقت الطبيعة المفتوحة للخدمات المصرفية الإلكترونية قضايا أمنية لإدارات المصارف تتعلق بالسرية وسلامة المعلومات والتحكم في الدخول إلى الأنظمة والشبكات والتأكد من هوية وسماحيات المستخدمين، إلى جانب ضرورة انتظام توفير الخدمات المصرفية الإلكترونية على مدار الساعة لأنّ العملاء غير معتادون على الانتظار في البيئة الإلكترونية.

إلى جانب ذلك، يمكن أن تنشأ المخاطر التشغيلية عن التعاقد مع أطراف خارجية في توفير الخدمات المصرفية الإلكترونية نظراً للاعتماد الكبير على التكنولوجيا المعقدة في كافة أوجه تقديم هذه الخدمات، كما أنّ التصميم أو التطبيق غير الكفء لنظم الصيرفة الإلكترونية، و إساءة الاستخدام من قِبل العملاء يمكن أن يشكل مصدراً آخر للمخاطر التشغيلية.

4-5-5- مخاطر السمعة

يرتبط نجاح المصارف في أعمالها بالسمعة التي تؤسسها كمؤسسات جديرة بالثقة، وكلما زاد اعتماد المصارف على التكنولوجيا الجديدة في تقديم خدماتها، كلما زاد

انكشـــافها لمخاطر الســـمعة (Reputational Risks) التي يمكن أن تنشـــأ في الحالات التالية:

- فشل المصرف في إرساء شبكة موثوقة وآمنة لتقديم هذه الخدمات؛
- تقديم خدمات غير كفوءة؛
- عدم انتظام تقديم الخدمة؛
- نقص متطلبات الإفصاح اللازمة للعملاء أو عند حدوث انتهاك للخصوصية.

يمكن أن تنشـأ هذه المخاطر أيضـاً عند حدوث اختراقات أمنية على موقع مصـرف ما على شـــبكة الإنترنت، والتي تؤدي إلى فقدان ثقة العملاء أو الســـوق بمقدرة المصـــارف بشـــكل عام على الإدارة الكفوءة والســـليمة للمعاملات المصـــرفية الإلكترونية.

يتوجب على المصارف لكي تتفادى مخاطر الإضرار بسمعتها، أن تسعى إلى وضع معايير لأنشـطتها المصـرفية الإلكترونية، وأن تقوم بمراقبة ومراجعة هذه الأنشـطة والخدمات بصورة دورية ومنتظمة، وأن تضع خطط تمكنها من الاستمرار في تقديم خدماتها، وأن تعمل على إرســـاء علاقة وطيدة مع العملاء من خلال إرشـــادهم عن المخاطر المحتملة في العمليات المصرفية الإلكترونية، وكيفية استخدام هذه الخدمات بالشـــكل الأمثل، وكيفية تجنب المخاطر الأمنية، وتقديم نصـــائح فنية لمواجهة أي تحديات أثناء اســـتخدام هذه الخدمات، إلى جانب آلية التعامل مع المشـــاكل التي قد تحدث، وكيفية استخدام الأسماء والأرقام السرية.

4-5-6- المخاطر القانونية

ترفع الأعمال المصـــرفية الإلكترونية من درجة المخاطر القانونية المصـــاحبة للمصرف، حيث تمكن الصيرفة الإلكترونية المصارف من توسيع النطاق الجغرافي لخدماتهم بشكل أسرع، ولكن في بعض الحالات قد يبدأ المصرف بتقديم خدماته في مناطق جغرافية معينة دون أن يكون على معرفة كاملة بالقوانين والقواعد والضوابط المقررة من قِبل الســلطات القانونية في تلك المناطق. ويحدث ذلك عادة عندما تكون الرخصــة غير مطلوبة للمصــرف ليقوم بمزاولة أعماله في منطقة معينة، حيث يجد

المصرف الافتراضي صعوبة في مواكبة التغييرات القانونية بسبب نقص التواصل مع السلطات الإشرافية في البلد المضيف، وبالنتيجة يمكن للمصرف أن يخرق دون معرفة منه قوانين حماية العميل نتيجة لعدم التحديد الواضح للحقوق والالتزامات القانونية الناتجة عن التعاملات المصرفية الإلكترونية والنقص في متطلبات الإفصاح المرتبطة بذلك.

يمكن أن تقع المخاطر القانونية أيضاً نتيجة الإخفاق في توفير السرية الواجبة لمعاملات العملاء أو نتيجة الإساءة في استخدام البيانات والمعلومات، ويعزز هذه المخاطر النقص في التشريعات المصرفية المتعلقة بالتعاقدات والعمليات الالكترونية والآليات القانونية لضبط تنفيذ هذه التعاقدات والتعاملات. ومن الأمثلة الشائعة لهذه المخاطر، قيام المصارف بتقديم خدمات مصرفية عبر شبكة الإنترنت لعملاء خارج نطاق القطاع القانوني، فقد سهلت الصيرفة الإلكترونية عمليات غسيل الأموال نظراً للمجهولية (Anonymity) التي توفرها بالنسبة لهوية العميل. فعند قيام العميل بفتح حساب لدى المصرف، من الصعب أن يتمكن المصرف من تحديد إن كان مالك الحساب الاسمي هو فعلاً من يقوم بتنفيذ المعاملات أو حتى أن يتمكن من معرفة مكان تنفيذ تلك المعاملات.

هناك مصدر آخر للمخاطر القانونية يتعلق بنوع التشريع الذي يجب أن يتم تطبيقه على معاملات الصيرفة الإلكترونية، هل هو تشريع الدولة التي ُمنح فيها المصرف الافتراضي رخصة مزاولة العمل أم تشريعات الدولة التي يقدم فيها المصرف خدماته، وذلك نظراً لاحتمال وجود تعارض بين تلك التشريعات.

للحد من هذه المخاطر، يتعين على المصارف التأكد من اكتمال متطلبات الإفصاح للعملاء وعلى وجه الخصوص التعريف بالإطار القانوني والإشرافي الذي تخضع له هذه المعاملات الإلكترونية وما قد ينشأ عن ذلك من حقوق والتزامات، إلى جانب التأكد من الإجراءات القانونية والقضائية السائدة في المناطق التي تقدم فيها خدماتها المصرفية الإلكترونية، والاهتمام بجوانب التسجيل والتوثيق للعمليات المصرفية الإلكترونية في كافة مراحلها وتفاصيلها وحفظها بصورة آمنة ليتسنى اللجوء إليها

عند الحاجة. ومن جانب آخر، يتوجب على السلطات الإشرافية السعي لتنظيم الأطر القانونية والرقابية لمعالجة القضـــايا القانونية والقضـــائية المرتبطة بالمعاملات المصرفية الإلكترونية.

الفصل الخامس

المخاطر التشغيلية في ظل الصيرفة الإلكترونية

5-1- مقدمة

ساعدت الصيرفةُ الإلكترونية المصارفَ على تمييز منتجاتها وخدماتها في البيئة التنافسية العالية التي تواجهها، إلى جانب تحقيق مزايا عديدة للمصرف ولزبائنه، ومنها: انخفاض تكلفة العمليات في المصرف على المدى الطويل نظراً للحاجة إلى فروع أقل وموظفين أقل؛ الوصول السريع للخدمات على مدار الساعة ومن أي موقع؛ إمكانية تسويق الخدمات المصرفية على مناطق جغرافية واسعة وخارج حدود الدولة الأم دون الحاجة إلى إقامة فروع للمصرف، الخ. ولكن على الرغم من هذه المزايا التي تتمتع بها الأعمال المصرفية الالكترونية، فإنّ اعتمادها على التقنيات والنظم جعل المخاطر التشغيلية من أهم المخاطر التي تواجهها الأعمال المصرفية الالكترونية.

5-2- تعريف المخاطر التشغيلية

نالت المخاطر التشغيلية في المصارف اهتماماً متزايداً منذ منتصف التسعينات، وذلك بسبب الأزمات المصرفية التي نتج معظمها عن حالات الاحتيال والأخطاء البشرية وغياب الرقابة، إضافةً إلى قيام لجنة بازل للرقابة المصرفية منذ عام 1999 بإظهار رغبتها في تقديم متطلبات رأسمالية جديدة للمخاطر التشغيلية إلى جانب المخاطر الائتمانية ومخاطر السوق.

نظراً لاختلاف تعريف المخاطر التشغيلية بين المصارف بشكل كبير، فقد قدمت لجنة بازل 2 تعريفاً موحداً للمخاطر التشغيلية،حيث عرّفتها بأنها **خطر الخسارة الناتجة عن فشل أو عدم كفاية العمليات الداخلية أو العاملين أو النظم أو عن الأحداث**

الخارجية [BCBS 2001][2]. هذا التعريف يشمل المخاطر القانونية ولكنه يستثني المخاطر الإستراتيجية ومخاطر السمعة.

5-2-1- العمليات الداخلية

تنتج المخاطر هنا عن المعالجة الخاطئة للمعاملات وحسابات العملاء وعمليات المصرف اليومية، والضعف في أنظمة الرقابة والتدقيق الداخلي، والإخفاق في تنفيذ المعاملات وإدارة العمليات. ومثال ذلك، الأخطاء في إدخال البيانات والدخول إلى البيانات لغير المصرح لهم بذلك.

5-2-2- العاملين

تنشأ المخاطر هنا عن فشل الإدارة والهيكل التنظيمي للمصرف، إلى جانب الخسائر التي يمكن أن يُسببها الموظفون بسلوكهم نتيجة للإهمال في تنفيذ المهام (بتقديم استشارات خاطئة مثلاً أو إعطاء معلومات لأطراف لا يجوز لها الاطلاع عليها من باب الخطأ) أو الأفعال التي يكون الهدف منها الغش أو إساءة استعمال الممتلكات أو التحايل على القانون واللوائح التنظيمية وسياسة الشركة، وكذلك الخسائر الناتجة عن العلاقة مع العملاء والمساهمين والجهات الرقابية وأي طرف ثالث. ومن الأمثلة عليها: عمليات الاحتيال الداخلي من قبل الموظفين كالاختلاس المالي، والتعمد في إعداد تقارير خاطئة عن أوضاع المصرف، والتجارة الداخلية لحسابات الموظفين الخاصة، وإساءة استخدام بيانات العملاء السرية، وعمليات التداول دون تخويل، والغرامات والعقوبات بسبب أخطاء الموظفين.

5-2-3- النظم

تتعلق المخاطر في هذا المجال بالخسائر الناتجة عن التوقف في العمل بسبب عدم توافر البنية التحتية الملائمة (ومثال ذلك، فشل البرمجيات أو العتاد الصلب أو فشل

[2] Basel Committee On Banking Supervision Consultative Document, "Operational Risk. Supporting Document to the New Basel Capital Accord", 2001.

وسائل الاتصال) أو الخسائر الناتجة عن عدم كفاءة نظام المعلومات، ويُعتبر الأخير هو أهم خطر تشغيلي متعلق بالنظم في مجال الصيرفة الإلكترونية.

5-2-3-1- عدم كفاءة نظام المعلومات

تتعلق كفاءة نظام المعلومات بما يوفره من سرية للبيانات وسلامة البيانات والنظام، بمعنى دقة (Accuracy) وموثوقية (Reliability) وكمال المعلومات المرسلة بين المصارف وعملائهم ومزودي الخدمة الخارجيين، إلى جانب استمرار إتاحة (Availability) النظام والطاقة القصوى للنظام.

يمكن أن تنتج عدم الكفاءة في نظام المعلومات عن مخاطر عامة أو عن مخاطر موجهة بالتطبيق (Application Oriented Risks). تتعلق المخاطر العامة بالوصول المادي إلى عتاد الحاسب، أو الوصول المنطقي إلى المعلومات وأنظمة تكنولوجيا الاتصالات، أو إجراءات استعادة النسخ الاحتياطية غير المناسبة المستخدمة في تخفيض الأثر الناجم عن فشل الأنظمة.

أما ما يتعلق بعدم الكفاءة في نظام المعلومات المرتبطة بالمخاطر الموجهة بالتطبيق (Application Oriented Risks)، فيمكنها أن تنتج عن أحد حالات الخطأ التالية:

- تسجيل البيانات بطريقة غير صحيحة بسبب الأخطاء في النظام؛
- تخزين البيانات بشكل خاطئ أثناء فترة استخدامها؛
- إدخال البيانات الصحيحة بشكل خاطئ؛
- عدم صحة الحسابات (Calculations) الأساسية للمعلومات؛
- عدم توافر المعلومات المعالَجة بالتطبيق في الوقت المناسب بسبب فشل الأنظمة.

5-2-4- الأحداث الخارجية

تتعلق المخاطر هنا بالأحداث التي تقع خارج بيئة العمل الداخلية للمصرف والمؤثرة على عملياته، وتشمل الاحتيال الخارجي مثل الاستيلاء على المعلومات الخاصة

بالعملاء للوصول إلى الحساب، والتغيرات الحاصلة في التشريعات القانونية أو عن الكوارث الطبيعية (على سبيل المثال،الهزات الأرضية، والحرائق، والفيضانات...الخ)، أو عدم التزام الأطراف الخارجية الموردة لخدمات معينة في أداء التزاماتها، أو المنافسة الشديدة من قِبل المؤسسات المصرفية وغير المصرفية.

5-5- المخاطر التشغيلية في ظل الصيرفة الإلكترونية

ذكرنا سابقاً أنّ المخاطر التشغيلية يمكنها أن تنشأ عن حالات الاحتيال أو أخطاء المعالجة أو تعطل الأنظمة أو عن أحداث غير متوقعة والتي ينتج عنها عدم القدرة على تقديم المنتجات والخدمات. وفيما يتعلق بالأعمال المصرفية الإلكترونية، فإنّ المخاطر التشغيلية تصاحب كل منتج وخدمة مقدمة، ويرتبط مستواها ببنية بيئة المعالجة المصرفية، بما فيها نوع الخدمات المقدمة ودرجة التعقيد في العمليات والتقنيات الداعمة. ونظراً لكون أنّ العملاء يتوقعون الحصول على خدمات الصيرفة الإلكترونية يومياً وعلى مدار الساعة، فإنه يتوجب على المصارف أن تقوم ببناء بنية تحتية ملائمة لأنظمة المصارف الإلكترونية، بحيث تستوعب الكم الهائل من البيانات التي يمكن أن تنهمر على قواعد بياناتها كل لحظة دون أن يتأثر مستوى الخدمة وسرعة الأداء بذلك. إلى جانب ذلك، فإنه يترتب على المصارف أن تسعى إلى تحقيق المعادلة الصعبة في الصيرفة الإلكترونية التي تتلخص بالوصول إلى **إرضاء العملاء وكسب ولائهم**، وذلك بتوفير ما يتوقعون من خدمات بالسرعة القصوى.

5-5-1- المخاطر الأمنية

تُعتبر المخاطر الأمنية هي المخاطر التشغيلية الرئيسية في ظل الصيرفة الإلكترونية، فقد بينت إحدى الدراسات أن مستوى السرية والأمان هو من أهم العوائق في تبني الخدمات المصرفية الإلكترونية من قبل العملاء، حتى أنه يفوق في أهميته المزايا الأخرى مثل التكلفة والملاءمة.

تُعرِّض طبيعة العمليات المصرفية الإلكترونية (المعتمدة على نظم المعلومات والاتصالات) المصارفَ التي تقدمِّها إلى تهديدات أمنية من مصادر مختلفة من داخل وخارج النظام ومن أمثلتها:

Back Doors وهي عبارة عن أجزاء (Pieces) من كود البرنامج (Program Code) التي تُكتب في التطبيقات أو النظم التشغيلية ليتمكن المبرمج من الوصول إلى البرامج دون الحاجة إلى العبور عبر الرقابة الأمنية الاعتيادية؛

Brute Force تقنية للاستيلاء على الرسائل المشفرة ومن ثم استخدام العتاد البرمجي لفك التشفير والوصول إلى المعلومات الخاصة بالعملاء؛

Hijacking وهي الهجمات التي يتم من خلالها سرقة الاتصال بعد أن يقوم العميل بتوثيق نفسه للنظام؛

Sniffing وهي عبارة عن استخدام البرمجيات التي يتم إدخالها بطريقة غير قانونية في مكان ما على الشبكة، وذلك للاستيلاء على كلمات سر المستخدم عندما يتم إدخالها إلى النظام؛

Spoofing تُشير إلى إرسال معلومات مزيفة إلى النظام أو الشبكة وإظهارها وكأنها معلومات مرسلة من قِبل مستخدم مرخص، وذلك للوصول إلى النظام.

إلى جانب ذلك، يمكن أن تتعرض المصارف لهجمات تؤدي إلى إعاقة عمليات المصرف، مثل هجمات توقف الخدمة (Denial of Service Attacks) التي تنشأ عندما يقوم المتطفل بإرسال المئات من الرسائل كل ثانية من عناوين خاطئة مولّدة عشوائياً، بحيث يُحمّل مخدّم البريد الإلكتروني لمزوّد خدمة الإنترنت بأعلى من طاقته ويتوقف عن العمل، أو أن يتم إرسال العديد من الطلبات لمواقع الويب بحيث يتوقف مخدّم الويب عن العمل.

وبالتالي فقد خلقت الطبيعة المفتوحة للخدمات المصرفية الإلكترونية قضايا أمنية لإدارات المصارف تتعلق بأمن المعلومات والتأكد من هوية وسماحيات المستخدمين، ولذلك تحتل الرقابة على الوصول إلى النظم المصرفية الحرجة أهمية كبيرة، وذلك لمنع اختراق غير المرخص لهم لنظم حسابات المصرف والحصول على المعلومات

الخاصة بالعملاء واستغلالها، سواء تم ذلك من خارج المصرف أو من العاملين فيه. وتزداد صعوبة الرقابة على الوصول إلى النظم المصرفية بسبب توسع الإمكانيات الحاسوبية، والتوزع الجغرافي لنقاط الوصول، إلى جانب استخدام طرق الاتصال المختلفة بما فيها الشبكات العامة مثل شبكة الإنترنت.

نظراً لما سبق، فإنه يترتب على المصارف أن تقوم بتدعيم إدارة المخاطر الأمنية لديها بشكل عام وللعمليات المصرفية الإلكترونية بشكل خاص، ومما لاشك فيه أن الضعف أو الخلل في التعامل مع هذه القضايا قد يقود إلى مخاطر إضافية لإدارة المصارف كالمخاطر القانونية ومخاطر السمعة. فعلى سبيل المثال، الوصول غير المشروع إلى المعلومات السرية الخاصة بعملاء المصرف يُعرّض المصرف لخسائر ناتجة عن المخاطر التشغيلية، وبشكل غير مباشر لمخاطر قانونية، لأنّ المصرف يمكن أن يتعرض للمساءلة القانونية، إلى جانب أن العميل يمكن أن يقوم بتجميد كل حساباته وإنهاء تعامله بالكامل مع المصرف بما يُعرّض المصرف لمخاطر السمعة.

إلى جانب الهجمات الخارجية على نظم الصيرفة الإلكترونية، فإنّ المصارف معرّضة لمخاطر تشغيلية متصلة باحتيال الموظفين الذين يمكن أن يستولوا بشكل تحايلي على بيانات التأكد من الهوية للوصول إلى حسابات العملاء، إضافة إلى المخاطر التشغيلية الناتجة عن أخطاء الموظفين التي يمكن أن تُعرض المصرف أيضاً للخطر.

5-5-2- تصميم وتنفيذ وصيانة النظم

تتعرض المصارف لخطر أنّ النظم التي تمّ اختيارها غير مصممة أو مطبقة بشكل جيد أو لا تتمتع بالكفاءة والقدرة العالية لاستيعاب الأعداد الكبيرة من العملاء. على سبيل المثال، يتعرض المصرف لخطر التوقف أو البطء في أداء النظم المستخدمة في حال كانت نظم الصيرفة الإلكترونية التي تمّ اختيارها غير متوافقة مع متطلبات المستخدمين، إضافة إلى ذلك، فإنّ عدم قدرتها على التعامل مع طلب العملاء على الخدمات المصرفية يمكن أن يعرّض المصارف إلى أضرار مالية وضرر بالسمعة، كما يمكن أن يعرّضها إلى التهديدات الأمنية وذلك في حال كانت النظم الإضافية التي

تمّ استخدامها لاستيعاب طلبات العملاء غير كفوءة أو لم يتم اختبارها بشكل جيد قبل الاستخدام.

إلى جانب ذلك، فقد خلقت الأعمال المصرفية الإلكترونية مشاكل متعلقة بتكامل التطبيقات والنظم التقنية، حيث يُعتبر جانب مواءمة ودمج نظم الأعمال المصرفية الإلكترونية بالأنظمة الرئيسية القائمة لدى المصرف بكفاءة أهم الشروط المطلوبة في هذا الصدد، وذلك نظراً للمخاطر التشغيلية الكبيرة التي قد تحدث من جراء وجود خلل ما في عملية الدمج والربط . وقد دفع ذلك الكثير من المصارف (الكبيرة على وجه الخصوص) نحو استثمار أموال ضخمة في البنية التحتية التقنية (الأجهزة والبرمجيات) وعلى الكوادر المؤهلة، في حين لجأت المصارف المتوسطة والصغيرة نظراً للمحدودية في الموارد نحو الاعتماد على موردي خدمات آخرين لتوفير إدارة البنية التحتية التقنية اللازمة لدعم العمليات والأنشطة المصرفية الإلكترونية.

إلى جانب ذلك، فإنّ التطور السريع الذي تتسم به تكنولوجيا المعلومات يُعرّض المصارف لخطر تقادم الأنظمة، فعلى سبيل المثال، تتطلب البرمجيات المصرفية التي تُسهّل استخدام منتجات الصيرفة الإلكترونية من قِبل العملاء تحديثاً دورياً، غير أنّ قنوات توزيع برمجيات التحديث قد تتضمن مخاطر للمصرف، وذلك لأنّ الوحدات البرمجية الطفيلية يمكن أن تعترض وتعدّل تلك البرمجيات. إضافةً إلى ذلك، فإنّ التغير التكنولوجي المستمر يمكن أن يؤدي إلى عدم الفهم الجيد من قِبل فريق العمل داخل المصرف لطبيعة التكنولوجيا الجديدة المستخدمة، بما يسبب مشاكل تشغيلية مع النظم الجديدة أو المعدّلة.

5-5-3- سوء استخدام الزبائن للمنتجات والخدمات

كما هو الحال مع الخدمات المصرفية التقليدية، فإنّ إساءة استخدام الزبائن لمنتجات وخدمات الصيرفة الإلكترونية سواء بشكل مقصود أو غير مقصود يُعتبر مصدراً آخر للمخاطر التشغيلية، وهذا الخطر يمكن أن يزداد إذا لم يقم المصرف بإحاطة عملائه بشكل كاف عن إجراءات الرقابة الأمنية المناسبة. إضافة إلى ذلك، فإنّ غياب

المعايير اللازمة لإثبات وتوثيق المعاملات، سيمكّن العملاء من رفض المعاملات التي قاموا بترخيصها سابقاً بما يفرض خسائر مالية على المصرف، كما أنّ استخدام الزبائن لمعلوماتهم الشخصية (معلومات التأكد من الهوية أو أرقام بطاقات الائتمان أو أرقام الحساب المصرفي) في عمليات إرسال إلكترونية غير آمنة، يمكن أن يسمح للمتطفلين بالوصول إلى حساباتهم، بما ينعكس على المصرف بخسائر مالية كبيرة وذلك بسبب الصفقات التي لم يتم الترخيص لها من قِبل العملاء.

5-5-4- انتظام تقديم الخدمة

بالإضافة إلى التأكد من كفاءة الإجراءات الأمنية وسلامة البيانات، فإن انتظام توفير الخدمات المصرفية الإلكترونية على مدار الساعة يمثل عنصراً هاماً من مكونات إدارة وتوفير هذه الخدمات، الأمر الذي تعززه متطلبات المنافسة من جهة، والحاجة إلى الحد من مخاطر السمعة التي قد تنشأ عن عدم انتظام تقديم الخدمة من جهة أخرى. بالتالي يتوجب على المصارف القيام بتقديم خدمات الصيرفة الإلكترونية على أساس ثابت وفي الوقت المناسب بما يتناسب مع توقعات العملاء، ولتحقيق ذلك على المصرف أن يمتلك القدرة على تقديم خدماته إلى المستهلكين النهائيين إما من مصادر أساسية (النظم الداخلية للمصرف والتطبيقات) أو ثانوية (تطبيقات ونظم موردي الخدمة)، والتأكد من كفاءة إجراءات انتظام الخدمة ووجود البدائل عند انقطاعها، كذلك وجود بدائل فيما يتعلق بالأطراف الخارجية الموردة للخدمات، فالتهديدات التي يمكن أن تعيق عمل النظام يمكن أن تنتج من عدة مصادر منها:

- فشل البرمجيات (Software) والعتاد (Hardware)؛
- الكوارث الطبيعية؛
- الأخطاء البشرية؛
- الفيروسات والبرامج المدمّرة؛
- هجمات توقف الخدمة (Denial Of Service Attacks) وغيرها من الأعمال التخريبية.

يمكن للرقابة المناسبة أن تخفض لا أن تتخلص بشكل نهائي من خطر هذه التهديدات المسببة لتوقف طويل في عمل النظام، ولهذا السبب تحتاج المصارف إلى تطوير خطط شاملة لإعادة النظام إلى الوضع السابق وذلك لتتمكن المصارف من استئناف عملياتها خلال وقت قصير بما يضمن استمرار العمل بعد حوادث معيّنة. إلى جانب ذلك، قد يكون من المفيد التعاقد بصورة دورية مع إحدى بيوت الخبرة لاكتشاف الخلل في الأنظمة.

5-5-5- التعاقد مع أطراف خارجية

يتزايد الاعتماد بشكل كبير على أطراف خارجية في تقديم الخدمات المصرفية الإلكترونية وعلى خبراء خارجيين لتطبيق وتشغيل ودعم أجزاء من أنشطة الصيرفة الإلكترونية سواء من قبل المصارف الكبيرة أو الصغيرة وذلك على اختلاف دوافعهما، هذا الاعتماد قد يكون مناسباً لأنه يسمح للمصارف الاعتماد على جهات خارجية في بعض الجوانب المتعلقة بتقديم الأعمال المصرفية الإلكترونية التي لا تتمكن المصارف من تقديمها بنفسها بشكل اقتصادي، ولكن رغم ذلك فإنّ الاعتماد على أطراف خارجية يّعرض المصرف لمخاطر تشغيلية؛ فموردو الخدمة قد لا يتمتعون بالخبرة المطلوبة لتقديم الخدمات بالشكل المطلوب من المصرف أو قد يفشلون في تجديد تقنياتهم في الوقت المناسب، إلى جانب أنّ أعمالهم قد تتوقف بسبب عطل في النظام أو لصعوبات مالية بما يعيق قدرة المصرف على تسليم منتجاته وخدماته.

بناءً على ما سبق، يتوجب على الإدارة المصرفية أن تتجنب التعاقد مع جهة خارجية واحدة فقط في تقديم الخدمات المصرفية الإلكترونية، وأن تتجنب التعاقد مع المؤسسات الحديثة قليلة الخبرة، إلى جانب القيام بمراجعة دقيقة لشروط التعاقد مع أي جهة خارجية، والقيام بمتابعة ومراجعة مستمرة لأدائها قبل وبعد التعاقد معها، كما يتعين على إدارات المصارف أن تمتلك القدرة والكفاءة على إدارة المخاطر المرتبطة بتلك التعاقدات وعلى وجه الخصوص الحفاظ على سلامة وسرية البيانات والمعلومات التي قد تحصل عليها الأطراف الخارجية.

الفصل السادس
إدارة المخاطر الأمنية

6-1- مقدمة

على المؤسسات المصرفية أن تُدرك أهمية الأمن والسرية في أعمالها المصرفية الإلكترونية وذلك لتتمكن من تحقيق مستوى ثقة عال من قِبل عملائها من الأفراد والمؤسسات، حيث يتوجب على الإدارة المصرفية أن تضمن أمن العمليات التي يتم تنفيذها وأمن المعلومات المتدفقة عبر قنوات الاتصال الإلكترونية. لهذا السبب لا بدّ من تطوير نظام قوي وشامل لأمن الصيرفة الإلكترونية والذي يجب أن يحقق المبادئ الأساسية التالية كما حددتها لجنة بازل للرقابة المصرفية:

6-1-1- التأكد من الهوية (Authentication)

تشير عملية التأكد من الهوية إلى التقنيات والإجراءات والعمليات المستخدمة من قِبل المصارف للتحقق من هوية العملاء الحاليين والمستقبليين، حيث يتوجب على المصارف أن تستخدم أساليب تأكد من الهوية موثوقة وآمنة للتحقق من هوية عملاء ومستخدمي نظم الصيرفة الإلكترونية، مع مراعاة تناسب أسلوب التأكد من الهوية المستخدم في تطبيق معين مع تقييم الإدارة للمخاطر المرتبطة بذلك التطبيق، فاستخدام عامل واحد فقط للتأكد من الهوية يُعتبر غير مناسباً للمعاملات ذات المخاطر العالية أو الاتصالات الحساسة والتي تتضمن الوصول إلى معلومات العميل أو تحويل الأموال إلى طرف ثالث أو دخول المستخدمين ذات الامتيازات العالية (مدير الشبكة مثلاً)، ففي هذه الحالات لا بدّ من استخدام التقنيات المعتمدة على أكثر من عامل واحد للتأكد من الهوية، مثلاً ما يعرفه العميل (كلمات المرور مثلاً) وما يملكه (Tokens)، لأنّ ذلك يوفر حماية أعلى موثوقية لتفادي عمليات الوصول غير المشروع. المثال الشائع على عملية التأكد من الهوية المعتمدة على عاملين نجده في معاملات أجهزة الصرف الآلي، حيث يُطلب من العميل إدخال ما يملكه (البطاقة) وما يعرفه (رقم إثبات الشخصية (PIN)).

إضافة إلى ما سبق، تساعد عملية التأكد من الهوية والتحقق من هوية مستخدم النظام على ضمان سرية البيانات وتحمل مسؤولية المعاملات التي يتم تنفيذها

6-1-2- سلامة البيانات والمعاملات (Data and Transaction Integrity)

يشير مصطلح سلامة البيانات والمعاملات إلى ضمان أنّ المعلومات لم يتم تعديلها دون سماحية القيام بذلك سواء أثناء تخزينها أو انتقالها إلكترونياً. فتقديم المصارف لخدماتها عبر الشبكات العامة يزيد من احتمال تعرّض المعلومات للتخريب والتلاعب، ولذلك يتوجب على المؤسسات المصرفية اتخاذ الإجراءات المناسبة لضمان دقة وكمال وموثوقية المعلومات المعالجة والمرسلة أو المخزنة، لأنّ الفشل في المحافظة على سلامة بيانات المعاملات والسجلات والمعلومات يمكن أن يُعرّض المؤسسات المصرفية لخسائر مالية إلى جانب المخاطر القانونية ومخاطر السمعة.

6-1-3- التأكد من السماحية (Authorization)

تتعلق عملية التأكد من السماحية بالرقابة الدقيقة على التفويضات الممنوحة وسماحيات الوصول التي يجب أن تُبنى حسب مسؤوليات العمل وضرورة أداء المهام، لأنّ الفشل في توفير رقابة مناسبة للتأكد من السماحية يمكن أن يسمح للمستخدمين باستبدال سماحياتهم والوصول إلى النظم المصرفية الإلكترونية والشبكات وقواعد المعطيات والتطبيقات التي لا يملكون سماحيات الوصول إليها.

تُخزّن حقوق الوصول المرتبطة بنظم الصيرفة الإلكترونية عادة داخل قواعد المعطيات، ويتم إنشاءها (أي حقوق الوصول) بطريقة مركزية أو غير مركزية، وبالتالي من الأساسي أن تتم حماية قواعد البيانات من التخريب والتلاعب لتحقيق رقابة فاعلة للتأكد من السماحية.

6-1-4- سرية المعلومات الحساسة (Confidentiality of Sensitive Data)

المقصود بالسرية ضمان أنّ المعلومات لا يتمكن من إرسالها أو الوصول إليها مصادر غير مخولة بذلك، أي أنّ الوصول واستخدام المعلومات الحساسة الأساسية للمصرف المخزنة داخل قواعد المعطيات أو التي يتم الوصول إليها عبر النظم يتم فقط من قِبل الأطراف المشروعة،

فإساءة الاستخدام أو الإفصاح غير المشروع عن البيانات والسجلات الحساسة يُعرّض المصرف لمخاطر قانونية ومخاطر السمعة، ولذلك يتوجب على المؤسسات المصرفية القيام بتطبيق تقنيات ملائمة للحفاظ على سرية وسلامة المعلومات الحساسة أثناء انتقالها عبر الشبكات الداخلية والخارجية أو أثناء تخزينها داخل النظم الداخلية للمصرف.

6-1-5- عدم الإنكار (Non-Repudiation)

وهي تتضمن توليد دليل للأصل أو لتلقي المعلومات الإلكترونية، وذلك لحماية المرسل من إدعاء المستلم بعدم تلقي المعلومات، أو لحماية المستلم من الإدعاء الكاذب من قِبل المرسل بعدم إرساله للمعلومات. في هذه الحالة يتوجب على المصارف أن تتخذ الإجراءات اللازمة بما يتناسب مع الأهمية النسبية لمعاملات الصيرفة الإلكترونية، وذلك لحماية دقة وسلامة المعلومات الإلكترونية المرسلة عبر الشبكات الداخلية والخارجية لضمان عدم الإنكار وسرية وسلامة معاملات الصيرفة الإلكترونية. على سبيل المثال، استخدام التشفير والتوقيع الإلكتروني واتفاقيات الشهادة الرقمية والتي سيتم تناولها لاحقاً من خلال هذا الفصل، يمكن أن يحدد بشكل دقيق هوية الشخص المنشئ للمعاملة، ومن قام بإضافة التوقيع الإلكتروني للمعاملة، وكشف التعديلات غير المشروعة ومنع الإنكار اللاحق.

6-1-6- الحفاظ على مسار المراجعة (Audit Trails)

تضعف الرقابة الداخلية للمؤسسات المصرفية في حال عدم قدرتها على القيام بتدقيق ومراجعة أعمالها المصرفية الإلكترونية، وذلك لأنّ معظم أو جميع السجلات والوثائق الداعمة المتعلقة بها متوافرة بصورة إلكترونية. بالتالي، على المصارف أن تضمن وجود مسارات مراجعة واضحة لكل المعاملات المصرفية الإلكترونية بحيث تتمكن من تدقيق كل الأحداث والتطبيقات المصرفية الإلكترونية بشكل منفصل وذلك لضمان أمن العملاء من أي إدعاء وإنكار من قِبل المصرف، وضمان سلامة المصرف من أي رفض من قِبل العميل. وبشكل أساسي لا بدّ من وجود مسارات مراجعة واضحة للمعاملات المصرفية الإلكترونية التالية:

- فتح أو تعديل أو إقفال حساب العميل؛

- جميع المعاملات ذات النتائج المالية؛
- أي تفويض ممنوح للعميل لتجاوز الحد؛
- أي منح أو تعديل أو سحب للسماحيات أو الحقوق للوصول إلى النظم.

6-1-7- فصل المهام والواجبات (Segregation of Duties)

يعتبر الفصل بين المهام والواجبات عنصراً أساسياً لعملية الرقابة الداخلية المصممة لتخفيض خطر الاحتيال في العمليات والنظم التشغيلية، وضمان أن تكون المعاملات مرخصة (Authorized) ومسجلة ومحمية بشكل مناسب. إلى جانب أنها تُعتبر أساسية لضمان دقة وسلامة البيانات ومنع الاحتيال الذي قد يقوم به المستخدمون داخل المصرف.

تتيح العمليات المصرفية الإلكترونية المعتمدة على النظم الإلكترونية مجالاً أكبر وأسهل في عمليات انتحال الشخصية والاحتيال، إلى جانب أنّ العمليات أصبحت متكاملة ومختصرة بشكل أكبر ضمن تطبيقات الصيرفة الإلكترونية، وهذا يتطلب مراجعة إجراءات الرقابة الاعتيادية المستخدمة لضمان الفصل بين المهام بحيث تتناسب مع طبيعة العمليات المصرفية الإلكترونية وضمان السيطرة عليها. ومن الممارسات السليمة المستخدمة لضمان الفصل بين المهام هي أن يتم تصميم العمليات التشغيلية بحيث لا يتمكن شخص واحد فقط من إنشاء المعاملة والموافقة عليها وتنفيذها وإدخالها إلى النظام لأنّ ذلك يسمح بارتكاب الأفعال الاحتيالية وإخفاءها؛ إلى جانب فصل المهام بين المسؤولين عن إنشاء البيانات الثابتة والمسؤولين عن ضمان سلامتها، واختبار نظم الصيرفة الإلكترونية لضمان عدم القدرة على تجاوز الفصل بين المهام. وبشكل عام يمكن القول أنّ المسؤوليات والمهام التي يجب أن تُفصل وتنفذ من قِبل مجموعات مختلفة من العاملين تتضمن ما يلي: تشغيل النظم (Operating Systems Function)، تصميم النظام وتطويره (System Design and Development)، برمجة صيانة التطبيقات (Application Maintenance Programming)، العمليات الحاسوبية (Computer Operations)، إدارة قواعد البيانات، إدارة الأمن (Security Administration)، أمن البيانات (Data Security)، الاحتفاظ بملفات النسخ الاحتياطية من البيانات.

6-2- الرقابة الأمنية

(Security Controls)

يتوجب على مجلس الإدارة والإدارة العليا في المصرف تحمّل مسؤولية إدارة ورقابة المخاطر المرتبطة بالصيرفة الإلكترونية، وهذه المسؤولية تتطلب القيام بتحليل الخطر عبر تحديد أصول نظام المعلومات (Information System Assets)، وتحديد نقاط الضعف الموجودة فيها، والتعرف على التهديدات الأمنية واحتمال استغلالها (أي احتمال الهجمات التي قد يتعرض لها النظام) وتقييم الخسائر المحتملة المرتبطة مع تلك الأحداث، واتخاذ الإجراءات الأمنية والرقابة الأمنية المناسبة لحماية تلك الأصول.

تُعتبر الرقابة الأمنية لأمن نظام المعلومات ضرورية لضمان سرية وسلامة وإتاحة مصادر تكنولوجيا المعلومات والبيانات المرتبطة بها، وهذه الرقابة الأمنية يمكن أن يتم تقسيمها إلى ثلاثة أنواع هي: الرقابة الوقائية والرقابة الكشفية والرقابة التصحيحية.

6-2-1- الرقابة الوقائية

(Preventive Controls)

تهدف الرقابة الوقائية (كما يُستدلّ من اسمها) إلى منع الحوادث الأمنية من الوقوع، وهذا يتطلّب القيام بوظيفتين مترابطتين: التأكد من الهوية (Authentication)، والتأكد من السماحية (Authorization).

تركِّز عملية التأكد من الهوية على اختبار هوية الشـــخص أو الجهاز (Device) الذي يحاول الوصـــول إلى النظام، في حين تقوم عملية التأكد من الســـماحية بتقييد وصـــول المســـتخدم المصـــدَّق (Authenticated User) إلى أجزاء محددة من النظام وتحديد الأعمال المســـموح له بتنفيذها. على سبيل المثال، الموظف في قسم التسويق قد لا يكون مخوّلاً للوصول إلى نظام كشف الرواتب، إضافةً إلى ذلك، فإنّ هذا الموظف قد لا يُسمَح له إلاّ بقراءة أسعار المنتجات والخدمات دون أن يملك السماحية لتغيير تلك الأسعار.

6-2-1-1- الرقابة المتعلّقة بالتأكد من الهوية

تحتاج المصارف التي تقوم بتقديم أي نوع من أنواع الخدمات المصرفية الإلكترونية إلى أساليب آمنة وكافية للتأكد من هوية عملائها، وذلك لحماية معلومات عملائها ومنع عمليات الاحتيال وانتحال الشخصية وغسيل الأموال إلى جانب توفير القوة القانونية للمعاملات والاتفاقيات الإلكترونية، فمخاطر العمل مع أشخاص غير مرخصين أو غير معرّفين بشكل صحيح في البيئة الإلكترونية يمكن أن يسبب للمصرف خسائر مالية وضرر بالسمعة، وذلك من خلال الاحتيال وكشف معلومات العملاء وتخريب البيانات وغيرها من المخاطر.

هناك العديد من الأساليب والتقنيات التي يمكن للمؤسسات المالية أن تستخدمها للتحقُّق من هوية عملائها، ويمكن أن يتم تلخيصها من خلال ثلاثة عناصر أساسية:

- بعض المعلومات، مثل كلمات المرور أو أرقام إثبات الشخصية Personal (PINs Identification Numbers)؛
- بعض الملكيات (Tokens) مثل البطاقات الذكية (Smart cards)؛
- بعض الخصائص الفيزيائية (المؤشر البيولوجي)، مثل البصمات أو الصوت.

لا يمكن اعتبار أي أسلوب من الأساليب الثلاث السابقة بمفرده مضموناً لأن لكل أسلوب محدودياته؛ فكلمات المرور مثلاً يمكن أن يتم تخمينها، والملكيات (Tokens) يمكن أن تُسرَق أو تُنسَخ، أمّا بالنسبة للتقنيات البيولوجية فهي مرتفعة الثمن، إضافةً إلى أنها ليست دقيقة 100%، فهي أحياناً ترفض مستخدمين شرعيين (على سبيل المثال، نظام التعرُّف على الصوت قد لا يتعرَّف على موظف مصاب بالزكام، وقارئات بصمة اليد قد ترفض شخصاً يرتدي خاتماً جديداً) وأحياناً تسمح بدخول أشخاص غير مرخَّص لهم بالدخول. إلى جانب ذلك، هناك نواحي أمنية تتعلق بتخزين المعلومات البيولوجية ذاتها، فتعرُّض القوالب البيولوجية (كالممثِّل الرقمي لبصمة الإصبع أو الصوت الشخصي) للانكشاف سيخلق مشاكل خطيرة لصاحبها مدى الحياة، لأنّ هذه الخصائص بعكس كلمات المرور أو (Tokens) لا يمكن استبدالها أو تغييرها.

بناءً على ما سبق، فإنّ استخدام أسلوبين أو الثلاثة معاً يُعتبَر أكثر فعالية، على سبيل المثال، يمكن أن يُطلَب من المســتخدم إدخال البطاقة الذكية في قارئة البطاقات إضــافةً إلى إدخال كلمة المرور، حيث يوفِّر ذلك تحكماً في الوصول أقوى من استخدام أي منهما على حدا.

تُستخدم أدوات التأكد من الهوية ذات العامل الواحد مثل كلمات المرور أو أرقام إثبات الشخصية (PINs) بشكل واسع للعديد من الأنشطة المرتبطة بالصيرفة الإلكترونية والتي تتضمن الاستعلام عن الرصيد ودفع الفواتير وخدمة تجميع الحساب للزبون، ولكن عملية التأكد من الهوية ذات العامل الواحد تُعتبر غير كفوءة للصفقات ذات المخاطر الكبيرة مثل الوصول إلى معلومات العميل أو تحويل الأموال إلى أطراف أخرى، بالتالي على المصارف أن تقوم بتقييم مدى كفاءة تلك التقنيات في ضوء المخاطر الجديدة المصاحبة للاعتماد على تقنيات الاتصال في تقديم خدماتها وخاصة شبكة الإنترنت. على سبيل المثال، يتم من خلال تقنيات Phishing وPharming الحصول على المعلومات الشخصية مثل كلمات المرور وتفاصيل الحساب وذلك عبر إرسال رسالة إلكترونية والإدعاء بكونها مرسلة من جهة قانونية توجه المستخدمين إلى مواقع ويب احتيالية يُطلب فيها تجديد المعلومات الشخصية أو ملئ الاستمارات التي تبدو قانونية، وكذلك Malware التي هي برمجيات مؤذية مصممة للاستيلاء على المعلومات الخاصة مثل كلمات المرور وأرقام الحسابات وأرقام الإثبات الشخصية وغيرها وإرسالها للآخرين. لذلك، يتوجب على المصارف أن تقوم بتطبيق عوامل متعددة للتأكد من الهوية أو أن تستخدم أنواع أخرى من الرقابة لتخفيض الخطر.

لا بدّ من مراعاة أنّ التطبيق المناسب هو أساس موثوقية وأمن أي نظام للتأكد من الهوية، وذلك لأنّ نجاح أسلوب معين لا يعتمد فقط على التكنولوجيا، بل يعتمد أيضاً على السياسات والإجراءات والرقابة المناسبة، فعلى سبيل المثال، يمكن أن يكون التطبيق غير المناسب لنظام التأكد من الهوية ذات العاملين أقل أمناً من النظام ذات العامل الواحد المطبق بشكل مناسب.

ليكون أسلوب التأكد من الهوية فاعلاً، يجب أن يحظى بقبول العملاء له وأن يكون أداؤه موثوقاً ومتوافقاً مع النظم الحالية والخطط المستقبلية.

تقنيات التحقق من هوية العميل (Verification)

تُعتبر عملية التحقق من هوية العميل عملية منفصلة ولكنها مكملة لعملية التأكد من الهوية (Authentication)، حيث يتم تنفيذها عادةً للتأكد من أنّ العميل مؤهل لاستخدام النظام الإلكتروني للمصرف وخدماته، وتتحقق عادةً من خلال ثلاث طرق أساسية:

- **التحقق الايجابي (Positive Verification)**

هنا يتم التحقق من أنّ المعلومات المالية المقدمة من قِبل صاحب الطلب (Applicant) مطابقة للمعلومات المتاحة من قِبل أطراف خارجية موثوقة، حيث يقوم المصرف بمقارنة إجابات صاحب الطلب على سلسلة من الأسئلة التفصيلية مقابل المعلومات الموجودة ضمن قاعدة معطيات موثوقة (مثلاً، التقرير الائتماني للعميل الجدير بالثقة) لمعرفة إن كانت المعلومات المقدمة من قِبل العميل المحتمل مطابقة للمعلومات الموجودة ضمن قاعدة المعطيات، وكلما كانت الأسئلة أكثر تفصيلاً كلما وفّرت الإجابات الصحيحة مستوى ثقة أعلى في صحة هوية مقدّم الطلب.

- **التحقق المنطقي (Logical Verification)**

وذلك للتحقق من أنّ المعلومات التي تمّ توفيرها مترابطة منطقياً، على سبيل المثال، تطابق رمز هاتف المنطقة التي يسكن فيها العميل، تطابق عنوان الشارع وغيرها من المعلومات.

- **التحقق السلبي (Negative Verification)**

هنا يتم التأكد من أنّ المعلومات التي تم تقديمها غير مرتبطة بنشاط احتيالي ما. على سبيل المثال، يمكن أن تتم مقارنة معلومات مقدّم الطلب مع قاعدة معطيات متوافرة عن عمليات

الاحتيال، وذلك لتحديد إن كان أي جزء من تلك المعلومات مرتبطاً بحوادث معروفة للسلوك الاحتيالي.

عند التعامل مع العملاء التجاريين فإنّ الاعتماد الكلي على تقنيات مقارنة قاعدة المعطيات الإلكترونية غير كاف بسبب غياب بعض الوثائق القانونية التي يمكن من خلالها الحكم على سلوك الشركة، بالتالي على المصارف الاعتماد على الأشكال التقليدية لإثبات الهوية الشخصية والمصادقة الوثائقية إلى جانب الأدوات الإلكترونية لإثبات الشخصية.

6-2-1-2- الرقابة المتعلّقة بالتأكد من السماحية

تُعتبر المكونات المادية والبرامج والبيانات هي مصـــادر نظام المعلومات الأســاســية، وقد تظهر الحاجة إلى وصول المستخدمين لكل مصدر من هذه المصادر لتنفيذ عمليات معينة، ولكن تمكن المســتخدمين من الوصــول إليها بما يتجاوز الحد الأدنى المطلوب لتنفيذ العمل يمكن أن يعرّض سرية وسلامة وإتاحة المعلومات للخطر. بناء على ذلك تحتل إدارة حقوق الوصول أهمية كبيرة في تعريف وتحديد الوصول لأي مصدر من مصادر نظام المعلومات إلى الحد الأدنى المطلوب لتنفيذ العمل.

مصفوفة ضبط الوصول

يمكن التحقُّق من السماحيات عن طريق إنشاء مصفوفة ضبط الوصول (Access Control Matrix)، وهي عبارة عن جدول يحدِّد ســماحيات كل مســتخدم (أجزاء النظام المســموح للمستخدم الوصول إليها والأعمال التي يمكن أن يقوم بتنفيذها)، كما هو موضّح من خلال الشكل (6-1)، بحيث عندما يحاول موظفٌ ما الوصولَ إلى مورد نظام معلومات معيّن، فإنّ النظام يستخدم مصفوفة ضبط الوصول للتأكد من أن هذا الموظف يملك صلاحية الوصول إلى المورد المطلوب وتنفيذ العملية المطلوبة [Romney 2006][3].

[3] M. Romney and P. Steinbart, "Accounting Information Systems", 10th Edition, Pearson Prentice-hall, Inc. 2006.

تجدر الإشارة هنا إلى أهمية التحديث الدوري لمصفوفة ضبط الوصول، وذلك حتى تعكس التغيّرات الحاصلة في واجبات العمل نظراً للترقيات والتحويلات.

المستخدم		الملفات			البرامج			
هوية المستخدم	كلمة المرور	A	B	C	1	2	3	4
Ahmad	X6$qT3w)	0	0	1	0	0	0	0
Nihad	M!Y23Czu	0	2	0	0	0	0	1
Reem	Ur8&mP3n	1	3	0	1	1	0	0
….	….	….	….	….	….	….	….	….

دليل رموز الوصول إلى البرنامج:
0 = عدم السماح بالوصول
1 = تنفيذ

دليل رموز الوصول إلى الملف:
0 = عدم السماح بالوصول
1 = قراءة/عرض فقط
2 = قراءة/عرض، تعديل
3 = قراءة/عرض، تعديل، إنشاء، حذف

الشكل (6-1): مثال عن مصفوفة ضبط الوصول

يجب أن لا يقتصر تطبيق إجراءات التأكد من الهوية والسماحية على المستخدمين، وإنّما يجب أن يشمل الأجهزة المستخدَمة أيضاً. حيث تحتاج كل أداة حاسوبية (محطة عمل، طابعة، الخ) إلى بطاقة واجهة الشبكة NIC (Network Interface Card) للاتصال بالشبكة الداخلية للمنظمة، وكل NIC لها معرِّف مميّز خاص بها يُشار إليه عادةً بـــ MAC (Media Access Control)، وبالتالي من الممكن استخدام عناوين MAC في عمليات التأكد من الهوية، بحيث يمكن أن يُحدَّد الوصول إلى الشبكة فقط لتلك الأجهزة التي تمتلك عناوين MAC التي تمّ التعرّف عليها.

يمكن أيضاً استخدام عناوين MAC في عمليات التأكد من السماحية، على سبيل المثال، يُتيح تضمين عناوين MAC في مصفوفة ضبط الوصول إمكانيةَ منح صلاحية الوصول إلى نظام كشف الرواتب مثلاً والملفات الرئيسية فيه فقط لموظفي قسم الرواتب وفقط عندما يسجِّلون دخولهم من حواسيب مكاتبهم أو من حواسيب شخصية محدَّدة.

على الرغم من أن التأكد من الهوية والسماحية هما الأساس في تحديد الوصول إلى مصادر نظام المعلومات، فإن توفُّر ضـوابط وقائية أخرى يُعتبَر ضـرورياً لتحقيق أمنٍ كافٍ ومنع حدوث الانتهاكات الأمنية، والأنواع الخمسَ الإضـافية الأسـاسـية للرقابة الوقائية هي: التدريب، والتحكم في الوصـول المادي، والتحكم في الوصـول عن بعد، والتشـفير، وتقوية الحاسب المضيف والتطبيق (Host and Application Hardening).

6-2-1-3- التدريب

يلعب التدريب دوراً أسـاسـياً في أمن المعلومات، لأنّ فاعلية إجراءات رقابية معيّنة تعتمد بالكامل على مدى فهم الموظفين وإتباعهم للسياسات الأمنية للمنظمة، ولذلك يُعتبَر التدريب رقابةً وقائية أساسية. فمن الضروري أن يتم تقديم الإرشادات لجميع الموظفين عن أهمية وضرورة الإجراءات الأمنية لبقاء المصرف على المدى البعيد، وأن يتم تدريبهم على إتباع الممارسات الحاسوبية الآمنة (على سبيل المثال، عدم فتح الروابط غير المطلوبة المرافقة للبريد الإلكتروني، واسـتخدام البرمجيات المصـدَّق عليها فقط، وعدم المشـاركة بكلمات المرور أو كشفها) واتخاذ الخطوات اللازمة لحماية الحواسيب مادياً.

يُعتبَر التدريب ضرورياً بشكل خاص لتنبيه الموظفين عن هجمات الهندسة الاجتماعية التي تعتمد على الخداع للوصول غير المشروع إلى مصادر المعلومات. على سبيل المثال، يجب تدريب الموظفين على عدم إفشـاء كلمات المرور أو أي معلومات أخرى عن حسـاباتهم أو عن مكوّنات محطات العمل لأي شـخص يتصـل عبر الهاتف، أو البريد الإلكتروني، أو الرسـائل الفورية (Instant Messages)، ويدّعي بكونه جزءاً من فريق أمن نظام المعلومات للمنظمة. إضافةً إلى ذلك، يجب تدريب العاملين على عدم السماح لأي شخص باللحاق بهم عبر البوابات المحدودة الدخول، لأنّ هجمات الهندسـة الاجتماعية، والتي يُطلَق عليها عادةً تسـمية Piggybacking (النقل على الظهر)، يمكن أن تحدث عند المداخل الرئيسـية للمبنى وعند أي أبواب مغلقة داخلية وخاصـةً الغرف التي تحوي المعدّات الحاسـوبية. إلى جانب ذلك، فإنّ محاولات Piggybacking (النقل على الظهر) يمكن أن تتم على السواء من قِبل غير المنتمين للمنظمة ومن قِبل الموظفين غير المخول لهم الدخول إلى أماكن محدّدة، وتنجح

هذه المحاولات عادةً لأنّ العديد من الأشخاص يشعرون بالإحراج بعدم السماح لشخص آخر بالدخول معهم عبر المدخل، ولذلك فإنّ لعب الأدوار يُعتبَر مهماً جداً للتعامل مع هجمات الهندسة الاجتماعية.

تجدر الإشارة إلى أنّ التطور التكنولوجي يولد تهديدات أمنية بشكل مستمر مما يجعل الحلول القديمة غير فعّالة، ولذلك يترتب على المصارف أن تدعم التعلّم المتمرّس المستمر لمختصّي الأمن لتطوير الاستجابة والمهارات لديهم.

6-2-1-4 - التحكم في الوصول المادي

يُعتبَر التحكم في الوصول المادي مستوى مهم آخر للرقابة الوقائية، فمع الوصول المادي المباشر غير المراقب إلى النظام يمكن للشخص المحترف أن يصل بنجاح خلال عدة دقائق إلى البيانات الحساسة وذلك عبر إدخال أقراص تحفيز خاصة توفر امتيازات وحقوق غير مقيّدة على الحاسب المستهدف، كما يمكن أن يتم تركيب أداة خاصة (Keystroke Logger) التي ستستولي على كلمات سر الضحية وعندما يعود المهاجم لاحقاً ويسترد الأداة يمكنه عندها أن يستخدم محددات الهوية (Credentials) المستولى عليها للوصول غير المرخّص إلى مصادر النظام.

أولاً: الرقابة على الدخول لمبنى المصرف

تبدأ عملية الرقابة على الوصول المادي مع نقاط الدخول إلى المبنى نفسه، حيث من الأمثل أن تكون هناك نقطة دخول واحدة دائمة تبقى مفتوحة خلال ساعات العمل، ونظراً للحاجة إلى وجود مخارج إضافية للحريق فإنّ هذه المخارج يجب أن ترتبط بنظام إنذار يُفعّل بشكل أوتوماتيكي عندما يُفتح مخرج الحريق، ولا تسمح بالدخول من خارج المبنى. إضافة إلى ذلك، لا بد من تعيين الحارس الأمني أو موظف الاستقبال عند المدخل الرئيسي لمبنى المصرف للتأكد من هوية الموظفين، وطلب التوقيع من كل الزائرين والحرص على مقابلة كل زائر بموظف يلاحقه أينما ذهب داخل المبنى.

ثانياً: الرقابة على الوصول المادي إلى الغرف داخل المبنى

أثناء التواجد داخل المبنى فإن الوصـــول المادي إلى الغرف التي تحوي العتاديات المختلفة للحاسـب يجب أن يكون مقيداً أيضـاً، حيث يتوجب أن تكون هذه الغرف مغلقة بإحكام، وأن تكون كـل المـداخـل والمخـارج المرتبطـة بهـا مراقبـة بـأنظمـة تلفزيونيـة (Closed Circuit Television Systems)، كما أنّ عدة محاولات فاشلة للدخول يجب أن تفعّل جهاز الإنذار.

يجب أن يتم دعم الأقفال الاعتيادية للغرف التي تحوي المخدّمات الممتلكة لبيانات حسـاسـة بشـكل خاص بتكنولوجيا أقوى مثل قارئات البطاقات أو لوحات المفاتيح الرقمية أو الأدوات البيولوجية المختلفة (على سبيل المثال، ماسحات الشبكية أو قزحية العين أو قارئات بصمة الإصبع أو معرّفات الصوت).

تعتبر إجراءات التحكم في الوصول إلى مخرجات النظام ضرورية أيضاً وتتضمن القيام بما يلي:

- عدم السماح للزوار بالتجوّل داخل المبنى دون مراقبة لمنعهم من رؤية المعلومات الحساسة على أجهزة عرض محطات العمل، أو قراءة التقارير المطبوعة؛
- خروج الموظفين من جميع التطبيقات عند تركهم لمحطات عملهم دون مراقبة، بحيث لا يتمكن الموظفون الآخرون من الوصول غير المشروع إلى المعلومات في تطبيق معين، إلى جانب ذلك، يجب أن تستخدم كل محطات العمل شاشات التوقف المحمية بكلمات المرور التي تعمل بشكل أوتوماتيكي في حال غياب أي نشاط لفترة معينة من الزمن؛
- تقييد الوصول إلى الغرف التي تحوي الفاكس والطابعات؛
- تشفير التقارير لتعكس أهمية المعلومات المحتواة فيها، وتدريب الموظفين على عدم ترك التقارير المحتواة على معلومات حساسة في أماكن مكشوفة على سطح المكتب عند غيابهم عنه.

ثالثاً: التخلص من مصادر المعلومات

تعتبر عملية التخلص من مصادر المعلومات من الجوانب المهمة التي يجب أن تتم مراقبتها بعناية، فالتقارير المطبوعة والمايكروفيلم المحتوية على معلومات حساسة يجب أن يتم تخريبها قبل رميها، أما المعلومات المخزنة على الوسائط الضوئية المغناطيسية فإنّ عملية تدميرها تحتاج إلى إجراءات خاصة لأنّ استخدام أوامر النظام التشغيلي لحذف تلك المعلومات غير كاف بسبب وجود العديد من البرامج (Utility Programs) التي تمّ تطويرها لاستعادة الملفات المحذوفة، فعلى سبيل المثال، تمكنت إحدى الشركات البريطانية عندما اشترت 100 قرصاً صلباً من أحد المواقع من استعادة البيانات الموجودة من 70% من تلك الأقراص.

يتطلب التخلص المناسب من الوسائط الحاسوبية استخدام برمجيات خاصة مصممة لتنظيف تلك الوسائط عن طريق إعادة الكتابة على القرص بشكل متكرر مع نماذج عشوائية من البيانات، وبشكل بديل يمكن إخضاع الأقراص والشرائط المغناطيسية لأجهزة تنزع الخصائص المغناطيسية عنها.

رابعاً: الرقابة على الوصول إلى عتاديات الشبكة الداخلية للمصرف

الوصول إلى الأسلاك المستخدمة داخل الشبكات الداخلية للمصرف LANs (Local Area Networks) يحتاج لأن يتم تقييده أيضاً لمنع عمليات التنصّت (Wiretapping)، هذا يعني أن الكابلات والأسلاك يجب أن لا تكون مكشوفة في أماكن يسهل الوصول إليها من قبل الزوار، إلى جانب أنّ المقابس غير المستخدمة يجب أن تكون منفصلة مادياً عن الشبكة لمنع محاولات الوصول إلى الشبكة من قبل شخص ما قام فقط بوصل حاسبه الشخصي بها.

يجب أن تكون الخزائن السلكية المخزنة لتجهيزات الاتصالات عن بعد مقفلة أيضاً بشكل آمن، وفي حال كانت هذه الخزائن مشتركة مع مستأجرين آخرين داخل المبنى فإنه يترتب على المصارف وضع تجهيزات اتصالاتها داخل أقفاص فولاذية مقفلة لمنع الوصول المادي غير المشروع إليها من قبل أي شخص آخر يملك إمكانية الوصول إلى تلك الخزانة.

تتطلب الحواسيب الشخصية (Laptops) والهواتف الخليوية وأجهزة PDA (المساعدات الشخصية الرقمية) اهتماماً خاصاً، فخطورة سرقة الحواسيب الشخصية مثلاً لا تتمثّل في تكاليف استبدالها وإنما في خسارة المعلومات السرية التي تحويها وتكلفة إشعار المتأثرين. على سبيل المثال، عندما تمت سرقة الحاسب الشخصي لموظف في مصرف (Wells Fargo) المحتوي على معلومات الحساب الشخصية، فقد تكبّد المصرف تكاليف إشعار الآلاف من الزبائن عن تعرض معلوماتهم الشخصية المحتمل للخطر، وتكاليف مساندتهم في تغيير كلمات المرور ومعلومات الحساب..

للتعامل مع تهديد سرقة الحواسب الشخصية يجب أن يُدرّب الموظفون على إقفال حواسيبهم بشكل دائم في مواقع غير متحركة، وهذا ضروري حتى أثناء تواجدهم في مكان العمل، فهناك حالات عديدة تمت فيها سرقة الحواسيب الشخصية والمعدات الأخرى خلال ساعات العمل وذلك عن طريق التظاهر كطاقم التنظيف. إضافة إلى ذلك فإن البيانات الحساسة يجب أن تُخزّن على وسائط تخزين قابلة للنقل وليس على مشغل الأقراص الصلبة (Hard Drive).

بناءاً على ذلك وبسبب احتمال السرقة فإن خبراء الأمن يقترحون القيام بتشفير البيانات الحساسة والسرية أثناء تخزينها لتخفيض احتمال وصول السارق إليها إلى الحد الأدنى، وبعض الشركات تقوم بتحميل برمجيات خاصة على حواسيبهم الشخصية بحيث في حال تمت سرقة أحدها سيتصل الحاسب أوتوماتيكياً برقم محدد ويكشف عن موقعه الحالي عندما يحاول السارق استخدامه للاتصال بشبكة الإنترنت.

تُستخدم الهواتف الخليوية وأجهزة PDAs أيضاً بشكل كبير في تخزين المعلومات السرية ولهذا السبب تحتاج لنفس أنواع الرقابة المستخدمة مع الحواسيب الشخصية، ومن المهم أيضاً تقييد الوصول إلى طابعات الشبكة لأنها تخزن عادة صور المستندات على مشغل الأقراص الصلبة الذي بسرقته سيتمكن السارق من الوصول إلى المعلومات الحساسة.

بالنهاية، أمن الوصول المادي يجب أن يكون اقتصادياً وهذا يتطلب مشاركة الإدارة العليا في تخطيط ذلك الأمن للتأكد من أنّ كل مصادر نظام المعلومات مقيَّمة بشكل مناسب وأن طبيعة وتشكيلة ضوابط الوصول تعكس قيمة الأصول المحمية.

6-2-1-5- التحكم في الوصول عن بعد

توفر معظم المنظمات لموظفيها وزبائنها ومورديها إمكانية الوصـــول عن بعد (Remote Access) إلى نظم معلوماتها (يتحقق ذلك الوصـــول عادة عبر شـــبكة الإنترنت). يمكن أن يكون الوصـول عن بعد ضـرورياً ليتمكن الموردون من دعم النظام وإصـلاح البرامج في الحالات الطارئة، ولذلك على الإدارة وضـع السـياسـات الملائمة التي تقيد ذلك الوصـول، وأن تكون على معرفة كاملة بجميع الأجهزة الملحقة بنظمها التي تتمكن من الوصـــول عن بعد ومراقبتها.

الوقاية الحدودية

وتتحقق عن طريق **الموجّهات** (Routers)؛ **والجدران النارية** (Firewalls)؛ **والنظم المانعة للاقتحام** (Intrusion Prevention Systems).

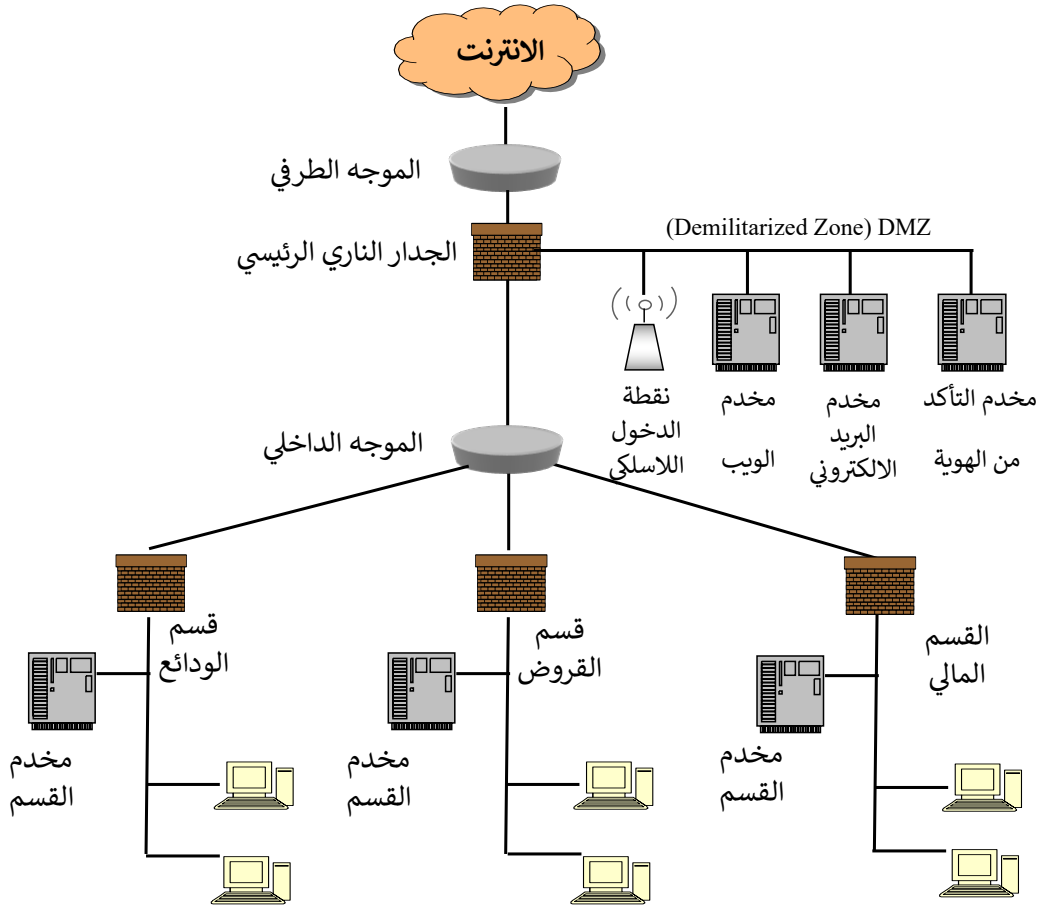
يبيّن الشـكل (6-2) العلاقة بين نظام معلومات المصـرف والإنترنت، حيث يتصـل نظام المعلومات بالإنترنت عبر جهاز يدعى الموجّه الطرفي (Border Router) يتبعه الجدار الناري الرئيسي (Main Firewall) والذي هو (الجدار الناري) عبارة إما عن عتاد صلب ذات هدف محدّد أو برمجية تقوم بعملها على حاسـب عام الغرض. كما يبيّن الشـكل (6-2) أنّ مخدّم الويب (Web) ومخدّم البريد الإلكتروني يقعان على شـبكة منفصـلة تدعى DMZ (Demilitarized Zone) لأنها موجودة خارج شبكة المصرف ولكن يمكن الوصول إليها عبر شبكة الإنترنت، وبالتالي فهي تعمل كصلة وصل بين الشبكة الداخلية الموثوقة للمصرف والشبكة الخارجية غير الموثوقة مثل شبكة الإنترنت.

يعمل كل من الموجّه والجدار الناري معاً كمفلتر للتحكم في المعلومات المسـموح لها بالدخول إلى والخروج من نظام معلومات المصـرف، ولفهم آلية عمل كل منهما لا بدّ أولاً من معرفة كيفية انتقال المعلومات عبر الإنترنت.

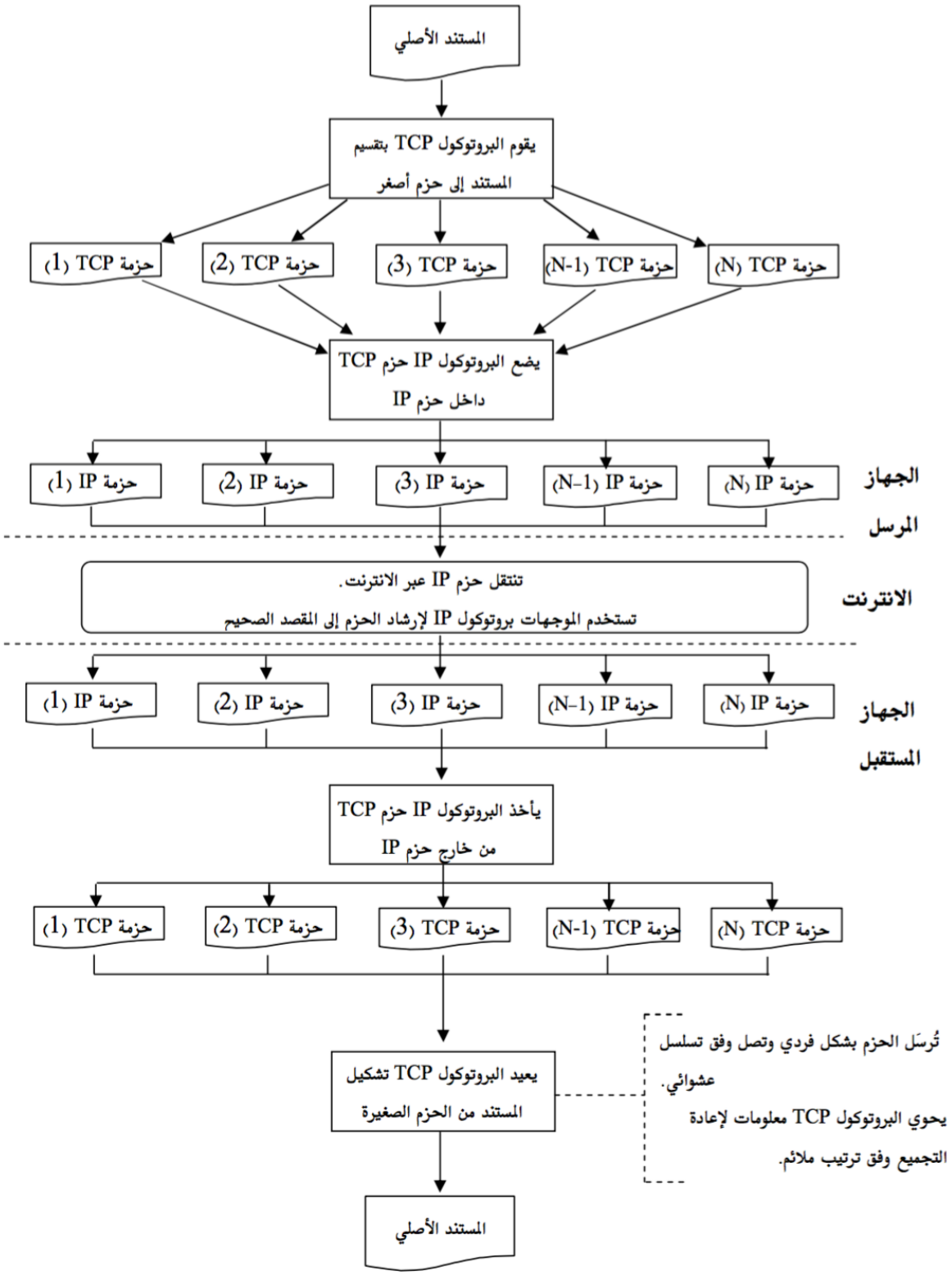
آلية انتقال المعلومات عبر الإنترنت

تنتقل المعلومات عبر الإنترنت والشبكات المحلية على شكل مجموعات من الرموز تدعى بالحزم (Packets)، بالتالي فإن المستندات والملفات لا تُرسل بكاملها وإنما يتم تقطيعها إلى حزم وهذه الحزم هي التي تُرسل عبر الشبكة المحلية أو الإنترنت إلى مقصدها، والأداة المستلمة لتلك المجموعات تُعيد تركيبها لإعادة خلق المستند أو الملف الأصلي.

قواعد وإجراءات معرّفة تدعى بروتوكولات تحدد كيفية تنفيذ هذه العمليات، حيث يبين الشكل (6-3) كيف تُنظَّم عملية إرسال المعلومات عبر الإنترنت باستخدام بروتوكولين رئيسيين يشار إليهما بـ IP/TCP.



الشكل (6-2): العلاقة بين نظام معلومات المصرف وشبكة الإنترنت



الشكل (3-6): وظائف البروتوكولين TCP/IP

بروتوكول التحكم بالنقل TCP (Transmission Control Protocol) يحدد الإجراءات اللازمة لتقسيم المستندات والملفات إلى حزم ليتم إرسالها عبر شبكة الإنترنت، وأساليب إعادة تركيب الملف أو المستند الأصلي عند الوجهة.

بروتوكول الإنترنت IP (Internet Protocol) يحدد بنية هذه الحزم وكيفية توجيهها إلى الوجهة المناسبة بما يسهل عملية الإرسال الفعّال عبر الإنترنت. تتكون كل حزمة IP من جزأين: الترويسة والجسم، تحوي الترويسة على عناوين مصدر الحزمة ووجهتها إضافة إلى معلومات عن نوع البيانات المحتواة في جسم الحزمة.

تتم قراءة عنوان الوجهة المحتواة في ترويسة حزم IP لتحديد وجهة الحزمة كخطوة تالية عن طريق أجهزة خاصة الغرض تدعى الموجّهات (Routers). يقوم الموجّه الطرفي للمصرف باختبار عنوان الوجهة الموجود في كل حزمة يستلمها حيث يقوم بإعادة إرسال الحزمة إلى موجّه آخر على شبكة الإنترنت إذا لم يكن العنوان مطابقاً لعنوان المصرف، وفي حالة المطابقة فإنّ الحزمة تخضع لاختبار واحد أو لعدة اختبارات قبل السماح لها بالدخول.

تستخدم الموجّهات مجموعةً من القواعد تدعى قوائم التحكم بالوصول ACL (Access Control List) وذلك لتحديد الحزم التي يجب أن يُسمح لها بالدخول والحزم التي يجب أن تُرفض، وبالتالي فهي تنفّذ ما يسمى بالفلترة المستقرة للحزم (Static Packet Filtering) لأنّ فحص الموجّهات لكل حزمة يعتمد بشكل كلي على مكونات المصدر و/ أو الوجهة الموجودة في ترويسة حزمة IP.

تتلخص وظيفة الموجه الطرفي على التحديد السريع لأنواع محددة من الحزم ومنعها من الدخول والسماح لكل الحزم الأخرى أن تتجاوزه إلى الجدار الناري، حيث يخضعون لاختبار أكثر تفصيلاً قبل أن يسمح لهم بالوصول إلى الشبكة الداخلية للمصرف.

الجدار الناري (Firewall)

رفعت الفيروسات والبرامج الطفيلية الحاجة إلى أمن الشبكة بمختلف أنواعها بشكل كبير، حيث تُشكل الفيروسات والبرامج الطفيلية القسم الأكبر من الأعمال الهجومية، وهي تبحث عن

أهدافها بشكل عشوائي. لذلك تحتاج جميع المنظمات حتى الصغيرة منها والتي لا تمتلك أي معلومات سرية إلى الجدران النارية لحماية شبكاتها من هذه الهجمات الآلية.

يُعرّف الجدار الناري بأنه عبارة عن جمع بين العتاد الصلب (Hardware) والعتاد البرمجي (Software) المتوضع بين شبكتين، حيث تعبر من خلاله جميع أنواع حركات العبور (Traffic) بغض النظر عن اتجاهها، وهو يُعتبر إجراء الأمن الرئيسي في ضبط الرقابة المرتبطة بالوصول وحماية النظام الداخلي

تعتمد قدرة الجدار الناري في حماية الشبكة على إعداداته (Configuration) وتوضعه داخل النظام، فمنتجات الجدار الناري لا تقدم حماية أمنية مناسبة بمجرد شرائها وإنما لا بد من أن يتم إعدادها لتسمح أو لتمنع من الدخول حركات العبور (Traffic) المناسبة.

هناك أنواع مختلفة للجدار الناري، ويعتمد اختيار نوع معين منها على العديد من الخصائص المرتبطة بالمنطقة الأمنية (Security Zone)، على سبيل المثال، كمية حركات العبور (Traffic) ودرجة حساسية النظم والبيانات والتطبيقات، إلى جانب مدى سهولة إدارة الجدار الناري ومقدار الدعم المطلوب لمتابعة الجدار الناري من خلال الدخول الآلي وتحليل معلومات الدخول، وقدرة الجدار الناري على الإنذار عند وجود نشاط غير اعتيادي. غير أنه من الأفضل للمصارف أن تقوم باستخدام أنواع مختلفة من الجدران النارية لأنّ استخدام نوع واحد فقط سيمكن المتطفل الذي تمكن من تجاوز جدار واحد فقط من تجاوز الجدران النارية الأخرى عن طريق استغلال نقاط الضعف في الأمن ذاتها الموجودة فيها، وبالتالي سيكون توضع الجدار الناري عند كل نقطة اتصال بين الشبكات الجزئية للمصرف لضمان أمن الشبكة الداخلية عديم الجدوى.

يستخدم الجدار الناري مثل الموجه الطرفي قوائم التحكم بالوصول لتحديد ما الذي يجب فعله مع كل حزمة تصل إليه، ولكن الاختلاف الأساسي يكمن في أنّ الجدار الناري مصمّم ليعمل كمفلتر حيث يسمح بالعبور فقط لتلك الحزم التي تقابل شروطاً معيّنة، حيث يعتمد قبول أو رفض الجدار الناري لحركة العبور على مجموعة من القواعد المحددة من قِبل المدير، وهذه القواعد قد تكون ثابتة أو متغيرة، ولتوفير مستوى أمن أعلى فإنّ القاعدة الأساسية يجب أن

تكون رفض كل حركات العبور إلا في حال كان السماح لها بالدخول واضحاً، وهذا يتطلب من مدراء النظم القيام بمراجعة وتقييم الحاجة لكل الأنشطة المسموحة إلى جانب تحديد من سيحتاج إلى استخدامها.

تتكون مجموعة القواعد الثابتة من تعليمات يتم تطبيقها على ترويسة الحزمة، على سبيل المثال منع دخول جميع حركات العبور (Traffic) القادمة من عناوين مصدر محددة مسبقاً، أما القواعد المتغيرة فهي تكون عادة نتيجة التوافق بين الجدار الناري ونظام الكشف عن الاختراق (IDS). على سبيل المثال، قد يُرسل نظام الكشف عن الاختراق -الذي يُنبِّه بوجود نشاط غير اعتيادي- رسالة إلى الجدار الناري لمنع عنوان IP القادم من العبور والذي يقوم بدوره أي الجدار الناري -بعد التأكد من عدم وجود ذلك العنوان ضمن القائمة المسموح لها بالعبور- بتوليد قاعدة تمنع حركات العبور القادمة مع ذلك العنوان من الدخول، ولكن بعد مرور فترة معينة تنتهي صلاحية تلك القاعدة ويُسمح لحركة العبور القادمة مع ذلك العنوان بالدخول.

لتوفير حماية أفضل لا بدّ من تحميل الجدار الناري عند كل نقطة يتصل فيها نظام الحاسب مع شبكة أخرى، إلى جانب ضرورة أن يتم إعداد الجدار الناري بحيث يمنع كل المحاولات للدخول في حال حدوث أي خلل في نظام الجدار الناري.

يستخدم الجدار الناري تقنيات أكثر تعقيداً من الموجّهات الطرفية في فلترة الحزم. على سبيل المثال، تستخدم معظم الجدران النارية فلترة الحزم المحتفظة بالحالة (Stateful Packet Filtering) التي تقوم بفحص كل حزمة IP على حدى، حيث يتم الاحتفاظ بجدول يسجل كل الاتصالات المنشأة بين حواسيب المصرف والإنترنت يعود الجدار الناري إليه لمعرفة ما إذا كانت الحزمة القادمة هي جزء من الاتصال الجاري المباشر من قِبل حاسب داخلي أو لا. تمكّن هذه المعلومات الجدار الناري من رفض حزم الهجوم التي عبرت الفلترة المستقرة للحزم البسيطة متظاهرة بكونها استجابة لطلب منشأ داخلياً، بينما في الواقع لم يحدث مثل ذلك الطلب سابقاً.

نظم إعاقة الاقتحام IPS

تســـتخدِم نظم إعاقة الاقتحام تقنيات مختلفة للتعرّف على الحزم غير المرغوبة، ومن هذه التقنيات:

- فحص محتويات الحزمة مقابل نماذج قاعدة معطيات (رموز التعريف/ علامات مميزة متشابهة) لأساليب هجوم معروفة؛
- تطويرَ ســـمات (Profile) لحركات العبور (Traffic) الطبيعية واســـتخدام التحليل الإحصائي للتعرف على الحزم التي لا تطابق تلك السمات؛
- الاعتماد على القواعد (Rule Bases) التي تحدّد معايير مقبولة مســـبقاً لأنواع محدّدة من حركات العبور ورفض كل الحزم التي لا تتطابق مع تلك المعايير.

6-2-1-6- تقوية المضيف و التطبيق

(Host and application Hardening)

يمكن تحسين أمن نظام المعلومات في المصرف عبر تدعيم الرقابة الوقائية الحدودية (الموجهات والجدران النارية ونظم منع الاختراق) برقابة وقائية إضافية على محطات العمل والمخدّمات والطابعات والأجهزة الأخرى التي تتكوّن منها الشبكة والتي يشار إليها جماعياً عادة بـ Hosts، وهذا يشبه دعم الأبواب الخارجية المقفلة وأنظمة الإنذار في المنازل ومكاتب العمل بالمكاتب المقفلة والخزن الحديدية المقفلة لحفظ الأشياء الثمينة.

إعدادات الأجهزة المضيفة

يمكن أن نجعل الأجهزة المضيفة (Hosts) أكثر أمناً من خلال تطوير إعداداتها، حيث تحتوي الإعدادات الافتراضية لمعظم الأجهزة عادةً على عدد كبير من الإعدادات الاختيارية التي نادراً ما يتم استخدامها. بشكل مماثل، تفعِّل الإعدادات الافتراضية لنظم التشغيل العديدَ من الخدمات غير الضرورية. وتجدر الإشارة إلى أنّ تفعيل الخصائص غير الضرورية والخدمات الإضافية يزيد من احتمال نجاح عملية التحميل للبرمجيات، ولكن هذه الملاءمة تكون على حساب خلق الضعف في الأمن، فكل برنامج يعمل على المضيف يمثل نقطة هجوم محتملة لأنه على الأرجح يمتلك نقاط ضعف يمكن أن يتم استغلالها إما لإيقاف النظام أو

للتحكم به، ولهذا السبب فإنّ أي خصائص أو برامج اختيارية غير مستخدمة يجب أن يتم إلغاءها.

إلى جانب عملية إلغاء الخصائص غير الضرورية والتي تسمى بـ Hardening ، هناك نوعان إضافيان للرقابة الوقائية للأجهزة المضيفة داخل الشبكة:

أولاً: يجب أن يمتلك كل مضيف برمجيات مضادة للفيروسات التي يتم تحديثها دورياً؛

ثانياً: يجب أن يحوي كل مضيف مخزّن لمعلومات حساسة على برمجيات الجدار الناري وأن يتم تحديثها أيضاً بشكل دوري.

إدارة حسابات المستخدمين والامتيازات

يجب أن تتم إدارة حسابات المستخدمين بحرص كبير وخاصةً تلك الحسابات التي تمتلك حقوقاً غير محدودة (إدارية) على حاسب معين. هذا يتطلب تخصيص حسابين لكل مستخدم يحتاج لسيطرة إدارية على حاسب معين، بحيث يمتلك حساباً لممارسة حقوقه الإدارية وحساباً آخر له امتيازات محدودة فقط، بحيث يسجل المستخدم دخوله تحت الحساب المحدود لتنفيذ التزاماته اليومية، وخاصة عند تصفح الويب أو قراءة البريد الالكتروني، لأنه بهذه الطريقة في حال قيامه بزيارة موقع إلكتروني مشبوه أو فتح رسالة إلكترونية مليئة بالفيروسات، فإنّ المهاجم سيتمكن من الحصول على حقوق محدودة فقط على الحاسب.

عند حاجة الموظفين المرخصين لممارسة حقوقهم الإدارية مثل تحميل برمجيات جديدة على الحاسب، يمكنهم القيام بذلك عبر تفعيل ذلك الأمر المحدّد فقط كمدير.

من الضروري أيضاً إدارة الحسابات الافتراضية التي يتم إنشاءها أثناء تحميل نظام التشغيل. على سبيل المثال، نظام Windows ينشئ حساب المدير وحساب الضيف، وعلى الرغم من أنّ حساب الضيف يمتلك قدرة محدودة فقط فإنه يؤمن دخولاً غير معروف، وبالتالي من غير الممكن معرفة هوية الشخص الذي استخدم ذلك الحساب وما هي مصادر النظام التي تمكن من الوصول إليها، وبالتالي فإنّ حساب الضيف الاختياري يجب أن يتم إلغاءه.

تصميم البرمجيات

تُعتبَر الرقابة على البرامج ضروريةً أيضاً، لأنّ الكود (Code) المكتوب بطريقة غير مناسبة يمكن أن يتم استغلاله لإعطاء المهاجمين امتيازات إدارية.

يُعتبر النقص الرئيسي في معظم التطبيقات المطورة أو المعدلة داخلياً هو الفشل في مراقبة بيانات الإدخال بشكل كاف، وتسمى نقطة الخلل الأكثر شيوعاً المرتبطة ببيانات الإدخال بهجمات امتلاء الذاكرة (Buffer Overflow Attack) التي يقوم المهاجم من خلالها بإرسال بيانات إلى البرنامج أكثر مما يستطيع البرنامج معالجته، ويمكن أن تسبب هجمات امتلاء الذاكرة توقفَ النظام أو حتى قد توفر سلطة توفر للمهاجم امتيازات إدارية كاملة وسيطرة على الجهاز.

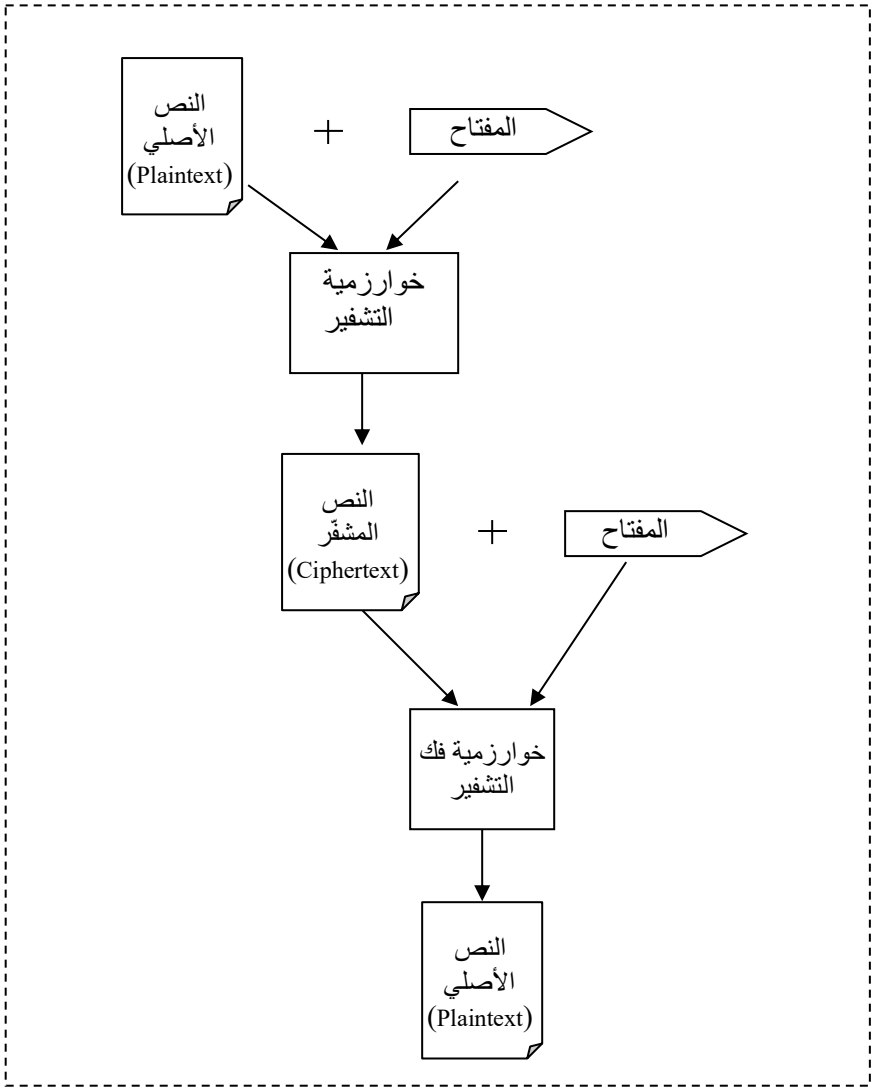
6-2-1-7- التشفير

تُعتبر عملية التشفير (Encryption) هي المستوى الأخير للرقابة الوقائية التي يجب تجاوزها ليتمكن المقتحم من الوصول إلى مصدر معلومات معين إلى جانب أنّ عملية التشفير تحل المشاكل الأمنية المتعلقة بسرية وسلامة المعلومات أثناء تخزينها أو انتقالها عبر الشبكات الداخلية أو الخارجية، إضافة إلى أهمية التشفير في توليد التواقيع الرقمية المستخدمة للتأكد من الهوية وعدم الإنكار (Non- Repudiation).

تقوم عملية التشفير بتحويل النص الأصلي الذي يسمى Plaintext إلى كتابات غير مفهومة تسمى Ciphertext. يعكس فك التشفير (Decryption) هذه العملية بتحويل النص المشفر (Ciphertext) إلى النص الأصلي (Plaintext).

تحتاج عملية التشفير إلى توفر الأمور التالية كما هو موضح في الشكل (6-4):

1- مفتاح التشفير: وهو معادلة حياكة لغز تشفير البيانات؛
2- خوارزمية التشفير (Encryption Algorithm): إجراءات عملية التشفير وتسلسلها؛
3- مفتاح فك التشفير: معادلة فك لغز التشفير؛
4- خوارزمية فك التشفير: إجراءات فك التشفير وتسلسله.



الشكل (6-4): عملية التشفير وفك التشفير

يرمّز الحاسب النصَّ الأصلي (Plaintext) و النصَّ المشفّر (Ciphertext) بسلسلة من الأرقام الثنائية (الصفر والواحد)، والمفتاح هو أيضاً سلسلة من الأرقام الثنائية ذات طول ثابت، فمثلاً مفتاح طوله 128 بت يتكون من 128 صف من الأصفار والواحدات، أمّا الخوارزمية فهي الصيغة التي تجمع المفتاح مع النص.

نظراً لكون معظم الوثائق أطول من المفتاح، يقوم الحاسب أولاً بتقسيم النص الأصلي (Plaintext) أو النص المشفّر (Ciphertext) إلى مجموعات بحيث يكون طول كل مجموعة مساوياً لطول المفتاح، وبعد ذلك يتم تطبيق الخوارزمية على كل مجموعة من النص. على سبيل المثال، إذا تم استخدام مفتاح طوله 128 بت يقوم الحاسب أولاً بتقسيم الملف أو المستند

إلى مجموعات طول كل منها 128 بت، ومن ثم يدمج (Combine) كل مجموعة مع المفتاح بالطريقة المحددة في الخوارزمية، وبالتالي تنتج نسخة النص المشفّر للملف أو المستند الأصلي المساوية في الحجم للأصل، ولإعادة إنتاج المستند الأصلي يقوم الحاسب أولاً بتقسيم النص المشفّر (Ciphertext) إلى مجموعات بحجم 128 بت ومن ثم يطبق مفتاح فك التشفير على كل مجموعة.

بما أنّ التشفير يحول المعلومات إلى مجموعة غير منظمة من الأحرف والرموز، فإنّ المعلومات تبقى سرية سواء أثناء تخزينها أو انتقالها داخل النظام وبالتالي حتى لو تمكنت الأطراف غير المشروع لها من الوصول إلى تلك المعلومات فهي لن تتمكن من قراءتها.

6-2-1-7-1-قوة التشفير

تتحدد قوة أي نظام تشفير من خلال ثلاثة عوامل أساسية هي: طول المفتاح، و سياسات إدارة المفتاح، و طبيعة خوارزمية التشفير.

- طول المفتاح: توفر المفاتيح الطويلة عادة تشفيراً أقوى وذلك من خلال تقليل عدد المجموعات المتكررة للنص المشفّر، وهذا يجعل من الصعب أن يتم اكتشاف نماذج في النص المشفر (Ciphertext) لتعكس نماذج في النص غير المشفر الأصلي (Plaintext). على سبيل المثال، (The) هي من أكثر الكلمات ذات الثلاثة أحرف شيوعاً في اللغة الإنكليزية، وبما أنّ كل محرف في اللغة الإنكليزية يُمثَّل بشيفرة طولها 8 بت فإن مفتاح تشفير طوله 24 بت سيولد نص مشفر في مجموعات تُمثل كل منها ثلاثة محارف متتابعة. يُعتبر مثل هذا المفتاح القصير ضعيفاً لأنه يوفر فرصة لتحديد المجموعات المتكررة عادة للنص المشفر التي من المرجح أن تُمثِّل كلمات شائعة وبالتالي تمكّن المحلل من فك رمز التشفير.
- سياسات إدارة المفتاح: تعتبر الإجراءات المستخدمة في تخزين وإدارة مفاتيح التشفير على درجة كبيرة من الأهمية، فمهما كانت خوارزمية التشفير قوية فإنه بمجرد الوصول إلى المفاتيح فإن التشفير يمكن أن يتم فكه بسهولة.

مفاتيح التشـفير يجب أن لا تخزن على الحواسـيب التي تسـتخدمها، ومن الضـروري الاحتفاظ بنسخ من المفاتيح في مواقع آمنة بحيث في حال ترك الموظف المصرف لأي سبب كان، فإن البيانات يمكن أن يتم فك تشفيرها.

- طبيعة خوارزمية التشفير:الخوارزمية القوية من الصعب -إن لم يكن من المستحيل- اكتشـافها باسـتخدام تقنيات تجريب كل الاحتمالات (Brute-Force Guessing)، والسـرية ليست ضـرورية للقوة، فالإجراءات المستخدمة من قبل خوارزميات التشـفير الشـائعة الاسـتخدام والأكثر قبولاً متاحة للجميع، لأنّ قبولها ليس ناتجاً عن كون هذه الإجراءات سرية وإنما لكون أنّ هذه الإجراءات تمّ اختبارها بشكل دقيق وبرهنت مقاومتها لهجمات Brute-Force Guessing.

6-2-1-7-2-أنواع نظم التشفير

هناك نوعان أسـاسـيان لنظم التشـفير: نظم التشـفير المتناظرة (Symmetric Encryption Systems) ونظم التشفير غير المتناظرة (Asymmetric Encryption Systems).

نظم التشـفير المتناظرة: تسـتخدم المفتاح نفسـه لعملية التشـفير وفك التشـفير ومن أمثلة هذه النظم DES (Data Encryption Standard) وAES (Advanced Encryption Standard).

نظم التشفير غير المتناظرة: تستخدم نوعين من المفاتيح هما المفتاح العام (Public Key) الموزّع بشكل واسع والمتاح للجميع، والمفتاح الخاص (Private Key) الذي يبقى سرياً ومعروفاً فقط لمالك زوج المفاتيح، حيث يمكن أن يتم استخدام إما المفتاح العام أو الخاص في عملية التشفير ولكن المفتاح الآخر فقط يمكنه أن يفك تشفير النص المشفّر (Cyphertext) لأنّ المفتاح العام والخاص مرتبطين رياضياً وبالتالي فإنّ المعلومات التي تم تشفيرها بواسطة المفتاح الخاص يمكن أن يتم فك تشفيرها فقط بواسطة المفتاح العام المقابل، وبشكل مماثل فإنّ المعلومات التي تم تشفيرها بواسطة المفتاح العام يمكن أن يتم فك تشفيرها فقط بواسطة المفتاح الخاص المقابل. من أمثلة هذه الأنظمة RSA و PGP (Pretty Good Privacy).

يعتبر التشفير المتناظر أسرع من التشفير غير المتناظر ولكنه يمتلك مشاكل عديدة وهي:

أولاً: لا بدّ من أن يكون المفتاح السري المشترك معروفاً لكل من المرسل والمرسل له، هذا يعني أن كلا الطرفين يحتاج لطريقة آمنة لتبادل المفتاح، فالبريد الإلكتروني لا يعتبر حلاً لأن أي شخص يستطيع أن يعترضه سيتمكن من معرفة المفتاح السري.

ثانياً: الحاجة إلى ابتكار مفاتيح سرية منفصلة مع كل طرف مختلف سيتم استخدام التشفير معه، وإلا فإنّ أي شخص يمتلك المفتاح السري العام سيتمكن من فك تشفير أي وثائق مشفرة تمكن من الوصول إليها قانونياً أو غير قانونياً وبشكل مقصود أو غير مقصود، إلى جانب أنّ النمو في عدد المفاتيح السرية المطلوبة سيخلق صعوبة في إدارتها وخاصة إذا كان التشفير مطلوباً مع الآلاف من الكيانات الأخرى.

ثالثاً: عند استخدام التشفير المتناظر فإنه يتوجب على كلا الطرفين معرفة المفتاح السري نفسه، وبالتالي ليس هناك من طريقة لإثبات من قام بتوليد مستند معين، فكل طرف يمكن أن يدّعي أنّ الطرف الآخر استخدم المفتاح السري المشترك في محاولة الاحتيال، ولذلك فإنّ التشفير المتناظر لا يوفر إمكانية إنشاء اتفاقيات التزام قانونية.

تحل نظم التشفير غير المتناظرة المشاكل الثلاثة السابقة، فمعرفة المفتاح العام لا تشكل أهمية كبيرة لأن أي نص مشفّر عن طريقه يمكن أن يتم فك تشفيره عن طريق استخدام المفتاح الخاص المقابل فقط، ولهذا السبب يمكن أن يتم توزيع المفتاح العام عن طريق البريد الإلكتروني أو حتى يمكن أن يتم تقديمه على موقع الويب، وبالتالي بإمكان أي شخص أن يُرسل معلومات مشفرة إلى مالك المفتاح الخاص. إضافة إلى ذلك، يمكن لعدد كبير من الأطراف أن يستخدموا المفتاح العام نفسه لإرسال الرسائل المشفرة لأنّ مالك المفتاح الخاص المقابل فقط يمكنه أن يفك تشفير تلك الرسائل. إلى جانب ذلك، فإنّ المعلومات يمكن أن يتم تشفيرها بواسطة المفتاح الخاص وبعد ذلك فك تشفيرها بواسطة المفتاح العام المقابل. وأخيراً نظراً لكون المفتاح الخاص مملوكاً من قبل طرف واحد فقط، بالتالي فإنّ مرسل الرسالة يمكن أن يتم توثيقه كمالك المفتاح الخاص من قِبل أي شخص يفك تشفير الرسالة بالمفتاح العام بما يوفر إمكانية خلق اتفاقيات إلكترونية ملزمة قانونياً. إلى جانب ذلك، فإنه من غير الممكن رياضياً لمالك أي مفتاح عام أن يستخدمه في معرفة المفتاح الخاص.

العيب الرئيسي في نظم التشفير غير المتناظرة هي السرعة، فهي أبطأ بآلاف المرات من التشفير المتناظر وبالتالي من الصعب استخدامها في تبادل كميات كبيرة من البيانات عبر شبكة الإنترنت. لذلك فإنّ الأعمال التجارية الإلكترونية تستخدم كلا النوعين من أنظمة التشفير، حيث تستخدم التشفير المتناظر لمعظم البيانات المتبادلة، والتشفير غير المتناظر لعملية إرسال مفتاح التشفير المتناظر للمرسل له ليستخدمه في فك تشفير النص المشفّر (Cyphertext).

6-2-1-7-3-التقطيع

التقطيع (Hashing) هو العملية التي يتم من خلالها تحويل النص الأصلي (Plaintext) مهما كان طوله إلى رمز قصير يدعى Hash. تعتبر MD5 وSHA-1 من خوارزميات التقطيع الأوسع استخداماً.

خوارزمية MD5 تنتج مقطعاً (Hash) طوله 128 بت من الرسالة الأصلية، والخوارزمية SHA-1 تنتج مقطعاً (Hash) طوله 160 بت.

تختلف عملية التقطيع عن التشفير في جانبين أساسيين:

1- ينتج عن عملية التشفير نص مشفر مساوي في الطول للنص الأصلي، بينما ينتج عن عملية التقطيع مقطع (Hash) قصير ذات طول ثابت بغض النظر عن طول النص الأصلي.

2- عملية التشفير قابلة للعكس، بمعنى أنّه بوجود خوارزمية التشفير ومفتاح التشفير يمكن أن يتم فك تشفير النص المشفّر (Cyphertext) وإعادته إلى النص الأصلي، بالمقابل فإن عملية التقطيع غير قابلة للعكس لأنها ترمي المعلومات. على سبيل المثال، استخدام خوارزمية MD5 في عملية تقطيع 20000 كلمة موجودة في وثيقة معينة ينتج عنها مقطع (Hash) طوله 128 بت، وبالتالي من المستحيل تحويل تلك السلسلة القصيرة من البتات إلى المستند الأصلي.

6-2-1-8-التوقيع الإلكتروني

يُستخدَم التشفير غير المتناظر وخوارزمية التقطيع في إيجاد ما يسمى بالتوقيع الإلكتروني (Digital Signature)، وهو – أي التوقيع الإلكتروني- عبارة عن معلومات تم إخضاعها لخوارزمية التقطيع ومن ثم تشفيرها بواسطة المفتاح الخاص بحيث يمكن أن يتم فك تشفيرها فقط باستخدام المفتاح العام المقابل. بالتالي، فإن فك التشفير الناجح للرسالة بواسطة المفتاح العام، يُثبت أنّ الرسالة قد تم إنشاؤها باستخدام المفتاح الخاص المرافق، وبما أنّ المفتاح الخاص معروف فقط من قِبل مالكه، فإن الكيان المالك لزوج المفاتيح الخاصة والعامة هو وحده استطاع أن يخلق تلك الرسالة.

نظراً لبطء التشفير غير المتناظر، فإن توليد التواقيع الإلكترونية لا يعتمد عادةً على تشفير الوثيقة بكاملها بواسطة المفتاح الخاص، عوضاً عن ذلك يتم إخضاع الوثيقة أولاً لخوارزمية التقطيع والمقطع(Hash) الناتج يتم تشفيره باستخدام مفتاح المرسل الخاص لتوليد التوقيع الإلكتروني.

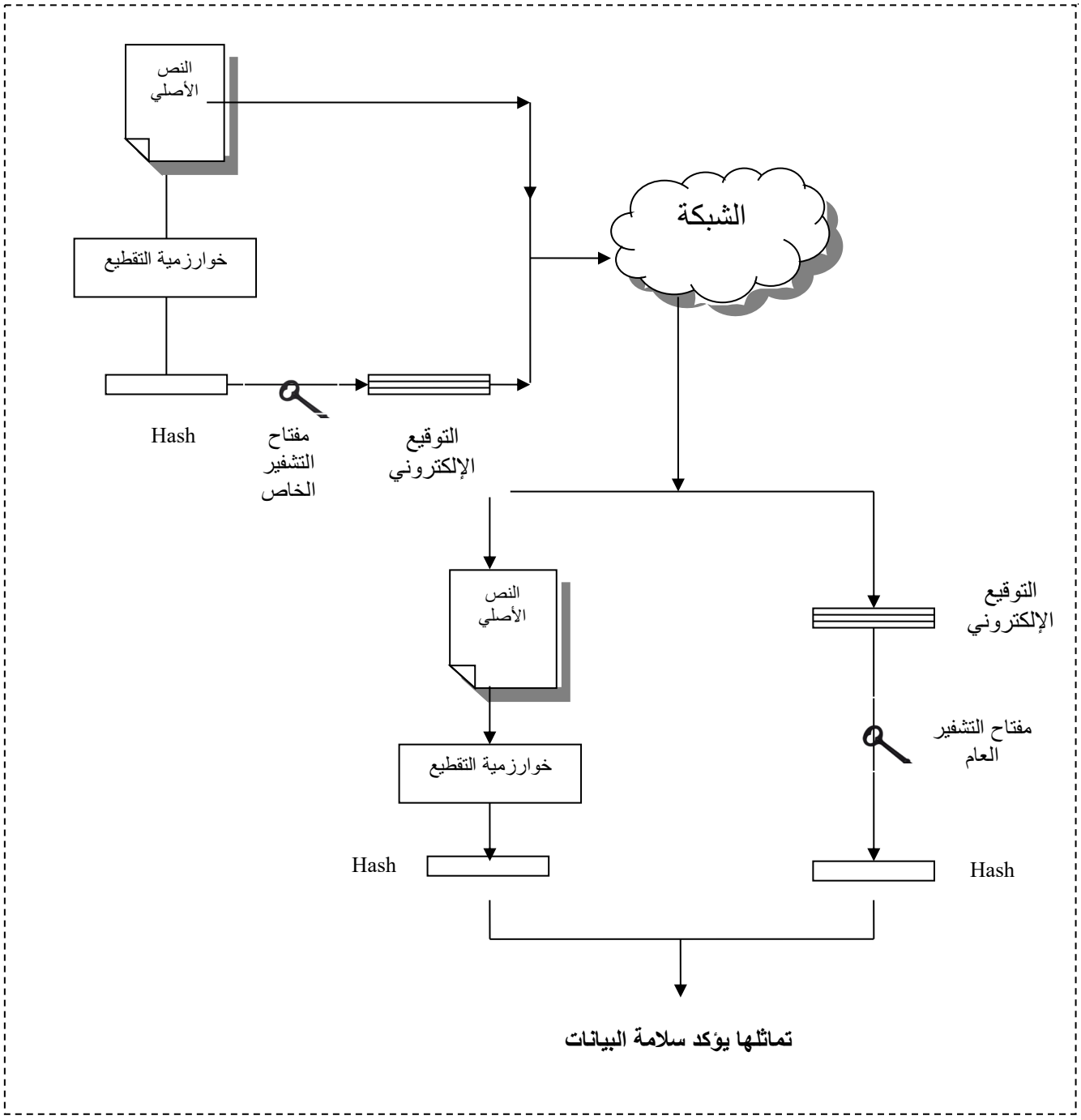
6-2-1-8-1- توليد التوقيع الإلكتروني

لتوليد التوقيع الإلكتروني يتم إخضاع الرسالة الأصلية غير المشفرة لخوارزمية التقطيع والتي ينتج عنها ما يسمى بملخص الرسالة (تمثيل محرفي مميز للبيانات) يُطلق على هذا الملخص بـ Hash، بعد ذلك يتم تشفير ملخص الرسالة بواسطة المفتاح الخاص للحصول على التوقيع الإلكتروني الذي يُرسل مع الرسالة، بحيث يحصل المرسل له على كل من الرسالة وملخص الرسالة المشفّر كما هو موضح من خلال الشكل (6-5).

يقوم المرسل له بفك تشفير ملخص الرسالة، ويُخضع الرسالة لخوارزمية التقطيع مرة أخرى، وفي حال تطابق ملخص الرسالة الناتج مع الملخص المرسل مع الرسالة، فإنّ ذلك يُثبت أنّ الرسالة لم يتم تعديلها وبالتالي ضمان كمال وسلامة المعلومات. وبما أنّ ملخص الرسالة قد تمّ تشفيره بواسطة المفتاح الخاص، فإنّ هوية المرسل يمكن أن تُعرف وتُربط برسالة معينة، إضافة إلى إمكانية تحقيق سرية وخصوصية المعلومات عبر تشفير الرسالة نفسها.

تساعد عملية التقطيع المستخدمة في توليد التوقيع الإلكتروني في إثبات أنّ الرسالة التي قام المرسل له بفك تشفيرها هي تماماً نفس الرسالة المنشأة من قبل المرسل، لأنّ خوارزمية التقطيع تستخدم كل بت في النص الكامل الأصلي لحساب قيمة المقطع، وبالتالي فإنّ تغيير أي محرف في المستند الذي تم إخضاعه لعملية التقطيع (مثلاً استبدال 1 بـ 7) سينتج عنه قيمة مختلفة للمقطع (Hash)، وهذه الخاصية المميزة لخوارزميات التقطيع توفر إمكانية التحقق من أنّ محتويات الرسالة لم يتم تغييرها .

يُساعد الاستخدام الناجح للمفتاح العام في فك تشفير المستند أو الملف في إثبات أنّ ذلك الملف أو المستند قد تمّ خلقه من قبل الكيان المالك للمفتاح الخاص المقابل، ولكن كيف يمكن للمستلم أن يتأكد من هوية ذلك الكيان؟ على سبيل المثال، كيف يمكن للعميل أن يتأكد من أنّ الملف المدّعى بكونه مرسلاً من قبل المصرف قد تمّ فعلاً إنشاؤه من قِبل ذلك المصرف وليس من قبل شخص آخر استطاع أن ينسخ زوج المفاتيح (الخاصة والعامة) واستخدامها في التظاهر بكونه المؤسسة المالية؟ وكيف يحصل المرسَل له على المفتاح العام للمرسِل؟ الإجابة على هذه الأسئلة تتضمن استخدام الشهادات الرقمية (Digital Certificates).



الشكل (6-5): استخدام التوقيع الإلكتروني للتأكد من سلامة البيانات

6-2-1-9-الشهادات الرقمية

الشهادة الرقمية (Digital Certificate) هي مستند رقمي مُنشأ وموقع إلكترونياً من قِبل طرف ثالث موثوق هو عادةً الوكالة المسؤولة عن الشهادات وذلك بواسطة المفتاح الخاص لتلك

الوكالة، حيث يُصادق هذا المستند على هوية الطرف الذي تمثله الوكالة، ويحوي المفتاح العام للطرف الممثَّل.

يمكن أن يتم تخزين الشهادات الرقمية على مواقع الويب (Web Sites)، حيث يتم تصميم المتصفحات للحصول أوتوماتيكياً على نسخة من تلك الشهادة الرقمية واستخدام المفتاح العام المحتوى فيها للتواصل مع موقع الويب، وبالتالي توفر ّ الشهادات الرقمية أسلوباً آلياً للحصول على المفتاح العام للمنظمة أو لشخص معين.

تقوم الوكالة المسؤولة عن الشهادات (Certificate Authority) بتقطيع المعلومات المخزنة على الشهادة الرقمية، ثمّ تقوم بتشفير ذلك المقطع الناتج (Hash) بواسطة مفتاحها الخاص وتُلحق التوقيع الإلكتروني الناتج بالشهادة الرقمية بما يوفر وسيلة للمصادقة على موثوقية الشهادة.

أثر التشفير على طبقات الحماية الأخرى

على الرغم من أنّ التشفير يوفّر السرية والخصوصية للمعلومات أثناء تخزينها أو انتقالها عبر شبكة الإنترنت (إلى جانب إثبات الهوية وعدم إنكار الصفقات الإلكترونية)، فإنه يخلق مشاكل للإجراءات الأمنية الأخرى. على سبيل المثال، يعتمد عمل الجدار الناري على التحقيق في مكونات الحزم التي تعبر من خلاله، ولكنه لا يستطيع أن يفحص بفعالية الحزم المشفَّرة، ولمعالجة هذه المشكلة تعمل بعض المنظمات على إعداد الجدار الناري ليقوم بتوجيه الحزم المشفرة إلى حاسب موجود على شبكة منفصلة تدعى DMZ (Demilitarized Zone) ، حيث يقوم هذا الحاسب بفك تشفير الحزم المشفرة، ومن ثمّ إعادة إرسالها إلى الجدار الناري لتتم فلترتها قبل السماح لها بالدخول إلى الشبكة الداخلية. على الرغم من أنّ هذه الطريقة تسمح للجدار الناري بفحص كل الحزم القادمة، فإنها تُعرِّض الحزم التي تمّ فك تشفيرها لهجمات سرقة المعلومات (Sniffing) داخل الشبكة الداخلية للمنظمة.

من جهة أخرى، فإنّ إعداد الجدار الناري الرئيسي بحيث يسمح بدخول الحزم المشفرة إلى الشبكة الداخلية يحمي سرية المعلومات الحساسة إلى أن تصل إلى مقصدها المناسب، غير أن ذلك يولِّد فجوات في عمليات ضبط الوصول، لذلك يجب أن تختار المنظمات الهدفَ

الأمني الأكثر أهمية بالنسبة لها: السرية أو ضبط الوصول، لأنّ الجدار الناري ليس وحده يواجه هذا النوع من المشاكل، حيث تواجه البرامج المضادة للفيروسات ونظم كشف الاختراق IDSs أيضاً صعوبة في التعامل مع الحزم المشفرة.

6-2-2- الرقابة الكشفية (Detective Controls)

لا يمكن أن تكون الرقابة الوقائية فعالة بشكل كامل في اعتراض كل أنواع الهجمات، ولهذا السبب تحتاج المصارف أيضاً إلى تطبيق رقابة مصمَّمة لكشف الاختراق في الوقت المناسب، حيث تقوم الرقابة الكشفية بتعزيز الأمن من خلال مراقبة مدى كفاءة الرقابة الوقائية والكشف عن الحوادث التي تمّ فيها تجاوز تلك الرقابة بنجاح.

تمثِّل الرقابة المتعلقة بالتأكد من الهوية والتأكد من السماحية سياسات المصرف التي تتحكم بالوصول إلى النظام وتقِّيد الأعمال التي يمكن أن يتم تنفيذها من قبل المستخدمين المرخصين، ولتقييم مدى التقيّد بتلك السياسات لا بدّ من أن يتم فحص الاستخدام الفعلي للنظام، حيث يُعتبر تحليل معلومات الدخول (Log Analysis)، ونظم كشف الاختراق IDSs (Intrusion Detection Systems) والتقارير الإدارية من الأساليب الأساسية لتحقيق الرقابة الكشفية، إلى جانب أهمية القيام باختبار فعالية الإجراءات الأمنية الموجودة بشكل دوري.

6 -2-2-1-تحليل معلومات الدخول

(Log Analysis)

تمتلك معظم النظم قدرة واسعة على تسجيل كل من تمكن من الوصول إلى النظام وتسجيل كل الأفعال التي قام كل مستخدم بتنفيذها، حيث تُتيح هذه المعلومات إمكانيةَ إجراء تعقب وتدقيق لعمليات الوصول إلى النظام.

إنّ عملية تحليل معلومات الدخول هي القيام بفحصها لمراقبة الأمن، ويحتاج هذا التحليل أن يتم القيام به بشكل دوري لكشف المشاكل في الوقت المناسب، وهذا ليس سهلاً لأنّ معلومات الدخول يمكن أن تنمو في حجمها بسرعة كبيرة، لهذا السبب، يستخدم مدراء النظم أدوات

برمجية عديدة لاستبعاد معلومات الدخول الروتينية ليتمكنوا من تركيز اهتمامهم على السلوك غير الطبيعي الذي يمكن أن يمثل إشارات عن الاقتحام.

6-2-2-2- نظم الكشف عن الاختراق

يُعتبَر الضعف الرئيسي في تحليل معلومات الدخول هو أنها تتطلّب الكثير من الجهد ومعرّضة للخطأ البشري، ولأتمتة جزء من عملية الرقابة تُستخدم نظم الكشف عن الاختراق التي تبحث عن علامات الهجوم من خلال نماذج سلوكية معينة تُعبّر عادة عن النوايا التخريبية وذلك داخل ملفات الدخول إلى النظام وتسمى في هذه الحالة نظم الكشف عن الاختراق على مستوى المضيف (Host-Based)، أو داخل حزم الشبكة وتسمى عندئذ بنظم الكشف عن الاختراق على مستوى الشبكة (Network-Based).

تُعتبر نظم الكشف عن الاختراق مكوناً أساسياً وهاماً في كشف أي عمليات تمكن فيها غير المرخصون من الدخول إلى النظام والشبكة الداخلية للمصرف، أو الكشف عن العمليات التخريبية سواء من قِبل المستخدمين المرخصين أو غير المرخصين من داخل وخارج المصرف. ومن الأفضل أن تستخدم المصارف نظم الكشف عن الاختراق على مستوى الشبكة وعلى مستوى الحاسب المضيف الواحد، لأنه ليكون نظام الكشف عن الاختراق فعالاً لا بدّ من وجود كلا النوعين من نظم الكشف عن الاختراق، لأنّ كل نوع يختص بمجال معين ويمتلك مزايا ومساوئ خاصة به، غير أنهما يكملان بعضهما البعض. وبالنهاية مهما كان نوع نظام الكشف عن الاختراق المستخدم سواء على مستوى المضيف أو على مستوى الشبكة أو الاثنين معاً، فإنّ استخدامه يُعتبر أساسياً وأداة فاعلة بيد مدراء الأمن لأنّ وجود الشبكة يفرض استخدام نظم الكشف عن الاختراق مهما كان نوعها.

مزايا نظم الكشف عن الاختراق على مستوى الشبكة

تتمتع نظم الكشف عن الاختراق على مستوى الشبكة بمجموعة من المزايا منها:

- تكشف الاختراقات التي لا تكشفها نظم الكشف عن الاختراق على مستوى المضيف لأنها تفحص ترويسة كل الحزم للتعرف على إشارات لأي عمليات مشبوهة أو

تخريبية، بينما نظم الكشف عن الاختراق على مستوى المضيف لا تفحص ترويسة الحزم القادمة، وبالتالي فهي لا تتمكن على سبيل المثال من كشف هجمات توقف الخدمة (Denial of Service) التي يمكن التعرف عليها فقط من خلال النظر إلى ترويسة الحزم التي تنتقل عبر الشبكة؛

- تستخدم في التحليل حزم الشبكة أثناء انتقالها مباشرة بما يوفر الكشف الفوري عن أي اختراق وبالتالي لا يتمكن المهاجم من إخفاء آثاره، فالعديد من المهاجمين يمكن لهم أن يتلاعبوا بملفات الدخول التي هي الأساس الذي تعتمد عليه نظم الكشف عن الاختراق على مستوى المضيف، وبالتالي يتمكنون من إخفاء آثار وجودهم؛
- تكشف الهجمات عند وقوعها بما يؤمن سرعة أكبر في الإعلام عنها والاستجابة لها، بينما نظم الكشف عن الاختراق على مستوى المضيف لا تتعرف على الهجوم قبل أن يتم تسجيل دخوله، وبذلك الوقت يمكن أن يكون قد تمّ اختراق نظام أساسي ما أو أن ينهار النظام الذي يعمل عليه نظام الكشف عن الاختراق نفسه؛
- لا تعتمد على نظام التشغيل الموجود على المضيف كمصدر للكشف عن الاختراق، بينما نظم الكشف عن الاختراق على مستوى المضيف تتطلب نظم تشغيل محددة لتتمكن من العمل بشكل جيد وتوليد نتائج معنوية؛
- تكشف عند توضعها خارج الجدار الناري الهجمات التي لم تتمكن من النجاح، وهذه المعلومات يمكن أن تكون أساسية في تقييم وتعديل السياسات الأمنية.

مزايا نظم الكشف عن الاختراق على مستوى المضيف

تُحقق نظم الكشف عن الاختراق على مستوى المضيف أيضاً مجموعة من المزايا منها:

- يمكن من خلال نظم الكشف عن الاختراق على مستوى المضيف التأكد من نجاح أو فشل الهجوم نظراً لاعتمادها على بيانات الدخول التي يمكن من خلالها معرفة ما تمّ تنفيذه فعلاً، وبالتالي فهي تُكمّل عمل نظم الكشف عن الاختراق على مستوى الشبكة التي تنبه عن وجود الاختراق ونظم الكشف عن الاختراق على مستوى المضيف تبين إن كان ذلك الهجوم ناجحاً أم لا؛

- يُراقب نظام الكشف عن الاختراق على مستوى المضيف تسجيل الدخول والخروج من قِبل جميع المستخدمين والأعمال التي قام كل منهم بتنفيذها أثناء اتصالهم بالشبكة، كما يُراقب عمليات الوصول إلى الملفات والتغييرات في سماحيات الوصول، ومحاولات تحميل برامج تنفيذية جديدة، ومحاولات الوصول إلى الخدمات ذات السماحيات، وغيرها من العمليات بينما نظم الكشف عن الاختراق على مستوى الشبكة لا تحقق ذلك المستوى من تفاصيل العمليات؛
- تُراقب التغييرات في ملفات النظام الأساسية والبرامج التنفيذية، فهي تكشف و تعمل على إيقاف أي محاولات لتعديل ملفات النظام الأساسية أو تحميل البرامج الطفيلية المختلفة؛
- تكشف عن عمليات الهجوم التي لا تتمكن نظم الكشف عن الاختراق على مستوى الشبكة من اكتشافها، على سبيل المثال، عمليات الهجوم من مخدم أساسي ما عبر لوحة مفاتيحه لا تعبر الشبكة وبالتالي لا تتمكن نظم الكشف عن الاختراق على مستوى الشبكة من اكتشافها؛
- تُعتبر مناسبة للشبكات الكبيرة التي تُستخدم فيها المحولات (Switches) والتشفير، فاستخدام المحولات التي تتيح إمكانية إدارة الشبكات الكبيرة كمجموعة من الشبكات الجزئية يزيد من صعوبة اختيار المكان الأفضل لنظم الكشف عن الاختراق على مستوى الشبكة لتأمين تغطية شاملة للشبكة، بينما تتوضع نظم الكشف عن الاختراق على مستوى المضيف على العدد المطلوب من المضيفات الأساسية بما يحقق مراقبة أوضح للشبكة، إلى جانب أن حزم المعلومات تصل إليه بعد أن يكون قد تمّ فك تشفيرها وبالتالي فهي لا تعاني من مشاكل مع المعلومات المشفرة؛
- إضافة إلى ما سبق فإنّ نظم الكشف عن الاختراق على مستوى المضيف لا تتطلب بنية تحتية إضافية على الشبكة لأنها تتوضع على بنى تحتية موجودة سابقاً مثل مخدمات الويب ومخدمات الملفات وغيرها من الموارد المشاركة، وهذا ما يجعلها اقتصادية لأنها لا تتطلب عتاد صلب إضافي.

6-2-2-3- التقارير الإدارية

تُعتبَر التقارير الإدارية (Managerial Reports) رقابة كشفية أساسية، فقد طوّرت جمعية الرقابة والتدقيق لنظام المعلومات (ISACA) ومعهد الحوكمة لتكنولوجيا المعلومات، إطار عمل شامل لرقابة نظام المعلومات سمّي بـ COBIT (Control Objectives For Information and Related Technology) (أهداف الرقابة للمعلومات والتكنولوجيا المتعلقة).

حدّد إطار عمل COBIT 34 هدفاً للرقابة مرتبطاً بتكنولوجيا المعلومات، كما قدّم توجيهات للإدارة تحدّد عناصرَ النجاح الرئيسية المرتبطة بكل هدف، واقترح مؤشرات الأداء المفتاحية التي يمكن للإدارة أن تستخدمها لمراقبة وتقييم فعّالية الرقابة.

على سبيل المثال، تتعلق أحد الأهداف الرقابية بتوفير الأمن الكافي، بحيث تكون معلومات المصرف محميةً من الوصول غير المشروع أو الخسارة. وتقترح التوجيهات الإدارية المرتبطة بهذا الهدف مؤشرات الأداء المفتاحية التالية:

- مدة التوقف (Downtime) الناتجة عن الحوادث الأمنية؛
- عدد النظم المحمَّلة بنظم الكشف عن الاختراق؛
- الوقت اللازم للاستجابة للحوادث الأمنية عندما يتم كشفها.

بالتالي يمكن للإدارة أن تستخدم مواد COBIT لإنشاء بطاقة الحساب لرقابة فعالية مقاييس الأمن المستخدَمة.

6-2-2-4- اختبار الأمن

من الضروري أن يتم اختبار فعالية الإجراءات الأمنية المستخدَمة بشكل دوري، وللقيام بذلك يمكن للمصارف أن تقوم بتنفيذ ما يسمى بمسح نقاط الضعف/الخلل (Vulnerability Scans) الذي يستخدم أدوات آلية مصمَّمة للتعرّف على امتلاك النظام لأي نقاط ضعف معروفة جيداً، حيث يُتيح ذلك إمكانية التحكم بالوصول إلى النظام وبالتالي تخفيض المخاطر التشغيلية. كما أنّ اختبار إمكانية الاختراق من قِبل فريق التدقيق الداخلي أو من قِبل شركة أمن استشارية خارجية من خلال المحاولات المرخّصة للوصول إلى نظام معلومات المصرف، يوفّر وسيلة فاعلة لاختبار فعالية أمن الحاسب (Computer Security).

6-2-3- الرقابة المصحِّحة

(Corrective Controls)

تُعتبَر عملية الكشـف عن أي محاولات للاختراق إلى جانب الكشـف عن عمليات الاختراق الناجحة أمراً ضـرورياً لكنه عديم الجدوى إذا لم يُتبَع بفعل تصـحيحي، لذلك لا بدّ من وجود إجراءات مناسبة للاستجابة للاختراقات الأمنية للنظام واتخاذ الأفعال التصحيحية في الوقت المناسب، ولتحقيق ذلك يجب على المصارف أن تقوم بما يلي:

- تشـكيل فريق الاسـتجابة للحوادث الطارئة المرتبطة بالحاسـب CERT (Computer Emergency Response Team)؛
- تحديد الأشخاص المسؤولين عن الأمن على مستوى المصرف ككل؛
- وجود نظـام منظّم لإدارة التعـديلات في الكود البرمجي الصـــادرة عن موردي البرمجيات (Management Patch).

6-2-3-1- فريق الاستجابة للحوادث الطارئة المرتبطة بالحاسب

يُعتبَر تشـكيل فريقٍ للاسـتجابة للحوادث الطارئة المرتبطة بالحاسـب الذي يقع على عاتقه مسـؤولية التعامل مع الحوادث الكبرى ومعالجتها مكوناً أسـاسـياً للقدرة على الاسـتجابة للحوادث الأمنية بشكل آني وفعّال. يجب أن يضم الفريق مجموعة من الأخصـائيين الفنيين، وأعضـاء من إدارة العمليات الرئيسـية (Senior Operations Management)، وذلك لأنّ بعض ردود الفعل المرتبطة بالحوادث الأمنية لها نتائج اقتصـادية كبيرة. على سبيل المثال، يحتاج قرار إغلاق مخدّم الصـيرفة الإلكترونية بشـكل مؤقت إلى تقييم المنافع والمسـاوئ المرتبطة بذلك، والإدارة التشـغيلية وحدها تمتلك المعرفة الواسـعة للقيام بتقييم كهذا، وبالتالي يجب أن تمتلك هذه الإدارة الصـــلاحية لاتخاذ ذلك القرار، لا أن يُترَك لحكمة طاقم أمن تكنولوجيا المعلومات.

6-2-3-2- مسؤول الأمن الرئيسي

يجب أن يكون مسـؤول الأمن الرئيسـي CSO (Chief Security Officer) مسـتقلاً عن وظائف نظام المعلومات الأخرى، وأن يقدّم تقريراً رسـمياً إما إلى مسـؤول التشـغيل الرئيسـي COO (Chief operations Officer) أو إلى المســؤول التنفيذي الرئيســي CEO (Chief Executive Officer)، كما أنّ عليه أن يفهم البيئة التقنية للمصرف، وأن يعمل مع المسؤول الرئيسي عن المعلومات CIO (Chief Informational Officer) وذلك لتصــميم وتطبيق وترويج الإجراءات والسياسات الأمنية السليمة.

يقوم مسـؤول الأمن الرئيسـي بنشـر المعلومات المتعلقة بالاحتيال والأخطاء والاختراقات الأمنية وغيرها من الاسـتخدامات غير الطبيعية للنظام إضـافةً إلى نتائجها. إلى جانب ذلك، من الضـروري أن يعمل مسـؤول الأمن الرئيسـي مع الشـخص المسـؤول عن أمن البناء، وذلك لأنّ الوصــول المادي غير المرخَّص يمكن أن يســمح للمهاجم بتجنب الرقابة المستفيضة المرتبطة بالوصول المنطقي.

يجب أن يقوم مسؤول الأمن الرئيسي أيضاً بتقييم وتقدير منصف لبيئة تكنولوجيا المعلومات IT، وبالتالي عليه أن يدير عملية تقييم الخطر و نقاط الضـعف (Vulnerabilities)، وأن يدقِّق المقاييس الأمنية المطبقة من قِبل المسؤول الرئيسي عن المعلومات.

6-2-3-3- إدارة عمليات تصحيح الأخطاء (Patch Management)

تُعتبَر عملية إصـلاح نقاط الضـعف (Vulnerabilities) المعروفة وتحميل المعلومات الجديدة لبرامج الأمن (كبرمجيات الجدار الناري والبرامج المضـادة للفيروسـات) والنظم التشـغيلية وبرامج التطبيقات الأخرى هي رقابة تصــحيحية إضــافية ضــرورية نظراً لارتفاع عدد تقارير نقاط الضــعف كل عام، والسـبب في ذلك هو الارتفاع الدائم في حجم ودرجة تعقُّد البرمجيات.

تحتوي العديد من البرامج الشـــائعة الاســـتخدام على الملايين من أســـطر الكود (Lines of Code)، وهذا يعني أنه حتى إن كان 99.99% من أسطر الكود خالياً من الأخطاء، فإنه يبقى هناك 100 سطر أخطاء محتملة لكل مليون سطر من الكود.

إن الـ Patch هو عبارة عن تعديلات في الكود البرمجي مُصدر من قبل موردي البرمجيات لمعالجة نقاط ضعف سابقة في منتجاتهم، وهذه التعديلات إن تمّ تطبيقها بشكل صحيح، فإنها ستعمل على إزالة نقاط الضعف الموجودة في النظم. أمّا إدارة الـ Patch فهي عملية تنفيذ منتظمة للـ Patches والتعديلات لكل البرمجيات المستخدَمة من قبل المصرف، غير أن الأمر ليس بهذه السهولة، لأن Patches تمثل تعديلاً على برمجيات معقدة، وبالتالي قد تخلق مشاكل جديدة بسبب آثارها الجانبية غير المتوقعة، ولهذا السبب، تحتاج المنظمات لأن تقوم بعملية اختبار دقيقة لأثر Patches قبل استعمالها، وإلا فإنها ستتعرض لخطر تدمير تطبيقات مهمة.

6-3- إجراءات الرقابة البرمجية

6-3-1- أمن قواعد البيانات (Database Security)

تُعتبر مخدّمات قواعد البيانات من أهم المخدّمات التي تمتلكها المنظمة نظراً لاحتوائها على المعلومات المالية الخاصة بالمنظمة إلى جانب المعلومات الخاصة بالعملاء والموارد البشرية وغيرها من المعلومات الهامة التي تمكّن المنظمة من الاستمرار في عملها، ولذلك لا بدّ من أن تكون قاعدة البيانات على درجة كبيرة من الأمن والسرية.

6-3-2- الأهداف الأساسية لأمن البيانات

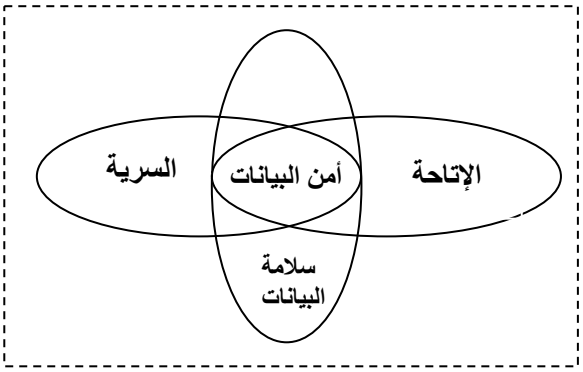
تُعتبر السرية والسلامة والإتاحة هي المكونات الثلاث الأساسية اللازمة لتحقيق أمن البيانات كما هو موضح من خلال الشكل (6-6).

السرية (Confidentiality) وهي حماية البيانات من عمليات القراءة غير المشروعة، بحيث لا يتمكن المستخدمون غير المخولون بذلك من الوصول إليها واستخدامها.

سلامة البيانات (Integrity) حماية البيانات من عمليات التعديل غير الرسمية التي تؤدي إلى أخطاء أو تزوير في البيانات، وبالتالي ضمان أن تكون البيانات صحيحة وخالية من التناقض بشكل دائم.

الإتاحة (Availability) ضمان أنّ الوصول المشروع إلى البيانات يتم في الوقت المناسب ولا يتم رفضه.

يُقدّم نظام إدارة قواعد البيانات إمكانية تعريف وتصميم قواعد معينة لضمان أمن البيانات المخزنة داخل قواعد البيانات، ويتم ذلك من خلال تحديد سلطات مستخدمي قواعد البيانات في الوصول إلى البيانات، وتحديد نوع العمليات التي يُسمح لهم القيام بها.



الشكل (6-6): مفهوم أمن البيانات

6-3-4- نماذج تحقيق الأمن في قواعد البيانات

6-3-4-1- استخدام الجداول الافتراضية

الجدول الافتراضي (View) عبارة عن جدول منطقي معتمد على جدول حقيقي أو جدول افتراضي آخر، وهو لا يحتوي على بيانات خاصة به وإنما هو بمثابة النافذة التي من خلالها يمكن الاطلاع أو تعديل البيانات (التعديل يكون بوجود شروط معينة) الموجودة في الجداول الحقيقية.

تُحقق الجداول الافتراضية فوائد كثيرة منها:

- إنّ البيانات غير موجودة فعلياً وإنما تعتمد في وجودها على الجداول الحقيقية وعند إنشائها يمكن وضع قيد (With Read only)، أي إمكانية القراءة فقط من الجدول الافتراضي وذلك لمنع عمليات تعديل تلك البيانات بما يوفر مستوى تلقائي من سلامة البيانات.
- عند إنشاء الجداول الافتراضية وتفويض استخدامها لأحد المستخدمين، فإنّ ذلك يعني أنه قد تمّ إدراج جزء فقط من هيكلية قاعدة البيانات كحق لهذا المستخدم وهذا يمنع عنه تلقائياً الأجزاء الأخرى التي لا يحق له الاطلاع عليها بما يوفر سرية للبيانات.

- تمكننا الجداول الافتراضية من إخفاء وتغيير الأسماء الحقيقية للأعمدة واستبدال أسماء وهمية بها لأسباب الأمن والسرية.

6-3-4-2- استخدام أوامر لغة الاستعلام البنيوية SQL (Structured Query Language)

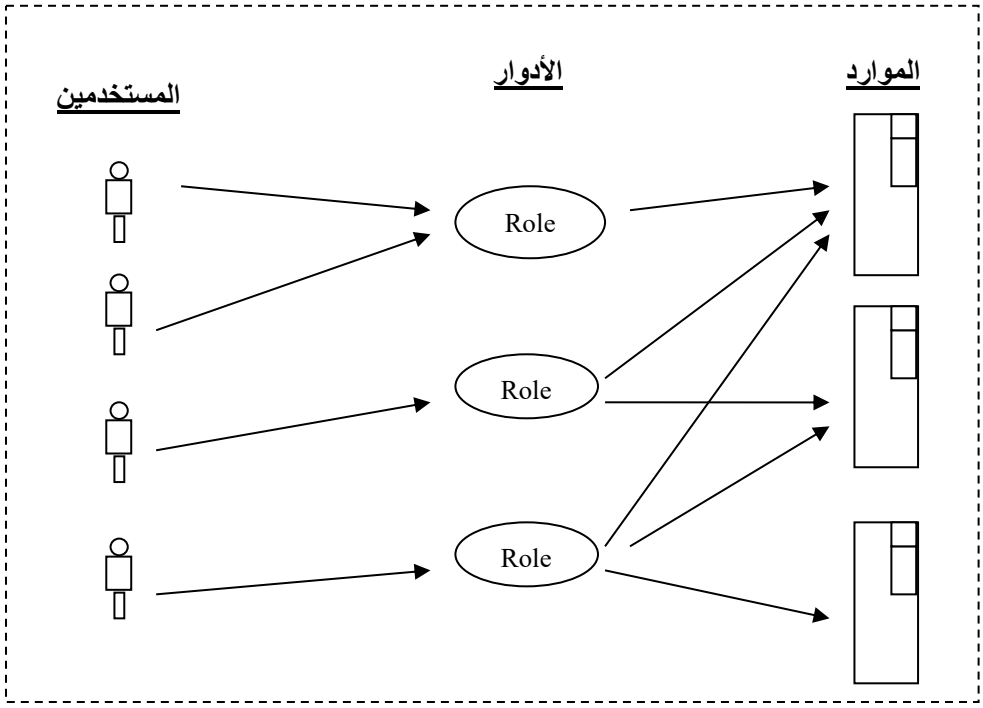
تحتوي لغة الاستعلام البنيوية SQL (وهي عبارة عن لغة نمطية للتعامل مع قواعد البيانات الترابطية) من خلال لغة التحكم بالبيانات DCL (Data Control Language) على أوامر لمنح أو لسحب حقوق الاستخدام مثل القراءة والتعديل والإضافة والحذف على الجداول الحقيقية والجداول الافتراضية، وقد تكون على عدة مستويات حيث يمكن أن يكبر أو يصغر حجم هذا التفويض حسب رغبة مدير قاعدة البيانات DBA (Database Administrator) التي تعتمد على طبيعة النظام وتعليمات المنظمة فيما يتعلق بالأمن.

6-3-4-3- الرقابة على الوصول المرتبطة بمنح الأدوار (Role-based Access control)

يتم التعبير عن معظم السياسات المرتبطة بالرقابة على الوصول من خلال استخدام مصطلحات Subjects وObjects والسماحيات (Privileges). المقصود بـ Objects كل ما يحتوي على بيانات مثل الجداول أو حزم الشبكة أو أدوات الإدخال والإخراج أو وسائط التخزين المادية وغيرها، أما Subjects فهي اختصار لأي كينونة نشيطة تقوم بتنفيذ عمليات ما داخل النظام مثل المستخدمين والأدوار والعمليات الداخلية، أما السماحيات فهي عبارة عن العمليات التي يمكن أن تنفذها Subjects على Objects داخل النظام (قراءة، كتابة، استرجاع، إدخال، تعديل، حذف...الخ).

تزداد درجة صعوبة إدارة الأمن عند إدارة النظم الكبيرة، حيث يكون هناك عدد كبير من Subjects وObjects وبالتالي عدد كبير جداً من السماحيات الممنوحة والمسحوبة بما يزيد من صعوبة إدارتها، وبما أنّ الرقابة تعتمد عادة على الأعمال التي يقوم الموظفون بتنفيذها، فقد سهلت عملية الرقابة على الوصول المرتبطة بمنح الأدوار من عملية إدارة تلك الرقابة ودعمت الرقابة على الوصول المعتمدة على الوظائف بشكل مباشر.

تُمثل الأدوار الوظائف ضمن منظمة محددة، حيث يتم منح السماحيات إلى الأدوار عوضاً عن المستخدم الفرد، وبالتالي يتم منح المستخدمين الأدوار المناسبة ليمتلكوا السماحيات المتوافرة ضمن تلك الأدوار كما هو موضح من خلال الشكل (6-7).



الشكل (6-7): آلية التعامل مع الأدوار

الفصل السابع

نظم قواعد البيانات

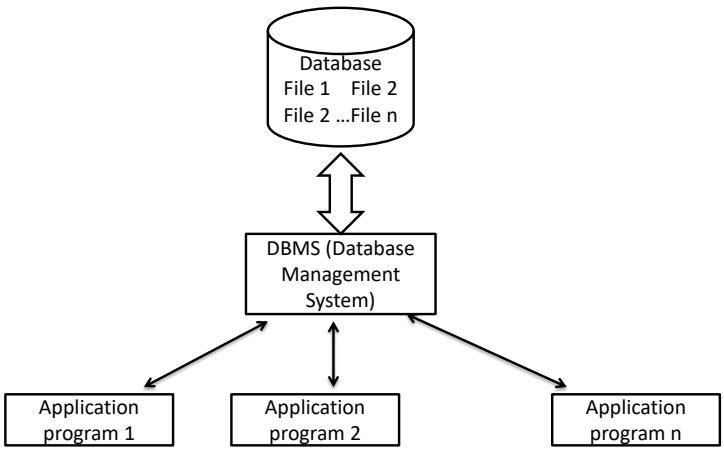
DataBase Systems

7-1- مفهوم نظام قاعدة البيانات

يتم تصميم وتشغيل معظم نظم المعلومات الحالية في المنظمات باستخدام نظم قواعد البيانات . يتكون نظام قاعدة البيانات من قاعدة البيانات ونظام إدارة قاعدة البيانات.

يمكن تعريف قاعدة البيانات (Database) بأنها مجموعة من الملفات ذات العلاقات المتبادلة المنسقة مركزياً، بينما نظام إدارة قاعدة البيانات (Database Management System) هو الحزمة البرمجية المصممة لإنشاء قاعدة البيانات وإدارتها والاستعلام عن المعلومات المطلوبة .

تتعامل نظم قواعد البيانات مع البيانات كمورد (Resource) للمنظمة يُستخدم ويدار على مستوى المنظمة ككل لا على مستوى قسم أو وظيفة معينة. تشكل نظم إدارة قواعد البيانات الترابطية (Relational Database Management Systems) أكثر الأنظمة استخداماً في تطوير نظم المعلومات.



الشكل ٧-١: تخزين الملفات باستخدام قواعد البيانات

7-2- عرض قاعدة البيانات (Database View)

تسمح نظم قواعد البيانات للمستخدمين الوصول إلى قاعدة البيانات وتحديثها دون معرفة طريقة أو مكان تخزين البيانات (الفصل بين تخزين البيانات واستخدامها لتسهيل تعامل المستخدمين مع النظام) ، يتحقق ذلك من خلال الفصل بين العرض المنطقي والمادي للبيانات:

- العرض المنطقي (Logical View) :يتعلق بفهم وتنظيم البيانات من وجهة نظر المستخدمين المختلفين لقاعدة البيانات
- العرض المادي (Physical View) : يتعلق بكيفية تخزين وترتيب البيانات مادياً

تربط نظم إدارة قواعد البيانات بين طريقة تخزين البيانات مادياً والعرض المنطقي للبيانات لكل مستخدم

7 -3- مخطط قاعدة البيانات (Database Schema)

مخطط قاعدة البيانات يعبر عن التركيب المنطقي لقاعدة البيانات (توصيف تركيب قاعدة البيانات، نوع البيانات، القيود). يتم التمييز بين ثلاثة أنواع لمخطط قاعدة البيانات :

- **المخطط المنطقي** (Conceptual Schema) **:** يعبر عن وجهة نظر المنظمة بشكل عام عن قاعدة البيانات (يشمل جميع العناصر والعلاقات بينها)
- **المخطط الخارجي** (External Schema) **:** يعبر عن وجهة نظر المستخدم الفرد عن جزء من قاعدة البيانات
- **المخطط الداخلي** (Internal Schema) : يعبر عن آلية تخزين البيانات وطريقة الوصول إليها

7-4- لغات نظم إدارة قواعد البيانات

- لغة تعريف البيانات (Data Definition Language) : تستخدم لتحديد مخطط قاعدة البيانات ، توصيف ملفات النظام والسجلات ،توصيف العلاقات بين الملفات وتوصيف العرض المنطقي لكل مستخدم.

- لغة معالجة البيانات (Data Manipulation Language) : تستخدم للاستعلام من قاعدة البيانات وتحديثها ، إدخال معلومات جديدة إلى قواعد البيانات (إضافة سجلات جديدة إلى ملف موجود)، الاستعلام عن المعلومات الموجودة داخل قواعد البيانات (قراءة السجل من ملف معين)، تعديل المعلومات الموجودة داخل قواعد البيانات (تغيير محتويات الحقول الموجودة في سجل معين)، وحذف المعلومات الموجودة داخل قواعد البيانات (مسح أحد السجلات من ملف معين).

7-5- قاموس البيانات

قاموس البيانات هو قاعدة بيانات خاصة داخل نظام إدارة قواعد البيانات تتضمن بيانات حول البيانات المخزنة في قاعدة البيانات. يتم من خلال قاموس البيانات تخزين مواصفات كل حقل من حقول قاعدة البيانات الأساسية (على سبيل المثال: اسم الحقل، نموذج البيانات، حجم الحقل، التطبيقات التي يحق لها أن تتعامل مع هذا الحقل). مدخلات قاموس البيانات هي السجلات عن أية بيانات جديدة أو محذوفة، التغيير في أسماء الحقول، مستخدمي عناصر البيانات الحاليين، الخ. ينتج عن قاموس البيانات تقارير مفيدة لمصممي قاعدة البيانات وتوثيق النظم.

7-6- وظائف نظم إدارة قواعد البيانات

- تحديد مخطط قاعدة البيانات (يتحقق ذلك من خلال لغة تعريف البيانات)
- الاستعلام من قاعدة البيانات وتحديثها (يتحقق ذلك من خلال لغة معالجة البيانات)
- ضمان أمن البيانات: حماية البيانات من عمليات الوصول غير المشروع إليها من خلال تحديد صلاحيات كل مستخدم في الوصول إلى البيانات وتحديد نوع العمليات التي يُسمح لهم القيام بها
- ضمان سلامة البيانات: ضمان أن تكون البيانات صحيحة وخالية من التناقض في كل وقت

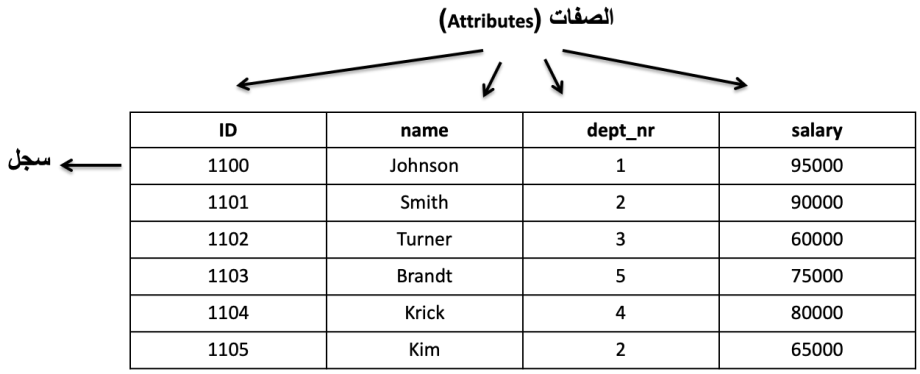
- ضمان استعادة البيانات في حال حدوث خطأ من قبل المستخدمين أو عطل في المكونات المادية للنظام إلى جانب توليد نسخ احتياطية من الملفات لاستخدامها في حالات الطوارئ
- ضمان عدم التداخل في التحديث عند وصول أكثر من مستخدم إلى عنصر البيانات الواحد في نفس الوقت

7-8- مزايا نظم قواعد البيانات

- التكامل: توزيع البيانات على عدة ملفات مع الحفاظ على ترابط البيانات ودون تكرار
- التشارك : الوصول إلى البيانات المخزنة من قبل عدة مستخدمين في نفس الوقت
- الاستقلالية بين الملفات والبرامج
- أمن البيانات: حماية البيانات من الوصول غير المشروع إليها
- سلامة البيانات: صحة البيانات وخلوها من التناقض في كل وقت
- إستعادة البيانات في حال حدوث أي طارئ وإنشاء نسخ احتياطية من الملفات

7-9- نظام قاعدة البيانات الترابطي (Relational Database)

يتم تمثيل المخطط المنطقي (Conceptual Schema) والمخطط الخارجي (External Schema) لقاعدة البيانات كما لو أن البيانات مخزنة (انظر الشكل ٧-٢). المفهوم الأساسي هوالرابطة/القائمة (Relation) التي هي عبارة عن جدول له أسطر وأعمدة، كل رابطة لها مخطط (Schema) خاص بها لتوصيف الأعمدة أو الحقول.



ID	name	dept_nr	salary
1100	Johnson	1	95000
1101	Smith	2	90000
1102	Turner	3	60000
1103	Brandt	5	75000
1104	Krick	4	80000
1105	Kim	2	65000

قائمة العاملين

dept_nr	dept_name	budget
1	Marketing	120000
2	Finance	100000
3	Research	90000
4	Statistics	95000
5	Engineering	80000

الشكل ٧-٢: مثال على قاعدة البيانات الترابطية

7-9- الصفات في النموذج الترابطي

- المفتاح الرئيسي (Primary Key) :صفة أو مجموعة صفات للتعرف على كل سجل داخل القائمة وتمييزه عن السجلات الأخرى، على سبيل المثال: رقم العامل في قائمة العاملين ورقم القسم في قائمة الأقسام
- المفتاح الأجنبي (Foreign Key): الصفة داخل القائمة التي تستخدم كمفتاح رئيسي في قائمة أخرى (تستخدم للربط بين القوائم). على سبيل المثال: رقم القسم في قائمة العاملين
- الصفات غير المفتاحية: الصفات الأخرى المستخدمة لتوصيف كل كيان

7-9-1- خصائص الصفات في النموذج الترابطي

- عدم التساوي: الصفة التي ستستخدم كمفتاح رئيسي للرابطة لا يمكن أن تأخذ القيمة نفسها مرتين في الرابطة
- عدم القدرة على الاختزال: عندما يكون المفتاح الرئيسي مجموعة من الصفات فإنه لا يمكن إلغاء أي صفة من هذه الصفات للتمكن من الوصول إلى سطر الرابطة المطلوب

- لا يجوز أن يُترك المفتاح الرئيسي خالياً بدون أي قيمة

7-10- متطلبات قواعد البيانات الترابطية

- كل حقل داخل أي سجل يجب أن يكون ذات قيمة أحادية
- قيم المفاتيح الرئيسية لا يجوز أن تكون خالية
- قيم المفاتيح الأجنبية (إذا لم تكن خالية) يجب أن تكون مساوية لقيمة المفتاح الرئيسي المقابل في قائمة أخرى (لضمان عدم تناقض البيانات(
- جميع الصفات غير المفتاحية ضمن القائمة الواحدة يجب أن تعبر عن صفة للكيان المعرف بالمفتاح الرئيسي

7-10-1- الخصائص الأساسية للقائمة

- عدم تكرار الأسطر ضمن القائمة: لكل سطر (سجل) مفتاح رئيسي مختلف عن السطر الآخر
- ترتيب الأسطر ضمن القائمة لا يغير من طبيعة القائمة
- ترتيب الصفات ضمن القائمة لا يغير من طبيعة القائمة
- قيم الصفات ضمن القائمة هي قيم أحادية
- درجة القائمة هي عدد الصفات (عدد الأعمدة) المكونة للقائمة

الفصل الثامن

تصميم قواعد البيانات

8-1- مقدمة

يهدف نظام قاعدة البيانات إلى تجميع البيانات عن الواقع في منظمة ما أو نظام ما من أجل ضمان الوصول إلى البيانات بسرعة وإجراء عمليات المعالجة عليها وتقديم المعلومات إلى المستخدمين. يتم تجميع البيانات حول الأحداث (مثل الإيداع أو السحب)أو الأشخاص (مثل العميل أو الموظف) أو الموارد (مثل النقدية أو الأوراق المالية). يطلق على هذه المكونات اسم الكيان(Entity) . الكيان هو عبارة عن شيء له وجود موضوعي أو شخصي في الواقع الفعلي أو في تصورنا (مثال: العملاء، البنوك، الموظفين). يُستخدم للتعبير عن كافة العناصر الموجودة في المنظمة. كل كيان له صفات (Attributes) تتطلب التخزين وهي عبارة عن مجموعة الخواص التي يمكن من خلالها توصيف الكيان (مثل رقم العميل، اسم العميل، العنوان، الرصيد). يتم التمييز بين **الكيان المفرد** (مثل العميل الواحد، الموظف الواحد) و**نموذج الكيان (Entity Type)** الذي يشمل مجموعة من الكيانات المفردة. على سبيل المثال، نموذج الكيان العميل عبارة عن مجموعة الكيانات العملاء الذي يمكن من خلاله عكس كافة عملاء المنظمة.

8-2- مراحل تصميم قواعد البيانات

- التصميم المنطقي (Logical Design): يتم في هذه المرحلة نقل المصطلحات السائدة في مجال المشكلة المعالجة إلى مصطلحات ومفاهيم لتوصيف البيانات باستخدام أدوات التصميم المساعدة، يتم نقل الواقع الفعلي وتصويره على شكل نموذج معين (Data Model)

- التصميم المادي (Physical Design): يتم في هذه المرحلة تحويل البيانات من نموذج البيانات (Data Model) إلى ملفات باستخدام لغة تعريف البيانات (Data Definition Language)

8-3- بناء نموذج البيانات (Data Model)

يتضمن بناء نموذج البيانات خطوتين أساسيتين:

- تحديد الكيانات المفردة التي يجب أن تنتمي إلى كيان معين
- تعريف وتحديد صفات الكيان: اختيار الصفات التي تساهم في تقديم المعلومات التي تفيد المستخدمين (الرقم، الاسم، العنوان، مكان التخزين، الخ)تتضمن هذه المرحلة اختيار الصفات الأساسية للمشكلة المعالجة وتحديد الصفات التعريفية التي تميز الكيان المفرد عن غيره ضمن الكيان (مثل رقم الحساب، رقم العميل)

8-3-1- أهداف بناء نموذج البيانات

- الخلو من الحشو والتكرار: عنصر البيانات الواحد يجب أن يخزن مرة واحدة في قاعدة البيانات
- التوافق: خلو البيانات المخزنة في كل وقت من التناقض
- التكامل: يمكن استخدام البيانات المخزنة من قبل كافة الأنظمة الفرعية ضمن المنظمة
- الاستقلالية: التعديل في استخدام البيانات من قبل الأنظمة الفرعية والبرامج يجب أن لا يقود إلى تغيير في البناء المنطقي للبيانات (تراكيب البيانات)

8-3-2- نموذج الكيان/العلاقة (Entity- Relationship Model)

يعتبر نموذج الكيان-العلاقة من أهم وأقدم التقنيات المستخدمة في تصميم البناء المنطقي لقاعدة البيانات. يفترض هذا النموذج أن الواقع يتكون من مجموعة من **الكيانات** و**الصفات** و**العلاقات** التي يمكن تمثيلها من خلال مجموعة من الرموز الرسومية:

- يتم تمثيل الكيان وفق هذا النموذج على شكل مستطيل يوضع بداخله اسم الكيان

- يتم تمثيل الصفات على شكل بيضوي يكتب داخلها اسم الصفة
- يتم تمثيل العلاقة على شكل معين

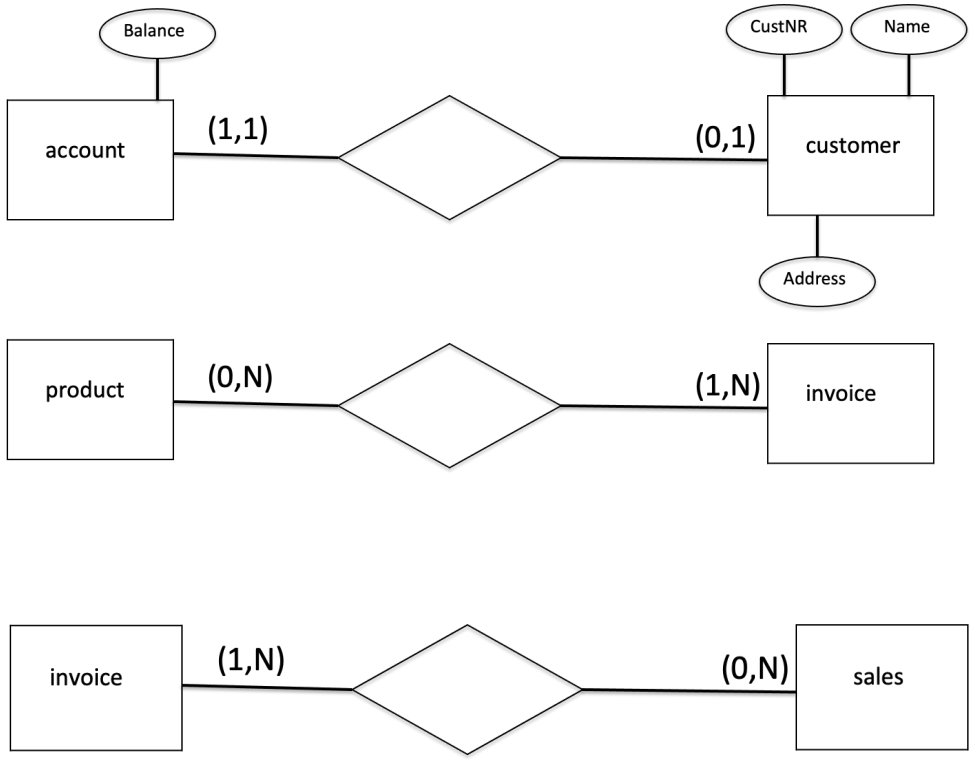
8-3-3- درجة العلاقة (Cardinaluty of Relationships)

المقصود بدرجة العلاقة هو تحديد الحد الأدنى والحد الأقصى للعلاقة بين الكيانات. الحد الأدنى لدرجة العلاقة هو أقل عدد ممكن من العناصر في كيان معين المرتبطة بعنصر محدد في الكيان الثاني، إما أن تكون صفر أو واحد. الدرجة الدنيا صفر تعني وجود عنصر من الكيان يمكن أن لا يرتبط بأي عنصر من الكيان الثاني. الدرجة الدنيا 1 تعني أن كل عنصر من الكيان الأول مرتبط على الأقل بعنصر من الكيان الثاني.

المقصود بالحد الأعلى لدرجة العلاقة هوالعدد الأقصى من العناصر في كيان معين المرتبطة بعنصر محدد في الكيان الثاني.

8-3-4- أنماط العلاقات وفق نموذج الكيان-العلاقة

- علاقة من نمط (1:1): تنشأ عندما يرتبط عنصر من الكيان الأول مع عنصر واحد فقط من الكيان الثاني (التعددية القصوى في كلا الكيانين هي 1). على سبيل المثال: العلاقة بين كيان العميل وكيان الحساب
- علاقة من نمط (1:N): تنشأ عندما يرتبط عنصر من الكيان الأول مع أكثر من عنصر من الكيان الثاني (التعددية القصوى في أحد الكيانين هي 1 والتعددية القصوى في الكيان الثاني هي N). على سبيل المثال: العلاقة بين كيان الموظف وكيان القسم
- علاقة من نمط (N:M): تنشأ عندما يرتبط عنصر من الكيان الأول مع عدد من عناصر الكيان الثاني كما يرتبط عنصر من الكيان الثاني مع عدد من عناصر الكيان الأول (التعددية القصوى في كلا الكيانين هي N). على سبيل المثال: العلاقة بين كيان الفواتير وكيان المنتجات (انظر الشكل ٨-١)



الشكل ٨-١: أنماط العلاقات وفق نموذج الكيان-العلاقة

4-8 -أهداف عملية تصميم قواعد البيانات

- الكمال: وجود كل البيانات التي يحتاجها المستخدمون
- الملاءمة: وجود البيانات الملائمة فقط القابلة للاستخدام
- الحداثة: حداثة البيانات وتمثيلها للواقع الآني للمنظمة
- المرونة: قدرة عدد كبير من المستخدمين الحصول على حاجتهم من المعلومات
- الفعالية: تخزين البيانات بأقل حجم ممكن وتخفيض الزمن اللازم لعمليات التحديث والحذف والإضافة والإستعادة
- السلامة: خلو البيانات من الأخطاء والتناقض
- السرية: حماية البيانات من الاستخدام غير المشروع