الضبط المعلوماتي في المصارف الاسلامية

د.محمد سليم وهبه

مجلة المستثمرون، العدد 73، نيسان 2008، الكويت، ص 80.

ما يمكننا ان نتعلمه من تجربة مصرف السوسيته جنرال المؤلمة، هو في معرفة كيف ان خرق الضبط الداخلي يمكن ان يؤدي الى خسائر مهمة في المؤسسات المالية، حيث يظهر من تحليل ما حصل في المصرف ان وسيط مصرفي واحد، تمكن من تنفيذ عمليات كبيرة، واخفاء قيم هذه العمليات بتحويرها وبالتلاعب في ارقامها دون ان تلحظها نظم المراقبه، والتي ربما اشارت الى هذه العمليات للمراقبة المستقبلية.

الخسائر بحجمها الكبير كانت ناتجة عن عدد من عمليات المضاربة التي كان يسمح لموظف القيام بها، وقد قام بدمج معرفته بخطط الرقابة التي لم يتم تطويرها وتغيير فتراتها الزمنية، بالاضافة الى استعارة كلمات المرور المعلوماتيه الخاصة لزملائه الموظفين.

الدرس الاول يكمن وبشكل واضح في عملية فصل الوظائف، وبالنظام المعلوماتي وبكيفية وضع الاجراءات الميكانيكية بحيث تساعد المكننة في عملية مراقبة المستويات التشغيلية.

كخطوة اولى على المصرف ان يحدد كافة العمليات المترابطة، والخاصة، والتي لا يمكن تركها لمستخدم واحد، وعلى المنشأة استخدام القدرات التقنية لمراقبة العمليات، وربما عبر اطلاق انذار بشكل تلقائي، بحال تم خرق موضوعية وصف الوظائف كمنح عمليات مترابطة لموظف واحد.

وعندما يغير احد الموظفين مركزه في المصرف، على صلاحيات الدخول المعلوماتي لهذا الموظف ان تتغير مباشرة. وما يحصل عادة، هو طلب مستخدمي النظم المعلوماتية من دائرة التقنيات المعلوماتية تصحيح العوائق عندما لا يمكنهم من الوصول للمعلومات التي يحتاجون لها، وبهذا يحصلون على تقديمات معلوماتية خاصة.

وبنظرنا يفترض لتحقيق ذلك اخذ الموافقة لاي اضافة من الادارة العليا، واعلام دائرة المراجعة الدخلية، وكمراجعة احترزية يطلب من المدراء مراجعة دورية لهذه التعديلات المعلوماتية الخاصة، ليكونوا بصورة صلاحيات الدخول المعلوماتي المبالغ بها. وتسوية الاوضاع، عبر وضع لائحة

بالمعلومات اللازمة لكل وظيفة، ولكل مستوى من مستويات الصلاحية، وان يوضع لائحة بكافة الصلاحيات الاضافية، مع وضع حدود مالية وتقنية لمستوى وحجم الاستخدام، وما هي تأثير الاضافات على الصلاحيات الاضافية.

ويتوجب لتاكيد الامان تغيير دوري لكافة كلمات السر المعلوماتية الخاصة، وذلك عبر وضع فترة صلاحية شهرية للمواقع الحساسة، هذه الكلمات يتوقف العمل بها تلقائيا خلال فترة شهر حيث يتوجب قطعا على الموظف تغييرها.

رغم ان التغيير لكلمة السر المتكرر له مساوئ عدة منها، نسيان الكلمة، حيث يلجأ البعض الى كتابتها اليومية، او في دفتر الهاتف، والذي يعارض الاهداف في بعض الاحيان، ويمكن حل الثغرة هذه بمساعدة الكترونية، فهناك تعديل جزئي للكلمات السرية، والذي يمكن ان يصبح يومي.

والاهم بما يتعلق بكلمات السر، ضرورة التأكيد على خصوصية هذه الكلمات، وعدم مشاركتها تحت طائلة المسؤولية، مع تثقيف العاملين على دور واهمية وخطورة مشاركة هذه الكلمات حتى في المستويات الدنيا، انعكاسها على تقييم الاداء واعطاء الحوافز والعلاوات.

من ناحية ثانية، ومع تعقد عمليات الدفع المصرفية، فالتقنيات المعلوماتية المكلفة والتي قد يمكنها وضع الاليات بشكل سريع، وفعال، يمكن للمصارف الكبرى تحمل نفقاتها، دون اي تأثير على ربحيتها، لما تؤمنه من قيمة مضافة.

بينما في المصارف الاسلامية وفي محاولتها الربط بين سرعة انجاز المعاملات، وبين ضمان وامان العمليات وصحة القيام بها، تبقى ثغرة من حيث مساندة الادارة المصرفية قدرات المعلوماتية النوعية، والتي قد تترك نظامها عرضة لهجمات او تأثيرات خارجية، وتكمن المشكلة في ان تجهيز نظام معلوماتي قد لا يغطي مجمل المخاطر، وعملية شراء نظام معلوماتي جاهز قد يكون اكثر مما تحتاجه المؤسسة المصرفية الاسلامية وغير مطابق لوضعية وخصوصية المصرف، حيث يتم اعداد هذه البرامج لخصوصية النظم المصرفية التقليدية، وترتكز على المعلومات المعتمدة في هذه المصارف، ويحاول المبرمجون اجراء بعض التعديلات عليها بما يتقارب مع الى حد ما الى ما يشابه المصارف الاسلامية.

فمن ناحية تشغيلية، يتعذز تعداد المخاطر التي تعترض عمليات الدفع والتي يمكن ان تصدر من داخل المنشأة، وتأخذ عدة اشكال، منها الدفع مرتين لنفس العملية، الاحتساب الخاطئ، الدفعات الغير مدعومة باصدة وضمانات، والمستفدين غير المناسبين، ومع التعقيدات التقنية لعمليات الاحتيال، يفترض وضع ادارة توقعية لما يمكن حدوثه.

عندما تفكر المصارف بمخاطر الاحتيال تفكر بشكل عام ان التهديدات سترد من الخارج، وقد اوردت بعض الدراسات ان 75% من عمليات الاحتيال يقوم بها موظفين من داخل المؤسسة، والمؤسف ان الخسائر على المصرف جراء عمليات الاحتيال تتخطى الخسائر المالية، الى قيمة السهم الشرائية، والسمعة، ومعنويات الموظفين.

عدد كبير من عمليات الاحتيال يقوم بها موظفين في مراكز ثقة، وهذه الاحتيالات لا يبلغ عنها قبل مرور فترة زمنية، كون المتضرر لا يمكنه التشكيك بالموظف الثقة، او بالزميل، او المستشار الذي قام بعميلة الاحتيال.

اصبح الاحتيال للمنشأة مشكلة تنطلق من سرقة هوية شخص آخر، او استعمال اسم مستعار، والحل يبدأ باجراءات اختيار الموظف، ومعرفة تاريخ عمله والمعلومات الاكاديمية والاديبة، خاصة للموظفين لذين لهم علاقة مباشرة بالنقد، والخزينة، ان لصالح المصرف او الزبائن، المدراء، ومسؤولي الادارات والمنفذين، المحاسبين، والقيمين على اعداد جداول الرواتب، المستشارين الماليين، والعاملين في القسم المعلوماتي.

هناك عدد من اجراءات الاستعلام البسيطة، والتي يمكن تعديلها تبعا لنوع الوظيفة، و التي يحتاج اصدار او التحقق من بعضها لموافقة امتقدم للوظيفة والتي قد تشمل بشكل عام:

- الهوية، بطاقة السوق، والتصريح الضريبي،
- التاريخ الاجرامي،
- المستوى الدراسي، وبامكانية تزوير مستندات، وشهادات، يمكن التحقق من المستندات من المؤسسات التعليمية المعترف فيها،
- مراجعة المستوى المهني،
- مراجعة الافلاس، الشيكات الغير مدفوعة،
- مراجعة المؤسسات المالية التي عمل، او تعامل معها،

- مرجعية مقدم الطلب واسماء الشركات التي عمل بها، وقد يتوجب على المصرف الاسلامي اجراء بعض التحقيقات عبر مكاتب المعلومات للتحقق من سيرة المتقدم للعمل،
- اجراء مقابلة صريحة بما يتعلق بمرجعية الشخص، والاتصال بالمرجعية، وسؤالهم اذا تسنت لهم الفرصة هل يقبلون بتوظيف الشخص مرة ثانية، حيث وفي كثير من الاحيان، يقوم الموظفين باعمال مشينة في مؤسساتهم، وحفاظا على سمعة لمؤسسة، يتم اعطاء الموظف شهادة حسن سلوك، فربما في هذه الحالة الطلب من احد موثوق على معرفة باحد الموظفين في الشركة التي عمل بها الموظف سابقا للسؤال.

هذه بالاضافة الى ما سبق ذكرة من ناحية تطور المسؤوليات في ادارة السيولة عبر لسنوات، والتي بها اصبح من الضروري اعتماد نظم معلوماتية تؤمن مراقبة شمولية، وتتحقق من موازين المراجعة، ومن الاسس والانظمة والحدود والسقوف المسموحة.

فالاصول الادارية هي هدف دائم للسرقة، من خارج ومن داخل المصرف، بالاضافة الى ان التهديدات الداخلية، لا تحتاج لان تكون ناشئة عن سوء نية، لتتسبب بخسائر كبيرة جدا على المصرف.

في القواعد الاساسية للمحافظة على موجودات وادارة الخزينة، يفترض حماية تنفيذ العمليات عبر اليات التاكد من هوية منفذ العمليات، وحمايتها من اشخاص قد تكون لهم سوء نيه تجاه المنشأة. والثغرة انه في الشركات يوجد يوميا موظفين مطرودين، او خفضت رتبهم، او تم نقلهم، فماذا يحصل لحساب المستخدم التي تم وضعه لهؤلاء الموظفين خلال هذ الاحداث؟.

فالمنشأة في مقابل ذلك تحتاج الى تعريف دور النشاطات الخاصة، وما هي معايير واجراءات تنفيذ العمليات، ومن هي الوظائف التي يمكنها ان تقوم بالتنفيذ، والموقع والجهاز الذي يفترض عبره القيام بالتنفيذ، مع استخدام بطاقة تعريف خاصة، تحدد مستويات الاستخدام.

مع تحديد المستلزمات الاساسية، يمكن للنظام المعلوماتي تطبييق الالية الموضوعة ومواكبة التغيرات التي يمكن ان تحصل، وبالتالي فالمنشأة لن تنشغل بموظف، بمقاول، او بشريك، والذي تم تحويله الى موقع آخر او مركز آخر، او تركه للمصرف.

فادارة الدخول الى الجهاز المعلوماتي، وترابطها بنظام ضبط داخلي يعتمد على فصل الوظائف، تخفف الى حد كبير كافة الخروقات، والذي يتطلب نظام ذكي يحد من العمليات المشبوه بها، ويتمتع بمرونة، ومثال ما يمكن ان يحصل في حال احتاج موظف لاخذ عطلة، فلا يمكن للنشاط ان يتوقف لمجرد ان يرحل موظف بصورة مؤقته، فمن المهم ان يتنازل الموظف الى اخرين عن صلاحياته ودوره بصورة مؤقته، بما يتوافق مع الاجراءات الداخلية.

فالمنشآت يمكنها القيام بالمراجعة الذاتيه وابداء الرأي بان العمليات امينه، بوضع نظام فصل و توزيع للوظائف، فالشخص الذي يقوم بدراسة جدوى مشروع، لا يفترض ان يكون من الاشخاص الذي يتخذون القرار باعتماد المشروع من قبل المصرف الاسلامي.

فنظام فعال لمراقبة الدخول الى النظام، يسمح بالنظر سريعا في اي وقت، الى اي فترة، واية عملية، ومن قام بها، ومن اي مركز، ولماذا، ويمكن للنظام اصدار تقارير، واوراق عمل، ليتمكن مراجعي النظام من تحمل مسؤولية اعطاء رأي بان المستندات والموازين صحيحة، وفي حال وجود انحرافات يتم مباشرة وضع التغيرات اللازمة.

لذا حاجة المصارف الاسلامية الى قاعدة معلومات موحدة، ودعوة الى التعاون فيما بينها للاستفادة من الاخطاء التي تقع في اطرها والتشاور في كيفية الحلول الممكنة، وفي اخطاء التطبييق، والعقبات، ما قد يساهم في اعداد نظم معلوماتية موحدة تخفض من الاكلاف لكل مصرف، في محاولة لتوحيد المعايير التشغيلية.