



٨٨٢١

الرقم : ٨٨٢١ / ١ / ١٠
التاريخ : ١٤٣٧ / ٩ / ٢٤ هـ
الموافق : ٢٠١٦ / ٦ / ٢٩ م

تعميم إلى البنوك المرخصة

تحية طيبة وبعد ،،،

في ضوء إزدياد اعتماد البنوك على أنظمة المعلومات وتكنولوجيا الاتصالات في أعمالها مما أدى إلى ارتفاع احتمالية تعرضها لمخاطر التشغيل والسمعة والسيولة وخصوصا تلك المخاطر الناتجة عن عمليات الاحتيال وسرقة الهوية والإبتزاز عبر وسائل تكنولوجيا المعلومات والاتصالات، وفي ظل تزايد مخاطر الهجوم الإلكتروني الذي تتعرض له البنوك في العالم، وأكد على ضرورة الاستمرار بتطوير وتشغيل آليات وأدوات قادرة بفعالية على حماية موجودات ومصالح البنك وعملائه من خلال تحديد وكشف والاستجابة والتعافي من أي محاولات إختراق إلكتروني.

وحيث يستخدم المخترقون في الهجوم الإلكتروني تقنيات متنوعة ومستحدثة مثل دَس البرامج الخبيثة التي تعمل على تعطيل خدمات البنك بطرق عدة ومنها ما يسمى بالـ (Ransomware)، بالإضافة لهجوم حجب الخدمة (DDoS) (Distributed Denial of Service) وسرقة بيانات الهوية والبيانات الحساسة للبنك والعملاء لتنفيذ عمليات مصرفية وتحويلات غير مشروعة ولإبتزاز البنك وعملائه.

أكد على ضرورة استمرار البنوك بتطوير عملياتها المتعلقة بتكنولوجيا وأمن المعلومات وإدارة المخاطر وضمان استمرارية العمل لمواجهة مخاطر الاختراق الإلكتروني بما فيها المذكورة أعلاه، وذلك من خلال مراعاة الأمور التالية والمبينة تفصيلها بالمرفق:

١. الاستمرار بتحديد وتقييم مخاطر تكنولوجيا وأمن المعلومات وبما يشمل المخاطر المستجدة بتقنيات الاختراق المستحدثة.

٢. ضبط معايير الأنظمة والبرمجيات وعناصر الشبكات وأنظمة الحماية المشغلة وإدارتها بطريقة تحد من مخاطر الاختراق الإلكتروني.

٣. توفير ضوابط الحماية من الاختراق غير المشروع، وذلك بحصر عدد رموز التعريف المستخدمة للنفاذ والاستخدام للأنظمة المختلفة من ذوي الامتيازات الحساسة (Administrators).

٤. توظيف موارد تكنولوجيا المعلومات لمراقبة ومنع النفاذ غير المشروع، مثل أجهزة كشف النفاذ (Intrusion Detection Systems) وأنظمة الحماية من الفيروسات والتأكد من تحديثها بشكل مستمر وتوظيفها بشكل فعال في عمليات المراقبة وكشف الاختراق.

٥. تحديث برامج التدريب والتوعية باستمرار لتشمل أساليب الاختراق الإلكتروني (Cyber Attack) وبما يشمل الابتزاز، وكيفية تحديد ومنع والتبليغ عن حوادث أمن المعلومات لكل من موظفي وعملاء البنك.

٦. توظيف وفحص ضوابط الحماية للأنظمة بشكل مستمر، مثل ضوابط النفاذ وتوثيق الهوية، وفصل المهام المتعارضة، وتوظيف أنظمة كشف الاحتيال والمراقبة.

٧. مراجعة وفحص اعتمادية وتحديث إجراءات الاستجابة ومعالجة الحوادث الخاصة بأمن المعلومات وخطط استمرارية العمل الخاصة بالبنك وتلك الخاصة بمزودي الخدمات.

٨. الاستفادة من المعلومات المزودة بخصوص تقنيات الاختراق المستجدة وكيفية التصدي لها ومعالجتها وتقليل مخاطرها من خلال الاشتراك بمننديات ومواقع موثوقة بالتوعية في الحماية من الإختراقات الأمنية الإلكترونية مثل (CERT) (Computer Emergency Response Team) حول العالم أو أية مصادر أخرى مشابهة.

مؤكداً على ضرورة الإلتزام بتبليغ البنك المركزي عن أية إختراقات أو حوادث يتعرض لها البنك في حينه وبحسب تعليماتنا بهذا الخصوص.

وتفضلوا بقبول فائق الاحترام ،،،

المحافظ

د. زياد فريز

- مرفق

مرفق

١. الاستمرار بتحديد وتقييم مخاطر تكنولوجيا وأمن المعلومات وبما يشمل المخاطر المستجدة بتقنيات الاختراق المستحدثة، والعمل على توفير ضوابط الحماية للخدمات والبيانات الحساسة من مخاطر سرقة الهوية باستخدام وسائل "توثيق الهوية القوي" (Strong Authentication) من خلال توفير تقنيات تأكيد الهوية التي تستخدم فئتين أو أكثر من فئات التوثيق التالية (Something you Know, Something you Have, Something you Are and) Security in Depth – (Something you Do)، وتوفير ضوابط الحماية الطباقية (Layered Security)، بالإضافة لتوفير آليات العمل اللازمة للتأكد من أن مزودي الخدمات المستعان بهم فيما يخص بيانات البنك وعملائه الحساسة ملتزمون بتوفير الضوابط اللازمة للسيطرة على المخاطر وبما يشمل عمليات الفحص المنتظم لتلك الضوابط ومن قبل أطراف ثالثة موثوقة (Trusted Third Parties)، والإلتزام بتزويد البنوك بتقارير فورية عن محاولات الاختراق وحوادث أمن المعلومات التي تتعرض لها بيانات وخدمات البنك لدى المزودين.
٢. ضبط معايير الأنظمة والبرمجيات وعناصر الشبكات وأنظمة الحماية المشغلة وإدارتها بطريقة تحد من مخاطر الاختراق الإلكتروني، من خلال توفير تقنيات عزل الشبكات الافتراضي والمادي واستخدام طرق التشفير القوي في تراسل وحفظ البيانات الحساسة، والاحتفاظ بسجل مخزون للأنظمة والأجهزة المصرح باستخدامها، وحذف أو تعطيل الأجهزة والخدمات غير المستخدمة.
٣. توفير ضوابط الحماية من الاختراق غير المشروع، وذلك بحصر عدد رموز التعريف المستخدمة للنفاذ والاستخدام للأنظمة المختلفة من ذوي الامتيازات الحساسة (Administrators)، ومراقبة استخداماتها بشكل مستمر لكشف أي محاولات اختراق غير مشروع، والعمل بشكل مستمر على مراجعة صلاحيات وامتيازات النفاذ والاستخدام الممنوحة على مختلف الأنظمة للتأكد من مناسبة طبيعتها لعمل (Role-based Access Privileges) واستخدامها بشكل مشروع، وحذف أو تعطيل رموز التعريف غير المستخدمة وبشكل فوري، ووضع قواعد للنفاذ والاستخدام للأنظمة مثل منح امتيازات النفاذ بالحد الأدنى (Least Privileges) وتعريف وقت ومكان خاص مراقب للنفاذ، بالإضافة لعمل مراجعات دورية منتظمة وعند الحاجة لامتيازات النفاذ والاستخدام الممنوحة على الأنظمة والبرمجيات المختلفة، وعدم السماح للمستخدمين بامتلاك امتيازات

(Administrator) على أجهزتهم إلا في أضيق الحدود وبموافقات استثنائية مبررة، وتغيير كلمات السر المصاحبة للأنظمة الجديدة (Default Passwords) بشكل فوري عند استخدامها، ومنع استخدام وربط أجهزة الكمبيوتر والأجهزة المحمولة والمملوكة من قبل الموظفين والمستخدمين ومن قبل الغير مع الشبكات والبنية التحتية التكنولوجية الخاصة بالبنك، وتوظيف الضوابط الرقابية لكشف الأجهزة المرتبطة بشبكات وموارد البنك بطرق غير مصرح بها.

٤. توظيف موارد تكنولوجيا المعلومات لمراقبة ومنع النفاذ غير المشروع، مثل أجهزة كشف النفاذ (Intrusion Detection Systems) وأنظمة الحماية من الفيروسات والتأكد من تحديثها بشكل مستمر وتوظيفها بشكل فعال في عمليات المراقبة وكشف الاختراق، وتوظيف قواعد الحماية بواسطة أنظمة (Firewalls) التي تعمل على مستوى الـ (Application Layer) وكشف ومراقبة التغيير لتلك القواعد بشكل فوري للتأكد من عدم تغييرها تمهيدا لاختراق (Passive Attack)، واستمرار تفعيل عمليات كشف الثغرات (Vulnerability Assessment) وفحص الاختراق (Penetration Testing)، والعمل على اتباع معايير القياس الدولية المقبولة في تطوير وتعديل البرمجيات ومراعاة توفر شروط الحماية الكافية عند تطويرها من قبل البنك، ومراعاة توفر شهادات الفحص بحسب المعايير الدولية المقبولة من أطراف ثالثة معتمدة عند شراء برمجيات جاهزة أو عند الاستعانة بالغير لدى تطوير البرمجيات، وتحديث أنظمة البرامج (System Software) المختلفة بشكل مستمر وخصوصا التحديثات المتعلقة بإغلاق الثغرات الأمنية من قبل المزودين لتلك الأنظمة.

٥. توظيف وفحص ضوابط الحماية للأنظمة بشكل مستمر، مثل ضوابط النفاذ وتوثيق الهوية، وفصل المهام المتعارضة، وتوظيف أنظمة كشف الاحتيال والمراقبة، وتحديد عتبة (Threshold) لعدد المستخدمين للأنظمة بشكل آني، وتوظيف ضوابط التنبيه وإعلام مستخدمي الأنظمة عند تغيير شروط الحماية أو عند النفاذ والاستخدام لتلك الأنظمة، وفحص ضوابط الأنظمة للتأكد من فعاليتها باستمرار وإطلاع الإدارة التنفيذية ومجلس الإدارة عند اللزوم، ومراجعة سياسات كلمات السر وتطبيقها بشكل مستمر، واتباع إجراءات محكمة في تخزين أو في إتلاف البيانات الحساسة حفاظا على سريتها بما يشمل وسائط التخزين المستخدمة، وحصر عملية نفاذ الموظفين للإنترنت بالمواقع الموثوقة فقط واللازمة لتشغيل عمليات البنك بأمان، واتباع إجراءات محكمة في آليات النسخ الاحتياطي لضمان توافرية البيانات وسريتها.

٦. مراجعة وفحص اعتمادية وتحديث إجراءات الاستجابة ومعالجة الحوادث الخاصة بأمن المعلومات وخطط استمرارية العمل الخاصة بالبنك وتلك الخاصة بمزودي الخدمات، وبما يشمل تحديد مسؤوليات الأفراد تجاه إدارة مخاطر التشغيل والسمعة والسيولة وأمن المعلومات والاحتياط وإدارة خدمات المزودين وطلبات وشكاوى العملاء، والتأكد من أن تلك الإجراءات والخطط تشمل حوادث الاختراق الإلكتروني والإبتزاز وهجوم حجب الخدمة (DDoS) بالتعاون مع مزودي خدمات الإنترنت (ISP) (Internet Service Provider) كلما لزم الأمر ذلك.