هيئة الأوراق المالية والسلع
SECURITIES & COMMODITIES AUTHORITY

ملخص تنفيذي لتقرير

Cyber resilience: Health check

المرونة الالكترونية : فحص السلامة

الصادر عن الهيئة الأسترالية للأوراق المالية والاستثمارات (ASIC)

إعداد :قسم العلاقات الدولية والمنظمات

مارس 2016م

ملخص تنفيذي - المرونة الالكترونية (Cyber Resilience)

يسلط هذا التقرير الضوء على أهمية المرونة الالكترونية (Cyber resilience) للجهات الخاضعة لرقابة هيئة الأوراق المالية والاستثمارات الاسترالية، ومساعدتهم في تحسين المرونة الالكترونية (Cyber resilience) الخاصة بهم من خلال:

- زيادة الوعي حول مخاطر القرصنة الالكترونية (Cyber risks).
- تشجيع التعاون بين الصناعة والحكومة.
- تحديد الفرص لتحسين المرونة الالكترونية (Cyber resilience).
- كما يهدف إلى تحديد كيفية معالجة مخاطر القرصنة (Cyber risks) كجزء من التزاماتها القانونية والامتثال الحالية التي لها ذات الصلة لهيئة تنظيم الأوراق المالية والاستثمارات الاسترالية.

أ) ماذا يقصد بالهجوم الالكتروني (Cyber attack)؟

هو أي واقعة سواء كانت فعلاً مقصوداً أو محاولة إحداث هجوم الكتروني إما:

- عن طريق استخدام تكنولوجيا الحاسوب أو الشبكات لارتكاب أو تسهيل ارتكاب الجرائم التقليدية كسرقة البيانات الشخصية (عبر استخدام الحاسوب).
- أو بغرض استهداف أجهزة الحاسب الآلي وأنظمة الحاسوب أو معلومات تكنولوجيا الاتصالات الأخرى وعلى سبيل المثال، القرصنة أو الحرمان من الخدمات (سلامة الحاسب الآلي).

ب) الآثار المترتبة من الهجوم الالكتروني (Cyber attack)

قد تسبب الهجمات الالكترونية المشاكل التالية:

- خسائر كبيرة في تكلفة الفرص البديلة – وعلى سبيل المثال: السرقات المتعلقة بالملكية الفكرية للمعلومات والتي تحدثها الاختراقات الناجمة عن القرصنة الالكترونية.

- فقد ثقة كل من له علاقة بالمؤسسة سواء كان من الجهات الخاضعة أو المتعاملين، والإضرار بسمعتها في المجتمع وعلى سبيل المثال من خلال انتهاك بيانات الخصوصية نتيجةً للهجمات الالكترونية.

ج) ماذا يقصد بالاعتماد الالكتروني (Cyber Reliance)؟

هو القدرة على الاستعداد للاستجابة والتعافي من الهجمات الالكترونية. من خلال وجود مرونة المنع والتصدي لأي هجوم الكتروني، كما يأخذ بعين الاعتبار القدرة على العمل خلال هذه الهجمات والتكيّف والاستعداد لها.

وفي هذا الصدد فقد أعدّت هيئة الأوراق المالية والاستثمارات الاسترالية بعضاً من المقترحات التي من شأنها أن تساهم في مساعدة الجهات الخاضعة لعملية التحسين على سبيل المثال الفحوصات الخاصة بأنظمة الحاسوب والشبكات (Health check)، وكذلك تمكينها من الاستعداد للهجمات الالكترونية. علماً بأن عملية الفحص الدورية هي مبادرة تطوعية وغير الزامية مما لا يتطلب على الشركات أو الجهات الرقابية القيام بها.

د) دور هيئة الأوراق المالية والاستثمارات الاسترالية:

ومن الجدير بالذكر تصدّر الجهات الخاضعة والمرخصة من قبل مكتبة تطبيق المكوّن القياسي (ASCL) طليعة إدارة المخاطر الالكترونية.

ولدى الكثير منهم ممارسات استباقية ومتطورة في إدارة المخاطر للتصدي للمخاطر الالكترونية. وكما تعتمد أنواع المخاطر التجارية التي تواجهها الجهات على طبيعة وحجم وتعقيد أعمالها. علماً بأن لهيئة الأوراق المالية والاستثمارات الاسترالية دوراً هاماً في توعية المشاركين والتعرف على المخاطر الالكترونية وإدراكهم لها، وعلى سبيل المثال:

- تطورات مراقبة السوق.
- مواصلة الانخراط ، إدراك أهمية المرونة الالكترونية مع زيادة تعريف القضايا.
- دمج المرونة الالكترونية في البرامج الرقابية، حيثما كان مناسباً، وعبر الأفراد والأعضاء الخاضعين.

هـ) كيف سيتم إجراء عملية الفحص:

وقد حددت هيئة الأوراق المالية والاستثمارات الاسترالية بعض الأسئلة الرئيسية التي من الممكن أن يتم أخذها بعين الاعتبار من قبل الجهات الخاضعة والمرخصة، على سبيل المثال:

- مدى علم مجلس الإدارة بالمخاطر الالكترونية.
- القدرة على تحديد مستوى الأمن الالكتروني للمؤسسات.
- وضع أهداف لتحقيق الأهداف الالكترونية.
- وضع خطط لتحقيق الأهداف.
- كيفية حماية البيانات.
- المخاطر التي تتعرض لها المؤسسة مع سبل الحد من تلك المخاطر.
- تدابير الاتصال التي يؤخذ بها عند حدوث مخاطر مماثلة.
- المخاطر الالكترونية المحتملة عبر مقدمي الخدمات (طرف ثالث).
- من خلال اختبار اجراءات وأنظمة تكنولوجيا المعلومات.
- توفير موارد كافية للتعامل مع الهجمات الالكترونية.