تعميم

الرقم: ت.ع.م/202204/246
التاريخ: ٢٠٢٢/٠٤/٢٤م

الموضوع: مبادئ تحليل التهديدات السيبرانية للقطاع المالي

Subject: Financial Sector's Cyber Threat Intelligence Principles

سعادة الرئيس التنفيذي المحترم
مسؤول الالتزام المحترم

السلام عليكم ورحمة الله وبركاته،

انطلاقاً من دور البنك المركزي السعودي الرقابي والإشرافي على القطاع المالي، وإشارةً إلى استراتيجية الأمن السيبراني للقطاع المالي الهادفة إلى خلق قطاع مالي آمن وموثوق يُمكّن من النمو والازدهار، وأخذًا بالاعتبار التغير في نماذج الأعمال للمؤسسات المالية، والاعتماد على التقنية في المعاملات المالية، واستقطاب تقنيات ناشئة وحديثة.

وحيث لوحظ تغيّر في مستوى التهديدات السيبرانية للقطاع المالي والذي نتج عنه تطور سريع وملحوظ من قبل مجموعات الاختراق المتقدمة والتي تستهدف القطاع المالي لأغراض مختلفة، وذلك على عدة أصعدة مثل الأساليب والأدوات والإجراءات مستخدمة من قبلهم؛ مما يتعيّن معه تطوير قدرات الرصد والتقصي للمؤسسات المالية للعمل بشكل استباقي يواكب تطور مجموعات الاختراق.

عليه، تم اعتماد مبادئ تحليل التهديدات السيبرانية للقطاع المالي "المبادئ" والتي تهدف إلى وضع أسس علمية وعملية للرصد والتقصي عن التهديدات السيبرانية وتعزيز ممارسات المؤسسات المالية في استقصاء التهديدات السيبرانية؛ لأخذ الإجراءات الاحترازية وتغذية مختلف الإدارات التقنية والتشغيلية وإدارات الأعمال بمعلومات استباقية تلائم عمل هذه الإدارات، حيث تم تقسيم المبادئ على عدة مستويات كالآتي:

Dear CEO,
Dear CCO,

Greetings,

Based on the supervisory role of the Saudi Central Bank on the financial sector, and in reference to the Cybersecurity strategy for the financial sector which aims at creating a secure and reliable financial sector that enables growth and prosperity. And taking into consideration the changes in business models of financial institutions, relying on technology in financial transactions, and attracting emerging and modern technologies.

Whereas a change has been observed in the level of Threat Landscape to the financial sector, which resulted in a rapid and noticeable development by the Advance Persistence Threat "APT" groups targeting the financial sector for different purposes on several levels such as their Tactics, Techniques, and Procedures; which requires the development of proactive detection and analysis capabilities for financial institutions to work proactively in line with the development of the threat actors.

Accordingly, the Financial Sector Cyber Threat Intelligence Principles "Principles" had been adopted, which aims to establish scientific and practical foundations for proactive detection and analysis of the cyber threats as well as enhancing the practices of financial institutions with regard to cyber threat intelligence; to take precautionary measures and feed the various technical, operational and business

departments with Threat Intelligence appropriate to the work of these departments, the Principles are divided on several levels, as follows:

- Core principles – required basis activities needed to perform planning, production and dissemination of threat intelligence.

- Strategic principles – strategic level cyber intelligence focused on the objectives, motivations and intent of threat actors.

- Operational Principles – to produce information about modus operandi, behavior and classification of the different stages of attacks (Taxonomization).

- Tactical principles – includes information about technical elements and components of cyber attacks

Accordingly, to enhance the cyber resilience of the financial sector and raise the maturity level of threat intelligence capability; The financial institutions shall be guided by these principles. In case of implementing the principles, we recommend that the stages of implementation are as following:

1. Conducting a gap assessment of the current status of Threat Intelligence management, compared to what is stated in the principles, with its various levels, to identify the gaps.
2. Develop a roadmap for full compliance with the Principles as of this circular date, according to the following periods:
   a. Six months for core, operational and tactical principles.
   b. Twelve months for strategic principles.
3. Present the prepared Roadmap to the Board of Directors, inform them of it, and obtain approval of the plan and the necessary support for its implementation.
4. The cyber security committee in the financial institution shall follow up the implementation of the principles and the extent of commitment to the approved plan and provide full support to solve the obstacles and challenges facing the competent teams in the financial institution; while escalating internally to the authorized person on anything that may affect or obstruct the implementation of the principles.
5. Provide the necessary support to the Cyber Security Department to fully implement the principles,

مبادئ أساسية – يتطلب العمل بها كأساس لجميع عمليات الرصد والتقصي عن تهديدات السيبرانية.

- مبادئ استراتيجية – تُركز على الجوانب الاستراتيجية للمعلومة المتقصَّى عنها مثل أهداف ودوافع مجموعات الاختراق وتحديد سيناريوهات الاختراق والهجوم المتوقعة حسب مستوى التهديدات السيبرانية للجهة والقيام بالتقييمات اللازمة.

- مبادئ تشغيلية – تستهدف تحليل الأنماط والأساليب التشغيلية لمجموعات الاختراق مثل البرامج الخبيثة والإجراءات المتبعة وتصنيف المراحل المختلفة للهجمات.

- مبادئ تقنية –المبادئ المتعارف عليها في تحليل التهديدات السيبرانية للخروج بمؤشرات الاختراق وضوابط الكشف والتصدي للهجمات السيبرانية.

بناءً على ذلك، ولتعزيز المرونة السيبرانية للقطاع المالي ورفع مستوى النضج للرصد والتصدي الاستباقي للتهديدات السيبرانية؛ فإنه يتعيّن على المؤسسات المالية الاسترشاد بهذه المبادئ، كما نوصي أن تكون مراحل العمل بالمبادئ في حال تطبيقها كالآتي:

١. إجراء تقييم دقيق للوضع الحالي لإدارة التهديدات الأمنية في المؤسسة المالية مقارنة بما ورد في المبادئ بمختلف تصنيفاتها لتحديد الفجوات.

٢. وضع خطة عمل للالتزام التام بالمبادئ اعتباراً من تاريخه، وذلك حسب المدد التالية:

أ. ستة أشهر للمبادئ الأساسية والتشغيلية والتقنية.

ب. اثنا عشر شهراً للمبادئ الاستراتيجية.

٣. عرض الخطة المعدة على مجلس الإدارة واطلاعهم عليها وأخذ الموافقة على الخطة والدعم اللازم لتطبيقها.

٤. قيام لجنة الأمن السيبراني في المؤسسة المالية بمتابعة تطبيق المبادئ ومدى الالتزام بالخطة المعتمدة وتقديم الدعم الكامل لحل العقبات والتحديات التي تواجه الفرق المختصة في المؤسسة المالية والتصعيد الداخلي لصاحب الصلاحية عن كل ما من شأنه أن يؤثر أو يعيق تطبيق المبادئ.

enhance the role of cyber threat intelligence, and ensure that they are provided with competency and trained national human resources, technological tools and appropriate training to carry out their tasks to the fullest.

If there are inquiries in this regard, you can contact the General Department of Cyber Risk Control represented by the Cybersecurity Fusion Center at the e-mail: (CFC@SAMA.GOV.SA)

To be informed and complied with.

Kind regards,
General Department of Insurance Control

Distribution to:
- Insurance sector companies

٥. تقديم الدعم اللازم لإدارة الأمن السيبراني لتطبيق كل ما ورد في المبادئ وتعزيز دور تحليل التهديدات السيبرانية والتأكيد على تزويدهم بالكفاءات والكوادر الوطنية المدربة والأدوات التقنية والتدريب الملائم للقيام بمهامهم على اكمل وجه.

وفي حال وجود استفسارات بهذا الخصوص يمكن التواصل مع الإدارة العامة للرقابة على المخاطر السيبرانية ممثلةً بالمركز الاستشرافي للأمن السيبراني على البريد الإلكتروني: (CFC@SAMA.GOV.SA).

للاطلاع والعمل بموجبه،

وتقبلوا تحياتنا،
الإدارة العامة للرقابة على التأمين

نطاق التوزيع:
الشركات العاملة في قطاع التأمين.

البنك المركزي السعودي
SAMA
Saudi Central Bank