OTS0042 5 WI 0477 FMA0001 WB Mo, 01.Jul 2019
Banken/IT/Finanzen und Dienstleistungen/Verbraucher/Wirtschaft und Finanzen

FMA und OeNB testen in einem Planspiel die Reaktionsfähigkeit des österreichischen Bankensektors auf Cyber-Attacken

Wien (OTS) - Die Österreichische Finanzmarktaufsichtsbehörde (FMA) und die Oesterreichische Nationalbank (OeNB) haben heuer den ersten Cyber-Stresstest für den Finanzmarkt Österreich durchgeführt. Unterstützt vom „Kuratorium Sicheres Österreich“ (KSÖ), wurde in einem Cyber-Planspiel die Widerstandsfähigkeit des Finanzsektors gegen verschiedene Cyberangriffe getestet. Teilgenommen haben zehn repräsentative Kreditinstitute, deren IT-Provider, das „Computer Emergency Response Team Austria“ (CERT.at) und das Innenministerium. Da laut internationalen Studien rund zwei Drittel der Cyber-Schäden durch Fehlverhalten von Mitarbeitern verursacht oder zumindest begünstigt werden, lag bei diesem Planspiel der Fokus auf dem Faktor Mensch. Gestresst wurde insbesondere die Zusammenarbeit zwischen Kreditinstituten und Aufsicht sowie den anderen cybersecurity-relevanten Institutionen im Falle eines Hackerangriffs.

Erster institutsübergreifender Cyber-Stresstest

„Das Cyber-Planspiel hat gezeigt, dass die Kreditinstitute im Großen und Ganzen organisatorisch gut auf Cyber-Attacken vorbereitet sind, wobei jedoch die praktische Ausgestaltung sich als sehr unterschiedlich erwiesen hat“, so der Vorstand der FMA, Helmut Ettl und Klaus Kumpfmüller: „Die Ergebnisse werden nun im Detail analysiert, die Lehren daraus gezogen und in der Folge in der regulatorischen und aufsichtlichen Tätigkeit umgesetzt.“ OeNB Vize-Gouverneur Andreas Ittner ergänzt: „Gerade bei der Abwehr von Cyberangriffen ist eine gemeinsame Vorgangsweise zur Sicherstellung der Stabilität des Finanzsektors essenziell. Wir begrüßen es daher sehr, dass sich hier Repräsentanten aller relevanten Institutionen am ersten institutsübergreifenden Cybersecurity-Planspiel für den Finanzsektor beteiligt haben.“

Das Ausgangsszenario des eintägigen Cybersecurity-Planspiels, an dem mehr als 100 Experten teilnahmen, bildeten insgesamt 170 individualisierte Hackerangriffe, auf die die Teams aus den beteiligten Kreditinstituten und Institutionen zu reagieren hatten. Die Attacken reichten dabei von Lösegeld-Erpressung mit Ransomware, der Kompromittierung von „Root-CAs“[1] und von „Online Banking Apps“, der Lahmlegung von Bankomaten und Websites, dem Ausfall des

Electronic Bankings, Manipulationen von Kontoständen und -transaktionen, Verlust von Kundendaten, „Phishing Mails“ und DDoS-Attacken[2] bis hin zu Kundenbeschwerden und Shitstorms in Social Media. Getestet wurden dabei die institutsinternen Vorbereitungen auf derartige Angriffe, die internen Kommunikations- und Entscheidungsstrukturen, die organisatorischen und technischen Back-up-Lösungen, Information und Kommunikation mit den aufsichtlichen Institutionen sowie die externe Kommunikation mit den Kunden sowie der breiten Öffentlichkeit.

„Die weltweite digitale Vernetzung bringt den Teilnehmern auf den Finanzmärkten viele neue Chancen und Möglichkeiten, birgt aber gleichzeitig enormen Risiken. Dementsprechend haben wir IT- und Cyber-Sicherheit als strategischen Aufsichtsschwerpunkt festgelegt“, betten Ettl, Kumpfmüller und Ittner den Cyber-Stresstest in die Aufsichtsstrategie ein. Dazu habe die FMA im Vorjahr ein Paket von IT-Sicherheits-Leitfäden erlassen, die klare Vorgaben für die Governance dieser Risiken darlegen. Die Einhaltung der Vorgaben der IT-Sicherheitsleitfäden bilde dementsprechend auch einen Prüfschwerpunkt der Aufsicht in diesem Jahr. Das Cyber-Planspiel hat die Implementierung der Vorgaben, die organisatorische wie infrastrukturelle Vorbereitung in der realitätsnahen, praktischen Anwendung getestet. Darauf aufbauend wird die Aufsicht ihre regulatorische und aufsichtliche Strategie weiterentwickeln und diese in weiteren Cyberstresstests prüfen und evaluieren.

* * *

[1] Zertifizierungsstellen für Wurzelzertifikate

[2] DDoS: Distributed Denial of Services

~
Rückfragehinweis:
Finanzmarktaufsicht
Klaus Grubelnik (FMA-Mediensprecher)
+43/(0)1/24959-6006 oder +43/(0)676/882 49 516
~

OTS0042 2019-07-01/10:00

011000 Jul 19

Link zur Aussendung:
https://www.ots.at/presseaussendung/OTS_20190701_OTS0042