FSSCC Releases "Financial Sector Return to Normal Operations Resource Guide" for US Financial Firms

On 27 May 2020, the Financial Services Sector Coordinating Council (FSSCC) released a 'Financial Sector Return to Normal Operations Resource Guide' (**FSSCC**) for United States of America financial services firms. The 13 page resource guide provides considerations for US financial services firms' decision makers as they determine how to safely return workers to offices and other facilities response to the global coronavirus pandemic (COVID-19). The guide includes resources for aligning with state and local restrictions and options to consider in making decisions about operational status while protecting the health and safety of workers, customers, and communities. While this resource guide is intended for US financial firms, given the global impact of COVID-19 and the interdependency of supply chains, it may prove useful for firms with global operations and those outside the US. FS-ISAC staff contributed to this resource guide in collaboration with other US associations and US government agencies.

MSFT Warns of COVID-19 Phishing Emails

According to a series of alerts from the Microsoft Security Team Reports (**Microsoft**), there is an ongoing, massive COVID-19-themed phishing campaign which is attempting to install the NetSupport Manage remote access tool on Windows devices. The legitimate remote administrative tool, known to be abused by hackers, can give the threat actors complete control over an infected device and gives them the ability to move laterally through other parts of the targeted network (**BankInfoSecurity**). This campaign, which started on 12 May 2020, leverages the COVID-19 pandemic and according to Microsoft, uses several hundred unique attachments, mainly malicious Excel documents that hide the NetSupport Manager. Microsoft reports that all the unique Excel files used that bewildered analysts, but they all pointed to the same URL to download the payload. The alert did not say if this phishing campaign was targeted to a geographic region, or its success rate.

Open-Source Libraries Producing Unintended Flaws

Veracode published their annual State of Software Security report which highlighted that 70 percent of applications in use today have at least one security flaw coming from usage of an open-source library, with 351,000 external libraries tested in 85,000 applications. While open-source libraries provide the ability for developers to add basic functionality quickly, there is a basic lack of understanding of where and how open-source libraries are being used. These developers may be using one library but the data being sourced may have been pulled from another open-source library, without the developer's knowledge. (**Threatpost**)

MSFT Warns of COVID-19 Phishing Emails

Ransomware, now being looked upon as a credible and potential future risk to public companies, is more prevalent in filings with the Securities and Exchange Commission (SEC). Due to the filings, shareholders of public companies become more aware of the vulnerability of a ransomware attack as well as garner a better understanding of possible losses incurred, should an attack occur. The SEC issued guidance in 2018 that asked public companies to improve their disclosure of cybersecurity risks, with an emphasis of ransomware to be disclosed. Ransomware gangs prefer targeting larger companies as the payouts are much higher than individuals (**ZDNET**).

Identity Protection in a Post-COVID-19 World

As organizations prepare to resume a "business as usual" routine in a post Covid-19 world, CIOs and CISOs are hard at work focusing on simplifying infrastructure management. Legacy Privileged Access Management (PAM) is now considered antiquated in today's hybrid cloud and multi-cloud environments, noting access management tools used for one vendor are not compatible with another vendor. Agility and speed are fundamental for privileged access requestors to support increasingly safer apps and platforms (**FORBES**).

FS-ISAC Intelligence Exchange

The FS-ISAC Intelligence Exchange is the new platform for members to utilize our services and collaborate with their fellow members. This will allow quicker, seamless access to all of FS-ISAC's capabilities, while also providing more control and customization of your engagement with FS-ISAC (**Learn more**).

This monthly update is brought to you by the Financial Services Information Sharing and Analysis Center (FS-ISAC) in coordination with the Investment Industry Association of Canada (IIAC), the International Council of Securities Associations (ICSA), the Financial Services Institute (FSI), the Insured Retirement Institute (IRI), the Securities Industry and Financial Markets Association (SIFMA) and the SPARK Institute.

The information provided in this monthly newsletter highlights cybersecurity topics and emerging threats to the securities industry globally. It is intended to increase the cybersecurity awareness of an organization's end-users and to help them interact in a more secure manner. This newsletter is not intended to replace the benefits of joining FS-ISAC. Learn more at fsisac.com.