SEC Releases 2023 Examination Priorities

On 7 February 2023 the Securities and Exchange Commission's Division of Examinations today announced its 2023 **examination priorities**. The annual publication by the division is to provide insights into its risk-based approach, including the areas it believes present potential risks to investors and the integrity of the U.S. capital markets. The publication includes insight on operational risk, it also highlights information security and operational resiliency which will include a focus on cybersecurity issues associated with the use of third-party vendors and the integrity of third-party products and services.

HardBit 2.0 Ransomware Campaign Asks for Cyber Insurance Policy Details

HardBit was initially observed in October 2022, with version 2.0 being observed in November 2022, and it targets organizations to extort cryptocurrency payments for the decryption of their data. HardBit differs from their peers by not having a leak site and not using the double extortion tactic. They also do not request a specific amount of cryptocurrency in the ransom note, but rather request to negotiate to reach a settlement. As part of this note, they advise that their victims with insurance policies disclose the details so that their demands can be crafted to fit the policy and to refrain from using intermediaries. Best practices indicate you should not disclose your insurance policy as it may impact your ability to claim damages from your insurer.

Patch Released for Zero-Day Bug in GoAnywhere MFT App

GoAnywhere MFT, a secure file transfer tool provided by Forta, has a recently **discovered vulnerability** which is being actively exploited. The vulnerability is an RCE flaw that involves gaining access to the admin console of the tool. Forta has released a patch and advises that customers apply it immediately, especially if you are running an admin portal exposed on the internet.

Usually, the admin console is only accessible through a private company network, VPN, or allow-listed IP addresses, but it has been revealed that close to 1,000 instances are exposed. If you are unable to apply the patch, you should **take measures** to allow admin interface access only from trusted sources or disable the licensing service. You should also check for any stored credentials in the environment and revoke them.

New Treasury Report on Financial Sector Cloud-Based Technology Adoption

The US Department of the **Treasury released a report** on the benefits and challenges associated with financial sector firms adopting cloud services technology. They indicate that while adopting these services can help institutions be more resilient and secure, and increase access and reliability, they come with significant challenges that often fall on the Cloud Service Providers (CSPs). The CSPs are not doing enough to be transparent for due diligence and monitoring and provide support for deploying and tailoring their service. The current market is concentrated around a small number of CSPs and, if there is an incident at one, many financial institutions and the overall sector can be impacted. Additionally, the CSPs bargaining power is stronger given the reduced competition. Navigating the many regulatory and supervisory approaches can make it impossible to adopt consistent cloud strategies globally for financial institutions, and impact CSPs ability to provide quality and security of services to all their clients.