Securities Industry Risk Group (SIRG)

Global Cybersecurity Brief – December 2021

Banks to Report Cyber Incidents Within 36 Hours

On 17 November, the Federal Reserve, Federal Deposit Insurance Corporation (FDIC) and Office of the Comptroller of the Currency (OCC) have **finalized a rule** that directs banks to report any major cybersecurity incidents to the government within 36 hours of discovery. The new bank rules stipulate that firms must notify their primary regulator of a significant computer breach as soon as impossible and no later than 36 hours after discovery and must also notify customers as soon as possible of the cyber incident if it results in problems lasting more than four hours.

This new rule applies to any cyber security incident that is expected to materially impact a bank's ability to provide services, conduct its operations or undermine the stability of the financial sector. Previously there was no specific requirement for how quick a bank must report a major computer breach. This new rule will now help regulators to catch up on the rapidly growing role technology is playing in every type of banking service.

Ransomware Attacks Highlight Stronger Cyber Measures in APAC

Ransomware has become a prolific and challenging problem for organizations in the **Asia Pacific (APAC) region**. The average cost of redeeming a ransomware attack has grown by more than US$1 million, with remediation costs, this also includes business downtime, operational costs, lost orders, and more. Earlier this year, Singapore's Cyber Security Agency reported **a rise of 154% in ransomware cases,** affecting small and medium size enterprises in sectors such as manufacturing, retail, and healthcare.

US Treasury Continues to Counter Ransomware with New Sanctions

Last week, the United States Treasury Department, Office of Foreign Assets Control (OFAC), State Department, Department of Justice (DOJ), and Financial Crimes Enforcement Network (FinCEN) issued a **ransomware advisory**. The Treasury announced a set of actions focused on disrupting criminal ransomware actors and virtual currency exchanges that launder the proceeds of ransomware.

The State Department announced **a series of rewards**, one is a reward offer of up to $10 million dollars for information leading to any individuals who hold a key role in the Sodinokibi Ransomware variant transnational organized crime group, also known as REvil.

The Office of Foreign Assets Control (OFAC) has identified Ukrainian Yaroslav Vasinskyi and Russian Yevgeniy Polyanin for their parts in perpetuating Sodinokibi/REvil Ransomware incidents against the US. Vasinskyi is said to have deployed ransomware against nine US companies, and is responsible for the July 2021 Ransomware against Kasey, an IT software company, which affected over 1,000 businesses around the world. The DOJ has charged Vasinskyi, who remains in custody after his arrest in Poland in October 2021. Separately, FinCEN has published an updated advisory reflecting information on current trends and typologies of ransomware and associated payments, as well as recent examples of ransomware incidents.

Protecting Endpoint Privilege Management

When targeting an organization, cyber-criminals will look to steal privileged account credentials in order to gain access to the entire organization's network, also known as targeting endpoints. As per the **Verizon's 2021 Data Breach Investigations Report**, 80% of breaches include compromised credentials, a common entry point by cyber-criminals. **Endpoint Privilege Management** (EPM) is a formidable approach for transforming a least privilege security posture breach. While implementing EPM may provide an initial challenge, it is imperative to provide an EPM strategy that does not impede employee performance while restricting user and application privileges.