ABSTRAK

ABSTRAK

Serangan siber terhadap perusahaan SolarWinds pada tahun 2020 merupakan salah satu serangan siber terbesar yang pernah dialami Amerika Serikat (AS). Serangan tersebut menggunakan metode *software supply chain attack* dengan menyisipkan malware SUNBURST ke dalam pembaruan *software* Orion SolarWinds sehingga memungkinkan pelaku memperoleh akses ke berbagai lembaga pemerintah federal AS dan perusahaan swasta. Serangan ini diduga dilakukan oleh kelompok Nobelium atau APT-29 yang berafiliasi dengan Badan Intelijen Luar Negeri Rusia (SVR). Perisitwa tersebut menimbulkan ancaman terhadap keamanan nasional Amerika Serikat serta menunjukan kerenatan keamanan *software supply chain*. Penelitian ini bertujuan untuk menganalisis dampak serangan siber SolarWinds bagi Amerika Serikat, mengidentifikasi upaya pemerintah federal Amerika Serikat dalam menanggulangi serangan tersebut, dan menganalisis peran Cybersecurity and Infrastructure Security Agency (CISA) sebagai aktor utama dalam penanggulangan serangan siber SolarWinds tahun 2020-2021. Penelitian ini menggunakan metode penelitian kualitatif dengan pendekatan deskriptif-analitis. Teknik pengumpulan data dilakukan melalui studi kepustakaan dengan memanfaatkan buku, jurnal ilmiah, laporan pemerintah, dokumen resmi, dan sumber-sumber akademik lainnya. Penelitian ini menggunakan teori liberalisme yang menekankan pentingnya kerja sama, interdependensi, dean peran aktor negara maupun non-negara dalam hubungan internasional. Hasil penelitian menunjukkan bahwa pemerintah Amerika Serikat melakukan berbagai upaya melalui pembentukan Unified Coordination Group (UCG), penerbitan Emergency Directive 21-01, pengembangan perangkat mitigasi, serta peningkatan koordinasi antarlembaga. CISA berperan penting dalam mengeluarkan kebijakan mitigasi, berbagi informasi ancaman siber, dan mengoordinasikan respons nasional. Selain itu, kerja sama antara CISA dengan sektor privat seperti Microsoft, FireEye, dan SolarWinds menunjukkan pentingnya kolaborasi antara aktor negara dan non-negara dalam menghadapi ancaman siber. Temuan penelitian ini memperlihatkan bahwa teori liberalisme relevan dalam menjelaskan upaya pemerintah Amerika Serikat melalui CISA dalam menanggulangi serangan siber SolarWinds.

Kata Kunci: CISA, SolarWinds, keamanan siber, serangan siber, liberalisme, Amerika Serikat, Rusia.

ABSTRACT

The cyberattack against SolarWinds in 2020 was one of the largest and most sophisticated cyberattacks ever experienced by the United States. The attack employed a software supply chain attack method by inserting the SUNBURST malware into SolarWinds Orion software updates, allowing the attackers to gain unauthorized access to various United States federal agencies and private sector organizations. The attack was allegedly conducted by the Nobelium or APT-29 group affiliated with Russian Foreign Intelligence Service (SVR). This incident posed a significant threat to United States national security and exposed vulnerabilities in software supply chain security. This research aims to analyze the impact of the SolarWinds cyberattack on the United Staes, identify the efforts of the United States federal government in responding to the attack, and examine the role of the Cybersecurity and Infrastructure Security Agency (CISA) in addressing the SolarWinds cyberattack during 2020-2021. This study employs a qualitative research method with a descriptive-analytical approach. Data were collected through library research utilizing books, academic journals, government reports, official documents, and other relevant scholarly sources. The study applies liberalism theory, which emphasizes cooperation, interdependence, and the role of both states and non-state actors in international relations. The findings indicate that the United States government implemented various measures through the establishment of the Unified Coordination Group (UCG), the issuance of Emergency Directive 21-01, the development of mitigation tools, and the enhancement of interagency coordination. CISA played a crucial role in issuing mitigation policies, sharing cyber threat intelligence, and coordinating the national response. Furthermore, cooperation between CISA and private sector entities such as Microsoft, FireEye, and SolarWinds demonstrates the importance collaboration between state and non-state actors in addressing cyber threats. The findings also show that liberalism theory is relevant in explaining the efforts of the United States through CISA in responding to the SolarWinds cyberattack.

Keywords: *CISA, SolarWinds, cybersecurity, cyberattack, liberalism, United States, Russia.*

ABSTRAK

Serangan siber ka pausahaan SolarWinds dina taun 2020 mangrupa salah sahiji serangan siber panggedéna anu kungsi kajadian di Amerika Serikat. Serangan éta ngagunakeun metode 'software supply chain attack' ku cara nyelapkeun 'malware' SUNBURST kana pembaruan parangkat lunak Orion SolarWinds sahingga ngamungkinkeun palaku pikeun meunang akses kana rupa-rupa lembaga pamaréntah federal jeung pausahaan swasta di Amerika Serikat. Serangan ieu diduga dilakukeun ku kelompok Nobelium atawa APT-29 anu aya patalina jeung Badan Intelijen Luar Negeri Rusia (SVR). Kajadian ieu nyebabkeun ancaman kana kaamanan nasional Amerika Serikat sarta némbongkeun ayana kalemahan dina kaamanan 'software supply chain'. Panalungtikan ieu miboga tujuan pikeun nganalisis dampak serangan siber SolarWinds ka Amerika Serikat, ngaidentifikasi upaya pamaréntah federal Amerika Serikat dina nanggulangan serangan éta, sarta nganalisis peran Cybersecurity and Infrastructure Security Agency (CISA) salaku aktor utama dina nanggulangan serangan siber SolarWinds dina taun 2020-2021. Panalungtikan ieu ngagunakeun métode panalungtikan kualitatif kalayan pendekatan deskriptif-analitis. Téhnik ngumpulkeun data dilaksanakeun ngaliwatan studi pustaka ku ngamangpaatkeun buku, jurnal ilmiah, laporan pamaréntah, dokumén resmi, jeung sumber akademik séjénna. Panalungtikan ieu ngagunakeu teori liberalisme anu nekenkeun pentingna gawé babarengan, silih gumantung (interdependensi), sarta peran aktor nagara boh aktor non-nagara dina hubungan internasional. Hasil panalungtikan némbongkeun yén pamaréntah Amerika Serikat ngalaksanakeun rupa-rupa upaya ngaliwatan pembentukan Unified Coordination Group (UCG), penerbitan Emergency Directive 21-01, pamekaran perangkat mitigasi, sarta ningkatkeun koordinasi antarlembaga. CISA miboga peran anu penting dina ngaluarkeun kawijakan mitigasi, ngabagikeun informasi ancaman siber, sarta ngakoordinasikeun réspon nasional. Salian ti éta, gawé babarengan antara CISA jeung sektor swasta saperti Microsoft, FireEye, jeung SolarWinds némbongkeun pentingna kolaborasi antara aktor nagara jeung non-nagara dina nyanghareupan ancaman siber. Hasil panalungtikan ieu némbongkeun yén teori liberalisme relevan pikeun ngajelaskeun upaya pamaréntah Amerika Serikat ngaliwatan CISA dina nanggulangan serangan siber SolarWinds.

Kecap Konci: *CISA, SolarWinds, kaamanan siber, serangan siber, liberalisme, Amerika Serikat, Rusia.*