Overview of the National Cyber Strategy (2023)

Sahmer Ismael

Old Dominion University

Professor Hamza Demirel

10/1/24

Introduction of the National Cybersecurity Strategy (2023)

The National cybersecurity strategy is a framework that was created by the Biden administration in 2023, that highlights the importance of securing the United States, cyber realm and protecting critical infrastructure, and citizens sensitive information, from malicious threat actors. The National cybersecurity strategy (NCS) highlights a crucial adjustment to the nations approach to cybersecurity, and the need of collaboration, between both public and private sectors to protect the digital realm (White house, 2023). Furthermore, the NCS also works to identify emerging trends in the digital space and hold malicious actors responsible for cybercrimes against the United States, through the implementation of 5 distinctive pillars. "These pillars are to defend Critical Infrastructure, Disrupt and Dismantle Threat Actors, Shape Market Forces To Drive Security And Resilience, Invest In A Resilient Future, and Forge International Partnerships to Pursue Shared Goals" (White house, 2023). The combination of these pillars, work to create a digital resilient ecosystem, for the United States and its allies, and strives to promote an inherently defensible, resilient, and a aligned approach, to pair with the nations values (White house, 2023).

The Importance of addressing Emerging Trends

Emerging trends are constantly being driven from advancements in technologies, in which brings upon innovation on one side, and much risk, due to insecure systems on the other. An example of this issue would be the upbringing of artificial intelligence, which has behaved in a way to further advance technology and promote protection but can also behave in a manner that is unexpected to even its creators. This causes panic and complexity when it comes to incorporating, such a technology to the United States most critical systems. Therefore, the NCS, calls for a plan of action to invest in resilient technologies such as AI, which can counteract these

emerging threats from causing major damage to the nation's most critical systems, and can be used to promote innovation and protection. Addressing emerging threats is important when it comes to protecting the cyber landscape of the nation, due to the internet, which connects individuals, businesses communities and countries on shared platforms.

Objectives of Pillars of the National Cybersecurity strategy (2023)

Pillar One defending critical infrastructure: Critical infrastructure is one of the most important aspects to the nations, security, public safety and economic prosperity (White house, 2023). Which is the reason why it's, important to safeguard are most critical systems, and minimize the harm of cyber events, so the United States can continue to be more resilient and secure, on building towards a digital ecosystem. The NCS is making a large investment into renewing the nations critical infrastructure through a variety of ways, such as digitalizing energy systems, updating cryptographic computerizations, and establishing new cybersecurity requirements in certain critical sectors (White house, 2023). This pursue of building up to defend the United states critical infrastructure, became a major goal for the United States after seeing the unprovoked cyber-attack by the Russian military in 2022, in which they disrupted major systems for Ukraine. This led the United States into collaborating with both the public and private sectors through a campaign called shield up, to increase preparation in combating malicious campaigns aimed at critical infrastructure. This pillar aims to restore trust for the American people, in which they are confident with the availability of their most critical systems.

Pillar two Disrupt and Dismantle Threat Actors: While the United States, look to further advance in the cyber realm, and protect its most critical systems of information. Threat actors continue to sabotage these goals and look to cause problems through a series of malicious activities. These crimes include, espionage and intellectual property theft, detrimental damage to

critical infrastructure, ransomware attacks, and campaigns aimed to destroy public trust in the foundation of the government (White house, 2023). Offensive tools, that where once only available, to well-resourced countries in the past, are now widely accessible across the globe (White house, 2023). These offensive tools look to empower countries, that lacked capabilities previously of damaging the United States, to know distributing cyberspace, and issuing a growing threat in the digital realm. The United states most malicious threat actors in cyberspace are, China, Russia, Iran, and North Korea, which all use aggressive cyber tactics with the goal to dismantle citizens trust in the United states. The NCS works to disrupt these malicious cyber activities and limit the impact these attacks have on critical infrastructure through the shift of, roles, responsibilities and resources in cyberspace (White house, 2023). Furthermore, the NCS objective, when it comes to dealing with threat actors, is to not only strengthen the nation's defense, but also change the fundamental dynamics, that go against the nation's goals. This pillar main objective is to, effectively cause disruption to adversaries and disrupt campaigns at scale of disrupting the United States cyberspace (White house, 2023).

Pillar three Shape Market Forces to Drive Security and Resilience: For the United States to be able to work towards sustaining a digital ecosystem, they must be able to shape market forces to reduce risk (White house, 2023). This pillar recognizes that implementation of security measures, can be very expensive, and calls for alternatives that are found on the market, for organizations to adopt, and implement into their originations (White house, 2023). Furthermore, this pillar addresses the need for a federal cyber insurance backstop, due catastrophic cyber events that would maintain the present market for cyber insurance (White house, 2023). This pillar aims to promote a security design approach across the digital ecosystem (White house, 2023).

Pillar four Invest in A Resilient Future: When it comes to progressing as a nation, towards a more secure and resilient future, there must be leverage that is committed towards investments in innovation, R&D, and education to pursue results that are economically maintainable and serve the nations purpose (White house, 2023). This pillar highlights the importance of funding a educational pipeline through a number of grant programs, such as the National Science foundation (NSF), in which will help to build the next set of innovate leaders to help safeguard and research into emerging trends, in the digital realm. This investment of the future workforce of cyber-leaders, will help to continue leadership in technology and innovation, through a future economic and development approach.

Pillar Five Forge International Partnerships to Pursue Shared Goals: This Pillar elaborates on the importance of collaborating with allies around the globe to battle cyberthreats. This includes the partnership of the declaration for the future of the Internet (DFI), which is a partnership that includes over 60 countries, including the United states, that have a shared goal of maintaining a reliable, secure digital ecosystem for their nations. Furthermore, the NCS work to strengthen agreements on the norms of cybersecurity between nations and help respond to efforts of malicious cyber-attacks (White house, 2023).

Implementation of National Cybersecurity strategy (2023)

There are many key components of the NCS (2023), since takes a different approach from previous strategies, when it comes to its defensive and offensive capabilities, through its pillars. This includes the commitment to use its offensive capabilities, in its third pillar to "Disrupt and dismantle threat actors", if necessary (White house, 2023). This approach shows that the government is not afraid to take the fight to threat actors if issues where to arise. Furthermore, the strategies highlight the importance of alliance between the private and the public sector is

needed for securing cyberspace. However, this can only be achieved if the government designs a market incentive, throughout their domains, that priorities security. This will help to position organizations that deal with defending critical infrastructure, to more likely algin with government security standards. Furthermore, the strategies highlights that there is a gap in cyber talent for the digital realm and wants to incorporate more funds and research for future cyber specialist to be able to safeguard the digital realm. This help the nation prepare for future combat and continue to build on emerging technologies.

Conclusion

In conclusion, the national cybersecurity strategy is a step forward for the United States, cybersecurity mission. This strategy highlights the importance of protecting critical infrastructure, disrupting threat actors, shaping market forces, investing in resilience, and forging partnerships, to securing the nations digital landscape. This strategy will need both the public and private sectors, however, to team up to safeguard the most critical systems of the United states, and defend against malicious threat actors, that have goals of disrupting the nations operations. furthermore, much investment will be needed for the strategy to be implemented, due to many smaller and medium sized organizations, not having the funds to be able to implement the strategy. Overall, the strategy sets guidelines, for the nation on how to be more resilient and be adaptive to cyber threats that occur and promotes best practices to sustain the nations digital ecosystem for the near future.

Worked cited

National Cybersecurity strategy. (2023, March 1). https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

In-depth Review of Pillar one: Defending Critical Infrastructure

When it comes to the importance of critical infrastructure, they are systems and networks that serve a major purpose in the daily lives of citizens, and promote national security, economic sustainability, health, and safety, in which the public relies on daily (White house, 2023). This includes systems such as water systems, emergency services systems, communication systems, and healthcare services, which are all very important to the sustainability of life (White house, 2023). The citizens of the United States must have belief in the systems that carry much weight for the nations task. Therefore, the NCS, looks to require owners of critical infrastructure, to adopt regulatory frameworks that are adaptive to the emerging trends in cyberspace, and are addressed to each sector biggest risk (White house, 2023). Furthermore, these frameworks must meet the need of national security, and promote public security, to organizations, employees, clients, and supporting operations.

The importance of establishing resilient regulations

When it comes to the protection of critical infrastructure, the best regulations and practices, must be prioritized by federal departments, that deal with the defending of critical infrastructure, in a deliberated and coordinated manner (White house, 2023). This helps to elevate market failures and gaps in statutory authorities (White house, 2023). This proposal also helps to move away from a one size fits all approach, and to regulations that are more performance based, leverage familiar cybersecurity frameworks, and practices, and is adaptive to adversaries' capabilities, such as the CISA and NIST frameworks (White house, 2023). Furthermore, the implementation of effective regulations for critical infrastructure can help to promote a secure by design approach, availability of crucial services, and quick recovery if issues where to occur (White house, 2023). Effective regulations can also, reduce the value and issue of disagreement,

between organizations, and more cap space for them to invest their funds in protection and resilience for their systems. Furthermore, The NCS highlights, that different infrastructure sectors, will all not be able to afford the cost of cybersecurity regulations, so the strategy wants to work with regulators, to ensure that they implement regulations that consider the resources used for its implementation.

The Importance of public- private collaboration to defend critical Infrastructure

When it comes to the defense of critical infrastructure, there must be a model that is implemented to mirror the internets disrupted structure (White house, 2023). However, this can only be achieved if there is collaboration between sectors, in which roles and responsibility are spilt, and connectivity is prioritized. Furthermore, this helps to create a "networks of networks model, enabling sectors to support each other in responding to incidents (White house, 2023). Through a collaboration of software, hardware, and managed service providers with the goal of improving resilience across the digital ecosystem. Furthermore, the collaboration of both public and private sectors, will also improve areas such as threat detection, incident response, and recovery of system during attacks or natural disasters, and further enhance the protection of critical infrastructure. However, this model cannot be implemented, without the coordination of the Cybersecurity and infrastructure security agency (CISA) and sector risk management agencies (SRMAs), overseeing the needs of the critical infrastructure sectors (White house, 2023). The coordination from agencies such as CISA will help to close gaps between sectors, and improve government capability's (White house, 2023). Moreover, the overseeing of SRMAs agencies and cybersecurity centers will help in putting together, all the governments abilities across the homeland of defense, justice systems, national security, diplomatic efforts, and economical goals. This scheme could lead to technical solutions, and the coordination of defense

strategies. Overall the collaboration of both public and private sectors, is much needed for the defense of critical infrastructure in the United states , and resilience and defense cannot be guaranteed, without the teamwork's of both sectors, into dealing with threat actors, trying to disrupt critical systems.

The Importance of Modernizing Federal Systems

When it comes to the IT and OT systems that are currently incorporated within the government, but are vulnerable to all cyber-attacks, it is important for them to be removed and updated as soon as possible (White house, 2023). The goal of the NCS is to get rid of old legacy systems, that are costly, and were created with cybersecurity not in mind. This is very important due to the amount of sensitive information these systems hold. The goal of modernizing systems for critical infrastructure protection, is to be able to incorporate zero trust architecture strategy and cloud security tools, to secure systems. The plan of the NCS, is working to incorporate the removal of all legacy systems, within the next decade and move to more resilient systems for the near future.

Conclusion

In conclusion, the protection of critical infrastructure, serves a major purpose in the daily lives of Americans, everyday and continues to serve the most reliant systems for emergencies and other remedies. Therefore, it is important for critical infrastructure owners, to adopt the most resilient regulations and frameworks that are adaptive to emerging cyber threats and are essential to security. Furthermore, these systems must be able to adapt to zero trust architecture strategies and can be implemented in all sectors of the government. However, this cannot be achieved if there is no collaboration, between both the pubic and the private sectors. The collaboration between both sectors, will help to ensure innovation, and resilience for the protection of critical infrastructure.

In-Depth Review of Pillar two: Disrupt and Dismantle Threat Actors

When it comes to the daily processes of IT and OT systems, they serve a core function in the everyday life of citizens, through services and security of critical information. This includes systems such as energy sectors, healthcare systems, water systems, emergency systems, and many more (White house, 2023). These government systems, however like all systems, have vulnerabilities that are constantly exploited by malicious threat actor campaigns. Which its damages can jeopardize the national security and public safety of the United States (White house, 2023). These attacks can conclude many different types of cyber tactics to obtain unauthorized access of critical systems. However, the most prominent cyber-attack that is used on critical systems to gain unauthorized access are ransomware attacks. Ransomware attacks are a type of malware attack in which, a user is tricked into downloading malicious attachments, through forms of email, websites, and even ads, to their devices (Kosinski,2024). And once downloaded all the user's files are encrypted, and can only be recovered, if a form of cryptocurrency is paid to the attacker (Kosinski,2024). This type of attack costs the United States billions of dollars every single year and continues to be a consistent threat in the protection of IT and OT systems. Which is why pillar two of the NCS addresses, that the United States will use all equipment of power to work to disrupt and dismantle threat actors, that's actions go against the nation's goals (White house, 2023).

The Need to Integrate Federal Disruption Activities

The need for integrated disruption campaigns, is essential for the security of critical systems in which it will have malicious threat actors, reconsider their actions. This is why the NCS highlights that the DOJ and other federal enforcement agencies, including the public sector, and international allies, will work together to deter malicious actors, through many means of

disruption, in which malicious threat actors, no longer find it an effective mean of achieving their campaign goals (White house, 2023). This includes the disruption of activities such as dismantling botnet chains, obtaining cryptocurrency from ransomware attacks, and terminating campaigns of fraud (White house, 2023). Furthermore, this approach helps to generate insights on threat actors, identify malware, and put a stop to malicious activity, before it effects targeted individuals (White house, 2023). This approach also helps organizations, notify individuals who were affected by the crime, and furthers diplomatic actions and intelligence operations (White house, 2023). However, to increase the speed of these distribution campaigns against malicious threat actors, the government will need to promote, and advance technological and organizational objectives to continue operations. Furthermore, these integrated campaigns will help to strengthen the incident response of systems and deter attacks from organized groups in advance.

The need for Public and Private collaboration to Dismantle Threat Actors

When it comes to administering the behavior of malicious threat actor campaigns, that are designed to disrupt critical government systems, this is a task the government cannot handle alone. Rather there must be collaboration between both the public and the private sectors, to administer the issue. The private sector also brings a lot of more capability to the government sector, due to the fact in which they have better visibility into adversaries' interest. The reason behind this is that the private sector unlike the government sector, continues to grow rapidly in the race of innovation, tools, strategy, and capabilities (White house, 2023). The private sectors are also very advance, when it comes to threat hunting, in which they have shown they have been able to take down the Emotet botnet, which was a very big issue for many organizations globally. While the government sector on the other hand, are outdated in their legacy systems that are not

compatible with offensive mechanism to battle cybercrime, which is why the collaboration is needed to further enhance dismantling threat actors.

The Importance of Addressing Ransomware capabilities of threat actors

Ransomware is the most impactful threat to public safety, national security and economic success of the nation (White house, 2023). Since ransomware has disrupted hospitals, school systems, service pipelines, and other essential services. Due to the major impact in which ransomware has carried out on key critical infrastructure of the United States, from cyber threat actors, across the globe such as North Korea, Russia, and Iran (White house, 2023). The United States has then implemented all elements of national power, along with 4 rules of effort against ransomware. rule number 1, is to collaborate with nations across the globe to decrease the ransomware ecosystem, and close off countries that protect cybercriminals, rule number 2, is investigating ransomware crimes and networks, plus bringing criminals to justice (White house, 2023). Rule number 3 is to strengthen critical infrastructure, to better restrain from ransomware attacks, and rule number 4, identifying the misuse of virtual currencies (White house, 2023). These tactics help to deter malicious threat actors, from using ransomware tactics, however ransomware continues to persist in the digital realm.

Conclusion

In conclusion, the spread of ransomware attacks continues, to cause major issues for the United States government, through critical infrastructure, and critical systems. The NCS highlights the need for the United States government to collaborate with the public sector, to be able to counter these cyber-attacks. Including the collaboration of international nations, to be able to lower the impact of ransomware networks worldwide. This strategy also helps to strengthen nations, against emerging threats, improve threat hunting techniques, and better prepare themselves, for

cybercrimes. This strategy also helps to send a message to malicious threat actor nations, across the globe, that there will be consequences for the crimes in which they commit in the United States digital ecosystem.

Work Cited

Ibm. (2024, October 1). What is ransomware?. IBM. https://www.ibm.com/topics/ransomware

National Cybersecurity strategy. (2023, March 1). https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf