President Biden's Cybersecurity Executive Order: Explained

On May 12 evening the Biden administration released an Executive Order on improving the USA's Cybersecurity. It took into consideration the recent mishaps with SolarWinds and the Colonial Pipeline incident and provided concrete measures to mitigate such events in the future. Now, is this an end-all to cybersecurity issues within the USA? The short answer is no. The Cybersecurity landscape is huge. What the Executive Order has successfully done is, it has made good use of the limited tools at its disposal and has provided directives to federal entities that would require them to take action from a cybersecurity perspective.

Even though these directives are issued for federal entities, the president has urged all private sector vendors and organizations to follow suit. This is because, as mentioned in the Executive Order, "Much of our (the federal government) critical domestic infrastructure is owned and operated by the private sector."

What is the SolarWinds breach/ Sunburst hack?

Back in early 2020, One of SolarWinds's most deployed products, Orion was subjected to a highly unusual and stealthy hack. The attackers managed to sneak in some malicious code in SolarWinds's systems. This malware was then sent to at least 18,000 Orion users through an update. It was one of the largest breaches the country had ever witnessed. The victims of the attack included government agencies like the US Treasury to Fortune 500 companies. This particular attack was a software supply chain attack.

What is the Colonial Pipeline incident?

The Colonial Pipeline incident happened two weeks ago, on May 7th. The Colonial Pipeline company was attacked with ransomware and the company ended up paying $5 million in ransom, to the perpetrators. The incident has had huge implications on the global economy and the cybersecurity landscape. Especially because, in this case, the ransomware used was a known variant and yet the systems of such a critical entity were not equipped to deal with it.

What does the Executive Order entail?

The first section of the Executive Order titled "Policy" clearly states,

> "But cybersecurity requires more than government action. Protecting our Nation from malicious cyber actors requires the Federal Government to partner with the private sector. The private sector must adapt to the continuously changing threat environment, ensure its products are built and operate securely, and partner with the Federal Government to foster more secure cyberspace.

The implications of this Executive Order go beyond just federal government entities. Each vendor and buyer in the private sector should have an understanding of these implications and try to adhere to them to the best of their abilities.

Sharing threat information

From the SolarWinds fiasco, federal agencies like the FBI and CISA found out that it was quite hard to extract information about cyber threats or attacks from private third-party vendors. This was quite the pickle because most of the federal systems are either run or are supported by private third-party vendors. The reason why these vendors weren't sharing such critical information is due to certain stipulations in their contracts. These stipulations either limit or prohibit the sharing of such information with federal agencies. To remedy this, the Executive Order has suggested a period of 120 days, within which the contracting rules will be reviewed to accommodate the changes that would alleviate the aforementioned problems. It is to be noted that software products or any product that would act as a support system for the said software is included in the disclosure rule. Vendors or providers are also asked to promptly convey any threat information as and when it happens.

So, what should vendors look out for? At the end of the day, the vendors would have to maintain information regarding event prevention or response. Share such information with the government when the need arises. And fully cooperate with the federal entities involved in the event.

As for the buyers, expect better accountability from tech vendors regarding threat information.

Cloud is here to stay

In the 3rd section, the Executive Order addresses the adoption of the cloud in the federal government. The Executive Order defines guidelines on secure cloud adoption practices and how vendors or agencies should work alongside the FBI or CISA during a cloud breach event. The order has also laid the groundwork for revamping the security authorization for cloud services.

Speaking of authorization, the zero-trust model is in. The order emphasizes the importance of the zero-trust model as a means to curb software supply chain attacks and other breaches.

As for tech vendors in general, try to follow suit and adopt zero-trust principles within their own organization. Eliminate implicit trust on every level when it comes to security planning for the software. As the philosophy of zero-trust elucidates, trust nothing, verify everything.

Transparency is Key

In sec 4 of the Executive Order, it is stated that

> "The development of commercial software often lacks transparency, sufficient focus on the ability of the software to resist attack, and adequate controls to prevent tampering by malicious actors. There is a pressing need to implement more rigorous and predictable mechanisms for ensuring that products function securely, and as intended.

As the USA witnessed multiple cyber-attacks, most of it on the software front, the administration came to a realization that software security is key and transparency regarding the development of the software is important. The SolarWinds event or the Sunburst Hack was a software supply-chain attack. A software supply chain includes all the components that go into the software's code. Since software suppliers are increasingly adopting open-source codes, certain components of the software are third-party-made. Cyber attackers hone in on the design flaws of these third-party components and exploit them to access critical data.
To combat this, this Executive Order has brought forward certain stipulations, in a nutshell, it is as follows:

- Calling upon the National Institute of Standards and Technology to provide guidelines regarding software supply chain security, the guidelines were as follows:

1. use administratively separate build environments;
2. audit trust relationships;
3. establish multi-factor, risk-based authentication and conditional access across the enterprise;
4. document and minimize dependencies on enterprise products that are part of the environments used to develop, build, and edit software;
5. employ encryption for data; and
6. monitor operations and alerts and respond to attempted and actual cyber incidents;

- Incorporating an SBOM or Software Bill of Materials. An SBOM is bound to bring transparency on what third-party components are mixed in with the code of the software you are purchasing. So, buyers call now identify shortcomings in each software they are buying.

So, what's the takeaway?
Software or SaaS vendors would be expected to have a better understanding of the components of their software. They should have a higher degree of knowledge regarding who authored each component, how it is being tested, and in what way it is being secured.
As for buyers, they are now equipped with a higher degree of knowledge regarding the

software they are using, thanks to the SBOM.

Creating a cybersecurity safety review board and a playbook

The Executive Order also managed to establish a cybersecurity safety board, headed by both government and private sector leads, to convene after any major cybersecurity event and analyze the situation and make necessary recommendations.

A standardized playbook was also established by the Executive Order for a response during a cyber incident. This playbook is meant for federal entities and agencies. It was noticed by the administration that, even within the government, the response towards cyber incidents was unsatisfactory in most cases. This playbook shall standardize the response across all federal agencies. The playbook shall also provide private sector organizations, a template to be used during such an incident.

What does it mean for vendors?

For too long, organizations both private and public, have made the same mistakes over and over again. By establishing a cybersecurity safety board, the cybersecurity problems that are encountered by these organizations will be analyzed and remedied.

Conclusion

So, after 38 pages of points and sub-points, where are we? While the Executive Order does not break any new ground, it certainly is a move in the right direction. The administration seems to have molded the Order around the findings of the Sunburst Hack and the more recent Colonial Pipeline Hack, of which the consequences are still unfolding. The administration didn't go for gradual changes and instead went for big sweeping changes. That is commendable and we are looking forward to seeing how this unfolds.