Reaction to: President Trump's Executive Order from 11 May 2017 on Strengthening Cybersecurity of Federal Networks and Critical Infrastructure

Divya T Aradhya

Table of Contents

Abstract

On May 11, 2017, President Trump signed an executive order on “Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure”. This is perhaps the single most important document that would dictate, for the foreseeable future, the cybersecurity culture in the United States of America. This paper aims at summarizing the salient features of the order and analyzing its contents.

Brief Summary

Having made a study of the current cybersecurity landscape in the country and drawing certain conclusions, the Executive Order has pushed for changes aimed at building a stronger system from within, as well prepare for the future. Towards this effect the order demands accountability and transparency from agency heads, sets specific deadlines for submitting of their plans and analysis reports, as well as offers support to the building of skilled workforce and international relations.

Analysis

The Executive Order has done well is recognizing three critical points: that "known but unmitigated vulnerabilities are among the highest cybersecurity risks"[1], that "the executive branch has for too long accepted antiquated and difficult–to-defend IT" [1] and that "effective risk management requires agency heads to lead integrated teams of senior executives with expertise in IT, security, budgeting, acquisition, law, privacy, and human resources." [1]

The recent WannaCry attack on the National Health Services in the United Kingdom are a direct reflection of the first two points. Antiquated Windows XP systems, long retired by Microsoft, were used by the NHS, making it a ready target for the ransomware worm which exploited a known vulnerability.[2]

The third observation above relates directly to best practices in security – that the culture of security starts from the top to effectively permeate through the entire organization or department. The Executive Order further cements this by laying down definite deadlines for heads of agencies and departments to submit reports, create strategies addressing the loopholes and threats, as well as submitting cybersecurity plans. It also explicitly states that these top officials "will be held accountable by the President for implementing risk management measures commensurate with the risk and magnitude of the harm that would result from unauthorized access, use, disclosure, disruption, modification, or destruction of IT and data"[1]

I laud this move and anticipate that it will bring about proactive security measures, rather than reactive ones.

The Executive Order also mandates that "effective immediately, each agency head shall use The Framework for Improving Critical Infrastructure Cybersecurity (the Framework) developed by the National Institute of Standards and Technology, or any successor document, to manage the agency's cybersecurity risk."[1] This is an excellent move as it ensures uniform, consistent security enforcements using the most current best available authoritative framework.

I also appreciate the recognition of the importance, and the support implied, for developing a skilled workforce in anticipation and preparedness for the future. The Executive Order also recognizes the importance of "cyber threat information sharing" and "international cooperation". These points, to me, is a clear indication of a confident leader State, preparing for the future and building allies.

Concerns

The only concern I do have with this well-drafted Executive Order is that it states that "effective immediately", agency heads "shall show preference in their procurement for shared IT services, to the extent permitted by law, including email, cloud, and cybersecurity services." I think mandating this change immediately without investigating the current cloud infrastructure and satisfactorily securing it, could have repercussions.

Conclusion

Though I am in no way near to being an expert of security**,** from my current realm of knowledge and limited experience in the field, I am highly appreciative of the issues, observations, attitude, and mandates that this Executive Order puts forth. It should go a long way in strengthening the cybersecurity of the country.

References

1. Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure. (2017, May 11). Retrieved from https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal
2. Keel, T. (2017, May 18). WannaCry and the NHS Windows XP Estate. Retrieved from https://www.deep-secure.com/blog/wannacry-nhs-windows-xp-estate/