From: Roger Grimes
To: cyberframework
Subject: Comment to CSF 2.0 draft
Date: Tuesday, August 15, 2023 10:13:18 AM

I think CSF 2.0 is a vast improvement in many ways over the previous versions. Kudos to the NIST team.

I have two comments on improvements.

The first has to do with the Awareness and Training controls (PR.AT). The current version takes the previous five PR.AT controls to just two in the current draft version. I actually like the consolidation and wording for the most part. My concern is that social engineering and phishing, which is what PR.AT addresses, is responsible for anywhere between 50% to 90% of all successful breaches. No matter what the percentage is, depending on the survey or report, you won't find another initial root cause involved in more data breaches. Nothing else is even close (although unpatched vulnerable software is usually 2nd). My concern is that by shrinking training coverage to just two sentences, the CSF will unintentionally mask the importance of employee training. I certainly realize that coverage space does not equate to importance and the CSF does spend time discussing risk assessment of controls. But still, I think NIST should strongly consider expanding the space and sentences given to employee training in an effort to get reliers to better understand the importance. This could be done by creating additional controls. Here are some possible PR.AT control candidates:

- Security awareness training should be conducted on a monthly cadence or more frequently.
- Use simulated phishing campaigns as part of the educational process.
- Educational assessments (i.e., quizzes, etc.) should be given to determine who needs more education.
- Ensure senior management demonstrates to employees the importance of completing security awareness training.
- Security awareness training should cover the most topical social engineering and phishing topics that employees are likely to face.
- Hold annual company-wide security awareness training meetings.

I cover this recommendation in an article I wrote: https://www.linkedin.com/pulse/nist-updates-cybersecurity-framework-good-bad-roger-grimes

The second recommendation is that I didn't see Secure By Default, Secure by Design in the CSF draft. This is essentially a movement to get strong, more secure software coded by default. CISA is pushing this in their own Secure By Design program: https://www.cisa.gov/securebydesign. Since unpatched vulnerable software is the second biggest reason for successful breaches (involved in around 33% of all successful breaches according to Mandiant), we need to more to ensure that every developer has the training, tools, and incentive to code more secure software by default.

Please excuse any typos. I'm recovering from a serious illness.

I think NIST is doing a great job and I really like every new document and program coming out of it. Keep up the good work.

Sincerely,

Roger A. Grimes

****

****

*Roger A. Grimes

[redacted]

*Author or co-author of over 1300 computer security articles and 13 books

*Amazon Author Page: amazon.com/author/rogeragrimes

*past weekly InfoWorld and CSO columns: http://www.infoworld.com/blog/security-adviser

*Any opinions expressed are purely mine own and not of my employers

*

*Blatant book plugs:

*A Data-Driven Computer Security Defense (https://www.amazon.com/Data-Driven-Computer-Defense-Should-Using/dp/B0BR9KS3ZF)

*Latest book: Ransomware Protection Playbook (https://www.amazon.com/Ransomware-Protection-Playbook-Roger-Grimes/dp/1119849128)

*Hacking Multifactor Authentication (https://www.amazon.com/Hacking-Multifactor-Authentication-Roger-Grimes/dp/1119650798)

*My quantum book, Cryptography Apocalypse (https://www.amazon.com/Cryptography-Apocalypse-Preparing-Quantum-Computing/dp/1119618193), about quantum computers breaking today's crypto

*Hacking the Hacker, (https://www.amazon.com/Hacking-Hacker-Learn-Experts-Hackers/dp/1119396212/)

****

****