Cutting Through the Cybersecurity Noise

Here's what's important this week: May 17, 2019

Take Action

- Microsoft Windows 7, Windows Server 2008 R2, and Windows Server 2008 users, patch your systems ASAP. The software has a vulnerability that requires ***no user action*** to spread (in other words, the malware that takes advantage of the vulnerability is a worm, not a virus).
  References: https://blogs.technet.microsoft.com/msrc/2019/05/14/prevent-a-worm-by-updating-remote-desktop-services-cve-2019-0708/
  https://www.phoenix.gov/itssite/Documents/everybody-malware-intro.pdf
- Secure your edge devices, like routers, switches, and firewalls, because bad guys are increasingly attacking them (surprise!). The Cyber Threat Alliance has a nice document that explains how.
  Reference: https://www.cyberthreatalliance.org/wp-content/uploads/2019/04/CTA-Network-Edge-Joint-Analysis_Final.pdf

Be Aware

- There's a new set of Intel chip vulnerabilities similar to last year's Spectre and Meltdown. These vulnerabilities are difficult to exploit (attacks have only been seen in labs). So, don't panic, but patch your devices.
  Reference: https://gizmodo.com/what-to-do-about-the-new-intel-chip-flaw-1834759126/amp
- The Business Software Alliance has developed a framework for secure software to identify, assess, and minimize cybersecurity risk throughout the software lifecycle.
  Reference:
  https://www.bsa.org/files/reports/bsa_software_security_framework_web_final.pdf
- NIST released their draft Privacy Framework for review and discussion. This is the companion to their Cybersecurity Framework.
  Reference: https://www.nist.gov/sites/default/files/documents/2019/04/30/nist-privacy-framework-discussion-draft.pdf

Reminders

The Arizona Counter Terrorism Information Center (ACTIC) and Urban Area Security Initiative issue this product to increase Arizona's awareness and cyber resilience. It's up to you to make sure you take the proper steps to secure your networks and devices. Although vendors, products, and/or services may be mentioned, we do not endorse any specific one.

Contact ACTICCybersecurity@AZDPS.GOV with any questions, to provide feedback, or to be added/removed from this distribution. Please note that this email address is not monitored 24x7.

Report potential, suspected, and/or confirmed cyber threats to the ACTIC via:

- https://www.azactic.gov/Tips/
- ACTIC@AZDPS.GOV

- (602) 644-5805 or (877) 2SAVEAZ (272- 8329)

* If links don’t come through, cut and paste all referenced URLs into your browser to access the sites.