The four elevated DoD guidelines you need to know

With each passing month, more organizations are storing more controlled unclassified information (CUI) that could lead to business shut down or reputational risk.

The Department of Defense (DoD) has introduced new standards targeted at helping businesses protect CUI, which includes information that isn't classified but needs to be protected, like engineering drawings, financial information, research data or source codes.

The standards are part of a Cybersecurity Maturity Model Certification program that's required for defense contractors. But the standards offer insights into the evolution that all organizations can implement to improve their cybersecurity maturity.

Steps you can take

DoD standards contain some of the recommendations you'll see anywhere, such as establishing role-based access and limiting admin access.

Here are four elevated DoD guidelines that can help you up the level of your cybersecurity:

Monitoring and alerting: One aspect that has been expanded on in recent years is the use of security information and event monitoring, or SIEM. These systems gather logs from your servers, network devices and other sources to collect evidence that can be beneficial in re-creating the events that lead to compromise. In addition, alerts can be generated to trigger additional reviews of suspicious activity. While this can be done through other methods, a SIEM collects information into a single resource and protects information by restricting who can change or delete information.

Encrypt at rest and in transit: How we communicate with outside resources, such as cloud service providers, should be considered like a conversation in public. Information that is sensitive in nature should be protected. One way that information can be protected is through encryption. While it is a good practice to encrypt information where it is stored, it is also important that encryption (such as Transport Layer Security or TLS) is used to send and receive information. Note that while encryption is important, it's more important that you use current methods of encryption. Older types of encryption often have exposed flaws, which may not make them completely secure. Review any connection that uses encryption and make sure they are using a current encryption.

Limit removable storage: Protect information by treating it as sensitive as information you would lock in a safe. Just as you wouldn't leave a safe door open, you should not allow devices to copy and remove information. This recommendation goes beyond basic encryption by restricting access to what devices have access to copy information that is sensitive in nature.

Use advanced email protections: Protection against spam and malicious links in email has become more common place. Additional protections, such as SPF (Sender Policy Framework), DMARC (Domain-based Message Authentication Reporting & Conformance) and DKIM (DomainKeys Identified Mail) can be implemented to further protect email communications, which are one of the more targeted areas within an organization.

WIPFLI