Server and Network Security Hardening

Server and network security hardening consists of Operating System Hardening, Hardware Hardening, and Application Hardening. My chosen path in information technology is software development and in my opinion this subset of information technology would be more heavily affected by Operating System Hardening, and Application Hardening than the Hardware Hardening, not to say that hardware hardening has no effect on software development or vise versa just that it would have a smaller impact.

Operating system hardening

Operating system hardening is basically applying software and service packs to the whichever operating system that you are running on the server hardware. The concept of Operating system hardening is to close known and unknown security openings within the operating system via patching, removing unnecessary drivers, limiting system access permissions and authenticating that the users that have permissions actually need the permissions, and Encrypting the hard drive or the solid state drive that houses the operating system. Operating system hardening effects software developers in that all of the software that they build will eventually run on an operating system and a hardened system will protect the software from attacks and unauthorized access. We as software developers need to ensure compatibility with the hardened system which might include testing our software on the hardened system, do our best to practice practice secure coding practices to produce software that are resilient to common vulnerabilities and threats, ensure that our software takes advantage of the security features offered by the operating system. And finally test our software to make sure that it will function as predicted within the secure environment.

Application hardening

Application hardening is the process of securing the code of an application to reduce it’s vulnerability to attacks from outside entities. The reason applications hardening is important to the software development of Information Technology is that the applications that are developed are very often targets for bad actors seeking to gain unauthorized access to sensitive data, some good examples of this are SQL injections and cross-site scripting attacks. Developers can use things like static code analysis, dynamic code analysis, and vulnerability scanning to find and eliminate such threats to their applications. It is best if the developer starts looking for vulnerabilities very early on in the development process so there is not a lot of drastic code rework later on in the development cycle to fix vulnerabilities that could have been caught early on.

Hardware hardening

Hardware hardening refers to the process of making computer hardware more resilient to compromise. Mostly this involves increasing the hardware’s physical security through the use of locks, cabinets and other physical impediments to limit a bad actor’s access to the actual hardware. Software developers shouldn’t be all that impacted by hardware hardening unless they need physical access to the device however they can be of assistance in hardware hardening by developing software for specific hardware platforms that have enhanced security features, verifying the updates to hardware firmware are authentic, and ensuring that applications that have the capability to use hardware based authentication use it.

I have no reference for hardware hardening’s effects on software development because when I looked it up there wasn’t a specific article to draw data from. Instead I referenced some of my experience doing physical hardening of various server rooms the Army and made some educated guesses as to what a software developer could help with as far as hardening the physical hardware.

**References**

[https://spectralops.io/blog/os-hardening-for-developers/#:~:text=OS%20Hardening%20(Operating%20System%20Hardening,and%20establishing%20strict%20access%20rules](https://spectralops.io/blog/os-hardening-for-developers/" \l ":~:text=OS Hardening (Operating System Hardening,and establishing strict access rules).

https://www.preemptive.com/application-hardening/