Bryce Jensen
CS-405
2-1 Journal: Defense-in-Depth
9-11-2024

Defense-in-Depth

How deep is too deep, and what's the tradeoff?

The depth of DiD (Defense-in-Depth) layers should be determined by an organization's risk tolerance, requirements, asset value, and resources. However, going "too deep" is possible. They could "add it all," but that might lead to bottlenecks and performance issues in the system, increase the cost, and make the system unusable.

What are some time, money, reputation, and operational considerations?

Time

The initial setup for a "deep" setup can take a lot of time. Research, testing, and deployment are essential considerations. Ongoing maintenance can also be an issue. Each layer will require regular updates, patching, and monitoring, which can be time-consuming. As more layers are added, the response times for detecting and responding to incidents can take longer, as filtering through all the logs and alerts takes more time.

Money

The cost of licensing, hardware, and support can increase as more tools or solutions are deployed. More specialized personnel will be required to manage the system in particularly complex setups, which means higher salaries. Some potential savings arise when the DiD reduces the chance of expensive breaches and data loss; this has the potential to save money in the long run.

Reputation

A deep DiD demonstrates a commitment to security, increasing an organization's security image, which may improve trust with customers and clients. However, failure can potentially happen at any level. Relying too heavily on DiD can create overconfidence in the organization and lead to reputational damage if an attack succeeds.

Operational

Multiple layers can slow down processes or prevent users from accessing the system quickly. They can also cause users to bypass the system, for example, sending a sensitive work-related email through their personal email rather than logging in through the company's extensive login process, potentially putting data at risk. Overly complex systems can have more points of failure, leading to downtime or disruptions. Each layer may need to be adjusted as threats evolve, requiring ongoing operational attention.

Bryce Jensen
CS-405
2-1 Journal: Defense-in-Depth
9-11-2024

What are some additional aspects of DiD that make it unique for each situation?

Smaller companies may focus on fewer but more effective layers, such as solid endpoint protection and firewalls. Larger companies with more assets may have comprehensive DiD strategies involving network segmentation, honeypots, and dedicated security teams.