: Can DSS help avoid hacking?

by Daniel J. Power

Editor, DSSResources.COM

Maybe. One way to explore this question is to examine specific hacking examples and consider if DSS would have helped. The following examples were originally from a news story at BBC News (7/20/2018):

Example 1: Hackers stole personal data in Singapore belonging to some 1.5 million people from a health database. How were systems breached? "It appears that a computer belonging to SingHealth, one of the state's two major government healthcare groups, was infected with malware through which the hackers gained access to the database." Malware comes in many forms: viruses, worms, Trojans, spyware, etc.

Example 2: Germany's government IT network was attacked by hackers targeting the interior ministries' private networks.

Example 3: "Malicious" cyber-attack on Ukraine that spread globally

Example 4: A cyber-attack crippled the UK's National Health Service (NHS) It involved malware known as WannaCry

Example 5: Cyber-attacks on Sony Pictures. According to a report a week after the attack, "Sony employees are still unable to use their old computers due to concerns that code left by the hackers may not have been completely removed from the system. (Peterson, 2014)"

Some anti-virus software includes decision support for the user of a computer systems. For example, Kaspersky notes "Good antivirus protection can also recognize — and warn against — even previously unknown malware threats, based on technical features ... In addition, robust antivirus software detects and warns against suspicious websites, especially those that may be designed for 'phishing'" ... Are alerts enough? When should anti-virus software actually block taking a dangerous action?

: Can DSS help avoid hacking?

Security decision support should focus on three major criteria: availability, integrity and confidentiality. Applying these criteria to guide policies for information security within an organization should reduce and avoid hacking. According to techtarget.com, "confidentiality is a set of rules that limits access to information, integrity is the assurance that the information is trustworthy and accurate, and availability is a guarantee of reliable access to the information by authorized people."

Applying the security criteria triad to evaluate security policies is challenging. Confidentiality should be the easiest criterion to apply, but it can be easy to overlook users who indirectly have access to data. Assuring integrity is an ongoing battle. When data is elicited and captured systems must be designed to ensure accuracy. Once data is stored care should be taken to limit and restrict changes in data values. Finally, the more secure data is the more problems with availability. The greater the availability of data the less secure is the data. Finding policies that optimize all three criteria may still leave gaping holes in an organization's data security profile.

References

Definition, confidentiality, integrity, and availability (CIA triad), at URL https://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA

"Singapore personal data hack hits 1.5m, health authority says," July 20, 2018 at URL https://www.bbc.com/news/world-asia-44900507

Kaspersky, "What is Malware and How to Defend Against It?," at URL https://usa.kaspersky.com/resource-center/preemptive-safety/what-is-malware-and-how-to-protect-against-it

Peterson, A., "The Sony Pictures hack, explained," Washington Post, December 18, 2014 https://www.washingtonpost.com/news/the-switch/wp/2014/12/18/the-sony-pictures-hack-explained

Author: Daniel Power
Last update: 2018-10-15 02:14