NIST guide provides way to tackle cybersecurity incidents with recovery plan, playbook

December 28 2016

"Defense! Defense!" may be the rallying cry from cybersecurity teams working to thwart cybersecurity attacks, but perhaps they should be shouting "Recover! Recover!" instead. Attackers are increasingly racking up points against their targets, so the National Institute of Standards and Technology (NIST) has published the Guide for Cybersecurity Event Recovery to help organizations develop a game plan to contain the opponent and get back on the field quickly.

As the number of cybersecurity incidents climbs, and the variety of types of attacks grows, "It's no longer if you are going to have a cybersecurity event, it is when," said computer scientist Murugiah Souppaya, one of the guide's authors.

For example, the number of companies experiencing ransomware events, in which attackers hold an organization's data hostage until the ransom is paid, have tripled between the first and third quarters of 2016 alone, according to the December 2016 Kaspersky Security Bulletin .

In addition to the overall rise in incidents, the 2015 Cybersecurity Strategy and Information Plan (CSIP), published by the Office of Management and Budget, identified inconsistent cybersecurity response capabilities across the federal government and called for agencies to improve these skills.

The CSIP defines "recover" as developing and implementing plans, processes and procedures to fully restore a system weakened during a cybersecurity event. Recovering may be as simple as restoring data from a backup, but usually it is more involved and the system may be brought back online in stages.

Recovery is a critical piece of the risk management process. Yet no federal policies, standards or guidelines focus specifically on recovering from a cybersecurity incident. And prior to the new report, no one publication has addressed recovery approaches in one place.

NIST computer researchers wrote the Guide for Cybersecurity Event Recovery to consolidate existing NIST recovery guidance such as on incident handling and contingency planning. It also provides a process that each organization—federal or otherwise—can use to create its own comprehensive recovery plan to be ready when a cybersecurity event occurs.

The publication supplies tactical and strategic guidance for developing, testing and improving recovery plans, and calls for organizations to create a specific playbook for each possible cybersecurity incident. The guide provides examples of playbooks to handle data breaches and ransomware.

This document also provides additional information related to the "Recover" function in the Framework for Improving Critical Infrastructure Cybersecurity, more commonly known as the Cybersecurity Framework.

"To be successful, each organization needs to develop its own plan and playbooks in advance," said Souppaya. "Then they should run the plays with tabletop exercises, work within their team to understand its level of preparation and repeat."

Provided by National Institute of Standards and Technology