PUBLICATION

State AGs Data Breach Settlement Reinforces the Importance of Patch Management

August 22, 2017

A recent settlement between Nationwide Mutual Insurance Company and attorneys general from 32 states and the District of Columbia (the "Attorneys General") over a 2012 data breach reinforces the importance of patch management.

On August 9, 2017, the Attorneys General and Nationwide, on behalf of itself and its wholly-owned subsidiary, Allied Property & Casualty Insurance Company (collectively, "Nationwide"), entered into an Assurance of Voluntary Compliance that requires Nationwide to, among other things, pay $5.5 million to the Attorneys General. The settlement is in response to an October 3, 2012 data breach experienced by Nationwide that resulted in the loss of sensitive personal information for 1.27 million consumers. The breach affected potential customers who were seeking insurance quotes from Nationwide. The sensitive personal information included driver's license numbers, Social Security numbers, and Nationwide internal credit-related scores.

The 2012 data breach was alleged to be the result of Nationwide's failure to apply a critical security patch that led to hackers exploiting a vulnerability in Nationwide's web hosting software. After the breach occurred, Nationwide addressed the software vulnerability by applying the previously unapplied software patch. Nationwide admits it experienced a data breach, but denies any wrongdoing related to the breach. Shortly after the data breach occurred, Nationwide notified the affected consumers and offered free credit monitoring and $1 million of free identity theft insurance coverage with no deductible.

In addition to the $5.5 million payment, the settlement – titled as an "Assurance of Voluntary Compliance" – requires Nationwide to complete additional tasks, which may or may not have already been completed, such as:

- Maintaining an online disclosure statement informing potential customers that it retains a consumer's personal information even if the consumer does not become an insured
- For a period of three years:
  - Appoint an individual to the role of Patch Policy Supervisor to maintain, review and revise Nationwide's patch management policies and procedures
  - Appoint an individual to the role of Patch Supervisor to monitor and manage the installation of available patches
  - Maintain and, on at least a semi-annual basis, update an inventory of all covered systems
  - Regularly review and update its Incident Management Policy and Procedures
  - Deploy and maintain a system management tool to identify available patches on a near real-time basis and scan covered systems to identify unapplied patches
  - Implement processes and procedures to notify Nationwide's patch management personnel about available patches
  - Implement processes and procedures to evaluate the severity of available patches and prioritize any responsive mitigation actions, and document in writing the applicable risk severity and actions taken

  - Purchase and install an automated feed of common vulnerabilities to Nationwide's intrusion detection/intrusion prevention systems and security information and event management technology
  - On at least a semi-annual basis, perform an internal patch management assessment of its covered systems
  - On at least an annual basis, hire an outside, independent provider to perform a patch management audit of its covered systems
- One year after the settlement, certify to the Attorneys General that it is in compliance with these requirements

All organizations that collect personal information from consumers should take heed of the requirements set forth in the Nationwide settlement. These requirements reinforce the importance of implementing an effective patch management program. Failure to apply critical security patches can not only lead to data breaches, but can also make organizations vulnerable to ransomware attacks (as seen by the recent WannaCry ransomware attacks on systems that had not applied an available Microsoft security patch).

If you have any questions or concerns about your organization's patch management program, or other data privacy and cybersecurity questions, please reach out to Bill O'Connor, CISSP, CIPP/US, or any member of Baker Donelson's Data Protection, Privacy and Cybersecurity Team, and we will be happy to assist.