Report in Brief

AUGUST 26, 2016

Background

In early September 2014, NOAA experienced a significant cyber attack. An attacker exploited vulnerabilities in Internet accessible web applications and eventually compromised important internal NOAA systems operated by the National Environmental Satellite, Data, and Information Service (NESDIS). NESDIS is responsible for providing global environmental data from satellites and other sources to promote, protect, and enhance the nation's economy, security, environment, and quality of life.

The attacker compromised three NESDIS systems and gained complete control of system components within one of them. The attacker was also able to use usernames and passwords gathered from one of these systems to obtain unauthorized access to another three NOAA systems.

Why We Did This Review

We conducted this audit to (1) determine the significant factors that contributed to the successful cyber attack on NOAA information systems and (2) evaluate NOAA's handling of the detection, analysis, eradication, and reporting of the attack, as well as recovery from it.

NATIONAL OCEANIC AND ATMOSPHERIC ADMINISTRATION

Successful Cyber Attack Highlights Longstanding Deficiencies in NOAA's IT Security Program

OIG-16-043-A

WHAT WE FOUND

Regarding our first objective, we found that NESDIS systems were vulnerable because the office had not addressed weaknesses in the information security practices applied to the compromised system components. Specifically, we found that (1) deficiencies in risk management left an application exposed to attack, (2) practices for detecting web application vulnerabilities were inadequate, and (3) the attacker obtained unauthorized access to additional systems because NOAA deferred implementation of additional access controls which had been required since 2006.

We limited our review of the second objective to NOAA's containment and recovery efforts, specifically focusing on the issues that prolonged the disruption of disseminating weather satellite data. We focused on these issues because they resulted in the greatest impact to NESDIS operations. We found that inadequate firewall management practices prolonged the disruption.

WHAT WE RECOMMEND

We recommend that NESDIS' Assistant Administrator do the following:

1. Improve risk management practices to reduce the exposure of web application vulnerabilities when decisions are made to not remediate known issues.
2. Formally review Internet exposed web applications and determine if access from the Internet is justified.
3. Deploy the specialized web application vulnerability scanning tool and an updated assessment process that requires more than one assessment tool; especially on web applications.
4. Ensure that all web applications are scanned for vulnerabilities on a quarterly basis.
5. Ensure that the same methodology used to identify a vulnerability is also used to validate its remediation.
6. Establish and implement procedures to periodically review firewall rules.
7. Develop an improved practice for managing plans of action and milestones (POA&Ms) to ensure that evidence showing actual remediation of a weakness identified in the POA&M is submitted, reviewed, and approved before the POA&M is closed.

We recommend that NOAA's Chief Information Officer do the following:

8. Ensure that adequate measures are taken to implement mechanisms for multifactor authentication in a timely manner for all applicable users and applications.