the Availability Digest

www.availabilitydigest.com
@availabilitydig

The Government OPM Hack Gets Worse

July 2015

In our June 2015 issue of the *Availability Digest*, "A Massive Hack on the U.S. Government"[1] said, "Starting in mid-2014, a sophisticated cyberattack began siphoning sensitive personal information from the computers of the U.S. Government's Office of Personnel Management (OPM). By the time the attack was discovered one year later, analysts estimated that the personal information of an estimated 4 million current and former federal employees had been compromised."

That number was a huge understatement. After further investigation by the U.S. Government, the people whose personal information was stolen numbers 21.2 million!

Not One, But Two Attacks

It turns out that there were two hacking attacks. They began in early 2014 when hackers infiltrated the systems of government contractor KeyPoint Government Solutions and stole employee credentials. KeyPoint's responsibility was to carry out background checks on potential government employees.

One set of hacked databases was the OPM repository of security clearance files. They included every security clearance application submitted since the year 2000. The data is submitted via the SF86 form, a 120-page application submitted by anyone seeking a government security clearance. The stolen data includes sensitive information on virtually every aspect of peoples' personal histories, including financial records, outstanding debt, gambling addictions, drug use, alcoholism, arrests, psychological and emotional health, foreign travel, foreign contacts, and an extensive list of relatives and friends. The attackers were active in these databases until January, 2015.

The attackers also hacked databases with personnel records. They were active in these databases until April 2015 when the attacks were discovered by the OPM. Information compromised included Social Security numbers, job assignments, and performance evaluations. About 4.2 million people were affected by the breach. This is the original number that was reported by the OPM.

By the time the OPM concluded its damage assessment, it discovered that the majority of those affected were those who had entries in the OPM repository of security clearance files. Eliminating duplicates of people who had information in both sets of databases, the government determined that the information of 21.2 million people was compromised. These victims include not only those who are working for, have worked for, or have tried to work for the U.S. government but also their family and friends who had been listed as references.

The hackers had access to OPM for more than a year. It was only while the OPM was installing advanced cybersecurity defenses in April 2015 that the attacks were discovered and disabled.

[1] A Massive Hack on the U.S. Government, *Availability Digest*; June 2015.
http://www.availabilitydigest.com/public_articles/1006/OPM_attack.pdf

Notification is Lagging

The OPM is offering a “comprehensive suite of monitoring and protection services” to those impacted. Services include three years of credit monitoring and other identity-protection options.

The OPM also is setting up a new system to inform victims of the security breach. So far, most of the 4.2 million people exposed in the one hacking attack have been notified. However, it may take weeks to get the notification system working before the other 18 million people are notified. OPM is facing rising anger from the federal employee unions, which are claiming that they have received scant information about the breaches.

Up to this time, there has been no indication to suggest any misuse of the stolen information. However, not much time has passed.

OPM Director Resigns

Under pressure from members of Congress to step down, Katherine Archuleta, the Director of OPM, resigned. She offered her resignation of her own volition and not because she was asked for it. The pressure for her to leave was in spite of the fact that the attacks were discovered as a result of the strategic cybersecurity plan she put in place in November 2014, shortly after she became Director.

Summary

A major security problem that OPM faces is that its databases are stored on forty-seven different servers, some operated by OPM and others operated by contractors. The servers are old and applications are written in old languages such as COBOL. Upgrading these systems is next to impossible, but replacing them could take years. Congress has yet to authorize any funds for such replacements.

However, even if all systems were upgraded, hackers continue to prove that they are smarter than us. Systems will continue to be hacked and data stolen. The only certain defense (well, almost certain) is to make the data useless to an attacker. Encryption must be used for all data-in-place and in-motion.

Acknowledgements

Material for this article was taken from the following sources:

22 Million Affected by OPM Hack, Officials Say, *ABC News*; July 9, 2015.
Hacks of OPM databases compromised 22.1 million people, federal authorities say, *Washington Post*; July 9, 2015.
US Personnel Chief Resigns in Wake of Massive Data Breach, *Continuity Insights*; July 10, 2015.
OPM Hack: US Has Not Notified 21.5 Million Victims of Massive Data Breach, *IB Times*; July 15, 2015.