Cyber Security Lessons from the U.S OPM Breach

claws.in/1410/cyber-security-lessons-from-the-us-opm-breach-monish-gulati.html

Abstract : *U.S. Office of Personnel Management(OPM), the human resources department for the US federal government, announced on 04 June that personal data of some 4.1 million current and former US federal employees had been exposed during a cyber-security breach that began last year but wasn't detected until 15 April 2015. The incident holds a host of lessons on cyber-security and management of digital data. This article culls out some such lessons relevant at the organisation level.*

US Office of Personnel Management (OPM) announced on 04 June 2015 that personal data of some 4.1 million current and former US federal employees (civilian agency and military employees) had been exposed during a cyber-security breach that began the preceding year but wasn't detected until 15 April 2015. The OPM is the human resources department for the US federal government and does checks for security clearances.

The detection of the breach in April pointed to the compromise of a personnel database containing Social Security numbers and other personal information. During further investigation into the cyber breach at the OPM, investigators on 08 June became aware of the possibility of a separate intrusion affecting a different set of OPM systems and data. This breach potentially compromised sensitive and personal information of employees working at the CIA, the National Security Agency, and the Pentagon.

Some analysts felt that the data breach could yield a "virtual phonebook" of US intelligence assets around the world and a list of these individuals' vulnerabilities including details of their family members. There is a view that the repercussions could be far devastating than the Snowden leaks. Investigators found solace in the fact that OPM records did not detail specific covert identities, missions or operations.

The investigation into the cyber-security breach is still on-going, including into the modus of the hackers and the extent of security damage. The details available at this preliminary stage hold a host of lessons on cyber-security and management of digital data. This article culls out some such lessons relevant at the organisation level.

The Intrusion and Response

Some investigators believe hackers first breached the OPM's networks as far back as late 2013, during which hackers made off with IT system manuals that, officials say, could have provided a blueprint of sorts into OPM's networks and laid the groundwork for future hacks.

Malware was discovered in an OPM sever that connected to the security clearance database. It was a never-before-seen variant known as PlugX. This led to the theft of login and password data for an employee of an OPM contractor, KeyPoint Government Solutions, sometime before October 2014.

Since both incidents were identified, OPM has partnered with the US Department of Homeland Security's Computer Emergency Readiness Team (US-CERT), and the Federal Bureau of Investigation (FBI) to investigate and determine the full impact of the incident.

The White House subsequently directed all US federal agencies to take a series of swift measures to lock down government systems. The US Chief Information Officer launched what officials are calling a 30-day cyber-security "sprint" which included the creation of a new task force, the "Cyber-security Sprint Team," to lead a month-long review of the US government's security hygiene practices.

Causes & Lessons

OPM had been hacked before, yet there appeared to be few follow-ups and lessons learnt. The Inspector General had told the OPM about their material weaknesses but nothing at all was apparently done. They did not employ basic authentication techniques and did not regularly scan for vulnerabilities in the system. 11 major systems out of OPM's inventory of 47, had not been certified as secure, yet they continued operating resulting in 65 percent of OPM's data being stored on those uncertified systems. Some of the causes and lessons are listed in succeeding paragraphs.

Lack of Emphasis on Cyber-security. This led to findings; one, there seemed to be a lack of experience in its personnel. There was no IT security staff until 2013. Most of IT was operated by contractors, whose contracts had expired, and; two, OPM apparently wasn't sure of what they had in their own network. According to The New York Times the OPM did not possess a comprehensive inventory of servers, databases and network devices. Apparently the hackers knew this network better than the people that operated it.

Upgrading of Hardware. The legacy systems had not been adequately protected or upgraded. Some experts suggested that the OPM should have encrypted the data in its database. However an OPM official revealed that was not feasible as the network was too old. Some of them were over 20 years old and written in COBOL, and they could not easily be upgraded or replaced. These systems would be difficult to update to include encryption or multi-factor authentication because of their aging code base, and would require a full rewrite.

Employment of External Personnel. Besides contractual issues some of the contractors that have helped OPM with managing internal data had security issues of their own—including potentially giving foreign governments direct access to data.

Zero-day Attacks. US federal networks are protected by a number of tools, the most robust being Homeland Security's Einstein program, a government-wide firewall designed to detect and, in its latest iteration block known security threats. However, as with most cyber-security solutions of its type, Einstein cannot protect against zero-day attacks or simply, methods not seen before. Some experts felt that the third version of the program — Einstein 3 Accelerated (E3A) — would have been effective, however it had not been deployed at OPM.

Coordination and Collaboration. Sharing information of cyber-attacks is the biggest weapon in the cyber-security war. Therefore it was not surprising that in February, US President Obama issued an executive order calling for the creation of Information Sharing and Analysis Organizations (ISAOs) to act as conduits between government and industry. By sharing threat information, the public and private sectors would work together to expose attackers and their methods, improving everyone's security posture.

Conclusion

Encryption or any other countermeasure may not have been effective in the OPM case because the attackers had gained valid user credentials to the systems that they attacked; possibly through social engineering. And because of the lack of multifactor (more than one method) authentication on these systems, the attackers would then have been able to use these credentials at will to access systems from within and potentially even from outside the network. The continuing weakness in OPM information security results directly from inadequate governance, a lack of leadership, policy, and guidance.

Finally cyber-security programmes are designed to lower risk; no matter how good security is or what SOPs are put in place, there is still that element of chance which can subject them to failure.

Monish Gulati is an independent defence analyst based in New Delhi. Views expressed are personal.

Research Area
Defence Technology including Cyber and Space