SANS Institute
InfoSec Reading Room

OPM vs. APT: How Proper Implementation of Key Controls Could Have Prevented a Disaster

Advanced Persistent Threat (APT) has been a leading buzz phrase in the security industry for most of the past decade. In some cases breached organizations have attempted to deflect attention away from their inadequate security by saying, in essence, the attack was APT we could not have defended ourselves. In April of 2015 the U.S. Office of Personnel Management detected a breach of its systems that would ultimately be determined to have exposed the personal information of up to 25.7 million people. While APT style...

OPM vs. APT: How Proper Implementation of Key Controls Could Have Prevented a Disaster

GIAC (GSEC) Gold Certification

Author: David Kennel, dakennel@gmail.com
Advisor: Chris Walker
Accepted: March 10, 2016

Abstract

Advanced Persistent Threat (APT) has been a leading buzz phrase in the security industry for most of the past decade. In some cases breached organizations have attempted to deflect attention away from their inadequate security by saying, in essence, the attack was APT we could not have defended ourselves. In April of 2015 the U.S. Office of Personnel Management detected a breach of its systems that would ultimately be determined to have exposed the personal information of up to 25.7 million people. While APT style attackers are very difficult to defend against not all of their attacks are as advanced as one might think. The OPM attack could have been defended against with existing tools and techniques documented in the Top 20 Critical Security Controls and in NIST 800-53. In particular two factor authentication and effective logging and activity analysis would have made the attack more difficult to perpetrate successfully.

1. Introduction

On June 4th, 2015 U. S. Government officials announced a breach of data at the Office of Personnel Management (OPM). The initial statement indicated that personally identifiable information on 4.2 million current and former government employees was exposed. On June 12th a second breach was detected. By July 9th the total number of exposed records had risen to 25.7 million (Bisson, 2015), and included the loss of 5.6 million peoples fingerprints (Williams, 2015). OPM has taken steps to contact the affected people and establish identity theft protections for them (OPM). On the surface this is similar to any of a number of breaches of identity information that have occurred. However, OPM hosts data of a distinctly different character than what is exposed in most identity breaches.

1.1 What was stolen and who wants it

The OPM is the government agency in charge of managing 90% of the background investigations for clearance seeking government employees and contractors (Levine 2015). Candidates for a security clearance are required to complete and submit SF-86, the "Questionnaire for National Security Positions". SF-86 is a 127 page form that collects information on residence history, friends and family, employment history, the applicants police record, drug use (alcohol and illegal), mental health, military history, and finances. This information, and other findings from the investigation are stored in a suite of applications known as "EPIC" (Gallagher, 2015).

Since the information contains Social Security Numbers and information on family members (mother's maiden name is a common authenticator that could be gleaned from this data), it is definitely something that would be of interest to traditional criminals participating in the identity fraud supply chain. The depth of information and the fact that this is data concerning people who hold security clearances suggests that the actor may have been a foreign intelligence service, frequently referred to as an Advanced Persistent Threat (APT).

An unusual piece of data that was stolen during the attack was a cache of 5.6 million sets of fingerprints. The Office of Personnel Management in their statement correcting the number of stolen fingerprints downplayed the risk stating, "Federal experts

believe that, as of now, the ability to misuse fingerprint data is limited" (OPM, 2015). Direct abuse is possible, Mythbusters famously proved that in some cases the security of fingerprint locks could be defeated (Discovery Channel, n.d.). Many believe that the theft of fingerprints was less about defeating single factor finger print locks, e.g. many cell phones, and more about espionage type uses including identifying undercover operatives or planting false identities (Roeder, 2015).

Attribution of an attack is often a difficult thing. Attackers will route traffic through compromised or legitimate looking systems to hide their tracks. DNS registrations for command and control systems are usually done under false names with one-time use email addresses. However, it was not long after the OPM breach that China was named as a suspect by multiple U.S. Government personnel including Director of National Intelligence James Clapper (Pepitone, 2015). ThreatConnect and FireEye also identified China as the likely perpetrator, naming a specific group of actors known as "Deep Panda" (ThreatConnect) (Hesseldahl, 2015).

The loss of the OPM data to a foreign intelligence service is a major issue. William Evanina, the Office of the Director of National Intelligence's National Counterintelligence Executive, was quoted as saying that analysis of the leaked data would allow a foreign government to determine, "who is an intelligence officer, who travels where, when, who's got financial difficulties, who's got medical issues, [to] put together a common picture" (Bennett & Hennigan, 2015).

Threatconnect asserts links between the OPM breaches and breaches of USIS (a contractor to OPM), Wellpoint/Anthem, Premera, Empire and CareFirst (all Blue Cross/Blue Shield companies providing services to Federal employees and contractors) (Threatconnect). That data, combined with the OPM breach data and open source information can yield a startlingly complete picture of an individual's life. This data would be extremely beneficial in attempting to recruit personnel with clearances for intelligence activities. Peter W. Singer, a Strategist and Senior Fellow at the New America Foundation, put his finger on the data correlation problem while talking with the L.A. Times; "A foreign spy agency now has the ability to cross-check who has a security clearance, via the OPM breach, with who was cheating on their wife via the Ashley

Madison breach, and thus identify someone to target for blackmail" (Bennett & Hennigan, 2015).

1.2 The Federal Cybersecurity Framework

The OPM breach did not happen because the agency did not know, or had not been told, how to secure their systems. Like all Federal agencies they are expected to comply with a comprehensive set of computer security controls. They were also routinely audited for the state of compliance with these controls.

1.2.1 FISMA

The Federal Information Security Management Act (FISMA) is a Federal Law enacted in 2002 and later enhanced by the Federal Information Security Modernization Act of 2014. The intent of the act is to "provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets" (Federal Information Security Management Act, 2002) (Federal Information Security Modernization Act, 2014). FISMA delegates to the National Institute of Standards and Technology (NIST) the role of developing standards and guidelines for securing Federal information systems (Federal Information Security Modernization Act of 2014 44 U.S.C. § 3553). The FISMA acts also require annual assessments of agency security programs by an independent auditor.

1.2.2 FIPS 199, FIPS 200 & NIST SP 800-53

FIPS 199 and NIST SP 800-53 are two of the most important documents generated by NIST. FIPS 199, Standards for Security Categorization of Federal Information and Information Systems, lays out a framework for categorizing data and systems based around the three key principles of computer security; confidentiality, integrity and availability. In the FIPS 199 framework for the data or system in question each of the three principles is assessed as to whether the consequences of compromise of that principle is low, moderate, or high. The framework uses a simple high water mark method that says that the control selection should be based on the highest concern answer (NIST, 2004). E.G. The system that the social security system uses to dispatch payments to beneficiaries might be assessed as follows: Confidentiality – Moderate, based on the fact that exposure of the data could have serious, but not life threatening impacts on

beneficiaries. Integrity – High, based on the fact that alteration of the data could have severe impacts on the social security system and/or beneficiaries up to and including life threatening (inability to pay the heating bill during the winter). Availability – High, based on the fact that a stoppage in payments to beneficiaries could have severe impacts up to and including life threatening (heating bills). Given an assessment of Moderate, High, High, that system would then be considered a High security category.

FIPS 200 Minimum Security Requirements for Federal Information and Information Systems delineates seventeen security areas that are expected to be the core of agency information security plans. After defining the 17 areas FIPS 200 then refers to SP800-53, Security and Privacy Controls for Federal Information Systems and Organizations, for details on the 17 control areas (NIST, 2006). Federal agencies and contractors are expected to then select and implement security controls from SP 800-53 that are specified for the security category of their system. SP 800-53 specifies controls, and control enhancements, covering everything from Access Control to System Integrity. The control set includes policy and administrative controls on down to fairly specific technical controls. 800-53 also covers a risk management framework, the concept of compensating controls, guidance for handling external service providers, trustworthiness, tailoring controls, and legacy systems (NIST, 2014).

A typical control from the 800-53 control catalog looks like this:

AC-12 SESSION TERMINATION

Control: The information system automatically terminates a user session after [Assignment: organization-defined conditions or trigger events requiring session disconnect].

Supplemental Guidance: This control addresses the termination of user-initiated logical sessions in contrast to SC-10 which addresses the termination of network connections that are associated with communications sessions (i.e., network disconnect). A logical session (for local, network, and remote access) is initiated whenever a user (or process acting on behalf of a user) accesses an organizational information system. Such user sessions can be terminated (and thus terminate user access) without terminating network sessions. Session termination terminates all processes associated with a user's logical

session except those processes that are specifically created by the user (i.e., session owner) to continue after the session is terminated. Conditions or trigger events requiring automatic session termination can include, for example, organization-defined periods of user inactivity, targeted responses to certain types of incidents, time-of-day restrictions on information system use. Related controls: SC-10, SC-23.

Control Enhancements:

(1) SESSION TERMINATION | USER - INITIATED LOGOUTS / MESSAGE DISPLAYS

The information system:

(a) Provides a logout capability for user-initiated communications sessions whenever authentication is used to gain access to [Assignment: organization-defined information resources]; and

(b) Displays an explicit logout message to users indicating the reliable termination of authenticated communications sessions.

Supplemental Guidance: Information resources to which users gain access via authentication include, for example, local workstations, databases, and password-protected websites/web-based services. Logout messages for web page access, for example, can be displayed after authenticated sessions have been terminated. However, for some types of interactive sessions including, for example, file transfer protocol (FTP) sessions, information systems typically send logout messages as final messages prior to terminating sessions.

References: None.

Priority and Baseline Allocation:

P2 LOW Not Selected MOD AC-12 HIGH AC-12

After controls have been selected and implemented the NIST 800-53 risk management framework states that the controls should be assessed to ensure the controls are working as designed. The expected process for new systems is to be assessed prior to being granted Authorization to Operate (ATO). Then every three years systems are expected to

be retested in order to maintain ATO. This process is spelled out in the Office of Management and Budget memorandum known as Circular No. A-130 Revised (NIST, 2014, April 1).

1.3 The State of OPM Systems

Per FISMA requirements each agency has an annual assessment of its security program by an independent auditor. Usually these are performed by the agency's Inspector General's office. OPM was audited in 2014 and the report is publicly available. The FY 2014 version of the report is referenced here because the 2015 version was completed after the breaches were discovered and the OPM had started taking remedial actions, thus the FY 14 version is likely to be more representative of the environment that the attackers faced.

The FY 14 report on the FISMA audit of the OPM makes for some grim reading. The fact that eleven major information systems at the OPM were operating without valid authorization was cited as a "material weakness in the internal control structure of OPM's IT security program" (U.S. Office of Personnel Management Office of the Inspector General Office of Audits, 2014, p. I). The Inspector General also noted weaknesses in:

- Security governance
- Security monitoring
- Execution and management of Plans of Action and Milestones (POA&M)
- Deployment of multi-factor authentication
- Inventory of systems and vulnerability scanning
- Configuration management

As damning as that is there is an admittance of incompleteness in the Inspector General's report, "In conducting our audit, we relied to varying degrees on computer-generated data provided by OPM. Due to time constraints, we did not verify the reliability of the data generated by the various information systems involved. "(U.S. Office of Personnel Management Office Of The Inspector General Office Of Audits,

2014, p. 3). The indications of time constraints and unquestioned reliance on data provided by OPM suggests that things could have been worse than the report indicates.

2. The Breaches

Like most breaches of federal organizations, details on the OPM breach are hard to come by. It is likely that much of the detailed information will remain classified. What is known is that on June 4 OPM announced the discovery of a breach of OPM systems maintained at the Department of the Interior's shared-services data center (Bisson, 2015)(ICIT, 2015). This breach was estimated to have exposed 4.2 million records of personally identifiable information (PII). This initial breach is believed to have started in December of 2014. News was released on June 12, 2015 that the investigators had discovered a second, larger, breach dating to March of 2014 (ICIT, 2015)(Bisson, 2015). In this second breach attackers stole 21.5 million SF-86 forms (ICIT, 2015). The two breaches also resulted in the loss of 5.6 million individuals fingerprints (Koren, 2015).

Ars Technica reported that the attack leveraged a malware package, probably delivered via a “phishing” attack that was able to install on a system on OPM's internal network and establish a channel for further access. The attackers were able to elevate their access on OPM systems to the point where they could access a large portion of OPM's data (Gallagher, 2015). During Senate committee hearing OPM Director Katherine Archuleta testified that attackers used a legitimate credential stolen in an earlier breach of OPM contractor KeyPoint Government Solutions (Boyd, 2015).

Threatconnect's analysis of the breach pointed to actors who routinely use malcode from the Sakula malware family. Their analysis also suggested that a malicious program named PlugX was used (Threatconnect, 2015). Sanjay Tandon, founder and CEO of Paramount Defenses Inc. and former program manager for Active Directory security at Microsoft, speculated that the attackers targeted an Active Directory administrator account using either the pass-the-hash or reset-the-password technique (Tandon, 2015).

2.1 Was this an isolated event?

In short, no, it was not. OPM suffered a breach in 2013 where attackers stole data on network assets and systems. US Investigations Services, USIS, a subcontractor to OPM, detected a breach of its systems in August 2014, as a result OPM terminated their relationship with USIS. Keypoint, also an OPM subcontractor, disclosed a breach of their systems in December of 2014 (Institute for Critical Infrastructure Technology, 2015). In February 2015 Anthem Inc. a health insurance giant reported a breach of its systems. In this case attackers targeted PII data on members and state actors from China the leading suspects (Krebs, 2015). In March 2015 Premera Blue Cross would be breached with indicators pointing to China and PII data pilfered (Krebs, 2015). Both Anthem and Premera are leading insurance providers to federal employees and contractors. Threatconnect believes that all of this activity was related based on a variety of tradecraft indicators. They also called out a 2014 report by Novetta "Operation SMN: Axiom Threat Actor Group Report" that had predicted attacks against agencies responsible for personnel management (Threatconnect, 2015). Clearly there was a pattern of activity that should have had personnel at OPM on high alert for cyber-attack activity.

2.2 Control Failure

It is safe to say that much of the data held by OPM fell into the Moderate and High categories using the methodology discussed in FIPS 199. Looking at the attack pattern, the attack results and the controls in NIST 800-53 that are selected for those categories of data, it's clear that there were a number of instances where if the control had been fully implemented, or had been implemented with security as opposed to compliance in mind, the attack would not have succeeded or, at minimum, would have faced far more significant hurdles than it did.

Control IA-2, Identification and Authentication (organizational users), with enhancements 1, 2, 3, 8, 11 and 12 as selected for Moderate systems requires two factor authentication for all accounts. The preferred two factor authentication source is the Personal Identical Verification smart card which is also required by OMB Memorandum 11-11. While OMB did have good deployment of PIV card use across its workstations use of the PIV was not required for access to systems. In particular none of OMB's major

systems required use of the PIV or other two factor authentication mechanisms (U.S. Office of Personnel Management Office Of The Inspector General Office Of Audits, 2014, p. 24). Had this control been in place it would have erected a serious barrier to lateral movement and further exploitation of the network. If the attackers had acquired a set of credentials from KeyPoint this control could have rendered that credential useless. Without credentials that could be trivially replayed or reset the attackers would have had to resort to other, possibly slower and noisier, ways to move through the network. This would have given defenders additional opportunities to detect and block the traffic before the attackers' objectives could be realized.

For those more familiar with the Center for Internet Security's (CIS) Critical Security Controls list, NIST's IA-2 control maps to Critical Security Control #5 Controlled use of administrative privilege. The requirement for multi-factor authentication appears in Critical Security Control 5.6 (CIS 2015).

On 5 January 2014 Dr. Eric Cole tweeted, "Dr. Cole's motto for 2014 is "Prevention is Ideal but Detection is a MUST"; Detection is going to be the KEY to success: Outbound Detection" (Cole, 2014). According to FireEye's M-Trends report the median average number of days that intruders were in a network before discovery has been improving; 205 days in 2014, 229 days in 2013, and 243 days in 2012 (Kerner, 2015). Unfortunately according to the Verizon 2015 Data Breach Investigations Report their charting of the time that attackers need to breach a victim as compared to the percentage of attacks detected in that same time window shows that while attacks are trending longer, defenders are getting less effective at discovering them quickly (Verizon, 2015). OPM's detection of the breaches of its systems was 7 months for the first detected breach and 15 months for the second detected breach. The first is close to the median average documented by FireEye, the second is well beyond the average.

SP 800-53 has quite a bit to say about auditing and logging with an entire control family, AU, dedicated to the topic. The recommended controls for moderate systems in the AU family require an organization to define an auditing policy, define events that need to be audited, requires that the content of audit records have sufficient information to establish what occurred, ensure synchronized time stamps, and use automated

processes to review, analyze, and report on audit records (NIST, 2014). One of the challenges and opportunities of this particular control family is that it leaves a lot of specifics up to the organization to define. The challenge being to not fall into the trap of defining the minimum that the auditors will let you get away with, the check the box response. The opportunity here is to define an auditing and logging program that provides ample, meaningful, information to detect malicious activity.

The Inspector General report called out weaknesses in the OPM's logging and response mechanisms. The finding included the following telling items: Only 80% of major OPM systems were forwarding their logs to OPM's security information and event management (SIEM) system. Systems that were logging to the SIEM systems were not tuned well and were sending a large volume of data that was resulting in a high false positive rate. This led to a backlog in responding to SIEM alerts (U.S. Office of Personnel Management Office of the Inspector General Office of Audits, 2014). Clearly OPM's ability to understand what was happening on its networks was deficient.

The NIST 800-53 AU control family maps to the CIS Critical Security Control #6 Maintenance, monitoring and analysis of audit logs. Like 800-53 the Critical Security Controls require time synchronization, regular log analysis and use of a SIEM tool to identify anomalies (CIS 2015).

NIST SP 800-53 contains an entire control family on risk assessment, RA. While risk assessment is one of the shorter control families, RA-1 through RA-5 cover some important ground including; risk assessment policy, security categorization, risk assessment, and vulnerability scanning. The Inspector General's (IG) report, while it did give passing grades for some elements of OPM risk management process, noted deficiencies in security governance including the following missing elements; "conducting a risk assessment, maintaining a risk registry, and communicating the agency-wide risks down to the system owners." (U.S. Office of Personnel Management Office of the Inspector General Office of Audits, 2014). The report also cites weaknesses in the OPM's vulnerability scanning, noting that they could not verify that scans had been routinely conducted and weaknesses for server systems were not documented. The IG also came down hard on OPM for failures in OPM's authorization process that allowed

11 systems that were due for re-authorization to continue to operate after their authorizations expired. The report cited this issue as a material weakness. Issues managing risk are particularly problematic because they result in cascading weaknesses in security posture. Systems that have not been correctly categorized or assessed for risk may not have security controls applied that are commensurate with the risk the system poses if breached.

The NIST 800-53 RA control family maps to several different points in the CIS Critical Security Controls: RA-5 Vulnerability Scanning maps to Critical Security Control # 3 Secure Configurations for Hardware and Software, #4 Continuous Vulnerability Assessment and Remediation and #7 Email and Web Browser Protections. RA-2 Security Categorization maps to Critical Security Control #14 Controlled Access Based on Need to Know. RA-6 Technical Surveillance Countermeasures Survey maps to Critical Security Control #20 Penetration Tests and Red Team Exercises (CIS 2015).

The overall picture painted by the Inspector General's report is not one of a well-managed security program. Failures in vulnerability scanning and re-authorization of systems would indicate that OPM did not have an accurate picture of the security posture and risk level of its major systems.

3. Key Controls for Prevention/Detection

In order to prevent a repeat of these breaches the OPM computer security program needs to turn some of its key weaknesses into strengths. Correcting the deficiencies in their risk management program, fully deploying strong multi-factor authentication, and building a robust auditing program are essential steps that need to be taken to shore up security at OPM and contain valuable lessons for other organizations as well.

3.1 Multi-factor authentication

Reusable passwords are broken. The computer security industry has known this for over two decades (Swaby, 2012). Reusable passwords can be guessed, brute forced, shoulder surfed, and stolen via keystroke logging. Once compromised a user name password combo can be used until the password is changed. Furthermore passwords play into a variety of human weaknesses; we can't remember long, complex passwords that are

unique for every single system that we touch, which means that passwords are shared between systems, weak and easy to remember, or both. Password loss and reset is a serious workload for help desks and automated reset mechanisms carry the potential for abuse.

Replacing reusable passwords with strong multi-factor authentication is a tremendous boost to system security. An attacker with a legitimate credential looks just like an authorized user to system access controls. By using multi-factor authentication, something you have, plus something you know and/or something you are (a biometric, fingerprint, voice, iris, etc.), the attackers job is a lot more difficult, particularly for attackers without local access to the systems. Replicating something you know is easy, all an attacker has to do is figure out how to capture it. Replicating something you have or something you are is much harder. Multi-factor authentication will usually cause the attackers to fall back to other techniques to move from system to system. These fall back techniques are typically slower and easier to detect via audit analysis.

The OPM was required by multiple policies and guidance to implement a smart card based PIV system for authentication. Had their deployment been complete and effective it would have likely stopped, or posed a serious problem for the attackers that exploited their networks. Other organizations should also look seriously at multi-factor authentication for their users, and, if applicable, their customers.

3.2 Logging and Alerting

One of the alarming things from the information released about the OPM breach was the duration that the attackers were active within the network. Had the attacker activity been detected in a timely fashion, the attack could have been intercepted before the attackers were able to exfiltrate any significant quantity of data. An effective logging, auditing and alerting program can be difficult to implement. It is easy to end up drowning in irrelevant data. In fact the OPM Inspector General's report from fiscal year 2014 called out this exact problem; “The OPM systems currently providing data to the SIEM are over-reporting log and event data, which results in an excessive amount of data for security analysts to review.” (U.S. Office of Personnel Management Office of the Inspector General Office of Audits, 2014).

David Kennel, dakennel@gmail.com

Log reduction, automated analysis and alerting are key to being able to detect, malicious and anomalous activity within a network. There are a variety of tools designed to assist with this task from Security Information and Event Management (SIEM) tools (e.g. McAfee Enterprise Security Manager, OSSIM, EMC RSA Security Analytics), to log data mining tools (e.g. Splunk, Graylog), and user (and entity) behavioral analytics (UBA, UEBA)(e.g. Niara, Exabeam).

Regardless of the specific tools used, the important thing is proper tuning and alert configuration. Had the OPM configured their tools to look for queries of their databases that were returning large numbers of records, and were not coming from an authorized backup process, they would have seen the attempted extraction of data in time to intercept the attack. Another useful rule would have been to look for connections to OPM themed URLs that were not owned by OPM or an authorized partner as this would have likely revealed the connections to the command and control infrastructure.

3.3 Risk Assessment

Proper risk assessments are a critical component of a security program. Without effective assessment and management of risk all of the other components of the security program are only correct through luck. Risk assessment and management is key to ensuring that the correct controls are specified for an organization's various systems. It also helps ensure that the security program is executed in a fiscally responsible manner as it helps guide security expenditures so that high cost controls are not wasted on low impact systems.

An effective risk program is driven by management excellence as much as it is by tools. Effective vulnerability scanning tools are an important component of understanding an organizations true risk position. However vulnerability scans are useless unless they prompt remedial action. Governance, risk and compliance tools (GRC) are frequently used by larger organizations to help manage the process of performing risk assessments and categorization. While GRC tools can be of significant assistance, performing risk assessments and categorizing the risk of various systems is still largely a manual, expertise driven, job function that requires a clear understanding of an organizations data assets and how they are processed and utilized.

David Kennel, dakennel@gmail.com

An effective, integrated, risk management function at OPM could have helped prevent the breaches that they suffered by properly categorizing and assessing the risk to the various systems used to access, process and store OPM data. This information would have helped them prioritize systems and security controls that needed attention and allowed work and expenditures to be focused on areas that would provide the largest security return.

4 Conclusion

The OPM breach was a disaster for the United States federal government. It resulted in fairly immediate impact on operations in many areas and will have long term repercussions that are difficult to predict. Even though most sources agree that an APT was involved, this was a breach that was very much preventable.

If the OPM had a mature risk management program, effective log analysis, and a fully deployed multi-factor authentication mechanism the outcome of the breaches announced in 2015 would have been very different. By effectively implementing these three controls, all of which were required for OPM systems under existing federal requirements, OPM could have caught the intruders before they achieved their objectives and terminated the attack. Federal cyber-security is often lambasted for its ineffective "check the box" mentality, the fault is not with the guidance but the implementation. These examples prove that the existing federal guidance is not out of line with the Top 20 and can be leveraged, with the proper investments, to produce an effective and compliant security program.

David Kennel, dakennel@gmail.com

References

Bennett, B., & Hennigan, W. J. (2015, August 31). China and Russia are using hacked data to target U.S. spies, officials say - LA Times. Retrieved from http://www.latimes.com/nation/la-na-cyber-spy-20150831-story.html

Bisson, D. (2015, June 29). The OPM Breach: Timeline of a Hack. Retrieved February 14, 2016, from http://www.tripwire.com/state-of-security/security-data-protection/cyber-security/the-opm-breach-timeline-of-a-hack/

Boyd, A. (2015, June 25). Contractor breach gave hackers keys to OPM data. Retrieved from http://www.federaltimes.com/story/government/omr/opm-cyber-report/2015/06/23/keypoint-usis-opm-breach/28977277/

CIS. (2015). *CIS critical security controls for effective cyber defense*. Retrieved from https://www.cisecurity.org/critical-controls/download.cfm

Cole, E. (2014, January 5). Dr. Eric Cole on Twitter: "Dr. Cole's motto for 2014 is "Prevention is Ideal but Detection is a MUST"; Detection is going to be the KEY to success: Outbound Detection". Retrieved February 22, 2016, from https://twitter.com/drericcole/status/419835752483020800

Discovery Channel. (n.d.). Fingerprint scanners are unbeatable. Retrieved from http://www.discovery.com/tv-shows/mythbusters/mythbusters-database/fingerprint-scanners-unbeatable/

Federal Information Security Management Act of 2002, 44 U.S.C. § 3541

Federal Information Security Modernization Act of 2014, 44 U.S.C. § 3551

Gallagher, S. (2015, June 21). “EPIC” fail—how OPM hackers tapped the mother lode of espionage data | Ars Technica. Retrieved February 14, 2016, from http://arstechnica.com/security/2015/06/epic-fail-how-opm-hackers-tapped-the-mother-lode-of-espionage-data/

Gallagher, S. (2015, June 8). Why the “biggest government hack ever” got past the feds | Ars Technica. Retrieved from http://arstechnica.com/security/2015/06/why-the-biggest-government-hack-ever-got-past-opm-dhs-and-nsa/

David Kennel, dakennel@gmail.com

Hesseldahl, A. (2015, June 19). FireEye Identifies Chinese Group Behind Federal Hack | Re/code. Retrieved from http://recode.net/2015/06/19/fireeye-identifies-chinese-group-behind-federal-hack/

Institute for Critical Infrastructure Technology. (2015). Handing over the keys to the castle - OPM demonstrated that antiquated security practices harm national security. Retrieved from http://icitech.org/wp-content/uploads/2015/07/ICIT-Brief-OPM-Breach2.pdf

Kerner, S. M. (2015, February 24). Breach Detection Time Is Dropping, FireEye Finds. Retrieved from http://www.eweek.com/security/breach-detection-time-is-dropping-fireeye-finds.html

Koren, M. (2015, September 23). OPM Announces 5.6 Million People's Fingerprints Were Exposed in Data Breach - The Atlantic. Retrieved from http://www.theatlantic.com/technology/archive/2015/09/opm-hack-fingerprints/406900/

Krebs, B. (2015, February 15). Data Breach at Health Insurer Anthem Could Impact Millions — Krebs on Security. Retrieved from http://krebsonsecurity.com/2015/02/data-breach-at-health-insurer-anthem-could-impact-millions/

Krebs, B. (2015, March 15). Premera Blue Cross Breach Exposes Financial, Medical Records — Krebs on Security. Retrieved from http://krebsonsecurity.com/2015/03/premera-blue-cross-breach-exposes-financial-medical-records/

Levine, M. (2015, June 11). OPM Hack Far Deeper Than Publicly Acknowledged, Went Undetected For More Than A Year, Sources Say - ABC News. Retrieved from http://abcnews.go.com/Politics/opm-hack-deeper-publicly-acknowledged-undetected-year-sources/story?id=31689059

National Institute of Standards and Technology. (2004). Standards for security categorization of federal information and information systems (199). Retrieved from http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf

David Kennel, dakennel@gmail.com

National Institute of Standards and Technology. (2006). Minimum security requirements for federal information and information systems (200). Retrieved from http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf

National Institute of Standards and Technology. (2014). Security and privacy controls for federal information systems and organizations (SP 800-53). Retrieved from http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

National Institute of Standards and Technology. (2014, April 1). NIST.gov - Computer security division - Computer security resource center - FISMA detailed overview. Retrieved February 22, 2016, from http://csrc.nist.gov/groups/SMA/fisma/overview.html

OPM. (n.d.). Cybersecurity Incidents. Retrieved February 15, 2016, from https://www.opm.gov/cybersecurity/cybersecurity-incidents/

OPM(2). (n.d.). The security clearance and investigation process. Retrieved February 15, 2016, from http://www.brac.maryland.gov/documents/Security%20Clearance%20101%20PP%20Presentation.pdf

OPM. (2015, September 23). Statement by OPM Press Secretary Sam Schumach on Background Investigations Incident. Retrieved from https://www.opm.gov/news/releases/2015/09/cyber-statement-923/

Pepitone, J. (2015, June 25). China Is 'Leading Suspect' in OPM Hacks, Says Intelligence Chief James Clapper - NBC News. Retrieved from http://www.nbcnews.com/tech/security/clapper-china-leading-suspect-opm-hack-n381881

Roeder, O. (2015, July 15). What To Do With A Million Stolen Fingerprints | FiveThirtyEight. Retrieved from http://fivethirtyeight.com/datalab/what-to-do-with-a-million-stolen-fingerprints/

Swaby, R. (2012, September 10). The Password Fallacy: Why Our Security System Is Broken, and How to Fix It - The Atlantic. Retrieved from http://www.theatlantic.com/technology/archive/2012/09/the-password-fallacy-why-our-security-system-is-broken-and-how-to-fix-it/262155/

David Kennel, dakennel@gmail.com

Tandon, S. (2015, July 7). Cyber Security Blog: OPM Data Breach Cyber Security Hack: Trillion $ Privileged Access Insight [Web log post]. Retrieved from http://www.cyber-security-blog.com/2015/07/opm-data-breach-cyber-security-hack-apt-privileged-access-insight.html

ThreatConnect. (n.d.). OPM Breach Analysis. Retrieved February 16, 2016, from https://www.threatconnect.com/opm-breach-analysis-update/

U.S. Office of Personnel Management Office Of The Inspector General Office Of Audits. (2014). *Final audit report federal information security management act audit fy14* (4A-CI -00-14-0 16). Retrieved from https://www.opm.gov/our-inspector-general/reports/2014/federal-information-security-management-act-audit-fy-2014-4a-ci-00-14-016.pdf

Verizon. (2015). *2015 data breach investigations report*. Retrieved from http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigation-report-2015_en_xg.pdf

Williams, K. (2015, Sept 23). *OPM underestimated number of fingerprints stolen in hack by millions – The Hill*. Retrieved February 14, 2016, from http://thehill.com/policy/cybersecurity/254620-opm-underestimated-number-of-fingerprints-stolen-in-hack

David Kennel, dakennel@gmail.com

Last Updated: January 23rd, 2019

Upcoming SANS Training

Click here to view a list of all SANS Courses

SANS Las Vegas 2019	Las Vegas, NVUS	Jan 28, 2019 - Feb 02, 2019	Live Event
SANS Security East 2019	New Orleans, LAUS	Feb 02, 2019 - Feb 09, 2019	Live Event
SANS SEC504 Stuttgart February 2019	Stuttgart, DE	Feb 04, 2019 - Feb 09, 2019	Live Event
SANS Anaheim 2019	Anaheim, CAUS	Feb 11, 2019 - Feb 16, 2019	Live Event
SANS Northern VA Spring- Tysons 2019	Tysons, VAUS	Feb 11, 2019 - Feb 16, 2019	Live Event
SANS London February 2019	London, GB	Feb 11, 2019 - Feb 16, 2019	Live Event
SANS FOR610 Madrid February 2019 (in Spanish)	Madrid, ES	Feb 11, 2019 - Feb 16, 2019	Live Event
SANS Dallas 2019	Dallas, TXUS	Feb 18, 2019 - Feb 23, 2019	Live Event
SANS New York Metro Winter 2019	Jersey City, NJUS	Feb 18, 2019 - Feb 23, 2019	Live Event
SANS Scottsdale 2019	Scottsdale, AZUS	Feb 18, 2019 - Feb 23, 2019	Live Event
SANS Secure Japan 2019	Tokyo, JP	Feb 18, 2019 - Mar 02, 2019	Live Event
SANS Zurich February 2019	Zurich, CH	Feb 18, 2019 - Feb 23, 2019	Live Event
SANS Riyadh February 2019	Riyadh, SA	Feb 23, 2019 - Feb 28, 2019	Live Event
Open-Source Intelligence Summit & Training 2019	Alexandria, VAUS	Feb 25, 2019 - Mar 03, 2019	Live Event
SANS Reno Tahoe 2019	Reno, NVUS	Feb 25, 2019 - Mar 02, 2019	Live Event
SANS Brussels February 2019	Brussels, BE	Feb 25, 2019 - Mar 02, 2019	Live Event
SANS Baltimore Spring 2019	Baltimore, MDUS	Mar 02, 2019 - Mar 09, 2019	Live Event
SANS Training at RSA Conference 2019	San Francisco, CAUS	Mar 03, 2019 - Mar 04, 2019	Live Event
SANS Secure India 2019	Bangalore, IN	Mar 04, 2019 - Mar 09, 2019	Live Event
SANS St. Louis 2019	St. Louis, MOUS	Mar 11, 2019 - Mar 16, 2019	Live Event
SANS Secure Singapore 2019	Singapore, SG	Mar 11, 2019 - Mar 23, 2019	Live Event
SANS San Francisco Spring 2019	San Francisco, CAUS	Mar 11, 2019 - Mar 16, 2019	Live Event
SANS London March 2019	London, GB	Mar 11, 2019 - Mar 16, 2019	Live Event
SANS SEC504 Paris March 2019 (in French)	Paris, FR	Mar 18, 2019 - Mar 23, 2019	Live Event
SANS Munich March 2019	Munich, DE	Mar 18, 2019 - Mar 23, 2019	Live Event
ICS Security Summit & Training 2019	Orlando, FLUS	Mar 18, 2019 - Mar 25, 2019	Live Event
SANS Secure Canberra 2019	Canberra, AU	Mar 18, 2019 - Mar 23, 2019	Live Event
SANS Norfolk 2019	Norfolk, VAUS	Mar 18, 2019 - Mar 23, 2019	Live Event
SANS Doha March 2019	Doha, QA	Mar 23, 2019 - Mar 28, 2019	Live Event
SANS Jeddah March 2019	Jeddah, SA	Mar 23, 2019 - Mar 28, 2019	Live Event
SANS Madrid March 2019	Madrid, ES	Mar 25, 2019 - Mar 30, 2019	Live Event
SANS SEC560 Paris March 2019 (in French)	Paris, FR	Mar 25, 2019 - Mar 30, 2019	Live Event
SANS Dubai January 2019	OnlineAE	Jan 26, 2019 - Jan 31, 2019	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced