CASES

All content is the property of the original sourced author – Case concept is Property of ExpandingSecurity.com

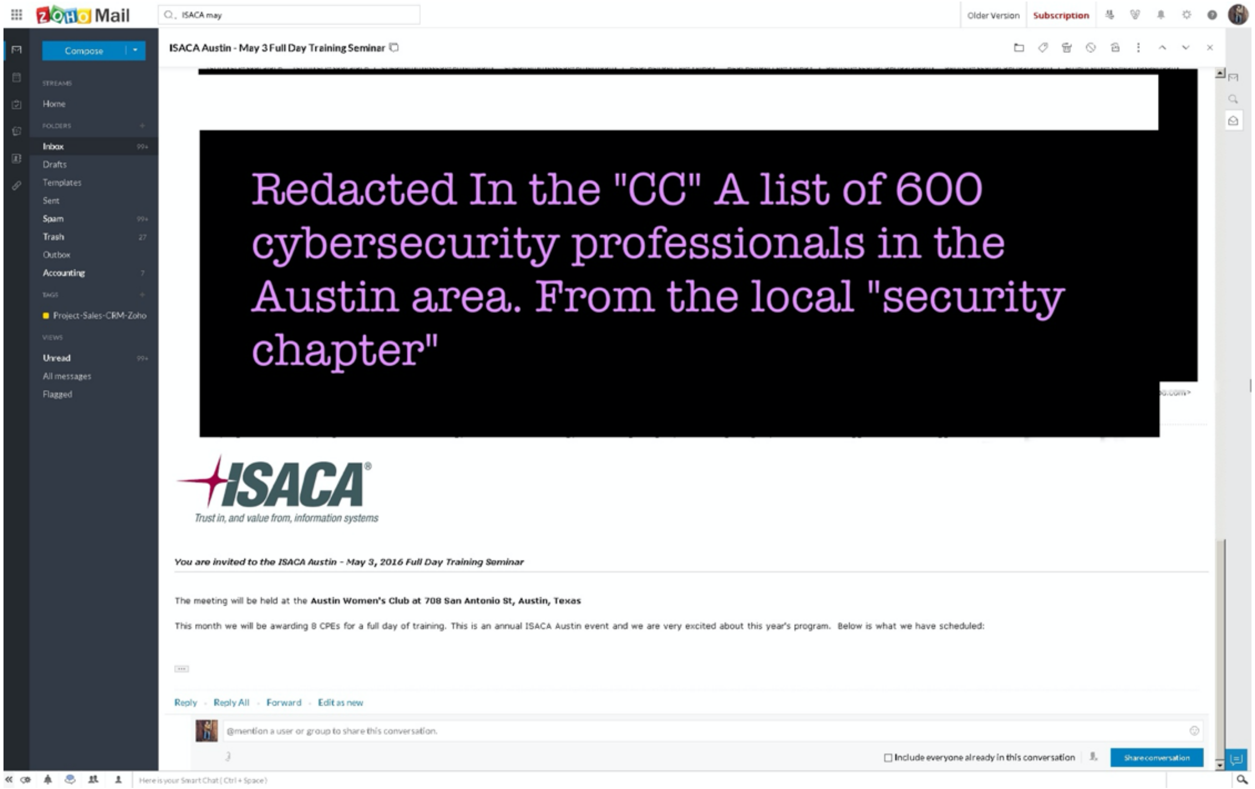
Each case is cited to the original source location, since sites disappear all the time I offer them to you for ease of use only.

SRM-5 Designing Security

CISSP-SRM-1-Case-20170101

Source: Dean Bushmiller

These are redacted screenshots:



ISACA Austin - May 3 Full Day Training Seminar

[redacted]

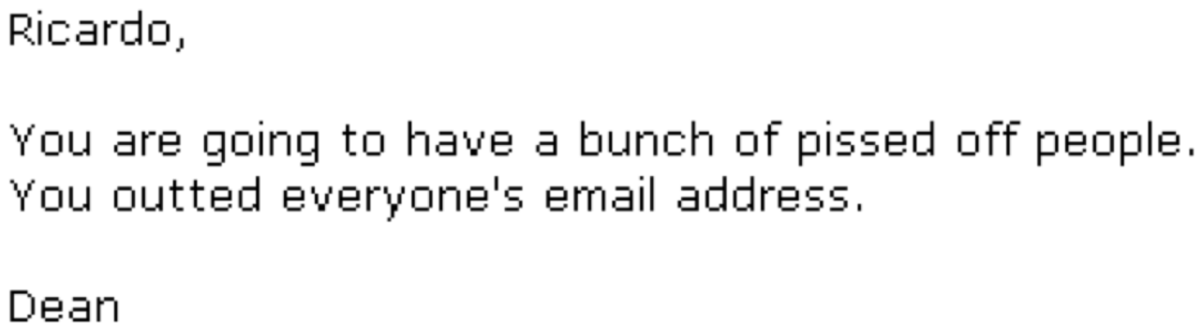
Redacted In the "CC" A list of 600 cybersecurity professionals in the Austin area. From the local "security chapter"

You are invited to the ISACA Austin - May 3, 2016 Full Day Training Seminar

The meeting will be held at the **Austin Women's Club at 708 San Antonio St, Austin, Texas**

This month we will be awarding 8 CPEs for a full day of training. This is an annual ISACA Austin event and we are very excited about this year's program. Below is what we have scheduled:

Dean's Response:

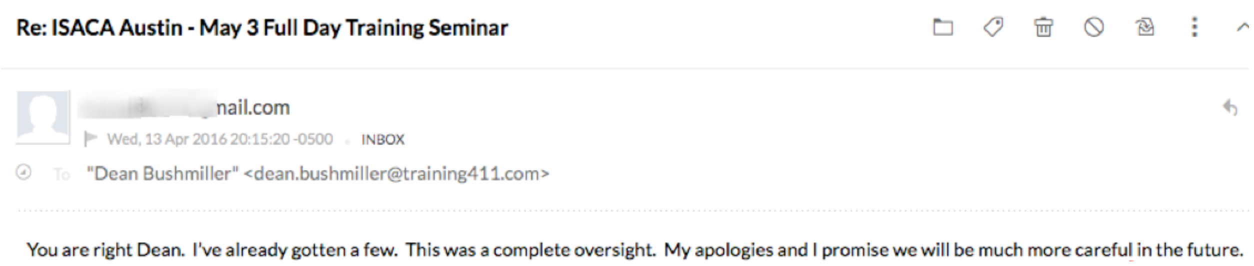


Ricardo,

You are going to have a bunch of pissed off people. You outted everyone's email address.

Dean

Ricardo's Response to Dean:



Re: ISACA Austin - May 3 Full Day Training Seminar

[redacted]nail.com

Wed, 13 Apr 2016 20:15:20 -0500 INBOX

To "Dean Bushmiller" <dean.bushmiller@training411.com>

You are right Dean. I've already gotten a few. This was a complete oversight. My apologies and I promise we will be much more careful in the future.

SRM-2 Policy Building & Paperwork

CISSP-SRM-3-CASE-20090216

Source https://www.strategypage.com/htmw/htmoral/articles/20090219.aspx

1. The British Army is facing a mutiny as the brass try to limit Internet use by the troops. On February 4th, British Ministry of Defence issued new rules that, basically, prohibited the troops from using blogs, message boards social networking sites (like Face book) or online games (which usually involve parallel use of messaging systems). The response was immediate and unexpectedly mutinous. Troops openly insisted that they would ignore the ban. Some simply pointed out that these communications tools were essential to maintaining morale. The Ministry of Defence got the message, sort of, and began backing off. The February 4th order was promptly watered down, and is expected to fade away, like a bad dream.
2. Military personnel, especially in the West, were quick to adopt the Internet as a way to keep in touch with family and friends, as well as each other. The troops also exchanged information on tactics and techniques, as well as anything else they knew that could help keep them alive in combat. This alarmed the U.S. Department of Defense three years ago, and some restrictions were imposed on active duty bloggers. The troops did not fight back, as, once reminded, they understood that, in public forums, anyone could read what they were saying, including the enemy. So a lot of this information continued to be exchanged via email and private message boards. The military got into the act by establishing official message boards, for military personnel only, where useful information could be discussed and exchanged. All this rapid information sharing has had an enormous impact on the effectiveness of the troops, something that has largely gone unnoticed by the mass media.

3. The brass have not tried to discourage all this communication, because the officers use it as well, for the same reasons as the troops. Most junior officers grew up with the Internet, and many of the older ones were using the Internet before it became popularized in the 1990s. Even the generals of today, have experience with PCs when they were young, so have no trouble getting into this new form of communication. The military is eagerly building a "battlefield Internet" for use during combat, and parts of this are up and running and heavily used in Iraq and Afghanistan.
4. But much of this is still uncharted territory. There's never been an army before where all the troops were so well connected with each other. So far, the benefits have outweighed any liabilities. But no one is sure where it will go next, and the public is largely unaware of the impact, because the mass media has not grasped nature and extent of the changes.

SRM-3 Risk Assessment

CISSP-SRM-4-CASE-20100322

Source: http://www.darkreading.com/story/showArticle.jhtml?articleID=224000393
Original report: http://www.gao.gov/new.items/d10355.pdf

By Tim Wilson, DarkReading March 22, 2010

1. With tax time rapidly approaching, the U.S. Internal Revenue Service still has not sealed up all of the holes that could allow insiders or external hackers to access taxpayer data, according to a new report.
2. In a study issued last week, the Government Accountability Office states that the IRS has corrected less than one-third of the 89 security weaknesses identified in its audit of the tax agency last year.
3. "While IRS has corrected 28 control weaknesses and program deficiencies, 61 of them -- or about 69 percent -- remain unresolved or unmitigated," the report states. "For example, IRS continued to install patches in an untimely manner and used passwords that were not complex. In addition, IRS did not always verify that remedial actions were implemented, or effectively mitigate the security weaknesses."
4. Weaknesses in IRS systems "continue to jeopardize the confidentiality, integrity, and availability of financial and sensitive taxpayer information," the GAO says. "IRS did not consistently implement

controls that were intended to prevent, limit, and detect unauthorized access to its systems and information.

5. "For example," the report continues, "IRS did not always (1) enforce strong password management for properly identifying and authenticating users; (2) authorize user access to permit only the access needed to perform job functions; (3) log and monitor security events on a key system; and (4) physically protect its computer resources."
6. A key reason for the slow resolution of the vulnerabilities is that the IRS has not yet fully implemented its agencywide IT security program to ensure controls are appropriately designed and operating effectively, the GAO says. The agency hasn't been conducting annual reviews of risk assessments, for example, and it hasn't been checking to ensure contractors received security awareness training.
7. "Until these control weaknesses and program deficiencies are corrected, the agency remains unnecessarily vulnerable to insider threats related to the unauthorized access to and disclosure, modification, or destruction of financial and taxpayer information, as well as the disruption of system operations and services," the report says.
8. The IRS permitted "excessive access" to systems and files by granting rights and permissions that gave users more access than they needed to perform their assigned functions, the GAO states.
9. "For example, about 120 IRS employees had access to key documents, including cost data for input to its administrative accounting system and a critical process-control spreadsheet used in IRS's cost allocation process," the report says. "However, fewer than 10 employees needed this access to perform their jobs."
10. The IRS also configured 18 of its routers with a protocol that allows unencrypted, plain-text authentication, and the agency did not always effectively log and monitor security events, the GAO says. Outdated and unsupported applications running on IRS systems could also put taxpayer data at risk, according to the report.
11. The IRS says it is developing a comprehensive plan that will address all of the vulnerabilities identified in the GAO report.

SRM-4 Risk Management

CISSP-SRM-5-CASE-20110101

Source web site URL:
https://www.theregister.co.uk/2017/06/24/anthem_115m_largestever_data_theft_settlement/

Anthem to shell out $115m in largest-ever data theft settlement

By Shaun Nichols

1. Health insurer Anthem has today agreed to pay $115m to settle a class-action suit brought on by its 2015 cyber-theft of 78.8 million records.
2. The settlement fund will be used to cover damage costs incurred by people who had personal information including their names, dates of birth, addresses, and medical ID numbers stolen when, in 2015, Anthem was hit by hackers.
3. While credit card details and medical records were not accessed, the exposed personal information was serious enough that credit monitoring services have been given to affected customers.
4. Now, after two years of legal wrangling, a settlement package has been agreed on and put forward for court approval. Judge Lucy Koh will review the proposal and sign off on the deal or send it back to be re-written.
5. "After two years of intensive litigation and hard work by the parties, we are pleased that consumers who were affected by this data breach will be protected going forward and compensated for past losses," lead attorney Eve Cervantez said.
6. As is usually the case with settlements, Anthem will not have to admit to any wrongdoing.
7. If you were one of those hit by the intrusion, don't expect a big payout. Plenty of others will be getting their cuts first. According to the terms of the settlement, a full third of the package ($37,950,000) has been earmarked to cover attorney fees.
8. An additional $17m will be paid out to Experian, who is handling the credit and identity monitoring services for victims. Any taxes the government levies on the $115m payout will also be deducted from the fund itself.

9. After all that, people affected will be able to fill out the necessary forms to claim a share of the settlement, including coverage of out-of-pocket expenses they have incurred from the breach (but only up to $15m – beyond that no more out-of-pocket claims will be accepted).
10. The timeline for submitting claims will be decided after (and if) the settlement deal is approved.

ANT-1 Penetration Testing

CISSP-CASE-ANT-1-20191106

Source: DRB

PLEASE review best practices for Pen testing and be prepared to report on what went wrong with this test.

A penetration testing story

1. I am the new help-desk/ junior incident responder at XYZ company. I was walking down the hall and my boss Bob waved me into his meeting. He was in there with a salesperson Sal from ABC penetration testing company. This was his third and final meeting. I knew Bob was about to choose this vendor. Here is what I heard:
2. Sal "We hire the best prior black hats available every month from a pool of about 10,000 in the piratebay. We have found items like M&A reports for the two largest credit unions in Arlington, Texas. We also did a few reports on-spec and found serious flaws in the way a company handled the online Japanese reverse auctions." Bob seems impressed with Sal.
3. Bob "You asked for the last pen test report and I emailed it to your boss last week. Did he review it so we can set the scope today?"
4. Sal "Yes, he forwarded it on to me." Sal and Bob looked at the report for a few minutes on Sal's iPad. They talked about the items that were not fix from last time (like the Apache Struts bug) and set them out of scope. I noticed the dora-the-explorer stickers and made a comment as he was leaving. Sal's only comment, "yeah my daughter and I swapped iPads by mistake yesterday"

5. The scope of the test was determined and the contract was really short: ABC wilk test the XYZ.com web server and database server that directly supports the webserver in the next 3 days. Sal's brother Al was the only one authorised to contact me and do the testing. ABC was given 2 sets of credentials: a user and customer service account.
6. My job was to capture all the packets to and from the web server for the next 5 days. My job was to take a call from ABC whenever they called, remote into the laptop and turn on the wireshark. My host was a big machine with a stack of drives shoved in it.
7. Day 1- Nothing
8. I get a call from Al saying they are delayed getting started because of another test. Nice! I get a long lunch and go home early.
9. Day 2- Charlie calls
10. Charlie is one of ABC's new testers who calls and asked me for the passwords. "Yeah it is userABC with password of userABC and CSR with a password of csrABC." Charlie says they will start at noon and will be done at 6PM. I turn on my wireshark and go home for the night. I remote in at 8 PM, I see Charlie's IP address is still pounding away. I call and ask how much longer. Charlie says "I need 2 more hours." Forget waiting around, I am going to bed.
11. Day 3- My laptop dies
12. I go in about 6AM and get to work turning off the capture. Yep, my hard drives are full and Charlie is still at it. He has pivoted to my laptop's IP and is working on our Mail server. I call Charlie and ask if they can stop. "sure, I could not get anything from the web interface and the mail server is yielding nothing. I have set up the phishing attack for your users, I can start fresh tonight"
13. Day 4- Done
14. I am really happy this is over. I have had to restore the customer database three times and our phone lines have been packed with pissed off customers. I call Al to make sure they are done. Yep- He ask me to send over my captures so he can verify a few attacks.
15. Day 5- The report

16. Charlie send the report to me via email. I have to scroll forever to get to the report attachment, it looks like Charlie, Sal, Al and two other people are passing it back and forth to confirm the results. It looks like the indent email forward chain from hell. It looks like a bunch of NMAP/Nessus scans. (I could have done that) I clean it up pull the report, print it, and plop it on Bob's desk. Bob is on to the next thing. He says, "I will get to it next month."
17. Post-mortum
18. I get a call from Charlie. "Hey, do you know if XYZ paid ABC? Will you poke around for me? I never got a check." I connect with Bob trying to be cool about it. "How did you like the report? Do you think we will hire them again?" I can see by our conversation this was a giant waste of time. Oh well, another early lunch for me.

ANT-2 Logs & Security Events Management

CISSP-ANT-2-SEIM-20191113

Source: Andrew Beeber, Dean Bushmiller &

- https://blogs.cisco.com/security/the-significance-of-log-sources-to-building-effective-intelligence-driven-incident-response
- https://www.business2community.com/cybersecurity/dhs-einstein-fail-01462281
- https://securityboulevard.com/2018/05/avoid-these-failures-with-siem-tools-at-all-costs/

FOCUS ON SEIM best practices - What is wrong from a best practices standpoint and how will you fix it?

Proposed log management by the Chief Incident Management Officer (CIMO)

1. We are going to build a log management system. We are moving to a DEVSECOPS deployment model. Here is what we have done so far and what we expect:
2. What we know so far: background, current policies, and assessment.
3. Background:
4. Last year we failed three audits. Our credit card charge rate increased by .2% due to a failed audit; we had the data but we could not get it organized in time. Our CISO built small test implementations from the three major vendors and found the pricing too high, we are going to phase out the small implementations that we have in London, New York, and Paris. All data will be centrally housed in our private cloud provider in New York.
5. Current policies:
6. Since we have operations that follow the sun we let the London IRT team start the day. Every incident starts at GMT-0 and ends with the Paris IRT. All log data is converted to english. When there is a policy change it is finalized by the NYC.
7. Assessment:
8. In the CISO’s last test she found people responsible for performing log analysis are responding well.

9. Our reliance on signature based detection technology and where to get these signatures is still in question. In the first testing by ABC pen testing company; they tested each one of the three systems by presenting 489 known security vulnerabilities in computer and web applications; ABC was only able to detect roughly 29 vulnerabilities for a 6% accuracy rate.
10. Our CISO has determined our staff solves one problem well manually. Incident response teams are finding malware is using newly registered random DNS names. We get a ton of fake randomized DNS names used by malware. In our analysis we want to automatically score phishing domains based upon the "born on" date of the domain registration. Currently our IRT uses a simple script of whois and a combination of unix command line pipes and filters. We end up with a "Creation Date: 2004-01-26T23:03:24Z" and compare that to the current date, to see if it is less than 10 days. We calculate that this script gets run 20,000 per day. This is a low level activity that we want to automate.
11. **What we expect from the system:**
12. Capacity and design:
13. Disseminate and integrate data for 20 global departments
14. The SIEM must be our system of record
15. Support 25,000 servers and 4,000 network devices
16. Collaborate with our threat intelligence
17. Safeguard any personally identifiable information
18. Meet regulatory standards for GDPR, HIPAA, PCI
19. Support internal audits performed 4 times per year by certified CISA's.
20. Be programmable and extensible by internal staff
21. Support custom build of dashboard/instrumentation
22. Integrate with databases, API's, windows events, network inputs
23. Be customizable and allow for network segmentation
24. Security capabilities:
25. Intrusion detection, intrusion prevention, log management, and information sharing
26. Ingest data from: cloud providers, on site servers, route switch equipment, and security tools

27. All data will be encrypted in transit and at rest

28. Environmental problems we see so far:

29. Some hosts are registered by IP, some by Active Directory, some by VMware.

30. Hosts are not uniformly named.

31. We can't reconcile a host to an IP addresses due to RFC 1918 networks.

32. We have no way to report on when a host fails to send logs.

33. We have too much data and our searches and dashboards take too long to load.

34. We have devices that are reporting event data in local time zones.

35. We are firewalled from obtaining some data

36. We want to be able to produce data for legal purposes.

37. Our process metrics that the SEIM will support:

38. 365x24 monitoring

39. Length of time to on-board new data source 3-5 days per source above.

40. response: new search rule writing in less than 24 hours.

41. response: compliance outputs in 48 hours.

42. Our system must support these roles:

43. 480 Helpdesk people - who write tickets - turn over 50% per year.

44. 24 full time IRT staff

45. 4 MOTD's

46. 6 Compliance log auditors - who spend 50% of their time with us and 50% with IT/finance

47. 6 IRT managers

48. 1 Chief Log Manager - reporting to CIO

ANT-3 CVE

NONE

ANT-4 Audit & Compliance

CISSP-CASE-ANT-5-20190719

Source:
https://cooleyma.com/2019/07/19/inadequate-cybersecurity-and-data-privacy-due-diligence-alleged-in-starwood-deal-as-uk-ico-fines-marriott-125m-for-gdpr-violations

1. On July 9, 2019, the UK Information Commissioner's Office (ICO) publicly announced its intent to impose a £99M (approximately $123M) GDPR fine on Marriott as a result of its acquisition of Starwood and the subsequent discovery and notification of a data breach at Starwood. --SNIP--
2. Background on the ICO's Proposed Marriott Fine
3. In an interesting twist, news of the proposed fine did not originate from the ICO. As a result of SEC cyber guidance from 2011 and 2018, which specifies that cyber risks and cyber incidents could trigger general SEC reporting obligations, Marriott released a statement on its website to coincide with a filing of its 8-K. The statement reiterated details of the breach that dated back to 2014 in which the personal information of almost 400 million Starwood guests was exposed, of which about 30 million were in the European Economic Area (EEA) and seven million were in the UK. The breach was discovered in November 2018. Following the Marriott disclosure, the ICO released its own statement about the fine, noting that Marriott and British Airways had been provided "a confidential notice of intent and they had market obligations to disclose it. They decided. So we followed up with a statement. That's why you don't see the full report with all the details. Usually this is a confidential exchange."

4. Further, according to the ICO, its “investigation found that Marriott failed to undertake sufficient due diligence when it bought Starwood and should also have done more to secure its systems” (emphasis added). Information Commissioner Elizabeth Denham went on to state, “Organizations must be accountable for the personal data they hold. This can include carrying out proper due diligence when making a corporate acquisition, and putting in place proper accountability measures to assess not only what personal data has been acquired, but also how it is protected” (emphasis added). While it is unclear whether or how an alleged failure to conduct due diligence during a merger constitutes a GDPR violation, the ICO clearly feels that appropriate due diligence around security and privacy is important.
5. Cyber incidents, however, are almost never straightforward, especially as they are first being investigated. Hindsight in a data breach is 20/20 and usually leads to pronouncements of things that could have been done to avoid the incident in the first place. While the ICO says it has done an “extensive investigation,” it’s entirely possible that at the time of the Starwood acquisition even a thorough cybersecurity evaluation wouldn’t have determined that an issue existed. As support for this, an article by Brian Krebs stated, “The intruders encrypted information from the hacked database (likely to avoid detection by any data-loss prevention tools when removing the stolen information from the company’s network).”
6. The deal documents, however, don’t necessarily look good for Marriott in hindsight. While stock purchase agreements or merger agreements often contain at least one provision addressing privacy and security, the Marriott/Starwood Agreement and Plan of Merger seems to indicate that security and privacy weren’t considered. While the agreement includes traditional IP representations and warranties, there are no separate reps and warranties around privacy or cybersecurity.

7. In any event, the ICO says Marriott can appeal and Marriott has said they would. We may see a detailed examination of at least some of the considerations for imposing fines (found in Article 83 of the GDPR) in light of the Marriott situation. For example, they could argue they took immediate steps to mitigate the attack, cooperated with the investigation and were in compliance with industry standards (such as PCI). Further, to the extent the failure to conduct due diligence is tied to a GDPR violation, they could argue their diligence was reasonable despite the terms of the merger agreement and they used best practices to contain the damage once the breach was discovered. It will be interesting to see how the ICO reacts to those (and any other) arguments Marriott will make.
8. Cybersecurity Diligence in M&A
9. Specialists with specific cybersecurity knowledge increasingly get called in to perform detailed diligence on privacy and cybersecurity matters in M&A. --SNIP--
10. In light of this, depending on the circumstances, acquirers may need to evaluate more closely the cybersecurity exposure brought on by the acquisition. An overall cyber risk assessment early in the process can help calibrate the cyber maturity of a target. In addition to a diligence review of the target's cyber documentation (e.g., security policy, incident response policy, access control policy, etc.) by the acquirer's legal team, something as simple as a cyber questionnaire could provide some perspective on the cyber aspects of the target. Alternatively, a more thorough (and technical) analysis could be performed by a third party brought in by the acquirer's legal team (in order to protect communications under attorney-client privilege). This could consist of a static analysis of the network defenses from inside the network to an active attempt to break into the network from the outside, which is known as a penetration test.

11. In addition, there are a number of internal and external cybersecurity assessment tools that can provide an ostensibly objective score and rating of the target. For software, a security audit could be performed as well as having any number of vulnerability tests performed that can help reveal various coding issues that could lead to security incidents. Finally, compliance can play a role in assessing security. If the target has gone through a PCI audit, an ISO 27001 assessment, a SSAE 16 audit or any other of an assortment of security compliance-related processes, the results can be examined for helping determine the security posture of the target.
12. Outcomes of Cybersecurity Diligence
13. In the event that any of the above techniques reveal issues the acquirer finds unacceptable, provisions of the acquisition agreement could be used to terminate the deal and allow the parties to walk away. For example, the acquirer, upon finding a very serious cybersecurity problem with the target, might be able to invoke a material adverse change (MAC) clause if drafted with cybersecurity breaches in mind. Typically, if a party to a transaction experiences a MAC in the party's business, operations, financial or other condition, a MAC clause could allow the other party to withdraw from the transaction.
14. For the target company, performing its own risk assessment could offer several useful benefits (particularly if performed before any particular transaction were to commence). For example, if a target conducts a risk assessment, the resulting gap analysis can be used to begin addressing any significant issues before they arise in the context of the transaction. Such foresight could ultimately result in a higher valuation of the target and reduced risk that major issues arise later that could derail a potential transaction. Further, any resulting certification or compliance assessment can be used as described above to demonstrate the security posture of the target to defend against regulatory investigations and potentially save millions on fines or other penalties. In the event a transaction moves forward before all deficient elements of a cybersecurity audit are met, a target will want to carefully evaluate which elements to disclose and how to disclose them. Having a plan for addressing such deficient elements can often ease concerns that might be raised by the acquirer.

DEV-1 DEV Life Cycle

Source: https://thedailywtf.com/articles/2017-the-new-manager

1. She'd resisted the call for years. As a senior developer, Makoto knew how the story ended: one day, she'd be drafted into the ranks of the manager, forswearing her true love webdev. She knew she'd eventually succumb, but she'd expected to hold out for a few years before she had to decide if she were willing to change jobs to avoid management.
2. But when her boss was sacked unexpectedly, mere weeks after the most senior dev quit, she looked around and realized she was holding the short straw. She was the most senior. Even if she didn't put in for the job, she'd be drafted into acting as manager while they filled the position.
3. This is the story of her first day on the job.
4. Makoto spent the weekend pulling together a document for their external contractors, who'd been plaguing the old boss with questions night and day— in Spanish, no less.
5. Makoto made sure to document as clearly as she could, but the docs had to be in English; she'd taken Japanese in high school for an easy A. She sent it over first thing Monday morning, hoping to have bought herself a couple of days to wrap up her own projects before the deluge began in earnest.
   It seemed at first to be working, but perhaps it just took time for them to translate the change announcement for the team. Just before noon, she received an instant message.
6. Well, I can just point them to the right page and go to lunch anyway, she thought, bracing herself.
7. Emilio: I am having error in application.
8. Makoto: What error are you having?
   A minute passed, then another. She was tempted to go to lunch, but the message client kept taunting her, assuring her that Emilio was typing. Surely his question was just long and complicated. She should give him the benefit of the doubt, right?
9. Emilio: error i am having is: File path is too long
10. Makoto winced. Oh, that bug ... She'd been trying to get rid of the dependencies with the long path names for ages, but for the moment, you had to install at the root of C in order to avoid hitting the Windows character limits. But I documented that. In bold. In three places!

11. Makoto: Did you clone the repository to a folder in the root of a drive? As noted in the documentation there are paths contained within that will exceed the windows maximum path length otherwise
12. Emilio: No i cloned it to C:\Program Files\Intelligent Communications Inc\Clients\Anonymized Company Name\Padding for length\
13. Makoto's head hit the desk. She didn't even look up as her fingers flew across the keys. I'll bet he didn't turn on nuget package restore, she thought, or configure IIS correctly.
14. Makoto: please clone the repository as indicated in the provided documentation, Additionally take careful note of the documented steps required to build the Visual Studio Solution for the first time, as the solution will not build successfully otherwise
15. Emilio: Yes.
16. Whatever that means. Makoto sighed. Whatever, I'm out, lunchtime. Two hours later she was back at her desk, belly full, working away happily at her next feature, when the message bar blinked again. Dammit!
17. Emilio: I am having error building application.
18. Makoto: Have you followed the documentation provided to you? Have you made sure to follow the "first time build" section?
19. Emilio: yes.
20. Makoto: And has that resolved your issue?
21. Emilio: Yes. I am having error building application
22. Makoto: And what error are you having?
23. Emilio: Yes. I am having error building application.
24. "Oh piss off," she said aloud, safe in the knowledge that he was located thousands of miles from her office and thus could not hear her.

    "That bad?" asked her next-door neighbor, Mike, with a sympathetic smile.

    "He'll figure it out, or he won't," she replied grimly. "I can't hold his hand through every little step. When he figures out his question, I'll be happy to answer him."

    And, a few minutes later, it seemed he did figure it out:

25. Emilio: I am having error with namespaces relating to the nuget package. I have not yet performed nuget package restore

    The sound of repeated thumps sent Mike scurrying back across the little hallway into Makoto's cube. He took one look at her screen, winced, and went to inform the rest of the team that they'd be taking Makoto out for a beer later to "celebrate her first day as acting manager." That cheered her enough to answer, at least.
26. Makoto: Please perform the steps indicated in the documentation for first time builds of the solution in order to resolve your error building the application.
27. Emilio: i will attempt this fix.

    Ten minutes passed: just long enough for her to get back to work, but not so long she'd gotten back into flow before her IM lit up again.
28. Emilio: I am no longer having error build application.

    "Halle-frickin-lujah", she muttered, closing the chat window and promptly resolving to forget all about Emilio ... for now.

DEV-3 Code Review

https://www.eweek.com/security/mac-trojan-builds-botnet-symantec-researchers-say

First spotted in January, the trojan had been bundled into copies of pirated MacOS software.

1. At the time of discovery, researchers noted that the malware payload included tools which could allow an attacker to remotely take control of an infected system. Now, it appears as if those components are being put to use.
2. In a recent article, Symantec researchers Mario Barcena and Alfredo Pesoli reported that systems infected by the trojan have been used in at least one denial of service attack. Other users are also reporting that their systems are displaying activity caused by the malware.

3. News of the botnet marks what experts have warned is a small but growing crop of malware which targets OS X systems.
4. "Quite frankly there is not any functionality in this 'bot' that we have not seen before," noted McAfee Avert Labs head of research and communications Dave Marcus.
5. "The only thing of concern here is that it does affect the Mac platform which certainly is fresh territory."
6. Marcus recommended that Mac users avoid installing pirated software applications and install antivirus software to guard against infection.
7. Malware attacks targeting users of pirated Mac software earlier in 2009 culminated in the creation of the first known Mac botnet, according to Symantec.
8. According to researchers at Symantec, the Mac botnet was built on the backs of users of pirated versions of iWork '09 and the Mac version of Adobe Photoshop CS4. In an article in the latest edition of Virus Bulletin, Symantec researchers Mario Barcena and Alfredo Pesoli of Symantec Ireland dubbed the network of computers iBotnet and stated it was used to launch a denial-of-service attack against a Web site in January.
9. The botnet is not especially large, most likely due to the fact that it was targeting users of pirated software. When Mac-focused security company Intego first released an advisory about the Trojan in late January, it put the number of infected computers at 5,000. The malware that infected the bots, known as OSX.Iservice, installs a backdoor on infected systems and begins contacting other hosts for commands. Hidden in the pirated software, the malware infects users sharing the files over peer-to-peer networks.

DEV-4 Open Web Application Security

CISSP-CASE-DEV-4-20190802

Source:
https://medium.com/@logicbomb_1/one-misconfig-jira-to-leak-them-all-including-nasa-and-hundreds-of-fortune-500-companies-a70957ef03c7

https://medium.com/@logicbomb_1/bugbounty-nasa-internal-user-and-project-details-are-out-2f2e3580421b

THIS IS A VERY TECHNICAL CASE - but there is a core business problem

One Misconfig (JIRA) to Leak Them All- Including NASA and Hundreds of Fortune 500 Companies!

Avinash Jain

1. Some months back, I published an article on “Exposed JIRA server leaks NASA staff and project data” in which I was able to find NASA staff details, their username, their email ids along with their internal project details which were getting leaked by one of their tools — JIRA which is an Atlassian task tracking systems/project management software used by around 135,000 companies and organization globally. The root cause behind the leak was the wild misconfiguration which was present in JIRA. Why the term “wild” being used is because, with the help of the same misconfiguration, I happened to access internal user data, internal project details of hundreds and thousands of companies which were using JIRA.
2. Lots of companies were from Alexa and Fortune top lists as well. The affected customers ranges from companies as big as NASA, Google, Yahoo to HipChat, Zendesk, Sapient, Dubsmash, Western union, Lenovo, 1password, Informatica, etc and many sectors of various government around the world also suffered the same privacy issue like one of the portal of European government, United Nations, NASA, Brazilian government transport portal, Canadain governement finance portal where due to some misconfiguration issues in JIRA, their internal user data, their name, email ids, their project details on which they were working, assignee of those projects and various other information were getting exposed.
3. Here, I’ll be sharing about what was that critical vulnerability that I happened to find in Jira (An Atlassian task tracking systems/project management software) or more specifically a misconfiguration issue which caused the leakage of internal sensitive information of organization and companies.
4. Let’s see what was the exact issue —

5. In Jira, while creating filters or dashboards it provides some visibility option to apply to them. The issue was due to the wrong permissions assigned to them. When the filters and dashboards for the projects/issues are created in JIRA, then by default the visibility is set to “All users” and “Everyone” respectively, which instead of sharing with everyone of the organizations (which people think and interpret), it share them publically. There is also a user picker functionality in Jira which gives a complete list of every user’s username and email address. This information disclosure is the result of an authorization misconfiguration in Jira’s Global Permissions settings. Because of the wrong permissions scheme, the following internal information appeared to be vulnerable:
6. all account’s employees’ names and emails,
7. employees’ roles through JIRA groups,
8. current projects, upcoming milestones through JIRA dashboards/filters
9. Anyone with the link can access them from anywhere and get hold of various sensitive information and because they are being indexed by all the search engines so anyone can easily find them with some simple search queries.
10. NASA Staff data because of misconfigured Jira user picker functionality
11. Jira Filter Publically accessible
12. Jira Dashboard Publically accessible
13. NASA Project details getting exposed due to public Filter and dashboard
14. As can be seen above, it discloses employees names, employee roles, upcoming milestones, secret project, and various other features due to these misconfigured Jira settings.
15. Now, how I found the links/URLs of these publically exposed user picker functionality, filters, and dashboards of so many companies and the help came from “Google dorks” (search query). To search for the companies having user picker functionality in Jira as misconfigured and so the complete list of their staff username and email address exposed, here is the search query —
16. inurl:/UserPickerBrowser.jspa -intitle:Login -intitle:Log
17. This query list all the URLs having “UserPickerBrowser” in their URI to find all the misconfigured Jira User picker functionality which are publically exposed and also not authenticated.

18. NASA Staff data exposed by misconfigured Jira
19. While for filters and dashboards, we can see the URLs of these filters and dashboards containing “Managefilters” and “ConfigurePortal” as a part. I went on to create the search query —
20. inurl:/ManageFilters.jspa?filterView=popular AND (intext:All users OR intext:Shared with the public OR intext:Public)
21. This query list all the URLs having “Managefilters” in their URI and having text as “Public” so to find all the misconfigured JIRA filters which are publically exposed and also not authenticated.
22. inurl:/ConfigurePortalPages!default.jspa?view=popular
23. This query list all the URLs having “ConfigurePortalPages” in their URI to find all the JIRA dashboard which are publically exposed.
24. On further recon(information gathering), I have found that various companies have JIRA URL in the format “company.atlassian.net” so if you want to check for any company who have misconfigured filter, dashboard or user picker functionality, you need to just put their name in the URL like —
25. https://companyname.atlassian.net/secure/popups/UserPickerBrowser.jspahttps://companyname.atlassian.net/secure/ManageFilters.jspa?filterView=popular https://companyname.atlassian.net/secure/ConfigurePortalPages!default.jspa?view=popular
26. Thousands of companies filters, dashboards and staff data were publically exposed. It occurs because of the wrong permissions scheme set to filters and dashboards hence providing their access even to non-logged in users and hence leading to leaking of sensitive data. I have discovered several such misconfigured JIRA accounts in hundreds of companies. Some of the companies were from Alexa and Fortune top list including big giants like NASA, Google, Yahoo, etc and government sites as well like
27. The Brazilian government has Jira filter misconfigured of their Road and Transport system hence exposing some of their project details, employee names, etc which was fixed after reaching out to them.
28. Similarly, the United Nations accidentally made their Jira filters and Jira dashboard public hence exposed their internal project details, secrets milestones, etc which was fixed by them after I reported it and was rewarded by them in their Hall of fame list.

29. Even the European government suffered the same exposure when their Commercial finance software systems and solutions had the same Jira misconfiguration and exposing their internal sensitive project and staff details. They also fixed it after I sent out the report to them and was also recognized in their Hall of fame list.
30. NASA Jira filters publicly accessible
31. Gov.uk Jira Filters publicly accessible
32. Informatica Jira filters publically exposed
33. Zendesk Jira dashboard publically exposed
34. Swiggy Jira filters publically exposed
35. Informatica Jira dashboard publically exposed
36. Western union staff data exposed
37. Luminate yahoo acquisition having Jira filters publically exposed
38. These publically available filters and dashboards were providing details such as employees roles, employees names, their mail id, upcoming milestones, secret project, and features. While the user picker functionality discloses internal user data. Useful information for a competitor company to get to know about the kind of upcoming milestones or secret projects their competitor is working upon. Even an attacker can gain some information from this and tie it with some other type of attacks. Clearly, it is something which shouldn’t be public. Not a security issue but more of a privacy issue.
39. I reported this to various companies, some rewarded me, some fixed it while some are still living with it. While it is more of a misconfiguration issue which Atlassian(JIRA) must take care of and be more explicitly clear about what is meant by “Any logged-in user” whether it is any logged-in user of JIRA or just a logged-in user belonging to a specific Jira company account.
40. Filter visibility settings and set the visibility to “Private” by default and if anyone wants to make their dashboard or filter public, they have to explicitly go to the setting and change them. While user picker functionality settings must also be taken into account.

DEV-5 Commercial off-the-shelf Risk

Source web site: http://blog.talosintelligence.com/2017/09/avast-distributes-malware.html

Author: Edmund Brumaghin, Ross Gibb, Warren Mercer, Matthew Molyett, and Craig Williams

CCleanup: A Vast Number of Machines at Risk

DO NOT FORGET YOU ARE REPRESENTING Piriform Inc

1. Supply chain attacks are a very effective way to distribute malicious software into target organizations. This is because with supply chain attacks, the attackers are relying on the trust relationship between a manufacturer or supplier and a customer. This trust relationship is then abused to attack organizations and individuals and may be performed for a number of different reasons. The Nyetya worm that was released into the wild earlier in 2017 showed just how potent these types of attacks can be. Frequently, as with Nyetya, the initial infection vector can remain elusive for quite some time. Luckily with tools like AMP the additional visibility can usually help direct attention to the initial vector.
2.
3.
4. Talos recently observed a case where the download servers used by software vendor to distribute a legitimate software package were leveraged to deliver malware to unsuspecting victims. For a period of time, the legitimate signed version of CCleaner 5.33 being distributed by Avast also contained a multi-stage malware payload that rode on top of the installation of CCleaner. CCleaner boasted over 2 billion total downloads by November of 2016 with a growth rate of 5 million additional users per week. Given the potential damage that could be caused by a network of infected computers even a tiny fraction of this size we decided to move quickly. On September 13, 2017 Cisco Talos immediately notified Avast of our findings so that they could initiate appropriate response activities. The following sections will discuss the specific details regarding this attack.
5.
6. On September 13, 2017 while conducting customer beta testing of our new exploit detection technology, Cisco Talos identified a specific executable which was triggering our advanced malware protection systems. Upon closer inspection, the executable in question was the installer for CCleaner v5.33, which was being delivered to endpoints by the legitimate CCleaner download servers. Talos began initial analysis to determine what was causing this technology to flag CCleaner. We identified that even though the downloaded installation executable was signed using a valid digital signature issued to Piriform, CCleaner was not the only application that came with the download. During the installation of CCleaner 5.33, the 32-bit CCleaner binary that was included also contained a malicious payload that featured a Domain Generation Algorithm (DGA) as well as hardcoded Command and Control (C2) functionality. We confirmed that this malicious version of CCleaner was being hosted directly on CCleaner's download server as recently as September 11, 2017.
7. In reviewing the Version History page on the CCleaner download site, it appears that the affected version (5.33) was released on August 15, 2017. On September 12, 2017 version 5.34 was released. The version containing the malicious payload (5.33) was being distributed between these dates. This version was signed using a valid certificate that was issued to Piriform Ltd by Symantec and is valid

through 10/10/2018. Piriform was the company that Avast recently acquired and was the original company who developed the CCleaner software application.

8. A second sample associated with this threat was discovered. This second sample was also signed using a valid digital certificate, however the signing timestamp was approximately 15 minutes after the initial sample was signed.
9. The presence of a valid digital signature on the malicious CCleaner binary may be indicative of a larger issue that resulted in portions of the development or signing process being compromised. Ideally this certificate should be revoked and untrusted moving forward. When generating a new cert care must be taken to ensure attackers have no foothold within the environment with which to compromise the new certificate. Only the incident response process can provide details regarding the scope of this issue and how to best address it.
10. Given the presence of this compilation artifact as well as the fact that the binary was digitally signed using a valid certificate issued to the software developer, it is likely that an external attacker compromised a portion of their development or build environment and leveraged that access to insert malware into the CCleaner build that was released and hosted by the organization. It is also possible that an insider with access to either the development or build environments within the organization intentionally included the malicious code or could have had an account (or similar) compromised which allowed an attacker to include the code.
11. It is also important to note that while previous versions of the CCleaner installer are currently still available on the download server, the version containing the malicious payloads has been removed and is no longer available.

CNS-1 Layer 1 2 Wireless

CISSP-CNS-1-CASE-201

Source:https://threatpost.com/poisontap-steals-cookies-drops-backdoors-on-password-protected-computers/121986/

1. Samy Kamkar's latest hacking device, PoisonTap, can steal HTTP cookies from millions of websites and install persistent web-based backdoors.
2. Even locked, password-protected computers are no rival for Samy Kamkar and his seemingly endless parade of gadgets.
3. His latest, PoisonTap, is a $5 Raspberry Pi Zero device running Node.js that's retrofitted to emulate an Ethernet device over USB. Assuming a victim has left their web browser open, once plugged in to a machine, the device can quietly fetch HTTP cookies and sessions from millions of websites, even if the computer is locked.
4. If that alone doesn't sound like Mr. Robot season three fodder, the device can also expose the machine's internal router and install persistent backdoors, guaranteeing an attacker access long after they've removed the device from a USB slot.
5. "[The device] produces a cascading effect by exploiting the existing trust in various mechanisms of a machine and network, including USB, DHCP, DNS, and HTTP, to produce a snowball effect of information exfiltration, network access and installation of semi-permanent backdoors," Kamkar said Wednesday in a writeup of PoisonTap.
6. According to Kamkar, who released an "Applied Hacking" video in tandem with the writeup, Windows and OS X machines recognize his device and load it as a low-priority network device. The device engages with DHCP requests, gives the machine an IP address, and allows the machine to re-route all internet traffic through PoisonTap.

7. “As long as a browser is running on the machine and an HTTP request is made automatically – such as through an ad, AJAX request, or other dynamic web content, which happens on most sites, even when the browser is entirely in the background, PoisonTap intercepts the request and responds with attack code that’s interpreted by the browser,” Kamkar says in the video.
8. https://youtu.be/Aatp5gCskvk

9. In addition to being able to siphon up internet traffic, PoisonTap installs a remotely accessible web-based backdoor in the HTTP cache of many domains. It only takes a few seconds for PoisonTap to do its job; the Websocket-based backdoors linger after the attacker has removed the device, allowing attackers with a command and control server an easy way into the machine after the initial hack.
10. "Whenever the websocket is open, the attacker can remotely send commands to the victim and force their browser to execute JavaScript code," Kamkar says.
11. The contraption also exposes victims' routers, making it so the attacker can remotely force HTTP requests and proxy back responses using the victim's cookies on backdoored sites without the user being any the wiser.
12. "Because a backdoor is left on each domain, this allows the attacker to remotely force the backdoored browser to perform same-origin requests (AJAX GET/POSTs) on virtually any major domain, even if the victim does not currently have any open windows to that domain," Kamkar wrote.
13. Because PoisonTap exposes the router – something the attacker may not have even had access to in the first place – it can lead to a wave of secondary attacks.
14. If it was running default admin credentials, the attacker could use it to overwrite DNS servers, or expose additional authentication vulnerabilities, he warns.
15. In addition to bypassing password protected lock screens, the device breaks a handful of mechanisms designed to safeguard browsers, including same origin policy, cross-origin resource sharing (CORS) and DNS pinning, to name a few.
16. As Kamkar does for most of his research, he's published the PoisonTap source code for free
17. https://github.com/samyk/poisontap
18. Web servers looking to thwart PoisonTap attacks should use HTTPS exclusively, in addition to HSTS to prevent any HTTPS downgrade attacks, according to Kamkar.
19. Kamkar said users looking to preventing a PoisonTap attack can do away with USB and Thunderbolt ports all together; adding cement to the ports "can be effective," he writes.

20. A less drastic move – making sure users close their browser before walking away from their machines – can be effective as well, Kamkar says, but impractical.
21. Kamkar told Threatpost he was sleep deprived on a plane one morning when he came up with the idea for the device.
22. “Was sleep deprived on a plane one morning and considered that maybe you can gain network access on a locked machine, tested it, it worked,” Kamkar said, adding that from there he “just started building automated network attacks together for a while until it seemed to be an effect demonstration of why a locked computer is not actually secure.
23. The device is the latest in a long line of nifty Kamkar devices over the last several years, including OpenSesame, which opened garage doors with a $12 child’s toy, KeySweeper, which allowed Kamkar to passively sniff, decrypt, and record keystrokes on Microsoft wireless keyboards, and OwnStar, a device that allowed him to intercept traffic from phones to vehicles running OnStar.
24. The Raspberry Pi, a credit card-sized single-board computer, has figured into several of those devices. With PoisonTap, Kamkar only added a micro-USB cable and microSD card to the existing 65 mm x 30 mm base.

CNS-2 Layer 3 4 Firewalls

CISSP-CASE-CNS-2-20090212

Source: (DEAD) http://www.cpni.gov.uk/Products/technicalnotes/Feb-09-security-assessment-TCP.aspx

1. The United Kingdom's Centre for the Protection of National Infrastructure has just released the document "Security Assessment of the Transmission Control Protocol (TCP)", on which I have had the pleasure to work during the last few years.
2. The motivation to produce this document is explained in the Preface of the document as follows: The TCP/IP protocol suite was conceived in an environment that was quite different from the hostile environment they currently operate in. However, the effectiveness of the protocols led to their early

adoption in production environments, to the point that to some extent, the current world's economy depends on them.

3. While many textbooks and articles have created the myth that the Internet protocols were designed for warfare environments, the top level goal for the DARPA Internet Program was the sharing of large service machines on the ARPANET. As a result, many protocol specifications focus only on the operational aspects of the protocols they specify, and overlook their security implications.
4. While the Internet technology evolved since it early inception, the Internet's building blocks are basically the same core protocols adopted by the ARPANET more than two decades ago.
5. During the last twenty years, many vulnerabilities have been identified in the TCP/IP stacks of a number of systems. Some of them were based on flaws in some protocol implementations, affecting only a reduced number of systems, while others were based in flaws in the protocols themselves, affecting virtually every existing implementation. Even in the last couple of years, researchers were still working on security problems in the core protocols.
6. The discovery of vulnerabilities in the TCP/IP protocol suite usually led to reports being published by a number of CSIRTs (Computer Security Incident Response Teams) and vendors, which helped to raise awareness about the threats and the best mitigations known at the time the reports were published. Unfortunately, this also led to the documentation of the discovered protocol vulnerabilities being spread among a large number of documents, which are sometimes difficult to identify.
7. For some reason, much of the effort of the security community on the Internet protocols did not result in official documents (RFCs) being issued by the IETF (Internet Engineering Task Force). This basically led to a situation in which "known" security problems have not always been addressed by all vendors. In addition, in many cases vendors have implemented quick "fixes" to the identified vulnerabilities without a careful analysis of their effectiveness and their impact on interoperability.
8. Producing a secure TCP/IP implementation nowadays is a very difficult task, in part because of the lack of a single document that serves as a security roadmap for the protocols. Implementers are faced with the hard task of identifying relevant documentation and differentiating between that which

provides correct advice, and that which provides misleading advice based on inaccurate or wrong assumptions.

9. There is a clear need for a companion document to the IETF specifications that discusses the security aspects and implications of the protocols, identifies the existing vulnerabilities, discusses the possible countermeasures, and analyses their respective effectiveness.
10. This document is the result of a security assessment of the IETF specifications of the Transmission Control Protocol (TCP), from a security point of view. Possible threats are identified and, where possible, countermeasures are proposed. Additionally, many implementation flaws that have led to security vulnerabilities have been referenced in the hope that future implementations will not incur the same problems.
11. This document does not aim to be the final word on the security aspects of TCP. On the contrary, it aims to raise awareness about a number of TCP vulnerabilities that have been faced in the past, those that are currently being faced, and some of those that we may still have to deal with in the future. Feedback from the community is more than encouraged to help this document be as accurate as possible and to keep it updated as new vulnerabilities are discovered.

CNS-3 Layer 5 6 7 VPN

CISSP-CNS-3-CASE-20170829

Source: https://www.csoonline.com/article/3223951/dnssec-key-signing-key-rollover-are-you-ready.html

1. Internet Corporation for Assigned Names and Numbers (ICANN), which administers the Internet namespace, has been engaged in a multi-year effort to update the cryptographic keys used to protect the Domain Name System (DNS) from abuse. The new root zone “key signing key” (KSK) used to secure DNS was generated last year.
2. Internet service providers, hardware manufacturers, and enterprises that operate their own recursive name servers and use Domain Name System Security Extensions (DNSSec) validation to protect their domains, needed to update their system with the public part of the key pair by October 11. On that day, ICANN planned to “rollover,” to start using the new root zone key signing key sign domains. If the systems aren’t updated with the new public key, when the old key is finally revoked in 2018, DNSSEC validations will fail and cause DNS to break.
3. Based on data ICANN received from the root zone servers, a “significant number” of resolvers used by ISPs and large network operators are not ready to use the new keys. Updating the encryption keys used to secure the Internet’s foundational servers is an exceptionally dicey challenge, so it makes sense to change the deadline and give network operators more time. Don’t knock as many as 60 million people offline.
4. "It would be irresponsible to proceed with the rollover after we have identified these new issues that could adversely affect its success and could adversely affect the ability of a significant number of end users," says Goran Marby, CEO of ICANN. “We would rather proceed cautiously and reasonably.”
5. ICANN did not announce a new deadline, but says the rollover will be rescheduled to the first quarter of 2018. The administrative body will use the extension to reach out to those ISPs and network operators it had identified to work with them to resolve issues.

6. Missing the deadline would have serious consequences for regular Internet users. ICANN estimates about 750 million people browse the web using information provided by DNSSEC servers. “Those who suffer will be those whose recursive name server operators performing DNSSec validation but which have not correctly received, stored, and configured the new key during its pre-publication period,” says internet security pioneer Paul Vixie, currently the CEO of Farsight Security and longtime DNS and DNSSEC developer.
7. "DNSSEC deployment has been slow, and I expected that the early adopters would be those most ready to handle something like a key rollover event," says Vixie. "ICANN has displayed a commendable abundance of caution throughout the rollover planning and execution, and one of their gut checks was to measure the adoption rates of the new key they're hoping to roll over to. They found slightly more than one out of 20 DNSSEC-capable networks to only have the old key. That's too high, and so they've postponed the rest of the execution of the rollover plan until they can resolve this adoption problem."
8. DNSSEC’s ultimate root key
9. The Domain Name System (DNS) acts as the internet’s phone book, translating IP addresses to easy-to-remember domain names. However, the distributed nature of DNS makes the system vulnerable to hijacking as users get diverted to fraudulent sites through DNS cache poisoning or DNS spoofing. The DNSSEC protocol, introduced in 2010, thwarts hijacking by using cryptographic key pairs to verify and authenticate the results of a DNS lookup. If the DNS response has been tampered with, the keys don’t match and the browser returns an error instead of sending users to the incorrect destination.
10. A modern, innovative approach to security is critical to reducing risk across the enterprise. Here’s how CISOs can keep pace with the ever-changing threat landscape.
11. DNSSEC works as a hierarchy with different bodies responsible for each layer and signing the key of the entities in the layer below. The key signing key is a cryptographic public-private key pair, and the root zone KSK secures the topmost layer of the hierarchy, the anchor point for DNSSEC validation.

12. DNS resolvers rely on the chain of trust the KSK builds from the root zone down through each layer of the system to verify they're getting good results to their queries. That a given IP address really does resolve to that domain.
13. There is nothing wrong with the key—it hasn't been stolen or tampered with—but it is good security practice to periodically rotate the signing key so that even if it falls into the wrong hands, everyone is already using the newer, stronger key. There is no reason to wait for something bad to happen—for the key to be cracked, for example—before updating to a newer, stronger, key.
14. "Updating the DNSSEC KSK is a crucial security step, similar to updating a PKI Root Certificate," the United States Computer Emergency Response Team (US-CERT) wrote in a recent advisory. "Maintaining an up-to-date Root KSK as a trust anchor is essential to ensuring DNSSEC-validating DNS resolvers continue to function after the rollover."
15. Keeping pace with a rapidly shifting threat landscape – and a growing skills gap – requires CISOs to take a fresh approach to security strategy and operations. Here's how.
16. Rollover process hits a glitch
17. ICANN and volunteers from the global technical community spent the last five years developing, reviewing, refining, and testing the rollover plan before kicking off the process last year by generating the new KSK. In July, ICANN published plans outlining the steps required to rollover the KSK so that ISPs, enterprise network operators, hardware manufacturers, and others performing DNSSEC validation can update their systems with the public part of the key pair. Even though the new key signing key will start being used to sign domains in October, DNSSEC will support both the old and new keys until early 2018 to give everyone time to complete the rollover process.
18. "There may be multiple reasons why operators do not have the new key installed in their systems: some may not have their resolver software properly configured and a recently discovered issue in one widely used resolver program appears to not be automatically updating the key as it should, for reasons that are still being explored," ICANN says.

19. It could also be an awareness issue—that enough operators were not aware of the deployment process. “ICANN is on schedule to begin using the private portion [for signing domains] shortly,” Vixie says.
20. The most challenging part of this multistep, multi-year process was overseeing the plan’s development, seeking broad review and approval, and obtaining approvals from multiple internet governance organizations to execute the plan, Vixie says. The ICANN Office of the CTO has already done the hard part; the technical implementation and publicizing the process is the easy part.
21. Many organizations operate validating name servers including ISPs, enterprises, universities, small offices, and even hobby users. Most of these recursive name servers have likely already received out-of-band key updates from their vendors through their normal software update process—or are scheduled to receive one over the next few weeks.
22. ICANN advises that network operators and ISPs ensure their systems are ready for the new rollover data, and to make use of its testing platform to ensure resolvers are properly configured. Administrators need to manually update DNSSEC validators lacking RFC 5011 support (automated updates) as they would not automatically receive, store, and configure the new key. Any DNSSEC validators offline during this period can theoretically update itself after the new key is in full effect and get up to speed, but that will happen only if those validators are online before March, before the old key is officially retired.
23. It is theoretically possible for a DNSSEC validator to miss all the update opportunities and not receive the new key from its root trust anchor. If that is the case, that validator will fail DNSSEC validation on all responses received from root name servers come March 2018 when the old key is revoked. That scenario is most likely to happen with test labs and not production networks, Vixie says.
24. Verify the updates
25. While most name servers are being updated automatically, every recursive validating name server operator should check by hand to ensure that the new key has been received, stored, and configured for validation use. There is no need to wait until DNSSEC validation fails to discover the update was incomplete.

26. DNSSEC validation is mandatory for federal agencies, and adoption in the private sector has been slow. Even so, ICANN estimates that 750 million people worldwide rely on DNSSEC validation and will be affected by the rollover. While it's theoretically possible to estimate how many enterprises are ready for the deadline, the number of public-facing recursive name servers performing DNSSEC validation is so small it would be "useless for predicting the results for the full population," Vixie says.
27. ICANN decided to slow down because there were too many operators that were not ready. It will continue evaluating and reassessing, but at this point, it's up to everyone else in the trust chain to do their part. "In this sense, we are benefitting from the fairly sparse and narrow adoption of DNSSEC," Vixie says, noting that the community is dominated by late adopters and those who understand the issues in detail. "Only an early adopter who has been living on Mars for the last few years could be expected to have trouble."
28. Vixie says he was "extremely impressed" at how the rollover implementation plan was conceived and executed. The fact that the rollover is proceeding according to plan makes it possible to have this kind of key rotation done on a regular basis. The next rollover is expected in 2022.
29. "I predicted early on that this could not be done without far more delay and pain than I've seen," Vixie says. "In the near future, it [the rotation] will no longer even be newsworthy."

CNS-4 Telephony

CISSP-CASE-CNS-4-20090406

Source: https://gcn.com/articles/2009/04/06/nist-dnssec-in-play.aspx

How NIST put DNSsec into play

By William Jackson

1. The digital signing of the .gov top-level domain in February completed the first step of the implementation of DNS Security Extensions (DNSSEC) in the government's Internet space. The next step is for agencies to sign their second-level domains by the end of the year.

2. It is not a simple process, which is one of the main reasons DNSSEC has not been widely deployed across the Internet’s Domain Name System despite its well-known vulnerabilities.
3. “There is a steep learning curve in deploying DNSSEC,” said Scott Rose, a computer scientist at the National Institute of Standards and Technology, the agency that is writing the rules for deployment. DNS typically takes little management. However, once DNSSEC is deployed, there is the constant chore of generating and managing cryptographic keys and signing and re-signing data.
4. But NIST is doing more than writing about it. The agency has had DNSSEC deployed in the NIST.gov domain for more than a year.
5. “We’re ready now,” Rose said. “We’re just ironing out and hardening processes,” refining best practices and changing security parameters so that acceptable levels of security can be maintained under the weight of DNSSEC management.
6. That is not to say that the process was — or is — easy, or that the full benefits of DNSSEC will be realized soon.
7. Robert Toense, an electronics engineer in NIST’s Office of the Chief Information Officer, said it still takes about 30 minutes a day to sign the updated zones, and “there is no well-defined method for exchanging keys” so that chains of trust can be established. And you don’t get the full benefits having digitally signed DNS data without chains of trust. “That’s some of the work that's going on now.”
8. Still, if agencies examine how DNS is being used in their network architecture and set their sights on reaching minimum requirements, they can meet the Office of Management and Budget’s Dec. 31 deadline for DNSSEC deployment.
9. The 26-year-old DNS maps domain names to IP addresses and underlies nearly all Internet activities. DNS replaced the Host Table naming system, which dates back to the Internet’s predecessor, ARPAnet, and predates the implementation of TCP/IP. A centrally managed file maintained by the Network Information Center at Stanford University was updated every week or so to map host names to locations.

10. That approach was adequate in the pioneering days of the interconnected network, but it would not scale to the levels needed as the Internet grew. DNS is a distributed, hierarchical scheme that lets everyone look up addresses without having to maintain a separate copy.

11. DNS has been successful at scaling to serve the Internet community, but like the rest of the infrastructure, it was not built with security in mind. Experts have been aware of the possibility of hackers poisoning DNS caches to misdirect or hijack traffic for some time, but last July, a significant flaw in the protocols was announced that made securing the system more urgent.

12. DNSSEC enables DNS queries and responses to be digitally signed using cryptographic keys so they can be authenticated and are harder to spoof or manipulate. In late 2006, new federal information security requirements called for agencies to use DNSSEC signatures on DNS servers that are classified as moderate- or high-impact information systems. Little implementation was done, however, in part because most servers were classified as low-impact and in part because managing DNS can be complicated. It involves cryptographic keys and digital signatures that must be refreshed regularly if they are to remain secure.

13. In the wake of last July's vulnerability announcement, OMB issued a memo requiring deployment of DNSSEC at the top-level .gov domain by January 2009. The General Services Administration, the lead agency in the program, missed the deadline by about a month but announced that DNSSEC became operational in the .gov domain on Feb. 28.

14. Agencies now have until the end of the year to sign their zones, although NIST had signed its zones well before OMB issued its mandate.

15. "We're NIST, we should be doing things on the leading edge," Toense said. "But there was always the pain of doing it. Then the government came along with an incentive" with the original 2007 deadline.

16. Because NIST was responsible for establishing the guidelines for deploying DNSSEC, it seemed as though the agency should have some practical experience, Toense said. "We were feeling that most of the government wasn't going to make it, but NIST was going to do its damnedest."

17. One of the first steps was to examine the NIST network to find out how many zones it had.

18. “We had partitioned things so that we would have to do a lot of signing,” Toense said. Fortunately, the agency no longer needed to maintain most of those partitions. “I spent a lot of time collapsing zones,” reducing the number from about 200 to about 15 zones for which keys would have to be managed.
19. But that was not the only challenge. The NIST zones have about 10,000 records that must be updated regularly, which is not a very big database. “In non-DNSSEC terms, that was not difficult to manage.” But when it came time to sign them on a powerful server that could handle routine DNS work at idling speed, the signing process took 100 percent of the server’s CPU cycles for 15 minutes. And the process had to be performed twice for every update because domain-to-IP address lookups are handled separately from IP address-to-domain lookups. That means every time the records are updated, it requires 30 minutes of DNSSEC signing, and a batch update is done nearly every day.
20. That burden could be eased by dynamic DNSSEC, which would allow updates to be signed on the fly rather than re-signing the zone during batch updates, but at this point there is no standard support for dynamic DNSSEC. And the entire zone will have to be re-signed eventually anyway. Another solution could be dedicated DNSSEC appliances, which have begun to appear and could automate much of the process.
21. “We’re working with some of them,” Toense said. “None of them have a complete solution yet that I’m aware of. But they are all trying very hard, realizing it is not a simple problem.”
22. The appliances are being tested on a laboratory network called the Secure Naming Infrastructure Pilot (SNIP), which is designed to give administrators some real-world experience managing a signed DNS zone on a live network.
23. “We have set up a test bed at dnsops.gov,” Rose said. “The main purpose is to give government agencies an environment they can test in.” A test bed for vendors to try products has been set up at dnsops.biz.
24. Among the appliances being tested on SNIP is Secure64 Software’s DNS Signer, which automates key generation, key rollover, zone signing and re-signing. It was developed with a Homeland Security Department grant and is built on the company’s SourceT secure micro-operating system.

25. “You have to think about the security of the signing keys,” said Mark Beckett, vice president of marketing at Secure64. DNS Signer keeps the keys online in secure boxes within SourceT so that the signing processes can be automated.

26. Afilias Ltd., the registry for the .info and .aero top-level domains, is taking another approach. The company plans to launch its 1-Click DNSSEC later this year as an add-on to its Managed DNS service. It would automate creation and management of keys and signing and the distribution of public keys to parent zones — all as a managed service rather than an appliance.

27. Right now, the lack of standards for exchanging keys with parent zones is a stumbling block to establishing the chains of trust that can make DNSSEC really effective, Toense said.

28. In the meantime, “you can be a trust island,” he said, without exchanging keys with other zones. That is all that the mandate currently requires, and that is what NIST has done. “Local key management was all we needed to do.”

29. But that will change soon, he predicted. The need for improved security will spur the adoption of standards and best practices once zones are being signed.