Colorado Springs ISSA March Security Event

The conference will be held at the Crowne Plaza Hotel, 2886 South Circle Drive Colorado Springs, CO 80906 on March 8, 2013, from 8:00 AM to 5:00 PM.

Pre-Registration Paid in Full $45 for ISSA® Members
Pre-Registration Paid at Door $50 for ISSA® Members
Registration Paid at Door $65 for ISSA® Members

A continental breakfast and full lunch is included. Eight CPEs will be awarded, and attendees are eligible for door prizes, including a valuable door prize from Econet. Happy Hour for attendees will be hosted by Barracuda Networks and Envision Software from 5 – 6 PM.

Additional details will be forthcoming.

Please visit www.issa-cos.org for registration information.
How it feels to be stalked


Some years ago, I found myself, to my surprise, the victim of a campaign of malicious e-mail stalking and online defamation by a former M.F.A. student.

Nasreen (all names here have been changed) was a talented writer, and she had an interesting story to tell about her family's experiences in Iran at the time of the revolution. During the term I taught her, I'd made it clear I thought highly of her work.

Two years after she graduated, she contacted me, asking me to help edit her novel. I was too busy at the time, but I put her in touch with my agent, who in turn introduced her to a freelance editor. Nasreen seemed grateful for the help, and an amicable correspondence began between us.

At a certain point her e-mails took an amorous turn. I told her I was happily married and not interested in having an affair. She seemed to take it well, and our friendly correspondence soon resumed.

But gradually the volume of her e-mails increased to several a day, and after a while I realized I was becoming the object of an obsession. As tactfully as I could, I asked her to ease up, but to no avail.

A deluge of e-mails poured into my inbox over the next few months. I deleted most without reading them. Those that I did read seemed innocuous, though the sheer quantity was disturbing. And then, on a July evening in 2007, they turned abruptly from banter and gossip to venomous hate mail (much of it violently anti-Semitic), along with accusations that I had plagiarized her work and had affairs with her classmates (though not with her).

Soon after that first volley, Janice (my agent) called, sounding upset. For several days, she had been receiving strange e-mails about me from Nasreen, and she was concerned for her safety. The e-mails contained the same baseless accusations of plagiarism, accompanied by threats of "hell to pay" if Janice and I connived to "steal" any more of Nasreen's work. Later that day, Nasreen began threatening Paula, the editor to whom Janice had introduced Nasreen.

"You all play a part in unleashing the fury," Nasreen wrote. Soon after, with this "fury" now apparently reaching for terms strong enough to account for its own escalating intensity, Nasreen brought on one of those words that scorch everything they come near. The word was "rape," and even though she used it figuratively rather than literally, I felt immediately the potency of its touch, as if I'd been splashed with acid: "I say if I can't write my book and get emotionally and verbally raped by James Lasdun, a Jew disguising himself as an English-American, well then, the Holocaust Industry Books should all be banned as should the films."

It's one thing to be abused in private: You experience it almost as an internal event, not so different from listening to the more punitive voices in your own head. But to have other people brought into the drama is another matter. It confers a different order of reality on the abuse: fuller and more objective. This strange, awful thing really is happening to you, and people are witnessing it.

Along with the accusations of theft, Janice had also received details of my supposed (but equally fictitious) affairs with Nasreen's former classmates, complete with descriptions of various kinky sexual practices that Nasreen claimed to have heard I went in for. (She had an uncanny way with that transparent yet curiously effective device of rumor, the unattributed source: "I'm told he ..." "I hear he ..." "Everyone knows he ..." )

Read the rest here:
Pupil expelled from Montreal college after finding ‘sloppy coding’ that compromised security of 250,000 students personal data

Ethan Cox, National Post Staff, January 21, 2013

A student has been expelled from Montreal's Dawson College after he discovered a flaw in the computer system used by most Quebec CEGEPs (General and Vocational Colleges), one which compromised the security of over 250,000 students' personal information.

Ahmed Al-Khabaz, a 20-year-old computer science student at Dawson and a member of the school’s software development club, was working on a mobile app to allow students easier access to their college account when he and a colleague discovered what he describes as “sloppy coding” in the widely used Omnivox software which would allow “anyone with a basic knowledge of computers to gain access to the personal information of any student in the system, including social insurance number, home address and phone number, class schedule, basically all the information the college has on a student.”

“I saw a flaw which left the personal information of thousands of students, including myself, vulnerable,” said Mr. Al-Khabaz. “I felt I had a moral duty to bring it to the attention of the college and help to fix it, which I did. I could have easily hidden my identity behind a proxy. I chose not to because I didn’t think I was doing anything wrong.”

After an initial meeting with Director of Information Services and Technology François Paradis on Oct. 24, where Mr. Paradis congratulated Mr. Al-Khabaz and colleague Ovidiu Mija for their work and promised that he and Skytech, the makers of Omnivox, would fix the problem immediately, things started to go downhill.

Two days later, Mr. Al-Khabaz decided to run a software program called Acunetix, designed to test for vulnerabilities in websites, to ensure that the issues he and Mija had identified had been corrected. A few minutes later, the phone rang in the home he shares with his parents.

“It was Edouard Taza, the president of Skytech. He said that this was the second time they had seen me in their logs, and what I was doing was a cyber attack. I apologized, repeatedly, and explained that I was one of the people who discovered the vulnerability earlier that week and was just testing to make sure it was fixed. He told me that I could go to jail for six to twelve months for what I had just done and if I didn’t agree to meet with him and sign a non-disclosure agreement he was going to call the RCMP and have me arrested. So I signed the agreement.”

The agreement prevented Mr. Al-Khabaz from discussing confidential or proprietary information he found on Skytech servers, or any information relating to Skytech’s servers or how he accessed them. The agreement also prevented Mr. Al-Khabaz from discussing the existence of the non-disclosure pact itself, and specified that if his actions became public he would face legal consequences.

When reached for comment Mr. Taza acknowledged mentioning police and legal consequences, but denied having made any threats, and suggested that Mr. Al-Khabaz had misunderstood his comments.

“All software companies, even Google or Microsoft, have bugs in their software,” said Mr. Taza. “These two students discovered a very clever security flaw, which could be exploited. We acted immediately to fix the problem, and were able to do so before anyone could use it to access private information.”

Taza explained that he was quite pleased with the work the two students did identifying problems, but the testing software Mr. Al-Khabaz ran to verify the system was fixed crossed a line.

Read the rest here:
January 9, CNNMoney – (National) **Hacker hits on U.S. power and nuclear targets spiked in 2012.** America's power, water, and nuclear systems are increasingly being targeted by cybercriminals seeking to gain access to some of the nation's most critical infrastructure. The number of attacks reported to a U.S. Department of Homeland Security cybersecurity response team grew by 52% in 2012, according to a recent report from the team. There were 198 attacks brought to the agency's attention last year, several of which resulted in successful break-ins. An earlier report from DHS sketched in details on some of those successes. An unidentified group of hackers targeting natural gas pipeline companies gained access to the corporate systems of several of their targets and “exfiltrated” -- that's security-speak for “stole” -- data on how their control systems work. Source: [http://money.cnn.com/2013/01/09/technology/security/infrastructure-cyberattacks/](http://money.cnn.com/2013/01/09/technology/security/infrastructure-cyberattacks/)

January 17, Help Net Security – (National) **Many Fed smartphones have zero password protection.** A Government Accountability Office report stated Federal Government-issued mobile devices are susceptible to hacking due to their lack of password protection. Out of half of all Federal employees, one in three is not protected and 85 percent contain downloaded unrestricted apps that make the devices more vulnerable to attacks. Sponsored by EMC, VMware, Cisco, and Carahsoft, the report reveals that more than half of smartphone users in the Federal government use their personal smartphone for job-related tasks. Out of this group, one in three workers do not have password protection. The Digital Government Strategy calls for embracing the opportunity of the digital world while ensuring mobility, security, and efficiency. As Federal employees continue to reap productivity gains as a result of using mobile devices, government data is potentially at risk. Source: [http://www.net-security.org/secworld.php?id=14254](http://www.net-security.org/secworld.php?id=14254)

January 16, NY Times — (International) **Rights Group Reports on Abuses of Surveillance and Censorship Technology.** A Canadian human rights monitoring group has documented the use of American-made Internet surveillance and censorship technology by more than a dozen governments, some with harsh human rights policies like Syria, China and Saudi Arabia. The Citizen Lab Internet research group, based at the Munk School of Global Affairs at the University of Toronto, used computer servers to scan for the distinctive signature of gear made by Blue Coat Systems of Sunnyvale, Calif. It determined that Egypt, Kuwait, Qatar, Saudi Arabia and the United Arab Emirates employed a Blue Coat system that could be used for digital censorship. The group also determined that Bahrain, China, India, Indonesia, Iraq, Kenya, Kuwait, Lebanon, Malaysia, Nigeria, Qatar, Russia, Saudi Arabia, South Korea, Singapore, Thailand, Turkey and Venezuela used equipment that could be used for surveillance and tracking. The authors said they wanted to alert the public that there was a growing amount of surveillance and content-filtering technology distributed throughout the Internet. The technology is not restricted from export by the State Department, except to countries that are on embargo lists, like Syria, Iran and North Korea. Source: [http://www.nytimes.com/2013/01/16/business/rights-group-reports-on-abuses-of-surveillance-and-censorship-technology.html?_r=0](http://www.nytimes.com/2013/01/16/business/rights-group-reports-on-abuses-of-surveillance-and-censorship-technology.html?_r=0)

January 18, 2013, SC Magazine— (International) **XSS, password flaws found in popular ESPN app.** Researchers have discovered two security holes in a popular mobile app used to track sports news and scores, leaving users vulnerable to having their data exposed. On Thursday, Michael Sutton, vice president of security research at Zscaler, published a blog post detailing flaws in the popular app ESPN ScoreCenter. The San Jose, Calif.-based cloud security firm discovered that the app was vulnerable both to a common coding flaw known as cross-site scripting (XSS), as well as a weakness through which an attacker could access usernames and passwords when users set up their accounts. Source: [http://www.scmagazine.com/xss-password-flaws-found-in-popular-espn-app/article/276723/](http://www.scmagazine.com/xss-password-flaws-found-in-popular-espn-app/article/276723/)

January 29, Network World— (International) **5 years after major DNS flaw is discovered, few US companies have deployed long-term fix.** Very few U.S. online retailers, internet service providers (ISP), and financial institutions have implemented a major vulnerability in the Domain Name System (DNS), five years after the vulnerability was discovered. Source: [http://www.networkworld.com/news/2013/012913/dnssec-266197.html](http://www.networkworld.com/news/2013/012913/dnssec-266197.html)
Cybersleuths Uncover 5-Year Spy Operation Targeting Governments, Others

An advanced and well-orchestrated computer spy operation that targeted diplomats, governments and research institutions for at least five years has been uncovered by security researchers in Russia.

The highly targeted campaign, which focuses primarily on victims in Eastern Europe and Central Asia based on existing data, is still live, harvesting documents and data from computers, smartphones and removable storage devices, such as USB sticks, according to Kaspersky Lab, the Moscow-based antivirus firm that uncovered the campaign. Kaspersky has dubbed the operation “Red October.”

While most of the victims documented are in Eastern Europe or Central Asia, targets have been hit in 69 countries in total, including the U.S., Australia, Ireland, Switzerland, Belgium, Brazil, Spain, South Africa, Japan and the United Arab Emirates. Kaspersky calls the victims “high profile,” but declined to identify them other than to note that they’re government agencies and embassies, institutions involved in nuclear and energy research and companies in the oil and gas and aerospace industries.

“The main purpose of the operation appears to be the gathering of classified information and geopolitical intelligence, although it seems that the information-gathering scope is quite wide,” Kaspersky notes in a report released Monday. “During the past five years, the attackers collected information from hundreds of high-profile victims, although it’s unknown how the information was used.”

The attackers, believed to be native Russian-speakers, have set up an extensive and complex infrastructure consisting of a chain of at least 60 command-and-control servers that Kaspersky says rivals the massive infrastructure used by the nation-state hackers behind the Flame malware that Kaspersky discovered last year.

But the researchers note that the Red October attack has no connection to Flame, Gauss, DuQu or other sophisticated cyber-spy operations Kaspersky has examined in recent years.

The attack also shows no signs yet of being the product of a nation-state and may instead be the work of cybercriminals or freelance spies looking to sell valuable intelligence to governments and others on the black market, according to Kaspersky Lab senior security researcher Costin Raiu.

The malware the attackers use is highly modular and customized for each victim, who are assigned a unique ID that is hardcoded into the malware modules they receive.

“The victim ID is basically a 20-hex digit number,” Raiu says. “But we haven’t been able to figure out any method to extract any other information from the victim ID.... They are compiling the modules right before putting them into the booby-trapped documents, which are also customized to the specific target with a lure that can be interesting to the victim. What we are talking about is a very targeted and very customized operation, and each victim is pretty much unique in what they receive.”

The statistics on countries and industries are based on Kaspersky customers who have been infected with the malware and on victim machines that contacted a Kaspersky sinkhole set up for some of the command-and-control servers.

Raiu wouldn’t say how his company came across the operation, other than to note that someone asked the lab last October to look into a spear-phishing campaign and a malicious file that accompanied it. The investigation led them to uncover more than 1,000 malicious modules the attackers used in their five-year campaign.

Each module is designed to perform various tasks — extract passwords, steal browser history, log keystrokes, take screenshots, identify and fingerprint Cisco routers and other equipment on the network, steal email from local Outlook storage or remote POP/IMAP servers, and siphon documents from the computer and from local network FTP servers. One module designed to steal files from USB devices attached to an infected machine uses a customized procedure to find and recover deleted files from the USB stick.

A separate mobile module detects when a victim connects an iPhone, Nokia or Windows phone to the computer and steals the contact list, SMS messages, call and browsing history, calendar information and any documents stored on the phone.

Based on search parameters uncovered in some of the modules, the attackers are looking for a wide variety of documents, including .pdf files, Excel spreadsheets, .csv files and, in particular, any documents with various .acid extensions. These refer to documents run through Acid Cryptofiler, an encryption program developed by the French military, which is on a list of crypto software approved for use by the European Union and NATO.

Read the rest here:

http://www.wired.com/threatlevel/2013/01/red-october-spy-campaign/all/
"Dementia' Wipes Out Attacker Footprints In Memory

By Kelly Jackson Higgins, Dark Reading, January 3, 2013

Forensics increasingly encompasses the analysis of potentially valuable clues and intelligence in the physical memory of an infected machine. But like anything in infosec, it's a constant cat-and-mouse game, with attackers finding new ways to hide their tracks in memory from incident response handlers trying to get to the bottom of a breach.

A researcher has developed a new tool called Dementia that cheats forensics tools that inspect attacker's footprints in a Windows computer's memory. Dementia basically renders a phony image of the infected machine's memory as a way to hide evidence of an attacker's movements. The tool removes "specific artifacts from the memory or the image being created. While the image itself is correct -- it can be analyzed -- specific artifacts are not present, which can hide traces of attacker's activities," says Luka Milkovic, who developed the tool. Milkovic, who is a information security consultant with Croatia-based Infigo, recently demonstrated the tool at the CCC conference in Hamburg, Germany.

Dementia demonstrates how an attacker who has wrested control of a system can muck with the forensics investigation process by fooling memory-acquisition tools. It can hide artifacts such as processes and threads from several popular tools: Moonsols Win32dd (in kernel-mode only); Mandiant Memoryze; Mantech MDD; FTK Imager; and Winpmem.

Memory analysis has become a vital process for triaging machines after an attack. Security experts say it's more efficient than just slogging through hundreds of gigabytes of hard drive space, for example, and to instead drill down on a few gigs of RAM where the attacker is executing code.

"Disk forensics has been prevalent for more than a decade, and there are lots of tools and methodologies for extracting valuable information or forensic evidence from a target computer or device," Milkovic says, such as files, folders, file and folder metadata, system logs, and registry entries.

"Incident handlers realized that by acquiring the memory of the examined machine, they might create less 'side effects' on the machine, while obtaining a cleaner and more trusted snapshot of the state of the machine," he says. "In the last couple of years, a significant rise in the number of tools for acquiring and analyzing memory can be seen, and memory forensics are now considered a vital part of the incident-handling workflow."

Read the rest here:

Data can be hidden in Skype's silence

Wojciech Mazurczyk at the Institute of Telecommunications in Warsaw, Poland, has discovered a method to use the silence between words in a Skype conversation. Skype speech is transmitted in 130-bit data packets. But rather than transmitting nothing between words, Skype transmits 70-bit packets that are ignored at the receiving end. Mazurczyk has developed a steganographic method to use these packets, combining both encryption and obfuscation.

Under normal circumstances, the ‘silent’ packets are simply ignored. The receiver – or any eavesdropper – will hear nothing. But Mazurczyk can hijack the packets and inject encrypted data. “The Skype receiver simply ignores the secret-message data, but it can nevertheless be decoded at the other end, the team has found," reports the New Scientist. "The secret data is indistinguishable from silence-period traffic, so detection of SkypeHide is very difficult," says Mazurczyk.

Skype was once considered a secure means of communication since it encrypts its content by default. But concerns have grown since the company was acquired by Microsoft. It is known that law enforcement agencies are trying to persuade major companies to include a backdoor that they could use for surveillance. Indeed, the Skype privacy policy explicitly warns that "Skype may disclose personal information to respond to legal requirements, exercise our legal rights or defend against legal claims, to protect Skype’s interests, fight against fraud and to enforce our policies or to protect anyone’s rights, property, or safety."

VentureBeat also notes that "Microsoft does have a patent application in process called "Legal Intercept" that enables the ability to record ‘any kind of voice-over-Internet-protocol (VoIP) communications’ by re-routing messages over ‘a path that includes a recording agent’. Legal Intercept would allow communications to be diverted through a recording device, giving law enforcement the opportunity to gain access to the content.

Read the rest here:
What makes a good information security professional?

Mirko Zorz, HelpNet Security, 21 January 2013

Information security is a very competitive industry, and one of the very few that kept doing fine even during the recession. It's also a dynamic field that promises a lot of fascinating work, so it's no wonder that so many individuals want to break into it.

"The infosec market has changed dramatically over the past decade. Changes in regulations, such as SOX, PCI DSS and Data Protection, and increased threats from online criminals have raised the profile of information security. At the moment, infosec in many regions is an industry with little or no unemployment and the market itself is predicted to grow to about $120.1 billion by 2017, double than the $63.7 billion size in 2011," says Brian Honan, infosec consultant and head of Ireland's CSIRT.

With the growing competition, it's only natural for some infosec professionals to be more vocal than others. They actively participate on social networks, write books, lecture at conferences, and work hard on creating a personal brand. Peers call them rockstars. But while some mean it as a compliment, others clearly don't.

"Like all markets in which the demand surpasses the supply, the infosec one attracts a number of individuals who claim expertise that they clearly do not have. They can be spotted and recognized by how they comment on topics on Twitter which they have no expertise in, hype up issues to create FUD, write blog posts that are inaccurate or present bad talks at conferences," observes Honan.

While some of these pundits are hailed as visionaries whose critical thinking urges hundreds to queue for event keynotes, others are regarded as self-proclaimed gurus whose main objective is to present themselves in the best possible light in order to score the next high profile job without actually doing much of security work in the process.

Companies adore both types. But while only one type engages the community, both impress clients with their credentials and help score high profile jobs. You know the old saying: "It's not what you know, it's who you know".

Marketing is king

Marketing and corporate identity really are everything, even in this field.

Only on rare occasions can I talk to a rockstar on the record and not go through their PR person. Occasionally they have an entourage of four or more people sitting in the meeting with them, making sure the celebrity doesn't say something they might view as inappropriate, even when we're not even talking company news.

I often wonder if the goal of these people is to make the interviewee look more important. I know for a fact that for some journalists this approach works like a charm and they end up being impressed.

"If companies select their 'experts' based on the number of their Twitter followers or web page view hits to their blog, then perhaps we need to ask whether this is a fault of the market, the 'expert' in question, or the company hiring that person," says Honan.

Will the real professional please stand up!

So, what makes a good information security professional? Is it a long list of certification credentials? Never-ending passion? A large Twitter following? A dedicated PR army?

Security advisor Per Thorsheim believes that you are not a security professional until other security professionals start to refer to you as being one. I couldn't agree more. You can buy Twitter followers or pay to present at conferences, but getting the demanding security community to recognize you for your work is not a simple task.

What about those with a strong academic background in research?

"An academically employed security researcher may be considered a security professional as well, but really should be connected to real world challenges, not just hypothesize. Personally I like to differentiate between security professionals and security researchers. In some cases their projects might overlap, in others they are doing completely different types of work," comments Thorsheim.

First-rate formal education can only help, but nothing works like innate curiosity. Wim Remes, Managing Consultant at IOActive, agrees: "It's not necessarily a matter of formal education but more about a trait the Italians call 'grinta' - a persistence to chase something relentlessly, educating oneself on the way to perfection."

Let's not forget that IT security work implies a great deal of responsibility and trustworthiness, traits that can't be acquired with a certification exam.

"The ideal security professional, one that I would look to hire, has a wealth of knowledge across disciplines yet continues to pursue knowledge and aims to become a better professional every day," concludes Remes.

http://www.net-security.org/secworld.php?id=14273
Are US Nuke Secrets Vulnerable to Cyberattack?

By Dana Liebelson, Mother Jones, Dec. 20, 2012

The Department of Energy, which is responsible for safeguarding America's nuclear weapons and secrets, has failed to tell law enforcement the details of when its computer systems have come under attack, "hindering investigations" into some of the 2,300 cybersecurity incidents the agency recorded between October 2009 and March 2012. This lack of timely and comprehensive cybersecurity reporting is putting the DOE's "information systems and networks at increased risk," according to a new investigation by the agency's internal watchdog.

The findings are "very problematic," says James Lewis, a senior cybersecurity expert at the Center for Strategic and International Studies, because "DOE sites are a primary target for espionage and have been successfully hacked in the past."

While preparing the report, the DOE's Office of Inspector General audited seven sites, including nuclear laboratories at Los Alamos and the Savannah River Site in South Carolina, and found that, of 223 incidents reported at DOE sites, 41 percent were not reported within established time frames. Another 10 incidents involving a loss of personally identifiable information (which affected 109 people) were reported late.

Joshua McConaha, a spokesman for the National Nuclear Safety Administration (NNSA), the DOE entity responsible for the nation's nuclear weapons stockpile, told Mother Jones that the cybersecurity incidents not involving identity theft "were normal computer issues such as viruses" that occur "on a regular basis." But experts say that the report's findings still don't bode well for nuclear weapons security.

Steven Aftergood, the director of the Project on Government Secrecy at the Federation of American Scientists, says that while the weapons themselves weren't at risk, "weapons-related information and facility security information could potentially be vulnerable." It wouldn't be the first time: In 2007, hackers believed to be from China launched a sophisticated cyberattack on several DOE laboratories in the United States. A spokesman for Los Alamos National Lab, which undertakes nuclear weapons design, told ABC News that "a significant amount of data was removed" from a small number of computers on the facility's unclassified network. This is the same lab that had its director step down in 2003 after a scandal involving widespread theft and security lapses.

Kevin Roark, a spokesman for Los Alamos National Laboratory, denies that the lab is reporting cyberattacks incorrectly. He told Mother Jones that the audit listed "six incidents where they believed Los Alamos was late in its reporting," none of which had to do with personal information being stolen. And according to Roark, "Los Alamos personnel have subsequently checked the six incidents, and determined that all were reported within the required time frame, but the information in the reports led the reporting authority to derive an inaccurate date and time."

When asked to about the incidents and Roark's response, a spokesman for the IG said that "the report speaks for itself and we have no additional comment."

It's well established that the NNSA faces regular cyberattacks—a spokesman for the agency told US News and World Report in March that if you count "security significant cyber security events," the number of cyberattacks goes up to 10 million per day. (Experts told Mother Jones that the number changes depending on how you categorize different types of incidents.) The real question is whether NNSA and DOE can deal with the attacks. The DOE has recently taken steps like improving cybersecurity training for employees and addressing weaknesses at facilities, according to a separate report released by the inspector general last month.

"Cybersecurity is a work in progress, both inside and outside government," Aftergood notes. "One would like to think that the nuclear weapons infrastructure would be ahead of the curve, but apparently that is too much to expect."

Left unanswered is the question of who's to blame for the cyberattacks that the DOE seems to have so much trouble reporting correctly.

"It's probably not Russia or China," Lewis snipes. "They've already gotten everything."

See the interactive map here:
http://www.motherjones.com/politics/2012/12/us-nukes-may-be-risk-cyber-attack
Feds Issue First Cloud Services Security Authorization

By J. Nicholas Hoover, InformationWeek, December 28, 2012

In a bid to accelerate and make more cost-effective the adoption of cloud computing, the federal government Thursday issued the first government-wide security authorization for a cloud computing service as part of the new Federal Risk and Authorization Management Program (FedRAMP).

The FedRAMP program will eventually be a mandatory, common approach to ensuring that cloud computing services meet federal cybersecurity requirements. It will replace the historically agency-by-agency and therefore often duplicative approach to certifying that services meet these requirements. For now, though, almost 19 months after being announced, FedRAMP is still just getting off the ground.

In issuing the authorization on Thursday, the General Services Administration met its goal of finalizing its first security authorization by the end of 2012 and vaulted little-known North Carolina-based government contractor Autonomic Resources LLC, which received the authorization, into the public eye.

[For more on federal cloud initiatives, see DOE, National Labs Reveal Sweeping Cloud Strategy http://www.informationweek.com/government/cloud-saas/doe-national-labs-reveal-sweeping-cloud/240144154?itc=edit_in_body_cross]

The authorization process required Autonomic Resources to implement and thoroughly document its implementation of dozens of required FedRAMP security controls in the vendor’s ARC-P infrastructure-as-a-service offering, and had auditors from cybersecurity consultancy the Veris Group verify and test those controls. The authority to operate granted by GSA serves as proof that Autonomic Resources meets federal cybersecurity requirements for cloud services, and enables any government agency to use ARC-P.

Autonomic Resources’ ARC-P is a community cloud infrastructure-as-a-service offering that can provide federal agencies with managed and unmanaged virtual machines. Autonomic Resources hires only employees with government security clearances to manage its cloud operations.

The company, which offers a variety of cloud and other managed services to government agencies, counts among its customers the Environmental Protection Agency, the Department of Homeland Security, the Navy, the National Institutes of Health, and a number of state and local governments. It has also been awarded contracts as part of several broader GSA contract vehicles, such as the government-wide cloud email contract vehicle.

Read the rest here:

Google Report Reveals Warrantless Surveillance of Users’ Data

By Ryan Gallagher, Slate, Jan. 23, 2013

In the first part of 2012, Google demonstrated that surveillance of Gmail and other accounts had skyrocketed to new levels. Now, in a transparency report (http://www.google.com/transparencyreport/) released today, the company shows that the trend of increased snooping continued unabated in the second half of the year—with much of it authorized without a search warrant.

U.S. authorities lodged 8,438 requests for user data between July and December, in comparison with 7,969 between January and June (an increase of 6 percent). On average, in 2012 Google complied with about 89 percent of the U.S. requests it received.

For the first time, Google has broken down the kinds of legal processes authorities used to request access to the data. The company reported that 68 percent of the requests it received from government entities in the United States were made without a search warrant and instead via subpoenas, which it says “are the easiest to get because they typically don’t involve judges.”

The rising surveillance figures, which in part may be correlated to growth in the use of Google services, show that between 2010 and 2012, U.S. authorities’ requests for user data have increased by a whopping 85 percent (from 8,888 in 2010 to 16,407 in 2012). That trend has continued globally, with Google reporting that user data requests of all kinds have increased by more than 70 percent since 2009. In total, Google says it received 42,327 requests for information about 68,249 users from in 2012. That’s a jump of about 25 percent when compared with 34,001 requests about 53,904 users in 2011. Google complied with an average of 66.5 percent of the total requests it received in 2012.

Civil liberties group Privacy International said in a statement issued this afternoon that it had analyzed the new transparency report and was alarmed by the trend of increasing surveillance. “Governments must stop treating the user data held by corporations as a treasure trove of information they can mine whenever they please, with little or no judicial authorisation,” said Carly Nyst, Privacy International’s head of international advocacy. Because of “the need for stronger national and regional privacy protections,” as demonstrated by the report, the group says it is planning to publish a new set of principles on surveillance and human rights that it hopes will prompt governments to put in place safeguards protecting online privacy.

Read the rest here:
Advanced algorithms driving improved data security

by Simply Security, January 7th, 2013

Anonymizing data to improve the safety of the information contained within files has been a controversial way to go as far as how much security it brings. Scientific American gives an example (http://www.scientificamerican.com/article.cfm?id=privacy-by-the-numbers-a-new-approach-to-safeguarding-data) from the Massachusetts Institute of the Technology after they cracked the supposedly anonymous patient health records that the state’s then-governor William Weld assured the public would be impossible to crack. Latanya Sweeney of MIT was able to crack the records by cross-referencing the obvious identifiers in the information with voter registration records.

“We’ve learned that human intuition about what is private is not especially good,” said Frank McSherry of Microsoft Research Silicon Valley told the website. “Computers are getting more and more sophisticated at pulling individual data out of things that a naive person might think are harmless.”

Scientific American said there is now more public awareness of these types of concerns than ever and organizations are starting to really get serious about making sure their sensitive data is safe. This, however, has cut off researchers from being able to look at valuable data, such as the patient data in Massachusetts, which has big data that may be able to help research into Alzheimer’s, cancer and help reduce hospital errors.

The website said one approach, “differential privacy,” is starting to help the security in situations like these, as it allows for the release of data while keeping a large standard of security in place. This type of algorithm allows researchers to execute a variety of complex database queries without exposing sensitive information.

Cynthia Dwork of Microsoft Research Silicon Valley said the idea is that the data can be viewed and researched without any additional risk and Avrim Blum of Carnegie Mellon University told Scientific American that it preserves the plausible deniability.

“If I want to pretend that my private information is different from what it really is, I can,” he said, according to the website. “The output of a differentially private mechanism is going to be almost exactly the same whether it includes the real me or the pretend me, so I can plausibly deny anything I want.”

How is this more safe?

Research from Microsoft said differential privacy makes sure that a given system can behave independently of any individual or small group is in it. With every possible output of the system, the probability is unchanged, the company said, adding that the problem of database linkage attacks are completed solved by this method. The goals of these databases can include identifying genetic markers for disease and fair allocation of resources, Microsoft’s research found, and said better participation would mean a higher quality of information available.

The University of Pennsylvania said on its website that the recent research into differential privacy has meant a big step closer to achieving the goal of securely taking information from databases without the worry of a security breach.

“Differential privacy allows us to reason formally about what an adversary could learn from released data, while avoiding the need for many assumptions (e.g. about what an adversary might already know), the failure of which have been the cause of privacy violations in the past,” the university said. “However, despite its great promise, differential privacy is still rarely used in practice. Proving that a given computation can be performed in a differentially private way requires substantial manual effort by experts in the field, which prevents it from scaling in practice.”

University of Pennsylvania said their project in differential privacy will work to build a system that supports private data analysis but can be used by what it calls the ”average programmer” and is general enough to be used by many applications. The university believes this could be used to make very strong privacy guarantees and become a standard feature for looking at any kind of sensitive or private data, with the long-term goal of combining ideas from this, distributed system sand programming language to make the data security even stronger.

Read the rest here: http://www.simplysecurity.com/2013/01/07/advanced-algorithms-driving-improved-data-security/
The Changing Role of Security Professionals

By John Pironti, ISACA, IP Architects, January 15, 2013

It’s no secret that one of the biggest threats to securing corporate information infrastructures isn’t, ultimately, the latest variation of the Flame virus or new malware that exploits vulnerability in an operating system or application. One of the biggest threats is employees themselves – either through a malicious action or, much more likely, inadvertent error.

That’s why information risk management is one of the most important new skills that security professionals need to master in order to add value. As the use of cloud computing and mobile devices increases substantially – from small start-ups to the Fortune 500 – corporate information assets have left the building, and keeping them secure has become much harder. As a result, security professionals must evolve into advisors. Information risk management, furthermore, is not the only new tool they must add to their arsenal; security professionals also need to master governance and compliance, privacy, metrics and data analytics, and business consulting skills.

Changing Gears

Protecting information no matter where it is located requires a fundamental shift in focus. Information security professionals who are accustomed to concentrating on technology need to switch gears and focus on business processes and data. Both cloud computing and mobile devices are driving this transition, demanding that security professionals spend more of their time on governance and providing advice to their organization than on direct operational responsibilities for cloud and mobile environments.

“Organizations are eager to leverage cloud solutions – not only as a means of reducing cost, but also to provide product/service scalability and redundancy not easily supported through traditional IT solutions”, says Erik Friebolin, managing principal at Verizon Enterprise Solutions – Global Risk Services. “As a result”, he adds, “security professionals must be prepared to address the new and emerging risks to these evolving business strategies”.

Shifting from managing information security to managing the provider of that security can be a leap. Security professionals must now learn how to obtain answers from third-party providers, not just provide answers themselves. Some of the most important information they need to obtain is the level of visibility they will have into the design, implementation, and operation of their cloud provider’s infrastructure.

As illustrated by the Amazon EC2 outage in June that took down high-profile services like Netflix, Instagram and Pinterest (and the more recent outage in October), it’s important to determine a cloud provider’s business resiliency capabilities (i.e., command and control, business continuity, disaster recovery, and incident response). It is also important to discover how they handle a deliberate denial-of-service attack, what service guarantees are offered, and how fully integrated risk management is into their core business processes and governance.

BYOD Accelerates the Evolution

On the mobile side, the rise of Bring Your Own Device (BYOD) is not the only driver of change, but it may be the most irksome. Half (50.5%) of information technology leaders in the US believe that the risks of BYOD outweigh the benefits, according to the 2012 IT Risk/Reward Barometer survey (http://www.infosecurity-magazine.com/view/29347/holiday-shopping-exposes-us-byod-users-to-online-privacy-security-risks) conducted by ISACA. Close to one in three (29%) enterprises prohibit BYOD. When asked to rank a range of employee activities as high, medium or low risk, a large number of respondents chose losing a work-supplied smartphone or downloading content on to it as high risk.

Like cloud computing, mobile device use is driving a bigger emphasis on process and people and a shrinking focus on technology. One illustration of this shift is the evolution away from mobile device management (MDM) to mobile enterprise management (MEM), which encompasses both MDM and mobile application management software. The importance of the device, or technology, is retreating compared with the overarching issue of managing mobility in relation to the enterprise.

Time to Rebrand

In today’s threat landscape, information security must go hand in hand with information risk. Yesterday’s ‘information security’ job title needs to change to ‘information risk and security’. Those who don’t fully embrace information risk are missing out on a major piece of alignment with enterprise goals.

Technology skills will still be important, but more to support execution of security processes once enterprise risk tolerance and risk profiles have been established. This aspect of the evolving role requires that these new information risk and security professionals venture into parts of the organization that may seem like foreign territory: enterprise risk management and the legal department. Like the rise of cloud and mobile computing, this shift requires the ability to think and act like a business consultant, not a technologist.

Read the rest here:
Piecing Together Digital Evidence

January 8, 2013, FBI

In a case involving the round-up of dozens of suspects indicted on public corruption and other charges, investigators were faced with processing large numbers of seized cell phones, desktop computers, and laptops belonging to the suspects. In another case, key evidence against a terror suspect arrested for attempted use of a weapon of mass destruction included data found on his computer. And after a U.S. Congresswoman was wounded and six people killed in Arizona, vital evidence was found on security camera footage, computers and cell phones.

Reflecting a trend that has become increasingly commonplace for law enforcement, all three of these cases involved the need to recover digital evidence. And our Computer Analysis Response Team, or CART, is the FBI’s go-to force for providing digital forensic services not only to our own investigators but also in some instances to our local, state, and federal partners.

CART consists of nearly 500 highly trained and certified special agents and other professional personnel working at FBI Headquarters, throughout our 56 field offices, and within the network of Regional Computer Forensics Laboratories across the nation. They analyze a variety of digital media — including desktop and laptop computers, CDs/DVDs, cell phones, digital cameras, digital media players, flash media, etc. — lawfully seized as part of our investigations.

During fiscal year 2012, CART — while supporting nearly 10,400 investigations—conducted more than 13,300 digital forensic examinations involving more than 10,500 terabytes of data. To put that last figure into perspective, it’s widely believed that the total printed content in the Library of Congress is equal to about 10 terabytes of data, so imagine the printed content of approximately 1,050 Libraries of Congress!

CART examiners are experts at extracting data from digital media...even when the media is damaged by the forces of nature or defendants attempting to prevent any data from being recovered.

The cases that CART examiners work span the gamut of FBI program areas: from cyber crimes and computer intrusions to violent crimes, financial crimes, organized crime, and national security matters. And once they have finished their forensic work, CART examiners are also available to testify in court as expert witnesses on their findings.

Because we come across computers and other digital media so often in the course of our investigative work, our CART examiners can’t possibly handle every piece of media. That’s why CART created a basic digital evidence training course and developed easy-to-use examination tools for field investigators — to give them the technical and legal knowledge they need to process simpler and more basic digital evidence from their cases without altering or damaging the data — which allows CART examiners to focus on more technically complex cases.

CART on the go. While much of CART’s work is done in stationary facilities in the field or back at our national Headquarters, we also have six mobile CART laboratories around the country. These mobile labs are especially valuable when time is of the essence, enabling digital evidence to be examined on the spot.

CART … an evidence response team for today’s high-tech environment.

Researchers have exploited critical vulnerabilities in two popular medical management platforms used in a host of services including assisting surgeries and generating patient reports.

The dangerous unpatched flaws within the Philips Xper systems allowed researchers to develop an exploit within two hours capable of gaining remote root access on the device.

From there, attackers would have administrative access to a host of patient data stored in connected databases.

The affected machine can operate any medical device which uses the ubiquitous HL7 standard.

"We have a remote unauthenticated exploit for Xper, so if you same see an Xper machine on a network, then you can own it," Cylance researcher Billy Rios told SC.

The holes were so severe that the US Department of Homeland Security (DHS) and Food and Drug Administration (FDA) stepped in to pressure Philips to fix the system.

"We've dropped exploits before on medical systems like Honeywell and Artridum, but we've never seen the FDA move like that," he says.

"It was quicker than anything else I've seen before."

After initial bids to contact Philips failed, researchers Rios and colleague Terry McCorkle sought assistance from the DHS, the FDA and the country's Industrial Control Systems Cyber Emergency Response Team (ICS CERT).

Two days later, DHS control system director Marty Edwards told the researchers the agency would from then on handle all information security vulnerabilities found in medical devices and software.

The announcement comes month after the US Government Accountability Office said in a report (pdf) that action was required to address medical device flaws, adding that the FDA did not consider such security risks "a realistic possibility until recently."

**Vulnerabilities**

Once an extensive 200Gb forensic imaging process of the Windows-based platform had completed and the system was booted into a virtual machine, it took the researchers "two minutes" to find the first vulnerability.

"We noticed there was a port open, and we started basic fuzzing and found a heap overflow and wrote up a quick exploit for it," Rios said.

"The exploit runs as a privileged service, so we owned the entire box - we owned everything that it could do."

The researchers suspect the authentication logins for the system, one with a username Philips and password Service01, are hardcoded and unchangeable by users, but when they warned Philips the company refuted the claim.

The dealer was reported to the DHS and the equipment was returned to Philips.

Article for the Newsletter?
If you would like to submit an article...

Are you a budding journalist? Do you have something that the Colorado Springs ISSA community should know about? Can you interview one of the “movers and shakers”? Tell us about it!

We are always looking for articles that may be of interest to the broader Colorado Springs security community.

Send your article ideas to Don Creamer at: doncreamer-issa@q.com

Ensure that “Newsletter” is in the subject line.

Looking forward to seeing you in print!

Upcoming ISSA Events

2013 Spring Conference, Friday, Mar 8, Crowne Plaza Hotel 7:30 – 5:00

2013 Fall Conference, Friday, Nov 15, Crowne Plaza Hotel 7:30 – 5:00

Training

From Harry Smith: Here is one that may interest ISSA-COS members:

Information Security and Risk Management in Context

https://www.coursera.org/#course/inforiskman

At the very least it is good for some CPEs. (And it's free!)
<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Feb 14</td>
<td>11:00 to 1:00</td>
<td>Bambino's Italian Eatery and Sports Bar, 2849 East Platte Avenue, Colorado Springs, 719) 630-8121</td>
</tr>
<tr>
<td>Mar 14</td>
<td>5:30 to 7:30</td>
<td>Bambino's</td>
</tr>
<tr>
<td>Apr 11</td>
<td>11:00 to 1:00</td>
<td>Bambino's</td>
</tr>
<tr>
<td>May 9</td>
<td>5:30 to 7:30</td>
<td>Bambino's</td>
</tr>
<tr>
<td>Jun 13</td>
<td>11:00 to 1:00</td>
<td>Bambino's</td>
</tr>
<tr>
<td>Jul 11</td>
<td>5:30 to 7:30</td>
<td>Bambino's</td>
</tr>
<tr>
<td>Aug 8</td>
<td>11:00 to 1:00</td>
<td>Bambino's</td>
</tr>
<tr>
<td>Sep 12</td>
<td>5:30 to 7:30</td>
<td>Bambino's</td>
</tr>
<tr>
<td>Oct 10</td>
<td>11:00 to 1:00</td>
<td>Bambino's</td>
</tr>
<tr>
<td>Nov 14</td>
<td>5:30 to 7:30</td>
<td>Bambino's</td>
</tr>
<tr>
<td>Dec 6</td>
<td>11:00 to 1:00</td>
<td>Carrabba’s North</td>
</tr>
</tbody>
</table>
Hack Turns Cisco’s Desk Phone Into a Spying Device

Cisco’s internet phones—which sit on thousands of desks around the world—have been shown to be easily hacked and turned into remote spying devices. The official announcement comes two whole weeks after Cisco first found out about the problem.

The exploit was discovered by Ang Cui and Salvatore Solf, a pair of computer scientists from Columbia University’s engineering department. They presented the finding at the 29th Chaos Communication Congress in late December. By attaching a small device to the local serial port on the phone, they were able to inject code that gave them complete control over the device—allowing them to remotely monitor phone calls and turn on the phone’s microphone to eavesdrop on conversations happening near the phone. In a statement, Cisco explained:

Read the rest here: http://gizmodo.com/5974814/hack-turns-ciscos-desk-phone-into-a-spying-device

Published at no cost to ISSA Colorado Springs by Sumerduck Publishing™, Woodland Park, Colorado