CCC News

Control Computer Crimes

Issue 0012 - 15 December 2009

Message from the Editor

Welcome to the Twelfth issue of CCCNews Magazine.

As usual, we bring you many more and tropical interesting and educational reports, analysis and research.

One of the big attractions in this issue is a research analysis on – What seven skills; any information security professional must have to be successful. These are –

1. An understanding of psychology
2. Social networking skills
3. Skills in marketing communications
4. Strong commercial management skills
5. Sophisticated crisis management skills
6. Digital forensic skills
7. A sound knowledge of legal and regulatory requirements

These skills cover a holistic approach to business and information security as an integral part of business. These are discussed in brief in an article in this issue.

Other important reports and analysis are (1) Most common attack vector in 2009; (2) Forecast of major threats for 2010 – 2 reports; (3) Is anti-virus dead? (4) Why computers does not save money to hospitals; (5) Certification is not panacea for cyber security woes.

Apart from these, there are some more reports, which I am sure, you will read, learn and enjoy.

Happy reading,

Rakesh Goyal
Editor

CONTENTS

CCC News
Issue 0012
15 December 2009

Rakesh Goyal
Editor
editor@cccnews.in

Published by
CCC Media
Mumbai, India

LAST ISSUE DOWNLOAD COUNT : 160,000+

REPORT ANALYSIS

15 Most Common Attacks of 2009

Keylogging and spyware are among the most commonly found exploits in breached companies, report says

Keyloggers and spyware are the most commonly occurring attacks in companies that suffer major data breaches, according to a report published today by Verizon Business.

The new report, "2009 Supplemental Data Breach Investigations Report: An Anatomy of a Data Breach," offers a look at the 15 most common security attacks and how they typically unfold. The data is extracted from Verizon Business' April 2009 study of its computer forensics service customers, all of whom have experienced a major data breach.

The report taps Verizon Business' detailed investigative records to identify, rank, and profile the most common attacks. For each type of attack, the report provides real-world scenarios, the warning signs, how the attack is orchestrated, how attackers got in, what information they took, what assets the attackers targeted, what industries are commonly affected, and what countermeasures are effective. In total, the report details nearly 150 ways to detect and combat security threats. This latest installment in Verizon's data breach study series is based on the "2009 Verizon Business Data Breach Investigations Report," issued in April. That landmark study analyzed more than 90 forensic investigations involving 285 million compromised records.

"We developed this report to answer a lot of the questions we've received about the report we issued in April," says Wade Baker, research and intelligence analyst at Verizon Business and one of the authors of the report. "We plot out the most common attacks and some of the indicators that can be used to spot them."

The report identifies and ranks by frequency the following top 15 types of attacks:

1. **Keylogging and spyware**: Malware specifically designed to covertly collect, monitor, and log the actions of a system user.

2. **Backdoor or command/control**: Tools that provide remote access to or control of infected systems, or both, and are designed to run covertly.

3. **SQL injection**: An attack technique used to exploit how Web pages communicate with back-end databases.

4. **Abuse of system access/privileges**: Deliberate and malicious abuse of resources, access, or privileges granted to an individual by an organization.

5. **Unauthorized access via default credentials**: Instances in which an attacker gains access to a system or device protected by standard preset (widely known) usernames and passwords.

6. **Violation of acceptable use and other policies**: Accidental or purposeful disregard of acceptable use policies.

7. **Unauthorized access via weak or misconfigured access control lists (ACLs)**: When ACLs are weak or misconfigured, attackers can access resources and perform actions not intended by the victim.

8. **Packet sniffer**: Monitors and captures data traversing a network.

9. **Unauthorized access via stolen credentials**: Instances in which an attacker gains access to a protected system or device using valid but stolen credentials.

10. **Pretexting or social engineering**: A social engineering technique in which the attacker invents a scenario to persuade, manipulate, or trick the target into performing an action or divulging information.

11. **Authentication bypass**: Circumvention of normal authentication mechanisms to gain unauthorized access to a system.

12. **Physical theft of asset**: Physically stealing an asset.

13. **Brute-force attack**: An automated process of iterating through possible username/password combinations until one is successful.

14. **RAM scraper**: A fairly new form of malware designed to capture data from volatile memory (RAM) within a system.

15. **Phishing (and endless "ishing" variations)**: A social engineering technique in which an attacker uses fraudulent electronic communications (usually email) to lure the recipient into divulging information.

In addition to the extensive threat catalog, the supplemental report includes an appendix that compares Verizon's caseload with DataLossDB, a public database of reported incidents worldwide.

"We developed the appendix to address some questions and concerns that people had expressed about the April report, which showed that internal threats weren't that prevalent," Baker says. "But when we went through the DataLossDB, we found that our numbers and theirs weren't really all that far apart."

Courtesy : Tim Wilson; DarkReading
Dec 09, 2009

REPORT ANALYSIS

13 PC Security Threats for 2010

After a year of unprecedented proliferation of spyware, malware and cyber attacks of all types, security software vendor Symantec warns there's plenty more where that came from in its just-released 2010 Security Trends to Watch report.

Kevin Haley, Symantec Security Response group product manager, posted a blog entry titled "Don't Read This Blog". "We love to click," he wrote. "Clicking on links and attachments that are accompanied by just the slightest bit of social engineering appears to be a basic human need."

"I expect it to show in a revision of Maslow's Hierarchy of Human Needs any day now -- behind love, but certainly ahead of safety," he added.

Whether it's a come-on for what appears to be a friendly game of online Monopoly or the incessant and sinister pleadings of a bogus antivirus application, malware scams have become more sophisticated and damaging with each passing day.

A report released earlier this year by the Anti-Phishing Working Group (APWG) found that fake anti-malware and security software programs soared up more than 585 percent in the first half of 2009 alone. In 2007, Gartner said that more than 3.6 million people lost more than $3.2 billion to malicious phishing scams.

"Yes, it's a cheap trick and not even close to original," Haley wrote of his creative blog title. "[But] since social engineering plays such a prominent role in future trends, it seemed appropriate."
The dirty baker's dozen

Whether you're using your mobile phone to check e-mail and surf the Web or an enterprise IT administrator charged with safeguarding your company's data, Symantec says the following 13 security issues will be most relevant in 2010:

1) Antivirus is not enough

With the rise of polymorphic threats and the explosion of unique malware variants in 2009, the industry is quickly realizing that traditional approaches to antivirus (including both file signatures and heuristic/behavioral capabilities) are not enough to protect against today's threats. We have reached an inflection point, where new malicious programs are actually being created at a higher rate than good programs.

Approaches to security that looks for ways to include all software files, such as reputation-based security, will become key in 2010.

2) Social engineering as the primary attack vector

More and more, attackers are going directly after the end user and attempting to trick them into downloading malware or divulging sensitive information under the auspice that they are doing something perfectly innocent. Social engineering's popularity is at least in part spurred on by the fact that what operating system and Web browser rests on a user's computer is largely irrelevant, as it is the actual user being targeted, not necessarily vulnerabilities on the machine.

3) Rogue security software vendors escalate their efforts

In 2010, expect to see the propagators of rogue security software scams take their efforts to the next level, even by hijacking users' computers, rendering them useless and holding them for ransom. A less drastic next step, however, would be software that is not explicitly malicious, but dubious at best.

For example, Symantec has already observed some rogue antivirus vendors selling rebranded copies of free third-party antivirus software as their own offerings. In these cases, users are technically getting the antivirus software that they pay for, but the reality is that this same software can actually be downloaded for free elsewhere.

4) Social networking third-party apps will fraud targets

With the popularity of social networking sites poised for another year of unprecedented growth, expect to see fraud being targeted toward social site users to grow.

As this occurs, and as these sites more readily provide third-party developer access to their APIs, attackers will likely turn to vulnerabilities in third-party applications for users' social networking account information, just as we have seen attackers take advantage of browser plug-ins more as Web browsers themselves become more secure.

5) Windows 7 will come in the crosshairs of attackers

Microsoft has already released the first security patches for its new operating system. As long as humans are programming computer code, flaws will be introduced, no matter how thorough pre-release testing is. And the more complex the code is, the more likely that undiscovered vulnerabilities exist.

Microsoft's new operating system is no exception, and as Windows 7 hits the pavement and gains traction in 2010, attackers will undoubtedly find ways to exploit its users.

6) Fast Flux botnets will increase

Fast flux is a technique used by some botnets, such as the Storm botnet, to hide phishing and malicious Web sites behind an ever-changing network of compromised hosts acting as proxies. Using a combination of peer-to-peer networking, distributed command-and-control, Web-based load balancing and proxy redirection, it makes it difficult to trace the botnets' original geo-location.

As industry countermeasures continue to reduce the effectiveness of traditional botnets, expect to see more using this technique to carry out attacks.

7) URL-shortening services become the phisher's best friend

Because users often have no idea where a shortened URL -- particularly from Twitter -- is actually sending them, phishers are able to disguise links that the average security conscious user might think twice about clicking on.

In an attempt to evade antispam filters through obfuscation, expect spammers to use shortened URLs to carry out their evil deeds.

8) Mac and Mobile Malware Will Increase

In 2009, Macs and smartphones will be targeted more by malware authors. As Mac and smartphones continue to increase in popularity in 2010, more attackers will devote time to creating malware to exploit these devices.

9) Spammers breaking more rules

As the economy continues to suffer and more people seek to take advantage of the loose restrictions of the Federal Trade Commission's Can-Spam Act, there will be more organizations selling unauthorized e-mail address lists and more less-than-legitimate marketers spamming those lists.

10) As spammers adapt, volume will continue to fluctuate

Since 2007, spam has increased on average by 15 percent a year. Spam volumes will continue to fluctuate in 2010 as spammers continue to adapt to the sophistication of security software and the intervention of responsible ISPs and government agencies across the globe.

11) Specialized malware on the rise

Highly specialized malware was uncovered in 2009 that was aimed at exploiting certain ATMs, indicating a degree of insider knowledge about their operation and how they could be exploited. Expect this trend to continue in 2010, including the possibility of malware targeting electronic voting systems, both those used in political elections and public telephone voting, such as that connected with reality television shows and competitions.

12) CAPTCHA technology will improve

This will prompt more businesses in emerging economies to offer real people employment to manually generate accounts on legitimate Web sites -- especially those supporting user-generated content -- for spamming purposes.

Symantec estimates that the individuals will be paid less than 10 percent of the cost to the spammers, with the account farmers charging $30-$40 per 1,000 accounts.

13) Instant messaging spam will surge

As hackers exploit new ways to bypass CAPTCHA (define) technologies, instant messaging attacks will grow in popularity. IM threats will largely be comprised of unsolicited spam messages containing malicious links, especially attacks aimed at compromising legitimate IM accounts.

By the end of 2010, Symantec predicts that one in 300 IM messages will contain a URL. Also, in 2010, Symantec predicts that one in 12 hyperlinks overall will be linked to a domain known to be used for hosting malware.

Courtesy : Larry Barrett; itmanagement.earthweb.com
November 20, 2009

SURVEY

AVG's Internet security threats prediction for 2010

'Cyber-criminals will, with increased sophistication, continue to make money via social engineering and phishing scams'

The year gone by has seen a significant rise in the incidence of spam, phishing, botnet activity, and malware. Each year cyber-criminals who have largely succeeded in duping the unsuspecting user, are investing in sophisticated and automated ways to run their operations.

It can be safely predicted that in 2010 the threat environment will witness higher volumes of web-threats and be even more transient, agile and organised! Internet security threats that AVG expects to have significant impact on users in 2010 are as follows:

1. **More diverse, automatically generated malware**: Cyber-criminals can now automatically create hundreds of thousands of unique pieces of malware a day, much of which has no unique signature and can bypass old-fashioned, signature-based virus detection software.

2. **The bad guys still want your money, identity and/or resources**: In the coming year, cyber-criminals will, with increased sophistication, continue to make money via social engineering and phishing scams, trick users into providing, or steal personal details.

3. **Cyber criminals in the cloud**: To keep ahead of the computer security industry's efforts to thwart their activities, the cyber-criminals are now using "in the cloud" technologies in far more sophisticated and effective ways than most legitimate businesses.

4. **Highly transient web threats**: In 2010, cyber criminals will continue to improve the speed with which they are able to move their campaigns from domain to domain, server to server. In early 2009, AVG researchers reported that 60% of these poisoned web threats were active for less than a day and 75 per cent for less than 30 days.

5. **Exploitation of major events, news and gossip**: Cyber-criminals exploit latest trends and topics that are gaining popularity on the internet by hijacking search results into clicks

on links to their malicious web pages. Expect to see more highly targeted, convincing attacks with custom malware in 2010.

6. **"Web two-point-uh-oh"**: Cyber-criminals exploit trust. With the rise of Web 2.0, attacks that impersonate social networking sites or spoof contacts from your "friends" list are more likely to be clicked on. It is likely we'll see a great deal more of similar scams in 2010.

7. **Emerging nations go online with poor security**: Many users especially from amongst developing countries, who are amongst the growing millions who are getting connected to the Internet, still use pirated software that can't be kept up to date with security patches. We expect to see a big increase in threats being delivered via emerging countries in 2010.

8. **Global economic crisis impacts security**: As employment has taken a hard hit due to the economic crisis, it is likely that more people will be lured by the easy money of cyber-crime. Also, individuals desperate in search of earning opportunities are more likely to fall prey to bogus offers or disgruntled employees may breach official data that could fall into the wrong hands.

9. **Business still too complacent**: Events in 2009 showed that many businesses simply weren't properly protected. The success of the exploits used to penetrate and establish Conficker into business and enterprise networks early in 2009 was largely because of complacency.

10. **More people will buy complete protection**: The good news is that reputable security vendors now provide full Internet security suites with multiple layers of protection. The majority of people that pay for security software now buy the full suite, complete protection solution instead of entry-level solutions. This trend continued through 2009, in spite of tougher economic times, and AVG expects it to be maintained in 2010.

It will get worse before it gets better

Sadly, the security threats in 2010 are likely to be nastier, more targeted and more frequent, with malware and cyber-crime being almost exclusively driven by organised crime and motivated by money.

www.ciol.com
December 08, 2009

DEBATE

Why Criminal Hackers Must Not Be Rewarded

Should we hire criminal hackers as security experts?

On a broader scale, consider the message you would be giving some thirteen year old proto-hacker. These kids, like most kids, are tremendously susceptible to peer pressure. They already find criminal hacking attractive because it's viewed as today's counter-culture — something fairly harmless (compared with, say, dealing drugs) but exciting because it's illegal. Now imagine that the older creeps can announce that they've just been hired by The Man (i.e., authority figures) to work in counter-intelligence, snooping in foreign companies' files for money (you don't imagine they'd keep it quiet, do you?). Oh man — not only is criminal hacking glittering with the allure of the forbidden now, but you can hope to earn money with it from the government!

The children and emotionally-arrested adolescents involved in criminal hacking already have a love/hate attitude towards The Man. Many of them claim that they'd like to work for security firms when (if) they grow up. This myth that criminal hacking is a reasonable basis for work in security would become even more pernicious if it were known that more hackers had in fact been solicited and used by government or corporate organizations. Using such people would reinforce the attractiveness of criminality.

Consider the outcry if the military in a democracy actively solicited murderers to be soldiers. The great challenge of military training is to temper savagery with honor; to provide a moral framework within which war is viewed as undesirable, killing as regrettable. A soldier who lies is a stain on his unit’s honor. A soldier who steals is a wretch who deserves expulsion. And a soldier who breaks his word is a traitor to his country. And so how shall we deal with people whose entire way of life is to lie and to steal and to cheat?

I say they're unfit to serve.

At the most fundamental level of all, the end does not justify the means. To use criminals, to honor them, to praise them, to pay them: this would be yet another blow against morality and decency. And it would be a blow without even the excuse of necessity. We do not need criminal hackers. Information security can be strengthened using the skills of honest people — hackers, if you like, but not criminal hackers. We should be encouraging children who enjoy using computers to learn more, to learn deeper. We need school teachers who have more than merely a superficial knowledge of the user interface: we need teachers with a thorough grounding in computer science. We need books for children to teach operating systems fundamentals and database theory in an enjoyable, challenging way; we need recognition for the gifted — support for the oddballs who prefer trackballs to basketballs. We need donations of computer equipment and texts from companies who see that helping kids learn is a wise investment in everyone's future. Why not donate used mainframes and servers to help kids learn about operating systems and networks? Let's give brilliant kids with a knack for security summer jobs so they can use their skills to help society instead of feeling marginalized.

What we don't need is reward for dishonesty and praise for sociopathy.

In the Hacker Debate at the InfoWarCon 95, someone asked me if I recommended blackballing all hackers who engaged in illegal activity in their adolescence. I answered that no, there should not be a lifetime ban on criminal hackers — as long as they show that they understand their moral and legal obligations to society and their employers or clients. If a person shows by their actions that they have matured and now repudiate their former lifestyle, by all means give them a chance. Keep them under supervision, avoid putting them in temptation's way, and be on your guard — but by all means welcome recovering hackers back to society.

Just don't solicit people because they are or were criminal hackers.

Courtesy : M. E. Kabay, Network World, http://www.networkworld.com
December 02, 2009

REPORT

SMEs should audit before outsourcing

Small businesses are exposing themselves to unnecessary risk through a lack of in-house skills, according to a white paper from vendor Fifosys.

"It is difficult for small companies to acquire the IT skills necessary to support today’s complex technology requirements. These can include the management of online order taking, continual email services, maintaining and servicing local and wide area networks, as well as business continuity. A one or two-person IT team simply will not be able to manage this," the report says.

As a result, many of these companies still have a "single point of failure" – a system where operations will grind to a halt if one element of the system crashes.

Mitesh Patel, managing director of Fifosys, said: "While businesses routinely assess the single points of failure in core operations, from manufacturing to distribution, they are patently failing to apply the same robust operations practices to IT."

He explained that the problem lies with the culture of the IT department: " Individuals within the IT team are not encouraged to look at mapping business needs with IT risks and availability, nor do they typically have the skills to do so."

Small companies may also find that inadequate third-party supplier contracts fail to reflect their operational requirements. These can be expensive and risk making small firms less agile.

The report recommends that SMEs avoid some of these problems by commissioning an IT infrastructure audit from a professional audit firm.

"This can provide immediate insight into the single points of failure... and will enable directors and management to determine and prioritise IT needs and investment based on real business requirements," the report says. This might include increasing staff training or numbers.

Only then should a small business look to purchase an IT services contract, making sure it carefully defines the terms.

"Once [this is] in place, SMEs can look to build on this relationship to attain quantifiable information regarding technology requirements, including advice on strategic investment and long-term budgeting," the report adds.

Courtesy : Tom Young, Computing.co.uk
30 Nov 2009

STUDY

Computers don't save hospitals money

Hospital computer systems are often built for administrators, not doctors

A Harvard Medical School study that looked at some of the nation's "most wired" hospital facilities found that computerization of those facilities hasn't saved them any money or improved administrative efficiency.

The recently released study evaluated data on 4,000 hospitals in the U.S over a four-year period and found that the immense cost of installing and running hospital IT systems is greater than any expected cost savings. And much of the software being written for use in clinics is aimed at administrators, not doctors, nurses and lab workers.

The study comes as the federal government prepares to begin dispensing $19 billion in incentives for the health industry to roll out electronic health records systems. Beginning in 2011, the Health Information Technology for Economic and Clinical Health (HITECH) Act will provide incentive payments of up to $64,000 for each physician who deploys an electronic health records system and uses it effectively.

The problem "is mainly that computer systems are built for the accountants and managers and not built to help doctors, nurses and patients," the report's lead author, Dr. David Himmelstein, said in an interview with Computerworld .

Himmelstein, an associate professor at Harvard Medical School, said that in its current state, hospital computing might modestly improve the quality of health care processes, but it does not reduce overall administrative costs. "First, you spend $25 million dollars on the system itself and hire anywhere from a couple-dozen to a thousand people to run the system," he said. "And for doctors, generally, it increases time they spend [inputting data]."

Himmelstein said that only a handful of hospitals and clinics realized even modest savings and increased efficiency -- and those hospitals custom-built their systems after computer system architects conducted months of research.

He pointed to Brigham and Women's Hospital in Boston, Latter Day Saints Hospital in Salt Lake City and Regenstrief Institute in

Indianapolis as facilities with some success in deploying efficient e-health systems. That's because they were intuitive and aimed at clinicians, not administrators.

Programmers of the successful systems told Himmelstein that they didn't write manuals or offer training. "If you need a manual, then the system doesn't work. If you need training, the system doesn't work," he said.

While many health care experts believe that computerization will improve quality of care, reduce costs and increase administrative efficiency, the Harvard Medical School report notes that no earlier studies closely examined computerization's cost or its effect on a diverse sample of hospitals. Even hospitals on the "most wired" list "performed no better than others on quality, costs, or administrative costs," the study found.

Himmelstein and his team of researchers pored over data on computerization at approximately 4,000 hospitals between 2003 and 2007 from the Healthcare Information and Management Systems Society, along with administrative cost data from Medicare Cost Reports and cost and quality data from the 2008 Dartmouth Health Atlas.

Himmelstein, who was once the director of clinical computing at Cambridge Hospital in Massachusetts, wrote that the misconception that computerization brings cost savings in hospitals is not new. He pointed to ads by IBM and Lockheed Corp. from the 1960s and 1970s touting computerization as a way to reduce paperwork and improve health care. In the 1990s, experts also espoused the benefits of computerized patient records, saying they would be adopted quickly and yield huge administrative savings.

In 2005, one analyst group projected annual savings of $77.8 billion through computerization; another predicted more than $81 billion in savings, as well as a big improvement in health. Today, the federal government's health information technology Web site proclaims that the "broad use of health IT will: improve health care quality; prevent medical errors; reduce health care costs; increase administrative efficiencies; decrease paperwork; and expand access to affordable care."

"Unfortunately," Himmelstein's report reads, "these attractive claims rest on scant data. A 2006 report prepared for the Agency for Healthcare Research and Quality, as well an exhaustive systematic review, found some evidence for cost and quality benefits of computerization at a few institutions, but little evidence of generalizability. Recent Congressional Budget Office reviews have been equally skeptical, citing the slim and inconsistent evidence base."

David Brailer, who served as the nation's first health information czar under President George W. Bush, noted in an interview with Computerworldearlier this year that 25% to 35% of the nation's 5,000 hospitals use or are in the process of rolling out computerized order-entry and medical records systems.

Brailer, now chairman of Health Evolution Partners, a San Francisco-based investment firm that specializes in funding health care providers, headed the Office of the National Coordinator for Health Information Technology from 2004 until 2006.

Implementing e-health records nationwide would cost between $75 billion and $100 billion, Brailer said, adding that individual hospitals "will have to make sizable, potentially multi-hundred-million-dollar budget commitments." Still, he said a fully functioning national electronic health system could reduce U.S. health care costs by $200 billion to $300 billion annually by cutting down on duplicate records, reducing record-keeping errors, avoiding fraudulent claims and better coordinating health care among providers.

Himmelstein called those claims "unsupported."

"For 45 years or so, people have been claiming computers are going to save vast amounts of money and that the payoff was just around the corner," he said. "So the first thing we need to do is stop claiming things there's no evidence for. It's based on vaporware and [hasn't been] shown to exist or shown to be true."

Courtesy Lucas Mearian, Computerworld, http://www.networkworld.com
November 30, 2009

REPORT

Security Pros In Demand

Security is among a broad mix of jobs expected to receive hiring attention from CIOs, according to the latest IT Hiring Index and Skills

Chief information officers are planning to increase hiring -- although at a low rate -- in the first quarter of 2010 with traditional jobs in networking, security, and application development most in demand, according to the latest IT Hiring Index and Skills Report from employment specialist Robert Half Technology.

Based on telephone interviews with 1,400 U.S. CIOs, the report, issued Tuesday, found that a net 3% increase in IT hiring activity, spread across companies of all sizes, is expected in the first quarter of 2010. Seven percent of the respondents expect additions to their staffs while 4% expect reductions, for a net 3% increase.

CIOs in the East North-Central Region (Chicago-centered) and the South Atlantic Region (Washington, D.C. to Florida) are planning the greatest hiring activity, according to the survey.

"After months of slow hiring activity, managers are beginning the year with new budgets and appear ready to carefully expand their IT departments," said Dave Willmer, executive director of Robert Half Technology, in a statement. "Many firms are investing in technologies that improve efficiency and competitiveness."

A broad mix of jobs is expected to receive hiring attention from CIOs. They range from entry-level and staff-level talent and swing all the way to senior-staff positions. The technical skill sets most in demand are network administration, which was cited by 70% of the responding CIOs, to desktop support, 66%, and Windows administration, 62%.

The health services industry stands out as a bright spot in the hiring report, with 16% of health services CIOs planning to expand their IT departments and just 3% planning cutbacks. Many health services CIOs pointed to increased staff needs stemming from the development of enterprise-wide applications. "The health services sector," said Willmer, "needs IT talent to manage the conversion to electronic medical records."

Courtesy : W. David Gartner, InformationWeek, DarkReading
Dec 01, 2009

ANALYSIS

Certifications are not a panacea for cybersecurity woes

As US Congress debates legislation to improve cybersecurity, one problematic idea that appears to have gained some traction is developing a national certification program for cybersecurity professionals.

If certifications were effective, we would have solved the cybersecurity challenge many years ago. Certainly more workforce training, although not a panacea, can help teach workers how to respond to known cyberattacks. However, workforce training is not certification, and organizations, not Congress, are in the best position to determine the most appropriate and effective training for their workers.

Organizations know that simply getting their employees certified will not solve their security challenges. Although a good certification standard might be a measure of a baseline level of competence, it is not an indicator of job performance. Having certified employees does not mean firewalls will be configured securely, computers will have up-to-date patches, and employees won't write passwords on the backs of keyboards. Nor has the increase in the number of certified cybersecurity workers nationwide resulted in any noticeable decrease in the number of computer vulnerabilities, security incidents or losses from cyber crime. Between 2001 and 2005, although the number of Certified Information Systems Security Professionals in North America quadrupled, the number of vulnerabilities cataloged by the U.S. Computer Emergency Readiness Team more than doubled, the dollar loss of claims reported to the Internet Crime Complaint Center increased more than tenfold, and the number of complaints the center referred to law enforcement increased more than twentyfold.

At the federal level, a certification mandate would be little more than a box-checking activity for agencies, akin to many of the Federal Information Security Management Act requirements that tax the federal budget and workforce, but produce few results. Even worse, Congress might go further and impose costly certification requirements on a broad range of private network operators and companies in many major industries. By requiring certification for so many jobs, Congress would in effect create a "license to practice" for cybersecurity professionals.

Licenses are typically only required in professions in which the public is harmed by the absence of licensure. (Perhaps that is an argument to require licenses for members of Congress.) Therefore, the implicit assumption in arguing for a certification program for all federal cybersecurity professionals, those involved in operating critical infrastructure and potentially many more individuals in the private sector, is that the public is being harmed because unqualified workers are filling those jobs -- not because of a lack of talent or insufficient training but because hiring managers cannot distinguish between competent and incompetent cybersecurity workers. That is the only problem that certification (in the form of a de facto license) could fix. However, no proponent of that approach has provided evidence to show that the problem exists, nor is the problem commonly cited in other studies as a factor contributing to cybersecurity risks.

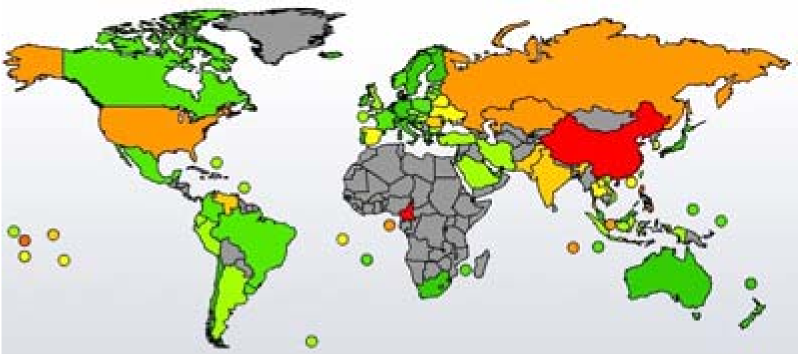
The security community needs to speak up. The cybersecurity challenge is too important to allow Congress to provide a paper-thin response that produces nothing more than the veneer of government action without reducing any real risks.

Courtesy : Daniel Castro, www. fcw.com
Dec 01, 2009

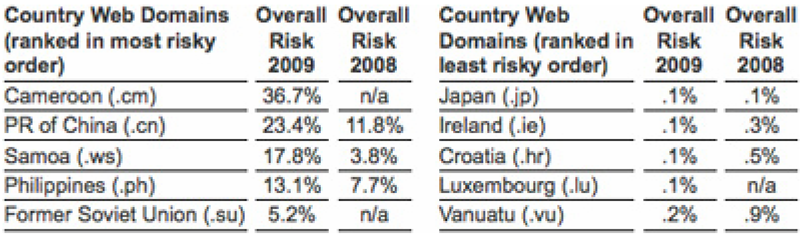
REPORT

Most dangerous web domains

Africa's Cameroon (.cm) has overthrown Hong Kong (.hk) as the Web's riskiest domain, according to McAfee's third annual Mapping the Mal Web report, released today. At the opposite end, Japan (.jp) is the safest country domain, landing in the top five safest domains for the second year in a row. The most heavily trafficked Web domain in the world, commercial (.com), jumped from the ninth to second most dangerous domain, while government (.gov) is the safest non-country domain.



Cameroon, a small African country that borders Nigeria, jumped to the number one spot this year with 36.7 percent of the .cm domain posing a security risk, but did not even make the list last year. Because the domain .cm is a common typo for .com, many cybercriminals set up fake typo-squatting sites that lead to malicious downloads, spyware, adware and other potentially unwanted programs.



Country Web Domains (ranked in most risky order)	Overall Risk 2009	Overall Risk 2008	Country Web Domains (ranked in least risky order)	Overall Risk 2009	Overall Risk 2008
Cameroon (.cm)	36.7%	n/a	Japan (.jp)	.1%	.1%
PR of China (.cn)	23.4%	11.8%	Ireland (.ie)	.1%	.3%
Samoa (.ws)	17.8%	3.8%	Croatia (.hr)	.1%	.5%
Philippines (.ph)	13.1%	7.7%	Luxembourg (.lu)	.1%	n/a
Former Soviet Union (.su)	5.2%	n/a	Vanuatu (.vu)	.2%	.9%

Following aggressive measures from .hk's domain managers to clamp down on scam-related registrations last year, Hong Kong fell 33 spots from the most risky domain in 2008 to the 34th most risky domain in 2009. Now only 1.1 percent of .hk sites pose a risk, whereas last year nearly one in five .hk Web sites were risky.

Among country domains, the People's Republic of China (.cn) and Samoa (.ws) remained in the top five most dangerous places in the last two years.

Additional findings from the 2009 Mapping the Mal Web report include:

- Of the 27 million Web sites and 104 top-level domains McAfee rated for this report, 5.8 percent pose a security risk – that is more than 1.5 million risky Web sites

- Sites registered to the Asia-Pacific Web domains are significantly riskier than the overall Web with 13 percent of sites posing a threat. This region includes the second riskiest domain with the People's Republic of China (.cn), and also, ironically, the safest Web domain with Japan (.jp)

- Ireland (.ie) is Europe's safest Web domain with only .1 percent risky sites.

Courtesy : www.net-security.org
02 December 2009.

REPORT

5 Key Cybersecurity Areas for DHS to Tackle

US GAO Advice Presented at US Senate Hearing on Post 9/11 Security

Five key cybersecurity challenges the Department of Homeland Security should tackle were outlined in testimony delivered Wednesday at a hearing on post-9/11 transportation challenges.

The only witnesses at a Senate Commerce Science and Transportation hearing on post-9/11 transportation challenges Wednesday was Homeland Security Secretary Janet Napolitano, but the managing director for homeland security and justice at the Government Accountability Office delivered a written statement for the record that outlined five key cybersecurity challenges the Department of Homeland Security should tackle.

According to the statement prepared by Cathleen Berrick, the five key cybersecurity areas include:

1. **Bolstering cyber analysis and warning capabilities;**
2. **Completing actions identified during cyber exercises;**
3. **Improving cybersecurity of infrastructure control systems;**
4. **Strengthening DHS's ability to help recover from Internet disruptions; and**
5. **Addressing cybercrime**

Berrick said DHS has made progress in strengthening cybersecurity, such as addressing some lessons learned from a cyber attack exercise, but further actions are warranted. "DHS has since developed and implemented certain capabilities to satisfy aspects of its responsibilities," she said, "but it has not fully implemented GAO's recommendations and, thus, more action is needed to address the risk to critical cybersecurity infrastructure."

Courtesy : Eric Chabrow, Managing Editor, www.govinfosecurity.com
December 2, 2009

ANALYSIS

Is Antivirus Software Dead?

Are we headed towards a future where the idea of an antivirus program, or security software in general, is simply not part of the picture? We might well be, but not for a good long time yet.

In the last few years, consumer computing has come under attack like never before, and the attacks are only growing more clever and more concentrated. In response, there need to be changes to the platforms on which we do most of our computing, and new approaches to securing the platforms we already use.

Antivirus isn't going away. It's just changing its shape to meet the times. Or rather, it had better change, because the other options are few and far between.

The History Of PC (In)security

For a long time, security as we know today simply didn't exist in the PC world. Antivirus software was created because the software we used (DOS and Windows, and their attendant programs) was never designed to ward off attacks. They were single-user environments with little or no network connectivity, so anything that went wrong was typically the user's fault.

The few really severe pieces of malware that circulated during this time were things like Robert Morris's Internet worm of November 1988 -- a program that routed itself through Unix machines by exploiting buffer overflow conditions in that OS. It worked the same way as its descendants: It exploited the always-on nature of networks and flaws in the Unix machines through which it propagated.

Once always-on connectivity and downloaded, rather than boxed software started becoming the norm, malware became commonplace, and the native insecurity of consumer computing became all too easy to see. Antivirus programs were retooled into generic system-protection suites, watchdogs that guarded everything from network connection to on-disk activity.

The problem was that such programs, by and large, were horribly obtrusive and a drain on system resources to boot. A PC might be safer, but it hardly mattered if the machine ran at what felt like half speed. Even worse was the false sense of security that such programs could create. It became easy to assume nothing could go wrong, to behave dangerously, and to consequently be hit by an attack that circumvented the whole defense system.

Now the picture has started to change for the better, thanks both to smarter operating system and program design. But there are serious doubts as to whether extant operating systems can be fixed to accommodate the kind of all-encompassing security that's best suited to fighting back against the way malware works today. Limiting Privileges

The most significant system-protection change that's been made as of late is the limiting of user and program privileges. A program should not, by default, be able to change any aspect of the system at will; it should only do what's required of it. If it wants to modify system settings, it can only do so after explicit admin authorization.

Linux, OS X, and the NT-based editions of Windows (NT, 2000, XP, and up) have this sort of privilege segregation. Up until recently, though, Windows made it too easy not to use this feature: most people simply logged in and ran as administrator because it was too much of a hassle not to. Too many programs were still written under the assumption they could change everything, and would break unless they didn't have admin privileges. But by the time Vista and User Account Control rolled around, things had changed: Windows programmers were now in the habit of writing apps that didn't need root privileges to run. The burden of making computing safer fell to both the platform and application providers.

Several things are immediately noticeable when you run as a non-admin by default. For one, this stops the majority of "invisible" attacks committed by malicious programs that run silently in the background. Two, it's much harder to unthinkingly make systemwide changes. And three, the majority of security problems that used to silently pile up under users' noses and then explode without warning don't. This isn't to say that it's not possible to trick users into running malicious programs at all, but that most of the common ways to do this have become harder.

I'll cite a personal experience as proof that this approach is hugely useful. I encouraged friends who used to run under the bad old security model (run as root) to do the right thing and run as non-admin. They were running Windows XP or Windows 2000, and in every single case, the number of malware infections and other security-related issues dropped off to just about nothing.

So does that mean UAC and similar technologies let you do without antivirus altogether? The short answer is "Yes, but not without some risk."

Zero-day Attacks

If operating systems were perfectly bug-free environments, then limiting user privileges might be a fairly bulletproof way to keep things secure. Unfortunately, bugs do exist, and the creators of malware have turned to exploiting newly revealed and as-yet-unpatched vulnerabilities -- the infamous "zero-day attacks" -- as their next big thing. Recent word about an OS X kernel flaw underscores this all the more: a bug like this could allow someone to write directly into kernel space, and completely bypass mechanisms like limited privileges. The odds are heavily mitigated by usage habits. If you aren't the sort of user who routinely exposes himself to danger -- you don't use file-sharing systems, don't open attachments without a pedigree, don't install software indiscriminately, don't visit Web sites of questionable provenance, and do use a late-model browser -- the risk goes way down. But it isn't completely gone. Even cautious people can get hit with the "drive-by infection", where an ad banner or other normally innocuous Web page element turns out to be a delivery mechanism for evil.

On top of zero-day attacks are a great many other vulnerabilities that remain chronically unpatched by the end user, and which can end up being an open door for the bad guys. Qualys, Inc., a network security firm, did its own research and found that the "half-life" of a given unpatched vulnerability is about 30 days across the industries it surveyed. The most chronically under-patched products were, ironically enough, some of the most widely used: Microsoft Office, Windows Server 2003, Sun Java, and Adobe Acrobat.

Acrobat in particular was not only highly vulnerable and chronically unpatched, but remains a major target of attacks -- almost 50% of document-format attacks charted through 2009 so far use .PDFs as a vector. Some of them do not even require any explicit user action: one recent .PDF flaw could be triggered by simply saving the document in question to the hard drive. Most people don't think of .PDFs as an attack vector, which is precisely what makes them dangerous.

The Limits Of Limited Privileges

How effective are reduced user privileges against such an attack? I talked to Didier Stevens, the researcher who conducted his own investigations into the .PDF vulnerability, and his answer was a little chilling: "It depends on the type of attack. Almost all malware requires local admin rights to execute properly, so it won't work. But if it's a targeted attack and the attacker knows you're running Vista, he can design the malware to perform its actions in this limited context. You don't need local admin rights to steal data, log keys or take screenshots. And a privilege escalation exploit can be used to gain system rights."

This points towards one of the major reasons why these attacks are taking place. They're not simply being done to ruin existing systems, but to steal things from their users. Therefore, many of the attacks that do the worst real-world damage (keylogging, information theft, financial crime, might not require privilege elevation to be effective in the first place. Taking control of the whole system is just a convenient bonus. So preventing privilege elevation alone isn't enough.

Still, how can you insure some degree of system security without the tedium of scanning everything that moves?

Whitelisting

One relatively new approach to system security is whitelisting, where only a pre-defined catalog of programs (identified by a hash or other cryptographic token) are allowed to run at all. Whitelisting makes it tougher for any program to run, whether or not it requires privilege elevation to do its dirty deeds. That makes it a good local line of defense against, for instance, keyloggers. Whitelisting works more like a members-only club where you need an invitation, instead of a sports arena where only the truly unruly and dangerous are ejected by security.

The problem with whitelisting is essentially the same problem with blacklisting: a list needs to be created and maintained. The plus side is that whitelists tend to be far smaller, easier to maintain, and more effective than blacklists. Group Policy in Windows, for instance, makes it possible to whitelist applications based on file paths or file hashes.

One approach is to have the list maintained by a third party. Kaspersky Lab, makers of a popular antivirus product, are using pre-created whitelists as a way to insure that only known, "good" software is loaded and running. The local user can add known-good applications to the list, of course.

It seems unlikely that whitelisting will become a default course of action for most platforms. Rather, it will be a lockdown measure taken by an admin or an end user, and for an environment that should be tightly controlled anyway (e.g., corporate desktops) it makes plenty of sense. It might well be possible to create a whitelisting mechanism that works elegantly enough to be nearly invisible, that like modern firewalls only squawks at the user when something is manifestly wrong. But for now, whitelisting is an option and not a standard strategy.

Trust Models

Another approach, which can work in concert with whitelisting, is trust modeling. One can use the provenance of a file to create a model for how trustable it is -- where it was downloaded from, how the download was triggered, and so on.

Existing antivirus packages Norton 360, for example, already use similar heuristics in combination with conventional scanning -- but it's not likely that trust modeling will take over completely from conventional scanning. As security blogger Dr. Luke O'Connor put it, "the likelihood of being infected by malware will actually increase simply because less scanning will be done and the risk factors will not correlate perfectly with the presence of malware." It's simply not possible to scan everything that comes or goes without incurring an intolerable overhead, and the overhead will only get worse as time goes on.

In short, trust modeling is best used as one heuristic among many, not as an approach unto itself. It can augment an existing method, but unless it's radically reinvented it's not a whole defense strategy.

Retroactive Protection

If the concept of antivirus has been broadened to include generic "system protection," the concept of system protection itself has also been broadened to include more than just stopping bad activity in its tracks. It also now includes ways to gracefully recover from disaster, or to contain disaster.

The disaster-containing approach, "sandboxing", allows any software downloaded or installed to be run in a virtual space and have its behavior analyzed. If the system determines the program's not a threat, its actions can be merged out to the system at large and the program runs normally from then on. The program Sandboxie allows you to do something very much like this right now -- but in the long run, it's something best developed into a full-blown platform feature, rather than an application add-on. The disaster-recovery approach assumes that something will go wrong, but makes it easy to pick up where you left off. Full-system incremental imaging -- like that available in Windows Vista and Windows 7, or the OS X Time Machine -- is a big aid to this, but could benefit from more fine-grained control or integration with the above-described sandboxing technologies to be even more effective. Example: being able to take snapshots of different aspects of a system state, such as the states of different programs, and selectively roll them back as needed if they are damaged.

Linux, Mac: Uncharted Territory

One area where many of these new techniques might well be tested in a live context is not Windows or even Linux, but the Macintosh. Malware protection for OS X has typically been very meager, and a good deal of that is because the Mac simply hasn't been that big a target for malware. Yet. If it does become a bigger target, it will have more protection than Windows did simply by dint of having processes not run as admin by default.

But, as described above, that approach only goes so far. If the Mac becomes popular enough to also be a regular malware target, then it will experience the same baptism by fire that Windows did. Then Apple will either have to add new platform-level features to fight such things more elegantly (e.g., whitelisting), or add antivirus products as a regular presence there. That by itself would knock out one of the major selling points of the Mac as a platform: its general lack of malware and inherent security. For now, however, it's a safe place.

The same could be said for Linux as well. Its measurable desktop marketshare is far below that of Windows or Mac, but that doesn't make it immune from being a target. And, as above, the fact that non-essential processes don't run as root is not a cure-all, and in many cases isn't even required to do the kind of harm most malware authors are after. It might not be possible to know how secure the average desktop Linux stack is from concerted attack without it actually becoming broadly used and therefore broadly attacked. There's something of a paradox here: if few people use Linux, it remains relatively untargeted but it also remains less use-tested in the real world, where attacks on computers are a way of life.

The ideal solution to malware would be a secure platform, where malware was a thing of the past. Unfortunately, software's very complexity makes a de facto secure platform almost impossible to guarantee.

The best long-term solutions will be platform-based. Such platforms can't be perfect, but they can approach a greater degree of security through continual, rigorous improvement (both internally and externally). The most useful interim solutions, though, will still come from third parties. What will be and already is pass is the old-school approach to system security, the "scan everything that moves" philosophy that creates at least as many problems as it solves.

Antivirus isn't dead. But it must evolve into a true complement to the kind of computing we now do, and to the threats we're now trying to guard against.

Courtesy : Serdar Yegulalp, InformationWeek
Nov. 7, 2009

REPORT

Cyber spies are costing billions in Australia

AN INTERNET crime centre should be set up by the Rudd Government so people can report spam, data loss, online scams and web fraud, a report by the Australian Strategic Policy Institute says.

The report by Alastair MacGibbon, a cyber security expert, says the Government needs to impose tighter control on ''backyard'' internet providers and adopt an enforceable code of conduct.

It says the Government has been slow and reactive and failed to combat cyber crime and espionage, which cost billions of dollars a year and threaten the security of government agencies and businesses.

''It is time for Australia to consider whether the current 'light touch' approach towards the internet has served its use-by date,''.

''It allowed Australia to develop its internet capacity in a relatively unfettered and competitive way, but at the cost of safety and security, which may now be inhibiting future growth.''

The report said the gap between the cyber security problem and the nation's capacity to deal with it was widening, and the Government should increase its efforts against economic espionage and expand its intelligence support for the private sector.

''Access to sensitive information, like the price a large exporting company will accept for wheat, coal or iron, could cost the nation billions of dollars in lost export revenue, either through purchasers driving a well-informed harder bargain or being undercut by a rival seller,'' it says.

''Yet - on the whole - such information is stored and accessed in corporate systems which have questionable defences, and often handled by staff unaware of the value of such information.''

The report says the implementation of a national broadband network should be matched by a more extensive cyber security plan because the boost to internet speeds will lead to increased computer use. One possible measure would require registrars of internet domain names to improve identity checks of applicants.

Courtesy : JONATHAN PEARLMAN, www.smh.com.au
December 4, 2009

REPORT

Do firms delay upgrading because of security fears?

The furore surrounding Microsoft's Black Screen of Death may finally be dying down, but it has raised more serious concerns about the integrity of new operating systems and whether firms are deliberately delaying upgrades to avoid becoming a bigger target for hackers.

That is, at least, according to security giant Symantec, which has commissioned a new survey into the upgrade habits of enterprise customers, either with alarming speed or uncanny foresight.

The vendor interviewed nearly 1,500 IT managers in UK, France, Germany and Italy and found that just over a third had major concerns over hackers targeting newer desktop software to find vulnerabilities.

A quarter said they would hold off on upgrading for at least another 12 months, while two-thirds said negative press coverage played a role in influencing their decisions to upgrade.

Which is all very well, but are IT decision makers really that easily swayed by so-called 'negative press coverage'? The letters and comments we get here at V3 would seem to suggest not.

Surely the level-headed IT manager would be wise enough to realise that any new operating system or desktop software is likely to receive an unduly large amount of media scrutiny, including how safe or otherwise it is.

We all know that bigger security risks lie with systems remaining unpatched against known flaws, whether those systems are fresh from the factory or not.

Courtesy : www.security-watchdog.co.uk
http://www.security-watchdog.co.uk/2009/12/do-firms-delay.html

ANALYSIS

Seven skills for the future information security profession

Last week I was lecturing at Royal Holloway University of London, as I've done for the past ten years or so. I've noticed a steady increase in sophistication in the audience over the years, and more recently an encouraging urge to challenge accepted wisdom. It's a reassuring trend, as many of today's practices today are questionable and future security requirements will demand a different set of skills from the ones we tend to find in security functions today. So what are these skills? And why aren't we grooming our apprentices in them?

Let's answer the latter question first. One reason is because security managers don't seem to be very good at forecasting emerging trends. Two leading information security institutes, ISF and ISC2, have attempted to predict future skills from member surveys. Unfortunately, that's not a reliable method of forecasting the future. The questions might not be the right ones (you don't know at the outset) and many of the members polled will not have the insight or time to make a realistic forecast. This is why these forecasts look more like a blueprint from ten years ago for the in-house function of a major bank.

Any kind of future planning requires three things. Firstly a selected group of subject matter experts and researchers that collectively possess knowledge of emerging trends in security, technology, politics, business, legislation, economics and social science. Secondly an environment in which they can pool knowledge and explore interactions between emerging trends. And thirdly a process in which they can 'wire together' a realistic road map of events, developments and impacts. There are existing methodologies for this, such as Technology Road Mapping, a process I've used many time with reasonable success.

In the absence of a proper planning exercise, I shall have a go at using my own intuition to forecast some emerging core competences that we will need for the longer term. Some things seem very clear about the long term future. Firstly most infrastructure and applications will be in the cloud rather than in-house, requiring more user education and less operational security. Secondly, risks will get bigger, more sophisticated and more damaging. Thirdly, regulatory compliance will get tougher and the penalties for failures more severe. And fourthly, social networks will be the primary means of communicating with company staff.

Thinking on these points, here are my seven top skills for the future security professional.

1. **An understanding of psychology to plan interventions that can might actually have an impact on the behaviour of staff**

2. **Social networking skills to influence and harness the support of large numbers of users and customers over social network**

3. **Skills in marketing communications to design compelling, effective awareness campaigns and materials**

4. **Strong commercial management skills to specify and manage security across business partnerships and outsourced supply chains**

5. **Sophisticated crisis management skills to safeguard the organisation's intellectual assets (not just the data) in the likely event of a major security breach**

6. **Digital forensic skills to detect and prove when an intruder has infiltrated or modified the organisation's intellectual assets**

7. **A sound knowledge of legal and regulatory requirements and issues**

In addition, a thick skin to take the flak from our increasingly brutal management teams might also be a useful survival skill. Further suggestions are of course highly welcome.

Courtesy : David Lacey's blog; www.infosecurityadviser.com
06-Dec-2009