CCC News
Control Computer Crimes
Issue 0011 - 30 November 2009

Message from the Editor

Welcome to the Eleventh issue of CCCNews Magazine.

In this edition, 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 report on – "IS Security Predictions for 2010". This report discuss Pirated Software, Social Engineering and Criminals taking to cloud computing as big burning issues facing IT Security industry during 2010.

In another interesting survey analysis, we discuss "5 Mega trends, which increases IT Security Risk". These mega-trends are Unstructured data (79 percent of responses), Cyber terrorism (71 percent), Mobility (63 percent), Web 2.0 (52 percent) and Virtualization (44 percent). These technologies are here to stay till new technologies replace them. To work safely, the industry need to workout strategies, policies, technologies and human resources, which will mitigate and manage the security risk due to these mega trends.

In another interesting analytic story, we discuss six greatest threats to cyber security for any nation. There are Foreign nations, criminal groups, hackers, hacktivists, disgruntled insiders and terrorists. No nation can escape these threats. To survive under difficult times and threats, all nations need to work individually and collectively to address these threats.

Similarly, we bring some more analytical articles on "why cyber crimes are kept secret"; "10 issues overloading IT Managers"; "11 secure tips for secure online shopping"; "seven deadly internet sins" and many more to enjoy and learn from them to keep your IT infrastructure secure.

Happy reading,

Rakesh Goyal
Editor

CONTENTS

CCC News
Issue 0010
15 November 2009

Rakesh Goyal
Editor
editor@cccnews.in

Published by
CCC Media
Mumbai, India

LAST ISSUE DOWNLOAD COUNT : 160,000+

ANALYSIS

Why Cyber breaches are kept secret

Corporate victims of cybercrime are reluctant to come forward as they fear the publicity will hurt their reputations and profits.

Cybercriminals regularly breach computer security systems, stealing millions of dollars and credit card numbers in cases that companies keep secret, said the FBI's top Internet crimes investigator.

For every break-in like the highly publicised attacks against TJX and Heartland Payment, where hacker rings stole millions of credit card numbers, there are many more that never make the news.

"Of the thousands of cases that we've investigated, the public knows about a handful," said Shawn Henry, assistant director for the Federal Bureau of Investigation's Cyber Division. "There are million-dollar cases that nobody knows about."

Companies that are victims of cybercrime are reluctant to come forward out of fear the publicity will hurt their reputations, scare away customers and hurt profits. Sometimes they don't report the crimes to the FBI at all. In other cases they wait so long that it is tough to track down evidence.

"Keeping your head in the sand on filing a report means the bad guys are out there hitting the next guy, and the next guy after that," Henry said.

He said the cybercrime problem has gotten bigger over the past three years because hackers have changed their attack methods as companies have tightened up security.

"It's absolutely gotten bigger, yes, absolutely," he said.

That is because the Internet is rapidly growing as a tool for commerce. As it does, consumers and companies alike are exposing valuable data such as business plans, credit card numbers, banking information and Social Security numbers.

"There are hundreds of billions of dollars that traverse the Internet," he said.

Seeking easier targets

Cybercriminals are now looking beyond large companies, which in the past 10 years have bolstered security on their networks using products from software companies including Symantec, McAfee and Trend Micro. Cisco Systems, International Business Machines and Websense also sell products to protect computer networks.

Instead, criminals are attacking small and medium-sized companies that don't have the inclination, money or expertise to prevent cybercrime.

They also target corporate executives and other wealthy public figures who it is relatively easy to pursue using public records. The FBI pursues such cases, though they are rarely made public.

On 4 November, the FBI warned of major fraud cases involving the theft of online banking credentials belonging to small and medium-sized businesses, local governments and school districts.

In this case, as in others, people hired through work-at-home schemes were used to move the money overseas.

A similar approach was used in a scheme that defrauded the Royal Bank of Scotland's RBS WorldPay of more than $9 million. A group, which included people from Estonia, Russia and Moldova, has been indicted for compromising the data encryption used by RBS WorldPay, one of the leading payment processing businesses globally.

The ring was accused of hacking data for payroll debit cards, which enable employees to withdraw their salaries from automated teller machines. More than $9 million was withdrawn in less than 12 hours from more than 2 100 ATMs around the world, the Justice Department has said.

Henry said it was relatively inexpensive to pull together a cybercrime organisation.

Some groups consist of a core of just about a dozen people, including strategists, hackers and programmers, who can get started with a budget of a few thousand dollars to set themselves up with computers and broadband access.

When they are ready to launch an attack, they might hire hundreds more people who help them launder the money. Known as "money mules", these people are often found through "work-at-home" schemes,

where they are hired to cash cheques for a few thousand dollars, keep a percentage and send the rest back to the core group.

"I think there are people who are ignorant completely and others who have their head in the sand," said Henry.

Courtesy : Reuters; www.itweb.co.za
25 Nov 2009

SURVEY

IT Security Predictions for 2010

Researchers from IBM and Sophos shared their thoughts on what the security threat landscape will look like for enterprises and consumers alike in 2010. Their predictions run the gamut from threats to social networking sites to an increase in attackers targeting hosted services.

In the past 12 months, the security industry saw a resurgence of worms, an increase in rogue antivirus software scams and much, much more. But with the sun setting on 2009, security pros are turning their eyes toward the coming year.

In it, they see a future with a threat landscape not all that much different from the present – but with a few changes in scenery. Here are the top 3 predictions from IBM's X-Force research team:

1) **Pirated software** will drive insecurity in much more dynamic ways than previously realized. Users of pirated software are afraid to download updates, thus are exposed to security risks because their software is entirely unpatched. Also, newer versions of pirated software now come with malware pre-installed. As a result, users of pirated software will become the new "Typhoid Marys" of the global computing community.

2) **Social engineering** meets social networks and ups the ante for creative compromises. Criminal organizations are increasingly sophisticated in how they attack different social networking sites. For example, Twitter is being used as a distribution engine for malware. LinkedIn, however, is being used for highly targeted attacks against high-value individuals. We will see these organizations use these sites in creative new ways in 2010 that will accelerate compromises and identity theft, especially as new commercial applications increase the disclosure of valuable personal information on these sites.

3) **Criminals take to the cloud**. We have already seen the emergence of "exploits as a service." In 2010 we will see criminals take to cloud computing to increase their efficiency and effectiveness.

The services referenced in point three can run the gamut from services to verify malware isn't detected by security tools to launching large-scale infections of chosen malware, noted Robert Freeman, senior technologist for IBMGlobal Technology Services.

"The exploitation industry - at least as it relates to criminal organizations - is becoming increasingly service-oriented," he said. "It is less about zero-day exploit sales and more about providing useful mechanisms at competitive prices for attackers of various sizes."

Social networks have increasingly gained ground as an attack vector, though it is not nearly as prevalent as e-mail. Still, worms using social network data can be even more successful, as they can contain personalized messages mentioning a victim's family, friends and interests based on information from their social networking profiles, said Jon Larimer, malware researcher for IBM X-Force.

"However, worms that spread through the sites of social network messaging systems will be short-lived, as the site operators have the ability to filter messages and stop worms pretty quickly," Larimer added. "This means that the most successful worms of this type will use social networking data but will spread through e-mail, which is more decentralized."

Over at Sophos, Security Analyst Michael Argast opined that attacks against hosted services will see an upswing as well.

"I expect that the continued interest in these services, combined with outages, targeted attacks and leaks will keep the balance of internal security vs. hosting data in the cloud to continue to be an area that will vex CISOs in the year to come…they will be under targeted attack, both directly via security vulnerabilities and attempted intrusions and indirectly through credential theft and phishing attacks," he said.

Perhaps unsurprisingly, Argast predicted the focus on targeted data theft will rise, but with attackers going through more indirect routes to get data. That includes using social networking sites, he said.

"The recent rise in consumer privacy data being lost via iPhone apps and Facebook apps is one example, but also examples like criminals signing up for direct access to credit bureaus, and taking advantage of the down market to involve insiders," he said. "Also, less obvious targets of data theft will be more common - smaller businesses will be under attack…A nasty example of this trend starting this year was the rise in attacks on the higher education market - since these organizations often struggle with IT security due to their open network access policies, but at the same time have hundreds of thousands of student records with confidential data."

"I expect next year, a rise in attacks on health care organizations will occur for similar reasons, continued attacks on retailers big and small, tax authorities, school systems - anywhere where lots of records are

kept by organizations that haven't traditionally had best practice security in place," he added.

Courtesy : Brian Prince; http://www.eweek.com
25-Nov-2009

ANALYSIS

Top 10 issues overloading IT managers

As we bring our Information Overload summit to a close, we have decided to name and rank the biggest culprits for the overload, the issues which more than anything else are causing companies to drown in a deluge of data..

Some of these problems have been around since the dawn of the computer age. Others are new, brought about by new technologies and different ways of working and servicing IT infrastructure. Nevertheless they all cut into the IT manager's time.

Honourable mention: Web management

Iain Thomson: Watching what people are doing on the internet is one of those tasks that IT managers are increasingly being tasked with, but I've yet to meet one that like the job.

Managers are increasingly overloaded these days and the prevailing view is they have more than enough on their plate without playing censor to an entire company. Yes, if someone's spending all their time looking at porn on the internet that's an issue for a company, but it's a problem in management, not in IT, seems to be the prevailing view.

If a company is that worried about web management then they should hire the services of someone like Websense to do the job for them, not force stretched IT departments to take up the role. The only time the IT department should get involved is after a complaint – either from someone on the floor who's spotted what's going on or from a manager who's concerned about lost productivity.

Shaun Nichols: The tasks of monitoring and managing web access has only become more difficult as interest in new web services has grown. Now, sites such as Twitter and Facebook aren't purely for consumers, but many companies are also making use of them for promotion and customer relations.

This means that simply blocking everyone off from these services is no longer possible, as they have become work tools.

At the same time, more and more new sites are popping up, more blogging platforms, social networks and casual gaming portals are emerging every day, making it far more difficult to keep up with what can and can't be blocked.

Then on top of it all, there's the ever-growing ranks of malware infections and phishing scams connected to web applications and tools, making the risk of security breaches through the browser stronger than ever.

As such, the task of web management at the corporate level is becoming both more complex and crucial at a most inopportune time.

Honourable mention- Integration of Web 2.0 tools

Shaun Nichols: It's one thing to have to deal with cloud computing, taking existing processes and applications online. It's another headache entirely when you're asked to find completely new uses for web tools.

We've all known at least one or two bosses and executives that love to throw about the latest buzzwords and demand that everyone adopt the latest business crazes, even if nobody is completely sure why they are doing so. Blogs, wikis and social networks are increasingly popular for companies as internal tools, and their implementation can be quite a task for IT staffs, particularly when nobody is quite sure how they will be used.

The only reason that we haven't placed this issue higher on the list is because it isn't really IT's problem. Yes, setting up and managing those services takes a bit of time and effort, but the real issue is how those services will be used, and that is mainly the concern of executives, managers and end users.

Web 2.0 tools can be very valuable to a company, but they are only useful when implemented correctly and used to improve communication and collaboration. Really, it's far more a human issue than a technological one.

Iain Thomson: The growth of Web 2.0 has caused some additional headaches for IT managers, but it's not as bad as it could have been.

Because much of this content is user generated then the demands on the T ma nager's time aren't too onerous. It's setting up the systems in the first place that's the real time waster.

A lot of I managers have also been rather smart about how they deploy such systems. Increasingly they will set them up, but in the spirit of user generated content they are tapping the users to police and edit such information. It's a smart move, but also a logical one.

10. Cloud integration

Iain Thomson: In many ways cloud is nothing more than a fashionable term from client/server but no matter – it's this year's thing and as such there's strong pressure on IT managers to get into cloud services.

While cloud computing offers many advantages it is increasingly looking like firms are better off hiring third parties to set up and run a cloud infrastructure. EMC is currently working with Intel to set up a do it yourself cloud system and Amazon is involved too. But building a cloud syste3m from scratch is still an enormous responsibility.

It's also something that shouldn't be rushed into. Some board members don't seem to get this. A cloud system is incredibly complicated to set up and operate and the consequences if it all goes wrong are huge.

Shaun Nichols: One of the biggest problems of could integration is that not everything goes into the cloud. As a result, companies are left with a mixture of cloud-based services and locally-stored applications.

This presents several headaches, the first of which is integration. How do you get your cloud applications compatible with your other applications, and how do you make sure that everyone is on the same page?

Then there's the management issue. Instead of simply having to manage who has access to applications and accounts on the local network, administrators now also have to keep track of online identities and access to web based services.

9. Internal/external data breaches

Shaun Nichols: IT has enough to worry about these days, and adding new security worries only adds to the problem.

Companies should already have policies and protections in place to deal with security and data breaches, but the growing piles of data only make it harder. As new storage systems go live and archives expand, the task of managing and tracking access only gets harder, and sometimes files and users can slip through the cracks.

Then of course there's the worry that not only are files left unencrypted and drives unaccounted for, there's also the possibility that people purposely decide to steal data and destroy systems. With more data than ever and fewer people to manage it, the chances of a disgruntled employee causing damage to a system only increase.

Iain Thomson: As we're seeing the greatest threat to a company's data is not the spooky external hacker, but the enemy within.

The insider problem is something that IT managers are only just getting to grips with. The biggest threat is still the clueless user – the idiot who decides to set up their own Wi-Fi point and forgets to lock it, the user who clicks on an unidentified attachment or the half-wit who sets their password as Passw0rd.

But there is also the problem of the wilful thief. This can either be the employee who is leaving for another job with a competitor and is sweetening the deal by bringing over corporate data or someone with a grudge who wants to cause harm. With more and more people getting laid off it's this scenario that is increasingly a concern.

8. OS migration

Iain Thomson: Shaun and I disputed this in the list, with Shaun thinking it should barely have made an honourable mention. But with the launch of Windows 7 it's higher on the priority list than it has been in the past.

Windows 7 is going to make operating system migration a much bigger deal than it has been in the past. Most companies have steered clear of upgrading from XP to Windows Vista because of the failings of that operating system. Instead XP, which is stable, has been left to rule the roost.

However, upgrading these systems to XP is going to be a major headache. To move from XP to Windows 7 will require a full system wipe and that spells a lot of trouble. I suspect IT managers are going to simply suggest a full hardware upgrade instead.

For those corporates not in Windows the problem is much simpler. If you're running Linux then the steps for upgrading the operating systems are much simpler but still problematical. If Apple is the company's operating system of choice then the job is also less difficult, but such companies make up a tiny fraction of the market.

Shaun Nichols: Last week we noted that the operating system was becoming less and less relevant to the actual practice of computing. And while I maintain that belief, I must also concede that it's still a huge issue, particularly in times of transition, such as what we are now in with the move to Windows 7.

This latest transition could be especially tough for the many companies who opted not to move to Windows Vista. For those companies, there is the unenviable task of taking stock of which machines are capable of running Windows 7 and which will need to be upgraded or replaced.

If you decide to switch to Linux or OS X, you have other headaches to deal with, such as making sure you have the same applications or at least new ones which can handle the old files. While operating systems have become far more compatible in recent years, there are still big problems to deal with.

7. Patch deployment

Shaun Nichols: This is a given to anyone who has spent time in enterprise IT. With more users, more workstations and more software to manage, the process of installing patches and fixes only becomes more difficult.

The addition of virtualised machines and servers only makes things more complicated, particularly as malware loads increase and exploits become increasingly common and dangerous.

One bit of relief has come from the vendors. Companies such as Microsoft, Adobe and Oracle have begun issuing regular, scheduled updates rather than issue individual fixes for each bug. This allows administrators to set a date and plan ahead for testing and deployment of patches. The down side is that this can leave machines vulnerable for a longer amounts of time, but for most the trade off is more than welcome.

Iain Thomson: Patching has certainly improved, and the lot of the IT manager has got a lot easier. But not so fast Shaun, a lot of these easing up has come from a difference in malware writing rather than a great effort from application and operating system vendors.

In the good old days when malware writers were simply maladjusted amateurs computer networks were beset by worms whose jobs was to spread as fast as possible and provide the author with bragging rights. In such circumstances when a worm hit the IT manager had to drop everything and patch systems as soon as possible.

But these days the opposite is true. Malware writers want to get in under the radar and steal all that valuable information without being recognised. Patching is still essential, but the need for it is less visible and I fear this may be fostering a dangerous sense of complacency, particularly given the speed with which patches are reverse engineered.

6. Remote workers

Iain Thomson: It's difficult to dispute the value of home working in most cases. People working from home are generally more productive, happier and healthier than their office brethren. I can say this with some confidence since both Shaun and I are writing this in the comfort of our own homes and communicating electronically.

But home workers are often not the friend of the IT manager, under certain circumstances. If the worker is using their own PC at home then it is an unknown quantity and the IT managerm can't control the security settings on the remote worker's computer. The one time (we know about) that Microsoft has lost source code for example came about because a home worker got an infection and allowed hackers into the network.

The other problem comes when staff are working overseas on business trips. When you entering the US and many other countries then the government retains the right to take a copy of the hard drive of any computer entering the country and that can be a security nightmare.

The simplest way to handle this is to issue company hardware to remote workers. For those working from home this ensures that security standards are kept. For those travelling a blank laptop can be issued and then confidential data can be sent via VPN once the traveller has cleared customs.

Shaun Nichols: Iain, we are lucky in that we were working from a branch office to start with. Since even when we are in San Francisco we're remotely accessing systems based in London, telecommuting is pretty much a non-issue. It's also a nice snapshot of just how much we take for granted the work behind setting things up for remote workers.

For IT staff, this sort of thing can be a major headache, as evidenced by the number of companies which specialize in setting up and managing network access and management for telecommuters. Aside from the headaches of leaving the network open to outside

connections, there's also the matter of access controls and oversight of what information is being accessed and stored.

As Iain noted, one good way to solve this is to simply issue employees with hardware for home use, but not every company has an extra notebook to hand out, and sometimes employees will simply insist on connecting with their own machines. Either way, you're left with more machines to manage and more traffic to worry about.

5. Compliance

Shaun Nichols: Whether its Sarbanes-Oxley, HIPAA or any of the other regulatory acts, more and more firms are being tested with compliance regulations. Dictating everything from access policies to the use of encryption, local and federal laws are making file protection and management mandatory.

This is a big enough issue on its own, but when combined with the increasing amounts of data and stricter financial pressures, ensuring that everything is in compliance can become a huge task.

What's even more troublesome is the risk involved with not being in compliance. Violations alone can be bad for a company, but should a massive data breach or other incident occur while a company was not meeting government standards, the consequences could be devastating.

Iain Thomson: While regulations are essential for the maintenance of stable, beneficial capitalism they are also the bane of the IT managers life.

Companies are increasingly having to hold increasing amounts of information in order to comply with the regulations government has been laying down, and it needs to be stored for years but accessible when the auditors come knocking.

When these regulations were first brought in management just threw up their hands and ordered the IT department to save everything. After all, storage was dirt cheap and getting a few hundred extra gigabytes cost a pittance compared to the fines the company would accrue if they were found to be in breach of the law.

This however is no longer sustainable. The amount of data companies are generating and the costs of keeping it are growing at such a rate that we are going to need new storage options, or better regulations.

4. Overmanagement by non-IT staff

Iain Thomson: To my mind this should have been higher but Shaun talked me down. I've just lost count of the number of IT managers moaning about the fact that they are being asked to do the impossible by management that have no idea about technology.

The cycle usually goes like this. A salesperson gets a meeting with a senior manager and promises them the moon on a stick with a flashy demo, lots of promises and occasionally a night on the town. I know of one senior IT salesman with a large corporation that can get virtually anythingt through expenses in the quest for a contract – hookers included.

The manager who's been one over then tells the IT manager about this new technology and insists that it be implemented. With any luck they will do this before the contract has been signed, since they need the IT manager to tell them if the plan is feasible or not. However, it isn't unknown for the whole deal to be signed and sealed before the IT manager even knows about it.

The second way this manifests itself is when managers ask for the impossible. They say a little knowledge is a dangerous thing and this is true, especially in IT. There are too many cases of managers watching something like 24 and ordering such systems to be installed in their company, only to be told that they are living in a fantasy world, in the nicest possible way.

Shaun Nichols: There's the old saying that too many cooks spoils the broth. It's even worse if several of those cooks lack the culinary skills to make so much as a bowl of cereal.

We're still in a strange era in that a great many senior executives are at an age where they need to know technology but are just not able to completely grasp it. The type of people who only a few years ago learned how to send email and still worry about teenage anarchists "hacking the mainframe." These are the same people who see IBM commercials during golf telecasts and on Monday morning say "I was watching Tiger Woods sink a putt this weekend when I got this idea I think we should try…"

Add the aforementioned to Iain's picture of slick salespeople and junior executives who feel it is fine to promise the world and then dump all the actual planning and implementation off on the IT people, and you can understand why your company's tech staff can be more than a bit cranky at times.

3. Virtualisation

Shaun Nichols: Virtualisation can be a great way to save money, increase efficiency and generally give IT departments much more to work with.

Unfortunately, it can also make things far more complicated. The problem is elementary: you take one physical server and turn in into several virtual ones, and you will be left having to monitor, manage and maintain far more servers than you ever had to before.

The number of tools and systems for managing and monitoring virtualised server deployments is growing every day, which only pays further testimony to how complex the task can be. Not only do you have to manage the various virtualised servers themselves, but there is also the hypervisor and virtualisation platform as well as the server hardware itself.

All in all, a virtualisation deployment can be a major asset to a company, but it can also be a nightmare for IT when problems arise.

Iain Thomson: Virtualisation is like living in the Playboy mansion with a whisky swimming pool – great idea but in practice it can be less than edifying, as anyone who's seen Hugh Heffner or the effects of liver failure can tell you.

Nevertheless it is the wave of the future, and as some have pointed out can bring major cost savings in terms of operation costs. But the downside is increased management time and complexity.

There's no getting around the fact that we will all be running a lot more virtualised servers in the future. But how we handle them will be the true test of the technology. I suspect that we're going to see a major shift in management tool technology, of the same scope as the shift to object orientated programming revolutionised the software industry. It is needed, and cannot come soon enough.

2. Storage

Iain Thomson: As companies and individuals we are now generating more content than at any point in human history. We're also having to store it for compliance purposes and this presents the IT manager with something of a problem.

It's an understandable human need to store everything that's done online. However, simply storing the data isn't the only problem, it's when someone wants to access it that the real fun kicks in. A good storage strategy needs to address both concerns.

Storage is essential, particularly off-site storage. If the company takes a physical hit you need off-site backup to be safe. In my first journalism job we had a break in and lost all our hardware, with two issues of the magazine and one handbook on and no backups. It took three weeks of hard labour (ie 100 hour weeks) to pull us back from financial ruin.

So an IT manager needs to be a master of the craft. Simply copying everything on the hard drives takes a huge amount of space and is rather wasteful. After all if someone has sent a large Powerpoint presentation to fifty staff there's no point in saving it 49 times when once will do. This explains why the bidding for Data Domains was so fierce.

Storage also remains a security problem. It's scary how often companies create storage systems that don't involve encryption. Miss this and the company not only faces a loss of data but also a law suit.

Shaun Nichols: This is of course the heart of information overload. We are creating more content than ever, through more channels than ever, with more tools than ever and it all has to go somewhere.

No matter how many analysts, hardware vendors or service providers we talk to, the warning is always the same: don't just throw more hard drives at the problem. Archives have become so large and so complex that it's not sufficient to simply increase the storage volume any more. Indeed, with budgets shrinking it isn't even possible for many companies.

Instead, the constant theme seems to be make better use of the storage you have. Iain mentioned de-duplication, erasing multiple copies of a file you only need to back up once. Other suggested fixes include tiering data, moving to online backup systems and using snapshots rather than full system backups.

Whatever the remedy, it's clear that simply expanding storage isn't enough any more, companies have to take a new look at how they manage their data and approach storage.

1. Budget constraints

Shaun Nichols: There's never a good time for a recession, but from a technological standpoint, this latest one could not have hit at a worse time.

Advances in hardware, software and network technology have given birth to entirely new fields of the industry, and just as many companies were looking to see the fruits of those new technologies, the economy took a dive and IT budgets everywhere took a major hit.

When you get down to it, the top two items on the list are pretty much interchangeable. The amount of data keeps growing and the budget for managing it keeps shrinking. From these two issues the entire problem of information overload really springs.

The crisis may, however, have a silver lining. Just as the Great Depression brought about economic and social reforms that improved the quality of life in later decades, this latest recession could necessitate advances in the approach to IT management and the business culture that will help speed up the recovery.

Having learned how to do more with less, IT departments could emerge from the crisis better able to manage their systems and with a greater understanding of how to squeeze the most out of the resources on hand.

Iain Thomson: Oh Shaun, you are a little ray of sunshine at times. I hope you're right about the recession being a good thing.

There is never enough money to do everything in IT. The only people with unlimited budgets are government security systems and even they must bow to the accountants at times. I suspect in a hundred years from now IT managers will still be complaining about having to do too much with too little funding, unless we're reached the Singularity by then and are no longer running the show (and I for one welcome our new overlords.)

But your broader point you may have hit the nail on the head. We have to learn to do more with less, and if the recession helps that then it's certainly a silver lining in a very dark cloud.

Courtesy : Iain Thomson; www.v3.co.uk / www.pcauthority.com.au
November 16, 2009

SEQUEL

Why IT managers drink

10 issues that drive them to the bottle

PCAuthority just carried a great feature "Top 10 issues overloading IT managers," that everyone should read. Nearly all of us who work with these demon machines depend on the IT folks. There are a lot of things we can do to make their lives easier (or at least not make their lives more hellish.)

The ten issues are:

10. Cloud integration (is waaaay complicated and must be done right. Integrating with local resources is both a technical and management issue.)

9. Internal/external data breaches (Think new technology, new hacks, external bad actors and internal bad actors. Oh yea, and consider the clueless twits who click on malicious attachments in spam.)

8. OS migration (W-I-N-D-O-W-S-7. This is really ugly if the enterprise opted out of Vista. Migration from WinXP to Win7 is serious work.)

7. Patch deployment (A big job that is made bigger by more users plus more work stations plus more software plus virtualized machines times more malware that is more dangerous.)

6. Remote workers (Those using their own machines are a real pain.)

5. Compliance (Regulatory acts like Sarbanes-Oxley and HIPAA as well as local and federal laws mean that most companies are holding onto more data.)

4. Over management by non-IT staff (They just don't understand, especially the sales folks who promise customers the impossible.)

3. Virtualization (This offers great benefits and great complexity)

2. Storage (Adding drives isn't the answer.)

1. Budget constraints (recession = do more with less.)

The writers also give honorable mention to:

-- Web management (Regulating on-the-job gaming, porn browsing, Facebook, Twitter and such should be a management responsibility.)

-- Integration of Web 2.0 tools (Blogs, wikis and social networks are useful internal tools, but they are work for IT)

As I write this, our IT staff is struggling to replace a major email server. Of course it started acting up late Saturday night.

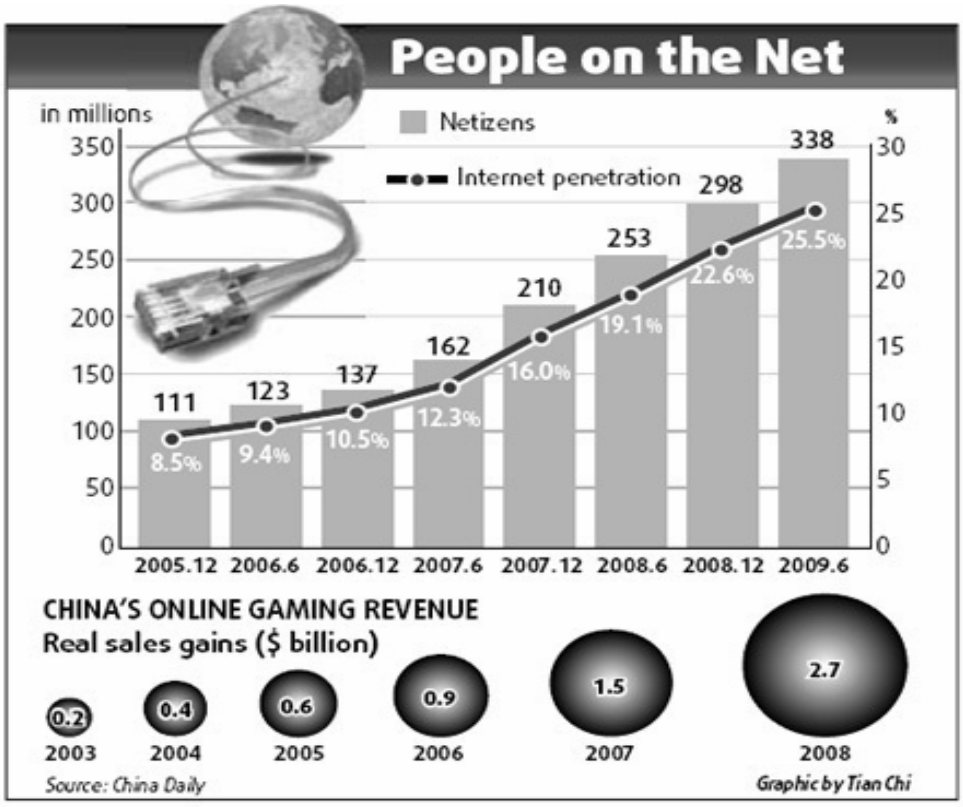
Courtesy : Tom Kelchner; sunbeltblog.blogspot.com
23 November 2009

REPORT

Hackers Exploit Chinese Online Gaming

The craze in online games among Chinese netizens is fueling an increasingly lucrative market for computer hackers, security firms have said.

"There is a huge underground market and major revenue comes from selling game accounts or virtual items stolen from hijacked computers," said Zhang Yumu, vice-president of Beijing Rising International Software Co, one of the largest domestic security firms.



A recent report by State broadcaster CCTV said that Trojan horse attacks, which allow hackers remote access to a targeted computer system, are making up a market that is expected to be worth 10 billion yuan ($1.4 billion) this year.

The CCTV report, aired on Wednesday, cited a hacker saying he could get hundreds of thousands of yuan every month by hacking into computers and stealing the user's personal information and game account.

The hacker would then log into the game account and transfer all the valuable virtual items such as weapons and clothes and sell them through online sites, according to the report.

The hijacked computer's accounts were later sold for other uses, such as participating in online attacks and piling up false traffic data.

Trojan horse attacks have became a major online threat in China in the past few years, accounting for more than 95 percent of all the online attacks in the country, according to figures from online security firms.

Zhang from Rising said the number of Trojan horse attacks surged 10 times last year in China and the number is expected to further increase 60 percent this year.

But he does not think the whole market turnover is as high as 10 billion yuan, estimating that the real market value is about 100 million to 1 billion yuan.

"The rise of the attacks increased in line with the rise of online games in China," he said, noting that over 95 percent of the revenue of the Trojan horse attackers came from selling online game accounts and virtual items.

Sales revenue of China's online game market grew 76 percent in 2008 to 18.3 billion yuan, according to government figures, making it one of the few industries that was not impacted by the world's economic slowdown.

Online gamers in China grew 22 percent to 49 million last year.

The number is expected to grow to 94 million by 2013, with industry sales revenue hitting 39 billion yuan.

Tie Jun, an engineer from Kingsoft, one of China's largest security firms, said online games companies in the country had not shown great interest in the past in prohibiting the trade of game accounts and virtual items in the underground market.

But with joint efforts from online gaming and security firms recently, the growth of Trojan horse attacks is seeing signs of slowing down, he said.

Courtesy : Wang Xing (China Daily); www.chinadaily.com.cn
27-Nov-2009

EDUCATION

11 Security Tips for Secure Online Shopping

Specially for Black Friday, Cyber Monday

If your business is physical security, Friday is more than likely going to be a rough day. Shoppers will storm your stores the day after Thanksgiving in what has become known as Black Friday and spend, spend, spend. That's what the retailer wants, of course. But for the security pro, it means a much bigger risk of shoplifting on the part of customers and employees alike.

For IT security practitioners, the day to watch is so-called Cyber Monday, when the masses turn on their office computers and, instead of working, storm the online marketplace for holiday gifts. Here, the worry is that hackers are lying in wait, ready to break into retail networks and steal customer credit card numbers.

To help ensure a more effective defense, CSOonline reached out to physical and IT security experts and gathered up the following 11 tips.

Tips 1-5 courtesy of David Bonvillain, vice president of Accuvant Labs

Tip 1: Make sure the security software is on. Ensure all systems that access the Internet are protected with anti-malware technology, specifically making sure browser security enhancements are configured and enabled in AV software, Bonvillain says. Much has been said about the sorry state of AV this year - for one example, read Experts Only: Time to Ditch the Antivirus?. But the chances of avoiding a security breach will still increase if the anti-malware is turned on.

Tip 2: Save users from themselves (otherwise known as awareness training). Forget that employees are shopping on company time, probably a career-limiting activity in some places. The bigger problem is that they're doing it on company machines online thieves are just itching to hijack. Since employees are going to do this anyway, Bonvillain says they should at least be educated on how to do it safely: "Awareness of common techniques and an understanding of how to identify malicious content can go a long way toward proactive prevention. Keep in mind that these types of attacks are also pervasive over IM and social networking technologies and are not simply limited to traditional Web browsing."

Tip 3: Monitor the networks. This may seem painfully obvious, but since warning signs tend to be missed and the breaches keep piling up,

Bonvillain says this one's worth repeating: "Comprehensive monitoring of both the network and the client will help you trend threats, identify weakness in your existing enterprise, and if necessary give you the tools to identify and contain a breach if one occurs."

Tip 4: Segment the networks. If you're a merchant bound by the requirements of the PCI security standard, you should be doing this anyway. The idea is to make it so the bad guys can't access the goods, even if they manage to break into another part of the network. Says Bonvillain: "By segmenting users from each other as well as network assets should a breach occur you limit your exposed footprint to potential malware, or even an attacker. Treat user computers as untrusted devices."

Tip 5: Stop the malware in the mobile machine. Cracking down on employees who shop online with company machines has become especially difficult because they are using mobile devices beyond the eyes of office managers and, often, beyond the eyes of IT, especially the laptops. To that end, Bonvillain says, "If employees are allowed to take corporate assets (laptops) home for personal use or access the corporate environment using mobile devices, ensure not only that secure VPN technologies are installed and utilized, but that some sort of endpoint security validation or quarantined access is in place."

Tip 6: Remove the cash. Here's some simple advice for physical security pros from the loss prevention manager of one of the largest department stores in the U.S.: The less cash you keep lying around, the smaller the payday for any potential robber. "Multiple cash pick-ups throughout the day to get the cash off the floor is a must," the manager said.

Tips 7-11 courtesy of MerchantWarehouse.

Tip 7: "Trust but verify". Ensure address verification system and card verification values match (i.e. 3 or 4 digit in signature panel)

Tip 8: Verify signature block. Sure, cashiers get overwhelmed when there's a long line of impatient people in front of them. But an important part of stopping credit card fraud is to check the signature block, particularly if the signature is worn out.

Tip 9: PIN the tail on the transaction. As a rule, PIN debit transactions are more secure (and typically cheaper) than signature-based transactions.

Tip 10: Bad things in store for those who store. Another basic requirement of PCI security is that companies store as little card holder

data after transactions as possible. The more that's stored, the more damage companies and customers can suffer at the hands of data thieves.

Tip 11: Encrypt it. Verify that your company has an encrypted card reader to ensure PCI compliance and, more importantly, to ensure the bad guys can't use what they steal.

Courtesy : Bill Brenner, CSO; www.cio.com
November 23, 2009

SURVEY

IT profession has most inactive workers

Less than one in five IT workers reach recommended government activity guidelines

A survey of 1,734 UK workers has found that of all nationwide professions, IT workers are the most inactive, as measured by government activity guidelines advocating half an hour of moderate exercise, five times a week.

Fewer than one in five (19 per cent) meet the government guidelines, and the IT workers also feature highly with respect to the unhealthiest diets.

The survey was conducted by personal training agency Fat Free Fitness -and found that 63 per cent of UK citizens fail to meet the activity guidelines, with the average person in the UK being active for just 90 minutes a week.

Only 14 per cent of IT workers claim to eat five pieces of fruit and vegetables throughout the day, whilst their caffeine intake is the highest nationwide - they drink the caffeine equivalent of 10 cups of coffee a day, two more than the recommended daily allowance (RDA) of eight cups per day (with an estimated caffeine intake of 800mg).

Receptionists, salespeople and checkout operators are just behind IT workers with regard to the activity guidelines, while bricklayers and construction workers topped the survey.

Fat Free Fitness founder Rich Leigh, said there was clearly a correlation between sitting at a desk or wheel all day and how active you're likely to be.

Leigh pointed out that the government had spent millions last year on obesity and healthy eating campaigns, "but aren't talking the language of the times. People are leaving gyms and becoming less active and it's because on the whole, people can't afford them. Some gyms and health clubs offer larger organisations company membership discounts, but where do the small businesses fit into this?" asked Leigh.

"It's not that wer're looking for a workforce of 2012 Olympic hopefuls, but we want to ensure that the provisions and opportunities are there

for them to both participate in activity and learn about healthy eating," said Leigh.

Courtesy : Dave Bailey; www.computing.co.uk
17 Nov 2009

ANALYSIS

The six greatest threats to cybersecurity

Cybersecurity threats from government insiders, foreign countries, terrorists all pose grave threats, GAO reports.

It's not a very good day when a security report concludes: Disruptive cyber activities expected to become the norm in future political and military conflicts. But such was the case today as the Government Accountability Office today took yet another critical look at the US federal security systems and found most of them lacking.

From the GAO: "The growing connectivity between information systems, the Internet, and other infrastructures creates opportunities for attackers to disrupt telecommunications, electrical power, and other critical services. As government, private sector, and personal activities continue to move to networked operations, as digital systems add ever more capabilities, as wireless systems become more ubiquitous, and as the design, manufacture, and service of information technology have moved overseas, the threat will continue to grow. "

Within today's report, the GAO broadly outline the groups and types of individuals considered to be what it called key sources of cyber threats to our nation's information systems and cyber infrastructures. From the GAO:

Foreign nations: Foreign intelligence services use cyber tools as part of their information gathering and espionage activities. According to the Director of National Intelligence, a growing array of state and nonstate adversaries are increasingly targeting—for exploitation and potential disruption or destruction—information infrastructure, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries.

Criminal groups: There is an increased use of cyber intrusions by criminal groups that attack systems for monetary gain.

Hackers: Hackers sometimes crack into networks for the thrill of the challenge or for bragging rights in the hacker community. While remote cracking once required a fair amount of skill or computer knowledge, hackers can now download attack scripts and protocols from the Internet and launch them against victim sites. Thus, attack tools have become more sophisticated and easier to use.

Hacktivists: Hacktivism refers to politically motivated attacks on publicly accessible Web pages or e-mail servers. These groups and individuals overload e-mail servers and hack into Web sites to send a political message.

Disgruntled insiders:The disgruntled insider, working from within an organization, is a principal source of computer crimes. Insiders may not need a great deal of knowledge about computer intrusions because their knowledge of a victim system often allows them to gain unrestricted access to cause damage to the system or to steal system data. The insider threat also includes contractor personnel.

Terrorists: Terrorists seek to destroy, incapacitate, or exploit critical infrastructures to threaten national security, cause mass casualties, weaken the U.S. economy, and damage public morale and confidence. However, traditional terrorist adversaries of the United States have been less developed in their computer network capabilities than other adversaries. The Central Intelligence Agency believes terrorists will stay focused on traditional attack methods, but it anticipates growing cyber threats as a more technically competent generation enters the ranks.

Testifying before the Senate Judiciary Committee, Subcommittee on Terrorism and Homeland Security today, FBI Deputy Assistant Director, Cyber Division said that while the FBI has not yet seen a high level of end-to-end cyber sophistication within terrorist organizations, it is aware of and investigating individuals who are affiliated with or sympathetic to al Qaeda who have recognized and discussed the vulnerabilities of the U.S. infrastructure to cyber attack; who have demonstrated an interest in elevating their computer hacking skills; and who are seeking more sophisticated capabilities from outside of their close-knit circles.

"In addition, it is always worth remaining mindful that terrorists do not require long term, persistent network access to accomplish some or all of their goals. Rather, a compelling act of terror in cyberspace could take advantage of a limited window of opportunity to access and then destroy portions of our networked infrastructure. The likelihood that such an opportunity will present itself to terrorists is increased by the fact that we, as a nation, continue to deploy new technologies without having in place sufficient hardware or software assurance schemes, or sufficient security processes that extend through the entire lifecycle of our networks," Chabinsky said.

Courtesy : Michael Cooney; Network World
Nov. 17, 2009

SURVEY

Top 5 Mega Trends that Increase Risks

If It's New, It's Harder to Secure

The main takeaway from a survey released last week by a privacy and data protection think tank is that the newer a mega trend, the harder it would be to secure data and systems connected with it.

The top five mega trends that increase security risks within government agencies, as identified by 217 senior federal IT pros surveyed by the think tank, Ponemon Institute:

1. **Unstructured data (79 percent of responses).**
2. **Cyber terrorism (71 percent)**
3. **Mobility (63 percent)**
4. **Web 2.0 (52 percent)**
5. **Virtualization (44 percent)**

Some of these mega trends have been around for years, such as unstructured data and mobility, but the soaring deployment of multimedia applications and the unstructured data needed to support them, as well as the rocketing use of mobile devices, create constantly evolving environments that information security professionals must protect.

As for cyber terrorism, the growing number of reports of infiltrations into government systems raises apprehension levels among government cybersecurity professionals that real damage could be a mouse click away, as the survey numbers reflect.

Virtualization is a big money saver, and the ability to use software to treat one machine as multiple servers has become popular in government and the private sector. But its security implications are just coming into focus. Indeed, my fellow GovInfoSecurity.com blogger and forensics expert Eric Fiterman wrote on that topic last week.

The remaining mega trends that the Ponemon Institute reported, except for one, have been challenges that have been around for years: Data breach (40 percent), cyber crime (40 percent), cloud computing (39 percent), outsourcing (34 percent) and open source applications (18 percent).

For the most part, cloud computing hasn't been deployed by federal agencies, but federal CIO Vivek Kundra is championing the technology.

So, look for more government IT security pros to express reservations about securing data on the cloud as this new mega trend gains traction.

Courtesy : Eric Chabrow; blogs.govinfosecurity.com
November 23, 2009

SURVEY

Over three quarters of security products fail an initial test and do not adequately perform

A report by ICSA Labs has claimed that nearly 80 per cent of security products fail to perform as intended.

The 'ICSA Labs Product Assurance Report', which is co-authored by the Verizon Business data breach investigations report research team, revealed that the main reason for product failures is because it does not adequately perform as intended. It claimed that the products fail to perform as intended when first tested and generally require two or more cycles of testing before achieving certification.

Across seven product categories, core product functionality accounted for 78 per cent of initial test failures, such as an anti-virus product failing to prevent infection or an intrusion prevention system product failing to filter malicious traffic.

The failure of a product to completely and accurately log data was the second most common reason security products do not perform as intended. Incomplete or inaccurate logging of who did what and when accounted for 58 per cent of initial failures.

The third most significant reason for product failure was that 44 per cent of security products had inherent security problems, including vulnerabilities that compromise the confidentiality or integrity of the system and random behaviour that affects product availability.

The report stated: "Unfortunately, the market's solutions to all this newness are not always as legitimate as the need. Product quality is often left behind in the rush to be latest and greatest. New is distorted with innovative bigger touted as better, and promises frequently exceed performance. Thus, the work of helping to distinguish fact from fiction is critical."

It further claimed that 'no-one ever said creating quality products was easy'. It said: "Of course, that doesn't mean they can't be substantially improved either. So, how often do violations occur during ICSA Labs certification testing? In short: almost always. It is unlikely that anyone's worldview will be radically altered if we claim that years of product testing at ICSA Labs upholds the old adage that 'nothing is perfect'.

"It is extremely rare that a product attains certification in its first round of testing with no criteria violations. This was true in the early days of ICSA Labs and it is true today. With the exception of anti-virus, there is no substantive difference with regard to this finding across the testing programs. Some products exhibit major criteria violations, others relatively minor. Some have numerous deficiencies, others only a few.

"After the almost invariable first failure, most vendors attempt to make corrections and resubmit products for further testing. On average, 82 per cent of products deployed eventually achieve ICSA Labs certification. While it might be obvious, it is worth making a distinction here. 82 per cent does not refer to all products in existence; it refers only to those submitted to ICSA Labs for testing. For some programs this includes nearly all products in that market, but for others it represents the minority."

George Japak, managing director, ICSA Labs and a co-author of the report, said: "Our goal is to help vendors develop more secure products. When a product fails, we encourage vendors to view that as an opportunity to improve the product before it goes to market.

"In addition to benefiting the security industry, this open exchange of information can greatly benefit enterprises by providing them more reliable and available information to make educated product purchasing and use decisions."

Courtesy : Dan Raywood; www.scmagazineuk.com
November 17, 2009

OPINION

Seven deadly Internet security sins

"IT will never happen to me" — most of us are guilty of believing in this one time or another.

When it comes to computer security, we hold on to a similar belief. But the reality is one in five people will fall victim to cybercrime — that can be anything from your email account being hacked into and your identity being stolen to your bank account being cleaned out.

The frightening part of cybercrime is that we can't put a face to the criminals. We don't know just who or when we can be deceived or tricked.

To avoid a scary experience on the Internet, computer security company Symantec is advising people to avoid the Seven Deadly Sins of Internet Security to keep their PCs, cash and their personal identities safe. David Freer, vice-president of Symantec Consumer Business, Asia Pacific and Japan, says there are simple steps people can take to protect themselves, but often people don't follow this advice. "I know it's tempting when you're offered half-price designer goods or a link to a juicy news story — but to avoid damaging your PC and bank account, you have to remember the Seven Deadly Sins of Internet Security. These are sloth, gluttony, pride, lust, envy, greed and wrath." It is best, says Freer, to take a common sense approach to combating cybercrime.

"Be vigilant with online security. This involves keeping an up-to-date browser and operating system, and ensuring anti-virus and firewall software is up to date with the latest definition set."

1. Sloth: Feeling too lazy to install security updates or patch your machine because you can't be bothered? This leaves you wide open to infection and potential upset when your identity is stolen!

2. Gluttony: Gorging yourself on Internet gossip — among celebrity pictures, there may be a dirty malware worm hiding, which could leave a nasty taste in your mouth.

3. Pride: "I know better than my security software" — people who turn their software off, or ignore the warnings, and proceed to sites or to download stuff anyway may be in for a nasty shock when malware creeps in!

4. Lust: Just be careful what you click on. If pictures, videos or links to exciting content take your fancy, check that the site is safe or trusted before you go! Website rating services will give you guidance.

5. Envy: So you want a designer handbag or Jimmy Choo shoes but don't want to pay full price? Beware of the tricksters who will try and con you into buying fake goods and potentially hand over your credit card details to criminals.

6. Greed: Bargain sales? Two for the price of one? If it sounds too good to be true, it probably is.

7. Wrath: What might happen if you succumb to all of the above? You'll be full of wrath, as your PC could get infected and your cash stolen.

Courtesy : Chandra Devi Renganayar; www.nst.com.my
2009/11/13

This edition of the magazine is brought to you courtesy

Sysman Computers Private Limited

Sysman is

1. Pioneer in IT Security in India since 1991
2. Empanelled with CERT-In
3. Done over 2000 IT Security assignments
4. Provide Research Support
5. Create Public Awareness
6. Published 6 Books / 50 papers
7. An associate consultant to BSI to implement ISO 27001-ISMS

Contact –

Sysman Computers Private Limited, Mumbai

sysman@sysman.in

+91-99672-48000
+91-99672-47000

www.sysman.in