For the Year 2010

10 Major Security Threats

Organizations' Security Flaws Brought to the Surface

IPA® 独立行政法人 情報処理推進機構
セキュリティセンター

March 2010

Contents

10 Major Security Threats for the Year 2010

"Organizations' Security Flaws Brought to the Surface"

Introduction

In 2009, a variety of security accidents and incidents occurred, including Website defacement and virus infections caused by Gumblar. Gumblar cases highlighted the need of comprehensive security countermeasures not only for organizations/enterprises themselves but also for their subcontractors. Security countermeasures requiring the involvement of both contracting and contracted parties are not an entirely new concept. Organizations should renew their awareness of existing security measures needed and implement those measures. It is advisable for organizations to implement appropriate, cost-effective security measures by determining the "risks" posed by the existing "threats" and the business impacts brought about by such threats, rather than ad hoc security measures.

In this document, the term "threat" refers to any events that cause loss or damage to an organization; "risk" refers to a possibility of an organization suffering loss or damage or encountering dangers that are caused by "threat"; "business impact" refers to the impact of "risk" on an organization's business and/or service continuity.

Based on their Business Continuity Management (BCM) concept, organizations should analyze and assess the business impacts brought about by the existing threats, and then take appropriate security measures based on the analysis and assessment results. As for important information and information systems necessary to ensure business continuity, organization should implement multilayered security measures. Security countermeasure has two major aspects: "proactive measures" and "incident response". The former addresses preventing security incidents and accidents and ensuring business continuity; the latter addresses minimizing the damages caused by the incident (or accident) that has happened and making a quick recovery.

Chapter one looks at the business impacts on organizations that were caused by the actual security threats during the year 2009. Chapter Two outlines 10 major security threats for the year 2010 and their impacts and Chapter Three presents possible countermeasures against those threats.

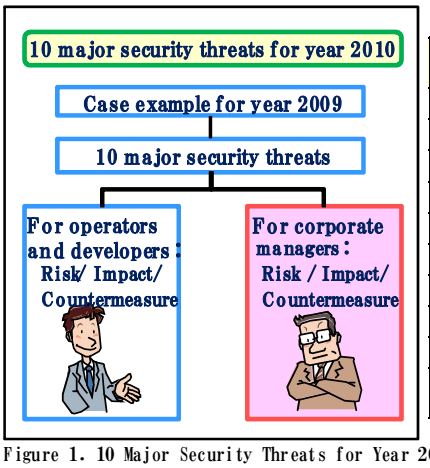


Figure 1. 10 Major Security Threats for Year 2010

List 1. 10 Major Security Threats for Year 2010

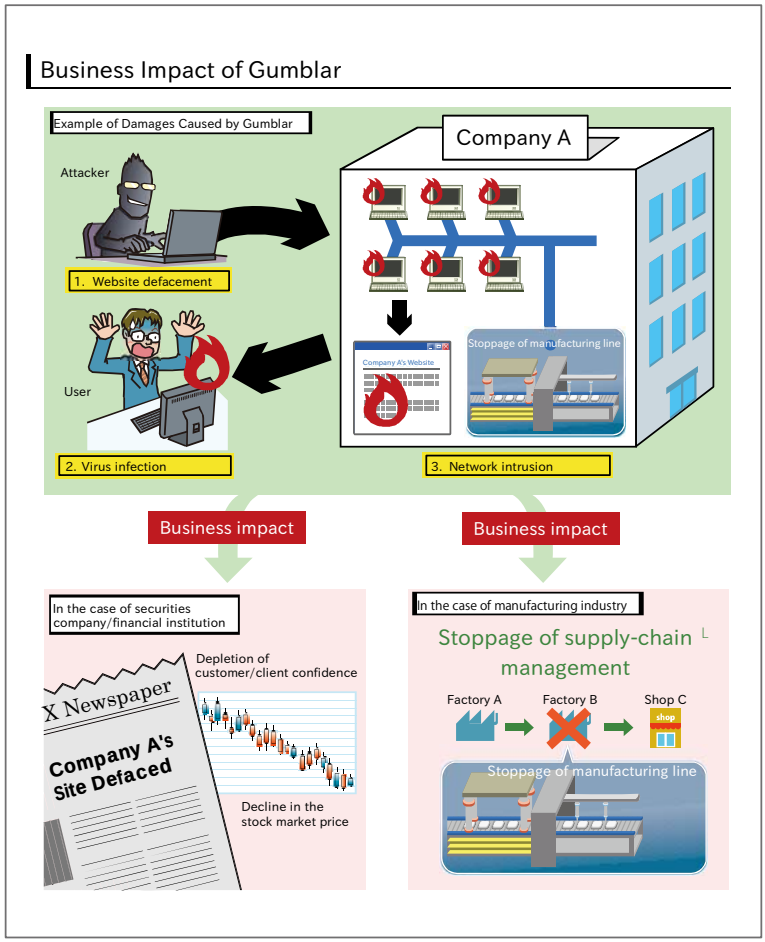
Rank order	10 Major Security Threats
1ST	EVER-CHANGING TACTICS FOR WEBSITE DEFACEMENT
2ND	CLIENT SOFTWARE NOT UPDATED
3RD	A VARIETY OF PURPOSES/OBJECTIVES OF COMPUTER VIRUS AND BOTS
4TH	VULNERABILITY IN UNSECURED SERVER PRODUCTS
5TH	INFORMATION LEAKAGE WITHOUT PROPER INCIDENT RESPONSE
6TH	TARGETED ATTACKS CARRIED OUT WITHOUT VICTIMS' NOTICING
7TH	DDOS ATTACKS THAT CAUSE SERIOUS DAMAGES
8TH	UNAUTHORIZED USE OF A LEGITIMATE ACCOUNT
9TH	SECURITY HOLES IN CLOUD COMPUTING
10TH	VULNERABILITY IN THE PROTOCOL SUPPORTING THE INTERNET INFRASTRUCTURE

Chapter One - Business Impacts Caused by the 2009's 10 Major Security Threats

In this chapter, we identify the risks posed by the existing threats on organizations, analyze and assess their business impacts, and consider organizational problems and countermeasures, based on the security incidents and accidents that happened in 2009. Security measures should be considered based on the BCM impact analysis. In this chapter, we took "financial institution" and "manufacturing industry" as an example and analyzed their business impacts.

The contents of this Chapter are based on the "Guidelines for the Formulation of a Business Continuity Plan " edited by the Ministry of Economy, Trade and Industry (METI).

1.1 A Spate of Incidents Occurring in Leading Companies by Gumblar



1.1.1 Threat and Risk of Gumblar

A virus infection tactic called "Gumblar" was widely covered by general newspapers and TV. "A best-known company/public institution's Website has been defaced and those who have visited that Website might have contracted a computer virus," the reports said. Among the victims to Gumblar-caused Website defacement were public transportation agency and major credit card companies.

Three major threats and associated risks of Gumblar are as follows:

1) Your organization's Website defaced

Your organization's Website is defaced to distribute a computer virus and as a result, your organization becomes a victimizer to the site visitors. In such cases, your organization will be regarded as the one not taking adequate security measures.

2) The site users' information stolen

If a user contracted a computer virus by visiting the defaced Website, his personally identifiable information might be stolen. In such cases, your organization would lose the trust of its clients.

3) Your organizations network attacked

The attacker might carry out an attack against

your organization's network due to which your organization's important information might be stolen or networks and/or important systems might become unavailable. As of March 2010, there had been no report on damages caused by this risk, but such incident could happen.

1.1.2 Business Impacts

In the case of securities companies and financial institutions

In the case of securities companies and financial institutions, the following business impacts can be considered for the threats and risks described in 1) and 2) in Section 1.1.1.

If a user buying or selling a company's stocks on a defaced Website suffered loss from false information, the company's credibility would be undermined.

Then the site user's personally identifiable information or money-related information might be stolen, resulting in compensation for damages and/or erosion of trust.

If a serious damage was caused to the user's property, the company would lose the trust of not only the victim but also the rest of its clients. If the fact gets a media coverage, the company would also lose the trust of its stakeholders, resulting in declined sales and stock prices.

If the company is relying heavily on sales on its Website, it might become difficult for them to continue their business.

In the case of Manufacturing Industry

In the case of a company producing precision instruments, the following business impacts can be considered for the threats and risks described in 3) in Section 1.1.1.

Such companies use computers in their production lines. Computers are also used for duration test and/or experimentations of their products and to store design documents for product development. The computer used for these purposes is generally not directly connected to the Internet. However, a virus downloaded by Gumblar might penetrate into such computer through the company's internal network or via external storage media and carry out an attack to steal the company's important information or to cause a computer service to stop.

If the production line was attacked and came to a stop, the shipment of products would be suspended and the supply chain would also be affected. It might also result in damages to affiliated companies and the company might have to pay for the damages.

If design documents were stolen, they might be used by its rival companies to produce a less-expensive product with the same quality. In such cases, the company would lose in the price competition.

1.1.3 Proactive Measures and Incident Response

Security measures should be implemented from the aspect of business continuity. Organizations, for example, may want to incorporate the following proactive measures and incident response.

Proactive measures include clarifying information and information systems particularly important to the organization; and establishing a framework and rules for protecting such information and information systems. The biggest problem concerning Gumblar was that IDs and passwords were stolen not only from organizations/enterprises themselves but also from their contracted Website operator. For this reason, organizations/enterprises should also consider security measures that should be enforced to their contractors and other organizations concerned.

For important information and information systems, organizations should restrict access to authorized users. This may include physical defense (e.g., prohibiting an unauthorized person from entering a room where important systems are in operation, prohibiting authorized personnel from bringing in any external media into such rooms, etc.) and system defense (e.g., not allowing authorized personnel to access important information and information systems across a network.)

Proactive measures to prevent damages caused by Gumblar should include: the enforcement of a rule in which those involved in important information and information systems are required to regularly perform update for client software and antivirus software's pattern files on their PCs. This rule should be applied to both contracting and contracted parties and other organizations con-

cerned.

Organization should also consider incident response by referring to documents such as the "Guidelines for the Formulation of a Business Continuity Plan." Incident response, for example, may begin by "activation of BCP ", followed by "investigation of the cause", "risk communication including corresponding with clients" and "implementation of the measures for preventing the recurrence of such incidents."

When the BCP is initiated, the person in charge should manage BCP related information thoroughly so that the information flow will be centralized and well-organized.

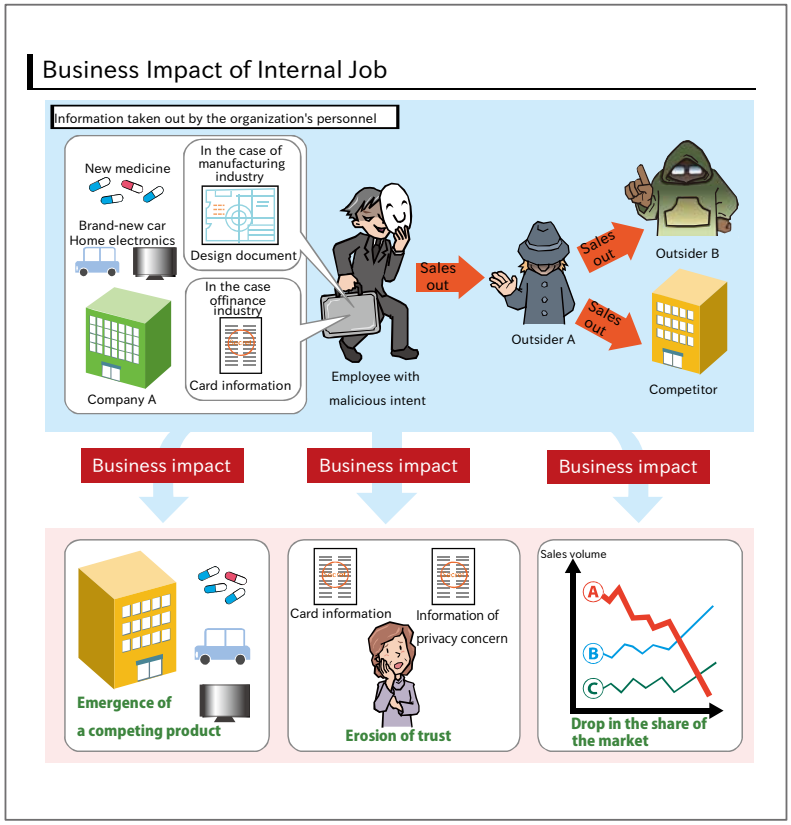
"Investigation of the cause" includes identifying the compromised items and their quantities. Organizations may consider using external specialists for this purpose.

"Risk communication" provides necessary information in a timely manner that is required by people concerned, including clients, potential clients, stockholders, relevant ministries. Provision of such information is achieved through the publication of the fact, press conference/press release, creation of a contact point, etc.

Risk communication is an important aspect of business continuity. If the organization did not release information needed by parties concerned in an appropriate manner, it might lose the trust of those parties, which might cause a major impact on its business continuity. Risk communication should include the release of "measures for preventing the recurrence of such incident." Continuous information disclosure makes the progress of the organization's security clear to the people concerned and ensures that the organization regains its credibility.

Minimizing the damages caused and responding sincerely to the incident might contribute to expanding the organization's business opportunity.

1.2 Theft of Information as An Internal Crime



1.2.1Threat and Risk of Internal Crime

In September 2009, there was a news report on an "internal crime" in which information was stolen in a leading company, resulting in the estimated loss of about 7 billion. According to the report, an employee sneaked client information out of the company and sold it to an external party, and the estimated amount indicates the possible losses

suffered by the company.

The criminal was arrested and convicted of stealing the company's CD, using the other person's ID, which is a violation of the act concerning the prohibition of unauthorized computer access.

In the case of internal crime, the probability of important information being stolen is higher than that of an attack from outside. In the above-mentioned case, because the criminal had authorization to access important information (or confidential information), it could easily be stolen. In the case of internal crime, stolen information is highly likely to be abused as it is stolen intentionally.

If the organization's client information (or confidential information) was stolen and abused, the organization might suffer from fallen credibility and deteriorating competitiveness. If this risk became a reality, the organization might suffer direct financial losses or have to spend much time in responding to the incident, the impact of which is considered a cost-related business impact.

1.2.2 Business Impact

In the Case of Manufacturing Industry (Automobile and medicinal product)

A possible business impact of internal crime is: drawing of a commodity or information on a medical product's ingredients might be stolen by an employee, and sold to, and used by, other organizations.

For example, the stolen information could be used by a rival company to produce a low-cost product with the same quality, leaving your company behind in the price competition. As a result, your company's product might get thrown off the market and its business continuity might be seriously affected.

If the stolen information was the one concerning a collaborative development project by multiple companies or the one concerning an entrusted development project, affiliate companies and costumers would also suffer the damages. As a result, the organization might have to compensate for the damages incurred by the stolen information and lose the trust of its affiliate companies and clients. In such cases, its business continuity would be seriously affected.

1.2.3. Proactive Measures and Incident Response

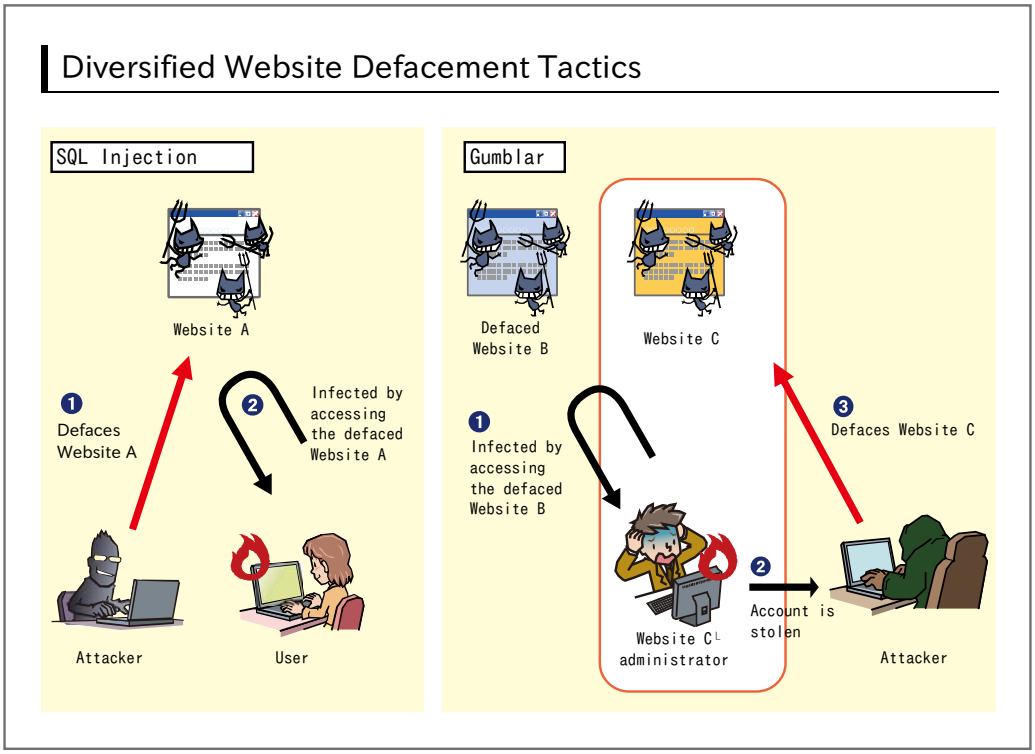
Among the internal crimes covered by general newspapers and other media are: false accounting and the forgery of a private document (official document). Corporate managers take countermeasures against the theft of information as well as these issues. This section describes countermeasures against the theft of information by an internal criminal.

Organizations should establish comprehensive security measures by referring to IPA's "Information Security Textbook – Handbook for CISO and Information Security Professionals". Such measures include access control. For important information, organizations should implement access controls covering both physical and system aspects. As a physical access control, organizations can use biometric authentication for those entering or leaving a room where the information systems containing important information are located. As a system access control, organizations can permit or deny the access from personnel's PCs to such systems by checking their access right. It is also effective to enforce a rule in which double-check should be performed for those accessing important information to perform certain tasks. This access control reminds employees that their operations are being monitored and thus prevents them from sneaking information out of their company.

Incident response is also of importance. Organizations should minimize the impact on their business continuity. Organizations should take the same response as the one described in Section 1.1.3. In the case of internal crime where important information might be stolen, it is of great importance to establish and maintain risk communication with people concerned, including clients, affiliate companies, police, and relevant ministries. Continuous information disclosure makes the progress of the organization's security clear to the people concerned and ensures that the organization regains its credibility. By taking these approaches, organizations should minimize the impact on their business continuity.

Chapter Two 10 Major Security Threats

【1st】Ever-Changing Tactics for Website Defacement



There are cases where users get a computer virus only by visiting a Website. A new attack method that brings such threat emerged – that is, "Gumblar" described in Section 1.1, Chapter One.

Threat

Many of the Website-mediated attacks carried out in recent years involved the defacement of a Website with a certain level of credibility, for which the site operator becomes a victimizer. Prior to the emergence of Gumblar, a similar threat had been brought by SQL injection attacks. If a Website vulnerable to SQL injection attack received such attack, information contained in the database might be falsified, the Website might be defaced to guide users to a virus-distributing site, and the virus might be downloaded to the users' PCs. As in the past, SQL injection attacks were detected in 2009, so we need to remain alert.

In the case of Gumblar which was one of the prevalent attacks carried out in 2009, the way to deface a Website is different from that of SQL injection attacks. While SQL injection is designed to attack databases, Gumblar has nothing to do with database. In most cases, Gumblar steals and alters authentication information of File Transfer Protocol (FTP) accounts used for updating Websites. Because Website update is performed by using FTP accounts in many Websites, a number of Websites have reportedly been hit by Gumblar. The flow of Gumblar-caused incidents is as follows:

1. A person in charge of updating Website A accesses Website B which has been exploited and defaced by Gumblar.
2. Website B guides the updater to Website C which is designed to distribute a computer virus.
3. The virus is downloaded to, and executed on, the updater's PC upon accessing Website C.
4. The virus compromises the FTP account which is used for updating Website A and sends it to the attacker.
5. Using the stolen account, the attacker de-

faces Website A.

As in the case above, if a person in charge of updating Website D attempts to access Website A, Website D will be also defaced. In this way, Gumblar is designed to cause damages in a chain reaction.

Case Examples and Statistics for the Year 2009

This Section outlines case examples and statistics for SQL injection attacks and Gumblar.

According to a domestic security vendor's report, a number of SQL injection attacks were observed in Japan from the end of 2008 to the beginning of 2009, but later on, the number of observed SQL injection attacks decreased to the 2007 level.

By February 2010, several tens of Gumblar-related cases had been reported by enterprises and other organizations. According to the reports of various security vendors, however, several thousands of such incidents have occurred in Japan and several tens of thousands throughout the world.

Impact

A leading company's Website has also been defaced by Gumblar and such incidents grabbed newspapers' headlines. Organizations running Websites are required to take appropriate countermeasures.

There have also been cases where a Website operator's FTP account was compromised. Therefore, when outsourcing Website operation to a contractor, organizations should also consider security measures that should be enforced to the contractor.

In 2009, a number of Websites were defaced. Organizations should review their security measures so that their Websites and the site users do not suffer damages caused by Gumblar.

Chapter Three: Countermeasure

"3.1 Establishing framework and rules (P28)", "3.2 Planning and designing secure operation approach (P29)", "3.3 Concluding a contract for secure operation (P29)"

"3.8 Examining the established framework/rules/systems (P31)", "3.9 Reviewing and modifying (if necessary) the established framework/rules/systems (P31)"

SQL Injection:

"3.4 Implementing countermeasure for server systems (P30)", "3.7 Performing secure programming (P31)"

Gumblar:

"3.5 Implementing countermeasure for client systems (P30)", "3.6 Managing account information (P30)"

<References> (All in Japanese)

IPA:

http://www.ipa.go.jp/security/txt/2010/02outline.html#5

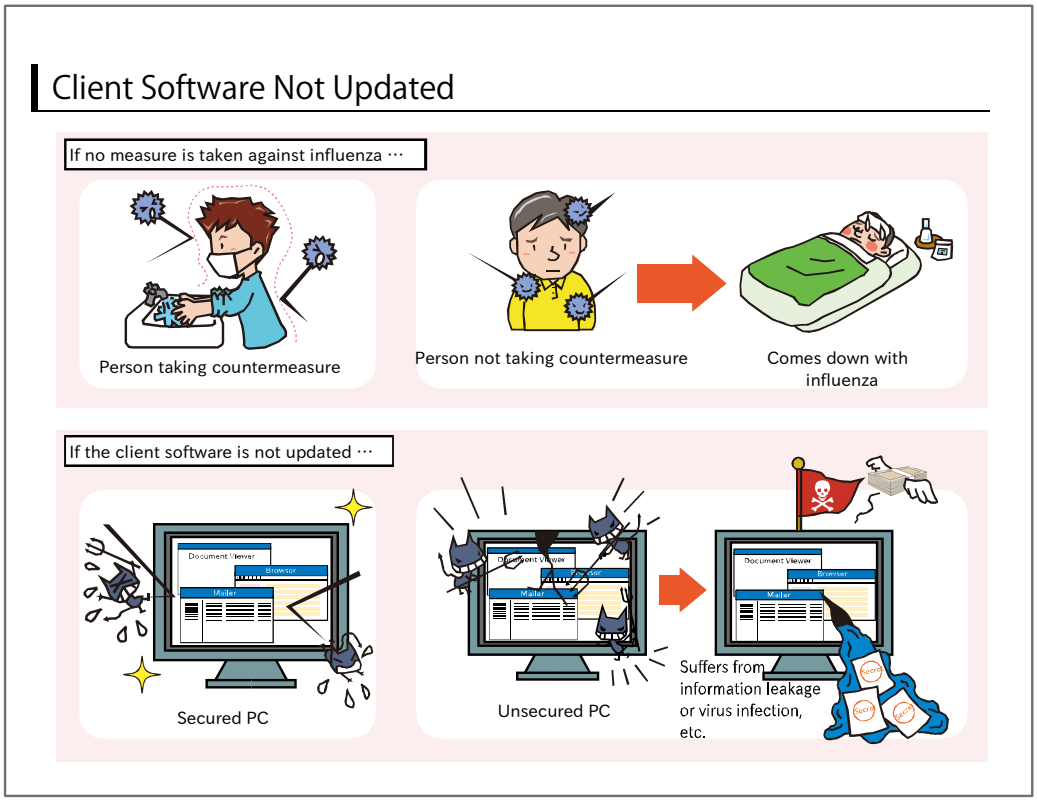
So-net:

http://www.so-net.ne.jp/security/news/newstopics_201001.html

LAC:

http://www.lac.co.jp/info/alert/alert20090609.html

【2nd】Client Software Not Updated



As in the past, software vulnerability was exploited by attackers in 2009. However, most of those vulnerabilities had been fixed by the software developers, so if the users had applied updates, damages would have been reduced.

Threat

Various software programs are running on a computer, including operating systems, accompanying software, software products purchased and installed, and free software. There are cases where vulnerability is detected in those software programs.

If known to attackers, software vulnerability could be exploited. To prevent this, software users should use updated versions where vulnerability has been fixed.

In the case of Gumblar described in Section 1.1, Chapter One, vulnerability in software running on a client PC is exploited. For most of those vulnerabilities, fixed versions had been released by software developers, so it is an effective measure to apply software updates.

Some of the recent operating systems and software provide an automatic update feature. Most of operating systems and accompanying software programs provide a dedicated batch update function. Other software products having an update feature display a notification message indicating that updates are available. In most cases, widely prevalent software products provide this update feature.

However, client PC users have a tendency to continue to use older versions of software products without applying updates.

Because vulnerability in client PCs is exploited by attackers nowadays, software update has become a pressing issue.

Case Examples and Statistics for the Year 2009

Through the "The Year 2009 Awareness Survey on Information Security Threats", IPA checked out the reasons why people do not apply updates (security patches).

According to the survey results, as the reason for not applying security patches, "Don't know how to apply security patches" marked the highest

point, accounting for 42.5 percent. It is assumed that automatic update feature provided by operation systems and software vendors is not understood by users.

Another reason ranked high was: "requires time and effort." It should be a matter of balance with having to stop their work temporary for updates. Among other reasons were: "Don't know what the benefit in applying updates is" and "Don't feel the need to apply security patches." These answers show that the need to apply updates is not understood by software users.

According to a survey conducted by an overseas enterprise around August 2009, among 2,500,000 people surveyed, 79.5 percent were using a vulnerable version of Adobe Flash while 83.5 percent were using a vulnerable version of Acrobat/ Adobe Reader.

For this reason, a virus exploiting Adobe products vulnerability is on the increase. Because Adobe products are being used by many people, vulnerability in such products is thought to be targeted by attackers to transmit a computer virus.

Impacts

Because many client PCs are not updated, attacks focusing on client PCs are expected to remain prevalent. This also indicates that attacks like Gumblar might be carried out anytime in the future. In the case of client PCs, they may be allowed to access important system via the network within the company. In such cases, possible damages include: other PCs within the company being infected with the virus, important systems receiving DDoS attack (see "7th DDoS Attacks That Cause Serious Damages"), important information being stolen. Therefore, organizations should ensure that users apply updates. Organizations should take appropriate countermeasures by referring to Section 3.5 "Implementing countermeasure for client systems", Chapter Three.

Chapter Three: Countermeasure

"3.1 Establishing framework and rules (P28)", "3.2 Planning and designing secure operation approach (P29)", "3.3 Concluding a contract for secure operation (P29)"

"3.5 Implementing countermeasure for client systems (P30)"

"3.8 Examining the established framework/rules/systems (P31)", "3.9 Reviewing and modifying (if necessary) the established framework/rules/systems (P31)"

<References> (All in Japanese)

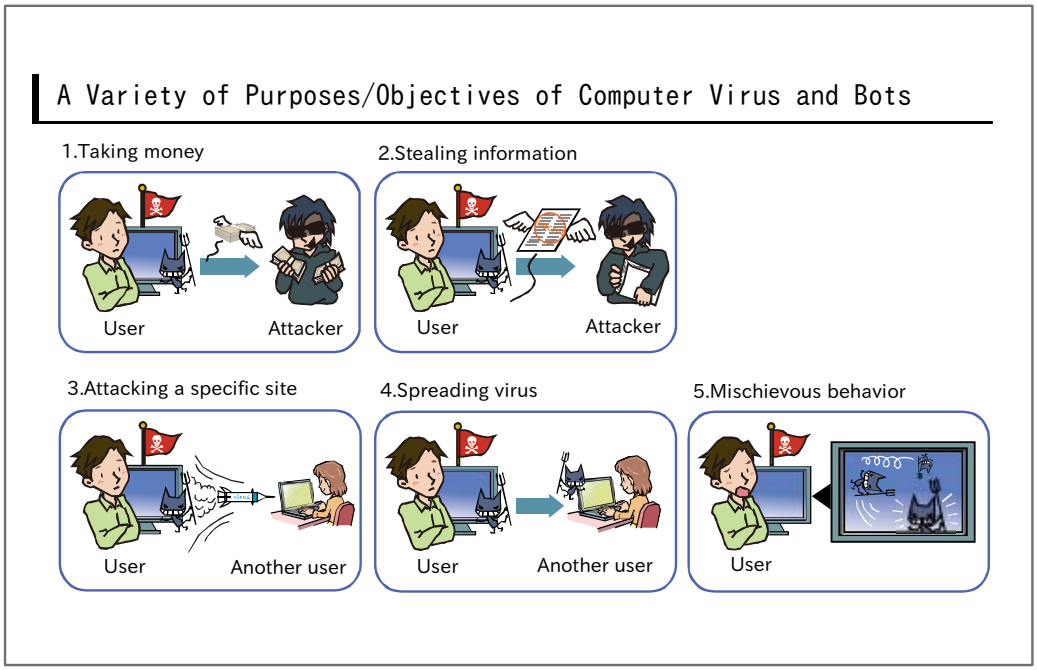
IPA:

http://www.ipa.go.jp/security/fy21/reports/ishiki/index.html

ZDNet Japan:

http://japan.zdnet.com/sp/feature/07zeroday/story/0,3800083088,20399036,00.htm

【3rd】A Variety of Purposes/Objectives of Computer Virus and Bots



Virus and Bots (hereinafter collectively-referred as virus) are an immediate threat to computer users. Virus has a variety of purposes/objectives. In 2009, we saw an explosive increase in the number of its subspaces.

Threat

Nature of the recent virus is: "PCs are infected without their users noticing."PCs are purposely infected for attackers to abuse After transmitting a virus to the target user's PC, the attacker uses that PC for a variety of purposes/objectives. Assumable primary purposes/objectives of attackers are as follows:

1) Stealing money

The first purpose/objective of attackers should be: stealing money from computer users. A typical example is "false antivirus software". False antivirus software is designed to trick users into purchasing a useless software product or to steal important information (e.g., credit card information) from users by displaying a message "Your PC has been infected with a virus! To clean the virus, you need to purchase the following antivirus software." By prompting fears among users, attackers take money away from them.

2) Stealing information

The second purpose/objective of attackers should be: stealing information stored in the user's PC. Once infected with a virus, important information (e.g., online banking information or account information) might be stolen. Using the stolen information (e.g., personal information registered in an online bank or account information), the attacker carries out unauthorized computer access or other malicious activities.

3) Attacking a specific target

Apart from stealing money and information from users (which makes the attacker richer), the purpose/objective might involve attacking a specific target. Attackers might carry out DDoS attack or SQL injection attack in which an order is given simultaneously to virus-infected PCs to cause a specific target to stop providing services. Attackers might also operate a rental service in which virus-infected PCs they can control and (ab)use to launch an attack are rented to a malicious entity.

4) Spread of Virus

From the nature of the viruses shown in the

past, it is assumed that attackers' intent was to transmit those viruses to as many PCs as possible. Virus creators think it's not enough to infect only one PC to carry out an attack for stealing money/information or for making services unavailable from a specific target. If the PC was secured enough, the purpose/objective of the attacker would not be achieved. For this reason, attackers attempt to transmit the virus to as many PCs as possible.

5) Nuisance

The purpose/objective of the attacker might be: annoying PC users or causing fears among people by transmitting the virus to their PCs. For example, there is a virus which turns the color of the screen into black, for which the user is scared. More malicious virus might render a PC unusable or disclose information stored in the PC to the Internet.

To achieve such purposes/objectives of attackers, viruses attempt to enter users' PCs through a variety of routes.

Case Examples and Statistics for the Year 2009

According to an antivirus software vendor's report, the number of virus type is increasing explosively. The report says that about 133,000 viruses were detected in 2007. The number has increased to about 1,600,000 in 2009. The figure is more than tenfold compared to the 2007 level. (About 900,000 in 2008)

A factor behind the increasing number of virus is the emergence of tools with which a virus can easily be created. These tools are supposedly designed to create a virus that cannot be detected by existing antivirus software products.

Impact

Once a PC within the organization has been infected with a virus, the virus might spread throughout the organization, causing the systems to stop. In fact, there was a case where one PC was infected with a virus first and then the virus was transmitted to more than 1,000 PCs, which affected the organization's business and operations. If the virus-infection was spread within an organization which is a part of critical infrastructure such as electricity/water, the impact would be much greater.

Chapter Three: Countermeasure

"3.1 Establishing framework and rules (P28)", "3.2 Planning and designing secure operation approach (P29)", "3.3 Concluding a contract for secure operation (P29)"

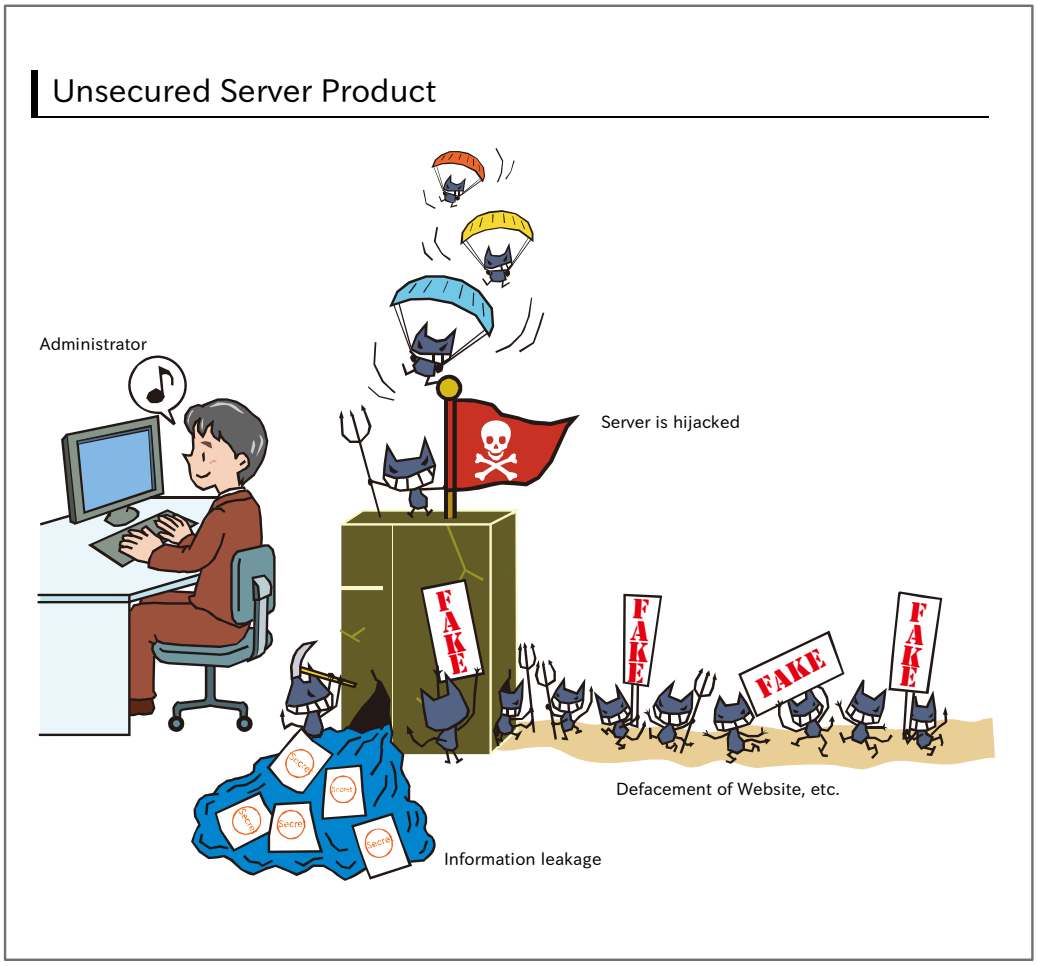
"3.5 Implementing countermeasure for client systems (P30)"

"3.8 Examining the established framework/rules/systems (P31)", "3.9 Reviewing and modifying (if necessary) the established framework/rules/systems (P31)"

<References> (All in Japanese)

G DATA Software:
http://gdata.co.jp/press/archives/2010/02/1160.htm
IPA:
http://www.ipa.go.jp/security/txt/2010/01outline.html

【4th】Vulnerability in Unsecured Server Products



It has been revealed that for some Websites, no measures are taken to overcome vulnerability of server products (Web applications, middleware, etc.) running on them.

Threat

If vulnerability exists in server products such as Web server and Web application, it might be exploited by an attacker. As shown in the past, the spread of virus (Worm) around 2003 was caused by attackers exploiting vulnerability of server products. In 2009, Website defacement by SQL injection was frequently reported. Server products are required to take appropriate measures to overcome vulnerability (hereinafter called vulnerability countermeasure).

In particular, where the server product is used for Website releasing information to the public, special attentions should be paid.

A Website consists of a Web server, a Web application that provides dynamic contents (i.e., making up a Web page based on the user or input value), and middleware (e.g., Perl, PHP). Organizations operating a Website should take into account vulnerability for all those software programs.

Vulnerability countermeasures on the side of server products are of importance, but even in the case where developers release updates to overcome vulnerability, some of server products are not updated by their users. Possible major reasons for not updating server products are as follows:

1) Not applying updates from the fear of a specific service becoming unavailable
2) Not understanding the need to apply updates on server products

If the Website operator understands the risk of not taking vulnerability countermeasures and takes alternative measures to protract their Web-

sites, that would be fine. Possible alternative measures include: "using Intrusion Prevention System (IPS) to protect against an attack exploiting vulnerability." Implementing such measures should reduce the possibility of risks being brought to the surface. It is important for server product administrators to understand the above-mentioned issue and to fix vulnerability or take alternative measures to protect their server products.

Case Examples and Statistics for the Year 2009

For a Website operator using two or more products on which a number of reports were filed to IPA in 2009, IPA issued "Security Alert for a Website Using an Older Version of Sever Product." The alert says that most of server products are not secured enough with appropriate vulnerability countermeasures. By the time IPA issued "Security Alert for Known Vulnerability of DNS servers used in Websites", it had received 1,307 reports concerning Websites where countermeasures against DNS Cash Poisoning had not been taken.

On the other hand, by the time IPA issued "Security Alert for a Website Using an Older Version of EC-CUBE", it had received 49 reports concerning Websites where known vulnerability of "EC-CUBE" had not been fixed. The reports on "EC-CUBE" were related to vulnerability to Cross Site Scripting in the product concerned. The product is also known to have vulnerability to SQL injection so early implementation of appropriate vulnerability countermeasures is required.

The fact has been highlighted that there are server products whose vulnerability has not been fixed.

Impact

If vulnerability in a server product was exploited, unspecified number of users might suffer damages. For example, information stored in the sever product might be altered. As a result, information on the users of the server product might be stolen or their PCs might be infected with a virus.

If vulnerability in a server product was exploited, not only the product itself but also its users might suffer damages. As you can see from the damages caused by Gumblar in the past, these things could happen.

Server product administrators should be fully aware that the damages might be extended to users and should take appropriate vulnerability countermeasures.

Chapter Three: Countermeasure

"3.1 Establishing framework and rules (P28)", "3.2 Planning and designing secure operation approach (P29)", "3.3 Concluding a contract for secure operation (P29)"

"3.4 Implementing countermeasure for server systems (P30)"

"3.8 Examining the established framework/rules/systems (P31)", "3.9 Reviewing and modifying (if necessary) the established framework/rules/systems (P31)"

<References> (All in Japanese)

IPA:

http://www.ipa.go.jp/security/vuln/documents/2009/200907_ec-cube.html

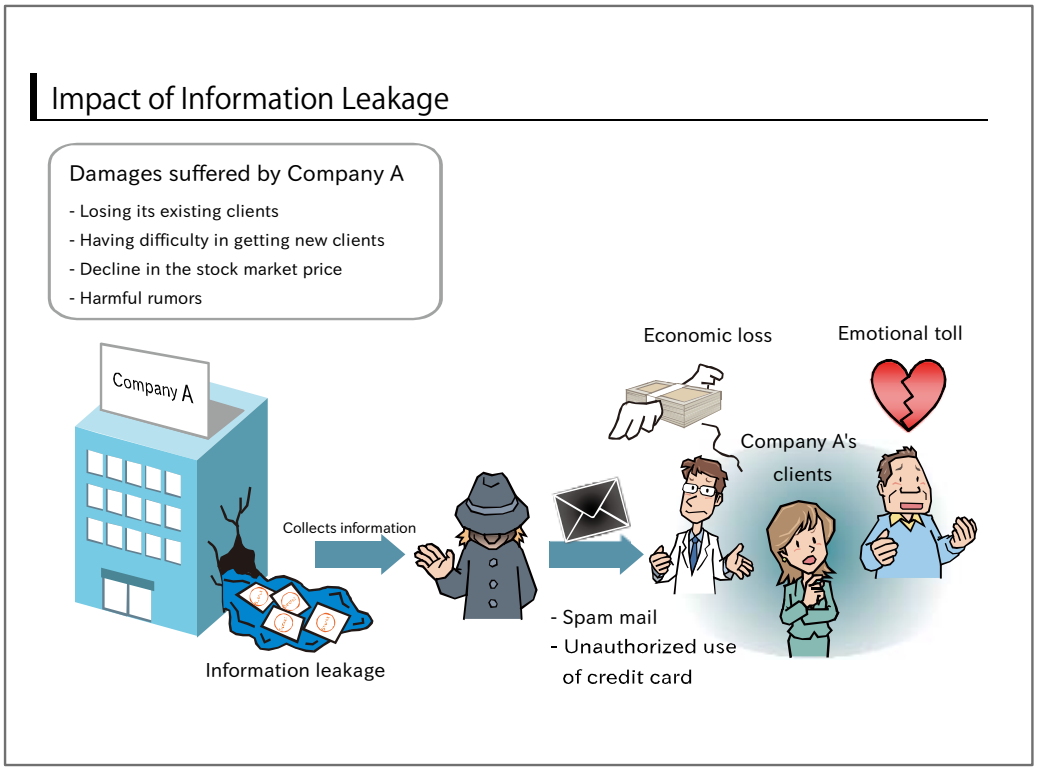
IPA:

http://www.ipa.go.jp/security/vuln/documents/2009/200909_openssl.html

ITMedia:

http://www.itmedia.co.jp/enterprise/articles/0909/08/news027.html

【5th】Information Leakage without Proper Incident Response



There are various causes for information leakage and the damage varies depending on the type of information leaked.

Threat

Causes of information leakage include: SQL injection attack, virus infection, internal crime described in Section 1.2, Chapter One, human error/negligence (e.g., e-mail transmission error, loss of storage media, etc.) Human fault/negligence is the most common cause of information leakage. In the case of information leakage caused by human fault/negligence, even if the organization enforces a rule to prevent e-mail transmission error or loss of storage media (e.g., checking the destination address before sending an e-mail (technical security control), prohibiting personnel from taking storage media out of the organization's premises (operational security control)), information leakage might be caused by the violation of that rule. So we cannot rely only on technical and operational security controls.

For this reason, organizations should take secondary preventive measures (e.g., enforcing a rule in which those sending important information by e-mail should gain approval (about destination and content) from their boss, limiting the storage media that can be taken out to those having encryption feature and requiring personnel to encrypt the data/information on such media, etc.)

The above-mentioned information leakage incidents are also attributed to the lowering of information security awareness of the organization's employees and therefore, organizations should regularly give their employees information security education and training to raise their security awareness.

Case Examples and Statistics for the Year 2009

As in 2009, there are still a number of cases involving internal crime. According to a survey conducted by an ISP, the number of information leakage incidents reported from June 2008 through May 2009 was 1,583. 291 cases, or 18.3%, of those incidents were caused by the loss or theft of notebook or external storage media such as USB memory sticks.

The report says, even if the organization enforces a rule in which personnel are prohibited from taking information out of the organization's

premises, there are occasions where they have to take out information for meeting a deadline, etc.

As the survey result shows, if the established rule is not in the context of the actual situation, it ends up in an only-by-name rule. Therefore, organizations should, in advance, determine the applicability of the established rule in the context of their business.

Other cases involved a contractor taking personal information out of the organization's premises. To protect against such incidents, organizations should implement comprehensive security countermeasures designed for not only themselves but also for their subcontractors. In the case where everything (from building to testing the systems) is outsourced to a contractor, information leakage might be caused by the contractor's fault or negligence. Organizations should establish a contract over what and how information is handled by and exchanged with their contractors.

Impact

Personal information that is held by enterprises and should be protected from leakage is classified into the following two types (see BPnet in <References>): the one whose leakage might result in "economic loss" (such as credit card number and security code) and the one whose leakage might give mental anguish to the victims (such as the results of health checkup and medical history.) Personal information whose leakage might result in economic loss is likely to be abused.

There is information that has both of these natures. For example, leakage of information on one's assets, deposit balance, and income causes both "economic loss" and "mental anguish." In the case of personal information whose leakage gives mental anguish to the victims, leakage itself becomes a serious humanitarian issue without involvement of a person with malicious intent.

As a result of leakage of such information, users might suffer "economic loss" and/or "mental anguish." Damages suffered by these users result in the loss for the organization.

Possible losses which the organization might suffer include: due to the breach of contract, it might be sued by those who suffered damages; it might lose its clients who suffered damages, etc. These losses are attributed to the loss of confidence in that organization, resulting from the damages suffered by the victims. Another possible result is that, the incident might be reported in the media and the organization might lose the trust of its stakeholders.

Incident response is also of importance. By taking quick, appropriate responses in the event of information leakage, the organization might be regarded as the one implementing appropriate security measures and its brand image and trust could improve. If possible, organization should take these measures.

Chapter Three: Countermeasure

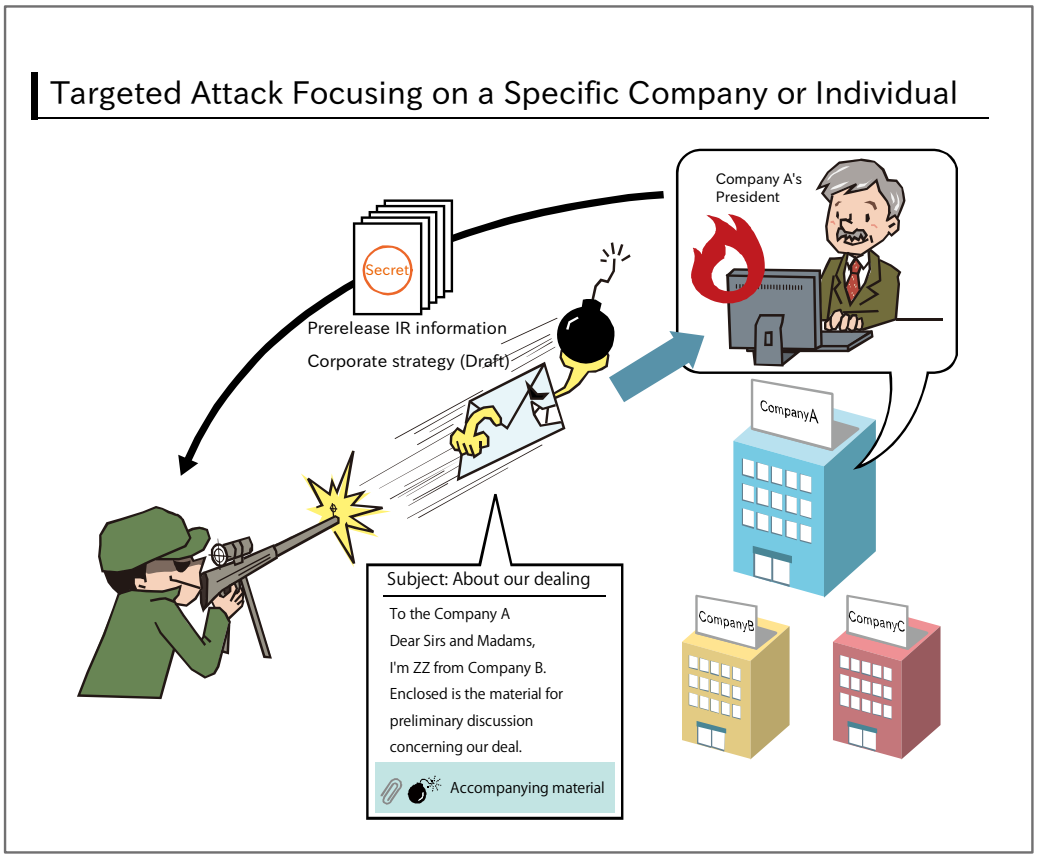
"3.1 Establishing framework and rules (P28)", "3.2 Planning and designing secure operation approach (P29)", "3.3 Concluding a contract for secure operation (P29)"

"3.8 Examining the established framework/rules/systems (P31)", "3.9 Reviewing and modifying (if necessary) the established framework/rules/systems (P31)"

<References> (All in Japanese)

BPnet:
http://www.nikkeibp.co.jp/sj/2/column/c/19/index.html
So-net:
http://www.so-net.ne.jp/security/news/newstopics_200907.html
SecurityNext::
http://www.security-next.com/cat_cat25.html

【6th】Targeted Attacks Carried Out Without Victims' Noticing



Targeted Attack is an attack method in which a virus is transmitted to the victim's PC via an e-mail whose sender address is spoofed as an acquaintance or a business partner.

Threat

Targeted Attack was acknowledged as a problem in 2005. Damages reported include virus infections reported by US-CERT and JPCERT/CC[1]. Since then, there have been a number of cases where a specific individual/organization was attacked and this attack method became a subject of researches.

It is natural for one to open an e-mail from his friend or client. If any suspicious elements were not found in the body message, the receiver would not think that a virus might be attached. This is true for an e-mail whose sender address is not spoofed as a friend or a business partner. One of the characteristics of Targeted Attack is that the receiver cannot distinguish an attached virus from an ordinary file. In most cases, this virus exploits software vulnerability. So the virus is sent in a manner that makes it difficult for the receiver to distinguish it from an ordinary file. When the file is opened, a document is displayed, so the user might not notice that the attached file contains a virus. In this way, Targeted Attach has a multi-layered mechanism to make the receiver unable to notice that an attack has been carried out.

A virus that exploits software vulnerability can be prevented by adequately updating software products. But a greater threat is that zero-day attack could be carried out that exploits vulnerabilities not fixed by vendors.

The target of Targeted Attack might include an individual having the enterprise's important information such as management personnel. In such cases, sensitive information concerning the enterprise's operations might be stolen.

Targeted Attack focuses on a specific individual/organization and makes it difficult for the victim to notice that an attack has been carried out. A basic countermeasure against this attack is to

[1] http://www.jpcert.or.jp/wr/2005/wr052701.txt

apply software updates. Those who have received such attack should consult with an organization engaging in information security and share the information so that other people do not receive the same attack.

Case Examples and Statistics for the Year 2009

In 2009, JPCERT/CC released “IT Security Inoculation Research Report.” In this research about 2,600 people from various types of industries went through a simulated Targeted Attack, in which an e-mail having the same mechanism as that of Targeted Attack was sent to them.

The research results showed that regardless of age, gender, type of job, anybody could be tricked by Targeted Attack from Targeted Attack. In the first test, those who opened that file accounted for 45.4 percent and the ratio decreased to 14.0 percent in the second test. The result may indicate that people have learned from an experience of receiving Targeted Attack.

According to a security vendor’s report, the number of Targeted Attacks observed from January 2009 through May 2009 was 663. The ratio increased for the case where a virus exploiting vulnerability in Adobe Reader/Acrobat was attached, compared to the previous year level. Apart from vulnerability in Adobe Reader/Acrobat, vulnerability in Microsoft Word, Excel and PowerPoint was targeted. Compared to 2008 (1,968 cases), cases involving Microsoft products decreased to about 51 percent from about 72 percent while those of Adobe products increased to about 49 percent from about 29 percent. The report says that vulnerability in Adobe products is relatively easy to detect.

Impact

In one case involving Targeted Attack, a management personnel having the company's important information was reportedly targeted. Information held by those in management layer is thought to be much more important than ordinary ones. If corporate strategy information or drafted management plan was stolen, the enterprise’s business continuity might seriously be affected. Needless to say, these scenarios are not limited to those in management layer but any personnel retaining sensitive information or having access to such information. Therefore, it is important for organizations to regularly provide information security education and training to their employees so that cautions are always exercised by all the people concerned. All the members of an organization should be aware of this threat.

Chapter Three: Countermeasure

"3.1 Establishing framework and rules (P28)", "3.2 Planning and designing secure operation approach (P29)", "3.3 Concluding a contract for secure operation (P29)"

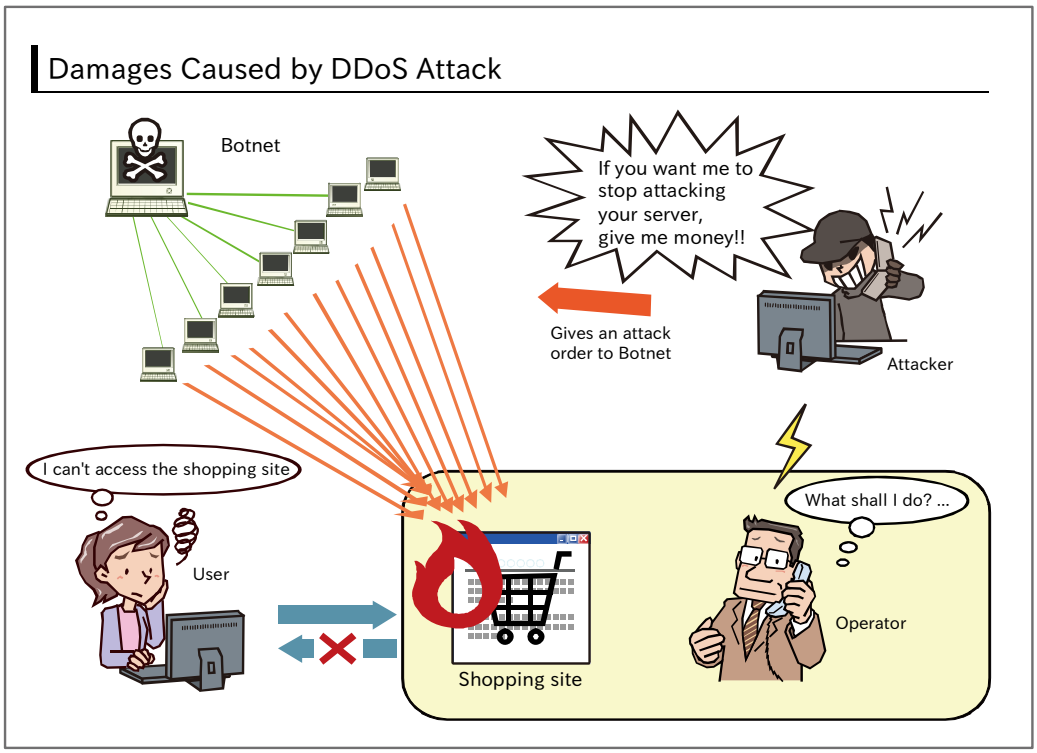
"3.5 Implementing countermeasure for client systems (P30)"

"3.8 Examining the established framework/rules/systems (P31)", "3.9 Reviewing and modifying (if necessary) the established framework/rules/systems (P31)"

<References> (All in Japanese)

JPCERT/CC:
http://www.jpcert.or.jp/research/index.html#inoculation
ITPro:
http://itpro.nikkeibp.co.jp/article/NEWS/20090507/329641/

【7th】DDoS Attacks That Cause Serious Damages



Distributed Denial of Service（DDoS） attack is a type of DoS attack that cripples the functions of a server or a router, etc.

Threat

DoS attack is broadly classified into the following two categories:

1) The one that exploits vulnerability in a server or a router
2) The one that sends a large volume of requests that exceed the performance limitations of a server or a network

DDoS attack is also called “Distributed Denial of Service” and mainly uses the method 2). In DDoS attack, an attack to a specific server is carried out from a number of distributed computers.

Example of an attack that uses method 2) is a large volume of HTTP requests being made to the target server. Some of DDoS attacks can be done in an unsophisticated way. In the attack mentioned above, the attack is achieved by just sending a large volume of HTTP requests simultaneously to the target server

If DoS attack was carried out from one point, it would be prevented by blocking access from that point. But in the case of DDoS attack where the attack was carried out from a large number of computers, it is not easy to counter the attack with access control while providing services.

Mechanism of HTTP request attack is not sophisticate. If a person holding a grudge against an organization called for participation to the attack and many people agreed to join him, a collaborated attack might be carried out. The result would be similar to the one brought about by many people accessing a specific server at the same time. Furthermore, if an attacker’s tool was distributed to collaborators, an attack would more easily be carried out, causing extensive damages.

Three major objectives for an attacker carrying out DDoS attack are as follows:

(1) Causing social disruption by making the Nation’s important information systems unable to provide services;
(2) Settling a grudge against the service provider;
(3) Making a profit through fraud or extortion in return for stopping such attack

In the case of objective (3), an attacker uses Bot or other methods to carry out DDoS attack and

cause denial of services, and then spoofing as security service provider, trick the victim into paying money.

There are other cases where Bot is used to carry out an attack. Bots do exist around the world, which means that attackers have a number of bases for carrying out DDoS attack.

Case Examples and Statistics for the Year 2009

In July 2009, there was a news report which said Websites of the U.S. government and Korean public institutions/ private companies received DDoS attack. In this attack, Bot-infected PCs were abused. The number of Bot-infected PCs used for this attack was more than 130,000 worldwide.

This Bot infection was difficult for PC users to prevent. Infection began by the defacement of a Website. Through this defacement, Bots were included in program updates provided by the Website. Because the updates were supposed to be provided by that Website, users executed them without any doubt.

In this attack, each Bot was assigned a specific role, indicating that analyzing only one Bot would not have lead to getting a whole picture of that attack. Furthermore, communication concerning an attack from a Bot was spoofed as an ordinary communication, so it was difficult for the victims to determine whether it was an attack or an ordinary communication.

In Japan, there has been a case where an attack was carried out against a rental server for an Application Service Provider (ASP). After receiving the attack, the ASP released a report on system failure, how the service provider responded、the actions./countermeasures the service provider took. This sort of incident response ensures that trust relationship with users is not deteriorated.

Impact

If an information system whose operating status (i.e., if not in operation) affects the organization's business continuity received DDoS attack, it would have a significant impact on the organization. Possible impacts on financial institutions and shopping sites include: economic loss incurred by the loss of opportunities for commodity trading.

As in the case of above-mentioned DDoS attack against a DNS server, if such attack was carried out against a network resource outside the organization's control, services that use the resource might become unavailable to users.

Chapter Three: Countermeasure

"3.1 Establishing framework and rules (P28)", "3.2 Planning and designing secure operation approach (P29)", "3.3 Concluding a contract for secure operation (P29)"

"3.8 Examining the established framework/rules/systems (P31)", "3.9 Reviewing and modifying (if necessary) the established framework/rules/systems (P31)"

<References> (All in Japanese)

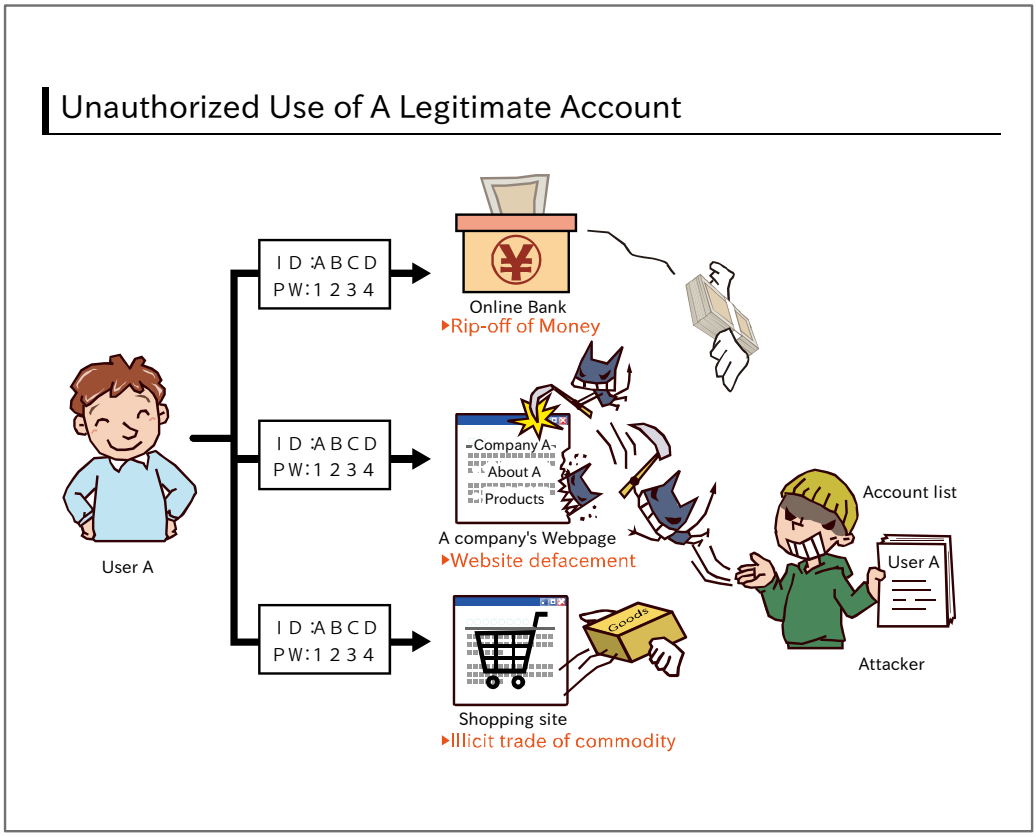
Impress:

http://internet.watch.impress.co.jp/docs/news/20090710_301397.html

ZDNet Japan:

http://japan.zdnet.com/news/sec/story/0,2000056194,20402570,00.htm

【8th】Unauthorized Use of A Legitimate Account



An account is information supplied by a person for his identification (e.g., User ID and password, etc.) when using Internet services such as online banking or computers. There have been many cases where an inappropriate account management led to incidents.

Threat

Account information, particularly passwords, should be known only by their owners and should be prevented from being known by others. For example, if your password was known by a third party, he might spoof as you and perform operations on your information systems.

Possible damages caused by the exploitation of account information include:

- The organization's Website being defaced
- Illicit transactions being performed on online banking or shopping sites.
- Fraudulent activities being performed on Social Network Service or other services by spoofing as the victim's friend

Possible causes of legitimate account exploitation include:

- A simple password being used

  According to a report, there have been many cases where a simple password such as "abcde" or "password" was used or the same character strings as user ID was used for a password. A simple password might easily be guessed by an attacker, resulting in the exploitation of account information.
- Account (ID & password) being used for multiple services

  Where the same account is used for multiple services on the Internet, if the account was compromised in one service, it might be used to exploit the rest of those services.
- A paper containing a password being left on one's desk or other places where anybody can see it

  User ID and password for important information systems are information that should be known only by those who need to operate them. Writing such information on a paper

and leaving it on one's desk or pasting it on one's computer desktop might lead to a security incident.

- Unnecessary accounts not being deleted

  There is a case where unnecessary accounts such as those of retired employees have not been removed, which might allow an attacker to use them to access the organization's internal systems.

Case Examples and Statistics for the Year 2009

Among the legitimate account exploitation incidents that occurred in 2009, what stood out most was Website defacement by Gumblar. In the past, there were cases where an account used for multiple services was compromised by an attacker, leading to the alteration of personal information and illicit commodity trading. According to a security vendor's survey results released in 2009, three out of ten people are using the same password for multiple services.

Exploitation of accounts is not limited to Japan; such incidents are also occurring in overseas, including tactic where an SNS account was compromised and a fraudulent activity was carried out against its owner.

In Japan, there was a news report on a case where a retired employee holding a grudge against his former company had defaced the company's Website by using his former account that had not been removed. Such incident could happen due to a security hole in account management.

Impact

If exploited, a legitimate account might allow an attacker to perform unauthorized operations on that system or to steal information stored, making it difficult for the system owner to distinguish exploitation from authorized use, delaying the time such exploitation is detected by the owner suffering damages.

For proper authentication, users and administrators should use a separate ID and password for each service/system. However, it is almost infeasible to remember all account information. Apart from ID and password, biological information and nonce can be used for authentication. When introducing new hardware, organizations may consider employing dual authentication with biological information for the second authentication.

Chapter Three: Countermeasure

"3.1 Establishing framework and rules (P28)", "3.2 Planning and designing secure operation approach (P29)", "3.3 Concluding a contract for secure operation (P29)"

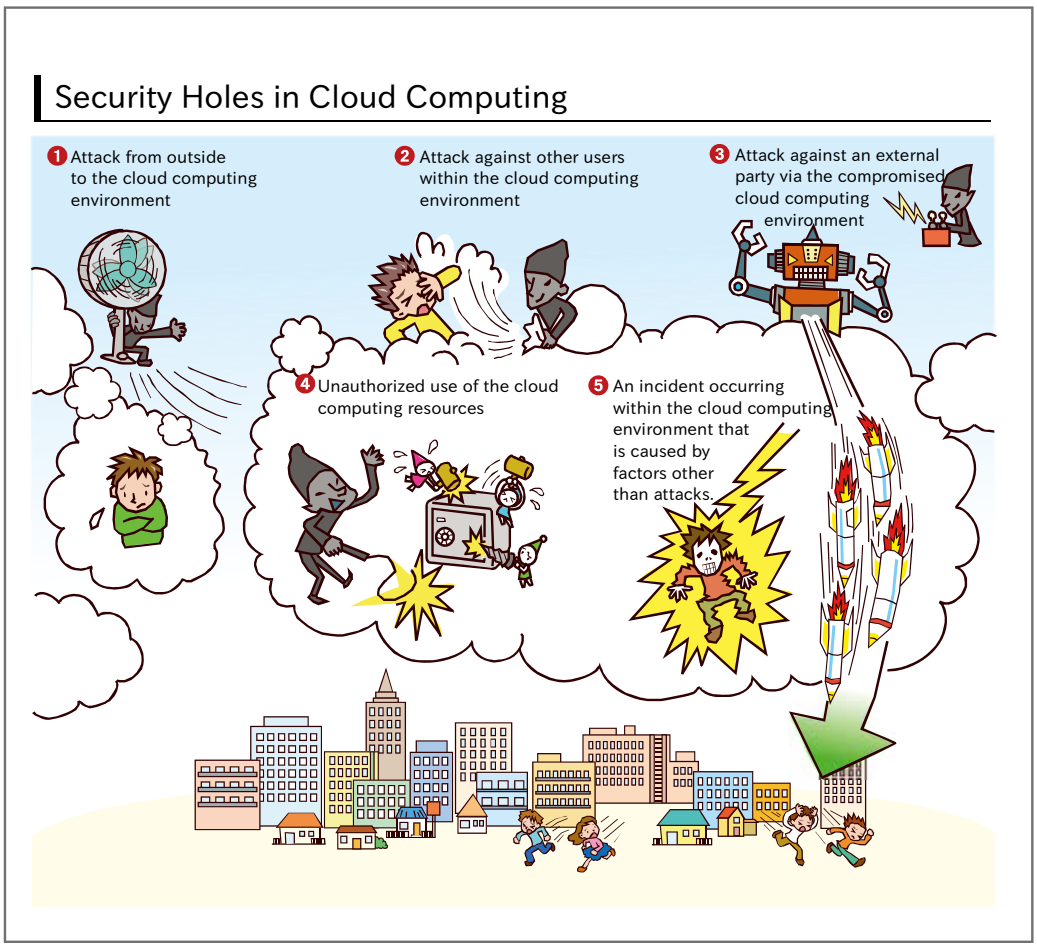
"3.6 Managing account information (P30)"

"3.8 Examining the established framework/rules/systems (P31)", "3.9 Reviewing and modifying (if necessary) the established framework/rules/systems (P31)"

<References> (All in Japanese)

ITMedia:
http://www.itmedia.co.jp/enterprise/articles/0903/12/news028.html
ITMedia:
http://www.itmedia.co.jp/news/articles/1001/22/news025.html

【9th】Security Holes in Cloud Computing



As cloud computing (hereinafter called 'cloud') has become prevalent, security issues concerning cloud have also been pointed out.

Threat

National Institute of Standards and Technology (NIST) in the U.S. defines cloud as: "Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort".

a. SaaS (Software as a Service): software service such as electric mail and groupware
b. PaaS (Platform as a Service): virtualized application servers/ databases, etc.
c. IaaS (Infrastructure as a Service): virtualized server and shared disk, etc.

Cloud-related security issues pointed out are as follows:

1) An attack against cloud environment from outside

Cloud environment might become the target of an attack. Unlike in the case where a server and service are provided by the company, data resides on a single point in the shared cloud environment. This means that if an attack was successful, it might have significant impacts.

2) An attack against other users within the cloud environment

Cloud environment is shared by other users, possibly including a person with malicious intent (e.g., attacker). By exploiting this environment, an attacker might carry out an attack against other users. For example, vulnerability of virtualization technology em-

ployed in the cloud environment might be exploited to carry out an attack against other users within the environment.

3) An attack against external parties by using the cloud environment as a stepping stone

Cloud environment could be exploited to carry out an attack. (e.g., DoS attack and other attacks against a third party.) An attacker might also embed malware in the environment of a well-meaning cloud user, aiming at attacking other systems outside the cloud environment.

4) Exploitation of cloud resources

Cloud environment could be used as a resource for carrying out an attack (e.g., cryptanalysis, password cracking). It is not easy for cloud service providers to detect and prevent such attacks as they have difficulty in distinguishing a legitimate use from unauthorized one.

5) An incident that occurs in the cloud environment from the causes other than an attack

In the cloud environment, service might become unavailable due to blackout at the data center or other facilities, or software/hardware failures.

Case Examples and Statistics for the Year 2009

In 2009, cloud-related incidents and accidents occurred.

There has been a case where a leading cloud computing service being deployed overseas received DDoS attack from outside as described in 1). In this case, although a user of the cloud service contacted the service provider, saying "I think there is something wrong with your service," the provider failed to detect the attack, for which it took much time to recover from the incident. This is a typical case where users are relying heavily on their service providers for the implementation of countermeasures against security incidents and accidents.

Impact

In the traditional case where a server and service are provided by the company, even if an incident occurred to such service or vulnerability was detected, cause(s) of them could be identified and response taken by the company.

In the cloud environment, the cloud service provider might respond to security incidents. If the cloud service provider lacks awareness of vulnerability and incidents, adequate information might not be conveyed to the cloud users, for which they might not be able to take appropriate responses to solve the problems they may face.

Chapter Three: Countermeasure

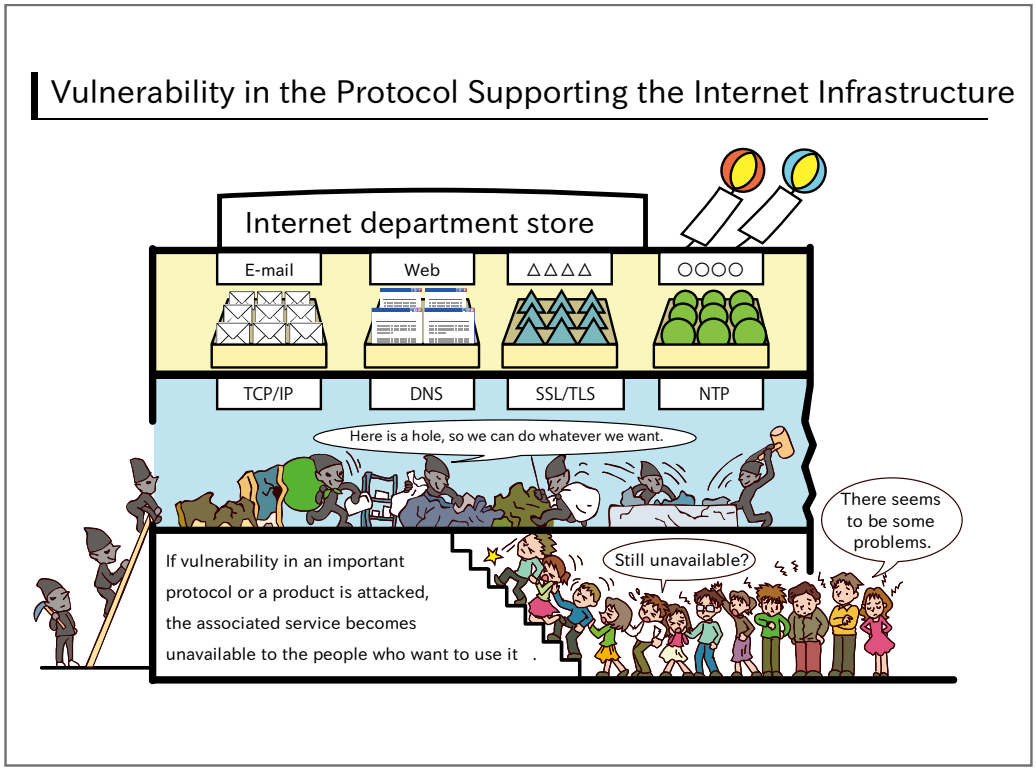
"3.1 Establishing framework and rules (P28)", "3.2 Planning and designing secure operation approach (P29)", "3.3 Concluding a contract for secure operation (P29)"

"3.8 Examining the established framework/rules/systems (P31)", "3.9 Reviewing and modifying (if necessary) the established framework/rules/systems (P31)"

<References> (All in Japanese)

Impress:
http://internet.watch.impress.co.jp/docs/news/20091208_334134.html
ITPro:
http://itpro.nikkeibp.co.jp/article/NEWS/20091209/341795/

【10th】Vulnerability in the Protocol Supporting the Internet Infrastructure



Many computers have the Internet access feature. If vulnerability in such feature was detected and attacked, the Internet might significantly be affected.

Threat

Among the technology and products that support the Internet infrastructure are: Internet Protocol (IP) which is a protocol for connecting one network to another for information exchange and Domain Name System (DNS) that maps IP addresses to domain names, HTTP used for World Wide Web (WWW), Simple Mail Transfer Protocol (SMTP) and Post Office Protocol (POP3) used for e-mail services, Network Time Protocol (NTP) used to synchronize the clocks of the devices connected with a network. Apart from them, routing technique for the selection of communication path and Secure Sockets Layer/Transport Layer Security (SSL/TLS) that encode communication are widely used on the Internet.

Vulnerability in the protocols that offer the above-mentioned feature and the products equipped with these protocols may pose serious risks to their users. If such vulnerability was attacked, the Internet might significantly be affected. For example, if DNS protocol has vulnerability to DoS attack and an attack was carried out against such vulnerability throughout the world, the Internet might be paralyzed in the end. And if a communication-encoding protocol has vulnerability, encoded messages might be decoded, resulting in the decreased reliability in cryptographic communication and secure use of the Internet being hampered.

For critical systems like the Internet, it is important to be in operation without interruption so, applying updates is not as easy as general systems. For this reason, organizations should establish a periodical update plan and whenever possible, a workaround plan.

Case Examples and Statistics for the Year 2009

Among the software product vulnerabilities released in 2009, there were several vulnerabilities related to the products supporting the Internet infrastructure. In this section, we present the four issues we paid particular attentions (See <References>)

The first issue is, vulnerability of Berkeley Internet Name Domain (BIND), which is a DNS server software provided by Internet Systems Consortium (ISC), to DoS attack. Because of this vulnerability, a BIND receiving a particular kind of packet fell into a halt condition.

The second issue is, vulnerability of TCP/IP to DoS attack. Because of this vulnerability, systems receiving a particular kind of packet began to reject communications with others. Since the beginning of 2009, vendors have been tackling this issue.

The third issue is, vulnerability of SSL/TLS. Because of this vulnerability, SSL/TLS was unable to prevent a third-party-relayed attack in which an attacker mediated communications. This vulnerability was related to the protocol itself and therefore, any products using this protocol might be affected. RFC for the protocol's technical specification has been amended in 2010.

The forth issue is, vulnerability of NTP. Up to now, several vulnerabilities have been reported concerning NTP and those vulnerabilities have been fixed. Because of those vulnerabilities, NTP receiving a particular kind of packet fell into a state of denial of service or systems could be hijacked through the buffer overflow attack.

Impact

All the Internet users might be affected by this threat. For those developing Internet access devices, the impact of this problem would be significant.

If such vulnerabilities were detected in their products, developers should fix them. In some cases, they may have to fix vulnerability in the protocol used in their products.

Among the users who might significantly be affected are: Internet Service Providers (ISPs) and hosting service providers handing a large number of such devices. Damages suffered by such provides might be extended to their clients and people concerned and therefore, these vulnerabilities are serious problems for them.

Chapter Three: Countermeasure

"3.1 Establishing framework and rules (P28)", "3.2 Planning and designing secure operation approach (P29)", "3.3 Concluding a contract for secure operation (P29)"

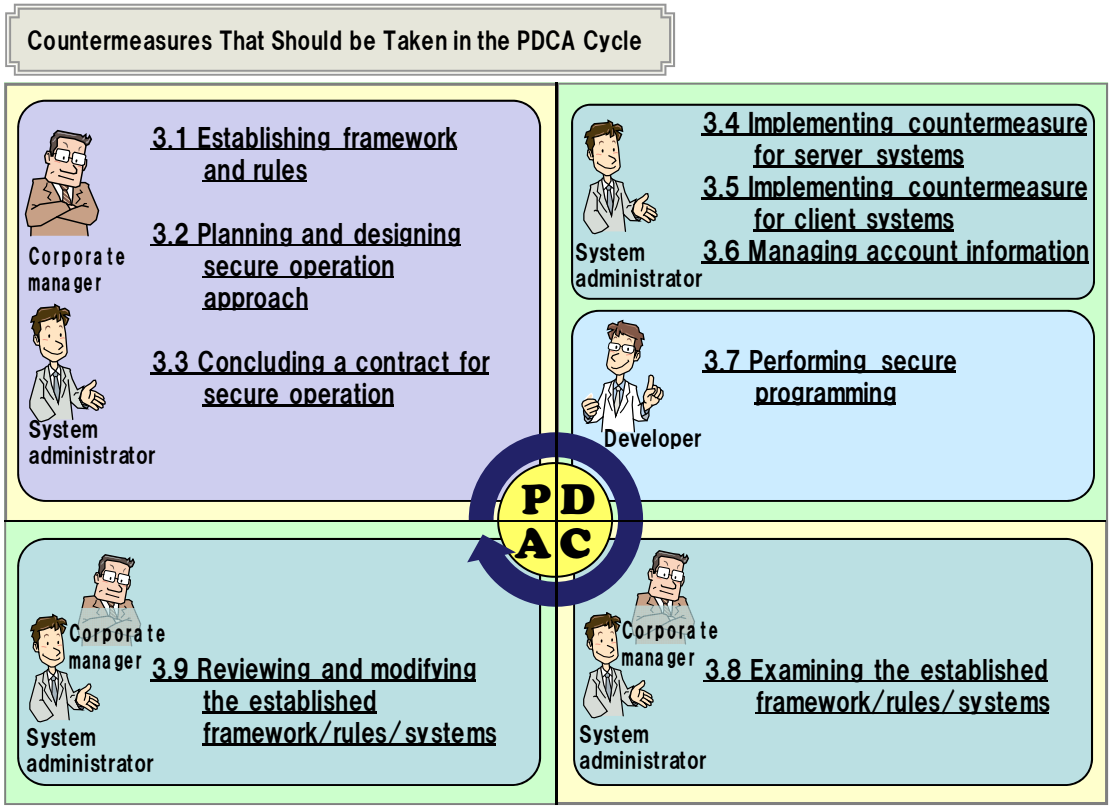
"3.4 Implementing countermeasure for server systems (P30)"

"3.8 Examining the established framework/rules/systems (P31)", "3.9 Reviewing and modifying (if necessary) the established framework/rules/systems (P31)"

<References> (All in Japanese)

JVN:
http://jvn.jp/cert/JVNVU725188/
JVN:
http://jvn.jp/cert/JVNVU261869/
JVN:
http://jvn.jp/cert/JVNVU568372/
JPCERT/CC:
http://www.jpcert.or.jp/at/2009/at090019.txt

Chapter Three Countermeasures



It has become a standard for organizations to include information security measures into their business challenges.

This chapter presents countermeasures against the threats described in Chapter two. There are a variety of books addressing information security and organizations should ensure the required and adequate level of information security by referring to those books.

This chapter relates persons concerned to the PDCA cycle as shown in the figure above. Persons concerned are required to take appropriate measures in each phase they are involved.

3.1 Establishing a Framework and Rules

[Person in charge: corporate manager/system administrator]

The first thing a corporate manager should do as a security measures is to establish a security management cycle within the organization. The established security management cycle should serve as a guideline for maintaining and improving the organization's information security level. The next step is to establish Contingency Plan (CP) and Business Continuity Plan (BCP) that are initiated in the event of an incident/accident affecting the organization's business continuity. BCP is a plan specifying how an organization will restore critical business and make a quick recovery in the event of information security incident/accident. By giving education and training to its employees and managing business continuity based on the established BCP, organizations can ensure the continuity of critical business.

This section is classified into two parts: "proactive measure" and "incident response". Corporate managers order the establishment of proactive measures and incident response and system administrators establish draft rules and framework based on the given instructions. Appropriateness of the draft is evaluated by corporate managers and put in practice if determined to be appropriate.

<Proactive Measure>

The first step to establish a security management cycle within the organization is, to establish team/framework to promote information security measures and then define the objective and prin-

cipal for the established security countermeasures. (Basic policy) This basic policy should include countermeasures described in Section 3.2 and 3.3. Following this, organizations should identify information assets within the organization that should be protected, conduct analysis on the risks posed on those assets, and then formulate concrete countermeasures. (Standard measure) Organizations should then establish concrete procedures to implement those countermeasures and corporate managers should responsibly communicate them throughout their organizations and ensure that their employees comply with them.

When developing BCP, organizations should first indentify important information and information systems that should be protected to ensure business continuity, and then identify the people responsible for them as well as potential impacts of information security incidents and accidents.

Based on the information extracted, organizations should determine how the established security countermeasures are implemented by whom with what framework and rules, analyze the level of impacts in terms of business continuity, and examine how to deal with the risks. For countermeasures, organizations should consider applying any of the followings: "Reducing the risk (decreasing the possibility of occurrence of a security incident/accident)"; "Accepting the risk (accepting the possibility of occurrence of a security incident/accident)"; "Avoiding the risk (removing the elements of occurrence of a security incident/accident)"; "Transferring the risk (allocating funds to the losses incurred by a security incident/accident)," as described in "Responses to Risks" in "Information Security Management and PDCA cycle." (Released by IPA)

<Incident Response>

As incident responses, organizations should consider the followings: "activation of BCP", "investigation of the cause", "risk communication including corresponding to clients", and "implementation of the measures for preventing the recurrence of such incidents."

Organizations should define the criteria for "initiation of BCP" in the event of a security incident/accident as well as incident response systems to respond to security incidents/accidents.

Based on the incident response systems, "investigation of the cause" and "implementation of the measures for preventing the recurrence of such incidents" should be performed. In case organizations need help from an external specialist research organization in responding to an incident, organization should decide in advance what organization to ask.

"Risk communication including corresponding to clients" requires organization to identify the people concerned as well as how to respond to assumable incidents.

For risk communication, organizations need to consider how they would appropriately release and explain the information necessary for people concerned.

3.2 Planning and Designing Secure Operation Approach

[Person in charge: system administrator]

For secure use of systems, organizations should conduct planning and designing by taking into account all the possible cases. Organization should define required information security level and countermeasure to ensure the secure operation of systems and information asset and whether they are going to implement them or outsource them to an external party.

For system operation planning and designing, see documents. For example, organizations need to consider the following security controls:

1) Asset classification and control
2) Human resource security
3) Physical and environmental security
4) Communications and operational management
5) Access control
6) Acquisition, development and maintenance of information systems
7) Information security incident management
8) Business continuity management
9) Compliance from the aspect of laws and audits

3.3 Concluding a Contract for Secure Operation

[Person in charge: corporate manager/system administrator]

The objective/purpose of this countermeasure is to ensure that appropriate level of information security is provided by the contracted party. Organizations may outsource to an external party part(s) of their business such as system management and operation. Organizations may also form a business tie-up with other organizations through supply chain etc.

If appropriate level of security countermeasures is not implemented by the contracted party or business partners, the contracting party's information systems might suffer damages in terms of business continuity. To prevent this, organizations should review, from the aspect of information security, their regulations related to contracts, operation rules and contracts (ordering agreement), contractor selection criteria, nondisclosure agreement, and handling of personal information. After reviewing them, organizations should have their audit department to periodically check their contractors for their compliance with the established regulations and rules.

3.4 Implementing Countermeasure for Server Systems

[Person in charge: system administrator]

The objective/purpose of this countermeasure is to prevent an attack against server products and collateral damages caused by such attacks. For server products, updates should be applied to counter vulnerability. However, unlike client products, the more important systems the server product handles, the harder it is to apply updates, as its services might be suspended due to the updates. On the other hand, if the server product continues to be used without fixing existing vulnerability, it might become the target of an attack.

The solution is to establish an update plan or a workaround plan and implement it. Organizations should first build a test environment for updates and test the updates they are going to apply in that environment, and if proven to be safe, they should apply those updates in their production environment.

If it is unavoidable for services to be affected by the update process, organizations should use a mechanism (e.g., IDS/IPS, WAF) to detect and defend against attacks. Use of IDS/IPS or WAF requires specialized know-how and the collection of expertise, so the organization considering using them should also take into account the balance between cost and risks. They may also consider using a monitoring service provided by a security company. Such service might provide a higher level of security compared to the one provided by the organization itself.

3.5 Implementing Countermeasure for Client Systems

[Person in charge: system administrator]

The objective/purpose of this countermeasure is to prevent an attack against client software and collateral damages caused by such attacks. If virus infection was caused by an attack, it might result in the spread of collateral damages.

The solution is to keep your operating systems and client software up-to-date. For operating systems, you can apply the automatic update function provided by the operating systems. For client software, an automatic update function might not be available. In such cases, you can use "MyJVN Version Checker" provided by IPA to check for the version of some of software products you are using.

Note, however, that even in the case of software product kept up-to-date, it cannot prevent zero-day attack. Zero-day attack can be prevented by using antivirus software with its pattern files kept up-to-date. It is also effective to use antivirus software that can check the behavior of an executable file for virus-infection. The objective/purpose of this countermeasure is to prevent virus infection and collateral damages caused by such infections.

3.6 Managing Account Information

[Person in charge: system administrator]

The objective/purpose of this countermeasure is to prevent one's account from being stolen. For this, organizations need to implement appropriate account management. Concrete countermeasures are as follows:

<Server settings>

Two major countermeasures concerning server settings are as follows:

- Remove or disable unnecessary accounts;
- Limit the points from which the organization's

server(s) can be accessed.

<User Education>

System administrators need to educate account users about the following three issues.

- For each account, set different passwords;
- Keep passwords and other authentication information only in your mind/secret place;
- Use a long, complex password

3.7 Performing Secure Programming

[Person in charge: developer]

The objective/purpose of this countermeasure is to prevent an attack against Websites and software programs. When building a Website, organizations should make efforts to improve security of their Website by referring to "How to Secure Your Web Site" and "Secure Programming," released by IPA.

Secure programming is also required for software products and embedded software products. Developers need to prepare for the case where all the measures required are not implemented or vulnerability is detected. It is recommended that developers provide a simple-update function along with their products so that users can easily upgrade to a new version with existing vulnerabilities fixed.

3.8 Examining the Established Framework/Rules/Systems

[Person in charge: corporate manager/system administrator]

The objective/purpose of this countermeasure is to verify whether security management cycle employed by the organization is appropriately operated and followed and whether security countermeasures employed in the organization's information systems are functioning effectively to re-evaluate the risks posed. After the evaluation and inspection, organizations should implement the review and improvement process described in Section 3.9.

Organizations need to bring existing risks to the surface by inspecting and evaluating whether security management cycle employed and operated by the organization and information security measures are functioning as effectively as planed to maintain the appropriate level of information security, and whether there is any potential vulnerability.

Among the evaluation systems for information security measures are: "self-inspection", "Information Security Management Benchmark" by IPA, "Information security audit." As an option, organizations may ask a third party to evaluate their information security for certification.

3.9 Reviewing and Modifying (If Necessary) the Established Framework/Rules/Systems

[Person in charge: corporate manager/system administrator]

The objective/purpose of this countermeasure is to review and improve security countermeasures based on the risks re-evaluated in Section 3.8. Organizations should review the appropriateness of their information security team/framework and rules based on the assessment and inspection results of security countermeasures being implemented.

In response to the re-evaluated risks, organizations should first conduct risk analysis. Organizations should select the most appropriate risk-handling from: "Reducing the risk"; "Accepting the risk"; "Avoiding the risk"; "Transferring the risk."

It is also important to review the appropriateness of security countermeasures currently being implemented.

Through the review, organizations should identify security countermeasures that have become a mere facade or that are missing.

【Appendix A】Relations among 10 Major Security Threats

Appendix Table 1 shows those who need to take countermeasures against 10 Major Security Th reats. Among the new threats ranked in Top 10 in this year are: "Client Software Not Updated" a nd "Vulnerability in Unsecured Server Products." Among the threats ranked higher than the previo us year level are: "Ever-Changing Tactics for Website Defacement" and "Malicious Purposes/Objec tives of Computer Virus and Bots."

Appendix Table 1. Overall Rankings and Those who Need to Take Measures

10Major Security Threats		Those who Need to Take Measures			Ranking 2009 [White Paper 2009]	Ranking 2008 [White Paper 2008]
		Management	System Administrators	Developers		
1st (Up)	Ever-Changing Tactics for Website Defacement	◎	◎	◎	2nd	5th
2nd (Up)	Client Software Not Updated	○	◎		–	4th
3rd (Up)	Malicious Purposes/Objectives of Computer Virus and Bots	○	◎		4th	6th
4th (Up)	Vulnerability in Unsecured Server Products	○	◎			
5th	Information Leakage without Proper Incident Response	◎	◎		5th	3rd
6th	Targeted Attacks Carried Out Without Victims' Noticing	◎	◎		3rd	4th
7th	DDoS Attacks That Cause Serious Damages	○	◎		–	–
8th (Up)	Unauthorized Use of A Legitimate Account	○	◎		10th	–
9th (Up)	Security Holes in Cloud Computing	◎	◎		–	–
10th	Vulnerability in the Protocol Supporting the Internet Infrastructure	○	◎		–	–

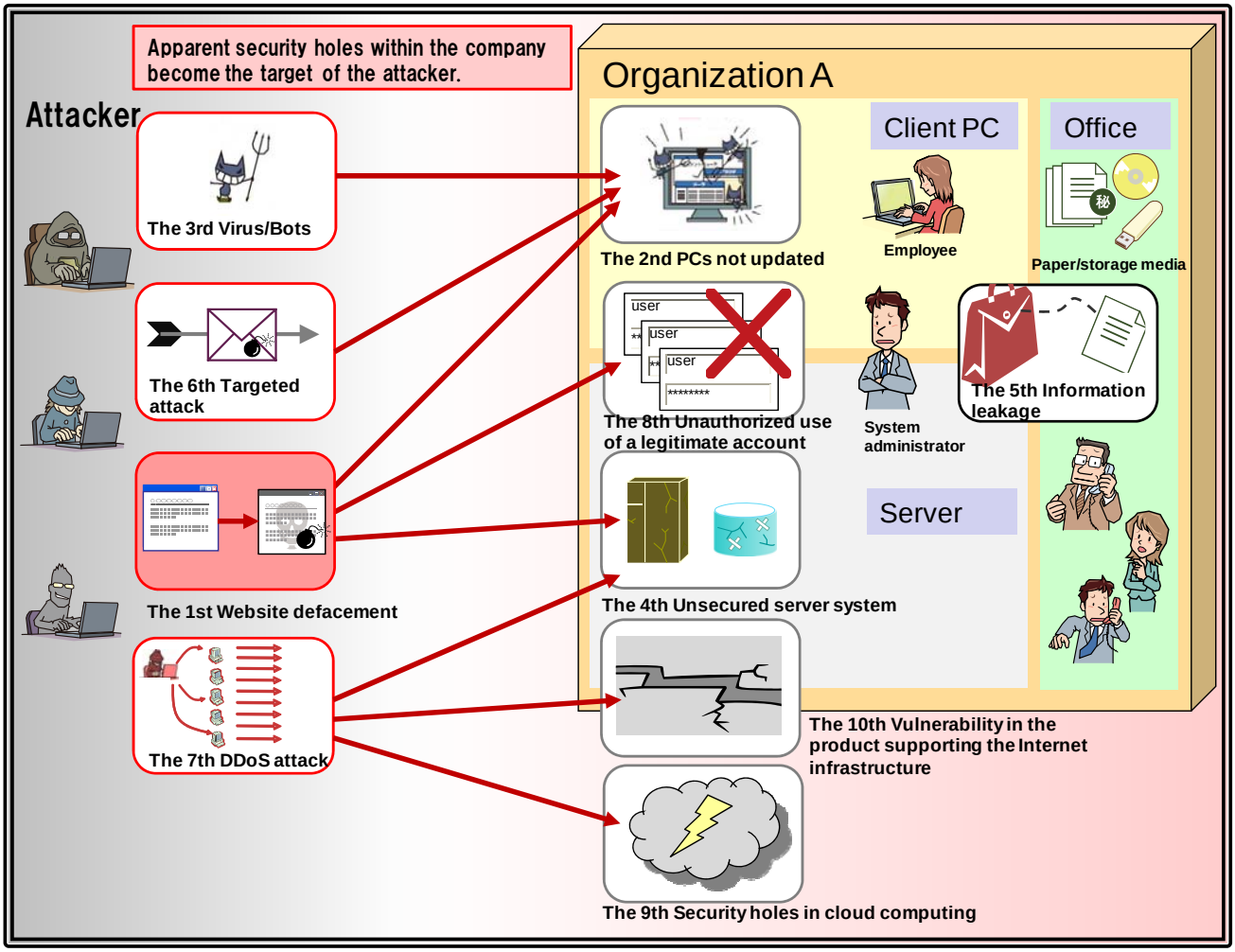
◎:Those who should take measures ○:Those who should take measures on an as-needed basis

(Up):Those ranked higher than the previous year level

【Appendix B】Correlation Diagram of 10 Major Security Threats

Appendix Figure 1 shows relations among 10 major security threats. These threats are categorized into three groups: a threat in which attackers use their attack tactics ("The 1st Ever-Changing Tactics for Website Defacement, "The 3rd Malicious Purposes/Objectives of Computer Virus and Bots", "The 6th Targeted Attacks Carried Out Without Victims' Noticing", "The 7th DDoS Attacks That Cause Serious Damages"), a threat in which attackers exploit security holes within the organization ("The 2nd Client Software Not Updated", "The 4th Vulnerability in Unsecured Server Products", "The 8th Unauthorized Use of A Legitimate Account", "The 9th Security Holes in Cloud Computing", "The 10th Vulnerability in the Protocol Supporting the Internet Infrastructure"), and a threat in which damages are caused regardless of the involvement of attackers ("The 5th Information Leakage without Proper Incident Response ").

Arrows in Appended Figure 1 indicate that the "attacker" is attempting to exploit vulnerability within the "organization". Appended Figure 1 does not cover all the relations among 10 Major Security Threats and it does not refer to other threats than 10 Major Security Threats.



Appended Figure 1. Relations among 10 Major Security Threats

Production Information-technology Promotion Agency, Japan (IPA)

Executive editor Hideaki Kobayashi Tadashi Yamagishi

Collaborator 10 Major Security Threats Authors' Committee

Author Motokuni Souma

For the Year 2010

10 Major Security Threats
"Organizations' Security Flaws Brought to the Surface"

Mar. 31, 2010 First Printing

[Editor] Information-technology Promotion Agency, Japan

2-28-8 Honkomagome, Bunkyo-ku, Tokyo

113-6591 Japan

http://www.ipa.go.jp/

How to Report Information Security Issues to IPA

Designated by the Ministry of Economy, Trade and Industry, IPA IT Security Center collects information on the discovery of computer viruses and vulnerabilities, and the security incidents of virus infection and unauthorized access.

Make a report via web form or email. For more detail, please visit the web site:
URL: http://www.ipa.go.jp/security/todoke/ (Japanese only)

Computer Viruses

When you discover computer viruses or notice that your PC has been infected by viruses, please report to IPA.

Unauthorized Access

When you detect unauthorized access to your network, such as intranets, LANs, WANs and PC communications, please report to IPA.

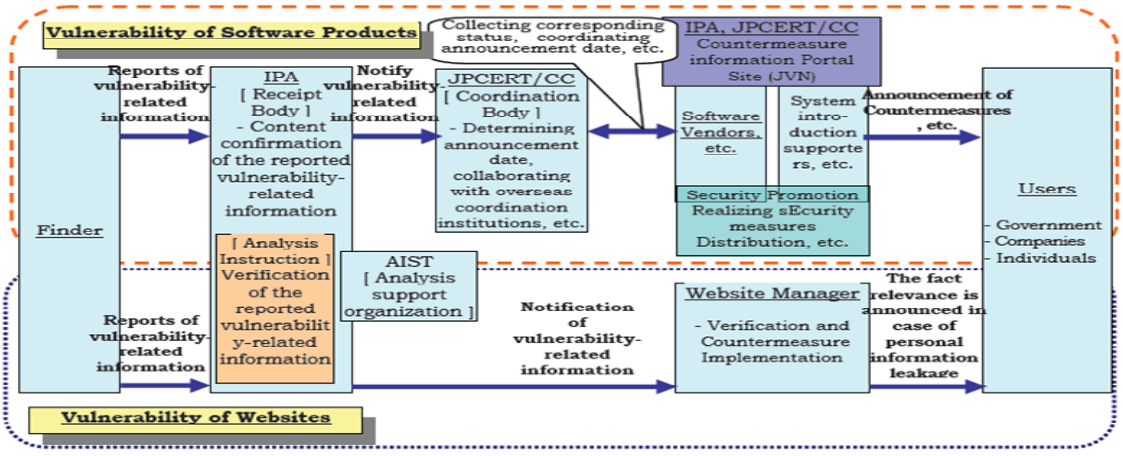
Software Vulnerability and Related Information

When you discover vulnerabilities in client software (ex. OS and browser), server software (ex. web server) and hardware embedded software (ex. printer and IC card) , please report to IPA.

Web Application Vulnerability and Related Information

When you discover vulnerabilities in systems that provide their customized services to the public, such as web sites, please report to IPA.

Framework for Handling Vulnerability-Related Information
～ Information Security Early Warning Partnership ～



JPCERT/CC: Japan Computer Emergency Response Team Coordination Center, AIST: National Institute of Advanced Industrial Science and technology

INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN
2-28-8 Honkomagome, Bunkyo-ku, Tokyo 113-6591 JAPAN
http:///www.ipa.go.jp/index-e.html

IT SECURITY CENTER
Tel: (0)3-5978-7527 FAX: (0)3-5978-7518
http://www.ipa.go.jp/security/index-e.html