Swedish Civil Contingencies Agency

Trend Report

– Information security in Sweden 2012

Trend Report

– Information security in Sweden 2012

Trend report – Information security in Sweden 2012

Swedish Civil Contingencies Agency (MSB)

Layout: Advant Produktionbyrå AB
Print: One Digitaltryck

Order No. MSB591 - September 2013
ISBN 978-91-7383-369-1

Foreword

Information handling and management are becoming ever more comprehensive and complex. The rapid pace of development in information technology allows for new and improved forms of information management, which in turn increase the quality of many services.

At the same time, technological development makes society more vulnerable to interruptions. Ever higher demands are made on the secure management of the growing volume of information about private individuals. Identifying and managing the risks that we face are challenges requiring joint action by all stakeholders in society.

Swedish Civil Contingencies Agency, MSB, is commissioned to support and coordinates information security efforts in Sweden, and with analyzing and assessing developments in the area. This work includes providing advice and support, of which the present report is a part.

Stockholm, 10 January 2013

Richard Oehme
Head of the Information Assurance Section

Summary

The present report provides an overall picture of the situation in the information and cyber-security area. It also provides an assessment of which areas are of particularly important to highlight. The content has been compiled on the basis of the analysis carried out at Swedish Civil Contingencies Agency, MSB, principally on developments during 2011 and 2012.

The developments described in the report paint a relatively mixed picture of the current situation in the information security field. Some trends are clear, however. Information management today is characterized by a high rate of change. Especially the combination of growing volumes of information, the rapid transition to centralized solutions, and increased mobility among users leads to a changing risk scenario, for individuals as well as organizations and society as a whole.

Social networking services are now part of everyday life for many people. The providers of these services store and have access to large amounts of user information and personal data, which are managed in accordance with agreements between provider and user. There is a risk, however, that this information is used in ways the user had not imagined.

Malicious code is a problem which has existed for some time but which to some extent today finds new forms as a result of increasing user mobility. Malicious code is a threat to all sectors of society, and over the past decade various forms of it have disrupted or disabled the operations of different stakeholders on a number of occasions.

Another challenge is crime that is more directly related to IT. This is a global phenomenon requiring crime-fighting agencies to adopt new methods and cooperate across borders. Businesses in the financial sector, among others, face considerable costs due to IT-related crimes. Moreover, the unrecorded side of this is likely to be very large.

Finally, it is possible today to see distinct risks connected with the increased integration and linking of industrial control systems with different communication networks and types of integrated systems. Since such systems are used in large numbers in critical infrastructure, e.g. electricity distribution and water supply, this is also an area with implications for security policy.

Content

Introduction

1. Introduction

The present report has been written to provide an accessible and comprehensive picture of the situation in the information security area. It also provides an assessment of what circumstances it is particularly important to highlight, and which may come to require measures primarily from the public administration side. The assessment is based mainly on developments during 2011 and 2012.

The trend report covers both national and international trends in the information and cyber-security area. Its contents have been compiled on the basis of formation security analysis carried out at Swedish Civil Contingencies Agency, MSB. Several different types of sources have been used: basic data from open sources, MSB's own incident monitoring, studies initiated following incidents, public documentation and interviews with different stakeholders.

IT developments and its consequences

2. IT developments and its consequences

Sweden is one of the world's leading IT nations, where over 90 per cent of the population has access to the internet.[1] The development and use of IT since the mid-1990s has created a number of new circumstances for communication, storage and extraction of data, as well as new standards and economic growth. Developments in IT have thereby created a series of new opportunities, while at the same time entailing several challenges.

Information management grows ever more extensive and complex. Very large amounts of data are being generated and stored today. In 2010, worldwide creation or copying of data amounted to just over 1 ZB.[2] This is equivalent to almost 150 GB – or just over 200 fully used CD-ROMs – per person in the world. The rate of increase is about 40 to 50 per cent per year.[3] Technological development has made it possible to store entire collections of documents on a small memory stick that fits easily into your pocket.

The storage networks that make up central data storage at today's IT service providers can, in turn, contain the total digital information from a large number of companies or government agencies. These developments create new possibilities, but they can also lead to undesired effects despite the most elaborate preventive security measures. A mislaid memory stick, for example, can turn out to contain sensitive information about hundreds of thousands of people. A more extensive IT disruption can lead to large volumes of data from completely different sectors of society suddenly becoming inaccessible.

The combination of increasing amounts of information, increased dependence on IT support in just about every sector of society, and a global tendency towards concentration in IT operations, has altered the risk scenario that all stakeholders have to adapt themselves to. In many cases, the information being managed is no longer even available on paper. Today the lion's share of information management is digital. As recently as at the turn of the millennium, most of it was still analogue.[4]

Add to this the fact that an ever growing share of the information is not sourced or processed locally. It comes from outside – or is stored at another location. Communication therefore also has a central role in our everyday lives, with the internet as its main channel. Functioning communications and IT support have become prerequisites for working ATMs and open shops. A part of society's communications furthermore needs to be protected against eavesdropping or corruption, which requires special measures.

Last but not least, IT development is closely linked to our dependence on electricity. Protection against and plans for dealing with power disruptions and outages therefore become an important part of the daily management of IT and data security.

Concentration and further centralized IT operations

3. Concentration and further centralized IT operations

A marked change in the information management area is the current gradual centralization of IT operations, as well as of various types of standardized information management services.

In the public sector, this is about everything from outsourcing fairly standardized functions such as personnel administration or travel services to dismantling significant sections of internal IT operations and transferring them to an external service provider.

Developments can be regarded as something of a return to the type of central data operations that was common in the 1970s and 80s. Over the last five or six years, technological development has led to considerable internal centralization by means of what are known as server consolidation and virtualization. This is now being followed by increased outsourcing.

There are many forms of outsourcing. A clear tendency is for businesses and other organizations to discontinue development and operations of their own systems and instead hire functions or services externally – variously termed web services, software-as-a-service (SaaS) or more recently, cloud services.

The fact that increasing numbers of organizations choose to outsource their IT operations or processes and store their data using cloud services leads unavoidably to a concentration of data management in the hands of a few actors. The idea is typically that the economics of scale thus achieved will contribute to a reduction in total client costs for IT operations.

It is possible that large-scale operations also can lead to an improvement in information security for many stakeholders. This applies in particular to small organizations who lack their own specialist competence, and for whom outsourcing thus provides access to the service provider's greater specialist competence. There is nevertheless a risk that information security becomes downgraded in everyday operations if explicit requirements for routines, controls and measures are not made already at the procurement stage.

A high degree of centralized IT operations also imply a concentration of risk. The Tieto incident at the end of 2011, which is described in this report, clearly illustrates the consequences of such a concentration in the event of an extended outage. Society's vulnerability increases

when large numbers of customers are simultaneously subject to an isolated outage. In its study of the society-wide consequences of this incident, MSB concluded that the public sector needs to have very clear requirements regarding information security in the procurement of IT operations.[5] Kammarkollegiet, among other government agencies, is currently involved in improving the conditions for procurement of IT operations from an information security perspective.

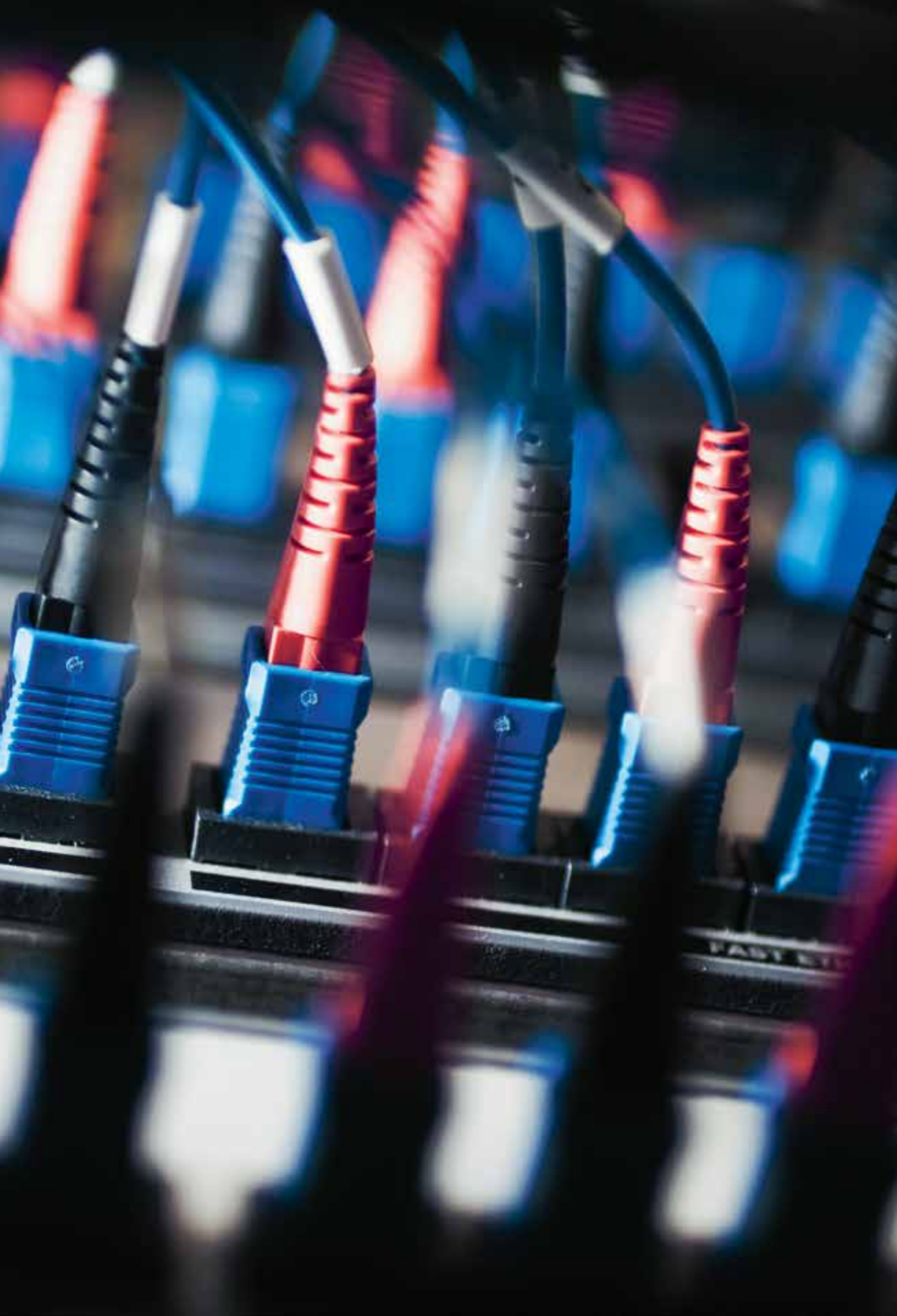
As outsourcing of IT services progresses, systematic data storage is also on the rise. Swedish government agencies, county councils and municipalities scan large numbers of documents which are then added in digital form to systems for administration or invoicing. In the healthcare sector, large medical records systems have been built which will soon be accessible to healthcare personnel wherever a patient requires care. More and more types of information are kept on record for a long time. These include credit card transactions, airline and train tickets, what items we purchase at the supermarket, and so on.

In some cases, e.g. at government agencies, data management is governed by clear regulatory frameworks or legislation; in other cases management is done more freely and on the basis of contract law.

In this environment, concepts such as "data mining"[6] and "big data"[7] have suddenly become hot topics. The art of finding and filtering the right information becomes valuable, as does the possibility of producing relevant information from other information (information derivatives).

Information we manage on a daily basis can be stored at other locations in the world, and often contains connections to many different information sources. Many of the services we use every day would stop working without such remote access to information. So far, society has only had time partially to adapt to this transformative characteristic of information, i.e. the possibility of making use of relationships between separate sets of information in increasingly sophisticated ways.

The European PSI (Public Sector Information) directive may become very significant in this context.[8] The directive deals with enhancing the re-use of public documents in electronic form. This could provide considerable scope for improving society's information supply, but could also imply risks if large amounts of information are compiled and analyzed for the purpose of surveying individuals or finding vulnerabilities in society.



Increasing mobility and mobile platforms

4. Increasing mobility and mobile platforms

The increase in mobile data communication is a global trend. In 2011, more smartphones than computers were sold worldwide.[9] According to one Google representative, 850,000 Android-based smart mobile terminals were being activated every day at the beginning of 2012, at which time the total number of activated such devices was 300 million.[10]

As in the rest of the world, developments in Sweden in recent years have been characterized by growing mobile information management. The first mobility wave, which placed digital mobile phones in the hands of a large proportion of the population in countries like Sweden just before the turn of the millennium, is now being followed by the rapid spread of smartphones and tablets. Over the past three to four years, a considerable share of Swedes has gained access to such handheld devices for data communication. These are devices that, in addition to voice calls and messaging, provide access to the internet and services such as email and web communication. The increased number of smartphones and tablets in the world has meant that they now also constitute an interesting target for developers of malicious code. There are several methods for infecting these devices. One is to use popular social networking services as channels for luring users to a website, where the user is then deceived into installing malicious code.[11]

Over the last few years a considerable share of internet traffic has moved from fixed to mobile network connections. One consequence of this is that accessibility in radio-borne segments of mobile networks risks becoming reduced, at least in the short term, as a result of extensive use of bandwidth-intensive services such as streaming video and services with extensive signaling.

It should be emphasized, however, that the greater proportion of total global data traffic is still transmitted via fixed connections (copper wire and fiber-optic cable), and that this situation is expected to continue.

Developments in the area of user mobility brings a new kind of risk exposure, when the equipment that was previously in the workplace now increasingly accompanies the user and risks being stolen or lost. Mobile devices, e.g. smartphones, tablets, memory sticks and similar, contain ever larger amounts of information but often lack the type of access protection developed for the equipment which is physically tied to the workplace.

In a way, these developments can be likened to the change that occurred a decade or so ago, when laptop computers became widespread and demands began to be made for information access outside of the fixed company networks. This is a challenge, as security measures can prove hard to uphold in an environment with equipment over which the information owner has no administrative control.

This weakness is becoming a problem today, as smartphones and tablets are increasingly being used for both personal and work purposes. Termed BYOD ("bring your own device"), this development has recently been pinpointed as one of the trends which will strongly influence IT over the next few years. To put it simply: when users are given access to work-related information via their personal mobile devices, protection of the business' information assets will depend on how good these users are at protecting themselves.

Allowing the use of personal smartphones for work can lead to a new type of risk exposure for organizations, in part because many applications today require a considerable level of access to the internal functions of the device. In order to be able to use the "app", the user generally has to allow such access.

The issue of using smartphones for work has been widely discussed within both government agencies and businesses over the past two years.[12]

Some organizations already protect their own mobile devices with both key locking and passwords as well as encryption and the possibility of remotely controlling the device and deleting all of its contents. Many larger organizations also acquire ready-made systems for the administration of mobile devices in large user populations.[13]

Identity management

5. Identity management

The possibility of certifying identity (authentication) is a fundamental requirement in modern information management and electronic communications. Technology in this area is now beginning to function in a satisfactory way. None the less, in many contexts simple passwords or PIN codes are still used to verify user identity or role, e.g. when logging in to a company network, for access to email accounts etc.

Access to and management of sensitive information – e.g. for carrying out transactions via internet banking – require better identity controls, however. These primarily use what is known as two-factor authentication, and are carried out with a smart card, an encryption device, or by having a unique password sent to the user's mobile.

Development in this area is moving ahead, and a growing number of big organizations use two-factor authentication for logins. In some areas of society and at some government agencies this infrastructure is well developed. This applies to the Swedish Police, the Tax Agency and the Social Insurance Agency, which all handle large amounts of integrity sensitive and confidential information.

In the healthcare sector smart cards for logins, abbreviated SITHS cards, have now been issued to nearly half a million users. This is an important step towards safeguarding access to information in systems such as the Nationell patientöversikt, NPÖ (The National Patient Overview) and the Medical Products Register.

Some institutions have long had electronic identification (e-identification) schemes for individual citizens, used for accessing internet banking services and public e-services. Developments in this area – the secure identification of individual citizens by electronic means – have been driven by the Tax Agency, among others. This has led to the use of e-identification by a relatively large share of the population. About 1.5 million people filed their tax returns in 2012 using e-identification, for example.[14] A large number also use the self-service functions available, e.g. for managing company matters vis-à-vis the Tax Agency and Companies Registration Office.

The Swedish Association of Local Authorities and Regions (abbreviated SKL in Swedish) has identified 38 typical e-services that municipalities furnish.[15] These are all different types of notifications and applications that a citizen may make via the municipality's website. In a survey of

municipalities by SKL, 82 per cent responded that they provide at least one of the 38 e-services specified in the survey, but it is likely that many municipalities in fact provide a large number of these services.

Still, it is clear that there are marked differences between municipalities in terms of security requirements for the authentication of citizens. Authentication solutions using e.g. Bank-ID are much more common in large municipalities than in small ones. Use decreases proportionally with municipality size. The tendency is the same for the prevalence of solutions for identification and authentication of companies and private providers.

Estimated only 16 per cent of the country's municipalities with fewer than 16,000 inhabitants have introduced or are about to introduce solutions for the identification and authentication of citizens.

The Swedish e-identification Board has been charged with promoting the further development of electronic identification. The Board's tasks include supporting and coordinating the public sector's need for secure methods of electronic identification and signatures, and these must be regarded as crucial requirements for the functional e-society from an information security perspective. Efforts are based on a decentralized model for linking together different private and public sector infra-structures for identification, referred to as the "federation model". It is expected that this model will be supplemented in 2013 with a system of free choice which, even in the short term, will open the market to new actors and service solutions.


286 711

Social networking services and privacy

6. Social networking services and privacy

Social networking services are widely used in society. Facebook is currently the dominant actor in the market, with more than 960 million users worldwide.[16] Today a large share of Sweden's population uses these services or similar ones.[17]

This intensive activity means that the providers of social networking services today store and have access to large amounts of user information, and a broad spectrum of personal data. This information is managed in accordance with agreements between provider and user. There is a risk, however, that this information will be used in ways the user had not imagined, which could have negative consequences for privacy among other things.

In order to address this issue and others, the European Commission proposed, early in 2012, a large-scale reform of EU rules on data protection with the aim of strengthening the protection of privacy on the internet.[18] Among other things, it proposed changes to the responsibility for conforming with security requirements when processing personal data.

The use of social networking services can be a challenge for the organization if, for example, public servants use social networks as private individuals in ways deemed not to be in keeping with regulatory frameworks and established practice. A number of such cases have been observed in recent years, e.g. when healthcare staff commented on or posted images of patients, or when a policeman wrote about an ongoing preliminary investigation on his blog. Existing regulatory frameworks such as the Public Access to Information and Secrecy Act, the provisions on libel in the Swedish Penal Code, and the Health and Medical Services Act can be applied to what and how a person may express themselves in social networking services. Additionally, the Data Inspection Board has provided guidelines both by means of general recommendations and in opinions on specific cases.

The big global providers of social networking services can, in certain situations, play a very important role as conveyors of information between individuals and organizations. For example, over the past year several municipalities have used services like Facebook and Twitter to communicate with their citizens on occasions when their own websites or telephone exchanges were not working. A large number of companies and government agencies also use Facebook as a complement to their website in order to communicate their messages to their respective target groups.[19]

In most cases it is a matter of an individual voluntarily using social networking services in his/her contacts with government agencies. The situation, although, changes, when a company or government agency makes services of this kind compulsory. These might be customer service functions or citizens' portals where, for example, users are urged to provide their personal data in order to receive better service in the healthcare sector. These cases require special consideration.

Privacy is also greatly affected by the growing concentration of personal data in government agencies' and companies' IT systems. Several countries have already passed laws about compulsory and public reporting of "data breaches", and have in some cases criminalized the subsequent spreading of data.[20] Over the last few years there have been reports of breaches involving large amounts of personal data in countries including the US[21], the UK[22], Israel[23] and Greece[24]. In Sweden in 2012, a case of data theft from a government agency subcontractor was investigated on the suspicion that large amounts of sensitive data from a population register had fallen into the wrong hands.[25]

The vast extent of computerized information exchange throughout society, not least within and between central government agencies and in the healthcare sector, has added to the increase in outsourcing of IT operations, which means that the risk of uncontrolled spreading of information is likely to remain high in the coming years.

Security in industrial control system and embedded systems

7. Security in industrial control systems and embedded systems

Data security is an area of concern not only for government agencies, businesses and other organizations that administrate large amounts of stored data, transaction systems, business systems or administrative processing systems. Over the past decade there has been increasing interest in data security-related risks connected with technology infrastructure and data management that directly affect e.g. traffic control, industrial production and electricity distribution. This is an area which has been collectively termed industrial data and control systems[26], or in some contexts SCADA systems.[27]

Such control systems are today present in larger technology infrastructures, where they e.g. control the transmission of electrical power, railway signaling and the regulation of our homes' central heating.

The vulnerability of industrial control systems to electronic and web attacks has long been well known among those who work with these systems. None the less, the risk of such undesired events has grown in recent years and will likely grow further over the coming decade. This development is concurrent with the increasing tendency to connect previously isolated systems or groups of systems to administrative support systems, for instance, and thereby also directly or indirectly to the internet.

The discovery of Stuxnet in the summer of 2010 was an event which launched a broad debate about vulnerabilities in industrial control systems. Stuxnet was a computer worm and appears to have been a targeted attack on control systems in an Iranian nuclear power facility. The worm became the first public example of an advanced and well planned attack against control systems in critical infrastructure. Stuxnet already has successors, and as the method of attack has been studied in depth among IT security specialists all over the world, there is reason to fear a gradual spread of similar attacks.

In some cases, attacks on control systems have severe consequences such as extended supply interruptions. This can be contrasted with the effects of accessibility attacks on websites, which are often temporary in nature and create attention rather than concrete or lasting damage.

The increased connection of modern control systems – everything from smaller systems for regulating household power consumption to large hydroelectric power plants – to the internet brings vulnerabilities which were not present previously. In Sweden we had an example of what can happen if such a control system becomes reachable from the outside when, at the end of 2010, someone breached security at a Swedish property company and changed the indoor temperature for an entire property complex.[28] There are similar examples from around the world.

About a year ago, it was revealed how a search engine now makes it possible to search for known vulnerabilities in industrial control systems. Researchers have also shown, via the same search engine, how it is possible to identify control systems which are connected to the internet and thereby may be vulnerable to attacks via the internet.

The reality that more and more control systems can now be accessed, directly or indirectly, via the internet has brought about a shift in risk. However, there are also other ways of reaching the control systems. Several suppliers are now making it possible to access, configure and debug systems via wireless network links (Wi-Fi or equivalent), which increases opportunities for attacking them. Moreover, many control systems were originally conceived to operate in complete isolation, and have then been further developed primarily to add functionality rather than ramp up security. This means that communication in many cases still uses plain text and is sent via simple terminal connections. This is a large and as yet insufficiently explored area of risks.

One area of technology which was still in its research stages only a few years ago is that of smart power grids, in which grid links and subscriber equipment can be read and controlled remotely. This new technology is partly a response to the need for improved control of the very fragmented electricity market in North America, but also in Europe in respect of environmental concerns. The ideas, however, have been developed into something much broader. This includes both large-scale load control and the possibility of individual adjustments at the subscriber level – as well as, eventually, of single electricity consumer appliances.

Today technology has been lifted straight out of laboratories, which has led to the large-scale installation of smart electricity meters that can be read remotely, or centrally by the electricity distributor. Such meters are now widespread among company and private subscribers in Sweden, and are expected to become increasingly advanced in the future.

In parallel with the development of smart grids, research is also being done about smart cities, which involves trying to install various types of information sources and sensors in the urban environment. This might

be about using the possibilities of building automation in new ways, or about connecting information systems in vehicles to street system information and traffic control – and, of course, linking the technology developed for an intelligent urban environment to the technology for smart grids.

Naturally, both of these areas will need to be studied from a data security perspective. There are still no standardized ways of communicating, collecting and delivering information across power grids or urban environments. But even if standards are established for this, the very complex job remains of guaranteeing the stability of the infrastructures involved, and ensuring that incorrect information does not lead to accidents. To a large extent, these technology areas are still at the research and development stage, which means that for stakeholders it is now primarily a question of continuing to support the research being carried out regarding security and stability in their application.

A related area is machine-to-machine (M2M) communication. This started to develop before the turn of the millennium, but has only begun to receive serious attention in the very recent past. Put simply, it is about providing equipment that already has embedded computing power with communication possibilities, e.g. to report usage, sales, operational status, geographical position and the like to the user, supplier or to a maintenance organization. This area, in which applications can be launched on a relatively small scale, is likely to have an impact much sooner than smart grids and smart cities, which involve and in fact are extensive infrastructures.

Security is important in M2M communication as well. If a car, a printer-copier or a goods dispenser is equipped with a GSM module that can warn the owner or repair services when, for example, maintenance is needed, then there is usually also a reverse link which can be used to connect with the appliance and possibly control or reprogram it.

This kind of technology is already being used today in alarm communication, e.g. with the security addition that when an alarm is triggered, a fixed or movable camera image from the property in question automatically comes online. Such an application obviously needs a mechanism for preventing unauthorized connections.

Machine communication appears to be a natural next phase in the development of the internet. Clearly, the security concerns this brings with it need be studied further. The examples referred to above moreover highlight the need to look at this new technology from a legal standpoint.

Malicious code and spam

8. Malicious code and spam

Malicious code (data viruses, worms, trojans and similar) can strike anywhere. For instance, over the past decade there have been repeated incidents in which malicious code has disabled operations throughout municipal administrations,. On some occasions, significant parts of the targeted municipality's IT support system were out of operation for a week or more.

In 2011, 403 million variants of malicious code were created, which was an increase of more than 40 per cent on 2010.[29] Trojans continue to be ever more common, while the number of worms and viruses is today growing smaller. In just over 60 per cent of infections by malicious code, the code is a trojan, while viruses and worms represent just under 8 per cent each of cases.[30]

Malicious code is often designed to be platform independent, and today more and more attacks are directed against web platforms and content management systems. One type of trojan which has become common is ransom ware. Hardware infected by ransom ware becomes unusable in the normal way by its owner/user until a ransom has been paid. One municipality, Skåne in southern Sweden, suffered such an attack in the spring of 2012.[31] Bank trojans are another variant of malicious code that has become common in the past year. It attacks the communication between the user and his/her internet bank.

The large sales increase of mobile devices has meant that smartphones and tablets are now attractive game for attackers. The number of known attacks grew sharply in 2012. The majority of these were directed against the Android platform.[32] In contrast with the types of malicious code directed against computers, those that infect smartphones can also be intended to track the user's position.

On average, just over a third of the world's computers with an internet connection are estimated to be infected by malicious code. That is just under 10 percentage fewer than in 2010. China continues to be the country with the highest rate of infection. The share of infected computers there is just over 54 per cent. This share is generally lower in Europe. In Pandalabs' study[33] of the first quarter of 2012, nine out of the ten countries with the lowest share of infected computers are European. Japan is the only non-European country on the list, and Sweden tops the list with less than 20 per cent of the computer population infected.

In Sweden the national IT incident facility at MSB, CERT-SE, has developed a service which allows users to see where in the country there are infected computers. Around 50,000 infected IP addresses per month is normal.[34]

The problem of spam is changing today. The total number of spam messages dropped by 34 per cent in 2011, while there was an increase in social spamming, or spamming done via social networks. From the hitherto highest figure, in August 2010, of 92 per cent of all email messages being spam, the share had dropped to just over 70 per cent in November 2011.[35] This reduction is regarded as being due to improved spam filters and to the fact that crime fighting agencies have succeeded in taking down several large botnets, in particular the world's biggest botnet for spam, Rustock.[36]

Instead spam has appeared in new forms on social networks such as Facebook and Twitter, where it is referred to as social spamming. The advantage for spammers in using social networks is that they can spread their messages via a chain of trusted sources and in an environment where the inclination for recipients to act in line with the perpetrator wants, increases.

Software vulnerabilities have become a strategic resource today. Previously unknown and unaddressed vulnerabilities (zero-day vulnerabilities) can now be produced by automation and on an industrial scale. That means the possibilities of making money from them increase, which in turn means that idealists and "amateur researchers" in the area are replaced by professional players with bigger resources and the intention of selling the vulnerabilities. Previously it was common practice to inform the manufacturer about vulnerability first, and give them the opportunity to correct it before the information was made public. The trend now, instead, is for vulnerabilities to be kept secret and be sold to clients with a criminal, commercial or security policy interest in having "private" back doors into an IT system. The once-extensive information exchange within the IT security community has already begun to diminish, to the detriment of those involved in building protection, analyzing and producing threat scenarios. The upshot is an "arms race" which it will become increasingly difficult to protect oneself against. Developments are expected to continue in this direction.

IT-related crime

9. IT-related crime

IT-related crime is a global phenomenon today. It is a challenge to both the state and to companies in sectors such as finance, whose costs can be severe. Traditional crime-fighting agencies around the world have had a difficult time learning to deal with growing IT-related crime. This has several causes, including differences in the burden of proof, nationally applicable legislation, and organizational structures.

An interesting consequence of this is that Microsoft today has its own "cybercrime unit" which works to support crime-fighting in the area. This unit is primarily focused on fighting malicious code and the abuse of children. Microsoft's IT crime unit has participated in taking down some botnets and bringing the criminal organizations behind them to justice. This work has been done in close collaboration with the FBI and the American courts, among other institutions. During an intervention at the end of March 2012, when a number of Zeus[37] botnets were taken down, Microsoft was also physically present and took part in the seizure.[38]

Even if most actors view the final outcome as positive, it seems reasonable to ask whether it is appropriate for private businesses to act as if they were a part of the justice system.

IT-related crime continues to make headlines, but at the same time it is difficult to give any definite answers about its overall scope and its actual costs to society. BAE Detica estimated that the cost of IT-related crime in the UK in 2010 was GBP 29 billion[39], Symantec calculated the global cost of copyright crime in 2011 at USD 250 billion, and the director of the US National Security Agency (NSA), Keith Alexander, claimed in 2011 that the global cost of IT-related crime is USD 1,000 billion annually.[40]

The British Ministry of Defence, expressing a certain scepticism about these estimates, appointed a research team from Cambridge University the task of analyzing the costs of IT-related crime. Its report, published in the summer of 2012, provides no unequivocal answer, instead highlighting the difficulties of categorizing and estimating the costs of IT-related crime.[41] These include the fact that the hidden numbers are considerable, that the costs of copyright crime are very hard to compute, and that it is unclear to what extent traditional crime should now be categorized as IT crime solely because it has "moved online".

The report does, however, point to the fact that the overwhelming majority of the costs come from what is known as traditional crime, in particular traditional crime that is now perpetrated with the help of IT. The first category includes the costs of various forms of card fraud, while the second includes tax fraud. Genuine IT-related crime – including different types of internet banking scams, phishing attacks, the use of malicious code and false anti-virus software – makes up a much smaller part of the cost, according to the report. The cost of copyright crime is not dealt with in the report.

The number of reported IT crimes in Sweden is growing. Preliminary figures from the Swedish National Council for Crime Prevention (BRÅ) indicate that 3,593 computer intrusions and 41 instances of data sabotage (as defined in Chapter 4, Section 9c of the Swedish Penal Code [1962:700]) were reported in 2011. That is an increase of 52 per cent on the previous year.

A comparison can be made with the situation in Norway, where a "hidden numbers study" in 2012[42] showed that in 2011 there were only 361 reported cases of computer intrusion, fraud, abuse of IT resources, information theft and the spreading of copyrighted material, while the true number of crimes of these kinds was estimated at almost 45,000.

Computer intrusions have also changed in character. Whereas they used to be mostly intrusions by employees at hospitals and the police, in the form of unauthorized consultations of records and registers, they now also include a growing number of reported intrusions against private individuals, e.g. in the form of hijacked email and Facebook accounts.[43]

It is also clear that IT developments in recent years have given the police in Sweden as well as in other countries a series of new tasks. Crimes such as computer intrusion, network fraud and internet libel require new investigation methods. Furthermore, criminal investigations today require the content analysis of vast amounts of IT hardware. This is a constantly growing workload, as the volume of data to be scrutinized grows and as certain categories of criminals use ever more advanced methods to conceal their activity.

In order to maintain the public's confidence in the justice system in this new criminal landscape, it is necessary for the entire crime investigating part of the legal chain to have access to the specialist competence and resources required. The frequently international character of these crimes furthermore means that greater international cooperation is needed in crime fighting. In this connection, however, important initiatives were taken in 2011 and 2012 at the European level, e.g. by setting up a special joint EU body for IT-related crime fighting (EC3) at Europol.

Examples of specific events

10. Examples of specific events

10.1 Certificate problems for SSL

The SSL security mechanism is used to encrypt communication between users and, for example, banking services, government agencies or online shops. SSL is thus an important component of security and basis for trust in e-commerce and other online transactions. Certificate issuers for SSL, and SSL itself, were subject to a series of different attacks in 2011. During the summer of 2011 it emerged that root certificates of the Dutch certificate authority DigiNotar had been compromised as a result of an intrusion, which in turn was due to inadequate routines and security awareness.

The intrusion was discovered after a user in Iran spotted an error when connecting to a Google service. It then turned out that a large number of internet domains had been affected by someone issuing false certificates in DigiNotar's name. These included well-known domains such as Google, yahoo and Skype (.com), as well as the web domains of several intelligence services.

DigiNotar issued certificates commercially, but was also responsible for issuing government agency certificates in the Netherlands. The IT intrusion therefore meant that Dutch government agencies' websites could no longer be trusted. The Dutch state chose not to revoke the certificates, in part because that could have caused unnecessary disruptions to certain services. The incident led to DigiNotar's bankruptcy and the subsequent takeover of the company by the Dutch state. The DigiNotar intrusion was perhaps the most publicized incident involving certificate authorities and SSL in 2011, but an attack also occurred on a partner of the certificate authorities Comodo and GlobalSign. At a security conference in September, two researchers demonstrated how their "concept tool", nicknamed BEAST (Browser Exploit Against SSL/TLS), made it possible to exploit vulnerabilities in the encryption used by SSL/TLS.[44]

Observations

It has long been known that the technology used to issue website certificates is sensitive. There are today just over 600 different companies that act as central certificate authorities, and there are risks associated with such a great diversity of certificates. Many experts already regard the Public key infrastructure (PKI) structure that is used as unreliable, as well as a dead end. If further false website certificates were to begin circulating in the near future, this would eventually reduce confidence in the data integrity of a large number of web services around the world that rely on SSL. Solutions are being devised, however. One of these is to transport certificates via the DNS domain system, a method in the process of being

standardized by the DNS-based Authentication of Named Entities, (DANE) working group at the Internet Engineering Task Force (IETF), a leading internet standardization body.

10.2 RSA – insecure security tokens

In mid-March 2011, the RSA security company wrote an open letter to its customers informing them that the company had been subject to a sophisticated IT attack. There was a risk that information which could potentially affect the security of RSA's product SecurID – used in authentication tokens for secure logins, for example – had been leaked from the company.[45] In particular the formulation that "some information is specifically related to RSA SecurID two-factor authentication products"[46] led to speculation about the magnitude of the intrusion.

RSA SecurID is a common security product with more than 30,000 customers around the world, a number of which in Sweden. The company's authentication tokens are frequently used in systems with stringent requirements for secure logins, or for users with extensive rights within a company network, e.g. network and system administrators.

The attack was carried out by means of a phishing email with the subject "2011 Recruitment Plan", sent to two different groups of employees.[47] When an employee subsequently clicked on the attached Excel sheet, a backdoor was installed. The attacker then installed an administration tool which enabled the remote control of machines and access to servers in RSA's network.

In order to compromise an RSA SecurID unit, an attacker needs to have access to information about the authentication token, user information and the victim's PIN codes. If the attacker does not have direct physical access to the token, he/she instead needs access to the information that is used to generate keys. One of the many questions that circulated in blogs and articles, and which remained unanswered, was whether the attacker had managed to steal this information during the attack.

In June 2011, RSA offered free security surveillance to all of its customers, or the replacement of all tokens.

Observations

The RSA intrusion is interesting in several ways. Not least, it demonstrates that targeted attacks and the method of duping users with appealing messages can succeed even in environments where extra

caution would be expected to prevail – such as in a security company. The attack also shows that IT attacks can affect an entire technological niche. Many of RSA's customers hurriedly had to work out supplementary or alternative login mechanisms when it emerged that one of the security industry's most established companies had got into trouble. Moreover, in many cases those affected turned out to be holders of key positions in their respective organisations.

10.3 Developments after Stuxnet

The big IT security incident in 2010 was Stuxnet, an advanced piece of malicious code which is assumed to have been developed with the goal of attacking industrial control systems in Iran.[48] Stuxnet was discovered during the summer of 2010 and led to intensive technical analysis and several reports from actors in the security industry over the following six months. The code is often described as an eye-opener in terms of what can actually be done, and particularly in relation to attacks on critical infrastructure, the industry began to refer to IT attacks and malicious code before and after Stuxnet. Among IT security experts there was speculation about what type of copycats and followers Stuxnet would have.

About a year later, in October 2011, a new piece of malicious code was discovered by a Hungarian research lab, and named Duqu. It contained elements that were almost identical to Stuxnet, which led many to assume that the developers behind Duqu had had access to the source code for Stuxnet. The aim of Duqu appeared to be quite different, however. While Stuxnet was self-replicating and carried a payload with which to attack carefully defined hardware, Duqu seemed designed to collect intelligence about what was assumed to be an unknown industrial control system. The discovery of Duqu reignited speculation about Stuxnet's aftermath.

Just over six months on, in May 2012, it happened again. Another piece of malicious code was discovered which appeared designed to collect information and which shared certain code segments with Stuxnet. It was denominated Flame, and differed in that it was much bigger than both Stuxnet and Duqu. Flame moreover spread in a new way: by posing as the updater for Windows.

A short time after the discovery of Flame, in June 2012, yet another piece of malicious code with similar characteristics appeared. It was christened Gauss. The most notable change was that Gauss contained encrypted parts, which has made analyzing the code more difficult. As a result, the aim of Gauss and how it was intended to work has not

yet been fully established. It also stole banking data and login data for social networks. The latter theft could indicate that the technology has now spread from actors with security policy motives to criminal ones. On the other hand Gauss spread mainly in the Middle East,[49] which could be interpreted as an indication that its purpose remains related to security policy.

Observations

The discovery of Stuxnet meant that the IT industry and the world as a whole were thoroughly awakened, during the autumn of 2010, to the reality that targeted threats against industrial control systems were not a possible development but a clear and present risk. The copycats and followers over the years that followed confirmed this picture. What these attacks have in common is that they were more or less targeted against specific system environments or geographical areas. The attacker also applied measures to prevent discovery of the malicious code, and in some cases to make analysis more difficult.

The concerns that attack methods and distribution mechanisms could be copied and thus contribute to the spread of similar attacks must today be regarded as having been confirmed. There is therefore reason to fear a continued spread of similar iterations of attack code. The size and complexity required, however, amount to a threshold level which may make it hard for smaller actors or single individuals to develop such code.

Stuxnet as well as its followers were detected during or after the spreading phase, at which point the code had been operative for varying lengths of time. Bearing in mind that the complexity of the code also required extensive underlying program development, it would be reasonable to assume that the projects had been initiated a long time before the malicious code was discovered.

A further characteristic of IT systems built to control physical processes is that the closer one gets to the control system environment itself, the fewer programming tools there are for detecting attacks or removing malicious code, for example.

While the anti-virus companies and other actors in the IT security industry have certainly drawn attention to this new family of risks, the supply of protective methods and tools still lags behind when compared with the personal computer environment.

10.4 Different forms of net activism

Over the last few years it has been made clear in several parts of the world how the internet can be used for new types of opinion making and net-based activism. For example, news about demonstrations and protests against authoritarian regimes can be spread via the internet the moment they happen. People can communicate and be mobilized quickly. Events during the Arab Spring of 2011 constitute some of the best examples of how the internet enables rapid news reporting under difficult conditions, a freer exchange of opinions, and how it in some places has facilitated the development of democracy.

However, net activism takes on different forms. The phenomenon of hacktivism, which involves computer intrusions and outright blocking attacks, has become a manifest feature of today's global internet environment. Critical infrastructure in Sweden has been subject to hacktivism on several occasions.

The threshold for participating in these actions has also been considerably lowered. Whereas fairly advanced knowledge used to be required to carry out attacks, today pre-packaged attack tools are available that just about anyone with an internet connection can use. Sometimes these tools are even delivered pre-configured to attack named targets.

Over the past two years, the loosely connected net activism movement Anonymous has repeatedly mobilized support for activities which have led, for example, to blocking attacks and the unsolicited publication of large amounts of information about or from the attacked party (what is known as "doxing"). Like several other net activism movements, Anonymous also played a small part in the Arab Spring by carrying out various types of net actions against the regimes in the countries where riots had broken out.

At around that time, however, the Anonymous movement broke up. Having previously been capable of mobilizing extensive support for a small number of large campaigns, it now splintered into countless groups and activities. Today the once fairly consolidated "non-movement" (anyone can become associated with Anonymous; the name itself represents a mass of nameless individuals on the move) appears not to have the same broad mobilization capacity as before. This may to some extent be connected with the fact that a number of identified activists have been prosecuted in the US, UK and Netherlands.

One of the biggest and most long-lived campaigns has been the one in support of Wikileaks and its founder, Julian Assange. The Swedish justice system was the target of that campaign in the late autumn of 2010, when Assange became a suspect in a Swedish criminal investigation.

Observations

From a society perspective, blocking attacks against government authorities and symbolically important stakeholders must be regarded as a recurring phenomenon which will probably become more frequent and extensive in the coming years. As recently as in early September 2012, for example, several blocking attacks were directed against Swedish government agencies, coinciding with a net activity in support of Julian Assange.

So far, the actions of net activists have usually caused limited damage. Consequences have been temporary inaccessibility of the victim's website and the accompanying damage to credibility. Over the last few years, the threshold for being able to carry out a blocking attack has also been lowered. Handling these tools no longer requires expert knowledge, and they are becoming increasingly widespread. These factors will make it possible for increasing numbers of individuals to stage this kind of protest attacks.

10.5 The Tieto incident

One of Sweden's major technical IT incidents in recent years occurred at the end of November 2011. A storage system at Tieto, an IT operations service provider, broke down, affecting around 50 customers including several municipalities and state-owned companies. This was not an antagonistic attack, but an operational disruption with technical causes. The consequences, however, were considerable. Among other things, prescription processing was halted for several days at numerous pharmacies around the country, and the Swedish Motor Vehicle Inspection Company suffered a complete stoppage of its production systems for close to a week. Two municipalities in the Stockholm region had extensive disruptions to their IT support which took several weeks to remedy, and a number of other municipalities around the country had problems with individual services.

Observations

In February 2012, MSB published a report about the incident[50] which notes, among other things, that the ongoing concentration of IT operations to a small number of large service providers increases the risk of this kind of incident happening. When a technical error occurs it can suddenly affect different sectors of society at the same time. The course of events during an incident of this kind is rapid – and it becomes increasingly difficult to get an overview of the consequences.

From a crisis management perspective it proved difficult during the Tieto incident to achieve a satisfactory picture of the situation, and to gain an overview of all the consequences of the event. This was partly because information about the service provider's customers and their operational status was handled with customary business secrecy, and partly because some of Tieto's customers appear to have been companies which in turn provided net-based services to other organizations.

Overall conclusions and assessment

11. Overall conclusions and assessment

The developments described above paint a relatively mixed picture of the current situation in the information and cyber-security field. Some trends are clear, however. Information management today is characterized by a high rate of change. Above all, it is the combination of growing volumes of information, the rapid transition to centralized solutions and increased mobility among users that means the risk scenario is changing, for individuals as well as organizations and society as a whole.

Information management is both extensive and complex, and its scope grows every year. Just about all sectors of society are permeated by a strong dependence on IT support. In addition, there is a rapid ongoing concentration of IT operations and data storage to locations often far removed from where the information was originally created.

Centralization of IT operations involves large-scale outsourcing and the use of standardized services from external providers. In Sweden this is particularly evident in healthcare and parts of public e-administration. This large scale can contribute to improving information security for many stakeholders, particularly among smaller organizations. There is, however, also a risk that inadequate solutions and vaguely formulated procurement specifications contribute to a deterioration of information security instead. Centralization can also lead to reduced redundancy in the system, and an increased risk of cascade effects in connection with disruptions.

When implementation is sourced outside of the organization, the requirements for well-conceived control and follow-up procedures have to be made more stringent than before, which in turn requires specialist competence. The absence of sufficiently effective control may, when the consequences accumulate, imply increased overall risk.

A characteristic of IT use in the world today is its constantly increasing degree of mobility. This also has consequences for information security. A particularly sensitive issue is the fact that many types of hardware give software of various kinds overly extensive access to the information stored. Often both private and work-related information is managed using the same hardware, which creates a challenge for organizations. The private and professional roles often prove difficult to separate, and there are a number of existing regulatory frameworks that impose requirements.

When personal equipment is given access to the information system at the workplace, the administrative control that previously existed often disappears in the process. If such access is to be allowed, clear guidelines are needed as well as an awareness of security concerns among users.

Another clear and global trend is the one towards ever more sophisticated and large-scale data collection and analysis. The extraction of data from the enormous volumes of information which are constantly being generated and altered in the world is something that is demanded not just by those who collected the information, but also by others and for completely different purposes than the original ones. Social media are an example of areas where information is often created for one purpose but then used for another. Government agency data is also an area where private actors are now beginning to "mine" public information.

From a public perspective, this data analysis is not unproblematic. In the case of government agencies' activities, the public interest must on the one hand be provided for, as must the possibility of further utilizing publicly administered information for commercial purposes. On the other hand, increased information storage and greater flow of information between systems must not mean that protection of citizens' personal data is undermined. Moreover there are protection concerns which apply to the possibilities that have been created for obtaining and analyzing, on a large scale, detailed information about critical infrastructure for example.

In several places around the world today, the possible consequences of IT-related disruptions to technological infrastructures are being highlighted. In recent years several incidents have also made it clear what can happen. Some related areas include smart grids, smart cities and machine-to-machine communication (M2M). Further research is needed here in respect of security aspects, as are studies into the need for new legislation.

Malicious code and spam continue to be a challenge. They are now spreading via new, "smart" mobile devices, as the incentive for attacks directed against these is also present. Traditional emailed spam is decreasing, while it is increasing in social media, where messages are spread via trusted sources. Operational disruptions and accessibility attacks caused by malicious code which has directly or indirectly made its way into the information systems of organizations and private individuals thus look set to continue.

Like malicious code and spam, IT-related crime is not a new phenomenon. The costs of IT-related crime impinge on both private companies and society as a whole through computer intrusions, information theft and

fraud. Unfortunately it has proven difficult to get a good picture of the scope of IT-related crime or of the real costs of it. What is perfectly clear is that the development of IT presents crime-fighting agencies with a major challenge.

Another major challenge is the work on security measures for various types of industrial control systems. These systems are used to control a series of critical infrastructures, from electricity distribution and water supply to traffic lights, hospital equipment and logistics centers. Antagonistic attacks on such systems can potentially cause very widespread damage. This area therefore also has a security policy dimension, which has been amply confirmed by the international cases it has been possible to study – the prime example being Stuxnet.

A particular phenomenon that has become evident over the last few years is a relatively widespread hacktivism, which on several occasions has received a lot of attention but which has not caused any broader damage from society's perspective. There are good reasons, however, to follow its further development closely, in order to learn above all about the operating procedures used. As with security policy motivated net attacks, such knowledge is a prerequisite for being able to deal with future incidents in which, for example, activism and IT crime may be mixed together – and where targets are no longer symbolic, with attacks instead occurring directly against critical infrastructure.

References

[1] It i människans tjänst – en digital agenda för Sverige. Regeringskansliet, oktober 2011. *http://www.regeringen.se/content/1/c6/17/72/56/-5a2560ce.pdf, 2012-11-01.*

[2] 1 zettabyte = 10^{21} bytes.

[3] IEEE Industry Connections Ethernet Bandwidth Assessment, IEEE 802.3 Ethernet Working Group, 19 July 2012, *http://www.ieee802.org/3/ad_hoc/bwa/BWA_Report.pdf, 2012-10-01.*

[4] The World's Technological Capacity to Store, Communicate, and Compute Information, Science 1 April 2011, Vol. 332 no. 6025 pp. 60-65, see also: *http://www.msnbc.msn.com/id/41516959/ns/technology_and_scienceinnovation/t/worlds-shift-analog-digital-nearly-complete/, 2012-10-01.*

[5] See MSB, Reflektioner kring samhällets skydd och beredskap vid allvarliga it-incidenter, 2012, *https://www.msb.se/RibData/Filer/pdf/-26170.pdf, 2012-10-01.*

[6] "Data mining" is the term used for the process of trying to find patterns in large volumes of data. This process is facilitated by specific software products for analysis.

[7] "Big data" is the term used for the enormous amounts of data generated on the internet. Big data is usually produced in real time and may originate from cameras, digital sensors etc., or be created on Twitter or Facebook, for example.

[8] Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information, or the PSI Directive. The directive was implemented into Swedish law on 1 July 2010 in the Act (2010:566) on the re-use of public administration documents.

[9] Canalys: 62.7% and IDC: 61.3% *http://mobithinking.com/blog/2011-handsetand-smartphone-sales-big-picture, 2012-10-01.*

[10] See Andy Rubin, Google+, 27 February 2012, *https://plus.google.com/u/0/112599748506977857728/posts/Btey7rJBaLF#112599748506977857728/posts/Btey7rJBaLF, 2012-10-01.*

[11] See AVG Community Powered Threat Report, Q1 2012, *http://aa-download.avg.com/filedir/news/AVG_Community_Powered_Threat_Report_Q1_2012.pdf, 2012-10-01.*

[12] See MSB, Vägledning för säkrare hantering av mobila enheter, 2012, *https://www.msb.se/en/Products--services/Publications/Publications-from-the-MSB/Vagledning-for-sakrare-hantering-av-mobila-enheter/, 2012-11-01.*

[13] A special product segment has emerged in this area: Mobile Device Management (MDM). See also Forbes magazine, Mobile Device Management Hits Center Stage, but Concerns Remain, *http://www.forbes.com/sites/tomkemp/2012/02/15/mobile-device-managementhits-center-stage-but-concerns-remain/, 2012-11-22*

[14] Rekordmånga e-deklarerade – smartphone växer snabbast, press release from the Swedish Tax Agency, 2012-05-08, *http://www.skatteverket.se/omskatteverket/press/pressmeddelanden/riks/2012/2012/rekordmangaedeklareradesmartphonevaxersnabbast.5.71004e4c133e23bf6db800078980.html*

[15] Sveriges kommuner och landsting, E-förvaltning och e-tjänster i Sveriges kommuner 2011. *http://brs.skl.se/brsbibl/kata_documents/doc40082_1.pdf, 2012-11-01.*

[16] *http://www.checkfacebook.com/, 2012-11-01.*

[17] See .SE, Svenskarna och internet 2012, Olle Findahl, *http://www.iis.se/docs/SOI2012.pdf, 2012-11-23*

[18] European Commission, proposal for the directive of the Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free flow of such data (general data protection directive). COM(2012) 11 final. 25 January 2012. *http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf, 2012-10-01.*

[19] According to a study by E-delegationen from 2010, 30 per cent of the agencies under the government used Facebook. *http://www.edelegationen.se/sites/default/files/imce/filer/publikationer/Enkatsvar_utdrag_ur_betankande.pdf, 2012-10-01.*

[20] See e.g. Information Commissioner's Office (UK), 2012-10-16, Police force pays £120,000 penalty for data breach, *http://www.ico.gov.uk/news/latest_news/2012/police-force-pays-120000-penalty-for-data-breach-16102012.aspx, 2012-11-30*

[21] The Huffington Post, 2012-09-19, 94 Million Exposed: The Government's Epic Fail on Privacy, *http://www.huffingtonpost.com/adamlevin/governmentdata-security_b_1897229.html, 2012-11-30*, see also Rapid7 Report: Data Breaches in the Government Sector, 2012-09-06, *http://www.rapid7.com/news-events/press-releases/2012/2012-federal-data-breach-report.jsp, 2012-11-30*, and Privacy Rights Clearinghouse, 2011-12-16, The Top Half Dozen Most Significant Data Breaches in 2011, *https://www.privacyrights.org/topdata-breach-list-2011, 2012-11-30*

[22] Help Net Security, 2012-09-30, UK data breaches up 1000% in five years, *http://www.net-security.org/secworld.php?id=13504, 2012-11-30*

[23] Jerusalem Post, 2012-05-13, Six indicted over Population Registry data theft, *http://www.jpost.com/NationalNews/Article.aspx?id=269728, 2012-11-30*

[24] Washington Post, 2012-11-20, Greek police arrest man on suspicion of theft of 9 million personal data files on Greeks, *http://www.washingtonpost.com/world/europe/greek-police-arrest-man-on-suspicion-oftheft-of-9-million-personal-data-files-on-greeks/2012/11/20/72dc5c64-331a-11e2-92f0-496af208bf23_story.html, 2012-11-30*

[25] Computer Sweden, 2012-03-29, Skatteverket hackat, *http://www. idg.se/2.1085/1.440750/skatteverket-hackat, 2012-11-30,* see also Computer Sweden, 2012-09-19, Logica-intrång kan ha pågått i flera år, *http://computersweden.idg.se/2.2683/1.466890, 2012-11-30*

[26] ICS stands for Industrial Control System.

[27] SCADA stands for Supervisory Control and Data Acquisition. The term is often used to describe control in a distributed environment, where monitoring and control of a large number of industrial control systems are brought together.

[28] Radio Sweden, Nyheter/Ekot, 700 hushåll utan värme efter hackerattack, *http://sverigesradio.se/sida/artikel.aspx?programid=160&artikel=4239787, 2012-11-01.*

[29] Symantec, Internet Security Threat Report, 2011 Trends, Volume 17, April 2012. *http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_2011_21239364.en-us.pdf, 2012-11-01.*

[30] PandaLabs Quarterly Report, January – March 2012, *http://press.pandasecurity.com/wp-content/uploads/2012/05/Quarterly-Report-PandaLabs-January-March-2012.pdf, 2012-10-01.*

[31] IDG.se, Nya hackartrenden: kidnappning, *http://www.idg.se/2.1085/1.443228/nya-hackartrenden-kidnappning, 2012-04-13.*

[32] McAfee Threats Report: Third Quarter 2012, *http://www.mynewsdesk.com/se/pressroom/mcafee/document/view/mcafee-threats-report-q3-2012-23141, 2012-11-01.*

[33] PandaLabs Quarterly Report, January – March 2012, *http://press.pandasecurity.com/wp-content/uploads/2012/05/Quarterly-Report-PandaLabs-January-March-2012.pdf, 2012-10-01.*

[34] See also *https://www.cert.se/megamap, 2012-11-22.*

[35] The Wall Street Journal, Spam Finds New Target, 4 January 2012, *http://online.wsj.com/article/SB10001424052970203686204577112942734977800.html, 2012-11-01.*

[36] In 2010, botnets were estimated to represent 88.2 per cent of spam traffic, while the figure was 81.2 per cent in 2011.

[38] Zeus is a botnet that reportedly controlled 13 million computers around the world. The computers in the Zeus botnet were used to send large volumes of spam, but also to steal money.

[39] Säkerhetsbloggen: CSI Redmond – Microsoft tar lagen i egna händer, *http://blog.eset.se/csi-redmond-microsoft-tar-lagen-i-egna-hander/, 2012-10-01;* F-Secure, Microsoft's Digital Crimes Unit Targets ZeuS.

http://www.f-secure.com/weblog/archives/00002337.html, 2012-11-22; Here's How Microsoft's Digital Crime Unit Is Taking Down Evil Spammers, *http://articles.businessinsider.com/2012-03-29/news/31253437_1_botnet-zeus-microsoft, 2012-11-22.*

[39] Bae Systems and Detica, Office of Cyber Security and Detica report estimates that the overall cost to the UK economy from cyber crime is £27 billion annually, 17 February 2011, *http://www.baesystemsdetica.com/news/office-of-cyber-security-and-detica-report-estimates-that-the-overall-cost/, 2012-11-01.*

[40] Does Cybercrime Really Cost $1 Trillion?, *http://www.propublica.org/article/does-cybercrime-really-cost-1-trillion, 2012-09-26*

[41] R. Anderson et al., Measuring the Cost of Cybercrime, 2012. *http://weis2012.econinfosec.org/papers/Anderson_WEIS2012.pdf, 2012-10-01.*

[42] Näringslivets sikkerhetsråd, Mørketallsundersøkelsen – Informasjonssikkerhet og datakriminalitet, 2012, *http://www.nsr-org.no/moerketall/, 2012-11-22*

[43] SVT.se, 12 December 2011, *http://svt.se/2.22620/1.2640303/dataintrangen_okar_kraftigt_i_landet, 2012-10-01.*

[44] Ekoparty Security Conference 8th edition. *http://ekoparty.org/eng/index.php, 2012-10-01.*

[45] CERT-SE, RSA drabbat av dataintrång, *http://www.cert.se/publikationer/namnvart/rsa-drabbat-av-dataintraang, 2012-10-01.*

[46] RSA, Open Letter to RSA Customers, *http://www.rsa.com/node.aspx?id=3872, 2012-10-01.*

[47] RSA, Anatomy of an Attack, 1 April 2011, *http://blogs.rsa.com/rivner/anatomy-of-an-attack/, 2012-10-01.*

[48] The malicious code appears to have been constructed to seek out and destroy parts of a processing plant for the enrichment of uranium, located in Natanz, Iran. See also Symantec, W32.Stuxnet Dossier, February 2011, *http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf, 2012-11-22;* New York Times, 2012-08-09, Times Topics: Cyberattacks on Iran – Stuxnet and Flame, *http://topics.nytimes.com/top/reference/timestopics/subjects/c/computer_malware/stuxnet/index.html, 2012-11-22;* and the line of reasoning in Sanger, David E. Confront and Conceal, 2012.

[49] Kaspersky Labs, Gauss: Abnormal distribution, (2012) *http://www.securelist.com/en/downloads/vlpdfs/kaspersky-lab-gauss.pdf, 2012-11-22*

[50] See MSB, Reflektioner kring samhällets skydd och beredskap vid allvarliga it-incidenter, 2012, *https://www.msb.se/RibData/Filer/pdf/26170.pdf, 2012-10-01.*

Swedish Civil Contingencies Agency (MSB)
SE-651 81 Karlstad Phone +46 (0)771-240 240 www.msb.se/en
Order No. MSB591 - September 2013 ISBN 978-91-7383-369-1