International Case Report On Cyber Security Incidents

Reflections on three cyber incidents in the Netherlands, Germany and Sweden

National Cyber Security Centre
Ministry of Security and Justice

Bundesamt
für Sicherheit in der
Informationstechnik

Swedish Civil
Contingencies
Agency

Preface

As cyber incidents are increasing worldwide, the protection of the functionality of IT systems, particularly if they are critical or vital to our societies, is high on the political agenda. Enhancing cybersecurity – both in the public and in the private sector – is of crucial importance for the future.

It has become a well cited truis, that these increasing threats do not stop at state borders. On the other hand, international co-operation in fighting against cyber-attacks and cyber-incidents appears to be in its infancy, compared to law enforcement efforts against physical crime.

Frequently, both the actual perception of IT or cyber incident and the initial response to it take place at a national level, either by private stakeholders or by state authorities. Hence, the editors of this study consider it worthwhile to share with our readers reflections and lessons learned of three cases from the Netherlands, Germany, and Sweden, which were dealt with mainly, but not exclusively, within these countries.The cyber incidents described, differ in scope, in the damage caused, and in many other aspects, but they have in common that their impact on society was considerable. Even though, on a technical level, these incidents were not very complex. Also, as a consequence of networks, these incidents escalated quickly, which put great emphasis on incident response. In two of the cases, the identities of the (possible) attackers have not as yet been revealed (in the Tieto case there was no attack) .

Hence, one lesson to be learned, as it were a priori, is that coping with cyber-attacks and cyber incidents always involves some degree of uncertainty. The publication of this case study, therefore, aims at providing transparency of past events as a starting point for preventive measures against future cyber threats. The report is a joint effort of three authorities: the National Cyber Security Centre (NCSC) in the Netherlands, the Bundesamt für Sicherheit in der Informationstechnik (BSI) in Germany, and the Swedish Civil Contingencies Agency (Myndigheten för samhällsskydd och beredskap, MSB).

Wilma van Dijk, *Director Cyber Security, Ministry of Security and Justice.*
Andreas Können, *Vicepresident, Federal Office for Information Security.*
Nils Svartz, *Deputy Director-General, Swedish Civil Contingencies Agency.*

Introduction

If we have learned one thing during the past decade, it is that cyber security is a complex affair. During this decade, we have seen many things go wrong in the digital domain. These incidents have left us much more experienced, but also a little confused. Where do we go from here? In this International Trend Report, three European national CERTs (Computer Emergency Response Teams) share some of their experiences of recent years by means of three case studies. The central theme for all cases is 'Trust': the need for it, and possibly the lack of it in the digital world. The Swedish national CERT, MSB, has contributed a case involving an availability disruption at IT operations provider Tieto. BSI, the German national CERT, describes the events during a DoS amplification attack on a major telecommunications provider in Germany. The contribution of the NCSC, the national CERT of the Netherlands, is a case on the DigiNotar crisis, which also had far-reaching international repercussions.

All three cases share certain characteristics. They all focus on the vital infrastructure of their country. They all affected not just one, but a whole network of organisations in their country. In each case, trust was lacking or was lowered after the incident. The Swedish case stands out because it focuses on non-intentional disturbance of vital infrastructure. The German case is about a deliberate attack to deny the availability of a telecommunications provider and the consequences of such an attack. The Dutch case, the hack of DigiNotar, was a deliberate act, but it probably was not the ultimatel goal of the attacker to hack into DigiNotar. The attacker used forged certificates from DigiNotar to eavesdrop on other citizens in different countries.

It is hard to reach an effective level of trust in the digital domain. By moving so many aspects of our lives to the digital realm, we automatically become potential victims of extensive data breaches at digital service providers. Assurance reports, Service Level Agreements and legal action can only do so much to reflect what is required from a digital service provider: that they perform at a level which deserves the trust their clients place in them.

We hope you will find benefit in reading this international publication which is the joint effort of the national CERTs of the participating countries. Let it be a reminder of known risks, and the medium for a message: that trust in the digital domain is not only hard to come by, but also crucial to its success.

The system of trust in security certificates based on the integrity of certificate authorities has shown to be flawed.

The DigiNotar case

Background

Even though the DigiNotar crisis was a cyber incident with an unprecedented impact on the Netherlands, it was not the first incident where the trust which organisations place in their providers was undermined by a security breach at one of these providers. Two examples:On 17 March 2011, RSA, a security company and provider of security tokens, announced that unknown parties had gained access to the company's network. Based on the limited information that RSA released, security researcher Steve Gibson concluded that it was clear that, at a minimum, a portion of the SecurID product (a two factor security token) was compromised. At the end of May 2011, three potentially related incidents were reported: at Lockheed Martin, at L2 and at Northrup Grumman, all American defence contractors. Although the reliability of the information available is difficult to assess, a link between these three incidents and the first attack against RSA seems extremely plausible.

A second incident took place at a business partner of Comodo, a provider of security certificates used for secure web communication. The hacker was able to obtain several fraudulent certificates and the corresponding keys from a Comodo partner. The certificates which were issued, included rogue certificates for Google, Microsoft, Yahoo and Mozilla web services. After some time, responsibility for the attack was claimed by an anonymous individual who claimed to have acted alone. Because these certificates allowed secure internet traffic for those web sites to be intercepted, the login data of millions of users of these services was at risk until the certificates were revoked.

In these examples, the security breach at a provider was a first step in successfully attacking targets which depended on this provider for their security.

The DigiNotar crisis

On 27 August 2011, an Iranian internet user received an invalid certificate warning from his browser when he visited the Gmail website. He reported this incident to Google. The certificate was generated on 10 July 2011. During the following weeks, it became clear that the fraudulent certificate was issued by DigiNotar, a Dutch security certificate provider, after a successful break-in into their servers.

The important role which DigiNotar fulfils in the Netherlands is threefold. First, DigiNotar is one of the security certificate providers for the Dutch government. Second, DigiNotar is an issuer of certificates for the Dutch national PKI (PKIoverheid). Third, DigiNotar issues certificates for qualified signatures. The framework for qualified signatures is an endeavour by the European Union to attach greater legal value to digital signatures. It gradually became clear that all three of these systems had been compromised during the break-in. This implied that trust could no longer be placed in the confidentiality or integrity of data or communications which had been secured with a DigiNotar certificate.

Response

When DigiNotar initially noticed the break-in into their systems, they decided to keep it a secret from the general public and the authorities. In the Netherlands, there was no explicit legal provision which required them to report such an incident. However, judging from the consequences of keeping this incident secret, this course of action was probably not in the publics best interest.

The Dutch government communicated extensively about the events at DigiNotar. However, the message varied greatly over time as more information about the break-in became clear. The PKIoverheid certificates serve as an example: as there was no initial indication that the certificate signing process for these certificates had been

Timeline of events (2011)

17 June
Initial breach of DigiNotar systems.

17 June – 1 July
Attackers use their access to the demilitarised zone (DMZ) to break through to the internal network.

10 July
First rogue certificate is signed with the access gained.

10 – 22 July
Attackers gain access to all certificate signing systems of DigiNotar and sign at least 531 rogue certificates for at least 53 different internet domains.

22 July
After discovering the attack, DigiNotar initiates an investigation into the events. They decide to keep silent about the break-in.

27 July – 27 August
Rogue certificates signed by DigiNotar are used in man-in-the-middle attacks in Iran. Such an attack is used in order to listen in on and possibly modify the communications of users of Google services such as Gmail. For Google services alone, at least 300,000 distinct users were confronted with fraudulent certificates.

27 August
An Iranian internet user who attempts to access Gmail notices that a rogue certificate has been provided. He notifies Google.

compromised, the government organisation Logius published a statement which declared that PKIoverheid certificates could still be trusted.

Once GovCERT[1] had been notified, they were in charge of handling the incident. When it became clear, a week later, that PKIoverheid certificates could also not be trusted, a full crisis management plan was initiated. The Dutch crisis management structure ('national crisis structure') was activated in accordance with existing procedures. The IRB (ICT Response Board)[2] is an advisor to the crisis organisation in case of a crisis involving an IT component. The IRB convened twice, which helped to gain a quick insight into the impact of revoking trust in DigiNotar certificates. Many parties cooperated in the crisis management. Some examples are the Dutch national police, public prosecutor, ministry of the interior, ministry of security and justice and IT security company Fox-IT.

Internally, the Dutch government investigated which processes depended on DigiNotar certificates for security or confidentiality of their communications. The filing system for tax returns was but one of these processes.

[1] Since January 2012 GovCERT has been included within the National Cyber Security Centre (NCSC).

[2] The IRB is a private public advisory board, which advises the national crisis structure about the situation and about the measures to be taken (including the impact).

29 August
Mozilla also discovers attack. GovCERT, the Dutch national computer emergency response team is notified of the attack by CERT-BUND, their German equivalent. DigiNotar publicly admits having been hacked.

1 September
Dutch governmental organisation Logius circulates an email message in which it asks other government bodies what the impact would be of revoking DigiNotar certificates.

3 September
Dutch government officially renounces DigiNotar as a trustworthy certificate provider.

6 September
At the explicit request of the Dutch government, Microsoft decides to postpone – only in the Netherlands – the update which will remove all support for DigiNotar certificates.

14 September
Dutch telecommunications authority OPTA announces that it revokes the licence of DigiNotar to issue certificates for qualified signatures. 300 Dutch government websites still use DigiNotar certificates to encrypt communications.

Revoking all DigiNotar certificates would disrupt many critical services which the government provides, as well as disrupting many interdepartmental communication channels. Also, it was unclear exactly what the impact would be of revoking DigiNotar certificates: there was only very limited knowledge about where DigiNotar certificates were being used. Even organisations which knew that they were using DigiNotar certificates could not say what the impact of revoking them would be on their business processes. A Dutch newspaper noted that abruptly revoking DigiNotar certificates would lead to a 'government blackout'. Microsoft agreed to postpone their update which would revoke these certificates in order to allow for one more week of repairs.

Final remarks

After the DigiNotar crisis, two measures were proposed:

- A legal obligation to notify a central authority of any significant data leaks or break-ins within an organisation. For providers of qualified certificates, such an obligation has since been introduced. In the case of DigiNotar, this would have led to an earlier awareness and understanding of the extent of the problems.
- The creation of a department of digital firefighters, which could act on behalf of the Dutch government in order to resolve a cybersecurity incident or crisis. Many proposed formats for this closely matched the role which GovCERT already had within the government. A discussion point within this concept was whether the government should have the power to take over IT operations and exercise it in case of a cyber crisis in order to protect the public interest.

Six days after the OPTA revoked DigiNotar's licence to issue qualified certificates, the company went bankrupt. Most of its property was auctioned off, but the hardware used to protect the private keys of the revoked certificates is still kept locked away. The original expiry date of the root certificates has not yet passed, which means it is possible some software still accepts certificates issued by DigiNotar. After this expiry date, the DigiNotar incident will be over.

The DigiNotar case has been evaluated extensively within all levels of the Dutch government. Some important conclusions can be made:

- Apparently, the certificate authority/PKI system is part of the critical infrastructure of a country. The DigiNotar case motivates one to re-evaluate whether his or her perception of what constitutes the 'critical infrastructure' of a country is both correct and complete. Also, in what way does any compromise involving such trust providers have a significant impact on the physical world?
- In cybersecurity, the effectiveness of the measures taken by a provider greatly affect the security stance of its clients. On the other hand, the insight and influence clients have over the security measures taken by their provider is very limited. This means that there will always be a residual risk associated with cooperating with providers of any kind.

Any lack of security at a provider which is responsible for trust-related services has an even higher impact. The security measures taken at DigiNotar were regularly evaluated by an external auditor. It is possible that if this audit had been performed differently or more in-depth, either the actual breach, or the vulnerabilities which allowed for it, would have been noticed. This leads one to ask whether the depth at which these audits are currently performed is suitable for a system where the integrity of every component is of such great significance.

- The system of trust in security certificates based on the integrity of certificate authorities (CAs) has been shown to be flawed. Every CA can testify to the authenticity of certificates for every domain. As such, a breach at a minor CA in the Netherlands can compromise the communications of Iranian citizens with US-based corporations such as Google. Several improvements to the CA system which have been proposed are:
  - using a web of trust-like structures (as is used in PGP);
  - including SSL key information in DNSSEC records (DANE);
  - convergence (an external authority which attests to the validity of certificates based on observations around the world).

It is unclear who has the power to initiate such a transition to a new and more secure system. Until such a transition occurs, we will see similar attacks occur regularly.

Since the internet is a worldwide network, it is necessary to establish national and international contacts and well-defined contact points between ISPs, but also between governmental agencies.

A Cyber-Attack on Deutsche Telekom

Background

A denial-of-service (DoS) attack is an attempt to make a machine or network resource unavailable to its intended users. There are different types of DoS attacks. One common method of attack on the internet involves saturating the target machine with external communications requests, so much so that it cannot respond to legitimate traffic or responds so slowly as to be rendered essentially unavailable. When multiple systems flood the bandwidth or resources of a targeted system the attack is called distributed denial-of-service (DDoS).[3]

DDoS attacks are very common on the internet. BSI is aware of about 1,800 DDoS attacks in Germany during the first half of 2013. It means that on average at least ten DDoS attacks are carried out daily. The real figure is probably much higher. Worldwide, several companies report that they observe thousands of DDoS attacks per day. On average, an attack lasts less than one hour. But in some cases it can last for several days or even months.

Statistics show that the main targets of DoS attacks are governments, banks, and e-commerce companies. Often adversaries attack a victim's web-server to disrupt its internet presence. But in some cases, other services, such as the Domain Name System[4] (DNS), are targeted as well.

There are different motivations for DoS attacks, e.g. political and ideological motives, competition, extortion. Adversaries can be government agencies, state-sponsored or patriotic hackers, hacktivists, or criminals. Some examples for adversaries and their DDoS attacks in the recent past are:

[3] For more information, see e.g. http://en.wikipedia.org/wiki/Denial-of-service_attack

[4] The DNS is a distributed system for computers, services, or any resource connected to the Internet or a private network. It associates a variety of information with domain names assigned to each of the participating entities. Most prominently, it translates easily memorised domain names to the numerical IP addresses needed for the purpose of locating computer services and devices worldwide. An oft-used analogy to explain the Domain Name System is that it serves as the phone book for the Internet by translating human-friendly computer hostnames into IP addresses. For more information, see e.g. http://en.wikipedia.org/wiki/Dns

- The international network of activists called Anonymous which has carried out many DDoS attacks against various entities (governments, organisations, companies) in order to protest against their activities.
- Patriotic hackers who attack organisations and companies of a foreign state during political conflicts. This was seen, for example, in conflicts between China and Japan, Israel and Palestine, Russia and Georgia, and so on.
- Criminals who have carried out a massive DDoS attack against an anti-spam organisation: The Spamhaus Project. During this attack, up to 300 gigabits per second of DoS traffic were experienced.

In some cases, however, as in an attack against Deutsche Telekom, neither the adversaries nor their motivation for an attack are known.

DoS attacks lead to direct and indirect costs for the victim. They cause costs for DDoS mitigation, direct revenue losses for e-commerce companies, reputational and brand damage, and customer turnover. Studies and surveys suggest that an hour of DDoS attack can cost a victim tens of thousands of euros. Attacks against critical infrastructure of a state can even disrupt its supply of essential goods and services to its population.

Timeline of events (2012)

03.09 12: 16:00
Attack started, outage of Deutsche Telekom's reverse DNS

03.09.12: 17:30
Attack mitigated by facilitation of DDoS Defence tooling, reverse DNS again up and running

03.09.12: 18:00
Attackers modify packet structure to adapt to Deutsche Telekom's countermeasures. Reverse DNS down again.

03.09.12: 18:30
Attack mitigated by reconfiguration of DDoS Defence tooling, reverse DNS up and running

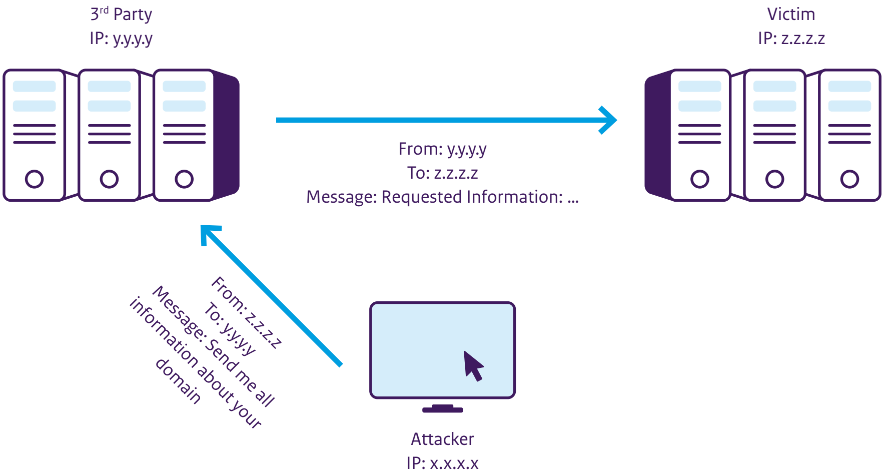
04.09.12: 00:00
Attack traffic stopped

05.09.12
Deutsche Telekom informs BSI about attacks

05.09.12: 14:15
New attack against reverse DNS, no DNS outages because DDoS Defence Tools still engaged

Incident

In September 2012 Deutsche Telekom AG, a large German internet service provider (ISP), was attacked by unknown adversaries. The Denial-of-Service attack was an attempt to block the Domain Name System of the provider. From a practical viewpoint, an outage of the DNS would cause an outage of the internet for most customers of that provider. The telecommunication and internet belongs to the critical infrastructure of a country. Its outage could have significant adverse effects on that country.



DNS reflection / DNS amplification attack

05:09.12: 16:00

Contact to web hosting provider with take down request for the attacking system IP addresses

05.09.12: 17:00

Deutsche Telekom asks BSI for emergency point of contact at web hosting provider

05.09.12: 22:00

New attacks against reverse DNS, no DNS outages because DDoS Defence Tools still engaged

07.09.12

Contact to German Federal Crime Office

13.09.12

Deutsche Telekom files formal criminal complaint to Public Prosecution Service

17.09.12

DDoS Defence mitigation measures closed down.

For this attack, the adversary used the server infrastructure of another web hosting provider. Although the attack vector is not completely clear, most probably the attacker used a technique known as DNS reflection or DNS amplification. It involves sending short queries with a spoofed source IP address – in this case the addresses of DNS servers of the ISP – to the DNS servers of a third party – in this case the web hosting provider – in order to trigger long responses to be sent by those servers to the victim's IP address within a short time window. The DNS protocol allows an amplification factor up to 100.

The motivation for the attack is unclear. The attacker made no demands to Deutsche Telekom. No information claiming responsibility for the attack was published. A possible explanation could be a "proof of concept" or test by which the attackers try out their capabilities, infrastructure and tools to carry out that kind of attack.

Response

Abuse messages sent to the web hosting provider to stop the attack were unsuccessful. After a short delay the ISP was able to mitigate the attack by redirecting the malicious traffic (see Timeline of events, above). The mitigation was possible, since the ISP possessed the necessary equipment and skills to monitor and mitigate such attacks and its network capacity was high enough not to collapse under the heavy traffic.

CERT-Bund was informed by Deutsche Telekom about the attack and helped it with the analysis. While the attack against a provider's infrastructure which provides services to the broad population was new, the attack method itself was already known. Since benign DNS queries need to be answered only once, repeated DNS queries were blocked by the mitigation systems of Deutsche Telekom.

Also, the Federal Criminal Police Office was involved in the investigation of the attack infrastructure. However, at first, it was not clear whether it was responsible in this case. It started to act after the Telekom provided additional information about the attack and it was recognised that the attack was targeting a critical infrastructure.

Final Remarks

For providers of Domain Name Services there are different technical advisories for strengthening their own DNS servers in such a way that they cannot be misused for this kind of attack. The DNS provider should be made aware of the threat and be forced to implement the necessary counter measures. The problem here is that this should be done by every single provider worldwide.

Possible victims should implement the necessary processes for detecting and mitigating such attacks in advance. The mitigation can be done directly by the victim using appropriate anti-DoS appliances offered by various manufacturers. Alternatively, the DoS mitigation can be used as a service offered by different providers.

Since the internet is a worldwide network, it is necessary to establish national and international contacts and well-defined contact points between ISPs, but also between governmental agencies (law enforcement, governmental CERT's) which can help to stop an ongoing attack in case the attacker does not respond to direct requests. In a federal state – such as Germany – it should also be clarified what agency (federal, state, communal...) is responsible if an attacker needs to be stopped.

The internet is a critical infrastructure. Its availability is essential for the functioning of a society and economy. Its outage can cause serious negative effects on almost all areas of life and can even inflict real damage in the physical world. Therefore, its protection should be an important goal for governments in every country.

Although the attack technique has been known for quite some time, its recent use for launching DoS attacks of unprecedented scale has brought renewed interest in it. Similar attacks are carried out against victims worldwide. A recent attack which made it into the headlines was a DoS attack on the anti-spam organisation, The Spamhaus Project, in March 2013.

The usage of internet servers – here DNS servers, in other cases also web, email, etc. servers – instead of home PCs enables the attacker to generate higher network traffic, since the internet connection of any such server is much faster than the connection of a typical private PC. This threat changes the general situation and demands immediate action for implementing appropriate counter measures.

The analysis that followed the event was able to establish that several of the affected parties did not have enough knowledge about their own dependencies.

The disruption at the IT service provider Tieto

Background

New technology and new business solutions have allowed a concentration of information, services, communication and IT operations in society. In the Swedish public sector, the trend towards concentration and integration has been strengthened through a number of initiatives such as the eGovernment Delegation, National eHealth, the Government service authority, as well as the framework agreements that the Legal, Financial and Administrative Services Agency has signed with major partners. The change in forms of delivery of IT services is seen as a way to both increase quality and reduce business costs.

An account of the disruption at the IT service provider Tieto in late 2011 is given below. The disruption affected both public and private organisations, and was debated both in the specialist press and in the general media. A similar event occurred in Sweden on New Year's Eve (January 1, 2014) as a fire in the server room of one of the Stockholm facilities of the IT service provider Evry caused considerable problems for the Stockholm metro, for railway traffic, and for postal and logistic services, among others. The fire extinguishing system was empty due to a human error. No one had restored (re-loaded) the system after a minor incident the day before. The fire resulted in a loss of power, and data storage systems had to be re-started. During the re-start, a software failure complicated matters, and Evry was not able to re-deploy several IT services. This incident started a chain reaction with implications for the whole society.

The disruptions at Tieto and Evry emphasise an already known circumstance, namely that increased concentration and integration create a new category of vulnerability where technical and human errors can shut down a number of societal functions over vast geographical areas in a short period of time. A disruption at a large IT service supplier can affect an entire society and the consequences can be considerable. Modern society is becoming more and more vulnerable when IT systems become unavailable.

The Tieto incident

On Friday, 25 November 2011, a hardware error occurred at IT service provider Tieto. A central part of a large data storage system at a facility in Stockholm suffered an emergency shutdown. First, an important key component of the system was lost. At that moment, it would still have been possible to fall back on a backup system that was on stand-by and ready to take over. However, after a short while the backup system malfunctioned as well, thereby rendering data storage for the connected server systems non-functional.

The exact details of what happened have not been made public by Tieto, but data storage for a large number of servers was suspended in a very short period of time. The disruption affected about 50 of Tieto's customers, including companies, governmental agencies and municipalities. Exactly which clients were affected by the disruption has still not been made public by Tieto. For some organisations, IT support nearly came to a complete halt, while other organisations experienced disruptions of specific services. In addition, several service suppliers seem to have been connected to the storage system, including companies that deliver web-based tools for administration, travel management and similar services. There were reports from several municipalities across the country about malfunctioning administration of financial services and pension services following the disruption at Tieto.

Timeline of events (2011)

25 November

A hardware error occurs at IT operations provider Tieto on Friday afternoon. A central part of a large data storage system at a facility in Stockholm suffers an emergency shutdown. For some of the approximate 50 affected organisations (Tieto's customers), IT support comes to a near-complete halt, while other organisations experience disruptions to specific services.

26-27 November

Tieto does not publicly acknowledge that it is experiencing operational problems caused by a hardware malfunction until Sunday afternoon, 27 November. The actual hardware error takes two days to correct. However, the customers' information, i.e. the data stored in the storage system, cannot be restored simply by replacing a single component of the technical equipment because the hardware problem causes a chain reaction of incidents that result in a complex and time-consuming restoration process. Therefore, it takes a considerably longer time for customers to restore saved data to the same state as before the disruption.

28 November

Early Monday morning, the mass media and the public have started to understand the widespread impact of the disruption. The disruptions are not limited to the capital Stockholm and the municipalities in the surrounding area. There are reports of problems caused by the disruption from several municipalities around the country.

29 November

Media attention is growing and additional reports on affected organisations are made public.

It is difficult to provide an exact account of the direct impact of the breakdown, such as the number of IT services or servers that went down. However, it is possible to get an approximate idea of the extent based on the outsourcing contracts between Tieto and some of the affected organisations. The storage system crash resulted in the malfunction of a large number of servers, or virtual servers, over a short period of time. Moreover, the effects were not limited to the systems operated by Tieto. The company also sold automated operational monitoring of customer servers. As a result, several Tieto customers quickly noticed that they no longer had any control over the status of their own servers. This meant that they had to move quickly to manual monitoring, which resulted in a significant amount of extra work.

30 November

Tieto has managed to restore operations at all of the 350 affected pharmacies across the country (about 50 % of the pharmacies are back in operation on Monday evening). The pharmacies lost contact with their IT systems and were unable to dispense prescribed medicines in accordance with normal procedures. Prescriptions were administered manually, and in some cases older IT systems were re-installed. The loan operations of the Government-owned mortgage lender SBAB are also fully restored.

1 December

The City of Stockholm concludes that there are no lingering effects of the disruption.

5 December

The 180 control stations of the motor-vehicle inspection company Bilprovningen once again have IT support. Bilprovningen inspects around 20,000 vehicles per day across the country, and the loss of IT services slows down the inspection process and leads to extra costs. One notable consequence is that the automatic reporting of all approved inspections normally made to the Swedish Transport Agency is halted. This, in turn, triggers a driving ban on many vehicles.

4 January, 2012

Nacka Municipality is able to announce that all computer systems are up and running again. However, there is still a lot of catching up to do and the municipality has identified lost data.

Response

The Tieto company solved the technical error in about two days. The major challenge for the company, however, was to restore the data and re-deploy IT services. This was a complex problem that took several weeks in some cases.

This section focuses on responses related to the consequences of the disruption. Many of the affected organisations had to resort to manual routines while Tieto was working on restoring their IT services. This halted some processes, and slowed down others considerably, due mainly to lack of personnel. Some organisations had frameworks and plans for dealing with the loss of IT services; others had to solve the problems as they emerged. A few organisations resorted to using old IT systems – systems that still existed, or could be re-installed. There was also an example of a public organisation that used Twitter and Facebook to communicate with people when their website and email systems were down.

The Swedish Civil Contingencies Agency (MSB) started working on the event, formally, on the morning of the 28th of November 2011. Regular meetings were held through the Agency's National Cybersecurity Coordination Function. Obtaining situational awareness was the most important part of that work. In addition to this, MSB published information on the Agency's websites, including the national crisis portal which is the responsibility of the Agency. On Tuesday, November 29, MSB completed an impact analysis and concluded that no critical societal functions were affected in such a way that would seriously threaten the functioning of society. This was followed by a status report to the Swedish Ministry of Defence. MSB followed the progression of events through open sources, its own contact networks, and contacts with affected parties as well as with Tieto. The Agency quickly contacted Tieto, as well as many of the affected organisations. However, it was difficult to gain a complete understanding of the situation through these channels from the perspective of societal considerations as regards the widespread effects of the disruption. Therefore, a request was drawn up on 6 December for the majority of agencies specifically indicated in the Emergency Management and Heightened Alert Ordinance (2006:942) to submit a situation report to the MSB regarding the disruption at Tieto. In summary, however, it can be concluded that the MSB had difficulty in quickly forming a comprehensive picture of how the event was affecting Swedish society. There is still no single party with a complete picture of the societal impact. In February 2012, the Agency submitted a formal report on the event to the Swedish Ministry of Defence.

Final remarks

It is difficult to assess fully the negative societal consequences of the disruption at Tieto. For some organisations, IT services were unavailable for weeks, while others only suffered minor problems. Apart from IT services becoming unavailable, there were also some cases of data losses. In terms of financial cost, it is even more difficult to estimate the consequences. It has not been possible to analyse the total cost, but, as an example, one of the affected municipalities (with approximately 100,000 inhabitants) estimated that their direct costs caused by the shutdown were at least SEK 7.5 million (circa EUR 850,000). It is very difficult to assess the costs that are related to loss of reputation. For the public sector organisations, it is also important to notice that even if an organisation has outsourced its IT operations, the organisation is still accountable to the public.

The Swedish Civil Contingencies Agency (MSB) did not activate the national IT response plan during the Tieto disruption. The consequences of the disruption at Tieto cannot be considered a social emergency. However, the disruption clearly had serious negative consequences for individuals and organisations, meaning that the event was very serious.

The analysis that followed the event was able to establish that several of the affected parties did not have enough knowledge about their own dependencies, nor about their need for cooperation. Had the disruption led to more extensive social problems, the MSB would have had trouble coordinating the relief work and alleviating the effects of the incident, as well as creating a satisfactory basis for collaboration. The affected organisations (Tieto's customers), have a great responsibility in terms of informing their users and other stakeholders themselves. The event shows that this responsibility is difficult for many organisations to comply with. Emergency preparedness and contingency planning for long disruptions are requirements for most organisations, but special needs arise when an organisation outsources IT operations or uses cloud services for vital parts of the operation. The impression after the disruption at Tieto is that the organisations' contingency planning was of varying quality. Further, only a small number of organisations had applied information classification or performed a risk analysis before their procurement and outsourcing of services.

In the event of cyber incidents, warnings come at short-notice or not at all, the pace is rapid and the incident is usually geographically independent. In order to prevent and handle cyber incidents, an increased capability of all organisations in society at all levels of responsibility and in all sectors is required. To this end, the MSB has identified four areas in which further work is required:

- *Strengthening preventive initiatives for cyber security (information security) throughout society.*
- *Procurement as a tool for better security:* There is a great deal of potential in public procurement, and all organisations need to develop further their competency in using procurement as a means of controlling their cyber security (information security).
- *Special focus on risk analysis and contingency planning:* The disruption at Tieto shows that there are shortcomings in the contingency planning and emergency preparedness among several of the affected organisations.
- *National and regional cyber security situational awareness:* The increased concentration of IT operations and other IT related services means that a large number of stakeholders

might be affected simultaneously by a cyber incident. The disruption at Tieto shows that the affected parties need to develop better processes for gathering and sharing information in order to create situational awareness. This should also include being able to communicate information to the public, and it assumes that the information is coordinated.

By stepping out of our own closed communities, opportunities to work together will show themselves everywhere. By recognising these opportunities and acting upon them, we ensure that we will be able to meet tomorrow’s threats today.

Lessons learned

Three case studies have been presented. Each one presents lessons learned from the events described and the role of their authoring organisation during these events. Two features are evident in each of these cases:

On a technical level, the incidents were not very complex, but the impact on society was great. The Swedish case describes a relatively simple system failure; the German story about the denial-of-service attack involves somewhat advanced but well-known techniques; and the hack at DigiNotar was mostly possible because of the lack of proper controls in place at DigiNotar.

In each case, the impact was large because of the role the target played in each country: a national telecommunications provider, a signer of the national PKI infrastructure, and an IT operations provider. All had many parties who depended on their cyber security. Through network effects, these incidents escalated quickly.

The **lessons learned** show many parallels as well. A few highlights:

1 New technology has created new opportunities as well as new risks in our society. New technology and new business solutions have allowed a concentration of information, services, communication and IT operations in society. This increased concentration, along with new forms of operation and increased integration, can lead to a vulnerability where small technical errors can shut down a number of societal functions in a short period of time.

2 Since the internet is a worldwide network, it is necessary to establish national and international contacts and well-defined contact points between ISPs, but also between governmental agencies (law enforcement, governmental CERTs), which can help to stop an attack. Incident response is an entirely different matter if the incident has taken place within infrastructures which may be halfway across the globe. International cooperation is essential in approaching this challenge. Special needs arise when an organisation outsources IT operations or uses cloud services for vital parts of the operation. Cloud services and service providers form an additional challenge for CERTs and their activities.

3 The internet is a critical infrastructure. Its availability is essential for the functioning of a society and economy. Therefore, its protection should be an important goal for

governments in every country. Governments should re-evaluate whether the perception of what constitutes the ‘critical infrastructure’ of a country is both correct and complete.

4 The incidents in this report show that a large cyber incident can have an effect on an entire society and that the impact can be considerable. In order to prevent and handle major IT incidents, an increased capability of all participants in society at all levels of responsibility and in all sectors is required. In this regard, the following areas are particularly important:
a Procurement as a tool for better control of cyber security
b Special focus on risk analysis and contingency planning
c Implementation of the necessary processes for early detection and mitigation of IT attacks
d National and regional situation status reports on cyber security.

5 In each of these cases, incident response plays a central role. Cooperation and coordination around a major cyber security incident are crucial. The timing and the quality of the initial response are both crucial in order to deal effectively with all aspects of an incident or with a crisis at a later stage. The examples in this report show that all participants must be able to act together and collaborate on decision-making and operations in the event of an emergency. It is important that the affected parties have developed processes for gathering and sharing information. This should also include being able to communicate information to the public and to other stakeholders. And finally the information should be coordinated.

6 During an incident or crisis it is important to have access to current and relevant information from different stakeholders. Each of these cases describes how more and more information became available during the crisis and how it was dispersed among trusted partners. Such trust relations are not built during a crisis, but rather in the relatively calm period beforehand. In order to respond adequately during a crisis, it is important to establish channels for communication and the conditions under which communication takes place.

7 Internet Service Providers (ISPs) are an important party in preventing cyber attacks. The effectiveness of the measures taken by a provider greatly affects the security stance of its clients. Any lack of security at a provider which is responsible for trust-related services has a great impact.

All in all, this report provides one with much to think about, but much to do as well. The opportunities presented by international cooperation are large indeed. We can no longer model the cyber security stance of an organisation on a fort, by assessing the thickness of the virtual wall built around it. Rather, we must secure the information within and between organisations. By stepping out of our own closed communities, opportunities to work together will show themselves everywhere. By recognising these opportunities and acting upon them, we ensure that we will be able to meet tomorrow's threats today.

Ministry of Security and Justice, The Netherlands
Federal Office for Information Security, Germany
Swedish Civil Contingencies Agency, Sweden

November 2014