Swedish Civil Contingencies Agency

Date
13 JAN 2010

Registration number
2009-14471

MSB 0163-10

Measures to improve Sweden's ability to prevent and handle IT incidents

Report on the government assignment to the Swedish Civil Contingencies Agency

(Fö2009/2162/SSK, 2009-10-29)

On 29 October 2009, the Swedish Civil Contingencies Agency (MSB) was tasked by the Government to submit proposals for the prevention and handling of IT incidents in Sweden, before 15 January 2010.

The assignment was presented in the report "Measures to improve Sweden's ability to prevent and handle IT incidents."

In this document, a summary of the report will be presented in English.

For more information about the assignment and the MSB's proposals, please contact Richard Oehme (`richard.oehme@msb.se`), Head of the Information Assurance Department.

Executive Summary

The development in the field of cybersecurity

The boundless digital information and communications infrastructure is needed in all areas of modern society. It provides significant support to important societal functions and critical infrastructures. Information technology has significantly changed our way of life and the way we communicate.

However, a growing group of governmental and non-governmental actors, such as foreign intelligence services, criminal organisations and terrorist groups have now acquired the ability to obtain, steal, alter and destroy information. These actors have interests in all functions of society; from individual citizens and businesses to critical infrastructures and important societal functions. Therefore, serious IT incidents could threaten the safety of Sweden and Swedish interests.

In recent years, increasingly more countries have increased their preventive activities in the field of cybersecurity. Increasingly more countries are creating national structures for coordination and cooperation and are developing extensive competencies and resources. Furthermore, more countries have introduced, or are about to introduce, new national collaborative functions in order to coordinate the handling of IT incidents.

Sweden has good prerequisites for creating strong structures to prevent and handle IT incidents. In Sweden, many of the competencies and resources needed in order to create a sustainable system for the preventing and handling of IT incidents are already available, both in the private and public sectors. However, these collective resources have to be supplemented in order to improve their suitability, coordination, availability and dimension.

The main proposal – a national structure

In order to prevent and handle IT incidents, the preventive information security work in Sweden should be strengthened and better coordinated. The implementation of the national plan of action for information security is of great importance for this undertaking, as is updating the national strategy for information security.

The MSB's main proposal is to create a coherent structure to strengthen the national ability to prevent and handle serious IT incidents. An important part of this national structure is a central operational coordination function for cybersecurity, which would make use of, and strengthen, the collective resources in Sweden. In addition, a number of measures should be implemented in order to improve management, cooperation and coordination, increase the information sharing, attain situational awareness and improve operational responsiveness.

A national operational coordination centre

The MSB intends to set up a national operational coordination centre for cybersecurity at the agency. The coordination centre will be assigned to support Sweden's preventive cybersecurity work and to help coordinating the handling of serious IT incidents.

The fundamental undertaking of the coordination centre should be the cooperation between government agencies with operational assignments in the field of information security. When necessary, experts from both public and private organisations should be able to assist the centre on-site. The coordination centre is to have access to secure and appropriate premises, adequate IT support and secure and redundant communication.

A guiding principle is that the national operational coordination centre for cybersecurity should be a central part of the crisis management system. The centre should work closely with both the situational awareness function already established at the MSB and the preventive work carried out within the framework of the agency's assignment to support and coordinate the

cybersecurity work in Sweden. That way, the centre becomes an integrated part of the crisis management system and the preventive cybersecurity work. This improves the ability of the Government and other affected actors to obtain collective information on the situation.

The private sector owns and operates the majority of the digital information and communications infrastructure, and it is important to develop the forms of cooperation between the public and private sectors, which are based on mutual trust and benefit. Therefore, it should be possible for people with operational roles of important societal functions and critical infrastructures to be temporarily relocated to the centre, depending on the character of the event.

Measures to strengthen the national structure

Besides the establishment of a national operational coordination centre, the following measures should be implemented in order to create a structure that aims to increase the national ability to prevent and handle serious IT incidents.

Measures to improve management, cooperation and coordination:

- The Government should assign an agency to, together with other affected actors, closely investigate how a secure digital information and communication infrastructure for the public sector, a so-called GovNet, can be created.
- The MSB intends to, in consultation with the Swedish Armed Forces and the Swedish National Defence Radio Establishment, analyse in detail how current or future cryptosystems can be utilised to protect sensitive or confidential information.

Measures to increase the information sharing:

- The MSB intends to work toward creating a clear national structure for private-public cooperation within the field of cybersecurity.
- The MSB intends to investigate how a system for compulsory IT incident reporting could be introduced in government agencies. Other actors in Sweden should be invited to voluntarily participate in such a system.

The different forms of distribution with regard to intelligence and other information should be investigated further, within the framework of the Joint Action Group for Information Security (SAMFI).[1] Information that is generated from the intelligence and security services' various government assignments could prove very valuable, both in the preventive cybersecurity work and in the handling of serious IT incidents.

[1] SAMFI comprises representatives from the Swedish Armed Forces, the Swedish National Defence Radio Establishment (FRA), the Swedish Post and Telecom Agency (PTS) and the Swedish National Police Board (RPS) and is directed by the MSB.

Measures to improve situational awareness:

- With regard to its assignment to regulate the government agencies' work through risk and vulnerability analyses, the MSB intends to make sure that the relevant cybersecurity parameters are presented in those analyses.
- The MSB intends to, in collaboration with the agencies that make up SAMFI, investigate whether a more structured technical intrusion detection and warning system for important societal functions and critical infrastructures could be introduced in Sweden.

Measures to improve operational responsiveness:

- The MSB intends to, in consultation with the agencies that make up SAMFI, produce a national response plan that clarifies how serious IT incidents are to be handled.
- The MSB intends to, in collaboration with the agencies that make up SAMFI, create technical networks of competencies that consist of experts who can provide support in the event of a serious IT incident.
- The MSB intends to continue working toward a trustful collaborative structure with actors in Sweden, in order to handle the practical issues during serious IT incidents.
- The MSB intends to continue its work with regular cybersecurity exercises, in order to develop and evaluate structures for the handling of serious IT incidents.