SWITCH-CERT for Banks

NIST[1] Cyber Security Framework functions form the basis of a comprehensive information security management strategy:

IDENTIFY	Development of organisational overview; Identification of business-critical assets, systems, data, etc.
PROTECT	Various security measures to contain the effects of a cybersecurity incident.
DETECT	Detection of cybersecurity incidents and their analysis via correlation and aggregation.
RESPOND	Swift response to security incidents to minimise damage (communication, coordination and mitigation).
RECOVER	Ability to remain resilient and to resume normal operations within the company as quickly as possible.

Relevance due to revised **FINMA circular 2008/21**

One of the new components of the revised version of the FINMA circular is an explicit requirement for a risk management concept for cyber risks. The corresponding points are strongly oriented towards the NIST Cybersecurity Framework.

"The Management Board should also implement a risk management concept for cyber risks. This concept should cover the following aspects at a minimum, and guarantee effective implementation through appropriate measures and an unambiguous definition of tasks, roles and responsibilities." (Extract from FINMA circular 2008/21)

IDENTIFY	Identification of potential institution-specific cyberattack threats.
PROTECT	Protection of business processes and technological infrastructure, with particular regard to CIA of critical and/or sensitive data and IT systems.
DETECT	Real-time detection and recording of cyberattacks, rooted in systematic monitoring of the technological infrastructure.
RESPOND	Prompt and targeted measures in response to cyberattacks.
RECOVER	Appropriate measures to ensure swift resumption of normal business operations following cyberattacks.

1) NATIONAL INSTITUTE OF STANDARDS & TECHNOLOGY

The **SWITCH-CERT service portfolio** supports **financial institutions** in **central functions** of the **NIST Cybersecurity Framework** and makes a decisive contribution to **fulfilling the requirements of the FINMA** circular 2008/21.

SWITCH-CERT core competencies

SWITCH-CERT for Banks covers the following action points, particularly within the core functions 'detect' and 'respond':

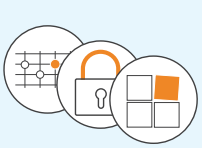
DETECT

- Identification of Swiss specific as well as banking specific threats from our own malware monitoring. Security monitoring of the Swiss academic network (NREN, 400'000 users).
- State-of-the-art malware analysis capabilities.
- Advanced detection through combination of own threat intelligence, open source intelligence and international not public resources.
- Efficient and highly trusted information exchange in a collaborative environment and moderated sharing of indicators of compromise.
- Cyber threat detection processes are continuously improved – processed threat intelligence is enhanced in tactical, operational and strategic terms.

RESPOND

- Event detection information is coordinated with appropriate parties for mitigation. This includes communication with Swiss ISPs for take-down, deactivation and mitigation.
- Development of technical mitigation measures to defend against attacks (e.g. web application firewall settings) and support for their implementation.
- Efficient collaboration on national and international level thanks to direct, informal contact with CERTs in Switzerland and worldwide.
- Correlation and supplementation of our own threat intelligence with information from a wide range of international sources in our global network.
- Security analysis and forensics capabilities for adequate response and support of mitigation and recovery activities.

Further valuable features are available for the following core functions



IDENTIFY PROTECT & RECOVER

- SWITCH facilitates collaborative exchange in trusted user groups on best practices and upcoming threats.
- SWITCHs Security Competence Center provides current IT security related information on operational and strategic level.
- Communication and restoration activities are coordinated with external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs and vendors.

Contact: SWITCH | michael.fuchs@switch.ch, https://security.switch.ch

SWITCH