SWITCH-CERT for Banks

Fact sheet

SWITCH-CERT in brief

SWITCH's Computer Emergency Response Team, SWITCH-CERT, is the leading centre of expertise in Switzerland for local threat intelligence, detection and incident response. It provides services tailored specifically to financial institutions under the name SWITCH-CERT for Banks with a choice of two service packages:

SWITCH-CERT Core Services

Core Services is the basic SWITCH-CERT for Banks package. It is particularly suited to financial institutions that have outsourced their security infrastructure or banking software and are looking for a provider-independent view and additional security measures. They also receive an accurate and up-to-date overview of the local threat situation with tailored monitoring, threat classification and recommended actions.

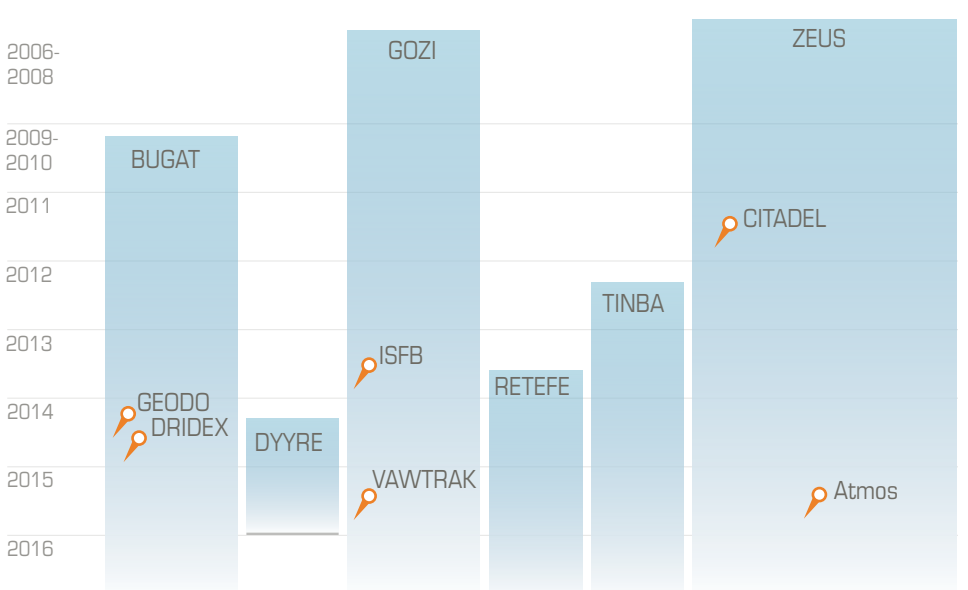
SWITCH-CERT Advanced Services

We help the people responsible for operational online security to strike a balance between innovation and keeping costs down so that they can spot complex threats at the earliest possible stage and successfully defend against attacks. The Advanced Services package includes everything in Core Services plus a few extras to guarantee banks the best possible protection. It is especially suited to banks that have their own IT security team and know that they cannot afford to sacrifice security in favour of low costs.

SWITCH-CERT add-on modules

The «threat intelligence sharing», «DNS Firewall» and «mobile security» add-on modules are based on the latest technology and ensure optimal protection in combination with SWITCH-CERT's comprehensive know-how.

Growth in malware



Malware goes through complex life cycles. Using a number of well-known examples, the chart shows the number of registered attacks on Swiss banks per year.

SERVICE MODULE	DESCRIPTION	SERVICE PACKAGE CORE	SERVICE PACKAGE ADVANCED
Monitoring	• Detection, identification and collection of Swiss-specific malware and advanced persistent threats (APTs) from our numerous sources • Quantification of the current threat situation in Switzerland • Passive monitoring of external IP addresses	✓	✓
Malware analysis & recommended actions	• Static and dynamic analysis of banking malware • Recommendations on minimising operating risk • Monitoring and classification of cyber threats and attacks • Identification and neutralisation of malicious data traffic and infection vectors such as drive-by downloads on the Web	✓	✓
Phishing (notice & takedown)	• Collection, verification, notification and takedown of phishing sites (around 10,000 a year) • Communication with Swiss ISPs regarding deactivation and mitigation; reporting to the APWG and the AV industry for blocked URL lists (digital brand protection) • Reporting and sharing of URLs with external partners, including SISA partners, banks or friendly CERTs and TLDs	✓	✓
Dummy client	• This method substantially reduces operational risks by flagging up malicious behaviour and attempted fraud. It works as an interactive simulation using dummy client data. The results take the form of recommendations for detecting and dealing with infected end-user devices	✓	✓
Bank support	• Assistance for internal bank support organisations with specific malware fact sheets • Customer-specific training for helpdesk staff	✓	✓
Cyber-CERT incident response	• Monitoring of public IP addresses with regard to types of infection on the internal network • Cyber threat enrichment: incidents are correlated, resulting in a holistic understanding of the threat context • Support for customers in cooperating with law enforcement		✓
Forensic analysis	• Rapid, targeted forensic analysis of end-user devices with an incident response kit • On-site drive image creation, analysis in the lab and an expert report		✓
Security hotline	• Direct assessment and evaluation of all kinds of security incidents by SWITCH security experts		✓
Info events	• Regular customer events, personal sharing of experiences and discussion of situations		✓
Info services	• Information on the current threat situation • Demos and white papers on increasing staff awareness, activity reports, Security Reports, periodic analyses and trend barometers		✓
Threat intelligence sharing	• Sharing and context-based enrichment of relevant of indicators of compromise (IoCs) on a secure, dedicated malware information sharing platform (MISP)		
DNS Firewall	• DNS Firewall is SWITCH's technology for blocking or rerouting DNS queries for malicious domain names infected by malware, phishing or ransomware. The DNS Firewall service for banks includes a list of malicious domain names, feedback from infected end-user devices and a landing page that can be adapted for each customer and posted on their website to raise awareness		
Mobile security	• Rogue app monitoring monitoring of official app stores (Google Play, Apple iTunes, Samsung, Amazon) on the basis of predefined search criteria, periodic checking of unofficial app stores and comparison against original apps to identify manipulation • Mobile malware analysis case-by case analysis of Android apps in the SWITCH-CERT lab		

SCF DE 4.2017

As of April 2017. Contact: michael.fuchs@switch.ch, https://security.switch.ch

SWITCH