SWITCH-CERT pour les banques

Fiche d'information

SWITCH-CERT en un mot

SWITCH-CERT, le Computer Emergency Response Team de SWITCH, est le principal centre de compétences en matière de Threat Intelligence, de Detection et d'Incident Response en Suisse. Sous le nom de SWITCH-CERT pour les banques, il fournit aux instituts financiers des services spécifiques à la branche.

SWITCH-CERT pour les banques est disponible au sein des deux paquets de services suivants:

SWITCH-CERT Core Services

Les Core Services constituent le paquet de base de SWITCH-CERT pour les banques. Ils sont particulièrement adaptés aux instituts financiers ayant délocalisé l'infrastructure de sécurité ou les logiciels bancaires et qui optent pour une vision indépendante du fournisseur ainsi que pour des mesures de sécurité complémentaires. Dans le même temps, un aperçu précis et en temps réel de la situation locale leur est fourni au moyen d'une surveillance et d'une classification sur mesure. Des recommandations d'actions contre les différentes menaces complètent l'offre.

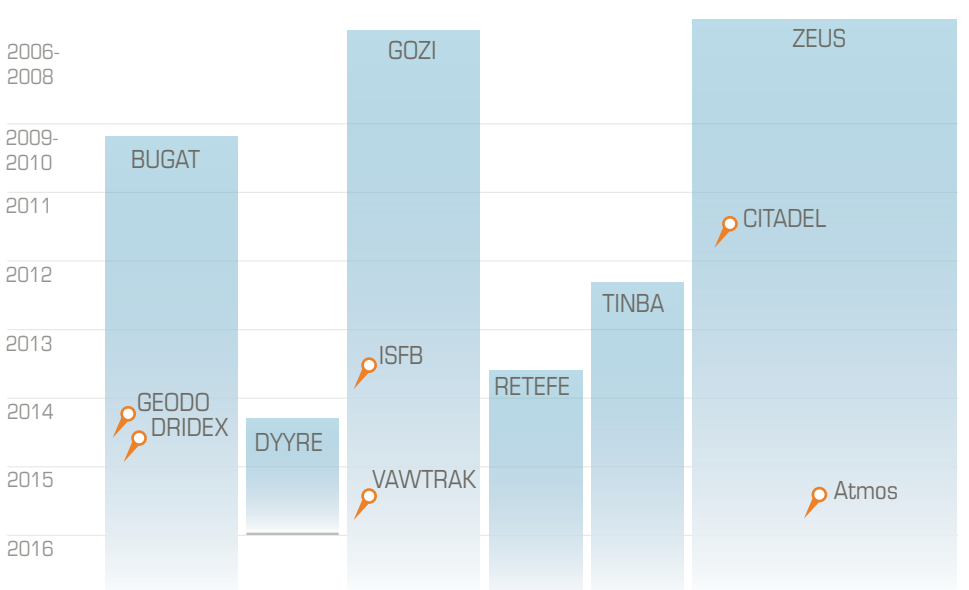
SWITCH-CERT Advanced Services

En regroupant l'innovation et la pression sur les coûts, nous aidons les responsables de la sécurité en ligne à anticiper les menaces complexes et à prévenir les attaques. Le paquet de prestations Advanced Services contient tous les Core Services ainsi que d'autres, dont l'ensemble permet de fournir une protection optimale pour les banques. Le paquet Advanced est particulièrement adapté aux banques disposant de leur propre service de sécurité et sachant qu'il n'est pas rentable de céder à la pression exercée sur les coûts au détriment de la sécurité.

Modules complémentaires SWITCH-CERT

Les modules complémentaires «Threat Intelligence Sharing», «DNS Firewall» et «Mobile Security» se fondent sur les technologies les plus modernes et garantissent, en association avec l'expertise de SWITCH-CERT, une protection optimale.

La dynamique des maliciels



Les maliciels traversent des cycles de vie complexes. Le graphique illustre les attaques recensées qu'ont subies les banques suisses au cours des années.

MODULES DE SERVICES	DESCRIPTION	PAQUETS DE SEVICES CORE	ADVANCED
Monitoring	• Détection, reconnaissance et inventaire de maliciels spéciques à la Suisse et d'Advanced Persistant Threats (APT) répertoriés dans nos nombreuses sources • Quantification de la menace actuelle en Suisse • Monitoring passif des adresses IP publiques	✓	✓
Analyse de maliciels et recommandations d'actions	• Analyse statique et dynamique de maliciels bancaires • Recommandations visant à minimiser le risque opérationnel • Surveillance et classification de cybermenaces et d'attaques • Identification et neutralisation du trafic de données nuisibles et des vecteurs d'infections sur le web comme les Drive-by Downloads	✓	✓
Hameçonnage (avertissement et neutralisation)	• Compilation, vérification, notification et neutralisation de pages de hameçonnage (près de 10 000 par an) • Communication aux ISP suisses à des fins de désactivation et de mitigation. Signalement au secteur APWG et AV concernant les listes d'interdiction (Digital Brand Protection) • Production de rapports et échange d'URL avec des partenaires externes. Il peut s'agir de partenaires SISA, de banques, de CERT ou de TLD partenaires	✓	✓
Utilisateur final fictif	• Cette technique diminue considérablement les risques opérationnels des clients, car elle reconnaît les comportements malveillants ou les tentatives de fraude. Elle fonctionne au moyen d'une simulation interactive effectuée au moyen de données de clients finaux fictifs, générant ainsi des recommandations quant à la détection des terminaux infectés et aux manipulations à effectuer	✓	✓
Aide aux banques	• Accompagnement des organisations d'appui internes aux banques à l'aide de fiches d'informations spéciques sur les maliciels • Formations de collaborateurs du service d'assistance à propos des clients	✓	✓
Cyber-CERT Incident Response	• Monitoring des adresses IP publiques des banques concernant la nature des infections provoquées sur le réseau interne • Cyber Threat Enrichment: les évènements sont mis en corrélation, ce qui permet de comprendre le contexte de la menace dans sa globalité • Accompagnement des clients dans la collaboration avec les autorités judiciaires		✓
Analyse approfondie	• Analyse rapide, ciblée et approfondie de terminaux au moyen d'un kit d'Incident Response • Production d'une image sur site: analyse en laboratoire et création d'une expertise		✓
Security-Hotline	• Evaluation et estimation immédiates d'incidents de sécurité de tout type par des experts en sécurité de SWITCH		✓
Info-Events	• Evénements clients réguliers, échange personnel d'expériences, analyses de situations		✓
Info-Services	• Informations sur la menace actuelle • Démos et livres blancs visant à sensibiliser les collaborateurs, rapports d'activité, rapports de sécurité, analyses périodiques et baromètres de tendance		✓
Threat Intelligence Sharing	• Echanges et révision contextuelle d'indicateurs de compromission (IoC) sur une Malware Information Sharing Platform (MISP) sécurisée et dédiée.		
DNS Firewall	• DNS Firewall est une technique permettant à SWITCH de bloquer ou de rediriger les requêtes DNS concernant des noms de domaines malveillants (Malware, Phishing, Ransomware). Le service DNS Firewall pour les banques inclut une liste de noms de domaines malveillants, des informations sur les terminaux infectés, ainsi que, à des fins de sensibilisation, une Web Landing Page paramétrable par le client		
Mobile Security	• Rogue App Monitoring Surveillance des App Stores officiels (Google Play, Apple iTunes, Samsung, Amazon) sur la base de critères de recherche donnés. Contrôle périodique d'App Stores non officiels et comparaison avec la vraie application pour constater des manipulations • Analyse Malware mobile Analyse au cas par cas d'applications Android dans le laboratoire SWITCH-CERT		

SCF DFE 5 2017

Etat: juin 2017. Contact: michael.fuchs@switch.ch, https://security.switch.ch

SWITCH