Cyber Security Hub

Intelligenter, schneller und genauer.
Die neue Sicherheit.

Ausgerichtet auf den Schweizer Finanzplatz:
Der Cyber Security Hub informiert Banken und Versicherungen zuverlässig und relevant über aktuelle Gefahren und gefährliche Entwicklungen.

Der Schutz vor Cyberangriffen ist ein wichtiges Fundament für die Attraktivität und Stabilität des Schweizer Finanzplatzes. Die Zusammenarbeit der beteiligten Organisationen verbessert den Schutz vor Cyberrisiken. Das sind die zentralen Elemente des Cyber Security Hubs:

- Austausch von Informationen und Erfahrungen.
- Koordinierte Massnahmen bei Angriffen und anschliessende Evaluation.

Eine gemeinsame Plattform eines unabhängigen Anbieters ist dafür unabdingbar. Der Cyber Security Hub gehört für SIX, die zentrale Infrastrukturproviderin des Schweizer Finanzplatzes, zur Kernaufgabe.

Um die kritische Infrastruktur des Schweizer Finanzplatzes zu sichern, hat SIX ein Security Operations Center (SOC) aufgebaut. Es arbeitet rund um die Uhr (24x7x365) und nutzt eine einzigartige branchenspezifische Threat Intelligence. Eine wichtige Aufgabe ist dabei die stetige Aktualisierung der Use Cases mit optimierten Detection Rules, insbesondere ausgerichtet auf die Risiken des Schweizer Finanzplatzes mit den neusten Erkenntnissen zur aktuellen Bedrohungslage.

Das gesamte Wissen fliesst in den Cyber Security Hub, sodass alle Mitglieder von den Erfahrungen der Community profitieren.

Ihre Vorteile

«Als **CEO/CIO** stärke ich die Mitarbeitenden meines Sicherheitsteams, vernetzte sie mit Arbeitskollegen und verbessere die Cyberresilienz meiner Organisation.»

«Als **CISO/CRO** erhalte ich aufbereitete Informationen für den C-Level, sodass ich über die aktuellen Trends und Entwicklungen jederzeit im Bild bin. Das erlaubt mir, die Risikoabwehr und die Abwehraktionen richtig zu priorisieren.»

«Als **Leiter SOC** erhalte ich Informationen, die für Banken und Versicherungen relevant sind. Das ermöglicht mir, im Risikomanagementprozess kurz- und mittelfristig die richtigen Fokuspunkte zu setzen.»

«Als **Security Analyst** erhalte ich Informationen über Cyberrisiken, -gefahren und -angriffe, die ich für die Echtzeitabwehr nutzen kann. Ich muss mich nicht um die Qualität und die Aktualität der verschiedenen Quellen kümmern.»

An wen richtet sich das Angebot?

Besonders kleine und mittlere Banken und Versicherungen profitieren davon. Ihre Ressourcen reichen für solche Tätigkeiten, neben der Abarbeitung von Sicherheitsvorfällen, oftmals nicht aus.

Das SOC von SIX greift auf eine Vielzahl nationaler und internationaler Quellen, bewertet und selektiert sie und bereitet sie für die Schweizer Finanzindustrie auf. Dazu hat SIX ein eigenes Rechercheteam, da aufgrund der sich ändernden Angriffsmuster eine ständige Fortentwicklung notwendig ist.

	Strategische Briefings	Austausch von Best Practices und Use Cases	Shared Treat Intelligence
	Die Briefings von SIX halten die Stakeholder mit relevanten Informationen up to date.	Repositorium für registrierte Benutzer, die Informationen und Best Practices tauschen.	SIX sammelt, filtert und bereichert die Cyber Security Threat Intelligence zur gemeinsamen Nutzung.
Inhalt	Bericht zur Bedrohungslage.	Use Cases, Runbooks und Incident Reports von SIX und Anwendern.	Informationen zur Bedrohung in strukturierter Form mit Referenzen zu Use Cases.
Verantwortlichkeiten SIX	SIX erzeugt Berichte über Informationen aus verschiedenen Feeds und erweitert diese mit Informationen aus eigenen Quellen.	SIX teilt die eigenen Fälle. SIX bereitet Benutzereingaben zur gemeinsamen Nutzung vor (Anonymisierung, Relevanz, gemeinsame Standards, ...)	SIX sammelt, verwaltet, bereichert und speichert Informationen über Bedrohungen. SIX überprüft und bereichert Feeds.
Verantwortlichkeiten Anwender		Anwender reichen eigene Fälle und Best Practices anonym ein. Diese werden danach zusammen überprüft.	Anwender reichen eigene Fälle und Bedrohungen anonym ein und geben Feedback.
Publikum	CISO, CRO, CSO.	Head of Security Operations, Analysts, Engineering Leads.	Security Analysts on duty.
Timing	Innerhalb von Monaten einsatzbereit, für Jahre nützlich.	Innerhalb von Tagen einsatzbereit, für Monate nützlich.	Innerhalb von Sekunden einsatzbereit, für Wochen nützlich. Links zu Bedrohungen, Untersuchungen und Lösungsmodellen.
Distribution	Persönliche Meetings, Telefon- und Videokonferenzen, Instant Messaging, E-Mail...		
Turnus	Halbjährlich (bei Bedarf auch häufiger).		Echtzeit Feeds und regelmässige Meetings.
Grundsätzliche Regeln	Trusted Communities werden auf Vorschlag von SIX definiert. SIX verwaltet die Gruppe. Eine Community besteht aus mindestens drei Firmen. Es gelten die Chatham House Rules. Keine Informationen dürfen die Gruppe verlassen.		

Was bietet der Cyber Security Hub?

Spezifisch für die Zielgruppen der Banken und Versicherungen aufbereitete Informationen zum Thema Cybersicherheit:

- **Strategisch:** Threat Landscape Report zum strategischen Briefing von Entscheidungsträgern.
- **Taktisch:** Bibliothek mit Best Practice Use Cases und Playbooks von SIX und weiteren Teilnehmern.
- **Operativ:** Threatinformationen (Indicators of Compromise) von SIX und weiteren Teilnehmern, die die Systeme lesen können.

SIX teilt Informationen auf Basis von eigenen Erkenntnissen aus Research und Cyber Threats. Zudem selektiert und aggregiert SIX relevante Informationen aus verschiedenen nationalen und internationalen Quellen. Zum Teilen der Informationen wird SIX die dafür notwendige Infrastruktur – wie beispielsweise eine Threat Intelligence Platform – betreiben und begleitende Veranstaltungen, wie etwa Closed User Group Meetings, organisieren. Teilnehmende Banken und Versicherungen teilen in solchen Meetings anonymisierte Informationen.

Eingeladen sind alle Schweizer Banken und Versicherungen, die FINMA reguliert sind.

SIX Group Services AG
Pfingstweidstrasse 110
Postfach
8005 Zürich

T + 41 58 399 3993
securityhub@six-group.com
www.six-group.com/cybersecurityhub