Cyber Security

Intelligenter, schneller und genauer.
Die neue Sicherheit.

Ausgerichtet auf den Schweizer Finanzplatz: Das Security Operations Center (SOC) schützt Banken und Versicherungen vor Cyberangriffen.

Geschäftsdaten sind das wertvollste Gut einer Firma. Mehrere Studien zeigen, dass Unternehmen in der Schweiz das Risiko eines Cyberangriffes unterschätzen. Zur Sicherung der kritischen Infrastruktur des Schweizer Finanzplatzes hat SIX das erste kognitive Security Operations Center (SOC) aufgebaut. Das SOC von SIX arbeitet rund um die Uhr (24x7x365) und nutzt als erstes in der Schweiz das Cognitive Computing von IBM Watson. Dadurch können Angriffe «intelligenter, schneller und genauer beurteilet werden», wie Thomas Rhomberg, Head Security Operations & Transformation, sagt.

Was sind meine Vorteile vom Security Operations Center?

Als **CEO/CIO** schütze ich meine Organisation optimal und kosteneffizient mit dem gleichen System, das wesentliche Komponenten der kritischen Schweizer Finanzplatzinfrastruktur schützt.

Als **CISO/CRO** schliesse ich schnell eine Ressourcen- und Kompetenzlücke in meiner Organisation und erfülle die regulatorischen Anforderungen (z. B. FINMA oder SWIFT). Meine knappen Personalressourcen kann ich gewinnbringend in anderen, wichtigen Aufgaben einsetzen.

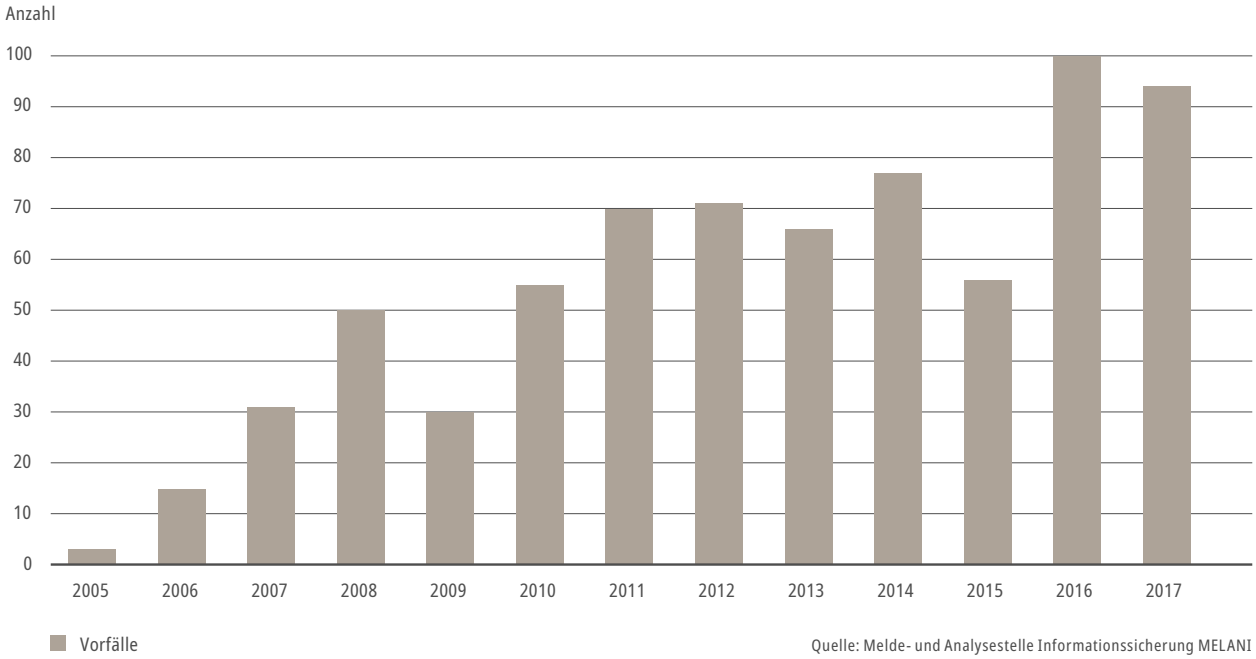
Als **Leiter SOC** bin ich in der Lage, Angriffe schnell zu erkennen und ihnen adäquat zu begegnen. Ich profitiere fortwährend von der neuesten Technologie und baue auf Use Cases auf, die auf die spezifischen Risiken des Schweizer Finanzplatzes ausgerichtet sind. Zudem bin ich optimal informiert: Zeitnah, rund um die Uhr, an jedem Tag der Woche.

Als **Security-Analyst** kann ich mich auf die wichtigen Aufgaben fokussieren und ich werde beim Monitoring und bei der Triage von Meldungen effizient unterstützt. Ich verliere keine Zeit bei der aufwändigen Triage von Fehlalarmmeldungen.

An wen richtet sich das Angebot?

Als Betreiberin der Börse ist SIX auf maximale Sicherheit angewiesen. Dementsprechend muss das SOC höchsten Ansprüchen genügen – SIX nutzt es auch selber. Besonders mittlere und kleinere Banken und Versicherungen haben durch das MSS-Angebot der SIX Zugang zu einer Sicherheitslösung, wie sie sonst nur Grossbanken für sich entwickeln können. Dank der Erfahrung von SIX mit komplexen regulatorischen Anforderungen ist die Lösung auf diverse Auflagen abgestimmt, auch wenn sich diese ver-

Gemeldete Bedrohungen und/oder Vorfälle bei der Melde- und Analysestelle Informationssicherung MELANI: 2005–2017



Quelle: Melde- und Analysestelle Informationssicherung MELANI

ändern. Die Daten bleiben jederzeit beim Kunden, nur die Security Incidents werden für die Analyse weitergeleitet – bleiben aber jederzeit und immer in der Schweiz.

Die grösste Gefahr für Unternehmen

2017 wurden 1765 Cybereinbrüche bei Firmen registriert und dabei 2.6 Milliarden Dateneinträge entwendet. Diese virtuellen Einbrüche sind teuer: IBM beziffert die durchschnittlichen Kosten pro Einbruch auf 3,62 Million Dollar, respektive auf 141 Dollar pro einzelnen gestohlenen Eintrag.

Auch Schweizer Firmen sind ein beliebtes Ziel. Laut der Meldestelle MELANI nehmen die Anzahl Vorfälle laufend zu, zwischen 2005 und 2017 stiegen sie von 3 auf 94. Gerade Banken und Versicherungen werden oft Opfer der Attacken.

Ginni Rometty, CEO und Präsidentin von IBM, formulierte schon 2015: «Cyberkriminalität ist die global grösste Gefahr für Unternehmen».

Laut einer Studie von IBM dauert es im Durchschnitt 191 Tage, um einen Datendiebstahl zu entdecken und nochmals 66 Tage, um darauf zu reagieren. Die Reaktionszeit korreliert stark mit den Kosten; je länger es dauert, bis der Angriff abgewendet ist, desto teurer wird der Einbruch für die Firma.

Was bieten die Managed Security Services (MSS)?

Was: Zur Erkennung von Sicherheitsvorfällen und Angriffen werden «Security Events» gesammelt und in Echtzeit korreliert. Verdächtige Vorgänge untersucht das Security-Team aus Zürich. Bestätigt sich der Verdacht, bereiten die Spezialisten eine Handlungsempfehlung vor und alarmieren das «Incident Response Team» des Kunden.

Wie: State-of-the art Technologie: Nutzung des ersten kognitiven Security Operations Center (SOC) in der Schweiz. Dank kognitivem Computing «können wir Angriffe intelligenter, schneller und genauer beurteilen», sagt Thomas Rhomberg, Head Security Operations & Transformation.

Wo: Datenhaltung bleibt beim Kunden, nur Security Incidents werden für die Analyse weitergeleitet – bleiben aber jederzeit und immer in der Schweiz.

Kompatibilität: Betrieb und Pflege des SIEM-Systems.

Updates: Stetige Aktualisierung der Detection Rules mit Zugriff auf Use Case Bibliothek, insbesondere ausgerichtet auf Risiken des Schweizer Finanzplatzes und auf neueste Erkenntnisse der aktuellen Bedrohungslage.

SIX Group Services AG
Pfingstweidstrasse 110
P.O. Box
CH-8021 Zürich

T + 41 58 399 3538
mss@six-group.com
www.six-group.com