Reglement
Incident Klassifizierung

zum Teilnahmevertrag bLink Plattform

Inhaltsverzeichnis

1. Inhalt

Dieses Reglement regelt die Klassifizierung, die Meldung sowie den Prozess zur Meldung von sicherheitsrelevanten und betrieblichen Störungen durch Teilnehmer.

2. Hintergrund

SIX BBS AG («SIX») ist Erbringerin der Dienstleistung bLink. Die an der bLink Plattform teilnehmenden Service-Provider und Service-User unterliegen aufgrund der ausgetauschten Daten speziellen Sicherheitsanforderungen. Die Erfüllung der Sicherheitsanforderungen sind ein essentieller Bestandteil der dem Endkunden erbrachten Dienstleistungen.

Die Dienstleistung bLink wird von SIX gegenüber einer Vielzahl von Teilnehmern erbracht. Bei einer solchen Anzahl Finanzinstitute sind klare Regelungen betreffs der Klassifizierung von Störungen und der damit verbunden Kommunikation unabdingbar.

3. Arten von Störungen

SIX unterscheidet zwei Arten von Störungen: sicherheitsrelevante und betriebliche Störungen.

Sicherheitsrelevante Störungen beinhalten alle Störungen des bLink Ecosystems, d.h. Service Provider, Plattformbetreiber und/oder Service-User, die eine Verletzung der Datensicherheit darstellen. Diese Störungen werden gemäss dem SIX Security Event and Information Management behandelt und nutzen vorhandene Informationen zum Identifizieren von sicherheitsrelevanten Vorfällen oder forensischen Analysen.

Betriebliche Störungen beinhalten alle Störungen, die den Ablauf, die Funktionalität und Verfügbarkeit des bLink Ecosystems, d.h. Service Provider, Plattformbetreiber und/oder Service-User, betreffen. Diese Störungen werden gemäss dem SIX IT Service Management behandelt und nutzen vorhandene Informationen, die das Verhalten der Applikationen und Infrastruktur beschreiben, respektive die Abweichung vom Normalverhalten, sowie weitere Informationen, um den root-cause der Störung zu identifizieren.

4. Kategorien von Störungen

4.1 Sicherheitsrelevante Störungen (SIEM)

Störungen betreffs der Sicherheit werden gemäss Tabelle 1 klassifiziert. Dabei gilt folgende Kategorisierung zur Störungsbehandlung:

- Störungen der Stufen Critical und Severe werden als Major Incident behandelt.
- Störungen der Stufe Serious werden als Level 2 Störung gemäss Anhang 3 des Teilnahmevertrags behandelt.
- Störungen der Stufe Minor werden als Level 1 Störung gemäss Anhang 3 des Teilnahmevertrags behandelt.
- Störungen der Stufe Negligible unterliegen nicht der Betriebsvereinbarung und dienen der internen Ablaufsteuerung.

4.2 Anomalien im Zugangsverhalten

Gemäss Ziff. 16 lit. a des Teilnahmevertrags prüft SIX Anomalien im Zugangsverhalten. Dafür gelten nachfolgende Bestimmungen:

1. Detektion: SIX prüft Anfragen der Service User permanent (24/7) auf Unregelmässigkeiten des Zugriffs, wobei im Besonderen geprüft wird, ob eine Anfrage von einem Teilnehmer an SIX mittels einer

Kombination von identifizierenden Merkmalen («Identifizierende Merkmale») gesendet wird, welche der Teilnehmer der SIX vorgängig gemeldet hat (z.B. IP Adresse, und/oder Zertifikat) oder ob eine Anfrage von SIX selbständig registriert (z.B. spezifische Verhaltensmerkmale) worden ist. Sollte dies nicht der Fall sein, liegt eine Unregelmässigkeit vor. Bei der Überprüfung der Anfragen des Teilnehmers auf Unregelmässigkeiten wendet SIX die geschäftsübliche Sorgfalt an.

2. Alarmierung/Incident Eröffnung im Security Operation Center («SOC») der SIX: falls SIX feststellt, dass eine Anfrage eines Teilnehmers eine Unregelmässigkeit aufweist, wird der Event sofort erfasst und die genauere Prüfung der Unregelmässigkeit im SOC eingeleitet (24/7) gemäss nachfolgender Ziffer 3.

3. Reaktion: SIX wird umgehend den Unregelmässigkeiten angemessene Massnahmen treffen, damit es nicht zu einem unberechtigten Datenzugriff kommt oder anderweitig die Sicherheit der Plattform oder des darüber abgewickelten Datenaustausches gefährdet werden könnte. SIX wird insbesondere:

   Fall a: eine Nutzeranbindung des Teilnehmers sofort unterbinden und das Zertifikat des Teilnehmers, respektive des Nutzers (Zertifikat) sperren, wenn die Identifizierende Merkmale für Anfragen von mehreren unbekannten IP Adressen aus verwendet werden und innerhalb von 15 Minuten mit dem Teilnehmer klären, ob die unbekannten IP Adressen von ihm benutzt werden. Sobald der Teilnehmer bestätigt, dass die verwendeten IP Adressen gültig sind, wird die Sperrung vom Zertifikat rückgängig gemacht und die IP-Adressen als Teil der Identifizierbaren Merkmale registriert.

   Fall b: innerhalb von 15 Minuten mit dem Teilnehmer klären, ob eine unbekannte IP Adresse von ihm benutzt wird, wenn die für ihn Identifizierenden Merkmale für eine Anfrage von einer unbekannten IP Adresse aus verwendet werden. Ist der Teilnehmer nicht erreichbar innerhalb dieser 15 Minuten oder bestätigt der Teilnehmer, dass er die verwendete IP Adresse nicht nutzt, sperrt SIX präventiv das Zertifikat des Teilnehmers, respektive des betroffenen Nutzers (Zertifikat) mit sofortiger Wirkung. SIX wird weiter versuchen, den Teilnehmer zu erreichen. Sobald der Teilnehmer bestätigt, dass die verwendeten IP Adressen gültig sind, wird die Sperrung vom Zertifikat rückgängig gemacht und die IP-Adressen als Teil der Identifizierbaren Merkmale registriert.

Anfragen mit einem gesperrten Zertifikat oder Anfragen von einer gesperrten IP Adresse aus wird SIX nicht mehr bearbeiten. Der Service User kann einen Antrag auf Entsperrung einer IP Adresse oder Rückgängigmachung der Sperrung stellen, wenn er später nachweist, dass er die IP Adresse dennoch benutzt.

Wird ein Zertifikat eines Service User gesperrt, werden die betroffenen Service Provider gemäss Anhang 3 des Teilnahmevertrags informiert.

Information Security Incident Severity Matrix

	Level 5 (Negligible)	Level 4 (Minor)	Level 3 (Serious)	Level 2 (Severe)	Level 1 (Critical)
Brand protection (lead by CMC-EC)	Registration of domain name(s) that contains any of the SIX brands without approval (no active use).	Emails impersonating any of the SIX brands to steal credentials (no URL). Unauthorised creation or usage of social media account containing SIX brands.	Emails impersonating any of the SIX brands to steal credentials (including a webpage). Active use of a domain (web, email, etc.) to impersonate any of the SIX brands.	Emails impersonating any of the SIX brands to steal credentials (including good quality webpage impersonating SIX). A non-critical SIX website gets compromised and/or defaced.	SIX corporate or customer-service websites get defaced and/or escalated incident with media exposure.
Data leakage	SIX internal information disclosed externally.	SIX internal information is publicly disclosed or employee information disclosed (<10). SIX customer information disclosed (<10).	SIX confidential information is or SIX customer simple PII information disclosed (1+). SIX employee internal information disclosed (10+). SIX confidential customer information is disclosed (<10).	SIX secret information or customer PII extended information is disclosed (1+). SIX employee confidential or secret information is disclosed (1+). The information is not made public. 100+ records of lower classification is disclosed publicly.	SIX secret (internal and/or customer) or sensitive PII information is disclosed and publicly available (1+). Escalated incident with media exposure.
Denial of service* (lead by CIT-*)	(d)DoS attack with limited impact on SIX operations or reputation. No customer impact.	(d)DoS attack with noticeable impact on SIX operations or reputation. No customer impact.	(d)DoS attack with significant impact on SIX operations or reputation and/or noticeable customer impact.	(d)DoS attack with large impact on SIX operations or reputation and/or significant customer impact.	(d)DoS attack with major impact on SIX operations or reputation and/or large service interruption for a large number of customers.
Malicious code	Malicious code on a single corporate asset. Malicious code in user-managed context.	Same malicious code in user mode on multiple corporate assets (<5).	Same malicious code on multiple corporate assets in user space (<10). Malicious code on single corporate asset with possible escalated privileges.	Same malicious code on multiple corporate assets (10+). Malicious code on multiple corporate assets with confirmed escalated privileges (1+). Malicious code on a high value or crown jewel corporate asset (1).	Malicious code on multiple high value or crown jewel corporate assets (1+), e.g. Active Directory. Escalated incident with media exposure.
Security policy violation	User without administrative privileges violating a security policy not resulting in an incident.	User with local administrator privileges violating a security policy not resulting in an incident. User without admin privileges violating a security policy repeatedly (more than 2 times) or resulting in an incident.	User with local administrative privileges violating the security policy multiple times. User with global administrative privileges violating the security policy not resulting in an incident.	User with global administrative privileges violating the security policy multiple times. User with local admin privileges violating the security policy resulting in an incident.	User with global administrative privileges violating the security policy resulting in an incident or compromise of the account.
Social engineering	Employee being targeted by a generic phishing campaign. Non-harmful message (with or without links or attachments).	Multiple employees being targeted by a generic phishing campaign. Employee that responded to a phishing attack. Phishing attack targeting the banking sector.	Multiple employees that responded to phishing attack. High value employee being targeted by phishing campaign. Employee(s) being targeted by a phishing campaign for high value information. Phishing attack targeting SIX specifically.	Employee(s) that responded to phishing attack with financial impact/loss or data disclosure. Multiple high value employees being targeted by phishing campaign.	Escalated incident with financial impact, loss or data disclosure.
System vulnerability	Attackers can collect information about the host via open ports, services, software versions, OS, etc. leading to disclosure of other vulnerabilities. CVSS V3 0.1 - 3.9 score.	Attackers can collect sensitive information about the host leading to disclosure of other known vulnerabilities. CVSS V3 4.0 - 6.9 score.	Publicly available & known vulnerabilty with attackers potentially having access to security settings, disclosure of file contents, directory browsing, read access to files etc. CVSS V3 7.0 - 8.9 score.	Publicly avialable & known vulnerability where attackers can gain control of the host, collect confidential information or execute commands remotely or cause a DoS scenario. Vulnerability specific to the banking sector. CVSS V3 9.0 - 10.0 score.	Attackers can easily gain control of a host (or multiple), which can lead to the compromise of the entire network. Severe vulnerability actively exploited in the wild and/or resulting in a DoS scenario for a cricital service. Escalated incident with media exposure.
Unauthorised access	Customer credentials being used on SIX service by an unauthorised party. Network scanning activity by an unknown party on resources exposed to the internet.	Multiple customer credentials being used on SIX service by an unauthorised party. Employee credentials being used by an unauthorised party.	Multiple employees credentials being used by an unauthorised party.	High value employee credentials being used by an unauthorised party. Social media account being used by an unauthorised party.	Multiple high value employee credentials being used by an unauthorised party. Escalated incident with media exposure.

Tabelle 1: Stufen von sicherheitsrelevanten Störungen

4.3 Betriebliche Störungen (Incidents)

Für betriebliche Störungen wird die Wirkung (impact) der Störung und die Dringlichkeit (urgency) der Störungsbehebung beurteilt. Die Wirkung wird auf einer 4-stufigen Skala bewertet:

1 – Grossflächige Wirkung

2 – Signifikante / grosse Wirkung

3 – Moderate / limitierte Wirkung

4 – Kleine / lokalisierte Wirkung

Die Dringlichkeit ist ebenfalls auf einer 4-stufigen Skala (1-tief, 2-mittel, 3-hoch, 4-kritisch) zu bewerten.

Die Kombination beider Werte ergibt die Priorität der Störungsbehebung gemäss

Tabelle 2.

Dabei gilt folgende Kategorisierung zur Störungsbehandlung:

- Störungen der Priorität Critical und High werden als Major Incident gemäss Anhang 3 des Teilnahmevertrags behandelt.
- Störungen der Priorität Medium werden als Level 2 Störung gemäss Anhang 3 des Teilnahmevertrags behandelt.
- Störungen der Priorität Low werden als Level 1 Störung gemäss Anhang 3 des Teilnahmevertrags behandelt.

Impact	Urgency	Priority
1 - Extensive/Widespread	1 - Critical	Critical
2 - Significant/Large	1 - Critical	Critical
1 - Extensive/Widespread	2 - High	Critical
3 - Moderate/Limited	1 - Critical	High
2 - Significant/Large	2 - High	High
4 – Minor/Localized	1 - Critical	High
1 - Extensive/Widespread	3 - Medium	High
3 - Moderate/Limited	2 - High	High
2 - Significant/Large	3 - Medium	Medium
4 – Minor/Localized	2 - High	Medium
3 - Moderate/Limited	3 - Medium	Medium
4 – Minor/Localized	3 - Medium	Medium
1 - Extensive/Widespread	4 - Low	Low
2 - Significant/Large	4 - Low	Low
3 - Moderate/Limited	4 - Low	Low
4 – Minor/Localized	4 - Low	Low

Tabelle 2: Priorität betrieblicher Störungen

5. Störungsmeldeprozess

Der für die Teilnehmer relevante Störungsmeldeprozess (Teil des Incident Managements) ist in Abbildung 1 dargestellt.

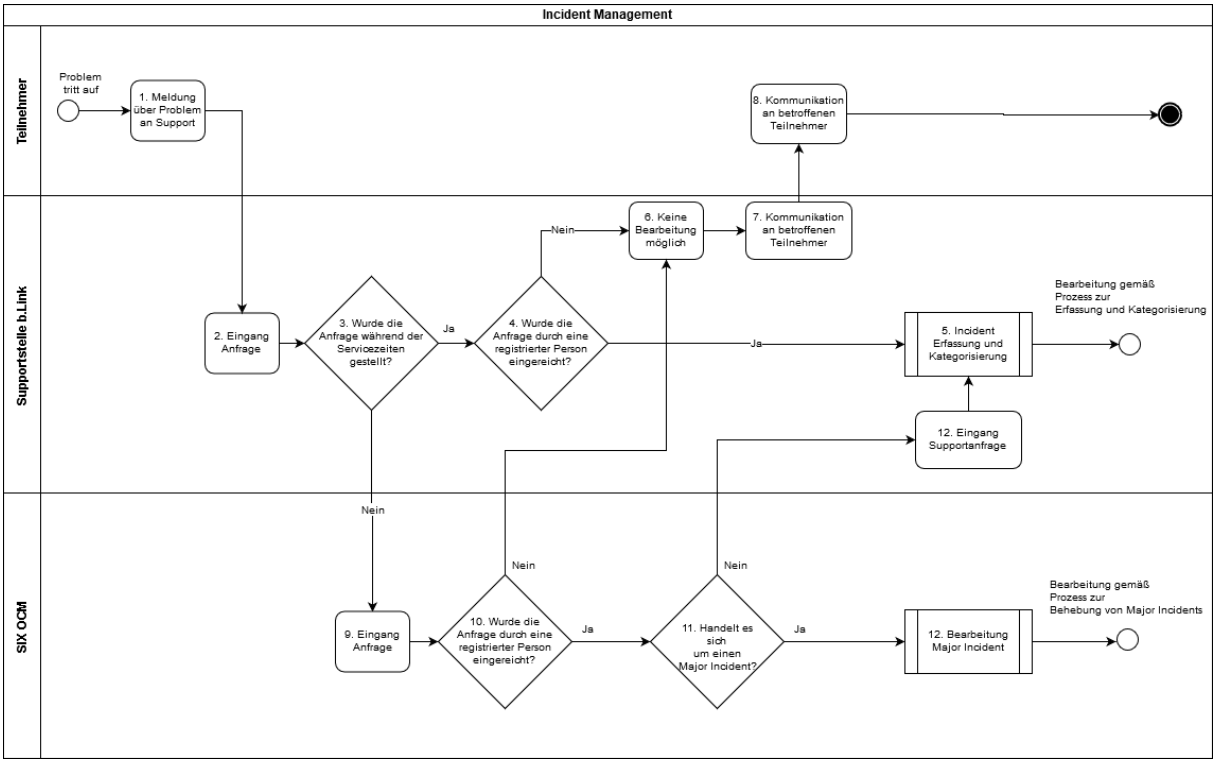

Abbildung 1: Störungsmeldeprozess

1. Der Teilnehmer meldet sein Problem unabhängig von dessen Umfang und unabhängig von den in der Betriebsvereinbarung definierten Supportzeiten der Supportstelle von SIX.

   Bemerkung: Der Prozess wird auch bei Störungen, die die SIX-interne Überwachung detektiert, angestossen.

2. Die Meldung des Teilnehmers geht an die bLink-Supportstelle per Telefon oder per Email.

3. Zunächst ist zu klären, ob die Anfrage während den im Anhang 3 des Teilnahmevertrags formulierten Supportzeiten eingegangen ist. Wird die Anfrage ausserhalb dieser Supportzeiten gestellt, können die Schritte 4 bis 8 übersprungen werden.

4. Wurde die Anfrage während den Supportzeiten gestellt, ist im Anschluss zu klären, ob dies von einer für den Support berechtigten Person erfolgt ist. Die genaue Regelung zur Berechtigung von Personen für den Support findet sich in Kapitel 4 des Anhang 3 des Teilnahmevertrags. Wenn dies nicht der Fall ist, erfolgt direkt Schritt 6.

5. Wenn die Anfrage durch eine autorisierte Person eingereicht wurde, wird die Anfrage erfasst und kategorisiert. Im Anschluss wird die Anfrage gemäss dem SIX-internen Prozess zur Behebung von Störungen bearbeitet.

6. Wurde die Anfrage von einer Person gestellt, die nicht für den Support berechtigt ist, kann diese nicht bearbeitet werden.

7. In dem Fall informiert der Support den Teilnehmer, dass die Anfrage aufgrund fehlender Berechtigung nicht bearbeitet werden kann.

8. Der Teilnehmer erhält den Hinweis, dass seine Anfrage aufgrund fehlender Berechtigung nicht bearbeitet werden konnte.
9. Wenn die Anfrage des Teilnehmers ausserhalb der Supportzeiten gestellt wird, wird diese automatisch an OCM oder im Falle einer sicherheitsrelevanten Störung an das SOC (Teil des OCM) weitergeleitet.
10. Ausserhalb der Supportzeiten muss ebenfalls geklärt werden, ob die Anfrage von einer Person kommt, die für den Support berechtigt ist. Wenn das nicht der Fall ist, übernimmt das OCM/SOC ebenfalls Schritte 6 – 8 und informiert die betroffenen Teilnehmer.
11. Wenn die Anfrage von einer für den Support berechtigten Person kommt, muss OCM/SOC entscheiden, ob es sich um einen Major Incident handelt oder aber um eine Supportanfrage, die nicht zeitkritisch ist.
12. Handelt es sich um einen Major Incident, wird dieser gemäss dem Prozess zur Behebung von Störungen behandelt.
13. Handelt es sich bei einer Anfrage an OCM/SOC, die ausserhalb der Supportzeiten gestellt wurde, nicht um einen Major Incident, wird die Anfrage an den Support zurückgestellt, der dies am nächsten Arbeitstag, gemäss dem in Anhang 1 dokumentierten Prozess, bearbeitet.

6. Vertraulichkeit

Die Störungsmeldungen, -beschreibung und der -status sind vertraulich und dürfen nicht an Dritte weitergegeben werden. Die Teilnehmer gelten hierbei nicht als Dritte. Die Weitergabe der Informationen innerhalb der Teilnehmer darf nur im Rahmen des «Need-to-know-Prinzips» erfolgen.

7. Überprüfung diese Reglements

SIX überprüft und beurteilt periodisch die Angemessenheit und Wirksamkeit dieser Bestimmungen in diesem Anhang.

Die Änderungen dieses Anhangs richten sich nach den Bestimmungen des Teilnahmevertrags.

8. Eskalationsmechanismus

Es kommt der Eskalationsmechanismus gemäss Anhang 3 des Teilnahmevertrags zur Anwendung.

9. Inkrafttreten

Das Reglement tritt per 1. Januar 2022 in Kraft.