Incident Response Plan

Übersicht

Dieser Incident Response Plan beschreibt die Reaktionsverfahren für Sicherheitsvorfälle im Nago Framework.

Eskalationspfad

```
@startuml
title Eskalationspfad bei Sicherheitsvorfällen

|L1 - Entwickler|
start
:Vorfall entdeckt;
:Erste Bewertung;
if (Schweregrad?) then (Kritisch/Hoch)
  |L2 - Security Lead|
  :Security Lead informieren;
  :Detailanalyse;
  if (Datenschutz betroffen?) then (Ja)
    |L3 - CISO/DSB|
    :CISO + Datenschutzbeauftragter;
    :Meldepflicht prüfen;
    if (Meldepflicht?) then (Ja)
      |L4 - Management/Legal|
      :Geschäftsführung + Rechtsabteilung;
      :Aufsichtsbehörde melden;
    endif
  endif
else (Mittel/Niedrig)
  :Ticket erstellen;
  :Im Sprint bearbeiten;
endif
stop

@enduml
```

Szenario 1: Master-Key-Kompromittierung

Beschreibung

Der 32-Byte Master Key für AES-GCM-256 Verschlüsselung wurde exponiert oder gestohlen.

Schweregrad

KRITISCH - Alle verschlüsselten Daten sind kompromittiert.

Detection

- Ungewöhnlicher Zugriff auf `.masterkey` Datei
- Umgebungsvariable `NAGO_MASTER_KEY` wurde exponiert
- Backup-Datei mit Master Key wurde geleakt
- Verdächtige Entschlüsselungsversuche im Log

Sofortmaßnahmen (< 1 Stunde)

Schritt	Aktion	Verantwortlich
1	**ALLE aktiven Sessions invalidieren** `session.Clear()` ausführen	Entwickler/Admin
2	**System offline nehmen** (falls notwendig)	Operations
3	**Neuen Master Key generieren** `backup.ReplaceMasterKey()` mit neuem 32-Byte Key	Security Lead
4	**Alten Master Key sperren**	Security Lead
5	**Forensische Kopie erstellen** Logs, Speicher, Netzwerkverkehr sichern	Security Lead

Containment (< 24 Stunden)

Schritt	Aktion	Verantwortlich
1	**Zugriffsanalyse** Wer hatte Zugriff auf den Key?	Security Lead
2	**Betroffene Daten identifizieren** Welche Stores waren verschlüsselt?	Entwickler
3	**Re-Encryption** Alle sensitiven Daten mit neuem Key verschlüsseln	Entwickler
4	**Passwort-Reset erzwingen** Alle Benutzer müssen Passwort ändern	Admin

Kommunikation

Zeitrahmen	Empfänger	Inhalt
< 1 Stunde	Internes Security-Team	Vollständige technische Details

Zeitrahmen	Empfänger	Inhalt
< 24 Stunden	Geschäftsführung	Executive Summary, Impact Assessment
< 72 Stunden (DSGVO Art. 33)	Aufsichtsbehörde	Falls personenbezogene Daten betroffen
< 72 Stunden (DSGVO Art. 34)	Betroffene Nutzer	Falls hohes Risiko für Rechte und Freiheiten

Recovery

- Neuer Master Key in sicherer Umgebung generieren
- Key via HSM oder Secrets Manager speichern (empfohlen)
- Alle verschlüsselten Stores neu verschlüsseln
- System wieder online nehmen
- Monitoring intensivieren

Post-Incident

- Root Cause Analysis durchführen
- Dokumentation aktualisieren
- Lessons Learned Meeting
- Prozesse verbessern

Szenario 2: Backup-Datei-Leak

Beschreibung

Eine Backup-ZIP-Datei wurde unbefugt zugänglich.

Schweregrad

HOCH - Abhängig von enthaltenen Daten.

Detection

- Backup-Datei an unerwarteter Stelle gefunden
- Verdächtiger Download von Backup-Endpoint
- Externe Meldung über exponierte Daten

Sofortmaßnahmen (< 4 Stunden)

Schritt	Aktion	Verantwortlich
1	**Backup-Quelle identifizieren** Welches Backup wurde exponiert?	Security Lead
2	**Master Key Status prüfen** War der Master Key separat gespeichert?	Security Lead
3	**Risikobewertung** Verschlüsselte vs. unverschlüsselte Daten	Security Lead

Bewertungsmatrix

Situation	Risiko	Maßnahme
Master Key NICHT im Backup, separat gespeichert	MITTEL	Verschlüsselte Stores sind sicher, unverschlüsselte analysieren
Master Key WAR im Backup	KRITISCH	→ Szenario 1 aktivieren
Master Key unbekannt	HOCH	Annehmen, dass kompromittiert → Szenario 1

Kommunikation

- Intern: Security-Team sofort informieren
- Management: Innerhalb von 4 Stunden
- Datenschutzbeauftragter: Innerhalb von 24 Stunden
- Aufsichtsbehörde: Falls personenbezogene Daten unverschlüsselt betroffen (72h)

Szenario 3: Bootstrap-Admin-Missbrauch

Beschreibung

Der temporäre Bootstrap-Admin wurde für unbefugte Aktionen verwendet.

Schweregrad

KRITISCH - Administrator-Zugriff missbraucht.

Detection

- Bootstrap-Admin nach Ablaufzeit noch aktiv
- Unerwartete RBAC-Änderungen im Audit-Log
- Neue Administratoren ohne Genehmigung erstellt

Sofortmaßnahmen (< 30 Minuten)

Schritt	Aktion	Verantwortlich
1	**Bootstrap-Admin deaktivieren** Zeitlimit auf vergangenes Datum setzen	Admin
2	**Session des Angreifers terminieren** Alle Sessions des Bootstrap-Admin invalidieren	Admin
3	**Audit-Logs sichern** `evs` Event Store exportieren	Security Lead

Forensische Analyse

```
-- Pseudo-Query für Event Store Analyse
SELECT * FROM events
WHERE user_id = 'bootstrap-admin'
ORDER BY timestamp DESC;
```

Zu prüfen: * Welche Rollen wurden erstellt/geändert? * Welche Benutzer wurden erstellt? * Welche Permissions wurden zugewiesen? * Welche Daten wurden eingesehen/exportiert?

Rollback

- Alle vom Angreifer erstellten Benutzer deaktivieren
- Alle RBAC-Änderungen rückgängig machen
- Neue Bootstrap-Admin-Credentials generieren

Szenario 4: Session-Hijacking

Beschreibung

Ein Angreifer hat eine gültige Session übernommen.

Schweregrad

HOCH - Unbefugter Zugriff auf Benutzerkonto.

Detection

- Gleichzeitige Aktivität aus verschiedenen Locations
- Ungewöhnliches Benutzerverhalten
- Benutzer meldet nicht selbst durchgeführte Aktionen

Sofortmaßnahmen (< 15 Minuten)

Schritt	Aktion	Verantwortlich
1	**Betroffene Session terminieren** Session-ID aus Cookie invalidieren	Admin
2	**Benutzer informieren** Passwort-Reset empfehlen	Support
3	**TLS-Konfiguration prüfen** Secure/HttpOnly-Flags validieren	DevOps

Analyse

- Cookie-Domain-Konfiguration prüfen
- XSS-Schwachstellen suchen
- MITM-Möglichkeiten evaluieren
- Netzwerk-Logs analysieren

Szenario 5: Privilege Escalation via Repository-ID

Beschreibung

Ein Angreifer hat versucht, über manipulierte Repository-IDs Systemrechte zu erlangen.

Schweregrad

KRITISCH (bei Erfolg) / **NIEDRIG** (bei Blockierung)

Detection

- Validation Errors für `nago.*` Präfix im Log
- Ungewöhnliche Repository-Erstellungsversuche
- Security Note in `flow/evt_repository_assigned.go:27` wurde getriggert

Code-Referenz

```
// application/flow/evt_repository_assigned.go:27-29
if strings.HasPrefix(s, "nago.") {
    // security note: Schutz gegen Privilege Escalation
    return fmt.Errorf("repository id cannot start with 'nago.'")
}
```

Sofortmaßnahmen

Schritt	Aktion	Verantwortlich
1	**Angreifer identifizieren** Welcher Benutzer hat den Versuch unternommen?	Security Lead
2	**Benutzer sperren** Account deaktivieren, Session invalidieren	Admin
3	**Repository-Integrität prüfen** Keine System-Repositories manipuliert?	Entwickler

---

Kommunikationsvorlagen

Interne Benachrichtigung

```
BETREFF: [SECURITY INCIDENT] [SCHWEREGRAD] - Kurzbeschreibung

Zeitpunkt der Entdeckung: [DATUM UHRZEIT]
Schweregrad: [KRITISCH/HOCH/MITTEL/NIEDRIG]
Status: [AKTIV/CONTAINED/RESOLVED]

ZUSAMMENFASSUNG:
[Kurze Beschreibung des Vorfalls]

BETROFFENE SYSTEME:
- [System 1]
- [System 2]
```

```
SOFORTMA□NAHMEN:
- [Maßnahme 1]
- [Maßnahme 2]

NÄCHSTE SCHRITTE:
- [Schritt 1]
- [Schritt 2]

KONTAKT:
Security Lead: [Name] - [Telefon]
```

Externe Benachrichtigung (Betroffene)

```
BETREFF: Wichtige Sicherheitsinformation zu Ihrem Konto

Sehr geehrte/r [NAME],

wir möchten Sie über einen Sicherheitsvorfall informieren, der
möglicherweise Ihre Daten betrifft.

WAS IST PASSIERT:
[Kurze, verständliche Beschreibung]

WELCHE DATEN SIND BETROFFEN:
[Liste der betroffenen Datentypen]

WAS WIR UNTERNOMMEN HABEN:
[Ergriffene Maßnahmen]

WAS SIE TUN SOLLTEN:
1. Ändern Sie Ihr Passwort unter [LINK]
2. Überprüfen Sie Ihre letzten Aktivitäten
3. [Weitere Empfehlungen]

KONTAKT:
Bei Fragen erreichen Sie uns unter:
- E-Mail: security@worldiety.de
- Telefon: [NUMMER]

Mit freundlichen Grüßen,
[Firma/Team]
```

Meldung an Aufsichtsbehörde (DSGVO Art. 33)

```
MELDUNG EINER DATENSCHUTZVERLETZUNG

Verantwortlicher: worldiety GmbH
```

```
Datenschutzbeauftragter: [Name, Kontakt]

Art der Verletzung: [Beschreibung]
Betroffene Datenkategorien: [Liste]
Ungefähre Anzahl betroffener Personen: [Zahl]
Ungefähre Anzahl betroffener Datensätze: [Zahl]

Wahrscheinliche Folgen: [Beschreibung]

Ergriffene Maßnahmen: [Liste]

Geplante Maßnahmen: [Liste]

Datum der Kenntniserlangung: [Datum]
```

Post-Incident Review Template

Zusammenfassung

Feld	Wert
Incident-ID	[INC-YYYY-NNN]
Zeitraum	[Start] - [Ende]
Schweregrad	[KRITISCH/HOCH/MITTEL/NIEDRIG]
Root Cause	[Kurzbeschreibung]
Impact	[Betroffene Systeme/Benutzer]

Timeline

Zeitpunkt	Ereignis
[T+0]	Vorfall entdeckt
[T+X]	Eskalation an Security Lead
[T+X]	Containment abgeschlossen
[T+X]	Recovery abgeschlossen

Lessons Learned

- Was hat gut funktioniert?
- Was hätte besser laufen können?
- Welche Prozesse müssen angepasst werden?
- Welche technischen Verbesserungen sind nötig?

Action Items

ID	Maßnahme	Verantwortlich	Deadline
1	[Maßnahme]	[Name]	[Datum]
2	[Maßnahme]	[Name]	[Datum]

Deployment-Security-Verweis

Dieser Incident Response Plan behandelt ausschließlich **Application Layer Security** des Nago Frameworks.

Für Deployment-bezogene Sicherheitsvorfälle (Infrastruktur, Netzwerk, Container) siehe die separate **Nago Hub Hosting Dokumentation**, die folgende Themen abdeckt:

- Reverse Proxy / Load Balancer Incidents
- TLS-Zertifikatsprobleme
- Firewall-Breach
- Container-Escape
- Host-System-Kompromittierung
- DDoS-Mitigation
- Disaster Recovery