# Handlungsempfehlung zum Aufbau eines Security-Incident Management

Arbeitskreis IT-Security des bvh

- was sind ein Security-Incident und ein Security-Incident Management
- Aufbau eines Security-Incident Management
- offene Punkte

Vorlage Version 0.1 am 21.2.2013 durch Ingmar Böckmann ingmar.boeckmann@bvh.info

bvh
Online • Katalog • TV
AK IT-Security

# Inhaltsverzeichnis

# Einleitung

## Was ist ein Security-Incident?

Als Security-Incident bezeichnet man ein Ereignis, welches den normalen Betrieb eines Services zum erliegen bringt oder diesen spürbar stört.
Ein typischer Security-Incident im E-Commerce wäre zum Beispiel ein DDoS-Angriff. Auch Vorkommnisse wie ein Verlust von Kundendaten sollten nach dem hier beschriebenen Schema behandelt werden, obwohl sie den Betrieb eines Services (z.B. Onlineshop) nicht unmittelbar einschränken müssen.

## Was ist ein Security-Incident Management?

Security-Incident Management erfasst den organisatorischen Prozess zum Umgang mit Sicherheitsvorfällen. Es soll keinen Katalog mit technischen Lösungsmöglichkeiten darstellen, sondern vielmehr eine koordinierte Vorgehensweise aller Beteiligten ermöglichen.
Ziel ist es den Verantwortlichen ein Handlungsschema an die Hand zu geben um nach Eintritt eines Security-Incidents:

- Schaden vom Unternehmen abzuwenden
- den betroffenen Service in der definierten Qualität wieder herzustellen
- die Integrität der Unternehmensdaten und -Services zu gewährleisten und gegebenenfalls wiederherzustellen

Dabei werden Verantwortlichkeiten klar geregelt, eigenmächtige Handlungen möglichst verhindert und Prozesse etabliert, die klar definieren wann eine Krisensituation als bewältigt gilt. Des Weiteren schafft man die Grundlage zur koordinierten Daten- und Wissenssammlung um ähnliche Krisenfälle künftig zu vermeiden.

# Handlungsempfehlung zum Erstellen eines Security-Incident Managements

## Aufgaben

Es können 4 Aufgaben ermittelt werden, an denen zwar teilweise gleichzeitig gearbeitet werden kann, deren tatsächliche Ausführung allerdings jeweils erst nach Abschluss der vorherigen Aufgabe durchgeführt wird, da grundlegende Verhaltensregeln sich immer erst aus der abschließenden Bewertung der vorhergehenden Aufgabe ergeben.

- Gegen- / Sofortmaßnahmen zur Schadensbegrenzung treffen
- Schadensausmaß ermitteln
- Ursachenforschung (warum konnte ein Schaden eintreten) / Beweissicherung
    - Handlungsmöglichkeiten / -alternativen
- Kommunikation (Öffentlichkeit, mit Geschädigten, mit Kunden)

Der Security-Incident ist mit Lösung dieser Aufgaben abgeschlossen. Die erlangten Informationen sollten zur Vermeidung zukünftiger Security-Incidents in einen Verbesserungsprozess einfließen.

## Aufbau

### 1. Definieren von Verantwortlichkeiten und Rollen

Jeder Mitarbeiter muss wissen an wen er sich wenden kann/muss wenn ihm ein Security-Incident auffällt. Dazu reicht es nicht, dass er die eMail oder Telefonnummer seines Vorgesetzten hat. Es muss klare und feste Vertretungsregeln geben, die eine ständige Erreichbarkeit einer verantwortlichen Person gewährleisten.
Das heißt:

- definieren Sie Ansprechpartner, ohne diese zu kategorisieren, d. h. jeder Ansprechpartner ist für JEDE Art von Security-Incident verantwortlich
- der Ansprechpartner, dem der Security-Incident zuerst gemeldet wird, übernimmt die Rolle des Security-Incident Managers
- der Security-Incident Manager verifiziert ob tatsächlich ein Security-Incident vorliegt
- für länger andauernde Security-Incidents müssen klare Übergabe- und Vertretungsregeln etabliert sein
- etablieren Sie eine Organisationsstruktur zur Innenkommunikation mit den Prozessverantwortlichen und der Geschäftsführung und zur Krisenbewältigung

Der Security-Incident Manager koordiniert in Zusammenarbeit mit den anderen Abteilungen die Bekämpfung der Störung bis zum erfolgreichen Abschluß der Maßnahmen. Statten sie den Security-Incident Manager mit dem entsprechenden Mandat aus! Ein Security-Incident

Manager verfügt über Kenntnisse der relevanten Geschäftsprozesse und über die notwendigen persönlichen Eigenschaften um Krisensituationen ruhig und entschieden zu managen.

## 2. organisieren Sie die Informationssicherung/ -beschaffung

Informationen über die Art einer Störung, deren Herkunft und, falls fremdgesteuert, deren Ziel sind essentiell zur Bekämpfung, Beweissicherung und Verhinderung zukünftiger Bedrohungen. Loggen Sie Systemdaten über einen sinnvollen Zeitraum mit und sichern Sie diese auch. Bereiten Sie erweitertes Logging von Daten vor, die normalerweise nicht geloggt werden oder geloggt werden dürfen (z. B. IP-Adressen).

- regelmäßige Logs einrichten
- unregelmäßiges Logging vorbereiten
- Logdaten sichern
- Was ist passiert?
    - Wann
    - Wo
    - Welche Geschäftsprozesse und Systeme sind betroffen
    - wer hat es gemeldet (Entdecker)
    - wer sind die Prozessverantwortlichen
- Wie konnte das passieren?
- Definieren Sie auch hier Verantwortliche die jederzeit Auskunft über den Stand der Informationssicherung und -beschaffung geben können

## 3. Herstellung der provisorischen Sicherheit

Die Daten die Sie durch die Informationsbeschaffung gewonnen haben, versetzen Sie in die Lage Gegenmaßnahmen einzuleiten und mindestens eine Schadensbegrenzung herzustellen. Das kann im Zweifel sogar die völlige Abschaltung des Systems bedeuten! Statten Sie Ihren Security-Incident Manager mit der Kompetenz aus, auch diesen äußersten Schritt zu gehen. Bereiten Sie sich auf diese Situation vor, indem Sie gegebenenfalls ein Notfallsystem bereithalten, welches über ein komplett autonomes System läuft.

## 4. Kommunikation definieren

### 4.1 Kommunikation auf operativer Ebene

Entwickeln Sie vor Eintritt eines Incidents eine standardisierte Kommunikation (Turnus, Form) der Fachabteilungen mit dem Krisenmanagement. Die Fachbereiche sollen Kenntniss über den Stand der Krisenbewältigung erlangen um ihre Fähigkeiten zur Aufgabenbewältigung realistisch einschätzen zu können.

## 4.2 Kommunikation auf strategischer Ebene

Entwickeln Sie vor Eintritt eines Incidents eine standardisierte Kommunikation (Turnus, Form) des Krisenmanagements an die Geschäftsführung. Das Krisenmanagement soll eine Bewertung der aktuellen Situation vornehmen, Handlungsempfehlungen aussprechen und Entscheidungen herbeiführen.

## 4.3 Außenkommunikation

Sie sollten nun wissen ob Kundendaten abhanden gekommen sind oder nicht. Sie wissen jetzt ob der Angriff, bzw. Unfall weiteren Schaden verursachen wird, oder ob die Gefahr, unter gleichbleibenden bzw. abzusehenden Umständen weiterhin besteht oder abgewendet ist. Sie sollten auch wissen ob der Schaden auch Dritte betrifft oder nur Sie selbst.
Gehen Sie die Information der Öffentlichkeit pro aktiv an! Besser die Presse erfährt von Ihnen das ein Schaden eingetreten ist, als dass ein Dritter diese Information an die Öffentlichkeit bringt.

- Definieren Sie genau was an die Öffentlichkeit darf
- Definieren Sie was unter keinen Umständen öffentlich werden darf
- Briefen Sie den Customer Service, damit der Ihren Kunden eine zufriedenstellende Auskunft erteilen kann
- Ermitteln Sie eventuelle Mitteilungspflichten gegenüber Dritten

## Literaturempfehlungen

http://de.wikipedia.org/wiki/Incident_Management

http://www.itil-officialsite.com/

http://www.heise.de/open/meldung/IT-Service-Management-Loesung-OTRS-ITSM-2-0-988722.html

http://wiki.de.it-processmaps.com/index.php/Incident_Management

## ToDo

- juristische Bewertung zu leistender Informationspflichten durch den bvh Rechtsausschuss
- Empfehlungen zur Krisenkommunikation durch den AK Presse und Öffentlichkeitsarbeit
- Empfehlungen zur Krisenkommunikation durch den AK Customer Service

## Kontakt

Ingmar Böckmann – Geschäftsführer AK IT-Security
Ingmar.boeckmann@bvh.info
030 / 206138511

Frank Seebach – Vorsitzender AK IT-Security
Frank.seebach@weltbild.com