Sicherheitsvorfälle erkennen und behandeln

Tritt ein Notfall ein, gilt es schnell die richtigen Schritte einzuleiten. Es ist wichtig, dass alle involvierten Personen wissen, wie und an wen ein Vorfall gemeldet werden muss. Bevor wild losgelegt wird, gilt es die Umstände genauer anzuschauen.

Was ist geschehen? Wer ist betroffen? Wie gravierend ist und kann dies werden? Die genaue Ursache ist in diesem Moment noch gar nicht das zentrale Thema. Falls möglich wird dies natürlich berücksichtigt. Aber nicht immer ist dies sofort ersichtlich. Wurde ein Überblick verschafft, werden die ersten Massnahmen eingeleitet. Ist der Vorfall unter Kontrolle gebracht, gilt es eine genaue Analyse durchzuführen, die Gründe herauszufinden und Systeme/Prozesse so anzupassen, dass ein gleicher oder ähnlicher Vorfall nicht mehr eintreten kann. Je nach Wissen und Erfahrung kann dieser Prozesse, oder Teile davon, an ein spezialisiertes Unternehmen übergeben werden.

Der Prozess-Ablauf in Bild 1 orientiert sich am US-amerikanischen NIST SP 800-61 (Computer Security Incident Handling Guide).

Meldung und Klassifizierung

Sollten Sicherheitsvorfälle eintreten, gilt es diese schnell zu behandeln. Ein Security Incident kann dabei von einem System oder durch Mitarbeitende, Externe oder weiteren Stellen gemeldet werden. Für Mitarbeitende sollte an einer zentralen Stelle gut sichtbar ein Link zum Meldeformular angebracht werden.

Wenn ein Incident gemeldet wird, gilt es einige Punkte festzuhalten:

- Titel
  Aussagekräftiger Titel
- Beschreibung:
  Kurze, aber möglichst genaue Beschreibung des Vorfalls.
- Sicherheitsstufe:
  Damit Tickets auch für vertrauliche Vorfälle genutzt werden können, sollte eine Sicherheitsstufe eingeführt werden. Damit können nur verantwortliche Personen auf dieses Ticket zugreifen.
- Asset/Wert:
  Welches System oder welcher Wert des Unternehmens ist vom Vorfall betroffen.
- Incident-Art_
  Um welche Vorfall-Art handelt es sich hier.
- Incident-Dringlichkeit:
  Wie dringend muss der Vorfall behandelt werden
- Incident-Auswirkung:
  Welche Auswirkung kann der Vorfall haben.
- Ursache:
  Falls möglich sollte die Ursache für den Vorfall beschrieben werden. Dies kann auch zu einem späteren Zeitpunkt ergänzt werden.
- Meldung:
  Wer muss über den Vorfall informiert werden. Dies könnten Kunden, Lieferanten, Mitarbeitende, Kunden, aber auch Behörden (zum Beispiel bei Datenschutzvorfällen) sein.
- Fälligkeit:
  Bis wann muss der Incident spätestens behandelt sein.

Normal wird der Prozess so konfiguriert, dass je nach Ereignis das Ticket gleich der richtigen Person zugeordnet wird. Klassisch werden technische Vorfälle, Sicherheits- oder Datenschutzverletzungen, physische Vorfälle, Personenunfälle und weitere unterschieden.

Priorisierung

Um die Incident-Dringlichkeit zu bestimmen, wird die höchste zutreffende Kategorie ausgewählt:

Gering

- Der vom Incident verursachte Schaden nimmt im Verlauf der Zeit nur unwesentlich zu.
- Die Aufgaben, die von den Mitarbeitern nicht erfüllt werden können, sind nicht zeitkritisch.

Mittel

- Der vom Incident verursachte Schaden nimmt im Verlauf der Zeit substanziell zu.
- Die Aufgaben, die von den Mitarbeitern nicht erfüllt werden können, sind nur mässig zeitkritisch.
- Ein einzelner Benutzer ist betroffen.

Hoch

- Der vom Incident verursachte Schaden nimmt im Verlauf der Zeit schnell zu.
- Die Aufgaben, die von den Mitarbeitern nicht erfüllt werden können, sind sehr zeitkritisch.
- Durch schnelles Handeln kann verhindert werden, dass aus einem Minor Incident ein Major Incident wird.
- Mehrere Benutzer sind betroffen.

Kritisch

- Der vom Incident verursachte Schaden nimmt im Verlauf der Zeit sehr schnell zu.
- Die Aufgaben, die von den Mitarbeitern nicht erfüllt werden können, sind sehr wichtig.
- Viele Benutzer sind betroffen.

Um die Incident-Auswirkung zu bestimmen, wird die höchste zutreffende Kategorie ausgewählt:

Vernachlässigbar

Die Schadensauswirkungen sind gering und können vernachlässigt werden.

- Der finanzielle Schaden ist irrelevant (bis CHF 10’000.–).
- Der Imageverlust ist gering (gelegentliche Beschwerden).
- Preisgabe wenig sensibler Daten (keine Datenschutzverletzung).
- Geringe interne Unkosten, von der Öffentlichkeit nicht bemerkbar.

Begrenzt

Die Schadensauswirkungen sind begrenzt und überschaubar.

- Der finanzielle Schaden ist tragbar (bis CHF 100'000.–).
- Der Imageverlust ist bemerkbar (gelegentliche Kritik in den Medien).
- Kurzzeitige negative Auswirkungen sind möglich.

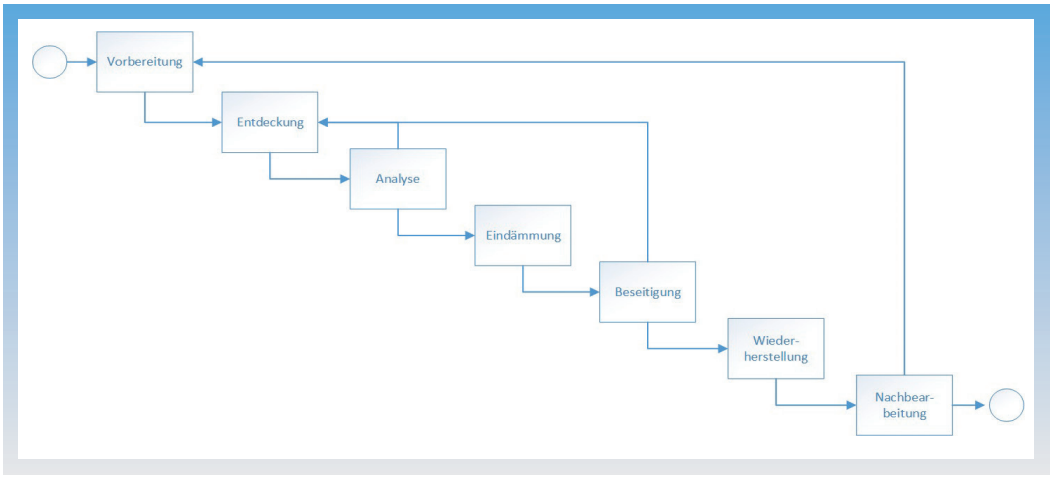

Bild 1: Prozess-Ablauf.

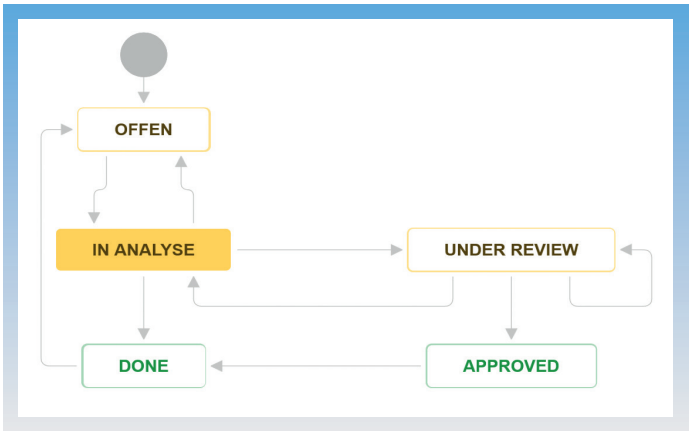

Bild 2: Behandlung der Incident-Massnahmen.

– Keine Datenschutzverletzung.
– Kosten spürbar, von aussen sichtbar.

Beträchtlich
Die Schadensauswirkungen können beträchtlich sein.
– Der finanzielle Schaden ist spürbar (bis CHF 1 Million).
– Der Imageverlust ist gross (schwere Kritik in den Medien)
– Ernsthafte negative Auswirkungen möglich.
– mögliche Datenschutzverletzung.
– Erhebliche Kosten sind zur Behebung notwendig.

Existenzbedrohend
Die Schadensauswirkungen können ein existenziell bedrohliches, katastrophales Ausmass erreichen.
– Der finanzielle Schaden bedroht die Existenz des Unternehmens (über 1 Million).
– Es ist mit bleibendem Schaden zu rechnen.
– Verlust von Leben/schwere Rufschädigung.
– mögliche Datenschutzverletzung.
– Erhebliche Störung des Betriebs, es besteht die Gefahr des Überlebens.

Behandlungsverfahren

Der Empfänger der Incident-Meldung zu einer Sicherheitsschwachstelle oder einem Ereignis analysiert die Information, klärt allenfalls fehlende Punkte ab, stellt nach Möglichkeit die Ursache(n) fest und schlägt Vorbeugungs- und Korrektur-Massnahmen vor.

Diese Massnahmen können in vier Kategorien unterteilt werden:

Geringer Vorfall
Wenn ein geringer Vorfall gemeldet wird, müssen folgende Schritte durchgeführt:
– Massnahmen zur Eingrenzung des Vorfalles einleiten.
– Analyse der Ursache(n) für den Vorfall.
– Korrekturmassnahmen für die Beseitigung der Ursache für den Vorfall einleiten.
– Information der vom Vorfall Betroffenen sowie an die Geschäftsleitung. Diese entscheidet, ob auch der Verwaltungsrat informiert werden muss.

Erheblicher Vorfall
Im Fall von erheblichen Vorfällen, die den Betrieb für eine inakzeptable Zeitperiode unterbrechen könnten, kommt ein Notfallplan als Teil des Business Continuity zum Tragen.

Datenschutzrelevanter Vorfall
Im Fall von datenschutzrelevanten Vorfällen muss eine umgehende Ist-Aufnahme durchgeführt werden.

Diese Aufnahme sollte durch den/die Datenschutzverantwortliche durchgeführt werden. Es muss unter allen Umständen verhindert werden, dass Daten verändert, manipuliert oder gar zerstört werden.

Handelt es sich um elektronische «Spuren», wird zuerst überprüft, ob der Vorfall mit internen Ressourcen und Wissen abgedeckt werden kann. Falls nicht, wird eine spezialisierte, forensische Firma beigezogen.

Die Behandlung der Incident-Massnahmen könnte gemäss folgendem Ablauf (Bild 2) durchgeführt werden. Die Prozess-Zustände sind wie folgt definiert:

– Offen
  Neu gemeldeter Incident, noch keine Bearbeitung.
– In Analyse
  Der Incident wird gerade untersucht.
– Under Review
  Die Lösung des Incidents wird überprüft.
– Approved
  Die Lösung wurde akzeptiert.
– Done
  Der Incident ist abgeschlossen.

Die Übergänge zwischen den Prozess-Zuständen sind wie folgt definiert:
– Offen -> In Analyse
  Incident wird nun behandelt.
– In Analyse -> Offen
  Die Behandlung des Incidents muss gestoppt werden (mit entsprechender Begründung).
– In Analyse -> Under Review
  Analyse abgeschlossen, Massnahmen sind eingeleitet.
– In Analyse -> Done
  Der Incident kann direkt abgeschlossen werden.
– Under Review -> In Analyse
  Die getroffenen Massnahmen sind nicht genügend (mit entsprechender Begründung).
– Under Review -> Under Review
  Eine weitere Kontrolle ist notwendig (Wechsel der verantwortlichen Person).
– Under Review -> Approved
  Massnahmen sind fertig umgesetzt.
– Approved -> Done
  Der Incident-Verantwortliche schliesst den Incident.
– Done -> Offen
  Sollte der Incident doch noch nicht erfolgreich abgeschlossen sein, kann er wieder geöffnet werden (mit entsprechender Begründung).

Vor dem Schliessen eines Incident-Tickets soll die angewendete Lösung einer Qualitätskontrolle unterzogen werden. Damit wird sichergestellt, dass der Incident tatsächlich gelöst worden ist und dass alle Informationen zur Lösung ausreichend dokumentiert sind.

Lernen aus Vorfällen

Wichtig ist, dass regelmässig die Vorfälle untersucht werden. Der CIO und/oder CISO muss alle geringeren Vorfälle vierteljährlich prüfen und jene, die sich wiederholen (oder solche, die sich bei der nächsten Wiederholung zu einem erheblichen Vorfall steigern könnten) entsprechend vermerken. Geeignete Schritte sind abzuleiten, damit sich diese nicht mehr wiederholen.

Fazit

Incidents gehören zum Firmen-Alltag dazu. Sei dies durch Unachtsamkeit der eigenen Mitarbeitenden, eine Verletzung durch einen Partner oder Lieferanten, ein Naturereignis oder ein Hacker, der auf das eigene Unternehmen abgesehen hat. Daher ist es wichtig, im Vorfeld geeignete Prozesse zu etablieren. Incidents sind so schnell wie möglich zu melden. Nach einer Analyse des Vorfalls können entsprechende Schritte eingeleitet werden. Ist der Normalbetrieb wiederhergestellt, ist die Arbeit noch nicht abgeschlossen. Es gilt die Ursachen zu eruieren und die Umgebung oder die Prozesse so zu gestalten, dass diese Art von Incident nicht nochmals vorkommen kann. So ist das Unternehmen gerüstet, sollte erneut ein Vorfall eintreten.

INFOS | KONTAKT
goSecurity AG
Schulstrasse 11
CH-8542 Wiesendangen

T +41 (0)52 511 37 37
www.goSecurity.ch
wisler@gosecurity.ch