Umgang mit Incidents in der heißen Phase

Global Communication Services

Woher kommt die Erfahrung?

Zum Unternehmen …

- … ein Team von 22 Digital Natives an den Standorten Berlin und Idstein.
- … entwerfen und realisieren Operations-Konzepte für Online-Plattformen jeglicher Größenordnung
- … begleiten Rechenzentren und Dienstleister bei Zertifizierungsprozessen nach ISO-27001 auf Basis IT-Grundschutz sowie PCI-DSS
- … realisieren überall auf der Welt die IT-Sicherheit bei Pre-Release-Events für einen der größten Videospielepublisher der Welt (Messen, Presse-Events etc.)
- … entwickeln sichere und skalierbare Online-Anwendungen im Enterprise-Umfeld

Zur Person …

- Stefan Siefert, Geschäftsführer
- Entwicklung von IT Sicherheits- und Betriebskonzepten seit 20 Jahren
- Berater in der Begleitung von Zertifizierungsprozessen nach ISO-27001 auf Basis IT-Grundschutz und PCI-DSS seit knapp 13 Jahren
- Immer noch externer IT-Sicherheitsbeauftragter für einzelne Kunden, um an operativen Entwicklungen dranzubleiben!

Sicherheitsvorfall! Und nun?

Was hilft, wenn der Ernstfall eintritt?

Ruhe bewahren! Wie?

- Klare Definition der Verantwortung und Rollen!
- Kategorisierung des Sicherheitsvorfalls
- Ansprechpartner und Kontaktpersonen müssen definiert sein!
- Schutzziele und Prioritäten müssen klar sein!
- Prozesse / Vorgehensweisen müssen definiert und präsent sein!
- Übersicht behalten!

Sicherheitsvorfall! Und nun?

Was kann man vorbereiten?

Nicht jeder Sicherheitsvorfall ist gleich „riskant“

- Sicherheitsvorfälle unternehmensspezifisch kategorisieren: Was ist ein einfacher Sicherheitsvorfall? Ein mittlerer? Ein schwerer? Ein Notfall?
- Wofür?
  - Zur richtigen Einschätzung der Priorität!
  - Richtige Kategorisierung erlaubt angemessene Eskalation!
  - Ein einfacher Sicherheitsvorfall erhält im Prozess vermutlich weniger Aufmerksamkeit als ein schwerer!
- Möglichst einfache Kriterien definieren
  - Kann jeder Service-Desk-Mitarbeiter „Imageschaden > 100.000 EUR“ bewerten?
  - Die ermittelte Kategorie des Sicherheitsvorfalls bestimmt ab dem ersten Kontaktpunkt das weitere Vorgehen

Aber wer kategorisiert den Sicherheitsvorfall?

- Häufige Herausforderung: Bereits im Service-Desk muss eine erste Einschätzung des Vorfalls erfolgen
  - Herausforderung: Wird hier eine zu niedrige Einschätzung vorgenommen, kann wertvolle Zeit verloren gehen ➔ pot. größerer Schaden!
  - Einfache Kriterien + Training!
  - Kontinuierliche Überprüfung der Einschätzung im weiteren Eskalationsverlauf
- Alternativ: Erster Eskalationsschritt für Sicherheitsvorfälle ist immer gleich hoch (kritisch) priorisiert und Sicherheitsvorfall wird sofort von der Risikomanagement-Seite / spezialisierter Stelle bewertet
  - Setzt gleiche Verfügbarkeit der spezialisierten Stelle voraus wie erstannehmende Stelle (bspw. Service-Desk)

Sicherheitsvorfall! Und nun?

Was kann man vorbereiten?

Prioritäten und Schutzziele festlegen

- Was sind die Risiken für das Unternehmen?
  - Verfügbarkeit von Diensten / Daten? Einhaltung von SLAs? / Welche Dienste bzw. Daten?
  - Verlust der Vertraulichkeit von kritischen Daten / Systemen? Welche Daten / Welche Systeme sind besonders schutzwürdig?
  - Datenschutzverstöße?
- Wie sind die Prioritäten der Schutzziele?
  - Lieber verfügbar als vertraulich?
  - Oder Vertraulichkeit um jeden Preis?
  - Kurzfristige Risikominimierung? Wie wichtig sind Beweise?
- Sinnvolle Dokumentation dieser Vorgaben, so dass sie im Ernstfall schnell und ggf. kleinteilig (system- / dienstbezogen) gefunden werden können ➔ bspw. in Asset-Management-Systemen hinterlegen?

Sicherheitsvorfall! Und nun?

Was kann man vorbereiten?

Verantwortung und Rollen festlegen

- Wer hat die Aufgabe (und Verantwortung) …
  - … an der Analyse und Lösung des Vorfalls aktiv zu arbeiten?
  - … die Übersicht zu behalten und die Einhaltung der Prozesse sicherzustellen?
  - … die Risikoeinschätzung / Kategorisierung des Sicherheitsvorfalls zu überprüfen?
  - … die Kommunikation mit Betroffenen (Stakeholder) zu koordinieren?
  - … die Kommunikation mit Betroffenen durchzuführen?
  - … eine Risikoentscheidung zu treffen?
  - … den Vorfall abschließend für bearbeitet / erledigt zu bewerten?
  - … den Vorfall und das Vorgehen zu dokumentieren?

Mehrere Hüte sind möglich, ABER …

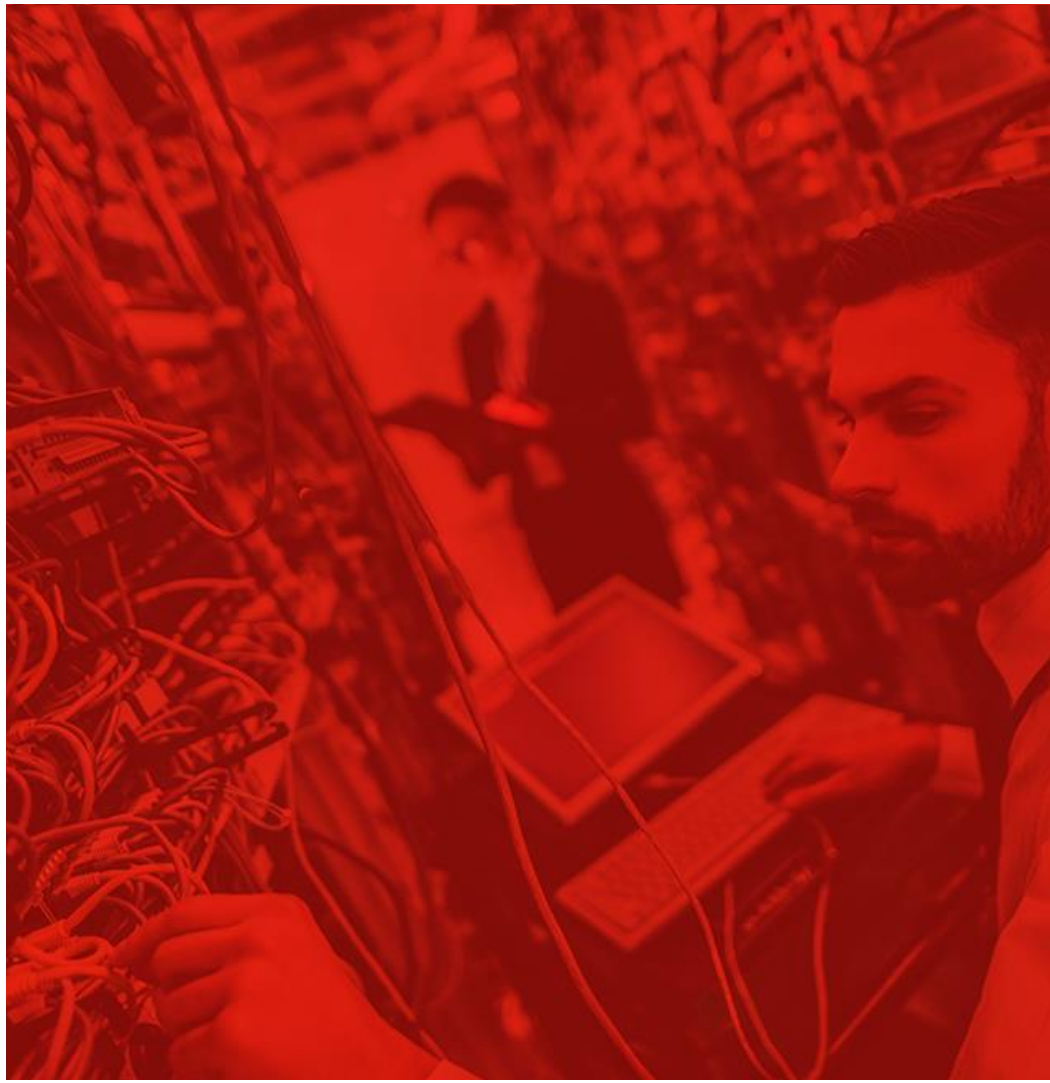
- … wer löst, sollte nicht für Kommunikation verantwortlich sein oder Kommunikation mit Betroffenen führen.
- … wer löst, behält selten den Prozess im Auge (Eskalation notwendig? Kommunikation notwendig?)
- …

Sicherheitsvorfall! Und nun?

Was kann man vorbereiten?

Spezialisten und Ansprechpartner kennen

- (Externe?) Spezialisten, die nicht Teil des Kernteams sind
  - IT-Forensiker?
  - Dienstleister-Kontakte für eingesetzte Lösungen (insb. Sicherheitslösungen wie Firewalls, Intrusion-Detection-Systeme etc.)?
  - Fachanwalt für IT- und Datenschutzrecht?
  - Datenschutzbeauftragter?
  - Spezialisierte Dienstleister (DDOS-Mitigation? Loganalyse? Datenwiederherstellung?)
- Wenn es externe sind … haben sie einen Rahmenvertrag? Garantierte Reaktionszeiten? Haben Sie das mal getestet?
- Ansprechpartner für Freigaben / Rücksprachen
  - Fachliche Ansprechpartner für Anwendungen, Daten und Systeme
  - Kunden?

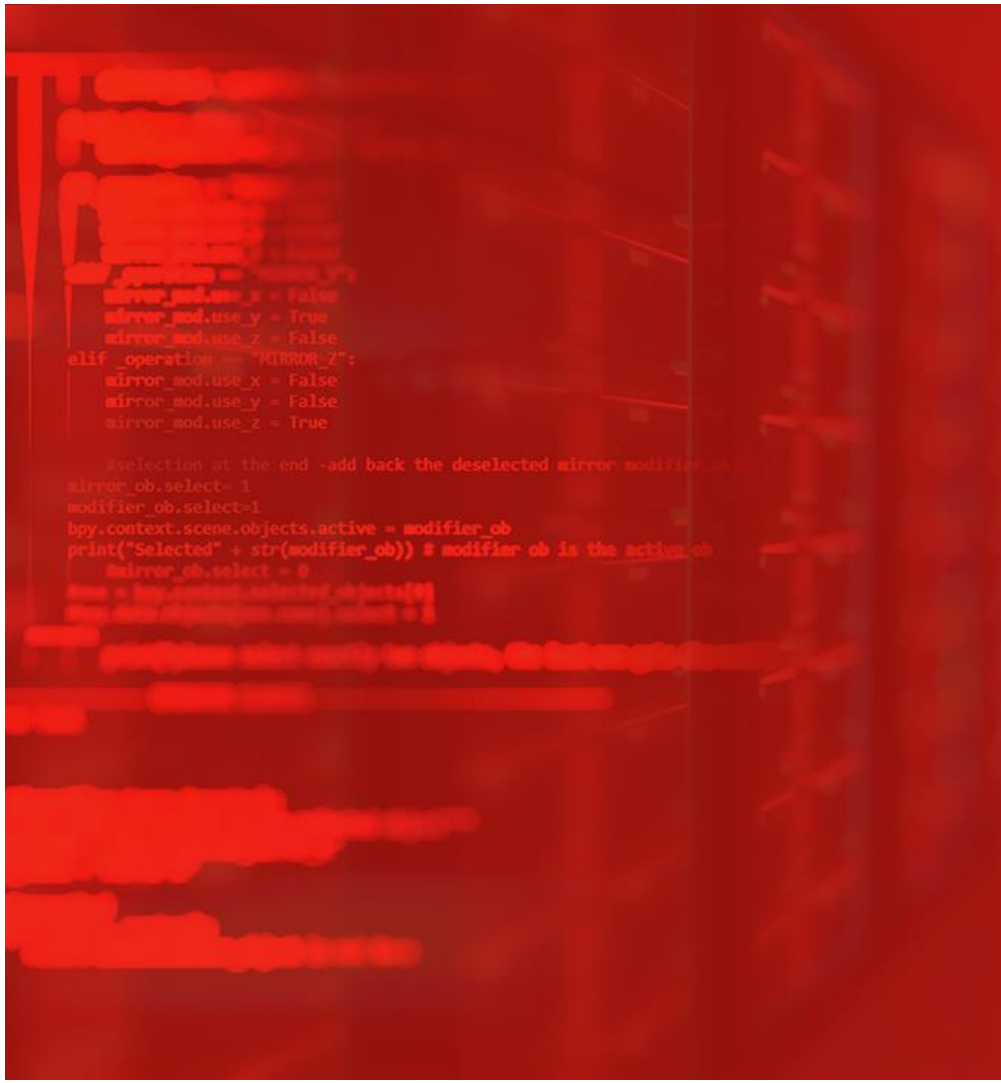


Sicherheitsvorfall! Und nun?

Was kann man vorbereiten?

Rahmenprozess(e) festlegen

- First Steps
  - Folgeschaden minimieren?
  - Wie wichtig ist eine Beweissicherung? **Hinweis:** Beweissicherung kann zur Reduktion von RECHTLICHEN Folgeschäden sehr wichtig sein!
- Kommunikationskonzept?
  - Wann / wie oft? ➔ Regelmäßigkeit empfohlen (stündlich, alle x Stunden)
  - Wie? ➔ Systemische Unterstützung? Push / Pull? Ist die Infrastruktur zur Kommunikation im Falle des Incidents verfügbar / vertrauenswürdig?
  - An wen? ➔ Woher kommen die Kontaktdaten der Betroffenen?
- Eskalationsprozess?
  - Wann muss eine Eskalation eintreten? An wen wird eskaliert und was sind die organisatorischen Folgen der Eskalation?



Sicherheitsvorfall! Und nun?

Was kann man vorbereiten?

Training, Training, Training

- Regelmäßigkeit
  - Wie oft ist sinnvoll?
  - Empfehlung: mindestens halbjährlich, besser kontinuierlich (siehe Praxisbeispiele)
- Zielgruppengerecht
  - Je nach Rolle im Prozess oder alle auf einmal?
  - Empfehlungen:
    - Auch Fachabteilungen müssen „trainiert“ werden. Nicht nur, wie sie Sicherheitsvorfälle erkennen und melden können, sondern auch durch welches Verhalten sie im Fall der Fälle die Behandlung des Sicherheitsvorfalls unterstützen können!
    - Unterschiedliche (knappe) Trainings für unterschiedliche Rollen + übergreifendes Zusammenspiel trainieren!
- Wie trainieren?
  - Trainieren und nicht dressieren!

Sicherheitsvorfall! Und nun?

Während des Vorfalls

Ruhe bewahren!

- Vorgehen nach Prozess!
- Wenn geht: kontinuierlich dokumentieren!
- Empfehlungen:
  - Darauf achten, keine Beweise (unbewusst) im Rahmen der Lösung des Sicherheitsvorfalles zu vernichten.
  - Wenn noch existent, konkretes Risiko schließen / reduzieren.
  - Dann Ursachenanalyse und Folgeprozesse
  - Separate Rollen mindestens für:
    - Umsetzung / technisches Doing
    - Steuerung des Vorfalls (Verantwortung)
    - Kommunikation mit Stakeholdern
  - Frühzeitige Einbindung des Datenschutzbeauftragten im Falle eines befürchteten Datenschutzverstoßes

Sicherheitsvorfall! Und nun?

Zwei unterschiedliche Ansätze aus der Praxis

RZ-Betreiber, flache Hierarchie, kleine Teams

- Weiter gefasste Prozesse und Vorgaben ➔ mehr Verantwortung und Entscheidungsgewalt bei den handelnden Personen
- Training auf den ersten Blick eher „regulär“
  - Quartalsweise Sensibilisierungen (kurzes Update-Training)
  - Halbjährlich bis jährlich (je nach Zielgruppe): Regeln und Prozesse („klassisches“ Training)
- Aber…
  - … hohe Integration der IT-Abteilung in Planungs- und Analyse-Prozesse zum betriebenen Information Security Management System
  - Dadurch stark verankertes Verständnis für „Hintergründe“ / „Reason why“
  - Hohe Identifikation mit den Prozessen und Regeln, da selber bei der Erstellung und Weiterentwicklung beteiligt
  - Sicherheitsprozess wird wirklich Teil der Service-DANN
  - Modell hat Probleme beim Skalieren und initial relativ hohe Personalkosten

Sicherheitsvorfall! Und nun?

Zwei unterschiedliche Ansätze aus der Praxis

Konzern, verteilte IT, viele Abteilungen

- Sehr strikte und detaillierte Prozesse / Wenig Entscheidungsspielraum für handelnde Personen
- Training in drei Intervallen
  - Wöchentlich: Einzelthema (fachlich, abteilungsspezifisch, dezentral, Teilnahme optional, mindestens 12 Teilnahmen im Jahr)
  - Monatlich: Planspiel abteilungsübergreifend (Zusammenarbeit)
  - Halbjährlich: Regeln und Prozesse („klassisches“ Training)
- Hat Gamification-Ansätze integriert
  - „Punkte“ für Training (Teilnahmen, Antworten, Lösungsbeitrag)
  - „Punkte“ für Prozesstreue / Lösungsqualität bei Vorfällen (u.a. können betroffene Fachabteilung am Ende Feedback geben, was zur Punkteverteilung indirekt genutzt wird)
  - Wettkampfcharakter („Bestenliste“, bei Sommerfest und Weihnachtsfest bekommen die drei Besten der Abteilung kleine Belohnungen)

FRAGEN SIE UNS

Stefan Siefert

(Geschäftsführer)

+49 6126 9375-241

s.siefert@global-communication.de

Global Global Communication Services GmbH
Walramstraße 26 • 65510 Idstein
Telefon +49 (0) 30 779 07 87 -00 • Telefax +49 (0) 30 779 07 87 -99
www.global-communication.de • info@global-communication.de