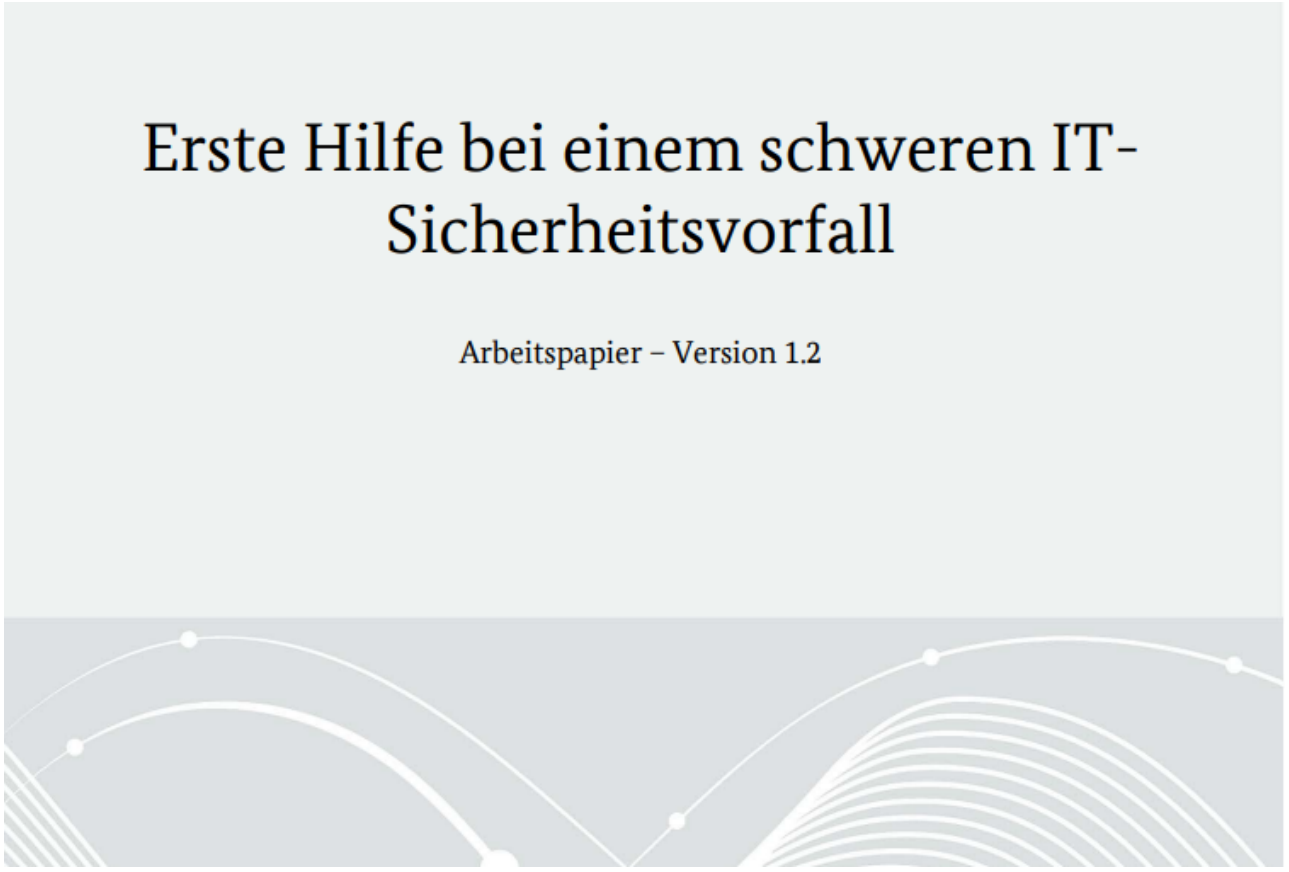
2024-07-11 Incident Management

- #LINK https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Internet-der-Dinge-Smart-leben/Smart-Home/Smarte-Ueberwachungskameras/smarte-ueberwachungskameras_node.html

IT-SEC



Incident Management

Organisatorische Maßnahmen

In diesem Kapitel werden generelle Maßnahmen und Empfehlungen für das Incident Management im Rahmen eines schweren IT-Sicherheitsvorfalls vorgestellt.

Stellen Sie sich drauf ein, dass Sie ggf. viele Tage lang (große) Teile Ihrer Dienstleistung nicht erbringen können oder Ihre Produktionsanlagen stillstehen (Erfahrungswerte bei vollständiger Kompromittierung: 2- 4 Wochen).

Richten Sie ein geeignetes Krisenmanagement (Kapitel 3.2) ein, das neben den technischen Wiederherstellungsaspekten (Kapitel 4) besonders die Kommunikation mit Ihren Stakeholdern, den Behörden und ggf. der Presse adressiert (Krisenkommunikation, Kapitel 3.3).

3.1 Vorfallsbewältigung als Projekt

Sollten Sie noch keine Erfahrung in der Bewältigung schwerer IT-Sicherheitsvorfälle haben, kann es sinnvoll sein, die Vorfallsbewältigung als Projekt aufzufassen und diese mit den Mitteln des Projektmanagements anzugehen.

Versuchen Sie die in Kapitel 3.2 genannten Maßnahmen des Krisenmanagements im Projektteam zu adressieren und umzusetzen.

Der Ablauf der Vorfallsbewältigung kann grob in drei Phasen eingeteilt werden.

- Phase 1: Analyse
  - Identifikation betroffener Systeme
  - Verhinderung weiterer Infektion und Verschlüsselung
  - Schadensfeststellung
    - Wer wurde alarmiert
    - Wer hat alarmiert
    - Wann wurde alarmiert
    - Wer wurde erreicht
    - Was ist das Resultat
  - Analyse der Schadprogramme
  -
- Phase 2: Übergangsbetrieb
  - Verhinderung weiterer Infektion und Verschlüsselung
  - Blockierung der Täterzugänge
  - Intensives Monitoring des Netzes
- Phase 3: Bereinigung
  - Konzeption / Umsetzung / Neustart
  - Weitere Sicherheitsmaßnahmen (neues Sicherheitskonzept)

Der Fokus dieses Dokumentes liegt darauf, Betroffene bei einem guten Einstieg in Phase 1 zu unterstützen.

3.2 Krisenstab

Wie bereits in der Vorbemerkung zu Kapitel 3 dargestellt kann der Vorfall Auswirkung auf Ihre Dienstleistungen und Produkte haben. Größere IT-Sicherheitsvorfälle benötigen neben operativtechnischen Bewältigungsmechanismen auch administrativ-organisatorische Maßnhamen. Diese werden im Themenkomplex des IT-Krisenmanagements zusammengefasst.

Hauptmerkmale der administrativ-organisatorischen Bewältigungsmechanismen sind:

- eine ebenen-übergreifende und interdisziplinäre Sichtweise,
- die Behandlung strategischer Fragestellungen und Themenfelder,
- die Kenntnis kritischer Geschäftsprozesse und deren Bewertung auf Managementebene,
- die Steuerung der internen und externen Kommunikation und
- weitreichende Entscheidungs- und Handlungskompetenzen.

Diese Merkmale (Anforderungen) sollten jederzeit durch Ihr Projektteam erfüllt werden und erfordern eine fortlaufende Selbstkontrolle zur Aufrechterhaltung der administrativ-organisatorischen Ausrichtung.

Binden Sie daher frühzeitig relevante interne Stellen ein, zum Beispiel in Form eines Krisenstabes:

- Leitungsebene als Leiter des Krisenstabes (nach Möglichkeit jedoch nicht „den Kopf“ der Institution),
    - Damit der Krisenstab auch formal die Unterstützung der Geschäftsführung hat, der Kopf des Unternehmens als Gesicht nach außen aber auch nicht überlastet wird.
    - IT-Leitung, o Als technischen Sachverstand für den Krisenstab, um operative Kräfte für die Arbeit freizuhalten.
    - Juristen, o Fragen zu Haftung, Strafanzeige, weitere rechtliche Aspekte.
    - Presse- und Öffentlichkeitsarbeit,
        - eine angemessene Krisenkommunikation nach innen und außen bewahrt die Reputation des Unternehmens, schützt Geschäftsbeziehungen und motiviert die Mitarbeiterinnen und Mitarbeiter
    - Datenschutzbeauftragte sowie
        - Für datenschutzrechtliche Fragen das wie Logging.
    - Personal- / Betriebsrat.
        - Wegen Zugriff auf Logdaten sowie personalrelevante Fragen wie Überstunden.

  Mögliche Punkte einer Sitzung des Krisenstabes finden Sie im Anhang 6.4.

  Planen Sie regelmäßige Beratungsphasen des Krisenstabes im Wechsel mit Arbeitsphasen.

  Sie benötigen nicht für alle Rollen des Krisenmanagements Personal aus der IT-Abteilung! Projektmanager und Bürofachkräfte können die nun dringend benötigen IT-Spezialisten bei vielen organisatorischen, planerischen, kommunikationsrelevanten oder logistischen Aufgaben unterstützen und entlasten. Holen Sie sich bei Bedarf Unterstützung durch einen erfahrenen externen Krisenmanager ins Haus, der Sie bei der Bewältigung des Vorfalls begleitet.

  Vermutlich müssen Sie kurzfristig das Active Directory (AD) bereinigen und mittel- bis langfristig neu aufsetzen. Prüfen Sie, ob an anderen Standorten oder in entfernten / separierten Unternehmensteilen nicht-betroffene ADs und (Teil-) Backups verfügbar sind. Richten Sie kurzfristig eine Projektgruppe ein, die - parallel zu Ihren Analysen und Eindämmungen - einen neuen Netzaufbau, insbesondere für kritische Geschäftsprozesse zur Aufrechterhaltung bzw. Wiederherstellung der Produktion, in einem segmentierten Bereich beginnt (ggf. mit externer Unterstützung).

  Kümmern Sie sich um Ihre Mitarbeiterinnen und Kollegen, die zur Bewältigung der Lage Höchstleistungen erbringen.
  Sorgen Sie für Entlastungen
  - (Getränke, Snacks, ggf. Taxinutzung, Hotel statt langer Heimfahrt).
  - Achten Sie auf Anzeichen der Überlastung und lösen Sie sie geeignet aus der Krisensituation, damit sie den Kopf wieder frei bekommen und frische Energie tanken können ("Dienst- / Schichtplanung").
  - Beachten Sie, dass alles was Sie für Ihre Kollegen tun, kostengünstiger ist als ein verlängeter Produktionsausfall durch Fehler oder Überlastung!
  - Denken Sie aber auch an Mitarbeiter, welche durch den Ausfall von IT wenig bis gar nicht mehr arbeiten können.
  - Versuchen Sie für diese sinnvolle Arbeiten zu finden und hierüber einen Notbetrieb einzurichten. Diese Mitarbeiter könnten auch noch (ggf. entgegen der Unternehmensrichtlinien) lokal gespeicherte Daten und Arbeitshilfen haben. Mit einem Hinweis „wird nicht geahndet“ könnten Sie hier noch wertvolle Daten finden. Stellen Sie kurzfristig eine zuverlässige Erreichbarkeit für interne und externe Kommunikation

sicher. Dies umfasst sowohl Telefone, im Zweifel kurzfristig beschaffte Prepaid-Handys. Gleichermaßen sollten E-Mail Adressen und falls nötig auch eine kurzfristig erstellte Übergangs-Webseite erstellt werden