Allianz für Cyber-Sicherheit

MASSNAHMEN-KATALOG ZUM NOTFALLMANAGEMENT

- Fokus IT-Notfälle -

Um eine ganzheitliche Cyber-Sicherheits-Strategie verfolgen zu können, sollten Sie ein Informations-Sicherheits-Management-System (ISMS) nach anerkannten Standards etablieren. Ein ISMS wird sinnvoll von einem Notfallmanagement/Business Continuity Management (BCM) ergänzt. Dieser Managementprozess obliegt den Notfallbeauftragten und beinhaltet u. a. die Erstellung folgender Produkte:

- einer Leitlinie zum Notfallmanagement,
- Entwicklung eines Notfallvorsorgekonzeptes sowie
- eines Notfallhandbuches.

Ein vollständiges Notfallmanagement/BCM beschränkt sich nicht nur auf den Ausfall der Ressource Informationstechnik, sondern betrachtet auch den Ausfall der Ressourcen Personal, Infrastruktur (z. B. Gebäude und Anlagen) und Dienstleister. Der Maßnahmenkatalog beschränkt sich auf IT-Notfälle und richtet sich in erster Linie an Geschäftsführer und IT-Verantwortliche in kleinen und mittelständischen Unternehmen, die

- ihren Einstieg in diese Thematik gestalten möchten,
- sich den vielfältigen Bedrohungen aus der voranschreitenden Digitalisierung stellen wollen und
- durch ein IT-Notfallmanagement die Cyber-Resilienz ihres Unternehmens erhöhen wollen.

VORBEREITUNG

- Bestimmen Sie Beauftragte für die Belange der Informationssicherheit und des Notfallmanagements in Ihrem Unternehmen, nach Möglichkeit nicht in Personalunion. Beide arbeiten bei IT-Notfällen eng zusammen.
- Stellen Sie in dem Zusammenhang sicher, dass Ihnen Ihre individuellen und fallbezogenen Erstmaßnahmen im IT-Notfall vorliegen (u. a. Alarmierungs- und Meldewege).
- Identifizieren Sie zeitkritische Geschäftsprozesse und Assets (Kronjuwelen) im Rahmen eines strukturierten Prozesses (Empfehlung: Business Impact Analyse (BIA)) und setzen Sie Schutzmaßnahmen für diese priorisiert um.
- Klären Sie mit Ihren IT-Dienstleistern, für welche IT-Vorfälle Unterstützung gewährt werden kann (Distributed-Denial-of-Service (DDoS), Ransomware, Online-Betrug, Hacking der Webpräsenz, u. a.).
- Identifizieren Sie Dienstleister, die Sie bei IT-Notfällen geeignet unterstützen können und nehmen Sie im Vorfeld Kontakt zu diesen auf.
- Fertigen Sie eine Liste mit allen Ansprechpartnern und treffen Sie Vorabsprachen mit diesen (u. a. Erreichbarkeit, Verfügbarkeit, ggf. Service-Level-Agreement).
- Legen Sie Regeln zur Kommunikation nach innen und außen fest. Eine erfolgreiche Presse- und Öffentlichkeitsarbeit während eines IT-Notfalls kann einen evtl. Imageschaden erheblich begrenzen. Auf diesem Gebiet gibt es Unterstützungsangebote von Dienstleistern. Prüfen Sie vorab, ob Sie solche Angebote in Anspruch nehmen möchten und nehmen Sie frühzeitig Kontakt auf.

Falls Sie bei einem Cyber-Angriff externe Unterstützung benötigen, können Sie auf folgende Angebote zurückgreifen:

Auf den Webseiten des BSI finden Sie qualifizierte Dienstleister.

Sie können sich auch an die Ansprechpartner Ihrer Industrie- und Handelskammer vor Ort wenden.

Bundesweit stehen speziell ausgebildete „IT-Sicherheitsbotschafter“ der Handwerkskammern den Betrieben zur Seite.

- Implementieren Sie, falls möglich, aktive Überwachungsmaßnahmen (Monitoring) für Ihre IT-Landschaft. Dies könnte auch durch IT-Dienstleister geschehen (Security-Operations-Center-as-a-Service). Beachten Sie Bestimmungen des Datenschutzes und machen Sie Ihre Maßnahmen transparent für die Belegschaft (Betriebs-/Personalrat).
- Üben Sie IT-Notfall-Szenarien jeglicher Art (IT-Ausfälle, Cyber-Angriffe, etc.) und lassen Sie Ihre IT-Infrastruktur auf Angreifbarkeit prüfen (Penetrationstest). Durch Übung gewinnen Sie an Professionalität und Kompetenz.
- Schulen und sensibilisieren Sie Ihr gesamtes Personal im Umgang mit den IT-Systemen und Cyber-Bedrohungen und zum Verhalten im IT-Notfall.
- Führen Sie vertiefende Schulungen für diejenigen durch, die mit der Bewältigung von IT-Notfällen betraut sind.
- Denken Sie an die grundlegenden Schutzmaßnahmen für Ihre IT-Infrastruktur:
  - Installieren Sie regelmäßig Patches und Sicherheitsupdates.
  - Setzen Sie Programme zum Schutz vor Schadsoftware ein und aktualisieren Sie diese regelmäßig.
  - Nutzen Sie Firewalls, um Ihre Netze und Rechner vor Angriffen von außen zu schützen.
  - Ändern Sie in jedem Fall Standard-Passwörter in jeglichen Komponenten und nutzen Sie sichere Passwörter und, wenn möglich, Zwei-Faktor-Authentisierung.
  - Erstellen Sie regelmäßig Sicherheitskopien (Backups) Ihrer Daten, um vor Verlust geschützt zu sein und testen Sie regelmäßig deren Wiederherstellung.
- Inventarisieren und dokumentieren Sie Ihre IT-Infrastruktur (u. a. Netzplan).
- Vergeben Sie restriktive Benutzerrechte an Ihren IT-Systemen. Schützen Sie besonders privilegierte Benutzerkonten und Administrator-Konten z. B. durch Zwei-Faktor-Authentisierung.
- Gehen Sie ebenso restriktiv bei der Vernetzung Ihrer IT-Systeme vor (Netzsegmentierung).
- Bereiten Sie Meldewege vor, damit Sie Ihren Meldepflichten während des IT-Notfalls fristgerecht nachkommen können.

BEREITSCHAFT

- Überprüfen Sie in regelmäßigen Abständen den Sicherheitsstatus Ihrer IT-Systeme.
- Stellen Sie sicher, dass Ihr Personal den richtigen Ansprechpartner für IT-Notfälle kennt und handlungssicher ist. An dieser Stelle empfehlen wir den Einsatz der IT-Notfallkarte.
  - Bestimmen Sie den für Ihr Unternehmen angemessenen Erstkontakt für IT-Notfälle. Das kann Ihr geschultes Personal oder ein IT-Dienstleister sein.
  - Gewährleisten Sie die Erreichbarkeit zu den relevanten Arbeitszeiten Ihres Unternehmens. Cyber-Angriffe werden nicht selten freitagnachmittags festgestellt.
- Bedenken Sie, dass nicht jede Fehlfunktion von Hardware oder Software ein Cyber-Angriff ist. Gleichwohl kann der Ausfall eines IT-Systems auf einen Cyber-Angriff zurückzuführen sein.

BEWÄLTIGUNG

Den Einstiegspunkt (Patient-Zero; das erste kompromittierte System) eines Cyber-Angriffs festzustellen, ist aufwändig, aber gleichzeitig wertvoll. Außerdem sorgen nur eine vollständige Erhebung des Ausmaßes der Kompromittierung und die vollständige Beseitigung für einen sicheren Wiederanlauf der Geschäftsprozesse.

- Bewahren Sie Ruhe.
- Kontaktieren Sie sofort alle Ansprechpartner in der Organisation, die Sie zur Bewältigung brauchen.
- Befragen Sie ggf. betroffene Nutzer über Beobachtungen und Aktivitäten.
- Kontaktieren Sie einen IT-Dienstleister, der Ihnen bei der Bewältigung des Notfalls behilflich sein kann.
- Sammeln und sichern Sie System-Protokolle, Log-Dateien, Notizen, Fotos von Bildschirminhalten, Datenträger und andere digitale Informationen am besten, bevor Sie auf den Systemen eine Analyse starten. Diese Daten sind im Fall einer forensischen Auswertung essentiell (auch Strafanzeige).
- Dokumentieren Sie fortwährend alle mit dem IT-Notfall im Zusammenhang stehenden Sachverhalte.
- Prüfen Sie die Kontaktaufnahme zur Zentralen Ansprechstelle für Cybercrime (ZAC) beim Landeskriminalamt Ihres Bundeslandes (nur für Unternehmen) und die Erstattung einer Anzeige.
- Prüfen Sie zusätzlich eine freiwillige Meldung des IT-Notfalls an die Meldestelle der Allianz für Cyber-Sicherheit.
- Beachten Sie Meldepflichten: Datenschutz, KRITIS, etc.

Weitere Infos auf der Webseite der Allianz für Cyber-Sicherheit:

Liste der Zentralen Ansprechstellen für Cybercrime der Polizeien der Länder und des Bundes

Onlineformular für freiwillige Meldungen eines IT-Notfalls

NACHBEREITUNG

- Überwachen und monitoren Sie Ihr Netzwerk und Ihre IT-Systeme nach einem Cyber-Angriff besonders intensiv auf ungewöhnliche Aktivitäten, um sicherzustellen, dass Ihre Systeme wieder einwandfrei funktionieren und um einen möglichen Wiederholungsversuch rechtzeitig zu erkennen.
- Lessons Learned; prüfen Sie, ob es Regelungen, Maßnahmen oder Prozesse gibt, die optimiert und abgesichert werden müssen.
- Halten Sie Ihre Dokumentation zum Notfallmanagement stets auf dem aktuellen Stand.
- Schließen Sie durch den IT-Notfall aufgedeckte Schwachstellen und Sicherheitslücken.
- Entwickeln Sie Ihre IT-Sicherheitsarchitektur – Ihre Systeme, Netzwerke und Dokumente – kontinuierlich weiter.

Der IT-Grundschutz des BSI bietet ausführliche Informationen für die Gestaltung von Informationssicherheit und Notfallmanagement.

Das Dokument ist ein gemeinsames Produkt nachfolgender Organisationen: Bundeskriminalamt, Charter of Trust, Deutscher Industrie- und Handelskammertag e.V., eco – Verband der Internetwirtschaft e.V., Initiative Wirtschaftsschutz, Nationale Initiative für Informations- und Internet-Sicherheit e.V., VOICE - Bundesverband der IT-Anwender e.V., Allianz für Cyber-Sicherheit des Bundesamtes für Sicherheit in der Informationstechnik