Einstieg ins IT-Notfallmanagement für kleinere und mittelständische Unternehmen (KMU)

1. Vorbereitung

Die nachfolgenden Aufgaben sollten Sie bearbeiten, um im Fall der Fälle geeignet auf einen IT-Notfall vorbereitet zu sein:

- Bestimmen Sie Beauftragte für die Belange der IT-Sicherheit und des Notfallmanagements.
- Stellen Sie sicher, dass Ihnen Ihre individuellen Erstmaßnahmen bei IT-Vorfällen vorliegen (u. a. Alarmierungs- und Meldewege im Unternehmen).
- Identifizieren Sie zeitkritische Geschäftsprozesse und Assets (Kronjuwelen) und setzen Sie Schutzmaßnahmen für diese priorisiert um.
- Klären Sie mit Ihren IT-Dienstleistern, bei welcher Art von IT-Vorfällen diese unterstützen können.
- Identifizieren und kontaktieren Sie ggf. weitere IT-Dienstleister, die Sie bei der Bewältigung unterstützen können.
- Fertigen Sie eine Liste mit Ansprechpartnern und deren Erreichbarkeiten und Verfügbarkeiten.
- Legen Sie Regeln zur Kommunikation nach innen und außen fest, Stichwort: Presse- und Öffentlichkeitsarbeit.
- Implementieren Sie aktive Überwachungsmaßnahmen (Monitoring) für Ihre IT-Landschaft. Beachten Sie den Datenschutz.
- Üben Sie IT-Notfallszenarien.
- Lassen Sie Ihre IT-Infrastruktur auf Angreifbarkeit prüfen (Penetrationstests).
- Schulen und sensibilisieren Sie Ihr gesamtes Personals.
- Denken Sie an grundlegende Schutzmaßnahmen:
  - Installieren Sie regelmäßig und unverzüglich 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 und nutzen Sie sichere Passwörter und, wenn möglich, Zwei-Faktor-Authentisierung.
  - Erstellen Sie regelmäßig Sicherheitskopien (Backups) Ihrer Daten, und testen Sie regelmäßig deren Wiederherstellung.
- Inventarisieren Sie Ihre IT-Infrastruktur (u.a. Netzplan).
- Vergeben Sie restriktive Benutzerrechte an Ihren Systemen.
- Vernetzen Sie Ihre Systeme restriktiv (Netzsegmentierung).
- Bereiten Sie Meldewege für externe Meldepflichten vor (Datenschutz, KRITIS etc.).

2. Bereitschaft

Um jederzeit einem IT-Notfall entgegnen zu können beachten Sie die nachfolgenden Punkte:

- Überprüfen Sie regelmäßig den Sicherheitsstatus Ihrer Systeme.
- Gewährleisten Sie, dass Ihr Personal den richtigen Ansprechpartner für IT-Notfälle kennt (Einsatz der IT-Notfallkarte). Bestimmen Sie einen angemessenen Erstkontakt für IT-Notfälle und gewährleisten Sie die Erreichbarkeit.

3. Bewältigung

Zur Bewältigung eines IT-Notfalls helfen Ihnen die folgenden Punkte:

- Kontaktieren Sie alle Ansprechpartner in der Organisation, die Sie zur Bewältigung brauchen.
- Befragen Sie betroffene Nutzer über Beobachtungen und Aktivitäten.
- Kontaktieren Sie IT-Dienstleister, die Ihnen bei der Bewältigung helfen können.
- Sammeln und sichern Sie Systemprotokolle, Logdateien, etc.
- Dokumentieren Sie Sachverhalte, die mit dem Notfall in Zusammenhang stehen könnten.
- Prüfen Sie Kontaktaufnahmen mit den ZACs der Polizeien, sowie freiwillige Meldungen an die ACS.
- Vermuten Sie als Urheber einen fremden Nachrichtendienst, wenden Sie sich an die Verfassungsschutzbehörden.
- Beachten Sie Meldepflichten.

4. Nachbereitung

Ein aufgetretener IT-Notfall muss auch nachbereitet werden. Hinweise geben die folgenden Punkte:

- Schließen Sie durch den IT-Notfall aufgedeckte Schwachstellen und Sicherheitslücken.
- Überwachen und Monitoren Sie Ihr Netzwerk und Ihre IT-Systeme im Nachgang besonders gründlich.
- Lessons Learned: Überprüfen Sie bestehende Regelungen, Prozesse und Maßnahmen, optimieren Sie diese gegebenenfalls.
- Halten Sie Ihre Dokumentationen zum Notfallmanagement auf dem aktuellen Stand.
- Entwickeln Sie Ihre IT-Sicherheitsarchitektur weiter.

Hinweis: Bei diesem Dokument handelt es sich um eine Kurzfassung des „Maßnahmenkatalog zum Notfallmanagement – Fokus IT-Notfälle“ welcher weitere Erläuterungen und Verweise enthält.

Stand: Mai 2021