Der Leitfaden für Ihre Sicherheit.

A1 Business

Bedrohungen aus dem Cyberraum ändern sich von Jahr zu Jahr, Cyberangriffe nehmen weltweit zu - auch österreichische Unternehmen sind zunehmend betroffen. Daher ist es wichtig, sich optimal vorzubereiten und im Ernstfall richtig zu reagieren - dieser Leitfaden hilft Ihnen dabei.

Profitieren Sie von der Expertise und den Erfahrungen unserer A1 Experten im Bereich Cyber Defense.

Vorbereitung:

- **Notfallkontakte bereithalten:** Im Ernstfall muss es schnell gehen. Stellen Sie sicher, dass wichtige Kontakte - z.B. zum IT-Administrator, Sicherheitsdienstleister oder relevanten Behörden – stets griffbereit sind. Halten Sie diese Informationen sowohl digital (z.B. auf dem Mobiltelefon) als auch als Ausdruck am Arbeitsplatz bereit, um schnell handeln zu können.
- **Notfallplan entwickeln:** Ein strukturierter Notfallplan legt fest, wie im Ernstfall reagiert wird: Wer ist verantwortlich? Welche Kommunikationswege gibt es? Welche Eskalationsstufen sind vorgesehen? Der Plan muss leicht zugänglich sein – sowohl digital als auch in gedruckter Form.
- **Kritische Systeme identifizieren:** Für eine effektive Reaktion müssen geschäftskritische Systeme und Datenquellen klar benannt sein. Nur so lassen sich Risiken gezielt erkennen und priorisieren.
- **Awareness-Training:** Regelmäßige Schulungen der Mitarbeitenden helfen, Sicherheitsvorfälle frühzeitig zu verhindern. Themen wie Phishing, Passwortsicherheit und das Melden verdächtiger Vorfälle sollten regelmäßig aufgefrischt werden.

Bedrohung identifizieren:

- **Erstanalyse:** Stellen Sie fest, ob es sich um einen echten Vorfall handelt – typische Hinweise sind ungewöhnliche Logins, verdächtige E-Mails oder Systemausfälle. Halten Sie erste Beobachtungen sofort fest. Vermeiden Sie voreilige Maßnahmen wie das Abschalten von System, um keine Spuren zu verlieren.
- **Reaktionskette vorbereiten:** Informieren Sie umgehend die zuständigen Personen laut Notfallplan. IT, Geschäftsführung und ggf. externe Partner müssen schnell eingebunden werden. Rollen und Verantwortlichkeiten sollten vorher definiert sein, um Verzögerungen zu vermeiden.
- **Informationen vorbereiten:** Sammeln Sie alle verfügbaren Daten zum Vorfall: Was ist betroffen, wann wurde es entdeckt, was wurde bisher beobachtet? Diese Infos helfen bei der Einschätzung und für spätere Meldungen an Behörden oder Partner. Dokumentation ist Pflicht.

Reaktion und Eindämmung:

- **Systeme isolieren:** Trennen Sie betroffene Systeme sofort vom Netzwerk, um eine Ausbreitung zu verhindern. Vermeiden Sie jedoch unüberlegte Neustarts oder das Löschen von Daten. Ziel ist Eindämmung, nicht sofortige Bereinigung.
- **Erstmaßnahmen dokumentieren:** Alle eingeleiteten Sofortmaßnahmen sollten strukturiert dokumentiert und den zuständigen Stellen zur Verfügung gestellt werden. Das umfasst z.B. Uhrzeit, beobachtetes Verhalten, betroffene Systeme und erste Reaktionen. Eine saubere Dokumentation erleichtert die forensische Analyse und hilft, Fehler zu vermeiden.
- **Behörden & Kommunikation:** Wenn personenbezogene Daten betroffen sind, muss die Datenschutzbehörde innerhalb von 72 Stunden informiert werden. Bereiten Sie eine klare interne und ggf. externe Kommunikation vor. Bleiben Sie sachlich und vermeiden Sie Schuldzuweisungen, bevor die Fakten geklärt sind.
- **Zugang sichern:** Ändern Sie Passwörter, besonders für Administratoren und sensible Zugänge. Deaktivieren Sie betroffene Konten temporär, falls nötig. Prüfen Sie, ob weitere Konten kompromittiert wurden.

A1 unterstützt Sie bei der Cybersicherheit – von Awareness-Trainings über Darknet-Analysen bis zur Incident Response. Kontaktieren Sie unsere Cyber Defense Experts für individuelle Lösungen.