Digitale Sicherheit

Checkliste Cyberangriff

Ein Cyberangriff kann für Unternehmen verheerende Folgen haben. Ein gut vorbereiteter Notfallplan hilft, im Ernstfall schnell und effektiv zu reagieren. Unsere Checkliste zeigt Ihnen die wichtigsten Schritte auf.

Sofortmassnahmen

- ☐ Bei Verdacht auf einen Cyberangriff ist es entscheidend, die betroffenen Systeme umgehend vom Internet und anderen Netzwerken zu trennen. Schalten Sie auch das WLAN aus.
- ☐ Informieren Sie Ihre Mitarbeitenden über den Vorfall und geben Sie klare Anweisungen zum weiteren Vorgehen.
- ☐ Benachrichtigen Sie unverzüglich die intern oder extern verantwortliche Person für IT-Sicherheit sowie Ihre Notfall-Organisation, falls vorhanden.
- ☐ Ideal ist, wenn die Liste mit den Kontaktdaten auch in gedruckter Form aufbewahrt wird, damit Sie sofort handeln können, wenn die IT blockiert ist.

Passwörter und Zugangsdaten

- ☐ Ändern Sie umgehend alle Passwörter von Diensten, die auf den betroffenen Geräten verwendet wurden.
- ☐ Verwenden Sie für jeden Dienst ein einzigartiges, starkes Passwort.
- ☐ Aktivieren Sie, wo möglich, die Zwei-Faktor-Authentifizierung für zusätzlichen Schutz.

Informations- und Anzeigepflichten

- ☐ Wenn Sie eine Cyberversicherung abgeschlossen haben, informieren Sie umgehend Ihren Versicherer. Erstatten Sie Anzeige bei der Polizei. Dies ist wichtig für die Strafverfolgung und kann bei der Schadensregulierung helfen.
- ☐ In der Schweiz besteht eine Meldepflicht für Cyberangriffe. Informieren Sie das Nationale Zentrum für Cybersicherheit (NCSC) innerhalb von 24 Stunden über den Vorfall.
- ☐ Falls anzunehmen ist, dass ein Vorfall «voraussichtlich zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person führen kann», muss man überdies dem eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) die Verletzung der Datensicherheit (Data Breach) melden.
- ☐ Informieren Sie die betroffenen Personen.

Schadenermittlung und -begrenzung

- ☐ Lassen Sie Ihre Systeme von IT-Experten begutachten, um das Ausmass des Schadens festzustellen.
- ☐ Identifizieren und schliessen Sie die Sicherheitslücken, die den Angriff ermöglicht haben.
- ☐ Nutzen Sie Back-ups, um Ihre Daten wiederherzustellen. Stellen Sie sicher, dass die Back-ups nicht ebenfalls kompromittiert wurden.

Kommunikation

- ☐ Halten Sie Ihre Mitarbeitenden regelmässig über den Fortschritt der Situation auf dem Laufenden.
- ☐ Informieren Sie bei Bedarf Kunden, Lieferanten und andere Stakeholder über den Vorfall und mögliche Auswirkungen.

Prävention für die Zukunft

- ☐ Halten Sie alle Systeme und Software stets auf dem neuesten Stand und führen Sie regelmässige Updates durch.
- ☐ Sorgen Sie dafür, dass das vom Datenschutzgesetz geforderte Bearbeitungsverzeichnis immer aktuell ist.
- ☐ Implementieren Sie eine robuste Back-up-Strategie mit regelmässigen Sicherungen und Tests zur Wiederherstellung.
- ☐ Verwenden Sie Firewalls, VPNs und segmentieren Sie Ihr Netzwerk, um die Ausbreitung von Angriffen zu erschweren.
- ☐ Führen Sie regelmässige Schulungen zur Cybersicherheit durch, um das Bewusstsein Ihrer Mitarbeitenden zu schärfen.
- ☐ Wichtig: Behandeln Sie alles, was die IT-Sicherheit betrifft, als zyklischen Prozess. Das gilt einerseits für die interne Handhabung. Es empfiehlt sich aber auch ein periodisches IT-Security-Assessment, bei dem ein unabhängiger externer Partner die Infrastruktur, die Applikationen und die Organisation einer kritischen Prüfung unterzieht.