Fachhochschule Nordwestschweiz
Hochschule für Wirtschaft

Schützen Sie sich vor Cyber-Attacken!

Kleine Checkliste zum Prüfen Ihrer Cyber-Risiken und Hinweise, wie Sie diese verringern können.

Beurteilen Sie die Abhängigkeiten Ihrer Geschäftsprozesse und IT-Infrastruktur.

? Was wären die **Folgen** bei Ausfall Ihres Systems oder der Nicht-Verfügbarkeit Ihrer digitalen Daten?
? Welche Massnahmen zur Reduzierung der Folgen könnten Sie ergreifen?
? Welche Alternativen gibt es im «Ernstfall» falls Ihre Systeme, Ihre Infrastruktur ausfällt?
☐ Erarbeiten Sie auf der Grundlage dieser Antworten einen für Sie umsetzbaren **Notfallplan**. Identifizieren Sie Ihre geschäftskritischen Daten und legen Sie für diese besondere Schutzmassnahmen fest.

Regeln Sie die Verantwortlichkeiten.

? An wen wenden sich Ihre Mitarbeitenden bei einem IT-Sicherheitsvorfall, einer entdeckten Cyber-Attacke? Ist die Person allen Mitarbeitenden bekannt?
? Welche Schritte werden im Falle einer Cyber-Attacke von wem unternommen?
☐ Erarbeiten Sie einen **Reaktionsplan** (Incident Response) wo die verantwortlichen Personen benannt sind.
☐ Überprüfen und testen Sie die Wirksamkeit Ihres Reaktionsplans und Ihrer Backups und nehmen Sie bei Bedarf Anpassungen vor.
! Falls Sie mit externen IT-Servicepartnern zusammenarbeiten, müssen die Zuständigkeiten zwischen Ihrem Unternehmen und die der Servicepartner geklärt und dokumentiert sein. Haftungsfragen sollten vertraglich festgehalten sein.

Sensibilisieren Sie Ihre Mitarbeitenden.

? Sind Ihre Mitarbeitenden im Umgang mit allfälligen Gefahren wie potentiellen Cyber-Attacken geschult?
☐ Bieten Sie Schulungs- und Sensibilisierungsprogramme für Ihre Mitarbeitenden an.

Identifizieren Sie Ihre sensiblen Daten und definieren Sie Richtlinien für den Umgang, die Speicherung, Archivierung, etc.

? Welche (Klassen von) digitalen Daten verarbeiten Sie in Ihrem Unternehmen?
? Wie werden digitale Daten gespeichert und an wen übermittelt?
? Wie geben Sie vertrauliche Daten weiter?
☐ Führen Sie eine Richtlinie zur Klassifizierung Ihrer Daten ein und gewährleisten Sie eine konsequente Umsetzung (Daten, welche für die Kontinuität des Betriebs unabdingbar sind, müssen besonders geschützt werden).

Stellen Sie die Sicherheit von Ihrer IT-Infrastruktur sicher (allenfalls mit Hilfe von externen IT-Servicepartnern).

? Werden Sicherheitsupdates automatisch installiert?
? Werden Ihre Unternehmensdaten regelmässig gesichert?
? Sind die Endgeräte Ihrer Mitarbeitenden nach dem aktuellen Stand der Technik geschützt?
☐ Gewährleisten Sie, dass Sicherheitsupdates automatisch auf all Ihren Servern und Endgeräten installiert sind.
☐ Halten Sie auch sonstige Geräte wie Drucker, Router usw. stets auf dem neuesten Stand.
☐ Richten Sie regelmässige Datensicherungen ein und gewährleisten Sie eine durchgängige Umsetzung.
☐ Sorgen Sie dafür, dass jeder Computer Ihres Netzwerkes mit einem aktuellen Virenschutz und Firewall geschützt ist.
☐ Nutzen Sie für externe Zugriffe zum Firmennetz (z.B. Reisen/Home Office) ein VPN (Virtual Private Network) mit Zwei-Faktor-Authentifizierung. Dies gilt auch für externe Servicepartner.
☐ Definieren Sie einen Prozess für die Ausserbetriebnahme von Geräten Ihrer IT-Infrastruktur, einschliesslich der zuverlässigen Entfernung vertraulicher Informationen. Bei Zugriffen von externen Dienstleistern empfehlen wir Ihnen eine Netzwerksegmentierung zu etablieren.

Verwalten Sie die Zugriffsberechtigungen des Personals.

? Arbeiten Ihre Mitarbeitenden mit Administratorenrechten?
☐ Gewähren Sie Ihrem Mitarbeitenden nur die minimal erforderlichen Zugriffsrechte für die jeweilige Arbeitsaufgabe.
☐ Beschränken Sie das Installationsrecht für nicht unternehmensnotwendige Software.

Führen Sie eine Passwort-Richtline (Policy) ein.

? Welche Richtlinien und Technologien für sichere Passwörter gibt es in Ihrem Unternehmen?
☐ Definieren Sie verpflichtende Richtlinien für Passwörter und stellen Sie die konsequente Umsetzung sicher.
☐ Etablieren Sie eine Zwei-Faktor-Authentifizierung für die Zugriffe auf Ihre IT-Infrastruktur und Ihre digitalen Daten.
☐ Führen Sie am besten eine Software zum managen von Passwörtern ein.
! Ein sicheres Passwort muss aus mindestens 14 Zeichen, Gross- und Kleinbuchstaben, Zahlen und Sonderzeichen bestehen. Passwörter sollten nicht mehrfach genutzt werden. Es ist ratsam, Passwörter regelmässig zu ändern. Passwörter und Zugangsdaten dürfen niemals weitergegeben werden.

www.fhnw.ch/wirtschaft

www.digitaltrust-competence.ch