SySTEM AG @data®
Funktionierende IT-Lösungen

IT Security Tage 2023

Diese 10 Punkte sollten sie umsetzen

01

Sensibilisierung der Mitarbeiter

Schulen Sie Ihre Mitarbeiter regelmäßig über die Grundlagen der IT-Sicherheit, einschließlich bewusster Nutzung von Passwörtern, Identifizierung von Phishing-Versuchen und dem Umgang mit verdächtigen E-Mails oder Dateien.

02

Starke Passwörter verwenden

Stellen Sie sicher, dass Ihre Mitarbeiter starke Passwörter verwenden, die aus einer Kombination von Buchstaben, Zahlen und Sonderzeichen bestehen. Passwörter sollten regelmäßig aktualisiert werden und die Verwendung von Mehr-Faktor-Authentifizierung (MFA) sollte gefördert werden.

03

Aktualisierte Software

Halten Sie Ihre Betriebssysteme, Anwendungen und Sicherheitssoftware auf dem neuesten Stand, um von den neuesten Sicherheitsupdates und Patches zu profitieren. Regelmäßige Aktualisierungen minimieren die Anfälligkeit für bekannte Sicherheitslücken.

04

Netzwerksicherheit

Implementieren Sie eine Firewall, um unerwünschten Netzwerkzugriff zu blockieren, und verwenden Sie Verschlüsselungsprotokolle (z. B. VPN, ZTNA) für den sicheren Zugriff auf Ihr Netzwerk von externen Standorten.

05

Datensicherung und Wiederherstellung

Führen Sie regelmäßige Backups Ihrer wichtigen Daten durch und testen Sie die Wiederherstellung, um sicherzustellen, dass Ihre Daten im Falle eines Ausfalls, einer Beschädigung oder eines Angriffs wiederhergestellt werden können.

06

Zugriffskontrolle

Implementieren Sie ein Berechtigungsmanagement, um sicherzustellen, dass Mitarbeiter nur auf die Informationen und Systeme zugreifen können, die für ihre Aufgaben erforderlich sind. Nutzen Sie auch die Prinzipien des „Least Privilege“, indem Sie den Zugriff auf sensible Daten und Systeme einschränken.

07

E-Mail-Sicherheit

Implementieren Sie Filtermechanismen, um Spam, Phishing-Versuche und schädliche E-Mails zu erkennen und zu blockieren. Schulen Sie Mitarbeiter, wie sie verdächtige E-Mails identifizieren und melden können.

08

Physische Sicherheit

Schützen Sie Ihre IT-Infrastruktur vor unbefugtem Zugriff, indem Sie Serverräume, Netzwerkschränke und andere sensible Bereiche physisch sichern. Stellen Sie sicher, dass nur autorisiertes Personal Zugang zu diesen Bereichen hat.

09

Incident Response-Plan

Entwickeln Sie einen detaillierten Plan, wie Sie auf Sicherheitsvorfälle reagieren, diese bewerten und darauf reagieren. Klare Verantwortlichkeiten und Handlungsanweisungen im Falle eines Sicherheitsvorfalls helfen, Schäden zu minimieren und die Wiederherstellung zu beschleunigen.

10

Regelmäßige Überprüfung und Schulung

Führen Sie regelmäßige interne Audits durch, um sicherzustellen, dass Sicherheitsrichtlinien eingehalten werden, und bieten Sie kontinuierliche Schulungen an, um das Bewusstsein zu steigern.