consol

BASIS-MAßNAHMEN ZUR IT-SICHERHEIT

CONSOL CHECKLISTE

Damit Sie beim Thema IT Security den Überblick behalten, haben wir Ihnen im Folgenden einige Basismaßnahmen zur IT-Sicherheit zusammengestellt.

1. Inventarisieren Sie Ihr IT-System

Um geeignete Abwehrmaßnahmen in Ihrem Unternehmen umzusetzen, ist es wichtig, einen vollständigen Überblick über die eingesetzten IT-Systeme und Systemtypen zu erhalten.

Leitfragen für eine Inventarisierung sind:

- Welche Betriebssysteme und Anwendungen werden auf Servern und stationären/mobilen Clients eingesetzt?
- In welchen Versionen werden diese Betriebssysteme und Anwendungen betrieben?
- Welche Patchstände haben die eingesetzten Betriebssysteme und Anwendungen?
- Welche Server werden mit welchem Funktionsumfang betrieben?

2. Sichern Sie Ihre Netzübergänge ab

Die Absicherung von Netzübergängen ist ein wesentlicher Faktor bei der Abwehr von Cyberangriffen. Identifizieren Sie in einem ersten Schritt Anzahl und Art der vorhandenen Übergänge. Von kritischer Bedeutung sind Zugänge, die die Schutzmaßnahmen der allgemeinen Netzinfrastruktur umgehen können wie beispielsweise:

- individuelle DSL-Zugänge oder
- verschlüsselte Kommunikationswege wie z. B. VPN-Verbindungen

Sorgen Sie für eine am Schutzbedarf unterschiedlicher Bereiche orientierte Netzsegmentierung und eine Minimierung der externen Netzübergänge. Die minimierte Zahl an Netzübergängen muss mit einem adäquaten Sicherheitsgateway abgesichert werden. Durch technische Schnittstellenkontrolle auf Servern und IT-Systemen ist eine Umgehung des Sicherheitsgateways auszuschließen.

In Zeiten von Mobile Work ist die Absicherung mobiler Zugänge unabdingbar. Die Gefahr von Verlust oder Diebstahl ist hoch. Die Berechtigung für User in mobilen IT-Systemen sollte daher auf ein Minimum beschränkt werden. Planen Sie proaktive Maßnahmen, die im Ernstfall schnell umgesetzt werden können wie z. B. die Sperrung des Netzwerkszugangs oder die Fernlöschung des mobilen IT-Systems.

3. Setzen Sie durchgängig auf Schutzprogramme

Setzen Sie Schutzprogramme gegen Schadsoftware auf allen Systemen durchgängig ein, allen voran:

- Sicherheitsgateway

- E-Mail-Server
- Dateiserver
- Stationäre und mobile Arbeitsplatzsysteme

4. Vermeiden Sie offene Sicherheitslücken

Die meisten IT-Angriffe basieren auf Schwachstellen in veralteter Software, die bereits in neueren Versionen behoben wurden. Schützen Sie Ihre IT-Infrastruktur durch effizientes Patchmanagement, das zeitnahe Software-Updates einschließt. Informieren Sie sich stets bei Herstellern über Sicherheits-Updates Ihrer genutzten Produkte. So profitieren Sie von erweiterten Schutzmaßnahmen.

5. Stellen Sie eine sichere Interaktion mit dem Internet sicher

Alle Vorgänge, bei denen Dienste oder Daten aus dem Internet abgerufen werden, sind abzusichern. Setzen Sie auf:

- Sichere Browser:
- Sichere E-Mail-Anwendungen
- Sichere Darstellung von Dokumenten

6. Werten Sie Logdaten regelmäßig aus

Das rasche Erkennen von nicht offensichtlichen Sicherheitsvorfällen und langfristig angelegten Angriffen sollte Teil Ihres IT-Konzeptes sein. Eine wichtige Rolle spielt die regelmäßige Auswertung von Logdaten. Legen Sie deshalb fest, welche Logdaten auf welchen Systemen erfasst werden müssen, um Angriffe frühzeitig zu erkennen. Hauptquelle für diese Logdaten sind das Sicherheitsgateway und die eingesetzten Betriebssysteme. Weitere Hinweise im Hinblick auf Angriffsversuche liefern Informationen zu anormalen Verhaltensmustern von IT-Systemen, beispielsweise in Zusammenhang mit Systemabstürzen.

7. Informationssicherheit: Bleiben Sie up-to-date

Versorgen Sie sich stets mit aktuellen Informationen zur Cyber-Sicherheit! Verlässliche Informationsquellen sind u. a.:

- Warn- und Informationsmeldungen eines etablierten CERT (Computer Emergency Response Team)
- Warn- und Informationsmeldungen zu industriellen Steuerungsanlagen
- Lagebilder von staatlichen Stellen, Herstellern und Sicherheitsdienstleistern

- Warnungen & Sicherheitsempfehlungen von Sicherheitsgruppen der jeweiligen Hersteller z. B. Microsoft Security Response Center.

8. Bereiten Sie sich auf Sicherheitsvorfälle vor

Üben Sie im Vorfeld die Bewältigung von Sicherheitsvorfällen. So proben Sie, wie Sie im Ernstfall Geschäftsabläufe wiederherstellen können. Denken Sie daran, auch die Wiederherstellung zu testen.

9. Stellen Sie eine sichere Authentisierung sicher

Die Authentisierung mittels Nutzername und Passwort bietet oft nur ungenügend Schutz. Setzen Sie deshalb auf eine Zweifaktor-Authentisierung. Hier müssen sich die User mittels einer Kombination von zwei unterschiedlichen und voneinander unabhängigen Komponenten identifizieren.

Trennen Sie die Authentisierungsdaten für verschiedene Aufgaben. Unterschiedliche Rollen erfordern unterschiedliche Authentisierungsdaten. Achten Sie darauf, eine klare Trennung zwischen den Konten von Administratoren und anderen Nutzern sicherzustellen.

10. Führen Sie nutzerorientierte Maßnahmen durch

Sämtliche technische Vorkehrungen bringen nichts, wenn die eigenen Mitarbeitenden nicht hinlänglich sensibilisiert wurden. Angestellte sollten sowohl spezifische Schulungen als auch regelmäßige, kurze Updates zu aktuellen Themen und zur Wissensauffrischung erhalten.

Folgende Checkliste fasst die Basismaßnahmen zur IT-Sicherheit zusammen:

☐ Der Bedrohungsgrad der eigenen IT-Infrastruktur wurde evaluiert.

☐ Sämtliche Netzübergänge wurden identifiziert und hinreichend abgesichert.

☐ Die Infektion mit Schadprogrammen wurde mit wirksamen Maßnahmen unterbunden.

☐ Die IT-Systeme wurden inventarisiert.

☐ Offene Sicherheitslücken auf IT-Systemen werden vermieden.

☐ Eine Interaktion mit dem Internet findet nur über abgesicherte Komponenten statt.

☐ Logdaten werden zentral erfasst und regelmäßig ausgewertet.

☐ Der Informationsfluss zu allen sicherheitsrelevanten Themen ist innerhalb des Unternehmens sichergestellt.

☐ Die Organisation ist auf die Bewältigung von Sicherheitsvorfällen vorbereitet.

☐ Die Mechanismen zur Authentisierung erschweren einen Missbrauch durch Dritte.

- ☐ Zur Sicherstellung der IT-Sicherheit im Unternehmen stehen ausreichend interne Ressourcen zur Verfügung. Externe Dienstleister werden bei Bedarf eingebunden.
- ☐ Angestellte werden in Fragen der IT Security qualifiziert und sensibilisiert.
- ☐ Je nach Aufgabe werden nutzenorientierte Maßnahmen zur Rollentrennung durchgesetzt.
- ☐ In den sozialen Netzwerken wird entsprechend der sicherheitsrelevanten Vorkehrungen agiert.
- ☐ Bei höherem Schutzbedarf werden Penetrationstests durchgeführt.

ConSol
Consulting & Solutions Software GmbH

St.-Cajetan-Straße 43
D-81669 München
Tel.: +49-89-45841-100
vertrieb@consol.de
www.consol.de
Folgen Sie uns auf LinkedIn:
@consol-software-gmbh

ConSol
Austria Software GmbH

Maysedergasse 2/25
A-1010 Wien, Österreich
Tel.: +43-1-9971392
info-austria@consol.com
www.consol-software.at
Folgen Sie uns auf LinkedIn:
@consol-austria-software-gmbh