Security Workshop in a Box

Machen Sie den Sicherheitscheck: modular – zielorientiert – budgetschonend

Sicher ist nicht sicher genug

»Security Workshop in a Box« ist ein Dienstleistungsprodukt der Medialine AG. Das Ziel des Workshops ist es, Ihnen aufzuzeigen, in welchen Bereichen Ihrer IT-Security noch Handlungsbedarf besteht. »Security Workshop in a Box« enthält verschiedene Gesprächsleitfäden und Vorlagen mit dem unsere technischen Mitarbeiter zusammen mit Ihnen Ihre IT-Security betrachten und den Bedarf ermitteln. Wir zeigen Ihnen dezidiert auf, welche IT-Sicherheitsrisiken in Ihrem Unternehmen bestehen und bieten Ihnen Lösungen an, welche Ihre IT sicherer gestalten.

Der Workshop ist modular gestaltet. Das heißt, Sie entscheiden, welche Aspekte Ihrer IT-Security betrachtet werden sollen. So haben Sie direkten Einfluss darauf, wieviel Sie in die IT-Sicherheit Ihres Unternehmens investieren möchten. In den Modulen ist ein Zeitenschlüssel hinterlegt. Durch Addition der Zeiten wird der Gesamtaufwand pro Modul berechnet. Jedes Modul hat folgende Inhalte: Aufgaben, Fragen an den Kunden, Zeiten und Ergebnis.

Zielsetzung

Mit Hilfe der Fragen wird geprüft, inwieweit Sie sich bereits Gedanken über die IT-Sicherheit gemacht haben und ob gewisse Voraussetzungen bereits erfüllt sind. Bei Fragen, die eine Dokumentation erfordern, kann es sinnvoll sein, auch einige dieser Dokumente gemeinsam zu betrachten. Zum einen kann damit überprüft werden, ob die Dokumentation aktuell ist oder ob hier Bedarf eines Re-Designs besteht. Zum anderen kann bei nicht vorhandener Dokumentation (nach Absprache mit Ihnen) frühzeitig eine solche erstellt werden.

Ergebnis

Als Ergebnis des Security Workshops wird eine Handlungsempfehlung zur Verbesserung Ihrer IT-Sicherheit erstellt. Es können sowohl organisatorische als auch technische Empfehlungen sein. Ergibt die Untersuchung ein unvertretbares Restrisiko, muss auf einen Anschluss des jeweiligen Netzes an dasInternet bzw. sonstige unsichere Netze verzichtet werden.

Wir informieren Sie immer über eventuelle Restrisiken, wenn die von Ihnen gewünschten Schutzmaßnahmen realisiert wurden. So können Sie in Zukunft weiter darauf reagieren und Ihre IT-Security gegebenenfalls sukzessive verbessern.

Die Workshop-Module in der Übersicht

Wir beraten – Sie entscheiden: Wo sehen Sie Handlungsbedarf, welcher Bereich ist unternehmenskritisch und wie hoch ist das zur Verfügung stehende Budget.

Stellen Sie sich aus den folgenden fünf Modulen einen individuell auf die Bedürfnisse Ihres Unternehmens zugeschnittenen Security-Workshop in a Box zusammen.

Modul Network Security

Inhaltlicher Leistungsauszug:

- Bestandsaufnahme aller Systeme
  (Firewall, Modem, Server, Bridge, Router, Switche) Netztopologie, Dokumentation Firewall-Software, Check Wartungsverträge, Dokumentation, Reaktionsszenarien & Netzintegration, Firewall als Gateway
- Firewall & Router
  aktueller Patchstand, Softwareversion, Hardware-Maintenance, Zugriffe über persönliche Adminzugänge, Protokollierung Konfigurationsänderungen
- Switche
  aktuelle Firmware, Hardware-Maintenance, Spanning Tree-Konfiguration, Zugriffsmöglichkeiten

Modul E-Mail Security

Inhaltlicher Leistungsauszug:

- Bestandsaufnahme aller Systeme
  (Server, Mail, Gateway, Antispam, Antivirus) Dokumentation Funktionseinstellung E-Mail Server, Rechte, Authentisierung, Check Wartungsverträge, Dokumentation Reaktionszenarien & Netzintegration Mail Relay, Gateway, Fax-/Modem-/Mailserver
- E-Mail Server
  aktueller Patchstand, supportete Software & OS, Hardware-Maintenance, Konfiguration Empfangsconnectoren, Verschlüsselung verwendet & eingerichtet, Hardware-Monitoring
- Mail Gateway
  aktueller Patchstand & Firmware, Hardware-Maintenance, Hardware-Monitoring
- Antispam & Antivirus
  aktueller Patchstand Gateway, Softwareversion, Hardware-Maintenance, E-Mail Prüfung, Empfangausschluss schadhafter E-Mails, Hardware-Monitoring
- Active Directory
  Personalisierung E-Mail Administratoren

Modul Backup/Data Loss Prevention

Inhaltlicher Leistungsauszug:

- Bestandsaufnahme aller Systeme
  (Server, Backup, Proxy, Backup-Target, Bandlaufwerk) Dokumentation Funktionseinstellung Backup-systeme, Wiederherstellungsprozesse, Authentisierung, Check Wartungsverträge, Dokumentation Reaktionsszenarien & Backup-Targets

- Backupserver & ggf. Proxy
  aktueller Patchstand, supportete Software & OS, Hardware-Maintenance, Fehler Backup-jobs, Einbindung Backuptarget, Verschlüsselung eingerichtet, Hardware-Monitoring

- Backup-Target
  aktueller Patchstand & Firmware, Softwareversion, Hardware-Maintenance, Hardware-Monitoring

- Bandlaufwerke
  aktueller Patchstand Laufwerk, Softwareversion, Hardware-Maintenance, Hardware-Monitoring

Modul Data Protection

Inhaltlicher Leistungsauszug:

- Bestandsaufnahme aller Systeme
  (Antivirenserver), Dokumentation Antivirensysteme, Funktionseinstellung, Kontrollprozesse, Authentisierung, Check Wartungsverträge, Dokumentation Reaktionsszenarien

- Antivirenserver
  aktueller Patchstand, supportete Software & OS, Systemsicherung durch Firewall, aktuelle Clientrichtlinien, alle Clients überwacht, Aktualisierung & Update Virensignaturen, Benachrichtigung bei Virenfund

Modul Archivierung

Inhaltlicher Leistungsauszug:

- Bestandsaufnahme aller Systeme
  (Archivierungssystem) Dokumentation Funktionseinstellung Archivierungsprozesse, Kontrollprozesse, Authentisierung, Check Wartungsverträge, Dokumentation Reaktionsszenarien

- Archivierungssystem
  aktueller Patchstand, Konfiguration Archivierungssystem, Aktualisierung & Update Virensignaturen, Benachrichtigung bei Virenfund