Lieferantenfragebogen Cyber Security

Name _____

Adresse _____

_____

Bitte wählen Sie eine der zu jeder Frage vorgegebenen Auswahlmöglichkeiten. Sie können zusätzliche Kommentare und weitere Anlagen hinzufügen.

1. **Unbekannte Geräte**
   Identifizieren bzw. blockiere Sie unbekannte Geräte in Ihrem Netzwerk?
   - ☐ Nein
   - ☐ Ja, identifizieren
   - ☐ Ja, identifizieren und blockieren

   Kommentar _____

   Anlagen _____

2. **Freigegebene Software**
   Pflegen Sie eine Liste freigegebener Software, und wenn ja, beschränken Sie die Möglichkeit, dass Anwender andere Software installieren?
   - ☐ Nein
   - ☐ Ja, Pflege einer Liste
   - ☐ Ja, Pflege einer Liste und Beschränkungen

   Kommentar _____

   Anlagen _____

3. **Verwundbarkeits-Management**
   Betreiben Sie ein Verwundbarkeits-Management, das auf bekannte Verwundbarkeiten auf Ihren Systemen scannt, und das die Verantwortung zur Behebung Ihren Mitarbeiten zuweist?
   - ☐ Nein
   - ☐ Ja, für Clients
   - ☐ Ja, für Server
   - ☐ Ja, für Clients und Server

   Kommentar _____

   Anlagen _____

OTTO FUCHS KG, Postfach 1261, 58528 Meinerzhagen, Germany
T. +49 2354 73-0, info@otto-fuchs.com

4. **Sicherheitspatches vom Hersteller**
Welcher Prozentsatz Ihrer Clients und Sever laufen mit einem Betriebssystem, für das der Hersteller noch Sicherheitspatches liefert?

- ☐ Weniger als 80%
- ☐ 81% - 90%
- ☐ 91% - 95%
- ☐ 96% - 100%

Kommentar _____

Anlagen _____

5. **Patch Frequenz**
Wie häufig installieren Sie Sicherheitspatches auf Clients und Servern?

- ☐ Jährlich oder seltener
- ☐ Halbjährlich
- ☐ Quartalsweise
- ☐ Monatlich oder öfter

Kommentar _____

Anlagen _____

6. **Passwort-Policy**
Wählen Sie eine Option, die Ihrer bestehenden Passwort-Policy am besten entspricht.

- ☐ Keine Passwort-Policy
- ☐ Länge und Komplexität
- ☐ Länge, Komplexität und Änderungsintervall
- ☐ Länge, Komplexität, Änderungsintervall und Wiederverwendung

Kommentar _____

Anlagen _____

7. **Zugriffsschutz für Clients**
Wer hat administrativen Zugriff auf Clients?

- ☐ Alle User
- ☐ Alle User nach Bedarf, dauerhaft
- ☐ Alle User nach Bedarf, temporär
- ☐ Alle IT-Mitarbeiter

Kommentar _____

Anlagen _____

8. Zugriffsrechte

Wie werden Zugriffsrechte auf Systemen, Anwendungen und Daten gewährt?

- ☐ Zugriff wird vom Eigentümer oder anderen Usern gewäht
- ☐ Zugriff wird von IT gewährt
- ☐ Zugriff wird nach Genehmigung vom Eigentümer durch IT gewährt
- ☐ Zugriff wird nach Genehmigung vom Eigentümer durch eine Gruppe von Rechte-Administratoren gewährt

Kommentar _____

Anlagen _____

9. Internetzugriff / Inhaltsfilter

Wie werden Internetzugriff und Inhalte von Unternehmensrechnern aus kontrolliert?

- ☐ User haben unbeschränkten Zugriff
- ☐ Zugriff ist nach Inhaltsklassen und Notwendigkeit beschränkt
- ☐ Zugriff ist beschränkt und schadhafte Seiten werden automatisch blockiert
- ☐ Zugriff ist auf eine Liste von Sites beschränkt, die benötigt und sicher sind
- ☐ User haben keinen direkten Internetzugriff

Kommentar _____

Anlagen _____

10. Backup und Recovery

Wählen Sie eine Option, die Ihre Backup und Recovery Umgebung am besten umschreibt.

- ☐ Es gibt keine Backups
- ☐ Backups werden bei Bedarf erstelle, z. B. vor Upgrades, etc.
- ☐ Backups werden regelmäßig erstellt
- ☐ Backups werden regelmäßig erstellt, Restores werden getestet um sicherzustellen, dass Systeme wiederhergestellt werden können

Kommentar _____

Anlagen _____

11. Backup Speicherung

Wie werden Backups gespeichert?

- ☐ Es gibt keine Backups
- ☐ Backups werden auf Netzwerk Shares gesichert, die im selben Netz wie die zu sichernden Geräte liegen.
- ☐ Backups sind auf Tape, virtuellem Tape, etc.
- ☐ Backups sind auf separaten Disks, die mit den Live Systemen verbunden bleiben.
- ☐ Backups sind auf Removable Medien oder Disks, die sonst nicht mit dem Live-System verbunden sind.

Kommentar _____

Anlagen _____

12. Hardware Inventur

Wählen Sie die Option, die Ihre Inventur von Hardware (Clients, Server, Netzte, Geräte, etc.) am besten beschreibt.

- ☐ Kein Inventur
- ☐ Manuell gepflegte Inventur
- ☐ Automatisch befüllte Inventur
- ☐ Automatisch befüllte Inventur, neue Geräte werden automatisch erkannt

Kommentar _____

Anlagen _____

13. Fernzugriff

Wie funktioniert der Fernzugriff in Ihrer Organisation?

- ☐ Es gibt keinen Fernzugriff
- ☐ Fernzugriff nur für E-Mail, Kalender, etc.
- ☐ Fernzugriff auf das Netzwerk, Anmeldung mit Benutzername und Passwort
- ☐ Fernzugriff auf das Netzwerk, Anmeldung mit zertifikatsbasierter Multi-Faktor-Authentifizierung
- ☐ Fernzugriff auf das Netzwerk, Anmeldung mit SMS, Token oder App basierter Multi-Faktor-Authentifizierung

Kommentar _____

Anlagen _____

14. Verwaltung von Wechselträgern

Wie verwalten Sie Wechseldatenträger (USB, …)?

- ☐ Wechseldatenträger sind ohne Beschränkung erlaubt
- ☐ Wechseldatenträger werden auf der Basis von Ausnahmen erlaubt
- ☐ Wechseldatenträger müssen freigegebene verschlüsselnde Geräte sein
- ☐ Wechseldatenträger müssen freigegebene verschlüsselnde Geräte sein, sie dürfen nur in Ausnahmefällen genutzt werden
- ☐ Wechseldatenträger sind verboten

Kommentar _____

Anlagen _____

15. Netzwerk Design

Select the option which best describes your organisations network design.

- ☐ In general, all systems (workstations, servers, machines) can talk to each other. A "flat" network

☐ Servers and workstations are isolated, facilities/factory/other systems can generally interact with many servers and workstations

☐ Servers and workstations are isolated, facilities/factory/other systems are only able to interact with a small set of required systems

☐ Servers, workstations, and other systems are isolated with virtualized networking,
micro segmentation, etc

Kommentar _____

Anlagen _____

16. Drahtlose Netze

Wie sichern Sie die drahtlosen Netze Ihrer Organisation?

☐ WEP

☐ WPA

☐ WPA2 PSK

☐ WPA2 RADIUS

☐ Kein Wireless Netz

Kommentar _____

Anlagen _____

17. Sensibilisierungsprogramm für Informationssicherheit

Wie lässt sich Ihr Sensibilisierungsprogramm für Informationssicherheit (Security Awareness Programm) am besten beschreiben?

☐ Kein Awareness Programm

☐ Das Programm umfasst einen der Bereiche (Erkennen von Social Engineering, Umgang mit sensiblen Daten, Gründe für ungewollten Datenverlust, Phishing, Identifizierung und Meldung von Sicherheitsvorfällen)

☐ Das Programm umfasst zwei der Bereiche (Erkennen von Social Engineering, Umgang mit sensiblen Daten, Gründe für ungewollten Datenverlust, Phishing, Identifizierung und Meldung von Sicherheitsvorfällen)

☐ Das Programm umfasst drei der Bereiche (Erkennen von Social Engineering, Umgang mit sensiblen Daten, Gründe für ungewollten Datenverlust, Phishing, Identifizierung und Meldung von Sicherheitsvorfällen)

☐ Das Programm umfasst alle Bereiche (Erkennen von Social Engineering, Umgang mit sensiblen Daten, Gründe für ungewollten Datenverlust, Phishing, Identifizierung und Meldung von Sicherheitsvorfällen)

Kommentar _____

Anlagen _____

18. Umgang mit Informationssicherheitsvorfällen

Was beschreibt Ihren Umgang mit Informationssicherheitsvorfällen (= Incident Response Programm) am besten?

- ☐ Kein Incident Response Programmm
- ☐ Dokumentierter Incident Response Plan
- ☐ Dokumentierter Incident Response Plan und dediziertes Personal
- ☐ Dokumentierter Incident Response Plan und dediziertes Personal sowie regelmäßige Tests und Übungen

Kommentar _____

Anlagen _____

19. Tests

Wählen Sie eine Option, die Ihr Penetrations-Testprogramm am besten beschreibt.

- ☐ Kein Penetrations-Testprogramm
- ☐ Ein Penetrations-Testprogramm ist eingeführt
- ☐ Ein Penetrations-Testprogramm ist eingeführt und regelmäßige Tests finden statt
- ☐ Ein Penetrations-Testprogramm ist eingeführt und regelmäßige Tests finden statt; die Ergebnisse werden bis zur Behebung nachverfolgt

Kommentar _____

Anlagen _____

Erstellt von _____

Datum _____ Unterschrift _____

CEO/CIO/CISO _____

Datum _____ Unterschrift _____