OTTO FUCHS

Lieferantenfragebogen Cyber Security

Lieferantenname _____

Lieferantenadresse _____

_____

_____

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

1. Unbekannte Geräte

Identifizieren bzw. blockieren Sie unbekannte Geräte in Ihrem Netzwerk?

- ☐ Nein
- ☐ Ja, identifizieren
- ☐ Ja, indentifizieren und blockieren

Kommentar
Anhänge

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 Beschränkung

Kommentar
Anhänge

3. Verwundbarkeits-Management

Betreiben Sie ein Verwundbarkeits-Management, dass auf bekannte Verwundbarkeiten auf Ihren Systemen scannt, und dass die Verantwortung zur Behebung Ihren Mitarbeitern zuweist?

- ☐ Nein
- ☐ Ja, für Clients
- ☐ Ja, für Server
- ☐ Ja, für Clients und Server

Kommentar
Anhänge

4. Sicherheitspatches vom Hersteller

Welcher Prozentsatz Ihrer Clients und Server laufen mit einem Betriebssystem, für das der Hersteller noch Sicherheitspatches liefert?

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

Kommentar
Anhänge

5. Patch Frequenz

Wie häufig installieren Sie Sicherheitspatches auf Clients und Servern?

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

Kommentar
Anhänge

6. Passwort- Policy

Wählen Sie die 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
Anhänge

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
Anhänge

8. Zugriffsrechte

Wie werden Zugriffsrechte auf Systeme, Anwendungen und Daten gewährt?

- ☐ Zugriff wird vom Eigentümer oder anderen Usern gewährt
- ☐ 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
Anhänge

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
Anhänge

10. Backup und Recovery

Wählen Sie die Option, die Ihre Backup & Recovery Umgebung am besten beschreibt.

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

Kommentar
Anhänge

11. Backup Speicherung

Wie werden Backups gespeichert?

- [ ] Es gibt keine Backups
- [ ] Backups werden auf Nezwerk 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
Anhänge

12. Hardware Inventur

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

- [ ] Keine Inventur
- [ ] Manuell gepflegte Inventur
- [ ] Automatisch befüllte Inventur
- [ ] Automatisch befüllte Inventur, neue Geräte ewrden automatisch erkannt.

Kommentar
Anhänge

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 or App- basierter Multi Faktor Authentifizierung

Kommentar
Anhänge

14. Verwaltung von Wechseldatenträgern

Wie verwalten Sie Wechseldatenträgern (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
Anhänge

15. Netzwerk Design

Welche Option beschreibt Ihr Netzdesign am besten?

- [ ] Generell können alle Geräte miteinander kommunizieren (Client, Server, Maschinen) Ein flaches Netz.
- [ ] Server und Clients sind isoliert, Einrichtungen, Maschinen und andere Systeme können mit vielen Servern und Clients kommunizieren.
- [ ] Server und Clients sind isoliert, Einrichtungen, Maschinen und andere Systeme können nur mit wenigen definierten und benötigten Servern und Clients kommunizieren.
- [ ] Server, Clients und andere Systeme sind durch virtuelle Netze, Micro-Segmentierung, etc. isoliert

Kommentar
Anhänge

16. Drahtlose Netze

Wie sichern Sie die drahtlosen Netze Ihrer Organisation?

- [ ] WEP
- [ ] WPA
- [ ] WPA2 PSK
- [ ] WPA2 RADIUS
- [ ] Kein Wireless Netz

Kommentar
Anhänge

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
Anhänge

18. Umgang mit Informationssicherheitsvorfällen

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

- ☐ Kein Incident Response Programm
- ☐ Dokumentierter Incident Response Plan
- ☐ Dokumentierter Incident Response Plan und dediziertes Personal
- ☐ Dokumentierter Incident Response Plan und dediziertes Personal sowie regelmäßige Test und Übungen

Kommentar
Anhänge

19. Tests

Wählen Sie die 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
Anhänge

Erstellt von _____

Datum und Unterschrift _____

CEO/CIO/CISO _____

Datum und Unterschrift _____