Cybersecurity Check

Initial Security Audit

für

LOREM IPSUM

Lorem Ipsum Musterfirma

Musterstraße 1

1010 Musterstadt

Inhaltsverzeichnis

Versionshistorie

Version	Datum	Ersteller	Beschreibung
1.0	<DATUM>	Fidela OG	Erstellung des Dokuments

1. Zusammenfassung

Der Cybersecurity Check wurde für die gemäß den im Angebot - und in Kapitel 3.2- enthaltenen Themenfeldern durchgeführt.

Die untersuchten Themenfelder zeigen sowohl positive Aspekte, als auch Bereiche, die noch Verbesserungspotenzial aufweisen.

Im Bereich der Cybersecurity-Richtlinien und Organisation gibt es nur in einem Bereich klare Zuständigkeiten und Prozesse. Es wird empfohlen, weitere Richtlinien und Prozesse in anderen Bereichen zu etablieren, um klare Strukturen und Arbeitsweisen zu schaffen.

Um die Mitarbeiterinnen und Mitarbeiter weiterhin für Cyberangriffe zu sensibilisieren, sollten regelmäßige Phishing-Kampagnen durchgeführt und individuell angepasste Schulungen integriert werden. Es wird empfohlen, auch im Arbeitsalltag Maßnahmen wie geänderte Hintergrundbilder, Poster oder Kurzlernvideos einzusetzen.

Im Bereich Notfallpläne und Business Continuity Konzept besteht ein kritisches Risiko, welches auch das höchste Risiko darstellt. Es existiert keinerlei Dokumentation in Form eines Notfallhandbuch oder Notfallplänen. In diesen Bereich besteht umgehender Handlungsbedarf. Es muss ein umfassendes Notfallhandbuch samt dazugehöriger Notfallpläne erstellt werden.

Das Fehlen eines dokumentierten Berechtigungskonzepts und die Nichtunterscheidung zwischen privilegierten und nicht privilegierten Benutzern stellen ein kritisches Risiko dar, welches einem Angreiger ein Ausbreiten im Unternehmen enorm erleichtert.

Die vorgeschlagenen Maßnahmen sollen dazu beitragen, die Sicherheitslage deutlich zu verbessern und Risiken zu verringern. Eine Umsetzung dieser Maßnahmen ist dringend anzuraten, um das Unternehmen gegen Cyberangriffe zu schützen und die Geschäftskontinuität zu gewährleisten.

2. Übersicht der Maßnahmen

Im folgenden Kapitel werden die einzelnen Maßnahmen und Handlungsempfehlungen zusammengefasst und dem Risiko entsprechend sortiert. Eine detailierte Beschreibung zu den einzelnen Maßnahmen finden sich in den jeweilgen Kapiteln.

#	Risiko	Beschreibung
1	Kritisch	Etablierung eines umfassenden Berechtigungskonzeptes
2	Kritisch	Trennung von privilegierten und nicht privilegierten Benutzern
3	Kritisch	Erstellung eines Notfallhandbuches und Notfallpläne
4	Mittel	Regelmäßige Awareness Schulungen und Phishing Kampagnen
5	Niedrig	Erarbeitung zusätzlicher Richtlinien und Prozesse

3. Allgemeines

3.1. Ziele

Die Lorem Ipsum Musterfirma strebt eine Erhöhung des Cybersecurity Niveaus und eine gesteigerte Cyber Resilienz an. Um einen Überblick über die aktuelle Lage zu bekommen, sowie die wichtigsten Maßnahmen zu identifizieren, wurde ein Cybersecurity Check durchgeführt.

3.2. Themenfelder

Beim Cybersecurity Check handelt es sich um ein „Initial Security Audit", welches folgende organisatorische und technische Themenfelder abdeckt:

- Cybersecurity Richtlinien und Organisation
- Awareness und Schulungen
- Notfallpläne und Business Continuity Konzept
- Berechtigungskonzept und privilegierte Benutzer
- Asset Management
- Basis Active Directory Check
- Netzwerkarchitektur
- Datensicherung
- Patchmanagement
- Schutz vor Schadsoftware
- Sicherer Betrieb von IT-Systemen

3.3. Geltungsbereich

Im Geltungsbereich des Cybersecurity Checks liegt ausschließlich die Lorem Ipsum Musterfirma.

Tochterunternehmen, anderweitige verbunden Unternehmen oder Lieferanten sind nicht im Geltungsbereich enthalten.

3.4. Zeitraum und Lokation

Der Cybersecurity Check fand am <DATUM> in den Räumlichkeiten der Lorem Ipsum Musterfirma am Standort in Musterstadt statt.

3.5. Bewertungsmethodik

Der Cybersecurity Check wurdes gemäß den Anforderungen an den aktuellen Stand der Technik durchgeführt. Als „Stand der Technik" werden Anforderungen gemäß ISO/IEC 27001 und den BSI IT-Grundschutz-Kompendium festgelegt, welche auf die spezifischen Anforderungen des geprüften Unternehmens umgelegt wurden.

Die Bewertung erfolgte durch Aussagen des Interviewpartners und durch Prüfung von Dokumentationen und Protokollen. Die Bewertung stellt eine Momentaufnahme zum Zeitpunkt des Checks dar.

3.6. Risikostufen

Alle Ergebnisse werden mit einem entsprechenden Risiko gemäß der nachfolgenden Tabelle bewertet. Die Bewertung ermöglicht es Ihnen, entsprechende Maßnahmen gezielt zu priorisieren und zu behandeln.

Kritisches Risiko	Ein kritisches Risiko steht für eine schwerwiegende und weitreichende Schwachstelle. Die Wahrscheinlichkeit eines erfolgreichen Angriffs ist extrem hoch und die potenziellen Auswirkungen können verheerend sein, einschließlich eines kompletten Systemausfalls, massiver Datenverluste oder eines irreparablen Schadens für das Unternehmen.
Hohes Risiko	Ein hohes Risiko weist auf erhebliche Schwachstellen hin, die von Angreifenden leicht ausgenutzt werden könnnen. Die Wahrscheinlichkeit eines erfolgreichen Angriffs ist hoch, die Auswirkungen können schwerwiegend sein, einschließlich erheblicher finanzieller Verluste, Reputationsschäden oder Datenlecks.
Mittleres Risiko	Ein mittleres Risiko deutet darauf hin, dass es einige Schwachstellen in der Infrastruktur des Unternehmens gibt, die potenziell von Angreifern ausgenutzt werden können. Die Wahrscheinlichkeit eines erfolgreichen Angriffs ist moderat, und die Auswirkungen könnten zu Betriebsstörungen führen.
Niedriges Risiko	Ein niedriges Risiko bedeutet, dass nur geringe Schwachstellen identifiziert wurden, die das potenzielle Schadenspotential minimieren. Die Wahrscheinlichkeit eines erfolgreichen Angriffs ist gering, und die Auswirkungen auf das Unternehmen wären geringfügig oder vernachlässigbar.

4. Ergebnisse

Im nachfolgenden Kapitel werden die Handlungsempfehlungen des jweiligen Themenblocks erläutert und mit dem entsprechenden Risiko bewertet.

4.1. Cybersecurity Richtlinien und Organisation

Interviewpartner	Herr Mustermann Max
Erbrachte Nachweise	■ Richtlinie Datensicherung ■ Organigramm
Maßnahme	■ Erarbeitung zusätzlicher Richtlinien und Prozesse
Risiko	Niedriges Risiko

Im Organigramm ist ersichtlich, dass die IT-Abteilungsleitung mit den Agenden rund um Cybersecurity betraut ist. Die Zuständigkeit für einzelne IT-Systeme ist an die jeweiligen Betreuer delegiert.

Es existiert eine Richtlinie für Datensicherungen. In diesen Bereich existieren klare Prozesse und Konzepte. Weitere Richtilinien und Prozesse existieren nicht.

Definierte Standardprozesse reduzieren das Fehlerrisiko enorm und tragen zu einer effizienteren Arbeitsweise bei.

- Um klare Strukturen und Arbeitsweisen zu schaffen, müssen auch in weiteren Bereichen Richtlinien und Prozesse etabliert werden.

4.2. Awareness und Schulungen

Interviewpartner	Herr Mustermann Max
Erbrachte Nachweise	■ Ergebnis Phishing Kampagne 12/2021 ■ Anzahl der Aufrufe des Awareness Videos 01/2022
Maßnahme	■ Durchführung von regelmäßigen Awareness Schulungen und Phishing Kampagnen ■ Integration von Awareness in den Arbeitsalltag
Risiko	Mittleres Risiko

Es wurde in der Vergangenheit eine einzelne Phishing Kampagne mit anschließender Awareness Schulung durchgeführt.

Um die Awareness der Mitarbeiteitenden gegenüber von Cyberangriffen zu steigern, müssen folgende Maßnahmen umgesetzt werden:

- Regelmäßige - min. 1 Mal jährlich bzw. über das ganze Jahr verteilte - Phishing Kampagnen.
- Eine auf das Unternehmen angepasste Awareness-Schulung.
- Vorgehensweisen und Tips auch in den Arbeitsalltag integrieren. Dies kann in Form von geänderten Hintergrundbildern auf dem Lockscreen, durch Poster, 2min Learning oder durch Tischaufsteller durchgeführt werden.

4.3. Notfallpläne und Business Continuity Konzept

Interviewpartner	Herr Mustermann Max
Erbrachte Nachweise	■ Keine
Maßnahme	■ Erstellung eines Notfallhandbuches und dazugehöriger Notfallpläne
Risiko	Kritisches Risiko

Es existieren keinerlei Dokumente in Form eines Notfallhandbuches oder Notfallplänen, welche beschreiben, was im Falle eines erfolgreichen Cyberangriffes durchzuführen ist. Alle Informationen, welche im Notfall benötigt werden, wie z.B. Kontaktdaten von Dienstleistern, Vertragsdaten, Versicherungspolizzen u.ä., sind nicht zentral gesammelt.

Die Systembetreuer sind im Notfall angehalten sich entprechend der Situaton abzustimmen und nach „besten Wissen und Gewissen" zu handeln.

Das Nichtvorhandensein entsprechender Dokumentationen und Informationen kann im Falle eines erfolgreichen Angriffes zu enormen Verzögerungen und Fehlverhalten führen. Entsprechende Informationen - z.B. Kontaktdaten zu Herstellern - müssen erst zusammengetragen werden und behindern dadurch die effiziente Behebung des Notfalls und eine schnelle Rückkehr zum Normalbetrieb.

- Es muss ein umfassendes organisatorisches Notfallhandbuch erstellt werden, welches die Organisation und Erreichbarkeiten im Notfall regelt. Dies umfasst alle relevanten Informationen, unter anderem Kontaktdaten zu Lieferanten und Dienstleistern, eine Übersicht über alle IT-Systeme und deren Kritikalität sowie Systemdokumentationen. Diese Informationen müssen digital und analog an einen zugänglichen Ort vorhanden sein.
- Für spezifische Ereignisse, z.B. Ransomware, müssen Notfallpläne vorhanden sein. Diese Notfallpläne müssen im groben Umfang die Vorgehensweise regeln. Notfallpläne sind auch für den Stillstand von geschäftskritischen Systemen anzufertigen.
- Das Notfallhandbuch und alle Notfallpläne sind regelmäßig und anlassbezogen zu prüfen und zu aktualisieren.
- Um die Wirksamkeit zu testen sind zusätzlich regelmäßge Notfalltests durchzuführen.

4.4. Berechtigungskonzept und privilegierte Benutzer

Interviewpartner	Frau Musterfrau Erika
Erbrachte Nachweise	■ Gruppenmitgliedschaften „Domain Admins“ ■ Liste der administrativen Benutzer im CRM-System
Maßnahme	■ Etablierung eines umfassenden Berechtigungskonzeptes ■ Trennung von privilegierten und nicht privilegierten Benutzern
Risiko	Kritisches Risiko

Es existiert kein dokumentiertes Berechtigungskonzept. Benötigte Berechtigungen werden auf Zuruf vergeben. Mitarbeitende besitzen potentiell ein Vielfaches an Berechtigungen wie diese für die Erfüllung der Tätigkeiten benötigen. Berechtigungen sind nicht nach dem Least-Privilege-Prinzip vergeben.

Die Administration von IT-Systemen, wie z.B. dem Active Directory und dem CRM-System, wird mit dem persönlichen Benutzer des Systembetreuers durchgeführt. Es wird keine Unterscheidung zwischen privilegierten und nicht privilegierten Account durchgeführt.

Wird ein Account eines Mitarbeitenden bzw. Systembetreuers kompromitiert, erhält der Angreifende potentiell privilegierten Zugriff auf geschäftskritische Systeme und kann sich in weiterer Folge schneller und leichter im Unternehmensnetzwerk ausbreiten.

Um die Ausbreitung eines Angreifers zu verhindern müssen folgende Maßnahmen umgesetzt werden:

- Erstellung eines Konzeptes zur Berechtigungsvergabe inkl. dazugehörigen Freigabeprozess. Die Einhaltung des Least-Privilege-Prinzips muss sichergestellt werden.
- Die Trennung von privilegierten und nicht privilegierten Accounts muss durchgeführt und sichergestellt werden.

4.5. Asset Management

<Dieses Kapitel ist nicht Bestandteil des Musterberichts>

4.6. Basis Active Directory Check

<Dieses Kapitel ist nicht Bestandteil des Musterberichts>

4.7. Netzwerkarchitektur

<Dieses Kapitel ist nicht Bestandteil des Musterberichts>

4.8. Datensicherung

<Dieses Kapitel ist nicht Bestandteil des Musterberichts>

4.9. Patchmanagement

<Dieses Kapitel ist nicht Bestandteil des Musterberichts>

4.10. Schutz vor Schadsoftware

<Dieses Kapitel ist nicht Bestandteil des Musterberichts>

4.11. Sicherer Betrieb von IT-Systemen

<Dieses Kapitel ist nicht Bestandteil des Musterberichts>