Bundesamt
für Sicherheit in der
Informationstechnik

ISACA®
Trust in, and value from, information systems
Germany Chapter

Muster-Beurteilungsbericht

zum

Cyber-Sicherheits-Check

der

Beispiel GmbH

Januar 2014

1. Rahmendaten

Beurteilungsgegenstand	Cyber-Sicherheits-Check der Beispiel GmbH, München
Beurteiler	Herr Dieter Mustermann (Muster-Consulting AG) Frau Erika Mustermann (Muster-Consulting AG)
Ansprechpartner	Herr Klaus Sicher (IT-Sicherheitsbeauftragter)
Anlass	Antrag der Beispiel GmbH auf Durchführung eines Cyber-Sicherheits-Checks vom 02.01.2014
Grundlagen und Anforderungen	1) Leitfaden Cyber-Sicherheits-Check (Version 1.0) 2) Verbindliche Liste der Maßnahmenziele (Version 1.0)
Zeitlicher Ablauf	Vor-Ort-Beurteilung: 09.01.2014 Berichtsübergabe 16.01.2014
Verteiler	Herr Klaus Sicher (IT-Sicherheitsbeauftragter) mit der Bitte um Weiterleitung an die Geschäftsführung der Beispiel GmbH

Datei	2013-12-11_CSC-Musterbericht.docx
Druckdatum	16.01.2014
Dokumentenstatus	Freigegeben

2. Management Summary

Der Cyber-Sicherheits-Check soll Unternehmen und Behörden einen Überblick über den Status der Cyber-Sicherheit in ihrer Institution geben und die Verantwortlichen anhand konkreter Empfehlungen dabei unterstützen, festgestellte Sicherheitsmängel abzustellen.

2.1 Cyber-Sicherheits-Exposition

Auf Basis der vorgelegten Dokumente und gesammelten Informationen wurde für die Beispiel GmbH folgende Cyber-Sicherheits-Exposition festgestellt:

Cyber-Sicherheits-Exposition	Vertraulichkeit	Integrität	Verfügbarkeit
	sehr hoch	normal	normal

Die Einstufung einer sehr hohen Cyber-Sicherheits-Exposition im Schutzziel „Vertraulichkeit“ resultiert maßgeblich daraus, dass die Beispiel GmbH als weltweit marktführendes Unternehmen bei der Entwicklung und Produktion innovativer Spezial-Motorsägen besonders gegenüber professioneller Konkurrenz-Spionage und Angriffen professioneller Cyber-Krimineller gefährdet erscheint.

2.2 Cyber-Sicherheits-Status

Die Ergebnisse des Cyber-Sicherheits-Checks sind in der nachfolgenden Tabelle dargestellt und geben den Status der Cyber-Sicherheit in der Beispiel GmbH je Maßnahmenziel wieder. Die Bewertungsergebnisse der einzelnen Maßnahmenziele werden in Kapitel 4 näher erläutert.

Grundsätzlich ist zu bemerken, dass im Rahmen des Cyber-Sicherheits-Checks der Beispiel GmbH in zwei Maßnahmenzielen schwerwiegende Sicherheitsmängel festgestellt werden konnten.

Insbesondere wurden jedoch im Maßnahmenziel H „Bewältigung von Sicherheitsvorfällen“ schwerwiegende Sicherheitsmängel festgestellt, die im Wesentlichen darauf beruhen, dass weder entsprechende Richtlinien/Konzepte noch Prozesse zur Behandlung von Sicherheitsvorfällen etabliert wurden. Da dies jedoch im Hinblick auf die sehr hohe Cyber-Sicherheits-Exposition im Schutzziel „Vertraulichkeit“ dringend notwendig erscheint, erfolgte hier eine Bewertung als „schwerwiegender Sicherheitsmangel“.

Darüber hinaus wurden ebenfalls im Maßnahmenziel B „Abwehr von Schadprogrammen“ schwerwiegende Sicherheitsmängel vorgefunden. Hier ist zu bemängeln, dass auf keinem der Fileserver eine angemessene Software zum Schutz vor Schadprogrammen installiert wurde. Diese Bewertung resultiert aus der sehr hohen Cyber-Sicherheits-Exposition im Schutzziel „Vertraulichkeit“.

Maßnahmenziel	Bewertet	Ergebnis	
A) Absicherung von Netzübergängen	Ja	Keine Mängel festgestellt	
B) Abwehr von Schadprogrammen	Ja	Schwerwiegende Sicherheitsmängel festgestellt	
C) Inventarisierung der IT-Systeme	Ja	Keine Mängel festgestellt	
D) Vermeidung von offenen Sicherheitslücken	Ja	Keine Mängel festgestellt	
E) Sichere Interaktion mit dem Internet	Ja	Keine Mängel festgestellt	
F) Logdatenerfassung und Auswertung	Ja	Sicherheitsmängel festgestellt	
G) Sicherstellung eines aktuellen Informationsstandes	Ja	Keine Mängel festgestellt	
H) Bewältigung von Sicherheitsvorfällen	Ja	Schwerwiegende Sicherheitsmängel festgestellt	
I) Sichere Authentisierung	Ja	Keine Mängel festgestellt	
J) Gewährleistung der Verfügbarkeit notwendiger Ressourcen	Ja	Keine Mängel festgestellt	
K) Durchführung nutzerorientierter Maßnahmen	Ja	Keine Mängel festgestellt	
L) Sichere Nutzung Sozialer Netzwerke	Ja	Keine Mängel festgestellt	
M) Durchführung von Penetrationstests	Ja	Keine Mängel festgestellt	

Tabelle 1: Cyber-Sicherheits-Status je Maßnahmenziel

3. Detaillierte Bewertungsergebnisse

Maßnahmenziel	A – Absicherung von Netzübergängen
Ergebnis	Keine Mängel festgestellt
Ansprechpartner	Herr Nerd (Netz-Betrieb)
Stichprobe(n)	CORE01, CORE02, ACCESS01, FW01
/	

Maßnahmenziel	B – Abwehr von Schadprogrammen
Ergebnis	Sicherheitsmängel festgestellt
Ansprechpartner	Frau Admin (System-Betrieb), Herr Wirus (System-Planung)
Stichprobe(n)	Konzept zur Abwehr von Schadprogrammen (Version 1.1), SEP01, CLIENT11, FILE01, FILE04

Schwerwiegender Sicherheitsmangel:

Auf allen Fileservern der Stichprobe konnte keine geeignete Software zum Schutz vor Schadprogrammen (weder Antivirensoftware, noch Host-basierte Intrusion Detection Systeme) festgestellt werden. Auf direkte Nachfrage wurde durch die Ansprechpartner bestätigt, dass kein Fileserver über einen angemessenen Schutz vor Schadsoftware verfügt.

Empfehlung:

Auf allen Fileservern sollte eine geeignete Software zum Schutz vor Schadprogrammen installiert werden.

Maßnahmenziel	C – Inventarisierung der IT-Systeme
Ergebnis	Keine Mängel festgestellt
Ansprechpartner	Herr Intemann (Netz-und Systemmanagement)
Stichprobe(n)	CORE01, CORE02, ACCESS01, FW01
/	

Maßnahmenziel	D – Vermeidung von offenen Sicherheitslücken
Ergebnis	Keine Mängel festgestellt
Ansprechpartner	Frau Admin (System-Betrieb)
Stichprobe(n)	Systemlogbücher (Sharepoint-Portal), Patchmanagement-Konzept (Version 2.4)
/	

Maßnahmenziel	E – Sichere Interaktion mit dem Internet
Ergebnis	Keine Mängel festgestellt
Ansprechpartner	Herr Surf (Netzwerk-Planung)
Stichprobe(n)	Konzept „sicheres Surfen und eMail“ (Version 1.2), PROXY02, FW01, CLIENT04
/	

Maßnahmenziel	F – Logdatenerfassung und -Auswertung
Ergebnis	Sicherheitsmängel festgestellt
Ansprechpartner	Herr Intemann (Netz- und Systemmanagement)
Stichprobe(n)	MANAGER01, SYSLOG02, DC03

Sicherheitsmangel:

Netzkomponenten protokollieren Ereignisse ausschließlich lokal, eine Auswertung erfolgt lediglich anlassbezogen.

Empfehlung:

Alle Netzkomponenten sollten Ereignisse auch auf einen zentralen Syslog-Server protokollieren. Es sollte eine regelmäßige, automatisierte Auswertung sicherheitsrelevanter Ereignisse erfolgen.

Maßnahmenziel	G – Sicherstellung eines aktuellen Informationsstandes
Ergebnis	Keine Mängel festgestellt
Ansprechpartner	Frau Admin (System-Betrieb)
Stichprobe(n)	Admin-Sharepoint Portal (Quellenverzeichnis und Meldungsaggregation)
/	

Maßnahmenziel	H – Bewältigung von Sicherheitsvorfällen
Ergebnis	Schwerwiegende Sicherheitsmängel festgestellt
Ansprechpartner	Herr Sicher (IT-Sicherheitsbeauftragter)
Stichprobe(n)	Sicherheitskonzept (Version 1.1), UHD01 (Ticket-System)

Sicherheitsmangel:

Eine Richtlinie zur Behandlung von Sicherheitsvorfällen konnte nicht vorgelegt werden.

Empfehlung:

Eine Richtlinie zur Behandlung von Sicherheitsvorfällen sollte erstellt werden.

===

Schwerwiegender Sicherheitsmangel:

Etablierte Prozesswege zur Behandlung von Sicherheitsvorfällen unter Einbindung des IT-Sicherheitsmanagements konnten nicht festgestellt werden.

Bei der Inaugenscheinnahme des Servers UHD01 konnte festgestellt werden, dass eine offensichtlich durch einen Sicherheitsvorfall verursachte Störung fälschlicherweise als fehlerhaftes Nutzerverhalten eingestuft und vorschnell geschlossen wurde.

Empfehlung:

Es sollten Prozesswege zur Behandlung von Sicherheitsvorfällen etabliert werden. Der IT-Sicherheitsbeauftragte sollte hierbei in angemessener Form eingebunden werden.

Maßnahmenziel	I – Sichere Authentisierung
Ergebnis	Keine Mängel festgestellt
Ansprechpartner	Frau Admin (System-Betrieb)
Stichprobe(n)	RADIUS02, DC01
/	

Maßnahmenziel	J – Gewährleistung der Verfügbarkeit notwendiger Ressourcen
Ergebnis	Keine Mängel festgestellt
Ansprechpartner	Herr Sicher (IT-Sicherheitsbeauftragter)
Stichprobe(n)	Sicherheitskonzept (Version 1.1), Notfallvorsorgekonzept (Version 2.3)
/	

Maßnahmenziel	K – Durchführung nutzerorientierter Maßnahmen
Ergebnis	Keine Mängel festgestellt
Ansprechpartner	Herr Sicher (IT-Sicherheitsbeauftragter)
Stichprobe(n)	Schulungs- und Sensibilisierungskonzept (Version 1.0), Weiterbildungsakte Herr Müller (Abteilung Z3)
/	

Maßnahmenziel	L – Sichere Nutzung Sozialer Netzwerke
Ergebnis	Keine Mängel festgestellt
Ansprechpartner	Herr Sicher (IT-Sicherheitsbeauftragter)
Stichprobe(n)	Richtlinie zur Nutzung von Social Media (Version 1.1), Facebook/Xing-Profil Frau Cisomeier
/	

Maßnahmenziel	M – Durchführung von Penetrationstests
Ergebnis	Keine Mängel festgestellt
Ansprechpartner	Herr Klaus Sicher (IT-Sicherheitsbeauftragter), Herr Faupenn (Netz-Betrieb)
Stichprobe(n)	Pentest-Konzept (Version 1.3), Pentest-Report VPN-Zugang (10.10.2022)
/	

(Datum/Unterschrift Beurteiler)	(Datum/Unterschrift Beurteiler)