

Security Baseline Check

Bericht CASE-6 für Muster Unternehmen GmbH

Datum: 01.04.2022

Vertraulichkeitsstufe: Streng vertraulich

Inhaltsübersicht

1. Ziel	3
2. Umfang der Analyse	3
3. Ergebnis des digitalen Fragebogens	4
4. Ergebnisse des Security Baseline Checks	7
Bewertung/Legende	7
Zusammenfassung	8
Detaillierte Übersicht	
Zugangssicherheit	9
Malware-Schutz	10
Patch-Management	11
Netzwerk-Sicherheit	12
Datensicherungs-Konzept	13
5. Haftungsausschluss	14

1. Ziel

Das Incident Management-Team der Perseus Technologies GmbH prüft, ob Ihr Unternehmen gängige IT-Sicherheitsstandards ausreichend erfüllt bzw. ob diese angemessen umgesetzt werden. Hierfür findet eine Bestandsaufnahme der aktuellen IT-Sicherheitsstrukturen als auch eine Bewertung ihres Reifegrads statt. In diesem Kontext werden unter anderem folgende Punkte geprüft:

Zugangssicherheit

"Hat jeder Mitarbeiter nur die Berechtigungen und passwortgeschützten Einzelzugänge, die er für seine Arbeit benötigt?"

Malware-Schutz

"Verwenden Sie einen Malware-Schutz (z.B. in Form eines Antiviren-Programms) und wird dieser automatisch aktualisiert?"

Patch-Management

"Werden vom Hersteller bereitgestellte Updates (z.B. Sicherheitsaktualisierungen) umgehend angewendet?"

Netzwerk-Sicherheit

"Sind alle Zugangspunkte zum Internet durch Firewalls gesichert?"

Datensicherungs-Konzept

"Wird zumindest wöchentlich eine Datensicherung in einem separaten System oder auf externen Speichermedien durchgeführt?"

2. Umfang der Analyse

Die Überprüfung, ob einzelne Sicherheitsanforderungen erfüllt werden, basiert auf stichprobenartigen Analysen einzelner Systeme, stichprobenartiger Einsichtnahme in Dokumente (z.B. Sicherheitsrichtlinien) und Gesprächen mit (technischen) Mitarbeitern, die zu bestimmten Fragestellungen Auskunft geben sollen. Im Rahmen von Stichprobenanalysen werden jeweils maximal drei Systeme oder Geräte untersucht. Um den Aufwand so gering wie möglich zu halten, werden nur Basiskonfigurationen, d.h. die wichtigsten Konfigurationen zur Gewährleistung des grundsätzlich sicheren Betriebs einer technischen Einheit, analysiert.

3. Ergebnis des digitalen Fragebogens

1. Allgemeine Fragen

1. Firmenname

Muster Unternehmen GmbH

2. Branche

Dienstleistungen & Handwerk

3. Wie viele Mitarbeiterinnen und Mitarbeiter hat Ihr Unternehmen?

11 - 100 Mitarbeitende

4. Verarbeiten und speichern Sie Daten im Sinne der Datenschutzgrundverordnung (DSGVO) oder des Sozialgesetzbuchs (SGB)?

Ja

5. Sind Sie gesetzlich dazu verpflichtet, einen Datenschutzbeauftragten zu benennen?

Ja

6. Wurde ein interner oder externer Datenschutzbeauftragter für das Unternehmen benannt?

Ja

7. Verarbeitet, speichert oder übermittelt Ihr Unternehmen (oder ein Dienstleister in Ihrem Auftrag) weniger als 20.000 Kreditkartendatensätze pro Jahr? Bitte berücksichtigen Sie sämtliche Endgeräte.

Ja

8. Gab es in Ihrem Unternehmen bereits Vorfälle im Zusammenhang mit Schadprogrammen (Malware)?

Nein

9. Betreiben Sie in Ihrem Unternehmen industrielle Kontrollsysteme (industrial control systems - ICS) / automatisierte Produktionssysteme?

Nein

2. Infrastruktur

10. Sind die Speichermedien der Arbeitsplatzrechner und tragbare Speichermedien (z.B. USB-Sticks) verschlüsselt - z.B. mit Bitlocker bei Windows?

Ja

11. Sind Mindestanforderungen für Passwörter mit mindestens 8 Zeichen, Zahlen und Buchstaben, Groß- und Kleinschreibung durchgängig vorgeschrieben?

Ja

12. Werden Betriebssystem-Updates für Client-Systeme (Kommunikation mit einem Server) automatisch installiert?

Ja

13. Werden Betriebssystem-Updates für Serversysteme automatisch installiert?

Ja

14. Wird die Installation anstehender Updates zentral gesteuert?

Ja

3. Unternehmensrichtlinien

15. Erlauben es die Unternehmensrichtlinien, firmeneigene Speichermedien auf Geräten von Dritten zu verwenden?

Nein

16. Erlauben es die Unternehmensrichtlinien, dass Mitarbeitende Software installieren?

Nein

17. Gibt es Unternehmensrichtlinien, die definieren, ob Drittanbieter-Software installiert werden bzw. auf Firmenarbeitsplätzen verwendet werden darf (Whitelist oder Blacklist)?

Ja

18. Existiert eine Unternehmensrichtlinie, die sicherstellt, dass Passwörter und PINs für den Zugang zu Telefonanlagen und Anrufbeantwortern vor der ersten Benutzung geändert werden müssen?

Ja

4. Datensicherung**19. Nutzen Sie eine Datensicherungs-Lösung (Backup-Lösung) in Ihrem Unternehmen?**

Ja

20. Wenn der Name der Datensicherungs-Anwendung bekannt ist, geben Sie ihn bitte hier ein:

Data Backup Pro

21. Werden Datensicherungskopien (Backups) der Arbeitsplatz-Rechner erstellt?

Ja, vollständige Datensicherung

22. Werden Datensicherungskopien (Backups) der Server erstellt?

Ja, vollständige Datensicherung

23. Wie viele Backup-Generationen speichern Sie?

3+

24. Haben Sie einen Zeitplan für die automatische Datensicherung aufgestellt?

Ja, tägliche Datensicherung

25. Wird der Datensicherungs-Prozess regelmäßig auf korrekte Funktionsfähigkeit überprüft? Beispielsweise durch Berichte oder Fehlermeldungen?

Ja

26. Werden die Sicherungsmedien an einem separaten Ort und geschützt vor unberechtigtem Zugriff aufbewahrt?

Ja

27. Sind die Sicherungsmedien durch Passwortschutz oder Verschlüsselung vor nachträglicher Manipulation geschützt?

Ja

5. Netzwerk-Sicherheit**28. Sind Systeme, die über das Internet erreichbar sind, ausschließlich über gesicherte Verbindungen zugänglich (z.B. VPN, CAG)?**

Ja

29. Verwenden Sie dasselbe Netzwerksegment für eine kabelgebundene (LAN) und eine drahtlose (WLAN) Internet-Verbindung?

Ja

30. Findet eine Netzwerksegmentierung statt, um interne Firmengeräte von externen Firmengeräten zu trennen (z. B. Gäste-WLAN, Netzwerk für private Geräte der Mitarbeitenden)?

Ja

6. Zugangssicherheit

31. Werden Sie von einem externen Dienstleister bei der Verwaltung Ihrer IT unterstützt?

Nein

32. Ist die Unterstützung in dringenden Fällen durch die IT-Administration oder den externen Dienstleister auch außerhalb der regulären Geschäftszeiten gewährleistet?

Ja

33. Verfügt das Unternehmen über eine Passwort- oder Datenschutzrichtlinie, die von den Nutzenden/Mitarbeitenden zu unterzeichnen und einzuhalten ist?

Ja

34. Gibt es Unternehmensrichtlinien, die den unbefugten Zugriff auf Geräte verhindern, wenn diese nicht in Gebrauch sind (z. B. die Verwendung eines Sperrbildschirms mit Passwortschutz)?

Ja

35. Besitzt jeder Mitarbeiter und jede Mitarbeiterin nur solche Rechte, die zur Erledigung der jeweiligen Arbeiten notwendig sind?

Ja





36. Sind Konten von Administratoren und Nutzenden voneinander getrennt?

Ja

4. Ergebnisse des Security Baseline Checks

Bewertung/Legende

Wir nutzen ein Ampel-System, um aufzuzeigen, in welchem Ausmaß das Unternehmen aktuelle Sicherheitsstandards erfüllt:

Bedeutung in den Gesamtbewertungen	Bedeutung bei der Bewertung einzelner Prüfpunkte
 Sicherheitsstandards wurden vollständig oder zum Teil nicht erfüllt. Es existieren kritische Sicherheitsprobleme.	Der Befund ist sicherheitskritisch und steht der Einhaltung der Sicherheitsnorm entgegen.
 Leider konnte die Prüfung nicht durchgeführt werden, weil wir keinen Zugang zu den notwendigen Informationen hatten (z.B. weil kein Passwort vorlag) oder weil deren Umfang den Rahmen gesprengt hätte (z.B. wenn eine spezielle Unternehmens-Firewall vorhanden ist oder wenn die IT-Sicherheit von einem externen Unternehmen geleistet wird). Daher liegen für diesen Punkt keine ausreichenden Informationen vor, um die Erfüllung des Sicherheitsstandards zu bewerten.	Leider liegen für diesen Punkt nicht ausreichend Informationen vor, um die Erfüllung des Sicherheitsstandards zu bewerten.
 Sicherheitsstandards werden größtenteils erfüllt. Es wurden jedoch Abweichungen festgestellt.	Das Ergebnis der Untersuchung entspricht nicht vollständig den Anforderungen des Sicherheitsstandards und erhöht das Risiko eines IT-Sicherheitsvorfalls.
 Sicherheitsstandards werden erfüllt.	Das Ergebnis entspricht den Anforderungen der Sicherheitsnorm und ist notwendig, um diese zu erfüllen.

4. Ergebnisse des Security Baseline Checks

Zusammenfassung

Die Analyse ergab folgendes Gesamtergebnis für die einzelnen Prüfpunkte mit Blick auf aktuelle Sicherheitsstandards:



Zugangssicherheit ✖

Dieser Sicherheitsstandard wird derzeit nur unzureichend erfüllt.

 **Workstation** ✔

 **Server** ✖



Malware-Schutz ✖

Dieser Sicherheitsstandard wird derzeit nur unzureichend erfüllt.

 **Workstation** ⚠

 **Server** ✖



Patch-Management ✔

Dieser Sicherheitsstandard wird derzeit erfüllt.

 **Workstation** ✔

 **Server** ✔



Netzwerk-Sicherheit ✔

Dieser Sicherheitsstandard wird derzeit erfüllt.



Datensicherungs-Konzept ⚠

Der Sicherheitsstandard wird teilweise erfüllt.

4. Ergebnisse des Security Baseline Checks

1. Zugangssicherheit ✘

Eine Grundvoraussetzung für den sicheren Betrieb eines Computersystems ist, dass jedes Nutzerkonto eindeutig einer einzelnen Person zugeordnet werden kann. Somit sollten sich niemals mehrere Personen ein einziges Nutzerkonto oder Passwort teilen. Um diesen Sicherheitsstandard zu überprüfen, wurden die Nutzerkonten der analysierten Systeme untersucht und entsprechende Informationen von den technischen Ansprechpartnern des Kunden eingeholt.

Dieser Sicherheitsstandard wird derzeit nur unzureichend erfüllt.

Diese Bewertung basiert auf einer stichprobenartigen Analyse der folgenden Systeme.

Workstation ✔

Arbeitsrechner 1

Die Analyse von "Arbeitsrechner 1" kam zu den folgenden Ergebnissen:

- ✔ Durch technische Maßnahmen wird sichergestellt, dass die Benutzerpasswörter eine ausreichende Komplexität aufweisen.
- ✔ Die im System eingerichteten Benutzerkonten sind eindeutig einer einzigen Person zugeordnet und werden nicht mit anderen Personen geteilt. Das Passwort ist nur einer Person bekannt.
- ✔ Das Konto wird zusätzlich durch 2-Faktor-Authentifizierung geschützt.

Dieser Sicherheitsstandard wird derzeit erfüllt.

Es sind keine weiteren Maßnahmen erforderlich, um den Sicherheitsstandard zu erfüllen.

Server ✘

Server 1

Die Analyse von "Server 1" kam zu den folgenden Ergebnissen:

- ✔ Durch technische Maßnahmen wird sichergestellt, dass die Benutzerpasswörter eine ausreichende Komplexität aufweisen.
- ✘ Die im System eingerichteten Benutzerkonten werden von mehreren Personen genutzt. Das Passwort wird von mehreren Benutzern gemeinsam verwendet.
- ! Es gibt keine technischen Maßnahmen, die sicherstellen, dass die Passwörter der Nutzer eine ausreichende Komplexität aufweisen.
- ✔ Das Konto wird zusätzlich durch 2-Faktor-Authentifizierung geschützt.

Dieser Sicherheitsstandard wird derzeit nur unzureichend erfüllt.

Um die Sicherheitsanforderungen zu erfüllen, sollten folgende Maßnahmen getroffen werden:

- Gemeinsam verwendete Benutzerkonten sollten entfernt werden. Für jede Person, die Zugang zum System benötigt, sollte ein eigenes Benutzerkonto eingerichtet werden.*
- Die erforderliche Passwortlänge sollte für alle Benutzerkonten technisch durchgesetzt werden. Nach aktuellem Sicherheitsstandard sollte ein Passwort mindestens 15 Zeichen lang sein.*

4. Ergebnisse des Security Baseline Checks

2. Malware-Schutz ✘

Malware (Schadprogramme) wird von Angreifern auf vielfältige Weise genutzt, z.B. um Daten zu stehlen, den Ablauf des Geschäftsbetriebs zu stören oder Daten zu verschlüsseln, um ein "Lösegeld" für deren Freigabe zu fordern. Ein grundlegender Schutz vor Malware kann durch die Installation von sogenannten Antiviren-Programmen erreicht werden. Die Einhaltung dieses Sicherheitsstandards wird überprüft, indem kontrolliert wird, ob ein anerkanntes Antiviren-Programm installiert und sicher konfiguriert ist.

Dieser Sicherheitsstandard wird derzeit nur unzureichend erfüllt.

Diese Bewertung basiert auf einer stichprobenartigen Analyse der folgenden Systeme.

Workstation !

Arbeitsrechner 1

Die Analyse von "Arbeitsrechner 1" kam zu den folgenden Ergebnissen:

- ✔ Ein anerkanntes Anti-Virenprogramm ist in dem System installiert.
- ! Das installierte Antiviren-Programm ist so konfiguriert, dass verfügbare Updates für die Software und ihre Signaturdatenbanken regelmäßig und rechtzeitig installiert werden. Das letzte Signaturdatenbanken-Update fand zwischen 2 und 6 Tagen vor der Prüfung statt.
- ✔ Das installierte Anti-Virenprogramm wird automatisch beim Systemstart gestartet.

Der Sicherheitsstandard wird teilweise erfüllt.

- *Das installierte Antiviren-Programm muss so konfiguriert sein, dass Updates automatisch und regelmäßig durchgeführt werden. Das empfohlene Intervall für die Aktualisierung der Signaturdatenbank ist mindestens einmal pro Tag.*

Server ✘

Server 1

Die Analyse von "Server 1" kam zu den folgenden Ergebnissen:

- ✔ Ein anerkanntes Anti-Virenprogramm ist in dem System installiert.
- ✘ Das installierte Antiviren-Programm ist so konfiguriert, dass verfügbare Updates für die Software und ihre Signaturdatenbanken ggf. nicht rechtzeitig installiert werden – alle 7 Tage oder seltener.
- ✘ Das installierte Anti-Virenprogramm startet nicht automatisch beim Systemstart.

Dieser Sicherheitsstandard wird derzeit nur unzureichend erfüllt.

Um die Sicherheitsanforderungen zu erfüllen, sollten folgende Maßnahmen getroffen werden:

- *Das installierte Antiviren-Programm muss so konfiguriert sein, dass Updates automatisch und regelmäßig durchgeführt werden. Das empfohlene Intervall für die Aktualisierung der Signaturdatenbank ist mindestens einmal pro Tag.*
- *Das installierte Antiviren-Programm muss so konfiguriert sein, dass es beim Systemstart automatisch gestartet wird.*

4. Ergebnisse des Security Baseline Checks

3. Patch-Management

Immer wieder werden Fehler und Sicherheitslücken in bereits ausgelieferten Anwendungen festgestellt. Aus diesem Grund werden Updates über einen längeren Zeitraum nach Produktion der Anwendung zur Verfügung gestellt. Daher ist die regelmäßige Installation aller verfügbaren Updates essentiell für den sicheren Betrieb eines Systems. Wenn Aktualisierungen nicht automatisch installiert werden sollen, muss die Patch-Verwaltung so organisiert sein, dass Aktualisierungen rechtzeitig durchgeführt werden. Die Einhaltung dieses Sicherheitsstandards wird überprüft durch Untersuchung der Einstellungen des Betriebssystems und einiger Nutzeranwendungen sowie durch Gespräche mit dem technischen Personal.


Dieser Sicherheitsstandard wird derzeit erfüllt.

Diese Bewertung basiert auf einer stichprobenartigen Analyse der folgenden Systeme.

Workstation

Arbeitsrechner 1

Die Analyse von "Arbeitsrechner 1" kam zu den folgenden Ergebnissen:

-  Aktualisierungen des Betriebssystems werden automatisch installiert, sobald sie zur Verfügung gestellt werden. Das letzte Sicherheitsupdate wurde innerhalb von 6-13 Tagen vor dem Live-Check installiert.

Dieser Sicherheitsstandard wird derzeit erfüllt.

Es sind keine weiteren Maßnahmen erforderlich, um den Sicherheitsstandard zu erfüllen.

Server

Server 1

Die Analyse von "Server 1" kam zu den folgenden Ergebnissen:

-  Aktualisierungen des Betriebssystems werden automatisch installiert, sobald sie zur Verfügung gestellt werden. Das letzte Sicherheitsupdate wurde innerhalb von 6-13 Tagen vor dem Live-Check installiert.

Dieser Sicherheitsstandard wird derzeit erfüllt.

Es sind keine weiteren Maßnahmen erforderlich, um den Sicherheitsstandard zu erfüllen.

4. Ergebnisse des Security Baseline Checks

4. Netzwerk-Sicherheit



Geräte, die mit dem Internet verbunden sind, sollten gegen unbefugten und unkontrollierten Netzwerk-Zugriff geschützt werden. Andernfalls können mögliche Sicherheitslücken auf den Geräten oft sehr leicht ausgenutzt werden. Um dies zu verhindern, sollte eine Firewall zwischen Endgeräten und Internet installiert werden. Eine Firewall filtert Netzwerkanfragen auf der Grundlage zuvor festgelegter Regeln. Dadurch kann beispielsweise mit hoher Wahrscheinlichkeit sichergestellt werden, dass Anwendungen, die nur im internen Netzwerk benötigt werden, auch nur von diesem Netzwerk aus erreichbar sind. Die meisten Router verfügen über eine integrierte Firewall, die für viele kleine Einsatzgebiete ausreichend ist, sofern sie entsprechend konfiguriert werden kann.

Dieser Sicherheitsstandard wird derzeit erfüllt.

Diese Bewertung basiert auf einer stichprobenartigen Analyse der folgenden Systeme.

Network

Die Analyse von "null" kam zu den folgenden Ergebnissen:

-  Die Firewall, die das Netzwerk schützt, verfügt über eine aktuelle Firmware. Die Firmware-Updates/-Patches werden automatisch oder manuell gemäß einem Aktualisierungsplan oder einer Benachrichtigung vom Kunden/IT-Dienstleister installiert, sobald diese vom Hersteller bereitgestellt werden.
-  Das Netzwerk wird durch eine Firewall geschützt. Diese ist so konfiguriert, dass nur die Ports, die von außen zugänglich sein müssen, von außen zugänglich und dem Kunden oder dem IT-Dienstleister bekannt sind.

Dieser Sicherheitsstandard wird derzeit erfüllt.

Es sind keine weiteren Maßnahmen erforderlich, um den Sicherheitsstandard zu erfüllen.






4. Ergebnisse des Security Baseline Checks

5. Datensicherungs-Konzept

Sicherungskopien sind notwendig, um Datenverlust im Fall von Hardware- und Software-Fehlern zu vermeiden. Datenverlust droht nicht nur durch die Aktivitäten möglicher Angreifer, sondern auch durch Fehler von Mitarbeitern oder Verschleiß von Datenträgern (z.B. Festplatten). Datensicherungen müssen regelmäßig durchgeführt werden, mindestens wöchentlich, um den Versicherungsvertrag zu erfüllen, der dieser Überprüfung zugrunde liegt. Außerdem sollten Datensicherungen und die auf ihnen basierende Datenwiederherstellung regelmäßig getestet werden. Die Datensicherungsmedien sollten an räumlich getrennten Orten aufbewahrt werden, damit die Daten beispielsweise bei einem Brand nicht verloren gehen und wieder hergestellt werden können. Auch räumlich getrennte Netzwerkspeicher (z.B. bei Cloud-Anbietern) können als Ziel für die Datensicherung in Betracht gezogen werden. Es sollte auch regelmäßig überprüft werden, ob die Datensicherung vollständig ist, beispielsweise ob alle wichtigen Daten enthalten sind. Die Datensicherungen sollten redundant durchgeführt werden. Die Einhaltung der Sicherheitsstandards wird überprüft, indem der Datensicherungs-Prozess analysiert wird, außerdem indem testweise Daten gelöscht und wiederhergestellt werden.

Der Sicherheitsstandard wird teilweise erfüllt.

Diese Bewertung basiert auf einer stichprobenartigen Analyse der folgenden Systeme.

-  Eine regelmäßige Datensicherung (Backup) für alle kritischen Daten wird durchgeführt. Das Unternehmen könnte die Arbeit auf der Grundlage der in den Sicherungskopien enthaltenen Daten wieder aufnehmen.
-  Die Sicherungsmedien werden nicht an einem sicheren, separaten Ort aufbewahrt, der vor unbefugtem Zugriff geschützt ist.
-  Die Sicherungsmedien sind durch Passwortschutz oder Verschlüsselung vor nachträglicher Manipulation geschützt.
-  Die Sicherungskopien sind auch gegen ein spätere unbefugte Manipulation von Daten (Tempering) geschützt, entweder durch eine Offline-Sicherungskopie oder durch ein "Layer 2"-Backup (eine Offline-Kopie oder ein Cloud-Backup).
-  Der Sicherungsprozess wird regelmäßig auf seine Funktionstüchtigkeit überprüft (durch Berichte, Erfolgs-/Misserfolgsbestätigung usw.).

- *Um eine nachträgliche Manipulation der Sicherungsmedien zu verhindern, müssen die Sicherungsmedien an einem sicheren, separaten Ort aufbewahrt werden, der vor unbefugtem Zugriff geschützt ist (z. B. in einem separaten Raum mit kontrolliertem Zugang, einem Tresor oder einem sicheren Schrankfach usw.).*

4. Haftungsausschluss

Dieser Bericht ist streng vertraulich und ausschließlich für die interne, vertrauliche Nutzung des Kunden gedacht. Der Empfänger verpflichtet sich, den streng vertraulichen Inhalt, wie er von der Organisation definiert ist, vertraulich zu behandeln. Der Empfänger übernimmt die Verantwortung für die weitere Verbreitung des Dokuments. In diesem speziellen Projekt wurde die Zeit der Prüfung begrenzt, um den Aufwand zu minimieren. Das bedeutet, dass die Perseus Technologies GmbH nur im gesetzten Zeitrahmen Schwachstellen identifizieren und dokumentieren kann. Daher kann auf Grundlage dieser Prüfung kein Anspruch auf Vollständigkeit der dokumentierten Schwachstellen erhoben werden. Darüber hinaus ist dieser Bericht als Momentaufnahme zum Zeitpunkt der Überprüfung zu betrachten. Eine Bewertung des zukünftigen Sicherheitslevels oder zukünftiger Risiken kann daraus nicht abgeleitet werden. Im Rahmen der Prüfung wurden gegebenenfalls lokale Dateien im System des Kunden kreiert (z. B. temporäre Dateien, Protokolldateien oder Programme, die vom Auftragnehmer hochgeladen wurden, um etwaige Schwachstellen auszunutzen). Dies wurde, falls notwendig, entweder manuell oder automatisch durch den Schwachstellen-Scanner vorgenommen. Diese Dateien wurden nach der Prüfung entfernt, soweit dies für den Auftragnehmer möglich war. Die vollständige Entfernung ist nicht immer möglich aufgrund des Verfahrens bei einer Sicherheitsüberprüfung (z.B. fehlender Systemzugang oder unzureichende Berechtigungen). Dadurch können diese Dateien nach Abschluss der Prüfung noch immer vorhanden sein und müssten anschließend durch den Kunden entfernt werden.