Sicherheits- und Datenschutzkonzept

mit dem Schwerpunkt Härtung und sichere Konfiguration

von

Windows 10 Enterprise – 1909

Ihr Ansprechpartner:
Name: Christian Biehler
E-Mail: christian.biehler@bi-sec.de
Telefon: (+49) 7130 5489 777

bi-sec · Eret 23 · 74182 Obersulm

Kundenkontakt

*Beispiel *

bi-sec-Kontakt

Technik
Christian Biehler
bi-sec GmbH
Eret 23
74182 Obersulm

(+49) 7130 5489 777
christian.biehler@bi-sec.de

Vertrieb
Verena Männel
bi-sec GmbH
Eret 23
74182 Obersulm

(+49) 7130 5489 778
verena.maennel@bi-sec.de

Informationen zum Dokument

Dieser Abschlussbericht enthält vertrauliche Informationen.

Version: 0.1 ENTWURF
Datum: 20.12.2019

Inhalt

Einleitung

Zusammenfassung

Dieses Dokument bildet die Basis für den Betrieb der jeweils aktuellen Windows-10-Version bei der bi-sec GmbH. Unter berücksichtigung der wesentlichen IT-Sicherheitsziele, sowie der Vorgaben aus der EU-DSGVO werden in diesem Dokument sowohl einzelne technische und organisatorische Maßnahmen zur Absicherung von Windows 10 und der umliegenden IT-Umgebung dargestellt, als auch die notwendigen Prozesse und Kontrollen zum Erhalt des angestrebten Schutzniveaus.
...

Schutzbedarf und relevante Verarbeitungen

Windows 10 ist ein Client-Betriebssystem, welche unternehmensweit für unterschiedlichste Geschäftsprozesse eingesetzt wird. Hierbei werden allgemeine personenbezogene Daten wie Name, Anschrift und Telefonnummer, aber auch besondere Kategorien personenbezogener Daten gemäß Art. 9 EU-DSGVO verarbeitet. Hierzu zählen beispielsweise Gesundheitsdaten, biometrische Daten zur Identifizierung der Person und Daten über Religions- oder Gewerkschaftszugehörigkeit.
Auf eine weitergehende Differenzierung nach Abteilungen oder einzelnen Mitarbeitern wird im Folgenden verzichtet, da einige Konfigurationseinstellungen zum Schutz der Daten lediglich maschinenbasiert wirken und somit z.B. beim Wechsel des Computers mitunter ein anderes Schutzniveau herschen würde.
Der Schutzbedarf der Windows-10-Clients in den Kategorien Vertraulichkeit, Integrität und Verfügbarkeit wird wie folgt bewertet:

- Vertraulichkeit: Hoch
- Integrität: Hoch
- Verfügbarkeit: Normal

Sowohl mit Blick auf die IT-Sicherheit, als auch auf den Datenschutz ergibt sich damit die Notwendigkeit eines angemessenen Schutzes der Windows-10-Clients.
Die konkreten Verarbeitungen, in denen Windows 10 involviert ist finden Sie im Dokument *...*

Referenzen und Standards

Um ein angemessenes Sicherheitsniveau nach dem Stand der Technik zu gewährleisten wurden insbesondere die Vorgaben und Hinweise der folgenden Organisationen berücksichtigt:

- Microsoft (Security Compliance Toolkit)
- BSI (relevante Grundschutz-Bausteine wie SYS.2.2.3)
- Center for Internet Security (Benchmark für Windows 10)
- Analyseergebnisse des bayerischen Landesdatenschutz „Windows 10 Investigation Report“
- Hinweise der Ergebnisse der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK), insbesondere „Datenschutz bei Windows 10“– weitergehende technische Aspekte

Neben diesen Orientierungshilfen [1]*...*

[1] https://www.it-sicherheit.mpg.de/Orientierungshilfe_Windows10.pdf
https://docs.microsoft.com/de-de/windows/privacy/manage-connections-from-windows-operating-system-components-to-microsoft-services

Prozesse und Vorgehensweise

Regelprozess zum Erhalt des Schutzniveaus

Microsoft veröffentlicht aktuell zwei Mal im Jahr eine neue Windows-10-Version in Form eines Feature-Updates. Neben diesen Feature-Updates liefert Microsoft regelmäßig Sicherheitsupdates und sonstige Patches zur Verbesserung der Stablität und Leistungsfähigkeit von Windows-10.
Um ein stets aktuelles und dem Stand der Technik entsprechendes Betriebssystem für die Verarbeitung der schützenswerten Daten bereit zu stellen, werden diese Updates nach angemessener Überprüfung in einem geordneten Prozess sukzessive im Unternehmen verteilt.
Größere Aktualisierungen der Dienste, Funktionen und Konfigurationsmöglichkeiten werden allgemein in Feature-Updates bereitgestellt. Diese werden im Unternehmen verteilt, sobald Microsoft die zugehörigen Konfigurations- und Schutzmöglichkeiten durch Gruppenrichtlinien (GPOs) veröffentlicht hat. Dies geschieht typischerweise einige Zeit nach dem Release des eigentlichen Updates.
Um an dieser Stelle den Erhalt des Schutzniveaus zu gewährleisten, werden nach jedem Feature-Update eine Überprüfung der bisherigen Systemhärtung, sowie eine Bewertung und Konfiguration der neu hinzugekommenen Einstellungsmöglichkeiten vorgenommen. Dies geschieht vor der Freigabe der Windows-10-Version im Unternehmen.
Darüber hinaus werden die Client-Systeme regelmäßig quartalsweise einem Schwachstellenscan unterzogen und etwaige Auffälligkeiten durch Anpassung der Konfiguration behoben.
Neben der IT-Sicherheit wird regelmäßig nach einem funktionalen Update die Konfiguration der Datenübermittlung geprüft. Hierbei wird insbesondere ein Blick in die Diagnosedaten geworfen, welche an Microsoft übermittelt werden (z. B. mit hilfe des „Microsoft Diagnostic Data Viewer“).

Sicherheit der Verarbeitung

Windows 10 stellt den Grundbaustein diverser unternehmenskritischer Verarbeitungen dar. Oberste Priorität ist daher die auch in Art 32 EU-DSGVO beschriebene Sicherheit der Verarbeitung. Nach eingehender Prüfung kommen wir zu dem Schluss, dass zur Gewährleistung der Funktionalität ein umfassendes Logging und Monitoring unerlässlich sind. Auf Grund der Komplexität des Betriebssystems kann eine Fehlerdiagnose ausschließlich durch den Hersteller erfolgen, welcher die hierfür benötigten Daten im Rahmen seines „Telemetrie“-Programs direkt von den Clients erhält. Eine vollständige Abschottung der Telemetrie-Daten zu Gunsten des Datenschutzes wäre in diesem Fall nach unserer Einschätzung nicht angemessen und würde die Sicherheit der Verarbeitung wesentlich gefährden. Die Rechtmäßigkeit der Verarbeitung nach Art. 6 EU-DSGVO ist somit durch ein berechtigtes Interesse gegeben, da zum Erhalt der Sicherheit der Verarbeitung Informationen zu Fehlern an den Hersteller zur Behebung übermittelt werden müssen und nur in seltenen Ausnahmefällen personenbezogene Daten enthalten sein können. Deren Schutz wird durch die Überprüfung des Anbieters und dessen Einhaltung der Vorgaben nach Art. 34 EU-DSGVO, insbesondere Verschlüsselung und Pseudonymisierung, sicher gestellt. Durch die Einschränkung des Umfang der übermittelten Daten, der Offenlegung aller gesammelten Telemetriedaten[2] durch Microsoft und der regelmäßigen Überprüfung des Anbieters entspricht die Verarbeitung der personenbezogener Daten unserer Auffassung nach den Anforderungen aus Art. 5 EU-DSGVO. Eine regelmäßige Überprüfung *...*

Überprüfung des Anbieters

Vor der Einführung von Windows und regelmäßig im Rahmen der jährlichen Risikoüberprüfung wird der Anbieter Microsoft auf Zuverlässigkeit und Eignung zum Betrieb und zur Weiterentwicklung des Client-Betriebssystems überprüft. Hierbei werden insbesondere die Zertifizierungen der Organisation und der zugehörigen Rechenzentren, beispielsweise nach ISO

[2] https://docs.microsoft.com/de-de/windows/privacy/windows-diagnostic-data-1703

27001 verifiziert. Microsoft verfügt über vielfach zertifizierte Rechenzentren, in denen auch die an Microsoft übermittelten Diagnosedaten verarbeitet werden. Die aktuell gültigen Zertifizierungen entsprechen nach unserer Überprüfung dem marktüblichen Standard für einen sicheren IT-Betrieb nach dem Stand der Technik. Darüber hinaus *...*

Umsetzung der Datenschutzvorgaben

Der Datenschutz hat mehrere Knackpunkte aus der EU-DSGVO für den Einsatz von Windows 10 im Unternehmen ermittelt. Hierzu zählen insbesondere:

- Art. 5 - Grundsätze für die Verarbeitung personenbezogener Daten
- Art. 25 - Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen
- Art. 32 - Sicherheit der Verarbeitung

Die Einschätzung zu Art. 5 haben wir im Abschnitt „Sicherheit der Verarbeitung“ dieses Dokuments erläutert. Die Notwendigkeit der Übermittlung von Daten und die Absicherung durch Microsoft gemäß Art. 32 ist durch die Überprüfung des Anbieters und der Telemetriedaten ebenfalls gegeben. Die Umsetzung von Art. 25 durch Microsoft bei der Auslieferung von Windows 10 entspricht nicht unserer Interpretation der Anforderungen der EU-DSGVO. Im Rahmen unserer Verantwortung zum Schutz der Rechte und Freiheiten der Anwender, Mitarbeiter und Kunden haben wir technische und organisatorische Maßnahmen ergriffen, welche das verbleibende Restrisiko auf ein akzeptables Niveau absenken. Die einzelnen Maßnahmen basieren auf den Empfehlungen und Ausarbeitungen der im Abschnitt „Referenzen und Standards“ benannten Werke und sind in den nachfolgenden Kapiteln beschrieben.

Technische Maßnahmen zur Härtung und sicheren Konfiguration

Minimale Installation

...

Entfernen nicht benötigter Standard-Komponenten

...

Verschlüsselung der Datenträger

...

Konfiguration der Verbindungssicherheit

...

Konfiguration von Cloud-Diensten

...

Malwareschutz

...

Updates

...

Benutzerverwaltung und administrative Konten

...

Universal Apps und Microsoft Store

...

Backup

...

Weitere Härtungsmaßnahmen

...

Organisatorische Maßnahmen zum Schutz pbD

Awareness und Schulungsmaßnahmen

...

Betriebs- und Anwenderhandbuch

...

Regelmäßige Überprüfung der Wirksamkeit der Maßnahmen

...

Zusammenspiel mit weiteren Sicherheitskonzepten

...

Anhang

A – Aktuelle GPO-Einstellungen

...

B – PowerShell-Scripte zur Härtung und sicheren Konfiguration

...

C – Ergebnisse der Compliance-Prüfung für Windows 10 Enterprise – 1909

...