# Auditbericht

| Sicherheitsüberprüfung betriebliche Aspekte E-Voting-System der Post | |
|---|---|
| Kunde | Bundeskanzlei |
| Datum | 28.06.2019 |

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

oneconsult®
the cyber security experts


| Hauptsitz | Büro Bern | Büro Deutschland |
|---|---|---|
| Oneconsult AG<br>Schützenstrasse 1<br>8800 Thalwil<br>Schweiz<br><br>Tel +41 43 377 22 22<br>Fax +41 43 377 22 77<br>www.oneconsult.com<br>info@oneconsult.com | Oneconsult AG<br>Bärenplatz 7<br>3011 Bern<br>Schweiz<br><br>Tel +41 31 327 15 15<br>Fax +41 31 327 15 25<br>www.oneconsult.com<br>info@oneconsult.com | Oneconsult Deutschland GmbH<br>Agnes-Pockels-Bogen 1<br>80992 München<br>Deutschland<br><br>Tel +49 89 248820 600<br>Fax +49 89 248820 677<br>www.oneconsult.com<br>info@oneconsult.com |

# Inhaltsverzeichnis



| Version | Datum | Beschreibung | Autor(in) |
|---|---|---|---|
| 1.0 | 28.06.2019 | Finalisierung Auditbericht | Christoph Baumgartner & Michael von Arx |

# 1 Vorwort

Bei einer Sicherheitsüberprüfung wird nach Schwachstellen im Untersuchungsobjekt gesucht und diese werden zusammen mit der Risikobeurteilung und geeigneten Massnahmenvorschlägen zur Steigerung des Sicherheitsniveaus im Schlussbericht (auch Audit Report) festgehalten. Weil der Schlussbericht in kompakter Form sämtliche entdeckten Schwachstellen inklusive Details enthält, ist er für einen potentiellen Angreifer von hohem Wert. Aus diesem Grund ist der Empfängerkreis eines Audit Reports üblicherweise möglichst klein und beschränkt sich auf einzelne Personen beim Auftraggeber.

In diesem Projekt wurde die Öffentlichkeit von der Bundeskanzlei als Empfängerkreis definiert. Deshalb sind die Aussagen aus Sicherheitsüberlegungen und rechtlichen Gründen allgemeiner als üblich gehalten und es werden keine Detailinformationen zu den getroffenen Sicherheitsmassnahmen der Post und der Kantone beschrieben. Zwecks besserer Lesbarkeit wird soweit möglich auf fachspezifische Ausdrücke verzichtet.

Dieses Security Audit wurde nach bestem Wissen und Gewissen der Auditoren durchgeführt. Die Auditergebnisse basieren auf den Basisinformationen, welche Oneconsult von den verschiedenen beteiligten Organisationen zur Verfügung gestellt wurden. Oneconsult übernimmt keinerlei Gewährleistung für die Vollständigkeit und Richtigkeit dieser Basisinformationen.

Die Auditoren:

Christoph Baumgartner & Michael von Arx

## 2 Zusammenfassung

Die Bundeskanzlei beauftragte die Oneconsult AG mit der Durchführung einer Sicherheitsüberprüfung der betrieblichen Aspekte des von der Post Informatik betriebenen E-Voting-Systems – somit lag nicht das eigentliche E-Voting-System im Fokus sondern das Drumherum, welches für den sicheren Betrieb desselben bei der Post relevant ist.

Das Security Audit wurde im Juni 2019 durchgeführt und basierte auf der Sichtung und Analyse der zur Verfügung gestellten Dokumente und Einzel- und Gruppeninterviews mit Vertretern der in den Betrieb involvierten Abteilungen der Post Informatik.

Die in den Betrieb des E-Voting-Systems involvierten Bereiche und Teams der Post Informatik sind professionell organisiert und entsprechen damit «Good Security Practices». Dies zieht sich durch die gesamte Organisationseinheit von der Personalrekrutierung über den Betrieb vor, während und nach Abstimmungen bis hin zum IT-Notfallmanagement.

Es wurden keine Schwachstellen entdeckt, welche das E-Voting-System ernsthaft gefährden. Die wenigen Schwachstellen, welche Oneconsult detektierte sind eher organisatorische Schönheitsfehler, welche ohne grossen Aufwand behoben werden können.

Die Zusammenarbeit mit allen beteiligten Organisationen und Stellen war vorbildlich. Es entstand zu keinem Zeitpunkt der Eindruck, dass irgendwelche Sachverhalte verheimlicht oder beschönigt wurden.

Oneconsult bedankt sich für das entgegengebrachte Vertrauen.

Oneconsult AG

Christoph Baumgartner
CEO & Senior Consultant
(ISO 27001 Senior Lead Auditor)

Oneconsult AG

Michael von Arx
Senior Information Security Consultant
(ISO 27001 Lead Auditor, ISO 27005 Risk Manager)

# 3 Projektumfang und Vorgehen

## 3.1 Projektauftrag und -abgrenzung

Die Bundeskanzlei beauftragte die Oneconsult AG mit der Durchführung einer Sicherheitsüberprüfung der betrieblichen Aspekte der von der Schweizerischen Post (Post) zentral betriebenen E-Voting-System-Komponenten. Somit wurde nicht die Sicherheit des eigentlichen E-Voting-Systems überprüft, sondern das Drumherum, welches für den sicheren Betrieb desselben bei der Post relevant ist. In diese Kategorie fallen primär Betriebsabläufe, personelle Aspekte und technische Sicherheitskomponenten. Die dezentralen Teile des E-Voting-Systems, welche im Hoheitsgebiet der Kantone liegen und nicht von der Post betrieben werden, wurden nicht untersucht. Ausserdem lag die Beurteilung der Auditqualität der von der KPMG durchgeführten Zertifizierungsaudits nicht im primären Fokus.

Aufgrund des von der Auftraggeberin vorgegebenen Zeitfensters wurde das Projekt im Juni 2019 durchgeführt und der Auditbericht wurde am 1. Juli 2019 abgeliefert.

## 3.2 Methode und Vorgehen

In den nachfolgenden Unterkapitel wird abstrahiert wiedergegeben, in welchem Rahmen die Sicherheitsüberprüfung der oben genannten betrieblichen Aspekte durch die Oneconsult durchgeführt wurden.

### 3.2.1 Auditansatz

Auf Basis des Projektbudgets und des zur Verfügung stehenden Zeitfensters wurde in Absprache mit der Auftraggeberin ein kombinierter Auditansatz gewählt:

- Neben der klassischen *Gap-Analyse* zu sogenannten «Good Security Practices» (in diesem Fall mit dem international anerkannten Industriestandard für Informationssicherheit ISO 27002:2013)
- kam ein *explorativer Ansatz* auf Basis der Auditerfahrung von Oneconsult zum Einsatz.

Weil die Informatik der Post das E-Voting-System als eines von vielen anderen Systemen betreibt, war die Gesamtinformatik der Post im Fokus dieser Sicherheitsüberprüfung.

### 3.2.2 Prüfnorm

Die ISO 27000 Familie publiziert als international anerkannter Industriestandard für Informationssicherheit Anforderungen und «Good Security Practices» für das Management von Informationssicherheit. Im Rahmen dieses Standards werden 14 Abschnitte (Klauseln) und 114 Massnahmen als Teil der «Good Security Practices» beschrieben. Im Rahmen der Sicherheitsprüfung hat Oneconsult punktuell Massnahmen aus der ISO 27002:2013 Norm bei der Post überprüft.

### 3.2.3 Informationsbasis

Das Security Audit erfolgte auf der Basis grundlegender Informationen der Bundeskanzlei und folgender Informationen der Post:

- Dokumente, welche die Post zur Verfügung stellten:
  - Die Auszüge aus den Zertifizierungsauditberichten, welche die betrieblichen Aspekte des E-Voting-Systems betreffen
  - Weitere Zertifizierungen der Post
  - Diverse Weisungen, Richtlinien, Stellungnahmen, Prozessbeschreibungen etc.
- Einzel- und Gruppeninterviews mit den aus Auditsicht für die verschiedenen relevanten Bereiche zuständigen Personen bei der Post. Hierbei fanden auch stichprobenartig die Verifikationen der Aussagen statt.

### 3.2.4 Vertiefte Überprüfung

Aufgrund des Projektbudgets konnte keine flächendeckende Sicherheitsüberprüfung durchgeführt werden. Nachdem Oneconsult die zur Verfügung gestellten Unterlagen gesichtet hatte, wurden mit der Auftraggeberin die Prüfbereiche definiert, welche vertieft auditiert werden sollten.

Dabei handelte es sich um Bereiche der Informationssicherheitsnorm ISO 27002:2013, welche einerseits in Risikobeurteilungen erschienen und sich andererseits mit den potentiellen Schwachstellenherden aus der Beratungserfahrung von Oneconsult decken:

- Systemhärtung
  - Konfiguration inklusive Deaktivierung nicht benötigter Dienste
  - Patch Management
- Personelle Aspekte
- Zugriffs- und Zutrittskontrolle
- Änderungssteuerung (Change Management)
- Generelle Aspekte
  - Minimalitätsprinzip: Jede Person erhält nur die Informationen und Berechtigungen, welche sie für die Aufgabenerfüllung benötigt.
  - Implementierung des Mehraugenprinzips: In kritischen Bereichen soll sichergestellt werden, dass mindestens zwei Personen benötigt werden, um potentiell riskante Aktivitäten umzusetzen (Beispiel: Zuteilung von Administrationsrechten auf IT-Systemen).

Die oben genannten Aspekte entsprechen spezifischen Massnahmen aus der Informationssicherheitsnorm ISO 27001:2013:

- A.7 Personalsicherheit
- A.9 Zugangssteuerung
- A.11 Physische und umgebungsbezogene Sicherheit
- A.12 Betriebssicherheit
- A.14 Anschaffung, Entwicklung und Instandhaltung von Systemen
- A.16 Management von Informationssicherheitsvorfällen

Aufbauend auf den oben gemachten Überlegungen gab die Oneconsult, nach der Abstimmung mit der Bundeskanzlei, die Prüfpunkte der Post vor. Die Post organisierte auf der Basis der Prüfpunkte die entsprechenden Interviewpartner und -termine. In den meisten Fällen waren die Interviewpartner die Teamleiter der entsprechenden Abteilungen, teilweise zusammen mit weiteren Fachspezialisten.

Die vertiefte Überprüfung erfolgte mittels gezielten Nachfragens, Prozess Walkthroughs, Dokumenteneinsicht und Plausibilitätschecks während der Interviews.

### 3.2.5 Projektorganisation

In der nachfolgenden Tabelle ist die Projektorganisation für die Durchführung der Sicherheitsüberprüfung aufgeführt:

| Rolle | Aufgabe |
|---|---|
| Projektleiter<br>(Bundeskanzlei) | → Projektmanagement<br>→ Schnittstelle zu Oneconsult<br>→ Koordination |
| Ansprechpartner<br>(Post) | → Projektmanagement<br>→ Schnittstelle zu Oneconsult<br>→ Koordination |
| Projektleiter<br>(Oneconsult) | → Schnittstelle zur Bundeskanzlei<br>→ Ressourcenplanung<br>→ Koordination |
| Security Auditoren | → Durchführung des Security Audits |
| Qualitätssicherung | → Controlling<br>→ Review Dokumentation |

Die Sicherheitsüberprüfung wurde in den folgenden Phasen durchgeführt:

| Phase | Daten | Teilnehmer | Aufgaben |
|---|---|---|---|
| Kick-off Meeting | 29.05.2019 | Bundeskanzlei<br>Post<br>Oneconsult | → Vorgehen und Zeitplanung<br>→ Evaluation von Methoden<br>→ Definition des Untersuchungsobjekts<br>→ Schnittstellen und Kontakte<br>→ Aufgaben zur Vorbereitung des Audits<br>→ Dokumentenanfrage |
| Analyse & Dokumentation | 03.06.2019 bis 21.06.2019 | Post<br>Oneconsult | → Sichtung der zur Verfügung gestellten Dokumente<br>→ Durchführung der Einzel- / Gruppeninterviews (an drei Kalendertagen)<br>→ Analyse<br>→ Verifikation<br>→ Verfassen des Auditberichts |
| Interviews – Teil 1 | 06.06.2019 | Post<br>Oneconsult | → Einführung in die E-Voting-Lösung<br>→ Competence Center E-Voting<br>→ Betrieb E-Voting |
| Interviews – Teil 2 | 12.06.2019 | Post<br>Oneconsult | → Physische Sicherheit<br>→ Personalprozesse<br>→ Benutzerverwaltung<br>→ Management von Informationssicherheitsvorfällen |
| Interviews – Teil 3 | 20.06.2019 | Post<br>Oneconsult | → Systemhärtung<br>→ Änderungsmanagement<br>→ Vieraugenprinzip |
| Dokumentation | 24.06.2019 bis 28.06.2019 | Oneconsult | → Analyse der Testergebnisse<br>→ Erarbeitung von Massnahmen<br>→ Verfassen des Schlussberichts |

# 4 Feststellungen und Massnahmen

Aus Gründen der besseren Lesbarkeit werden die Auditbefunde in generelle und spezifische Ergebnisse gegliedert. Die Aussagen sind aus Sicherheitsüberlegungen und rechtlichen Gründen allgemeiner als üblich gehalten.

## 4.1 Generell

Das Sicherheitsdispositiv der Post Informatik besteht aus technischen und organisatorischen Massnahmen, welche sich ergänzen und ist nach dem sogenannten Zwiebelschalenprinzip aufgebaut. Dies bedeutet, dass es einem Angreifer keinen echten Nutzen bringt, wenn er eine Schicht überwunden hat. Denn die anderen Schichten (Sicherheitsmechanismen) verhindern weiterhin einen erfolgreichen Angriff.

Die Kooperation der Post war während des ganzen Projekts vorbildlich. Alle Interviewpartner und die bei Detailfragen situativ beigezogenen Spezialisten konnten sämtliche Fragen von Oneconsult kompetent beantworten. Oneconsult hatte zu keinem Zeitpunkt den Eindruck, dass irgendwelche Sachverhalte seitens Post verheimlicht oder beschönigt wurden.

## 4.2 Maturitätsniveau

Oneconsult stellt fest, dass im Rahmen des Zertifizierungsaudits die Anforderungen an die E-Voting-Lösung gemäss Anhang der Verordnung der BK vom 13. Dezember 2013 über die elektronische Stimmabgabe (VEleS, SR 161.116) geprüft wurden. Das System der Post wurde damit als E-Voting-Lösung für 50% der Stimmberechtigten zertifiziert. Von der Post Organisation sind aus der Sicht der E-Voting-Lösung zwei Bereiche ISO 27001:2013 zertifiziert. Teile dieser Organisationseinheiten sind für den Betrieb der E-Voting-Lösung seitens Post zuständig.

Die in den Betrieb des E-Voting-Systems involvierten Bereiche und Teams der Post Informatik sind professionell organisiert und entsprechen damit «Good Security Practices». Dies zieht sich durch die gesamte Organisationseinheit von der Personalrekrutierung über den Betrieb vor, während und nach Abstimmungen bis hin zum IT-Notfallmanagement.

## 4.3 Schwachstellen

Es wurden keine Schwachstellen detektiert, die direkte Manipulationen am E-Voting-System ermöglichen.

Das Audit deckte dennoch sieben Schwachstellen auf, welche für sich alleine betrachtet kein direktes Risiko bergen, sondern eher einen organisatorischen Schönheitsfehler darstellen. Konkret werden die Sicherheitsmassnahmen und -prozesse gelebt (was gemäss «Security Good Practices» einem hohen Maturitätsniveau entspricht), aber insbesondere vereinzelte Prozessdokumentationen und -vorgaben sollten nachgeführt werden, um das hohe Sicherheitsniveau personenunabhängig beizubehalten.

Marginales organisatorisches Verbesserungspotential wurde in den folgenden Bereichen identifiziert:

- → Zutrittskontrolle
- → Zugriffskontrolle
- → IT-Notfallpläne
- → Authentisierung
- → Personalprozesse (3)

Die Post wurde anlässlich der Interviews darauf hingewiesen.

Das von den entsprechenden Schwachstellen ausgehende Risiko wird von Oneconsult im Gesamtkontext als niedrig eingestuft. Dies ist durch die obigen Punkte sowie das in Kapitel 4.1 erwähnte Zwiebelschalenprinzip zu begründen, wodurch die Post verschiedene Massnahmen zur Adressierung von Risiken umgesetzt und weitere Massnahmen risikomindernd wirken.

## 4.4 Massnahmenempfehlungen

Die zugehörigen Gegenmassnahmenvorschläge zur Behebung der Schwachstellen wurden der Post bereits kommuniziert und lassen sich mit relativ geringem Aufwand umsetzen.

Dokumentenende