Interpretazione errata della "verificabilità" nel voto elettronico CH

L'argomento principale citato per la sicurezza è la verificabilità: l'individuo, dove ognuno può controllare il proprio voto, così come quello universale, dove un ufficio centrale può verificare la correttezza del risultato.

La verificabilità universale è formalmente richiesta dalla Cancelleria federale come "verificabilità completa". Ma non può mai essere raggiunto, perché richiede che si possa determinare a livello centrale se tutti i voti degli aventi diritto al voto sono arrivati correttamente e sono stati elaborati correttamente. Tuttavia, se questo non può essere garantito già nel dispositivo utente (a causa del processo insicuro di guida per l'utente), è impossibile fino in fondo. Anche questi fatti sono riconosciuti e comunicati dal BFH. Tuttavia, ciò viene ignorato dalla Cancelleria federale e porta al riconoscimento delle soluzioni esistenti.

- **Perché abbiamo bisogno della verificabilità individuale (VI)?**

Con VI l'elettore si assicura il diritto di voto in sicurezza. Con VI l'elettore può verificare se il suo voto è arrivato come voleva. Se il processo sul dispositivo di input funziona perfettamente e non è falsificato da un attacco informatico, è guidato dall'utente e sa sempre cosa viene dopo e come interpretare i display. Le voci e i controlli del codice si alternano con la scheda di voto ricevuta per posta.

Questa scheda di voto con i relativi codici deve essere inviata per posta, perché qualsiasi codice generato elettronicamente potrebbe essere falsificato dallo stesso cyberattack e, al massimo, avere l'effetto opposto a quello desiderato dall'utente. L'uso di un secondo percorso di comunicazione per la trasmissione del codice fa parte della sicurezza che si desidera creare.

Solo questa macchinosa procedura manuale garantisce VI sul dispositivo di input non protetto. Se il processo sul dispositivo di input (telefono cellulare, computer) non funziona più correttamente al 100% o se viene visualizzato qualcosa di sbagliato, l'utente deve riconoscerlo e quindi ha solo la possibilità di votare per posta o a piedi verso l'urna.

Purtroppo, è facile superare le informazioni linguistiche manipolate sullo schermo e i suggerimenti che non devono essere presi in considerazione per non mettere in pericolo l'IVA. La mancanza di un singolo codice di controllo o di finalizzazione o l'inserimento prematuro del codice di conferma potrebbe portare alla manipolazione o alla mancata votazione, che l'utente noterà solo se memorizza il complicato processo.

Qualsiasi tipo di semplificazione con mezzi elettronici come le "nuove applicazioni", che potrebbero essere utilizzate per l'input, avrebbe di nuovo il rischio di manipolazione intrinseca e questo non può più essere superato con i.V.. Pertanto, qualsiasi approccio per semplificare questa complicata procedura sarebbe il colpo mortale per la verificabilità del voto elettronico CH, perché la verificabilità universale offerta dal voto elettronico CH non è indipendente e funziona solo con la completa applicazione dell'IVA. I fornitori di tali aiuti dovrebbero essere riconosciuti immediatamente e all'unisono come potenziali manipolatori e quindi vietati. Se si fosse saputo, il BK avrebbe certamente emanato raccomandazioni per non usarli.

Poiché, tuttavia, non si può presumere che tutti gli utenti si comportino correttamente e che non ci sia mai un incentivo a semplificare questa complicata procedura, l'i.V può essere riconosciuta solo come una garanzia teorica della scoperta di una possibile manipolazione. Tuttavia, come diritto dell'individuo, la procedura soddisfa i requisiti.

- **Perché abbiamo bisogno di una verificabilità universale?**

Poiché il fatto di cui sopra è noto ai lavoratori scientifici, essi hanno chiesto la verificabilità universale oltre alla verificabilità individuale. Si tratta di una questione di verifica da parte di qualsiasi organismo centrale per verificare se il risultato complessivo è corretto, che è un obbligo dello Stato di garantire la corretta determinazione della volontà del popolo.

Ora, quindi, ogni elettore dovrebbe essere in grado di comunicare allo Stato in modo sicuro se il suo voto è arrivato correttamente. Come abbiamo visto alVI, in realtà lo ha fatto, ma solo nei casi in cui non usa un dispositivo manipolato o riconosce la manipolazione dello stesso e poi usa un canale di sintonia alternativo.

Tutti gli altri casi (non-rilevazione, resa, furto di codice, ecc.) non possono essere individuati a meno che tutti non debbano rivelare pubblicamente se sono stati in grado di utilizzare correttamente VI Ma anche questo non è possibile, perché anche queste informazioni sono soggette al segreto di voto. Nessuno può essere obbligato a rivelare se ha votato o meno. Inoltre, quasi nessuno annuncia pubblicamente che non padroneggia la procedura, perché non si è mai abbastanza sicuri di aver fatto tutto nel modo giusto.

Poiché l'individuo ha anche il diritto alla corretta determinazione dell'intera volontà del popolo, e non solo il diritto di far contare correttamente il proprio voto, la verificabilità universale deve avvenire in modo tale da non dipendere da tutti gli altri elettori, che forse non hanno compreso tutte le complicate procedure o sono stati messi in ombra da un attacco informatico.

Con l'attuale concezione di E-Voting CH questo non è garantito. Pertanto, questo non può essere chiamato Verificabilità Universale. Il termine "verificabilità completa", così come utilizzato dalla Cancelleria federale, non rappresenta nient'altro che un tentativo di oscurare il problema con termini apparentemente scientifici.

Lì la verifica si divide in votazione e conteggio e il primo è (solo) legato al diritto dell'individuo e (solo) il secondo al dovere dello Stato. Ma entrambi dovrebbero valere per entrambi.

Pertanto, siamo giunti alla conclusione che la verificabilità universale del voto elettronico in Svizzera non è fondamentalmente possibile alle condizioni legali date e non rispetta la segretezza del voto.

La Cancelleria federale conta sul fatto che alcuni che notano una manipolazione potrebbero comunque segnalare. Può essere vero, ma come vengono trattate e ascoltate queste persone in seguito? E qual è la conclusione finale da trarre quando si sa che è solo una piccola parte del danneggiato che ci contatta? Chi sarà responsabile di ciò che deve essere fatto? Vogliamo ripetere la votazione o no? Tali messaggi erano forse solo un pretesto per ottenere una ripetizione? Chi controllerà tutto questo e come? Forse si possono trovare tracce, ma quante? Forse non riesci a trovarne nessuno. Perché queste indagini sono arbitrariamente complesse, lunghe e richiedono conoscenze specialistiche forensi di altissima qualità. Il termine per opporsi al risultato della votazione è di 6 giorni. In questo periodo l'amministrazione non otterrà alcun risultato.

Allora che cosa significa? Tutte queste domande relative alla gestione del rischio non sono state chiarite durante l'introduzione dell'E-Voting CH. L'unico risultato certo di un tale processo è un enorme caos e la perdita di fiducia nei processi democratici.

- **Come funziona la "piena verificabilità" del POST (garantendo il conteggio dell'autenticità)?**

Poiché, tuttavia, non si può presumere che tutti gli utenti si comportino correttamente e che non ci sia mai un incentivo a semplificare questa complicata procedura, l'i.V può essere riconosciuta solo come una garanzia teorica della scoperta di una possibile manipolazione.

Durante il controllo di conteggio, il POST presuppone che un possibile problema (cyberattack) sia localizzato su una parte del sistema e se questa parte è gestita in modo ridondante e la sequenza è gestita tramite entrambe le ridondanze, che l'errore è scoperto dalla formazione della differenza. Questo assunto è corretto in linea di principio, ma contiene un numero enorme di insidie.

Sebbene i componenti del sistema possano essere gestiti in modo ridondante, anche il produttore (non solo il fornitore) deve essere gestito in modo ridondante. La domanda è se si sa veramente chi è il produttore della mia parte del sistema? Che cosa succede se "Manufacturer 1" acquista anche le sue parti (chip, middleware, software, compilatori, ecc.) dallo stesso subappaltatore di "Manufacturer 2"? Chiunque lavori nel settore IT sa di non avere mai nessuna di queste informazioni e che molti componenti di sistema provengono dalle stesse grandi aziende (Intel, AMD, Microsoft, Apple, Apple, ecc.). Questo porta alla consapevolezza che i punti deboli sono automaticamente localizzati su sistemi ridondanti.

Inoltre, anche gli operatori di questi sistemi dovrebbero essere separati, perché altrimenti non sarebbe garantito che uno dei due operatori manipolerebbe entrambi i sistemi se avesse un incentivo corrispondente a farlo. Si dovrebbe anche guidare il controllo degli operatori in modo ridondante, perché altrimenti qualche superiore potrebbe avviare una manipolazione corrispondente, ad esempio con il pretesto di un aggiornamento necessario.

A causa della complessità di questi controlli delle differenze di tutte le parti del sistema, sono necessarie anche procedure di aiuto corrispondenti che mostrano le differenze e quindi anche l'autenticità dei risultati del conteggio. Se questi non indicano una differenza, si presume che siano corretti. Ma ora devi assicurarti che queste procedure non siano manipolate. Puoi assicurarti che questo sia il caso solo se hai altri strumenti per controllarlo. Questo ciclo potrebbe continuare per un po' di tempo fino al punto che un abile capo operatore dice: "Ho tutto sotto controllo". Ma credo che sia l'unico a poterlo giudicare. Oppure parla per mancanza di esperienza o per eccessiva sopravvalutazione di se stesso perché non conosce i suoi avversari? E: possiamo o dobbiamo fidarci di lui?

Anche se tutto è stato fatto alla perfezione e i dipendenti erano affidabili: È arbitrariamente complesso e non può essere trascurato da terzi, soprattutto dalla commissione elettorale che ne è responsabile.

L'11.9.9.2018 il Parlamento ha affondato un'avanzata che chiedeva la trasparenza dei processi, così come questa è richiesta anche come parte dei diritti umani per la credibilità di una democrazia. Con questa edizione non si vede più la possibilità di utilizzare il voto elettronico e si fa riferimento a processi che non tutti possono capire senza una conoscenza specifica, anche nel caso del voto classico. La sorprendente differenza tra i requisiti per comprendere il "doppio Pukelsheim" e l'IT

moderno viene elegantemente ignorata. Anche un secondo anticipo, che richiedeva solo una moratoria, non ha avuto alcuna possibilità.

Rimane una conseguenza: la democrazia diventa un'espertocrazia. La domanda è, vogliamo noi così?