Domande e risposte

Voto elettronico. Test pubblico d’intrusione

1. La Confederazione ha il diritto di ricompensare finanziariamente gli attacchi degli hacker?

La Posta Svizzera è incaricata di ricompensare le persone che segnalano violazioni della sicurezza. Essa determinerà l’importo del compenso e procederà a versarlo. La Confederazione e i Cantoni stanzieranno un importo di 250 000 franchi per la realizzazione del test pubblico d’intrusione, conformemente al piano strategico del Governo elettronico Svizzera.

2. Con un test pubblico d’intrusione si cerca di dimostrare che il sistema di voto elettronico non può essere violato?

No. Lo scopo del test pubblico d’intrusione è di identificare i punti deboli e, se necessario, porvi rimedio. Inoltre, è nell’interesse della trasparenza che il maggior numero possibile di esperti indipendenti si intenda di sicurezza del voto elettronico. Il test pubblico d’intrusione potrebbe offrire loro l’opportunità di esaminare il sistema di voto elettronico.

3. Spetta dunque a esperti indipendenti identificare tutti i punti deboli?

No. Il test pubblico d’intrusione è una delle tante misure di sicurezza. Ogni sistema informatico presenta dei punti deboli, come nel caso del sistema di voto elettronico anche dopo il test pubblico d’intrusione. È fondamentale che nessun punto debole comporti un rischio maggiore. I punti deboli devono essere contrastati con misure di sicurezza sufficientemente efficaci. Con la verificabilità completa, il voto elettronico si avvale di una misura di sicurezza globale e particolarmente efficace che non esiste per altri servizi. Inoltre, i sistemi sono controllati e certificati a intervalli regolari da un organismo accreditato.

4. Per la verificabilità completa sono necessari anche i computer. Questi computer non presentano punti deboli?

La verificabilità completa presuppone essenzialmente il fatto che la manipolazione di una sola componente non basta per falsificare i voti senza che nessuno se ne accorga. Se viene manipolata una sola componente, altre concorrono a identificare qualsiasi tentativo di manomissione.

5. Quanto serio deve essere un punto debole perché la persona che lo segnala riceva un compenso finanziario?

A essere determinante non è la gravità del punto debole quanto piuttosto il fatto che durante il test i partecipanti si attengano alle regole del gioco. In linea di principio sono ammessi e auspicati tutti gli attacchi che potrebbero portare maggiori conoscenze sulla sicurezza del voto. Gli attacchi destinati esclusivamente a identificare vulnerabilità note non potranno essere ricompensati. Alcuni attacchi sono addirittura vietati, benché siano indubbiamente legati a un rischio elevato: tuttavia, per tenere questi rischi sotto controllo, sono disponibili mezzi più efficaci.

6. Quali attacchi sono esclusi?

Sono autorizzati e ricompensati gli attacchi condotti a buon fine che sono stati mossi contro l'infrastruttura di voto elettronico della Posta Svizzera. Altre organizzazioni (Cantoni, tipografie, altri servizi offerti dalla Posta) non partecipano al test pubblico d'intrusione e non devono di conseguenza essere attaccate. Inoltre, gli attacchi di diniego dei servizi (*distributed denial of service*) sono vietati, in quanto non forniscono alcuna nuova informazione nell'ambito di un test pubblico d'intrusione, possono essere testati in altro modo e disturberebbero altresì lo svolgimento del test. Allo stesso modo, non sarà corrisposto alcun compenso per gli attacchi alle piattaforme utente degli aventi diritto di voto. Lo stesso vale per gli attacchi che mirano a persuadere gli attori a discostarsi dai processi previsti con messaggi falsati (*social engineering*). Gli attacchi condotti a buon fine traggono vantaggio dai comportamenti inappropriati che non possono essere simulati in modo realistico nell'ambito di un test pubblico d'intrusione. Chi riesce comunque a manipolare il sistema di verificabilità individuale (quando viene votato il «sì», ed è un «no» che viene visualizzato) senza che gli elettori riescano ad accorgersi della manipolazione, riceverà un compenso finanziario.

7. Il test pubblico d'intrusione non rischia di insegnare anche agli hacker come violare il sistema di voto elettronico?

Qualcuno potrebbe segnalare un punto debole a un potenziale hacker e non agli organizzatori del test pubblico d'intrusione. Questo non rappresenta un problema purché gli organizzatori siano a conoscenza del punto debole e lo eliminino se necessario. Il compenso promesso dalla Posta vuole essere un incentivo a segnalare i punti deboli del sistema (anche) agli organizzatori. Inoltre, i tentativi illegali di individuarli possono essere effettuati anche indipendentemente dal test pubblico d'intrusione. Il test permetterà invece anche a persone ben intenzionate di esaminare il sistema nel dettaglio per cercare di identificarne le vulnerabilità.

8. Perché ci si serve del voto elettronico se il sistema non è ancora stato sottoposto ad alcun test pubblico d'intrusione?

Il sistema che sarà sottoposto a un test pubblico d'intrusione è il primo sistema a offrire la verificabilità completa. I sistemi attualmente in uso offrono una verificabilità individuale, ma non ancora una verificabilità completa. Poiché la verificabilità completa consentirà un uso più ampio del voto elettronico, qualsiasi sistema che offra tale verificabilità dovrà soddisfare requisiti di sicurezza ancora più elevati, comprese la certificazione e la pubblicazione del codice sorgente. Inoltre, la Confederazione e i Cantoni hanno deciso che i sistemi di voto elettronico che offrono la verificabilità completa devono essere sottoposti a un test pubblico d'intrusione prima di poter essere utilizzati per la prima volta.