Il voto sulla piattaforma Rousseau: una barzelletta pericolosa

Giornali e TV hanno dato al voto dei giorni scorsi sulla piattacforma Rousseau una vastissima eco. Il futuro del nostro paese sarebbe dipeso da un voto online di 100000 persone in barba ai princìpi costituzionali ed alle prassi istituzionaliche regolano la nostra comunità. Siccome io non credo al fatto che una piattaforma online possa e debba determinare il futuro di una nazione, vi propongo un articolo nel quale alcuni esperti ci mostrano quanto la piattaforma Rousseau sia sicura e come non possa essere un organo di ratifica delle decisioni prese in Parlamento. Dal Movimento assicurano che la piattaforma è inviolabile. La mia esperienza dice che nessuna piattaforma Internet è inviolabile. Riporto qui un intervista rilasciata a Daniele Bonistalli da Gianni Cuozzo, esperto di cybersecurity. Buona lettura e aprite gli occhi.

> *Gianni, ci sono molte polemiche attorno al voto delle prossime ore sulla piattaforma Rousseau. Dal Movimento 5stelle fanno sapere che il sito è sicuro. Ma come stanno davvero le cose? Rousseau è vulnerabile?*
> *Ogni produttore o fornitore di servizi online giurerebbe sulla sicurezza informatica dei propri sistemi ma, sfortunatamente, non è così. Da Rousseau proclami del genere ne sono sempre arrivati, anche quando la situazione era chiaramente più critica di quella attuale. Ne è testimonianza l'operazione dell'agosto 2017 di Luigi Gubello aka "Evariste*

Gal0is", che dimostrò come il database utenti non fosse sicuro e come le password policies (la politica per l'utilizzo di password, ndr) dei propri amministratori non fossero esattamente all'ultimo grido. Quell'operazione costò alla fondazione Rousseau una multa di circa 50.000 euro da parte del garante della privacy. Davide Casaleggio, tra l'altro, reagì scompostamente con una querela, invece di ringraziare Gubello per aver sottolineato le falle del sistema.

Oggi leggendo il comunicato rilasciato dal Movimento 5 Stelle, rimango colpito da informazioni a dir poco fuorvianti. Al punto 2 del comunicato. Si bollano come "FAKE NEWS" le preoccupazioni avanzate dagli esperti sulla sicurezza della piattaforma, elencando poi una lista di tecnologie che, a loro dire, dovrebbero rassicurare sugli standard utilizzati. Nel comunicato ad esempio si dice che Keycloak (programma per la gestione del login, ndr) "non è mai stato hackerato". E' falso: Keycloak è un software open-source, cioè con codice sorgente libero e aperto alla contribuzione di terzi, e negli anni ha avuto diversi problemi di sicurezza. Basta cercare su Google "keycloak cve" (Common Vulnerability Exposure) per rendersene conto. Stesso discorso va fatto per le dichiarazioni sull'utilizzo di "moduli e framework per la piattaforma aggiornati". I sistemi aggiornati sono utili solo contro vulnerabilità o tecniche di exploitation note, questo non significa che il sistema sia sicuro o "immune" bensì che non è facilmente aggredibile (il che è già un bene). Gli amministratori della piattaforma però non devono dormire sugli allori: non sono da escludere attacchi provenienti da altre nazioni volte a gettare benzina sul fuoco in un momento istituzionale delicato come quello che stiamo vivendo. In sintesi, penso si siano fatti buoni passi in avanti per quanto riguarda la sicurezza della piattaforma Rousseau ma rimane comunque vulnerabile ad attacchi più sofisticati e strutturati.

E come si potrebbe riuscire a mettere a segno questi

attacchi?
Sul blog dei 5 stelle si fa riferimento ad un sistema di sicurezza con doppio fattore via SMS (2FA). Esistono diverse tecniche che hanno dimostrato come sia possibile bypassare questa autenticazione a doppio fattore:alcune possono intercettare il codice di autenticazione rendendo vana la misura di sicurezza. Ad esempio esistono tecniche di SIM Swapping per replicare il messaggio che viene inviato via sms: il tutto grazie a delle falle nei protocolli di comunicazione delle celle telefoniche (SS7). Un attacco simile è stato subito da "Coinbase", la più grande piattaforma per lo scambio di Cryptovalute al mondo, che di sicuro aveva requisiti di standard di sicurezza molto più restringenti e budget molto più alti di quelli della fondazione Rousseau. Un altro modo per "bucare il sistema", che potrebbe impedire il voto in toto, risiede nel tracciare l'architettura che genera il codice che viene inviato via SMS e abbattere uno specifico server. Questo impedirebbe agli utenti di ricevere l'SMS per accedere alla piattaforma e quindi far saltare la votazione. Purtroppo la Fondazione non ci dà indicazioni del livello di resilienza dell'intera piattaforma ma, considerando i budget dichiarati, ho ragione di pensare che la sicurezza sia piuttosto limitata e quindi fossi in loro ci andrei piano nel parlare di "immunità della piattaforma Rousseau".
Gianni Cuozzo, classe 1990, è esperto di cybersecurity e consulente strategico per diversi paesi Nato
Quindi il voto per il "progetto di governo" del 3 settembre può essere manipolato dall'esterno?
Sì. Molti degli attacchi di cui abbiamo parlato sono mirati, quindi non replicabili su vasta scala, ma possono colpire singoli utenti particolari come quelli con privilegi d'amministrazione all'interno della piattaforma. Inoltre esistono tecniche di "elevazione dei privilegi" con le quali, sfruttando degli errori nel codice, si può trasformare un utente semplice in un utente con

privilegi
d'amministrazione. Da lì tramite tecniche di "escaping" si può passare dalla piattaforma ad attaccare il server nella sua interezza e quindi andare poi a cercare il database ed alterarne i valori. Ovviamente stiamo parlando di attacchi non semplici da eseguire, ma sono possibili. Un'altra via per manipolare l'esito delle votazione risiede nell'attaccare il database in cui questi voti vengono salvati. Ogni
volta che un utente effettua una votazione viene popolata una tabella su un database e, per analizzare la votazione, può venir fatta una richiesta alle varie tabelle degli utenti votanti. Se alterate, queste
tabelle nel server, possono esporre dati alterati agli stessi amministratori di Rousseau. E nessuno se ne accorgerebbe. Le statistiche ci dicono che circa il 70% di chi subisce un attacco non sa che è sotto attacco o che è stato sotto attacco.
E dall'interno? E' possibile che in piattaforme del genere sia prevista la modifica degli esiti di una consultazione senza renderne conto agli utenti?
Assolutamente sì. Dall'interno un amministratore con i giusti livelli di privilegi può, tramite semplici script, sovrascrivere le tabelle dei database a proprio piacimento ed alterare il risultato della votazione.
Così quando vengono prodotti i risultati, essendo anonimi, nessuno può rendersi conto della cosa.
Ci sono precedenti che testimoniano come si possa modificare il voto?
Al Def Con, la più grande conferenza hacker al mondo che si tiene tutti gli anni a Las Vegas, da diversi anni è presente una sezione dedicata all'alterazione dei sistemi di votazione online. L'anno scorso, ad esempio, sono state manomesse le cabine digitali utilizzate nelle ultime votazioni negli Stati Uniti. Quindi sì, è assolutissimamente fattibile e
ci sono diversi sospetti che ciò sia accaduto durante alcune votazioni nell'est Europa e in Sud America: sia da apparati statali che da organizzazioni criminali che agivano per conto

terzi.
Che capacità e che strumenti deve avere un potenziale attaccante della piattaforma? E' così difficile?
Per quanto riguarda gli strumenti, non si ha bisogno di nulla oltre ciò che si può facilmente reperire in internet: basta un pc qualsiasi ed una connessione. Per quanto riguarda operazioni ad alta intensità computazionale, come ad esempio decodificare HASH (Codici che nascondono le password) o generazione di traffico massiccio, vi sono diversi servizi online sia su internet in chiaro, sia nel deep web, che con qualche migliaio di euro possono fornire tutta la potenza necessaria.
Quello che cambia molto però è la preparazione dell'hacker, in gergo lo "skill". Come detto penso che, anche se non perfetta, negli ultimi anni la sicurezza di Rousseau ha fatto passi in avanti, ma ovviamente ciò non la rende immune, bensì più difficile da violare. Del resto tutte le contromisure di sicurezza informatica non mirano a rendere inviolabile un'organizzazione o una piattaforma, ma a rendere più complesso l'eventuale attacco, per far sì che l'equazione costo:target:rischio sia sconveniente. Per quanto riguarda Rousseau però il target è molto appetibile quindi penso che oltre agli "hacker della domenica" ci possano essere strutture ed organizzazioni ben più complesse che abbiano lo skill necessario per compiere operazioni del genere.

Esistono piattaforme veramente inviolabili?
Assolutamente No. Fino a poco tempo fa si sono sentiti teorici puntare molto sulle votazioni tramite blockchain. Personalmente ritengo anche quell'approccio fallimentare. La blockchain non è necessariamente "anonima" in quanto si basa su registri pubblici che vengono condivisi con tutti gli utenti di una rete e, sebbene questo approccio possa essere anonimizzato, sono culturalmente contrario ad un sistema di votazione basato su registri pubblici. Inoltre, da un punto di vista

tecnico, essendo la blockchain basata su registri decentralizzati su più nodi, l'alterazione di un solo nodo comporterebbe la sincronizzazione dei nodi di tutta la rete, mettendo a repentaglio l'intera catena di sicurezza. E questo è dimostrato anche dai recenti attacchi alla blockchain descritti in un articolo apparso sul MIT Tech Review.

In conclusione, il voto online è da considerarsi una pratica pericolosa?

Non è ancora giunto il tempo per votazioni di questo tipo online. Finchè non avremo tecnologie di anonimizzazione efficaci e sicure, penso che la cara e vecchia matita debba avere vita lunga. Il voto online è ancora più pericoloso quando poi avviene su una piattaforma chiusa, appartenente prima ad una società privata e poi ad una fondazione privata, di cui non si conosce il codice sorgente, non è possibile vedere gli audit di sicurezza e non se ne conosce con esattezza l'architettura. Consiglio alla fondazione Rousseau di dare certezze tecniche in tal senso, con documenti e codici sorgenti visionabili e non con proclami da televendita anni '90.

Daniele Bonistalli

Fonte: https://medium.com/@daniboni/altro-che-fake-news-vi-spiego-perché-rousseau-non-è-inviolabile-77267febd5c4