O *i-voting*: benefícios, precauções e ameaças

Em prol da transparência e para permitir um maior entendimento sobre o que é a proposta do Voto Universal/*i-voting*, identificamos de seguida algumas questões, não de forma exaustiva, para discutir o tema com a seriedade que merece. Qualquer atenção aos detalhes *i-voting* não será desperdiçada, pois esclarecerá os Sócios.

A proposta de *i-voting* tem de esclarecer e dar cabal resposta em três domínios:

1. **PESSOAS**
    a) **Autenticação de Sócios Votantes**
        i. A complexidade da *password* é imposta? (O objetivo é evitar *passwords* como sporting123)
        ii. É de suma importância garantir que o eleitor seja verdadeiramente o Sócio do Sporting. As melhores práticas apontam para o uso de autenticação multifatorial ao validar a autenticidade de um utilizador. Existem três (3) fatores que podem ser usados:
            1. 1. Algo que o Sócio conhece (ou seja, uma *password*, um número PIN)
            2. Algo que o Sócio possui (ou seja, um *smartphone*, um cartão)
            3. Algo que o Sócio é (ou seja, leitura de íris, impressão digital)
        iii. Uma combinação de pelo menos dois destes fatores é considerada segura. Embora não seja 100% seguro, pois existem maneiras de contornar cada fator.

A AMEAÇA: O Sporting propõe a utilização de credenciais de utilizador (algo que conhece) e algo que possui (cartão de Sócio Sporting, utilizando os últimos 5 dígitos do código de barras). Ora, neste momento isto é questionável, pois terceiros já conhecem os 5 dígitos. O facto de a *Gamebox*, que é transmissível, ser atualmente o cartão de Sócio, invalida também esta utilização. Além do mais, a efetivação de uma candidatura, obriga o regulamento, pressupõe a recolha de assinaturas com cópia do Cartão de Cidadão e do cartão de Sócio, tonando um dado que devia de ser privado num dado público que passa por diversas “mãos”. Assim, fica invalidada a integridade desta informação vital para a solução proposta pela direção.

Existe uma alternativa para o uso de autenticação de pelo menos dois (2) fatores para autenticação do utilizador?
Que não utilize os 5 dígitos do cartão de Sócio, ou seja, *password* de uso único (*one time password*) enviada para o número de telefone registado?
Pelo menos o risco seria de alguma forma minimizado já que o código a ser enviado é gerado no momento e durante a autenticação do utilizador/Sócio.

b) Rastreabilidade de Voto

Assim que o utilizador estiver autenticado no sistema e prosseguir com a votação:

i. Onde é que o voto é registado?
ii. É numa base de dados central?
iii. É num sistema intermediário (coletor) que envia as informações para uma base de dados central?
iv. Quem/quais entidades estarão autorizadas a manipular os dados?
v. Todas as ações são registadas e enviadas para uma solução de registo centralizada, sem possibilidade de serem adulteradas?
vi. O utilizador é capaz de confirmar o voto antes de ser registado no sistema?
vii. O utilizador pode alterar seu voto? Se sim, como?
viii. O utilizador/Sócio é informado sobre seu voto final?

2. TECNOLOGIA

a) A solução a utilizar será a mesma colocada em prática nas últimas eleições? Ou seja, a Universidade do Minho que desenvolveu a solução informática (em 2009 acrescente-se) era ao mesmo tempo a entidade que estava a auditar o processo eleitoral. Esta prática é claramente errada, uma vez que quem implementa não deve auditar a sua própria implementação.
b) Quem são as entidades já identificadas e consultadas, capazes de desenvolver a solução técnica?
c) Quais serão os critérios usados para selecionar o fornecedor?
d) Essas entidades a selecionar estarão certificadas de acordo com padrões de segurança da informação, como é exemplo o ISO 27001/NIST/Cyber Essentials?
e) A solução será certificada de acordo com práticas seguras de revisão de código (*secure code review*)?
f) Que garantias serão dadas para que a solução selecionada esteja protegida contra os principais ataques cibernéticos e ataques de código conhecidos?
g) Durante o processo de seleção estão previstos a realização de testes de penetração às soluções propostas?
h) A solução é capaz de identificar o comportamento normal e esperado do *host* e da rede para identificar atividades anormais? Ou seja, acesso remoto suspeito, tráfego de rede, regras de *firewall*, etc.?
i) As melhores práticas de gerenciamento de vulnerabilidades são aplicadas na solução proposta?
j) As melhores práticas de gestão de credenciais são aplicadas nos repositórios de utilizadores a serem usados/integrados na solução proposta?

k) Como serão os votos guardados nos sistemas? Serão encriptados? Quem é que terá acesso aos mesmos? Quem serão as pessoas internas do Sporting e pessoas externas, sejam entidades parceiras/fornecedores que terão acesso aos votos? Quais serão os privilégios sobre essa informação? Em que papel terão esses mesmos privilégios?
l) Que papel será atribuído às listas concorrentes e quais os privilégios que terão para participação e controlo do processo?

3. PROCESSOS

a) Que alterações ao regulamento eleitoral existirão?
b) Que forma existirá para relatar um incidente?
c) O que está previsto em termos de equipa e processo para dar resposta a incidentes que sejam relatados por eleitores elegíveis durante a votação?
d) Existirá um processo alternativo para permitir que um eleitor vote?
e) Vai ser possível acompanhar o histórico de incidentes?
f) Vai estar disponível aos Sócios eleitores para fins de auditoria?

Nuno Sousa, Sócio nº6257-0
Candidato à presidência dos órgãos sociais do SCP nas eleições de 2022
#PeloMeuSporting