ork_
OIKEUSREKISTERIKESKUS
RÄTTSREGISTERCENTRALEN

Trends in Securing Election Technology

28.10.2024 Juha Mäenalusta

Who

- Senior Information Security Specialist
  - CISSP, CEH
- Legal Register Centre
  - IT services for agencies of Ministry of Justice (courts, prisons, elections, data protection agency etc)
  - ~200 staff
  - 100M€ yearly IT budget
  - Election Information System, postal voter registration system, party registration system…

Practical cybersecurity

- From an actual old slide:
  - All the usual stuff, like firewalls, SIEM, DDOS protection, backups, backup systems, backup offices etc have also been tested in multiple exercises and are tested before every election
- Pre-2016 some countries may have had slightly non-standard approach to practical cybersecurity
- Since then, (most) election administrators have realized
  - That election information systems are information systems
  - That information systems need to be secured
    - Especially if connected to the Internet
  - That this is business as usual for all organizations (that have information systems)
  - That there are good standard ways to do this stuff
    - But that these are not static
  - That weaponized disinformation needs to be countered with transparency

Specific to Elections

- High visibility target-> Resilience and backup systems and processes
  - Front pages are reserved for elections even when everything goes smoothly
- Time-critical -> High availability
  - Very detailed time requirements that are extremely hard to modify
- Multiple stakeholders-> Networks and communication, professional IT management
  - Several state agencies, municipalities, multiple service providers, media, parties, citizens…
- Interesting target for multiple adversaries-> Preparation for APTs and script kiddies
  - Multiple and constantly rapidly evolving methods, that spread to others
- Processes have components in digital, physical and information space-> Comprehensive security, not cybersecurity
  - Attacks can happen in any or all spaces
- Essential component of democracy-> Build trust
  - Requires transparency and understandability

Government systems are not the easiest targets

- Initially good or improved government systems and procedures have done a lot to secure national government-run election-related systems
  - Not perfect, but..
- The result is not nearly as good with the other stakeholders in the election space
  - Candidates / Parties
  - Media
  - Service providers (to the governments and others)
  - Sub-national level government organizations
- And this is widely known and used
  - Most recent public attacks: Germany 2024: CDU and SDP
- These organizations need support from governments
  - There are many stakeholders, and some might not be receptive to support

Paper mail decline

- Use of paper mail is in decline globally
- Lots of changes
  - Takes more time, especially with international mail
  - Less mail overall -> election mail easier to identify
  - Access to postal mail getting harder
- Affects postal voting, but also in many countries polling stations abroad and nationally
- Change is quite rapid
- Might lead into countries looking into I-voting

- Some similarities with the transition to mobile first or mobile only approach with citizens, but is an important trend if there is I-voting

Post-Quantum Encryption

- Seems to be the main topic today, for very good reasons
- Security of ”existing data”
  - Asymmetrically encrypted data can be captured now or can have been captured a long time ago
  - Can be any data, voter rolls, I-votes, credentials…
  - Can also be digital signatures claiming to be created in the past but created in the future by adversaries
- Transition to the future
  - So many technologies, anything can be the weakest point, and almost everything needs to be updated
  - The new algorithms have years of analysis, not decades…
    - Hybrid algorithms are the usual solution, but do their features work in election usage?
  - Math is even harder than with the current asymmetrical algorithms -> who can understand verify all the implementations?

Increasing regulation

- Many sources
  - International: GDPR, NIS2…
  - National
  - Intergovernmental: Council of Europe recommendations, EU Compendium
- Some is general cybersecurity
  - Risk management, management, policies, reporting, encryption, suppy chain security, security testing
  - Both technical and organizational
- Some is election-specific
  - Principles of democratic elections, inter-agency collaboration, transparency, capacity to operate and assess security of election-related information systems

Balancing transparency and secrecy

- ” Providing transparency in all aspects of an election is key to conducting a **successful and trustworthy election**, and to **promoting trust** in the process, even more so when ICT solutions are used. Increasingly, non-IT experts experience difficulties understanding ICT solutions.” CoE Guidelines
- But this needs to be balanced with the need to keep some information confidential to be able to secure the systems
  - Acknowledged in the guidelines
- Hard process that needs a lot of expertise and transparency in the process itself
- Especially hard, as time to exploit vulnerabilities has become significantly shorter
  - Anything exposed to the Internet can and will be exploited fast, possibly with AI assistance
- Audit and certification cannot be for a static system, the need to patch at short notice needs to be considered
- Trust needs to be built on the processes and actors, instead of just static systems

Management, not technology

- Multiple hard problems that require
  - Expertise, in multiple disciplines
  - Collaboration, with all the stakeholders
  - Communication, to the public
  - Fast response, to vulnerabilities and incidents
- Responsibility can never be outsourced
  - EMB:s need the competence to manage hard technology and technology-related processes
  - Includes all parts of the lifecycle: setting requirements, procurement, quality control, operation, auditing, providing transparency
- The list of things to consider is getting longer and so the level required of competence in management is getting higher
  - Also, horizon scanning should be a part of this ☺

ork_

OIKEUSREKISTERIKESKUS
RÄTTSREGISTERCENTRALEN