[SingCERT] Cyber Threat Advisory for Singapore Presidential Elections 2017

Background

Over the past few years, there have been reports of hackers launching cyber-attacks and/or compromising IT systems used by political parties and election candidates in an attempt to disrupt the election processes. With the upcoming Singapore Presidential Election due to be held in September 2017, there is a need for candidates and personnel involved in the election process to be aware of the risks involved and to take actions to heighten their defence against the possibility of a cyber-attack on their supporting IT systems.

Aim

This advisory provides information on the possible cyber threats, examples of past election-related events, and how candidates can mitigate and prevent against the threats.

Managing and Securing IT Systems

Candidates relying on Internet and digital IT systems to support their campaign should be mindful of potential cyber threats. Attempts to interfere with the electoral processes through cyber means cannot be underestimated as demonstrated in recent events such as the US Democratic National Committee (DNC) hacking incident in 2016. Candidates need to take steps to safeguard their digital systems, including their Internet election advertising platforms. While such platforms have become an essential tool for campaigning, they need to be properly protected against potential cyber threats.

Candidates should appoint a trusted IT system administrator to oversee the implementation of such systems. The role of an IT system administrator is to:

- Be responsible for the security of the IT systems used to support the election campaign.
- Familiarise themselves with the IT core infrastructure and ensure that security measures are incorporated into the system design.
- Ensure that such systems are closely monitored for signs of a cyber-attack, with appropriate incident response plans and resources put in place as a contingency. [*Incident Response Planning Guideline:* https://security.berkeley.edu/incident-response-planning-guideline]
- Ensure that system resiliency and disaster recovery plans are established. [*An IT Administrator's 5 Simple Steps for Disaster Recovery:* https://siliconangle.com/blog/2012/09/19/an-it-administrators-5-simple-steps-for-disaster-recovery/]

Possible Cyber Threats

Some of the possible threats that could be encountered during election period includes:

1. **Defacement** of campaigning or any election-related websites involving candidates

   1.1 Definition of Defacement

   Website defacement is an attack on a website that changes the visual appearance of the site's homepage or subsequent pages. The defaced page usually displays a message left behind by the hacker to mock system administrators on the weak security of the system. Website defacement is also carried out to express political unhappiness and may sometimes contain disturbing graphics or images.

   1.2 Impact

Defacements can bring damage to a political candidate's or political party's reputation. It can also be used as a distraction to cover up another wave of attack.

1.3 Recent Example

During the United Kingdom's General Election 2015 voting period, Wikipedia pages of political leaders were defaced, replacing it with a picture of the opposition leader and a red background.

Read on for more information at:
http://www.express.co.uk/news/politics/575693/Election-2015-David-Cameron-s-Wikipedia-HACKED-and-replaced-with-Ed-Miliband-image

1.4 Recommendations

The following are recommendations to IT system administrators on the steps to take to secure the IT systems used in election.

LINKS

Web Defacement Best Practices

https://www.banffcyber.com/best-practices-to-address-the-issue-of-web-defacement/

Tools and Strategies Against Defacement

http://searchsecurity.techtarget.com/tip/It-doesnt-take-rocket-science-to-prevent-Web-site-defacement

1. Carry out security audits and penetration testing
    a. Regular evaluation of the IT infrastructure (operating systems, service and application flaws, improper configurations or risky end-user behaviour) to better protect the system
2. Strengthening defences against SQL injection attacks
    a. Preventing the usage of SQL statements that could be inserted into data entry fields to affect the execution of predefined SQL statements (Using bound variables with prepared statement method)
    b. Validating input where possible, such as limiting input only to accepted characters, whitelisting possible set of values and checking the length of input
3. Strengthening defences against Cross-Site Scripting (XSS) attacks
    a. Prevent the passing of scripting code into a web form to deny the attempt to run unauthorised code on the website (Encode HTML Output and Encode URL Output)
    b. Usage of Web Application Firewalls (WAF) to check for malicious input values, modification of read-only parameters, filter out malicious output and block suspicious requests
4. Use defacement monitoring and detection tools
    a. Monitor any defacement or unauthorised integrity change in the websites
    b. Carefully evaluate and configure the tools to detect both full and partial defacements involving HTML as well as linked images, scripts and stylesheets.
    c. Consider tools that find, detect and automatically reverse unauthorised changes to your site
5. Prepare ahead to respond to defacement incidents

a. Form a technical response team involving the security manager, web master, web developers and the web server team

b. Prepare a public message to preserve the reputation of the candidates

c. Be on standby to take down the defaced web server for offline investigation and forensics

d. Assess the level of penetration and determine if any sensitive information is compromised

Prepare a maintenance page or create a secure replica to handle the restoration process and reduce the recovery period

2. **Distributed Denial of Service (DDoS)** attacks launched at candidate's websites and supporting IT systems to disrupt election processes

2.1 Definition of DDoS

DDoS is another form of cyber-attack that aims to make servers, websites or network services unavailable by overwhelming it with data packets from multiple compromised machines, thereby denying legitimate users access to the services.

2.2 Impact

Successful DDoS attacks may not be as simple as crashing a website or network service. Skilled hackers may use DDoS to infiltrate a network, steal sensitive data and leak the data onto the Internet.

2.3 Recent Example

A three-pronged wave of cyber-attacks, including DDoS, were aimed at Ukraine's Central Election Commission to cause interference to the 2014 Ukrainian presidential election processes.

Read on for more information at:
https://www.csmonitor.com/World/Passcode/2014/0617/Ukraine-election-narrowly-avoided-wanton-destruction-from-hackers-video

2.4 Recommendations

The following are recommendations to IT system administrators on the steps to take to secure the IT systems used in election.

LINKS

DDoS Prevention and Mitigation Methods

http://www.techrepublic.com/blog/it-security/ddos-attack-methods-and-how-to-prevent-or-mitigate-them/

https://security.stackexchange.com/questions/73369/how-do-major-sites-prevent-ddos

https://www.wired.com/insights/2012/12/the-5-essentials-of-ddos-mitigation/

1. Increase Bandwidth Subscription

a. Candidates should lease a significantly larger capacity than they need to account for sudden increase in views from the members of public and DDoS attacks.The increase in bandwidth will prevent an attacker from mustering enough traffic to overwhelm, causing a volumetric attack to be generally ineffective

2. Use Automated Mitigation

a. Consider using tools to monitor net flow data from routers and other data sources to determine the baseline for traffic. DDoS mitigation tools can attract the traffic to them when the traffic patterns step out of the baseline or they can utilise mechanisms that can filter out noise to direct the clean traffic further into the network

    b. Consider using tools to detect both volumetric attacks and insidious attacks such as Slowloris

3. Perform Upstream Blackholing

    a. Filter UDP traffic using router blackholing as there are no need to receive UDP traffic to their infrastructure. This prevents reflected NTP or DNS amplification attacks

LINKS

CloudFlare DDoS Protection

https://www.cloudflare.com/ddos/

Amazon Web Services Shield

https://aws.amazon.com/shield/

    b. Drop junk packets and block ICMP with the setup of a good firewall

4. Engage a Reliable Third Party Service Provider

    a. Consider the purchase of Anti-DDoS services from reliable third party providers to monitor and prevent DDoS attacks (Cloudflare, Amazon Web Services Shield, etc)

5. System Hardening

    a. Configure both your operating systems and applications to be more resilient to application layer DDoS attacks. Ensure that there are sufficient inodes on the Linux server to configure the right number of Apache worker threads.

    b. Cache your servers to provide as much static content as possible. This will prevent the database or custom scripts that are running from failing.

3. **Hacking** into unauthorized email accounts and/or IT systems to steal information

3.1 Definition of Hacking

Hacking is an attempt to exploit a computer system or a private network inside a computer. It is the unauthorized access to or control over computer network security systems to steal confidential information or plant malware.

3.2 Impact

It results in the breach of data and compromised systems which can be further utilised to launch attacks at other IT systems.

3.3 Recent Example

In 2016, Russian hackers allegedly broke into the Democratic National Committee (DNC) servers and leaked thousands of emails to the whistleblowing activist group WikiLeaks. The leaked information was released 48 hours before the kickoff of the Democratic National convention.

Read on for more information at:
http://mashable.com/2016/07/25/dnc-email-leak-wikileaks/

3.4 Recommendations

The following are recommendations to IT system administrators on the steps to take to secure the IT systems used in election.

1. Be wary of emails, instant messages and phone calls of unsolicited people such as service providers. Verify the source of message or identity of the caller with the respective company
2. Do not click on suspicious links and email attachments
3. Do not send personal information over the internet before checking a website's security
4. Do not provide personal information or information about the organisation, including the IT infrastructure or network
5. Install and maintain an up-to-date anti-virus software, firewalls and filters to reduce network traffic
6. Understand and utilise any anti-phishing features provided by your email client and web browser
7. Check and monitor if any private and confidential information are uploaded to the website
8. Enable 2-factor authentication for administrator logins to prevent unauthorised access
9. Patch your software and operating systems
10. Pay attention to the website URL as it may be changed to direct users to spoofed websites.

LINKS

Cyber Hygiene Tips
https://www.us-cert.gov/ncas/tips/ST04-014

Social Engineering Preventing Tips

http://lightcyber.com/8-tips-to-prevent-social-engineering-attacks/

https://www.hackread.com/simple-tips-manage-prevent-social-engineering-attacks/

Cyber Incident Reporting
Candidates who require advice to deal with cyber threats can approach SingCERT at singcert@csa.gov.sg.