Enhancing Your Cybersecurity Posture Amidst Developments in Israel-Hamas Conflict

Global concerns about cyber threats have arisen due to the recent Israel-Hamas conflict, with threat actors leveraging the situation to propagate disinformation and launch cyber-attacks, such as phishing, distributed denial-of-service (DDoS) and ransomware attacks. There have also been reports of more than 100 websites in Israel disrupted, including sites belonging to the government, media as well as relief groups providing aid. Pro-Palestinian hacktivists have threatened to carry out hacking operations including web defacements. Websites impersonating relief groups seeking donations have also been set up to trick the public.

Organisations and individuals are strongly recommended to remain vigilant and put in place cybersecurity measures to fortify their online defences.

The following are some recommendations covering systems, processes, and general cyber hygiene.

Recommendations for Systems

Secure Your Systems and Network Infrastructure

- Require strong, multi-factor authentication (MFA) for all remote, privileged, and administrative access and encourage the use of strong passphrases and password management tools.
- Keep all systems and software up-to-date with the latest security patches and implement a regular patch management process to address vulnerabilities promptly.
- Disable any ports and protocols that do not serve essential business purposes.
- Use firewalls and IDPS to monitor and filter network traffic and block suspicious or unauthorised access attempts.
- Enforce strict access controls with the basis of the principle of least privilege (PoLP), to limit user and system access to only what is necessary for their roles.

Install Anti-Virus Software

- Keep the software and its virus definition files updated.
- Perform systems and networks scans at least once a week and always scan any received files before opening them.

Recommendations for Processes

Monitor Network Connections and Review System Logs to Quickly Detect a Potential Intrusion

- Regularly review and analyse logs of network and system activities to identify anomalies or signs of compromise.
- Enable user access logging and use applications, such as Security Information and Event Management (SIEM), for aggregating and monitoring logs, to ensure continuous visibility beyond logging timeframes.
- Actively review both Active Directory sign-in logs and unified audit logs for any signs of unusual or suspicious activity.
- Monitor the network continuously to detect and respond to suspicious activities and threats promptly.

Prepare for Ransomware Attacks

Organisations need to remain vigilant for possible ransomware attacks. Succumbing to such attacks can be detrimental to an organisation's operations and its ability to maintain business continuity. To find out how you can protect your organisation's systems and data from ransomware, read our full advisory here.

Put in Place Incident Response and Business Continuity Plans

- Back up data regularly and ensure that backups are isolated from network connections.
- Establish and validate an incident response and management plan.
- Ensure that critical business functions remain operable if the network becomes unavailable.
- Establish clear and easily accessible reporting channels for cyber incidents which may include a dedicated email address or phone number of the IT or cybersecurity team responsible for incident response.
- Develop incident reporting templates to guide employees in providing the necessary information pertaining to cyber incidents. Such information may include the date, time, description of the incident and any relevant evidence. Organisations may also consider creating detailed guidelines on the process of reporting a cyber incident to ensure the accuracy of the information provided.

Recommendations for Cyber Hygiene

Be Vigilant about Phishing Attempts

- Exercise caution when dealing with suspicious emails/SMSes, especially those that create a sense of urgency, and ensure you verify their legitimacy before clicking on any links or downloading attachments.
- Be cautious when you receive emails from unknown senders who may be pretending to be someone you know or from a reputable organisation.
- Individuals are advised not to download software or media files from unknown sites; instead, they should rely on verified and trustworthy sites for downloads. Make sure that the browser address bar of the page you are visiting uses "https" instead of "http". A shield or lock symbol in the address bar can also indicate that the page is secure.

Regularly Monitor Your Financial Accounts

- Check for any signs of suspicious activities or unauthorised transactions.

Report a Compromise

Organisations and individuals in Singapore who are affected by a cyber-attack or have evidence of any compromise of your networks should report to SingCERT. A report can be made via our Incident Reporting Form at https://go.gov.sg/singcert-incident-reporting-form

References

https://www.channelnewsasia.com/world/hackers-disrupt-israel-gaza-conflict-hamas-palestinians-cybersecurity-ddos-3836641

https://www.bloomberg.com/news/newsletters/2023-10-18/war-tests-israeli-cyber-defenses-as-hack-attempts-soar