Security Playbook

Ransomware

Security Playbook

Overview. The objective of the playbook is to show how it meets with or supports a security control for the user to adapt as part of their Security Playbooks

This Playbook can also be applied to other security standards such as NIST, ISO, CIS and ISA, or adapted to meet with local regulatory and/or client security obligations.

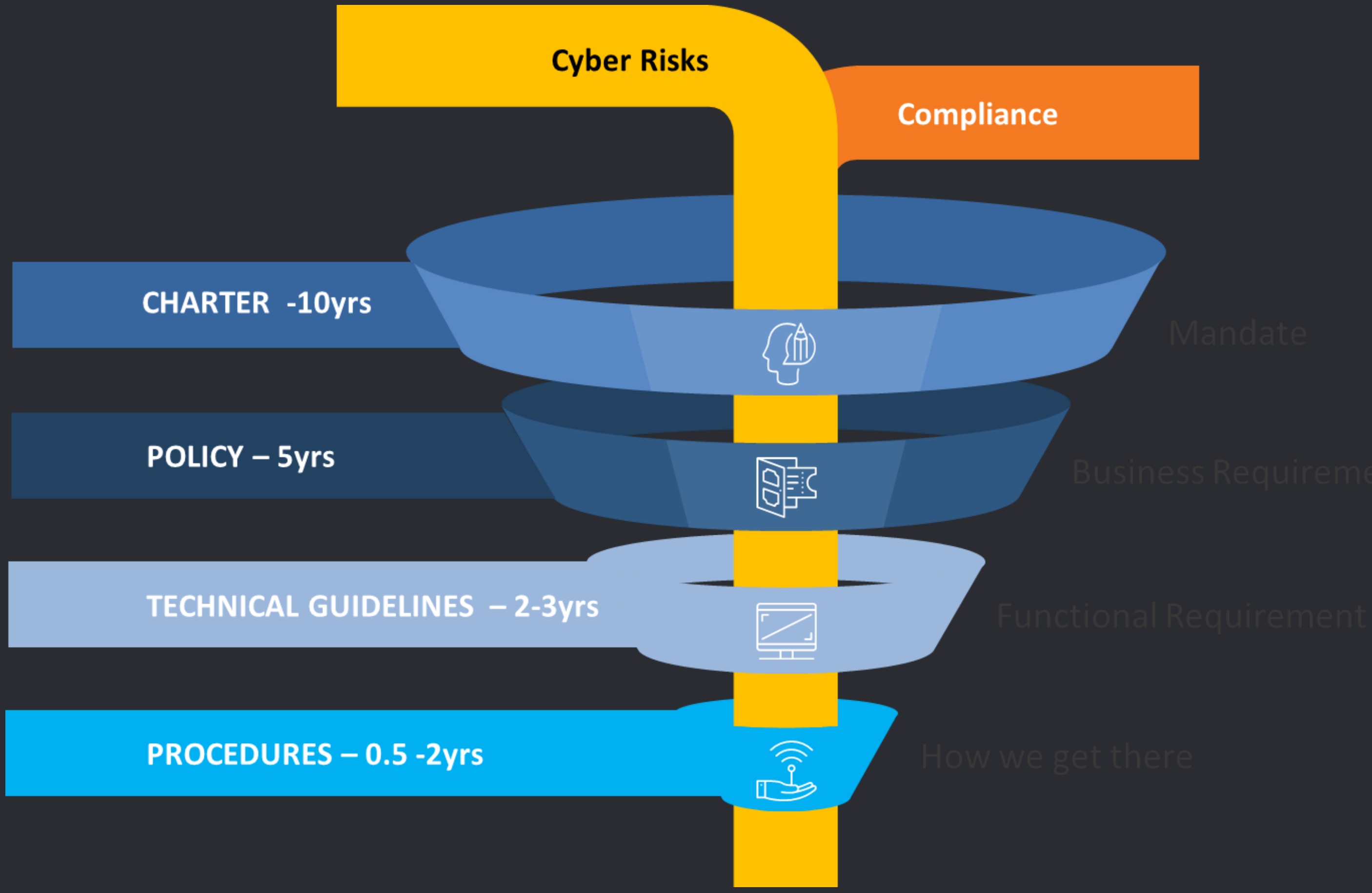
Inside a Playbook

- **Playbook Scope**
- **Scenario Process and Procedure**
- **Tasks, Roles and Responsibilities**

Other Playbooks

- **Ransomware**
- **Denial of Service**
- **Data Leakage**

Security Playbook



As the diagram suggests the average lifetime expectancy of a Playbook or Procedures is 1-2 years. However new technologies are being developed to address new risks and therefore a process to create new Playbooks are important.

Playbooks are developed with a one (1) year lifetime in mind and are therefore tactical in design. Your technology operational procedures are more regularly changed and are therefore designed in such a way to address the rapidly changing technology and the risk landscape or security ecosystem.

Playbook: Format

The playbook is a step-by-step instruction guide for handling a particular incident response cyber-attack. Each playbook is a living document that must be regularly updated and peer-reviewed before being tested by your incident response team. It is important to collect feedback from your team and amend the process accordingly before the playbook becomes irrelevant and must be consider for retirement.

Part1: Incident Response Identify & Clarify

A checklist of items to confirm the incident playbook is relevant. Time length will be stated to ensure incident can be identified early to move to contain phase.

Part2: Contain

Step by step guide on how to contain the incident. Time length will be stated to ensure incident can be contain as early as possible where respond phase could be action upon.

Part 3: Respond

What next steps to take once the incident is contained and no longer as active.

Part4: Recover

How to get the business back to normal

Playbook: Ransomware

This runbook provides instructions for handling end-user reported phishing campaigns against The Companyemployees. The goal is to prevent the introduction of backdoors into the company infrastructure, which may lead to data theft.
The process aims to lower the success rate of the phishing campaign by blocking emails and back door attempts.

Part A: Identify & Clarify (Within 20 Minutes)

HELP DESK STEPS (VERIFY SENDER) (WITHIN 5 MINUTES)

- Where possible, the helpdesk will assist the user to contact the sender via phone to validate the intent of the email or to confirm this is a false positive.
- Where the incident is not a false positive, helpdesk will update the ticket and utilize the check list to input the details (e.g. SCALE, BUSINNES IMPACT) and escalate to email administrator for further respond actions.
- Helpdesk will confirm with user whether any actions were already taken within the email content (e.g. entered user credentials, downloaded attachment) and update the ticket and escalate to virus administrator for further respond actions.
- If the user report behavior that has ransomware symptoms,
    - PC is very slow after clicking on email links
    - these files appear at user PC %UserProfile%\enc_files.txt, %UserProfile%\last_change.txt
    - File/s with extensions listed in appendix for ransomware appear in user PC %UserProfile%\ directory or subdirectories

Playbook: Ransomware

- Identify which shared file directories are mapped to affected user for ransomware and proceed to escalate to infrastructure owner to shutdown server if ransomware is encrypting files within.
- Helpdesk will activate support to remove the machine (PC/ Server) from the LAN and/ or wireless connection from the corporate network and switch off/power down the machine, as if that PC is infected with ransomware!
- Helpdesk will escalate all updated details to IR Team leader.

EMAIL ADMINISTRATOR STEPS (CONFIRM PHISHING & VOLUME) (WITHIN 5 MINUTES)

- Check The Company exchange gateway inbound queues, spam filters and user inbox for the Phishing email. The Exchange search filters should be applied to automate the identification of the email by subject header and /or email address.
- Record the current system locations of the phishing email e.g. user mailbox, gateway queues via SMTP logs, spam filters or other files.
- Prepare to block and / or remove phishing emails (to go Contain)
- Email Administrator to obtain the original phishing email/s from the exchange or end-user and attach it to the Incident ticket. (Send to relevant parties e.g. security teams)
- Continuously monitor the email exchange for new inbound phishing emails. Note: Typically, emails are ‘dripped’ into the system in batches of 200-300 in an attempt to try and circumvent spam filter alerts. (Not within the 5 minutes scope)

Playbook: Ransomware

EMAIL ADMINISTRATOR STEPS (IOC) (WITHIN 5 MINUTES)

- Collect and record the incident below into the help desk ticket:
- Full download URL(s) from the email
- Hostname from URL
- Visit http://www.kloth.net/services/nslookup.php and get the IPs belonging to the hostname
- Do reverse lookup and record the PTR record
- Subject link of the email
- Sender of the email
- Hostname and IP address of the sender's SMTP server

EMAIL ADMINISTRATOR STEPS (CONFIRM CAMPAIGN) (WITHIN 5 MINUTES)

- Search for emails with similar senders, subjects, contents or URLs
- If this is the first phish in a new campaign, skip to the next paragraph
- If the phish is part of a campaign
- Create a master ticket (if necessary) in IR ticket system
- Relate new ticket to master ticket

VIRUS ADMINISTRATOR STEPS: (VALIDATE KNOWN MALICIOUS EMAIL) (WITHIN 5 MINUTES, PARALLEL FROM EMAIL ADMINISTRATOR)

- Validate the email links payload is effective and malicious: Go to www.vitrustotal.com and copy the email URL link in the phishing email to the virus total page and scan.

Playbook: Ransomware

Part B: Contain (Within 20 minutes)

HELP DESK STEPS: (ALERT EMPLOYEES) (WITHIN 15 MINUTES)

- If there are multiple tickets from Help Desk first step is to warn the end-users of the emerging threat.
- Retrieve the comms template from *<server://Internal-Comms-Phishing>* and take the pre-approved phishing email template
- Send the template to Security Team for the approval of the content.
- Security Team need to approve or amend the content within 10 minutes
- Helpdesk will send out the content immediately on *<communications@domain.com> as a company-wide alert upon the receipt of the approval of content from Security Team*

EMAIL ADMINISTRATOR STEPS (BLOCK EMAILS ON SMTP SERVER) (WITHIN 5 MINUTES)

- As the phisher can easily change the subject line or sender of the emails, try to find a common pattern in the email headers of the related emails. For instance, all emails might share the *X-Mailer:* and *X-PHP-Script:* headers.
- View the source of the original phishing emails under the master ticket
- If you manage to find a common attribute block all incoming emails based on the identified pattern. Set the exchange filters (spam, gateway queues, SMTP queues to block or divert the pattern.

EMAIL ADMINISTRATOR STEPS (DIVERT “BAD” EMAILS) (WITHIN 5 MINUTES)

- Divert all phishing emails to an email admin inbox *<itphish@domain.com>* to monitor for genuine emails. Some emails may get caught by the filter process and will require email admin to regularly monitor the mailbox to release genuine emails.

Playbook: Ransomware

EMAIL ADMINISTRATOR STEPS (REMOVE FROM MAILBOX) (WITHIN 5 MINUTES)

- Check the SMTP logs whether the same email has been delivered to other users. Start to remove emails from the affected employee mailboxes.
- Search for the subject line from the original phish
- Search for the sender email address from the original phish
- If you identify other recipients in the SMTP logs
- Export affected recipients into a CSV file
- Remove the phishes from the affected mailboxes

FIREWALL ADMINISTRATOR STEPS (BLOCK IP) (WITHIN 5 MINUTES)

- Can be perform parallel with email administrator, where possible
- This process will block the sender IP for any further communications between The Company and the malicious IP
- Go to the egress firewall console and enter the following IP from the incident report to be blocked.
- Malicious phishing URL IP, Malicious attachment download URL IP, Malicious sender IP

WEB OR FIREWALL ADMIN STEPS (BLOCK URL) (WITHIN 5 MINUTES)

- Can be perform parallel with email administrator, where possible
- This process will block the dropper to be downloaded if a user clicks on the malicious URL in the phish.
- Try to identify a pattern in the URL. For example, if the URL is: http://hackedwebsite.com/dl.php?campaign=ra&id=12731342834923919
- Create a regex from the pattern
- Send the regex pattern and original URL link to the web proxy team to block all outbound web traffic.

Playbook: Ransomware

Part C: Respond (Within One hour unless specified)

VIRUS ADMINISTRATOR STEPS (REPORT MALWARE & DEPLOY SIGNATURES)

- How to send the malware and URL link to the AV provider for updated malware signature. The time frame for DAT file creation will vary accordingly with AV vendors :
    - Open a Linux VM machine, curl the URL to retrieve the file or simply save email attachment to local drive
    - Record the md5 or sha256 hash values
    - Pack the file with “zip” on the VM and encrypt it with the password: “virus”
    - Copy the zipped file to your desktop
    - Attach file and hashes to the IR ticket system
    - Send the malware sample from the IR ticket system to *<AVresearch@provider.com>*
    - If AV provider replies with the additional signature file, push it out to the endpoints as the following:
    - Take the *dat* file received from AV provider and attach it to the ticket
    - Push the *dat* file immediately from AV console to All Pcs and Servers.
    - For Desktop machines that were affected and switch off, helpdesk will assist the virus administrator to manually copy the dat file into the machine upon power on immediately and initiate an immediate scan and clean action.

Playbook: Ransomware

VIRUS ADMINISTRATOR STEPS (RANSOMWARE REMOVAL)

How to scan the infected PC where suspected ransomware may be present:

- If the machine is suspected that it may have been affected by Ransomware,
- Proceed to download SpyHunter as stated in the APPENDIX section.
- Install and run the tool in the suspected PC to attempt to remove the malware.
- If not proceed to back to capture the suspected malware file for AV DAT file creation from the AV provider.
- How to possibly remove the ScreenLock and malware from infected PC:
- If the machine has been ScreenLock by a Ransomware,
- Proceed to download TrendMicro Ransomware Removal tool as stated in the APPENDIX section.
- Depending on whether safe mode is accessible, download the corresponding tool accordingly.
- install and run the tool in the suspected PC to attempt to remove the malware and unlock the screen.
- If not proceed to back to capture the suspected malware file in safe mode for AV DAT file creation from the AV provider.
- How to possibly decrypt files that are encrypted by certain RansomWare family:
- If the files are encrypted by Ransomware,
- Proceed to download the decryptor tool from Kaspersky to unlock files.
- Submit details from encrypt ransom note or download the according decrypt tool for the ransomware file.
- Install and run the tool to decrypt the file.
- If not proceed to back to capture the suspected malware file in safe mode for AV DAT file creation from the AV provider.
- Restore files from backup solution if otherwise the tools are unable to decrypt files.

Playbook: Ransomware

SYSTEM ADMIN STEPS (ACCOUNT CREDENTIALS RESET)

- System admin to initiate an account password reset for the end-user when the phishing campaign involves credentials stealing via a fake URL page.

FIREWALL, SPAM ADMIN STEPS (UPDATE ALL PROVIDERS FOR SIGNATURE)

- This process allows The Company to respond to the phishing incident with additional controls via firewall, IPS and/or SPAM gateway
- Provide the following information to the firewall, IPS and/or SPAM gateway vendor or managed service provider for an updated signature to be deployed
    - The time frame for DAT file creation will vary accordingly with AV vendors
    - Malicious phishing URL IP
    - Malicious attachment download URL IP
    - Malicious sender IP
    - The md5 and sha256 hashes from the collected malware samples

RANSOM OR MONEY TRANSFER RESPONSE.

- Depending on the success of the phishing campaign and the payload will depend on the response you direct.
- Money transferred to a fraudster: Please contact the Legal team whom will work directly with the banks.
- Ransomware: We do not pay! Please refer to your IT backup recovery process. If there is NO backup recovery, then management need to work on a user recovery plan e.g. recovery of emails and personal backups.

Playbook: Ransomware

Part D: Recovery

EMAIL ADMINISTRATOR STEPS (RESUME EMAIL SERVICE)

- Resume email service and notify all users via desktop support or other notification systems.
- **VIRUS ADMINISTRATOR STEPS (PROVIDER FOR MALWARE RECOVERY)**
- Depending on the success of the phishing campaign and the submitted payload, AV providers are able to provide recovery/decrypting tools on the recovery of data required. Failing that, resort to backup restore and don’t pay the ransom.

DESKTOP ADMIN (DATA BACKUP RECOVERY)

- Refer to The Company Backup recovery procedures

End Of Playbook