**Security and Risk Assessment of IT Defense Strategies Considering the Cyber Kill Chain**

Defensive IT architecture helps to deploy defense-in-depth concepts in an organization's IT architecture, which helps to prevent, identify, detect, contain, respond to and recover from cyberincidents in a timely manner. Defensive architecture in information systems includes responses to cyberincidents, systems protection and assurance of information for organizations. Since cybercriminals are constantly introducing complex attacks, defensive infrastructure is essential for critical information systems to protect organizations from cyberattacks and ensure the safeguarding of assets.

IT security, risk assessment and audit function professionals can review the IT infrastructures of the organizations by following attack chains and identifying the gaps in the implementations of defense strategies to protect the infrastructure from cyberattacks.

Lockheed Martin introduced the Cyber Kill Chain concept to help organizations analyze and review attack chains and identify gaps in defensive strategies. From there, other defensive strategies can be implemented to protect the infrastructure from cyberattack. An IS audit, information security, risk, governance or compliance professional can review the IT infrastructure in their workplace for effective and efficient management and assessment of cyberattacks to achieve the business objectives.

Defense is the idea by which information security professionals analyze the attack chain, step-by-step, and then design and implement the controls in each step so they can kill the attack chain. By doing so, organizations can contain attacks and prevent the movement of intruders toward the rest of the infrastructure. Analyzing infrastructure and security postures of the reviewed organization is a tremendous responsibility for information assurance professionals; using Cyber Kill Chain steps to identify the defensive measures of the organization provides a detailed view to an assessor. By analyzing and assessing the attack chain, it can be divided into steps, and an assessor or information security architect can use these steps to identify the gaps and strengths of the reviewed infrastructure:

1. Determine target locations.
2. Monitor the target locations.
3. Track the targets.
4. Develop, collect and select the required weapons (e.g., malware, virus, apt or logic bomb) for a specific target.

**Muhammad Mushfiqur Rahman**, CISA, COBIT 5 Foundation, CCISO CCNA, CEH, CHFI, CISSP, CLTP, CND, CSA, CTIA, ECI, ECSA, ISO 27001 LA, ITIL v3, LPT (Master), MCITP, MCP, MCSA, MCSE, MCT, MCTS, OCP, OSCP, PCT, PRINCE2, SCISA

Has 17 years of experience in information security, risk analysis, IT governance, compliance, vulnerability assessment and penetration testing (VAPT), IT operations, project management and custom business solutions, and enterprise resource planning implementation. He can be reached at mushfiqur98@gmail.com.
5. Deliver and apply the weapons to the target.
6. Review and analyze the effects on the target.

Steps of a Cyber Kill Chain

It is important for information assurance professionals to understand the cyberattack chain, attack methodologies followed by intruders and defensive approach needed to take the necessary steps to secure the IT infrastructure of the organization. Information security and risk professionals and auditors can review the infrastructure by using the following steps to help them uncover the gaps and be able to recommend possible solutions for an organization to implement.

Reconnaissance, Information Gathering and Footprinting

In this step, attackers analyze social media, search engines, job sites and stock exchanges to identify and detect the specific target and collect as much information as possible about the target. Reconnaissance or footprinting can be active and passive. In active reconnaissance, attackers try to connect and interact with the target to get the information and vulnerabilities of the targeted systems. In passive reconnaissance, attackers can perform scanning to gain information by using a number of strategies, including (but not limited to):

- **Nmap**—A popular tool to scan networks and identify live hosts, ports, operating systems and opened services
- **Port scanning**—A technique to identify open ports of hosts in an audited network
- **Banner grabbing**—A technique used to gain information about a computer system on a network and the services running on its open ports
- **Vulnerability scanning**—A methodology by which an assessor is able to uncover existent vulnerabilities of systems using different tools
- **Physical visit**—Assessors plan to visit physical sites to assess physical threats
- **Internet-facing servers**—Scanning an organization's Internet-facing services

In passive reconnaissance, attackers try to collect information about targeted systems and organizations without actively connecting with the systems. Passive methods include investigating the following:

- Whois
- Google
- Social media
- Shodan
- Job listings
- Job sites
- Enterprise websites
- Stock exchanges
- Press releases, contract awards, conference attendee lists
- Harvested email addresses

Weaponization

This is the preparation step for attackers in which they design, develop and collect a weapon based on the identified vulnerabilities of the target. Sometimes the weapon is target-specific, and sometimes it is generic to carry out an attack on a large number of targets. Attackers try to minimize detection of their weapon by the target’s security solutions.

In the weaponization step, attackers can either develop attack tools themselves or collect them from different sources. Possible tools for an attack include:

- Malware
- Virus
- Worm
- Trojan
- Remote code execution
- Cain & Abel
- Sqlmap
- Aircrack-ng
- Maltego web app
- Metasploit
- Exploit
- Exploit DB
- Social-Engineer Toolkit (SET)
- SAINT
Delivery
In this step, attackers take initiative to reach the target, deliver their weapon to the victim systems and implement the attack. Attackers use different methods and media to deliver the weapon to the targeted infrastructure and systems, including CD-ROM, Universal Serial Bus (USB), email, Internet browsers and social media. These media may become platforms for the attackers to increase phishing and, through these, attackers can deliver a specific payload/weapon to the targeted systems.

Exploitation
In this step, delivered malicious codes initiate the execution on the victim systems. The delivered payload exploits the targeted system's vulnerabilities and executes its malicious binary payload to provide the attacker with the minimum required access to the target environment. Attackers look for additional vulnerabilities and try to exploit them inside the organization's targeted systems. During the exploitation phase, the attacker may not have access from the outside, but the attacker can perform a deep dive into the system to identify more vulnerabilities to be exposed.

In the exploitation step, the following attacks may occur:
- Structured Query Language (SQL) injection
- Buffer overflow
- Javascript
- Shellscript
- Malware
- Fileless malware

Installation
In this step, attackers create a backdoor to continue remote access to the targeted infrastructures and propagate the malicious codes to more systems. In this phase of the attack chain, the intruders install a persistent backdoor or implant malicious code in the victim environment to maintain access for an extended period. Backdoor tools include:
- Installing webshell on web server
- Installing backdoor/implant on client victim
- Dynamic Link Library (DLL) hijacking
- Meterpreter
- Remote access tools
- Registry changes
- Privilege escalation
- Access token manipulation
- Path interception
- Sudo attack
- Process injection

Command and Control
In this step, malicious code or intrusions move to other systems to identify the most vulnerable or valuable systems and information to gain access to privileged accounts, business-critical data and critical assets. In this phase, attackers try to establish a command channel to enable the intrusions to manipulate victims remotely. Intrusions move laterally and are a coordinated effort that may spread in multiple systems. Command and control (C&C) is the last chance for the information assurance professional to defend or block lateral movement. Information security professionals can reduce impact when intruders fail to issue commands because intruders need to establish an outbound communication channel using systems compromised of C&C. The C&C phase is normally manual (not automated), so the intruders need to establish connection with the compromised systems. Defenders must design and implement the monitoring systems to ensure that the defensive approach is working properly and security solutions are able to identify, detect, track, monitor, observe, contain, stop and destroy the adversaries. In the C&C step, the following attacks may occur:
- Most common C2 channels are over web, Domain Name System (DNS) and email protocols
- Secure Shell (SSH) hijacking
- Internal spear phishing
- Windows remote management

Obfuscation
In this step, criminals actively cover their tracks on the compromised systems and infrastructure by deleting or modifying logs or manipulating timestamps. Hiding the actions taken in earlier steps of the attack chain makes it difficult for security professionals to detect the compromised system, data or signs of intrusion. Obfuscation
efforts include:
- File deletion
- Hidden users
- Binary padding
- Code signing
- Process hollowing

**Actions on Objective**
In this step, attackers attempt to dive deeper into the compromised systems and infrastructure to collect, encrypt, extract and exfiltrate the data. This is a critical phase for information security/assurance professionals—they must have the mechanisms to identify the intrusions as early as possible, or long-term intruder access may destroy more information and have a higher impact.

Actions-on-objective phase activities include:
- Collecting user credentials
- Privilege escalation
- Internal reconnaissance
- Lateral movement through environment
- Collecting and exfiltrate data
- Destroying systems
- Overwriting or corrupt data
- Surreptitiously modifying data
- Financial loss
- Political espionage
- Corporate espionage
- Malicious insider activity

To protect systems and information from intruders, organizations should design their architecture to prevent, detect, correct, deceive and contain attackers in a timely manner. IS professionals need to have a good understanding of different controls and attack-chain steps, and which control is needed at each step. It is important to implement reviews to show that controls are implemented properly and to monitor the controls on a regular basis to identify any intrusions as early as possible. There are several different control categories including (figure 1):

- **Physical controls**—Countermeasures that take physical measurement, (e.g., lock, fence, guards) to prevent, detect, correct and deter intruders from performing any unauthorized activities
- **Technical controls or logical controls**—Countermeasures that take technical or logical measurement (e.g., firewall, IPS, antimalware) to prevent, detect, correct and deter intruders from performing any unauthorized activities
- **Administrative controls**—Countermeasures that take administrative measurement (e.g., policies, awareness training, business practices) to prevent, detect, correct and deter intruders from performing any unauthorized activities

There are several different control types, including (figure 2):
- **Preventive controls**—Help to prevent attacks from occurring.

<table>
<thead>
<tr>
<th>Control Categories</th>
<th>Preventive</th>
<th>Detective</th>
<th>Corrective</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical</td>
<td>Door locks, fences, gates</td>
<td>Inventory count, bank reconciliation</td>
<td>Reissue access cards, repair physical damage</td>
</tr>
<tr>
<td></td>
<td></td>
<td>closed-circuit television (CCTV) and surveillance camera logs</td>
<td></td>
</tr>
<tr>
<td>Technical</td>
<td>Firewall, intrusion protection systems (IPS), multifactor authentications (MFA), anti-malware software</td>
<td>Intrusion detection systems (IDS), security information and event management (SIEM), honeypots</td>
<td>Patch implementation, reboot a system, contain or quarantine malware</td>
</tr>
<tr>
<td>Administrative</td>
<td>Policies, user awareness, data classification</td>
<td>Review access rights, audit logs, unauthorized changes</td>
<td>Implement a business continuity plan or incident response plan</td>
</tr>
</tbody>
</table>
• **Detective controls**—Help to detect any unwanted actions already taking place or in progress.

• **Corrective controls**—Help to repair and restore the system from damage to the production environment.

• **Deterrent controls**—Warn any attacker not to perform illegal actions on the system and describes legal consequences.

• **Disrupt controls**—Help by stopping or changing the flow of the attack after detection.

• **Degrade controls**—Help the information assurance professional attempt to minimize the impact of an attack.

• **Deceive controls**—Help the information security professional misguide the attacker by providing false information to disrupt the attack.

• **Destroy controls**—Countermeasure neutralizes or eradicates the attack weapon to recover systems and services to a normal state.

The steps for a defensive approach include:

1. Any one mitigation step can break the attack chain.
2. An information assurance professional has an opportunity at every step to break the attack chain.
3. IT audit, security and risk professionals should review infrastructures by following the steps of the attack chain to identify the gaps in the defense approach. This ensures that they meet business objectives and secures the organization’s infrastructure and systems.

<table>
<thead>
<tr>
<th>Phase</th>
<th>Preventive</th>
<th>Detective</th>
<th>Corrective</th>
<th>Deterrent</th>
<th>Disrupt</th>
<th>Degrade</th>
<th>Deceive</th>
<th>Destroy</th>
<th>Contain/Quarantine</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Reconnaissance</strong></td>
<td>• Policies</td>
<td>• Web analytics</td>
<td>• Delete posted confidential data</td>
<td>• Use banner with legal notification</td>
<td>• Block access from unauthorized virtual private networks (VPNs)</td>
<td>• Social media honeypot</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td><strong>Weaponization</strong></td>
<td>• End user awareness/training and education</td>
<td>• Build detection for browsing behaviors</td>
<td>• Reconfigure and review of systems (e.g., OS, database, domain name system [DNS], web, application server)</td>
<td>• Use banner with legal notification</td>
<td>• Use banner with legal notification</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td><strong>Delivery</strong></td>
<td>• End user awareness training and education</td>
<td>• Delivery medium analysis</td>
<td>• Reconfigure and review of systems (e.g., OS, database, DNS, web, application server)</td>
<td>• Inline antimalware email encryption/authentication</td>
<td>• Queueing</td>
<td>• Ingress, parcel and mail redirection for high-risk items</td>
<td>• Router and firewall access control list (ACL)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Phase</td>
<td>Preventive</td>
<td>Detective</td>
<td>Corrective</td>
<td>Deterrent</td>
<td>Disrupt</td>
<td>Degrade</td>
<td>Deceive</td>
<td>Destroy</td>
<td>Contain/Quarantine</td>
</tr>
<tr>
<td>----------------</td>
<td>------------</td>
<td>-----------</td>
<td>------------</td>
<td>-----------</td>
<td>---------</td>
<td>---------</td>
<td>---------</td>
<td>---------</td>
<td>-------------------</td>
</tr>
<tr>
<td><strong>Exploitation</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>End user awareness/training and education</td>
<td>Policy for systems configuration, patch management, configuration standard, change management, email plugins</td>
<td>AV/AM/EDR/XDR/MDR</td>
<td>Firewall, IPS</td>
<td>Delivery medium analysis</td>
<td>Detect new malicious payloads at the point of delivery</td>
<td>Honeyhops</td>
<td>IDS</td>
<td>SIEM</td>
</tr>
<tr>
<td><strong>Installation</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>End user awareness/training and education</td>
<td>Policy for systems configuration, patch management, configuration standard, change management, email usage policy, Internet browsing policy</td>
<td>Policy for antimalware/anti-virus</td>
<td>Restrict the use of USB</td>
<td>Disable unused ports/services</td>
<td>Patch management</td>
<td>Disable: Office macros, Java scripts and browser plugins</td>
<td>AV/AM/EDR/XDR/MDR</td>
<td>Firewall</td>
</tr>
<tr>
<td><strong>Command and Control</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Policy for systems configuration, patch management, configuration standard, change management, email usage policy, Internet browsing policy</td>
<td>Restrict the use of USB</td>
<td>Disable unused ports/services</td>
<td>Patch management</td>
<td>Disable: Office macros, Java scripts and browser plugins</td>
<td>AV/AM/EDR/XDR/MDR</td>
<td>Firewall</td>
<td>IPS</td>
<td>Delivery medium analysis</td>
</tr>
</tbody>
</table>
Figure 2—Specific Controls for Attack Chain Phases (cont.)

<table>
<thead>
<tr>
<th>Phase</th>
<th>Preventive</th>
<th>Detective</th>
<th>Corrective</th>
<th>Deterrent</th>
<th>Disrupt</th>
<th>Degrade</th>
<th>Deceive</th>
<th>Destroy</th>
<th>Contain/Quarantine</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Patch management</td>
<td>Delivery medium analysis</td>
<td>Reconfigure and review of systems (e.g., OS, database, DNS, web, application server)</td>
<td>Use banner with legal notification</td>
<td>N/A</td>
<td>Quality of service</td>
<td>Honeypot</td>
<td>N/A</td>
<td>Incident response</td>
</tr>
<tr>
<td></td>
<td>Application control</td>
<td>Detect new malicious payloads at the point of delivery</td>
<td>Prioritize defenses around particular technologies or people based on recon activity</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Firewall ACL</td>
</tr>
<tr>
<td></td>
<td>File integrity module (FIM)</td>
<td>Honeybots</td>
<td>AV/AM/EDR/XDR/MDR</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>DLP</td>
<td>IDS</td>
<td>Restore or reimage</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>AV/AM/EDR/XDR/MDR</td>
<td>SIEM</td>
<td>Forensic agents pre-deployed to endpoints for rapid triage</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Firewall</td>
<td>Perform malware analysis in details</td>
<td>Network package capture to recreate activity</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>IPS</td>
<td>Need to build a mechanism to detect the weaponizers</td>
<td>Conduct damage assessment with subject matter experts</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Sandbox</td>
<td>Enable and preserve audit logging</td>
<td>Establish incident response playbook, including executive engagement and communications plan</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>DEP</td>
<td>Collect files and metadata for future analysis</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>MFA</td>
<td>Determine which weaponizer artifacts are common to which APT campaigns</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Email security</td>
<td>Revert engineering for malware</td>
<td>Reverse engineering for malware</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Advanced Threat Protection (ATP)</td>
<td>Collect email and web logs for forensic reconstruction</td>
<td>Collect email and web logs for forensic reconstruction</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>DLP</td>
<td>Obfuscation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Prohibit read, write, execute permission of logs</td>
<td>SIEM</td>
<td>Forensic tools</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Review syslog server</td>
<td>Use banner with legal notification</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Prioritize defenses around particular technologies or people based on recon activity</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Block access from unauthorized VPNs</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Tor exit nodes, high-risk locations</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Operations security user education (especially around social media)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>N/A</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Conclusion

Each step of the Cyber Kill Chain necessitates a precise process and technological solutions to detect cyberattacks. Information security professionals, risk practitioners and IT auditors can follow the steps, review the measures already taken by the organization and identify the gaps, and recommend the proposed actions the organization needs to take to remediate the vulnerabilities or risk. Information systems assurance professionals can use the Cyber Kill Chain during the information security and risk assessment, and information security auditors can follow each step during their review and audit to uncover any gaps in their organization’s defense strategies and identify the adequacy of the control strength or weakness by mapping controls to the steps an attacker must go through to successfully execute a cyberattack.