A1 Cyber Range Angriffsszenarien

Einsteiger Szenarien

DDOS SYN Flood
In diesem Szenario verwendet der Angreifer eine große Anzahl von Bots im Internet, um massiven Traffic auf einer der Websites des Unternehmens zu erzeugen. Der Datenverkehr überflutet die Bandbreite und die Ressourcen des Ziels, lähmt den Server und verursacht einen Denial-of-Service (DoS) für den Webserver.

SCADA VPN
In diesem Szenario stammt der Angriff von einem vertrauenswürdigen Supportunternehmen des SCADA-Systems. Das Cyber Training System (CTS) greift den VPN-Server über das externe Netzwerk an, indem es die Heartbleed Sicherheitslücke nutzt. Nach dem Verbergen der Anmeldeinformationen für das VPN, verbindet sich das CTS mit dem VPN und greift die SPS weiterhin direkt an, wodurch die Anlage abgeschaltet wird.

Web Defacement
In diesem Szenario scannt das Cyber Training System das Netzwerk nach bekannten Serviceports. Sobald es einen SSH-Server gefunden hat, verwendet das System einen Brute-Force-Angriff, um vollen Zugriff auf den Server zu erhalten. Sobald das erreicht wurde, scannt das CTS den Server nach gehosteten Websites und ersetzt jede Website durch eine Seite mit destruktivem Inhalt.

Wordpress Bad Plugin
In diesem Szenario wird ein Unternehmensblog, der sich im DMZ-Netzwerk befindet, gehackt und als Drehpunkt verwendet, um sensible Daten aus einer Datenbank zu exfiltrieren, die sich im internen Netzwerk befindet. Der WordPress-Blog hat ein verwundbares Plugin installiert, das von einem Angreifer verwendet wird, um eine PHP-Shell auf den WordPress-Server hochzuladen. Mit Hilfe der Shell durchsucht der Angreifer das Netzwerk und findet eine zugängliche Datenbank im internen Netzwerksegment. Anschließend erlangt der Angreifer mit Hilfe eines Brute-Force-Angriffs Zugriff auf die Datenbank und exfiltriert sensible Daten (Zahlungsinformationen).

Mittelschwere Szenarien

Apache Shutdown
In diesem Szenario greift das Cyber Training System einen bekannten öffentlichen Apache-Webserver mit einem SSH-Brute-Force-Angriff an, um Zugriff auf den Server zu erhalten, lädt dann Backdoor-Dateien und Skripte hoch, die dem Angreifer jede Minute die Benutzernamen und das Passwort des Servers senden. Um den Zugriff auf den Server aufrechtzuerhalten, fügt es schließlich einen Cron-Job hinzu, der den Apache-Dienst jede Minute herunterfährt.

DB Dump via FTP Exploit
In diesem Szenario nutzt das Cyber Training System eine bekannte Schwachstelle des FTP-Servers, um Root-Rechte auf dem FTP-Server zu erhalten. Der Angriff verwendet dann diese Berechtigungen, um mit Hilfe eines Brute-Force-Angriffs Zugriff auf die Datenbankserver zu erlangen und auf die sicheren Daten zuzugreifen.

DDOS DNS Amplification

In diesem Szenario verwendet der Angreifer den DNS-Server der Organisation, um einen viel breiteren DNS-Verstärkungsangriff durchzuführen, der ein reflection-based Distributed Denial of Service (DDoS) auf einem Ziel ist. Der Angreifer sendet DNS-Suchanfragen mit gefälschter IP-Adresse der DNS-Server mit Schwachstellen, die offene rekursive Relays wie unseren DMZ-DNS-Server unterstützen. Die großen DNS-Antworten werden "zurück" an das Ziel geschickt, als ob es sie angefordert hätte, wodurch die Bandbreite und die Ressourcen des Ziels überschwemmt, der Server lahmgelegt und ein Denial-of-Service (DoS) ausgelöst wird.

Java NMS Shutdown

In diesem Szenario lädt das Cyber Training System eine Website, die einen Java Applet Trojaner enthält, und verbindet sich nach dem Ausführen mit dem Zennoss NMS-Server und fährt ihn herunter. Von diesem Moment an wird die gesamte Überwachung gestoppt und der Angreifer kann alle Dienste ohne visuelle Überwachung beenden.

Killer Trojan

In diesem Szenario verbindet das Cyber-Trainer-System eine trojanerinfizierte CD mit einem Windows-Rechner. Beim Einlegen wird der Autostart ausgeführt und die Malware geladen. Der Wurm durchsucht das Netzwerk und sucht nach den geheimen Dateien. Es sammelt auch Passwörter und Active Directory-Dumps. Die vertraulichen Daten werden an den Angreifer-C&C-Server gesendet. Um die Verbreitung fortzusetzen, erstellt der Trojaner ein infiziertes PDF und verbreitet sich über E-Mails im Netzwerk.

SCADA HMI

In diesem Szenario wird das Cyber Training System einen Angriff auf die Anlage nachahmen. Der Einstieg in das SCADA-Netzwerk erfolgt durch die Nutzung veralteter HMI-Software, die auf dem HMI-Computer im SCADA-Netzwerk installiert ist. Der Angriff lähmt die Anlage komplett und schaltet die Anlagenmaschinen ein- und aus. Der Angriff wird von einem bösartigen Laptop aus durchgeführt, der mit dem internen Netzwerk verbunden ist. Der Angreifer führt den Angriff aus dem Benutzersegment aus.

SQL Injection

In diesem Szenario greift das Cyber Training System einen bekannten öffentlichen Webserver mittels SQL-Injection an. Während des Angriffs aktiviert das Cyber Training System die interne SQL Systemprozedur namens xp_cmdshell, die später verwendet wird, um alle Computernamen und E-Mail-Adressen der Mitarbeiter mit Hilfe von PowerShell-Skripten aus dem Active Directory zu extrahieren und die internen Serverdienste mit Hilfe der Remote Service Control zu stoppen. Der Angriff wird wiederholt durchgeführt, bis er vom Trainer gestoppt wird.

Trojan Data Leakage

In diesem Szenario sendet das Cyber Training System eine infizierte E-Mail mit einem Link zu einem ausführbaren Trojaner. Nach dem Öffnen der ausführbaren Datei wird ein Trojaner installiert, der eine lokale Suche nach den geheimen Dateien durchführt und diese per E-Mail an den Angreifer sendet.

WPAD Man in the Middle

In diesem Szenario führt das System einen Man-in-the-Middle (MiTM)-Angriff auf das Netzwerk durch. Der Angreifer lässt Hosts glauben, dass er ein legitimer Proxy im Segment ist, indem er Web Proxy Auto-Discovery (WPAD) Domain Name System (DNS) Abfragen nutzt. Sobald der gesamte Datenverkehr aus dem Benutzersegment durch den Angreifer geleitet wird, werden sensible Daten extrahiert und mit zwei verschiedenen Methoden - ICMP-Paketen und DNS-Abfragen - an den CNC-Server im Internet weitergeleitet.

Dragonfly
In diesem Szenario erhält ein Entwickler eine E-Mail mit einem Link zur Aktualisierung seiner HR-Zeitmessungssoftware. Sobald diese Software jedoch ausgeführt wird, ist das System des Benutzers mit einem Trojaner infiziert. Der Trojaner verbreitet sich dann im gesamten Netzwerk und erfasst Screenshots aller infizierten Computer. Zu den infizierten Computern gehören der Computer des Benutzers sowie die Firmendatenbank, die mit einem nach außen gerichteten Webserver verbunden ist. Diese Screenshots werden auf dem Firmen-Webserver gespeichert, um von einem entfernten Angreifer über eine Web-Shell heruntergeladen zu werden, die auf dem Server installiert wurde.

Fortgeschrittene Szenarien

Java Sendmail
In diesem Szenario lädt das Cyber Training System eine Website, die einen Java Applet Trojaner enthält. Einmal ausgeführt, verbindet er sich über SSH mit dem Sendmail-Server und fügt allen Mails eine Forward-Regel hinzu. Alle organisatorischen E-Mails werden an den Angreifer weitergeleitet.

Ransomware
In diesem Szenario sendet das Cyber Trainer System eine mit Ransomware infizierte E-Mail. Die E-Mail stellt eine legitime E-Mail mit einem angehängten Dokument dar. Nachdem ein ahnungsloser Mitarbeiter das Dokument geöffnet hat, werden die Daten im System verschlüsselt und der Mitarbeiter wird aufgefordert ein Lösegeld für den Erhalt des Entschlüsselungscodes zu zahlen. Der Teilnehmer wird geschult, wie er den Angriff erkennt und analysiert, wie er Daten wiederherstellt und wie er dies in Zukunft verhindern kann.

SCADA Field to Field
In diesem Szenario simuliert das Cyber Training System einen Angriff, der von einer SPS im Feld ausgeht, direkt zu einer anderen SPS. Das Ergebnis des Angriffs in diesem Szenario ist "still" und lässt keine auffälligen Anzeichen von physischen Schäden erkennen. Der Teilnehmer sollte das Netzwerk und den Alarm am SIEM untersuchen, um den Angriff und das genaue Problem mit der SPS zu identifizieren.

Trojan Share Privilege Escalation
In diesem Szenario wird ein Trojaner per E-Mail an eine Arbeitsstation gesendet. Der Trojaner wird unter Benutzerrechten gestartet und ist somit eingeschränkt. Es findet eine Skriptdatei, die sich auf einer Netzwerkfreigabe befindet. Sobald das Skript gefunden wurde, fügt der Angreifer einen speziellen Befehl in das Skript ein, der es ihm ermöglicht, ein neues Administratorkonto zu erstellen. Mit dem neuen Konto bricht der Angreifer in den Datenbankserver ein und verwendet ihn als File Gateway, um geheime Dateien auf die Unternehmenswebsite hochzuladen, was zu einem größeren öffentlichen Datenverlust führt.

WMI Worm
In diesem Szenario verbindet das Cyber Training System eine mit einem Wurm infizierte CD mit einem Windows-Rechner. Beim Einlegen wird die automatische Datei ausgeführt und der Wurm geladen, der sich selbst kopiert und die komprimierte WatchDog-Ausführungsdatei in das Windows-Verzeichnis kopiert und ausführt. Der Wurm scannt das interne und externe Netzwerk, verbreitet sich über WMI-Befehle und blockiert jede Ausführung von Systemüberwachungsanwendungen (z. B. TaskMgr, ProcMon, Regedit,...) indem er die Anwendungsthreads einfriert.