Red Teaming: Eindringen in der wirklichen Welt

Mit Hand und Fuß

Sascha Herzog

Der fünfte Artikel der Serie zu „Red Team Assessments“ beschreibt das Thema physisches Eindringen in Gebäude und gesicherte Bereiche. Von den Analysten verlangt das, ihre gewohnte Komfortzone am Schreibtisch zu verlassen und sich die Hände schmutzig zu machen.

Der erste Artikel dieser Serie [1] skizzierte bereits einen Fall, bei dem es uns nachts gelang, über schlecht gesicherte Tiefgaragen Zugang zu wichtigen Gebäudeteilen einer kritischen Infrastruktur zu erlangen. In solchen Fällen verwendet man häufig auch Werkzeuge wie Lockpicking-Sets und geklonte RFID-Karten, um verschlossene Türen zu öffnen (Links zu den Werkzeugen und alle weiteren Links des Artikels sind unter ix.de/ix1810080 zu finden).

In dem Fall, der heute beschrieben werden soll, bevorzugten wir Social Engineering als Werkzeug der Wahl, um uns physischen Zugang zu einem gut gesicherten Bereich in einem der Gebäude unseres Kunden zu verschaffen. Bei dem Kunden handelt es sich um ein internationales Unternehmen aus einem speziellen Bereich der industriellen Fertigung.

Die gesamte Aktion erforderte ein hohes Maß an Planung und Vorbereitung – weshalb wir uns wie immer zu Beginn möglichst viele taktisch relevante Informationen beschafften, um daraus die effektivsten Angriffspfade zu konstruieren. Eine Idee war, sich als Servicetechniker auszugeben, der die Wartung einer zentralen Maschine vornehmen muss. Diese stand im gut gesicherten Reinraum zur maschinellen Fertigung spezieller Komponenten und würde einem Angreifer nach erfolgreicher Kompromittierung ermöglichen, die gesamte Produktion nachhaltig und lange Zeit unbemerkt zu stören oder vollständig lahmzulegen.

Im schlimmsten Fall droht der Ruin

So etwas ist beispielsweise durch die Veränderung von Bohrlöchern im Millimeterbereich oder durch die Zerstörung extrem teurer Spezialmaschinen möglich. Deren Austausch kann viele Monate dauern, ohne dass währenddessen weiter produziert werden kann. Im schlimmsten Fall bedeutet das für ein Unternehmen den finanziellen Ruin oder eine anhaltende Rufschädigung.

Nur zwei Personen im Unternehmen hatten Zugang zu dem gut gesicherten Bereich, in dem die Maschine stand. Um in diesen Raum zu gelangen, musste man zuvor mehrere zugangsgeschützte Bereiche und eine Schleuse passieren, ganz abgesehen von den Überwachungskameras und dem Alarmsystem. Der beste Weg dorthinein war also ein autorisierter Zugang per Einladung durch das Unternehmen selbst.

Durch unsere Informationsbeschaffung zu Beginn kannten wir den Maschinenhersteller und die Techniker, die für Servicewartungen zuständig waren. In einem ersten Schritt klonten wir die Webseite des Maschinenherstellers, besorgten uns ein gültiges Serverzertifikat und richteten einen Mailserver für die neue Domain ein. Daraufhin meldeten wir uns telefonisch beim Fertigungsleiter, den wir über LinkedIn ausfindig machen konnten, unter dem Vorwand, dass wir aufgrund eines Fehlers in der Software der Maschine gerade überall manuell Patches einspielen müssten, da es sonst zu Fehlern in der Produktion kommen könnte.

Angekündigter Servicebesuch

Der Fertigungsleiter kaufte uns die Geschichte am Telefon ab, verwies uns aber an seinen Teamleiter, der ihn während seines Urlaubs, den er eine Woche später

Termin Wartung [redacted]

Sehr geehrte Damen und Herren,

vor kurzem wurde ein Fehler in der Steuerungssoftware der [redacted]-Serie gefunden. Laut unserer Kundendatenbank verfügt Ihr Betrieb über mindestens eine [redacted].
Der Fehler führt bei einzelnen Maschinen zu Fehlproduktion (ca. 1/500) und/oder Produktionsstillständen sowie Verringerung der Produktionsraten. Der Software-Fehler scheint datumsabhängig ausgelöst zu werden.

Da in letzter Zeit vermehrtes Auftreten dieses Fehlers und mehrtätige Produktionsausfälle gemeldet wurden, sendet [redacted] aktuell Service-Techniker zu allen Kunden aus. Unser Terminplan sieht Anfang Juni für den Raum [redacted] vor. Gemäß Absprache mit Ihrem Betrieb würde ein Service-Techniker am
[redacted]
gegen
10:30
die Wartung vornehmen.

Die Länge des Wartungsfensters beträgt ca. 30 Minuten. Die Aktualisierung kann im laufenden Betrieb durchgeführt werden, sodass die Produktion nicht unterbrochen werden muss.

Wir entschuldigen uns für die Unannehmlichkeiten. Sollten bei Ihrer [redacted] Fehler auftreten, teilen Sie uns dies bitte umgehend unter not-service@[redacted] mit.

Freundliche Grüße / Best regards,

[redacted] | Service
| [redacted] | Germany
T +49 (0) 17[redacted] | F +49 ([redacted]

service@[redacted] | [redacted]

Sitz (Seat): [redacted]

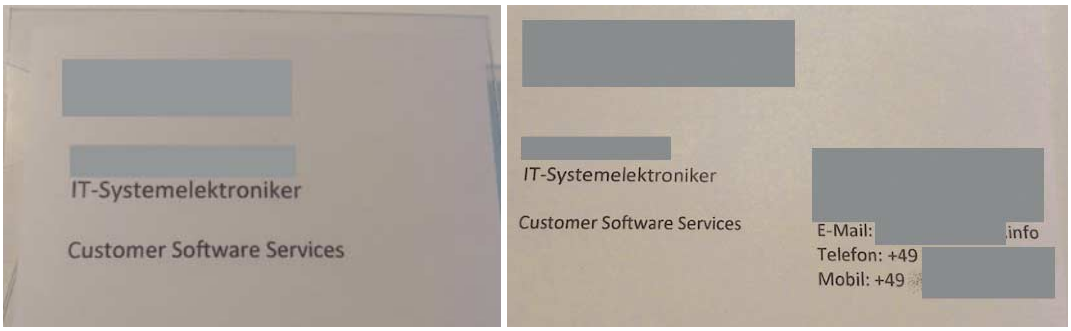
Dank der ähnlichen Domain und des echten Hersteller- und Maschinennamens ließ sich eine plausible, echt wirkende E-Mail konstruieren (Abb. 1).

antreten wollte, vertreten sollte. Er bat uns, diesem eine E-Mail zu schicken und einen Termin vorzuschlagen. Da wir ja eine sehr ähnliche Domain wie der echte Servicetechniker besaßen, konnten wir eine authentisch aussehende E-Mail an den Vertreter des Fertigungsleiters versenden (Abbildung 1).

Der Ortstermin wurde uns kurze Zeit darauf bestätigt und wir konnten einen Analysten schicken, der, als Servicetechniker verkleidet, versuchen würde, an die Maschine zu kommen. Dafür brauchte er natürlich echt aussehende Visitenkarten und einen Mitarbeiterausweis. Beides erstellten wir kurzerhand mit unserem Visitenkartendrucker (Abbildung 2).

So vorbereitet, erschien unser Mitarbeiter pünktlich um 10:30 Uhr am Haupteingang des Unternehmens, meldete sich bei der Empfangsdame und übergab ihr gleich seine Visitenkarte. Die Empfangsdame bat die Vertretung des Fertigungsleiters telefonisch, ihn abzuholen.

Der Fertigungstechniker führte unseren Analysten bereitwillig durch sämtliche Türen. Auf dem Weg zu dem Raum, wo die Maschine stand, warf unser Mitarbeiter nebenbei noch einen USB-Stick mit einem Trojaner unauffällig in ein offenes



Visitenkarte und Mitarbeiterausweis unterstreichen die Glaubwürdigkeit des Auftretens als Servicemitarbeiter (Abb. 2).

Büro. Die Vertretung des Fertigungsleiters wollte beobachten, was unser Mann machte, und fragte nach, was denn jetzt genau das Problem sei und wie es behoben werden würde.

Angebliches Diagnoseprogramm eingeschmuggelt

Unser Analyst entgegnete, dass er erst mal ein Diagnoseprogramm starten werde, um mögliche Fehler zu lokalisieren, und dann den Patch einspielen wolle. Wie genau der Patch funktioniere, wisse er auch nicht, allerdings wisse er, dass dieser Patch selten verwendete Steuerungsroutinen korrigieren werde. Das sei es, was man ihm mitgeteilt habe. Das System lief in einer UNIX-Umgebung, weshalb wir das angebliche Diagnoseprogramm im Vorfeld erstellen und auf einen USB-Stick bringen konnten.

Unser Programm war harmlos und gab nur ein paar gefälschte Codezeilen auf dem *stdout* der Konsole aus und beendete sich danach. In der Realität hätten Angreifer hierüber allerdings spezielle Konfigurationsparameter der Maschine verändern oder Malware auf das System spielen können. Wie unser gefälschtes Diagnoseprogramm aussah, zeigt Abbildung 3.

Nach Beendigung des Programms machte unser Analyst noch einen Schnappschuss von dem Bildschirm samt Maschine, um einen Beweis für die Kompromittierung zu haben. Zu dem anwesenden Fertigungstechniker sagte er, das brauche er, um die „Response Codes“ zu dokumentieren, die er in seinen Bericht schreiben müsse. Der Techniker kaufte ihm alles ab und begleitete ihn anschließend noch bis zum Ausgang. Alles in allem dauerte der Vorortteinsatz nur 25 Minuten. Somit hatten wir den Beweis angetreten, dass und auf welche Weise es möglich ist, das Herzstück der Fertigung und damit das Herzstück des Unternehmens vollständig zu kompromittieren und das Ziel dieser Red-Team-Kampagne zu erreichen.

Wir erfuhren später, dass der USB-Stick mit dem Trojaner zwar von einer Mitarbeiterin gefunden, allerdings nicht in ihren PC eingesteckt, sondern vorbildlich bei der Unternehmensleitung abgegeben wurde.

```
top:~$ ./[redacted]update.sh

[redacted] Updater v.1.1.3 -----

radio signal to activate wireless maintenance module.....

 maintenance module activated!

g for unpatched machines.....

[redacted] found! Commencing update.....

ng file /lib/modules/3.19.0-16-generic/kernel/drivers/firewire/nosy.ko.
ng file /sys/devices/LNXSYSTM:00/LNXSYBUS:00/PNP0A08:00/device:22/device
ce:29/power/runtime_enabled.
ng file /sys/devices/LNXSYSTM:00/LNXSYBUS:00/PNP0A08:00/device:3a/device
ce:3c/device:44/power/runtime_usage.
ng file /sys/devices/platform/PNP0C14:02/power/runtime_active_time.
ng file /etc/apparmor.d/abstractions/likewise.
ng file /etc/vmware-installer/components/vmware-ovftool.
ng file /lib/modules/3.19.0-18-generic/kernel/drivers/net/ethernet/qlogi
```

Das in diesem Fall harmlose Diagnoseprogramm hätte auch schlimme Auswirkungen nach sich ziehen können, etwas das Manipulieren von Konfigurationsparametern (Abb. 3).

Festgelegte Prozesse etablieren

Ein paar Wochen nach diesem Einsatz führten wir eine Awareness-Kampagne bei dem Kunden durch und schulten die Mitarbeiter, wie sie mit solchen und ähnlichen Angriffen umgehen sollten. Zudem unterstützten wir den Kunden in der Entwicklung von Richtlinienkatalogen und Prozessen, um so etwas zukünftig zu vermeiden. Alleine das Anfordern von Ausweisen am Empfang kann hier schon einiges bewirken und hätte einen realen Eindringling wahrscheinlich abgewehrt.

Auch die Rücksprache mit bekannten Ansprechpartnern im echten Serviceunternehmen hätte dabei helfen können, das falsche Unternehmen zu enttarnen. Positiv zu bemerken war, dass das Unternehmen in Sachen Zugangsschutz und physischer Überwachung bereits sehr gut ausgerüstet war. Und ebenso waren einzelne Mitarbeiter, wie die Dame aus dem Büro, schon ausreichend geschult, um auf manche Arten des Social Engineering nicht hereinzufallen.

Im nächsten Artikel unserer „Red Teaming“-Serie befassen wir uns intensiv mit der Technik hinter Backdoor-Trojanern, dem Umgehen von Sicherheitstechnologien, schwer zu entdeckenden „Command & Control“-Kanälen und dem Ausbreiten in internen Netzwerken, dem „lateral Movement“. (ur@ix.de)

Sascha Herzog

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

[1] Sascha Herzog; Awareness; Mit allen Mitteln; Sicherheitstests: Angriffe auf Technik und Mensch; *iX* 2/2018, S. 78

Alle Links: ix.de/ix1810080