SECURITY AWARENESS: MICROSOFT JAGT DAS PHANTOM

SECURITY AWARENESS: MICROSOFT JAGT DAS PHANTOM

Privatwirtschaftliche Unternehmen und Behörden haben jahrelang die Sicherheit ihrer Computersysteme und Netzwerke verbessert. Gut konfigurierte Firewalls, Virenscanner und Intrusion Detection Systeme erschweren Computerkriminellen und Spionen deutlich Ihr Handwerk.
Aus diesem Grund haben die Angreifer ihren Fokus in den letzten Jahren immer mehr auf ein neues, vermeintlich einfacheres Angriffsziel verändert: die Mitarbeiter. Mittlerweile gilt „der Mensch“ als das schwächste Glied in der unternehmensweiten Sicherheitskette. Moderne Industriespione versuchen z.B. nicht mehr primär, Computersysteme zu hacken, sondern Sie erschleichen sich von Mitarbeitern Benutzername und Passwort und erhalten somit „legitimierten“ Zugriff auf kritische Systeme.

Microsoft ist als Marktführer immer ein potenzielles Ziel. Deshalb haben wir unsere Mitarbeiter für solche Angriffsszenarien sensibilisiert. Die Erfahrungen aus unserer Security Awareness Kampagne möchte ich mit Ihnen teilen.

Eine interessante Lektüre wünscht Ihnen

Tom Köhler
Direktor Strategie Informationssicherheit & Kommunikation Microsoft Deutschland GmbH

1 | DIE GROSSE HERAUSFORDERUNG: SOCIAL ENGINEERING

Das Eindringen in ein Unternehmen durch List und Manipulation bezeichnet man als **Social Engineering**. Der Angreifer hat das Ziel, sich das Vertrauen der Mitarbeiter zu erschleichen und dann zu missbrauchen, um so schrittweise über mehrere Phasen an Geheimnisse und Interna zu gelangen bzw. die Opfer zu manipulieren.

Die einzig effektive Antwort auf diese Bedrohung lautet: Sensibilisierung der Mitarbeiter und des Managements zum Thema Informationssicherheit, d.h. die Schaffung eines Sicherheitsbewusstseins (in Englisch **Security Awareness**) als Bestandteil der Unternehmenskultur.
Hierzu bedarf es einer bewussten Verhaltensänderung der Mitarbeiter in sicherheitsrelevanten Situationen, zum Beispiel:

- Den PC sperren, auch wenn man nur kurz den Arbeitsplatz verlässt.
- Vertrauliche Unterlagen wegsperren.
- Unbekannte Personen im Gebäude ansprechen.
- Niemandem sein Passwort weitergeben.

Eine Verhaltensänderung im Bereich Sicherheit bedingt jedoch eine Änderung der Einstellung zum Thema Sicherheit. Da sich die Einstellung aus kognitiver Ebene (Wissen) und emotionaler Ebene (Sympathie) zusammensetzt, reicht eine reine Wissensvermittlung nicht aus. Eine erfolgreiche Sensibilisierung der Mitarbeiter benötigt eine positive emotionale Komponente. Deshalb wird die Wissensvermittlung im Rahmen einer Security Awareness Kampagne positiv aufgeladen und verstärkt.

Wie soll man starten?

Eine zielgerichtete Sensibilisierung setzt voraus, dass die „Schwachstellen“ bekannt sind. Aus diesem Grunde hat Microsoft einen simulierten Industriespionageangriff durchführen lassen. Der Spezialanbieter HvS-Consulting GmbH erhielt den Auftrag, die Sicherheitskultur im Rahmen eines Social Engineering Assessments zu testen und zu dokumentieren.

Die Ergebnisse dieses Angriffs haben nicht nur die nötige Aufmerksamkeit in der Geschäftsleitung erzeugt, sie eigneten sich auch hervorragend als Basis für die nachgelagerten Sensibilisierungsmaßnahmen.

Zudem erlauben sie die Erfolgsmessung der Kampagne. Ein Wiederholungsangriff nach Abschluss der Kampagne sollte zu einer signifikanten Reduktion erfolgreicher Angriffe führen.

2 | MICROSOFT JAGT DAS PHANTOM!

Eine besondere Herausforderung für die Kampagnenplanung stellte die Vielfalt an bestehenden internen Marketingkampagnen dar. Da Microsoft neue Produktreleases und Innovationen auch intern intensiv kommuniziert, bestand die Gefahr, dass unsere Sicherheitsbotschaften in der allgemeinen Kommunikationsflut untergehen.

Deshalb haben wir uns für eine Kampagne mit hoher Interaktion entschieden:

Basierend auf der Idee der “virtuellen Bedrohung” hat ein Phantom Microsoft den Kampf angesagt. Es will sich nicht persönlich bereichern, will aber beweisen, dass es die Sicherheit des Softwareanbieters cracken kann. Unauffälliges Verhalten erscheint ihm zu einfach und bringt keinen Ruhm und Ehre, deshalb kündigt es seine Angriffe jeweils vorab an und fordert die Microsoft Mitarbeiter auf, sich zu wehren.

Das Phantom erfüllte alle unsere Forderungen an eine Awareness Kampagne:

- Es erzeugt Emotionen, die das Thema Sicherheit nicht negativ aufladen.
- Es erlaubte eine Zerlegung der Kampagne in flexible Kapitel, die auch nach Jahren wiederholt werden können.

Das „Phantom“ Thema konnte in Form des weißen Handschuhs problemlos in allen Kampagnenelementen visualisiert werden und spannte den übergreifenden Bogen.
Zudem passte die gemeinschaftliche Phantomjagd zur stark Team orientierten Unternehmenskultur von Microsoft.

Der Ablauf

Das Phantom führte 5 Angriffe zu folgenden Themen durch:

1. Unerlaubter Zutritt zum Gebäude
2. Gesperrter PC
3. Umgang mit Passwörtern
4. Umgang mit mobilen Geräten
5. Informationsklassifizierung

Es sendete vor jedem Angriff eine Ankündigungs-Email an den Microsoft Geschäftsführer. Dieser leitete die Mail an die Belegschaft mit der Aufforderung, gemeinsam den bevorstehenden Angriff abzuwehren. Einige Tage später wurde der angekündigte Angriff durchgeführt.

Nach ca. 2 Wochen meldete sich das Phantom per Email und bewertete den Erfolg. Ein erfolgreicher Angriff gab einen Punkt für das Phantom, eine erfolgreiche Abwehr einen Punkt für Microsoft. Zeitgleich kündigte es den nächsten Angriff an.

Alle Kommunikationselemente innerhalb der Kampagne führten über den Intranet Link http://phantomjagd auf einen Sharepoint Server.

Dort erhielten die Mitarbeiter Hintergrundinformationen zum bevorstehenden Angriff und konnten ein Security Online Training absolvieren, welches das relevante Wissen zu Richtlinien und korrektem Verhalten vermittelte. Die Inhalte des Online Trainings wurden auf die Bedürfnisse der Kampagne abgestimmt und um Videos ergänzt, die anschaulich erläutern, wie die bevorstehenden Phantomangriffe erfolgreich abgewehrt werden können.

3 | DIE ANGRIFFE IM DETAIL

1. Unerlaubter Zutritt zum Gebäude

Viele Mitarbeiter halten die physische Sicherheit bereits für einen wirksamen Schutz vor Eindringlingen. Das Phantom sollte uns das Gegenteil beweisen. Als ersten Schritt kündigte es den unerlaubten Zutritt zu unseren gesicherten Gebäuden an. Es wolle die Unaufmerksamkeit der Mitarbeiter ausnutzen und durch „Tailgaiting“ ohne Zugangskarte in gesicherte Bereiche eindringen.

Parallel zur Ankündigungs-Email wurden an alle Türen mit Zugangskontrolle Aufkleber angebracht:

Ich komme Euch besuchen!

Ich werde mir Zutritt durch diese Sicherheitstür verschaffen – und zwar ohne Ausweis. Mal sehen, wer von euch mich rein lässt…

Gruß vom Phantom

http://Phantomjagd

Dieser Punkt ging klar an das Phantom.

2. Gesperrter PC

Ungesperrte PCs sind ein erhebliches Sicherheitsrisiko, da Angreifer in kürzester Zeit Dateien manipulieren oder auf USB-Sticks ziehen können.

Nachdem das Phantom den Beweis erbracht hat, dass ein Zugang zum Gebäude möglich ist, kündigte es in seinem 2. Angriff an, ungesperrte Rechner näher unter die Lupe zu nehmen. Hierzu wurden lebensgroße Phantomaufsteller aus Pappe in den Fluren platziert.

Dein Rechner ist mein Rechner!

Ist Dein Rechner gesperrt? Lass ihn lieber nicht ungeschützt zurück! Denn ich werde jede Gelegenheit nutzen…

Gruß vom Phantom

http://Phantomjagd

Der Angriff erfolgte zu Mittagszeiten. Das Phantom suchte ungesperrte PCs und legte auf diese eine DIN A5 Phantomkarte:

War dein Rechner wirklich gesperrt? Überleg mal, was ich alles hätte machen können! Dieser Punkt geht wohl an mich :-)

Gruß vom Phantom

Diese Karten entwickelten sich im Laufe der Zeit zu einem hervorragenden viralen Marketinginstrument: die ursprünglichen „Besitzer“ der Karten warteten nur darauf, bis ein Kollege seinen Rechner ungesperrt alleine lies, um ihm dann den „schwarzen Peter“ auf den Rechner zu legen. Somit haben sich die Mitarbeiter auf spielerische Weise gegenseitig sensibilisiert.

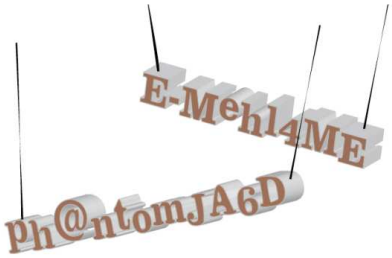
Zudem haben Manager diese Phase der Kampagne genutzt ihre Teams zu motivieren, z.B. das Phantom zu enttarnen und auf unbekannte Personen zu achten. Auch dieses Verhalten trug zu einer hohen Authentizität der Botschaft bei.

3. Umgang mit Passwörtern

„Niemand benötigt Euer Passwort! Nicht einmal ein Administrator“ lautet eine der Kernbotschaften zum Umgang mit Passwörtern bei Microsoft. Die Weitergabe des eigenen Passwortes stellt ein hohes Sicherheitsrisiko dar, da der Angreifer dauerhaft auf alle Informationen zugreifen kann, auf die auch sein Opfer zugreifen kann. Das Phantom wollte daher testen, ob sich die Mitarbeiter wirklich daran halten.

Während die ersten beiden Angriffe noch eher spielerisch mit Fehlverhalten umging, erhöhte der dritte Angriff deutlich die persönliche Betroffenheit der Mitarbeiter: das Phantom kündigte an, sich Zugangsdaten und Passwörter über fingierte Telefonanrufe und gefälschte Emails zu erschleichen.

Zeitgleich hingen während dieser Phase mehrere, ca. 2 m breite Styropor Passwörter im Foyer und in der Kantine an Angelhaken und symbolisierten die bevorstehende Phishing Attacke:



Die Social Engineering Angriffe wurden wieder von HvS-Consulting durchgeführt.

Die ersten Angriffe verliefen (leider) durchaus erfolgreich für das Phantom. Allerdings entwickelte sich innerhalb kürzester Zeit ein enormer Sport- und Teamgeist. Mitarbeiter, die auf das Phantom hereingefallen waren, versendeten Warnmails an Kollegen mit den möglichen Angriffsvarianten. Innerhalb kürzester Zeit verbreiteten sich diese Mails in einem Schneeballsystem im gesamten Unternehmen.

Diese virale und hochgradig authentische Kommunikation erzeugte einen derart hohen Aufmerksamkeitswert, dass sich selbst Wochen nach dem Angriff die Sensibilisierung für Social Engineering Attacken auf einem sehr hohen Niveau hielt.

4. Umgang mit mobilen Geräten

Da die meisten Mitarbeiter bei Microsoft mit Notebooks arbeiten und häufig reisen, wurden sie in dieser Phase zur Nutzung unsere haueigenen Festplattenverschlüsselung BitLocker motiviert. Unverschlüsselte Daten sind im Falle von Verlust oder Diebstahl des Notebooks eine leichte Beute.

Nach einer Weihnachtspause meldete sich das Phantom mit der Ankündigungs-Email zu Angriff 4 zurück. Notebooks hingen von der Decke und die aus Phase 2 bekannten Aufsteller gaben Auskunft über den bevorstehenden Angriff.

Verschlüsselt Eure Daten, bevor ich sie mir hole!

Ist der Inhalt Eurer Notebooks schon mit Bitlocker verschlüsselt? Ich werde es bei meinem nächsten Besuch überprüfen.

Gruß vom Phantom
http://Phantomjagd

Das Phantom schlug diesmal in der Nacht zu. Es überprüfte Notebooks auf Festplattenverschlüsselung, die sich nachts ungesichert am Arbeitsplatz befanden. Unverschlüsselte Notebooks erhielten eine Karte:

Im den nachfolgenden Tagen nahmen (erhofft und erwartet) die Anfragen zur Festplattenverschlüsselung beim Helpdesk erheblich zu. Nach wenigen Wochen waren die gesteckten Ziele hinsichtlich des vermehrten Einsatzes von BitLocker übertroffen.

5. Informationsklassifizierung

Informationsklassifizierung ist ein Grundlagenthema in nahezu jedem Unternehmen. Wer klassifiziert? Nach welchen Kriterien? Was bedeutet eine entsprechende Klassifizierung für den Umgang mit dieser Information? Zum Abschluss der Angriffsreihe wollte man auf dieses Thema noch einmal fokussieren.

Das Phantom machte sich auf die Suche nach vertraulichen Informationen. Jeder Mitarbeiter fand in seinem Postfach eine Nachricht des Phantoms: es werde auf Schreibtischen, in Meetingräumen und in Papierkörben nach vertraulichen Dokumenten suchen.

WICHTIGE MITTEILUNG!

Hallo Microsoft-Mitarbeiter und -Partner,

die Sicherheit Eurer digitalen Daten habt Ihr mittlerweile ja gut im Griff. Wie stehts denn mit Euren Textdokumenten auf?

Wie ich weiß, verwendet Ihr bei Microsoft folgende Klassifizierungen für Eure Informationen:

- High Business Impact (HBI): Verlust hat schwerwiegende bis katastrophale Folgen
- Moderate Business Impact (MBI): Verlust hat ernste Folgen
- Low Business Impact (LBI): Verlust hat geringe bis keine Folgen

Nutzt Ihr diese denn, und handelt Ihr auch entsprechend?

Im Security 101 Training unter **http://phantomjagd** könnt Ihr Euch schlaumachen.

Natürlich werde ich Euch wieder besuchen und testen, ob ich ein paar HBI- und MBI-Dokumente auf Schreibtischen, an Kopiermaschinen und in Besprechungsräumen finde. Also räumt lieber auf!

Gruß vom Phantom

PS. Ihr könnt dieses LBI-klassifizierte Dokument jetzt vernichten, indem Ihr es aufesst …

Um die Aufmerksamkeit zu erhöhen, wurde diese Nachricht mit Lebensmittelfarbe auf Esspapier gedruckt und die Mitarbeiter aufgefordert, dieses Dokument nach dem Lesen aufzuessen.

Microsoft ist weitestgehend ein papierloses Büro. Daher hatte das Phantom keine Erfolge zu verzeichnen. Dennoch wurden den Mitarbeitern in dieser Phase noch einmal die Informationsklassen und der Umgang mit Dokumenten der entsprechenden Klasse vermittelt.

4 | ERGEBNISSE

Informationssicherheit war in der Wahrnehmung der Mitarbeiter vor der Kampagne ein eher beiläufiges Thema. Dies wirkte sich entsprechend auf das tägliche Verhalten aus.

Zudem wurde die Unkenntnis über moderne Angriffsmethoden wie z.B. Social Engineering als eine der größten Schwachstellen identifiziert.

Dank der kreativen Unterstützung der beteiligten Agenturen (Wunderman ,HvS-Consulting) konnte mit der Phantomkampagne die „Security Awareness“ bei Microsoft Deutschland signifikant gesteigert werden.

Bereits während der Kampagne wurde Informationssicherheit ein viel diskutiertes und ständig präsentes Thema. Das Steuerungsteam der Kampagne erhielt schon während der Angriffe zahlreiches positives Feedback von den verschiedensten Abteilungen.

Dies wurde auch in einer anonymen Mitarbeiterbefragung nach Abschluss der Kampagne bestätigt:

- 91% der Befragten antworteten, dass sich Ihre Einstellung zum Thema Sicherheit positiv verändert habe,
- 80% gaben an, dass sie Ihr Verhalten geändert haben.

Die Erfolgsfaktoren

Die Geschäftsleitung zeigte durch ihre aktive und motivierende Rolle in der Kampagne den Stellenwert der Informationssicherheit für das Unternehmen.

Die hohe Interaktion zwischen Phantom und Mitarbeitern und der daraus resultierende Teamgeist erschufen eine hohe Motivation und positive Emotionen.

Die viralen Kommunikationselemente der Kampagne (Karten, Motivations-Emails, Warnungen, etc.) verliehen den Botschaften eine hohe Authentizität und Glaubwürdigkeit.

Das webbasierte Training vermittelte das Wissen zu Richtlinien und korrektem Verhalten. Die Aufklärung zur Abwehr bevorstehender Phantomangriffe gab einen zusätzlichen Anreiz, sich dieses Wissen schnell anzueignen.

Das „Phantom“ Thema erlaubte mit dem weißen Handschuh eine sehr wirkungsvolle Visualisierung, die sich durch alle Kampagnenelemente zog.

Übrigens: Microsoft hat das Phantom letztendlich mit 3:2 geschlagen!

Fazit

Die Phantomkampagne hat einen beträchtlichen Beitrag zur Steigerung der Informationssicherheit bei Microsoft geleistet.

Sind wir jetzt sicher? Gewiss nicht vollständig, aber wir sind unserem Ziel einen großen Schritt näher gekommen.

Wird dieser Erfolg nachhaltig sein? Ja, wenn wir die Sensibilisierung kontinuierlich immer wieder aufleben lassen. Security Awareness ist ein ständiger Prozess, der in seinen Phasen unterschiedlich präsent sein kann, jedoch nie endet.

Daher können wir fast sicher sein, dass uns das Phantom irgendwann wieder besuchen wird!