Cybersecurity

Case Study 2021

Inhalt

Einleitung 3

Zusammenfassung 4

Warum? 5

Phishing-Erst-Audit 5

Handlungsempfehlung 7

Ergebnis 7

Einleitung

Schon im Jahr 2000 stellte der Sicherheitsexperte Bruce Schneier fest, dass sich die IT-Welt nach der Ausbeutung von Schwächen in Hardware und Software schon mitten in der dritten „semantischen“ Welle von Netzwerkangriffen befinde: die Angriffe auf Menschen, die Hardware und Software benutzen. Diese seien schlimmer als physische oder syntaktische Angriffe, denn, so Schneier, sie „richten sich direkt auf die Mensch-Maschine-Schnittstelle, die unsicherste Schnittstelle. [...] Und jeder Versuch zur Lösung des Problems muss sich mit Menschen auseinandersetzen, nicht mit Technik.“

Diese Case Study zeigt auf, dass die Sensibilisierungsmaßnahmen, im Rahmen einer Phishing-Simulation, zu einer wesentlichen Änderung des Nutzungsverhalten mit E-Mails geführt haben.

Im Fall des anonymisierten Firmenkunden (GmbH) fand das Phishing-Training für die Mitarbeiterinnen und Mitarbeiter, die Personalvertretung, zwei Datenschutzbeauftragte sowie die IT-Abteilung in zwei Aussendungen statt.

In der Aussendung des Phishing-Trainings wurden unter anderem drei Spear-Phishing-E-Mails verschickt. Eine dieser E-Mails, augenscheinlich vom Management ausgehend, hätte im Ernstfall versucht, durch einen Drive-by-Exploit, Schadsoftware auf dem Rechner der betreffenden Personen zu installieren. Eine weitere E-Mail, augenscheinlich von der Finanzabteilung, simulierte eine mögliche, aber recht unwahrscheinliche Arbeitsanweisung: Alle personenbezogenen Daten sollten im Rahmen einer Adressprüfung via E-Mail der zuständigen Abteilung zugesandt werden.

> “Cyber-Angreifende halten sich nicht *an Regeln, ethische Normen oder kulturelle Traditionen.*”

Zusammenfassung

Der Phishing-Attack-Simulator (PAS) wurde bei dem anonymisierten Firmenkunden (GmbH) in Form des Phishing-Erst-Audits eingesetzt, um die Resilienz der Angestellten auf Social Engineering Angriffe zu prüfen. Dazu wurden in einer Spear-Phishing-Kampagne mithilfe von Open Source Intelligence (OSINT) Mechanismen individuelle Angriffsszenarien erstellt und ausgeführt.

Ziel war es, folgende Metriken zu messen, um einen individuellen Security-Score für das Unternehmen auszugeben:

- Öffnungsrate schädlicher E-Mails
- Klickrate auf schädliche Links in E-Mails
- Eingabe von Login Credentials auf Phishing-Websites
- Öffnungsrate schädlicher Anhänge versch. Dateiformate

CYBERSICHERHEIT: DER WEG VOM WISSEN ZUM HANDELN IST WEIT

Warum?

Der Human Factor Report von 2019 zeigt, dass mehr als 9/10 Cyberangriffen die Schwachstelle Mensch nutzen um einzudringen (vgl. https://www.proofpoint.com/sites/default/files/gtd-pfpt-us-tr-human-factor-2019.pdf).

Somit zeigt sich, dass Security-Awareness der wichtigste Baustein beim Aufbau einer sinnvollen IT-Sicherheitsstruktur und der größte Treiber für die Verringerung von Schadensszenarien ist.

Weiterhin wird aus einer repräsentativen Umfrage mit Unterstützung durch pwc sichtbar, dass der größte finanzielle Schaden von Cyberangriffen auf Phishing zurückzuführen ist (vgl. https://www.pwc.de/de/cyber-security/cyberangriffe-gegen-unternehmen-in-deutschland.pdf).

Phishing-Erst-Audit:

Zur Evaluierung der Schadensrisiken wurde ein Erst-Audit bei der Kundschaft durchgeführt, dafür hat die IYS-Awareness-Plattform folgende Bausteine durchgeführt:

- Erstellung von 3 individuellen Phishing-Szenarien gemäß individueller Analyse der Kundschaft
- Übersendung von 12 Phishing-E-Mails pro Teilnehmer:in
- Managementbericht als PDF

> Dieser epochale Wandel ist eine Reise, und wie jede Reise, ist der Weg gepflastert mit Risiken und Bedrohungen.

Folgende Ergebnisse kamen zutage:

Öffnungsrate schädlicher E-Mails

Klickrate auf schädliche Links in E-Mails

Eingabe von Login Credentials auf Phishing-Websites

Öffnungsrate schädlicher Anhänge versch. Dateiformate

> Cyberkriminelle werden **immer** neue Wege finden, um Angriffe zu monetarisieren.

Das Risikolevel wurde somit mit der Ratingklasse C- bewertet. Der genaue Score bemisst sich mit dem Index 4,8 (siehe Scorebeschreibung). Auch wenn dies erschreckende Werte sind, ist es doch der Branchendurchschnitt, was aufzeigt, wie vulnerabel das Unternehmen ist.

Eine Klickrate von 40% auf schädliche Links aller Teilnehmer:innen gibt Anlass zu vier Fragen:

1. Warum haben so viele Personen auf den Link in der E-Mail geklickt?
2. Warum haben nicht mehr Empfänger:innen auf den Link in der E-Mail geklickt?
3. Wie beurteilen die Betroffenen die Auflösung der Kampagne?
4. Was halten die Anwendenden von dieser für sie ungewöhnlichen Awareness-Maßnahme?

Scorebeschreibung

Cybersecurity-Index	Score	Ratingklasse	Risikoprofil
1,0 – 1,4	100 – 91	A	ausgezeichnet
1,5 – 1,9	90 – 81	A	sehr niedrig
2,0 – 2,4	80 – 71	B	niedrig
2,5 – 2,9	70 – 61	B	mittel
3,0 – 3,4	60 – 51	C	mäßig
3,5 – 3,9	50 – 35	C	erhöht
4,0 – 4,3	34 – 25	D	hoch
4,4 – 4,9	24 – 15	D	sehr hoch
5,0 – 5,0	14 – 0	D	extrem hoch
6,0 – 6,0	–	E	unbewertet

GEWOHNHEITEN SIND SCHWER ZU ÄNDERN

Handlungsempfehlung

Um den Security-Score des Unternehmens nachhaltig zu verbessern und das Risikopotential zu verringern, haben wir folgende Empfehlungen ausgesprochen:

1. **Grundsensibilisierung in Form von Onlinekursen für alle Angestellten**
2. **Spezialschulung und Webinare für alle Angestellen und Abteilungen mit Ratings von 2,5 – 4,8**
3. **Phishing-Kampagnen verschiedener Schwierigkeitsgrade im 3-Monats-Rhythmus und aschließende Nachbesprechung der Angriffsszenarien**
4. **Newsletter mit aktuellen Angriffsszenarien**
5. **Meldeformular für erkannte Phishingangriffe**
6. **Nachkontrolle nach 6 Monaten mit Hilfe einer weiteren Evaluierungskampagne**

Ergebnis

Nach 6 Monaten wurde eine weitere Phishing-Kampagne mit selbigen Parametern an das Unternehmen gesendet. Es wurden ähnliche Schwierigkeitsgrade der Angriffsszenarien genutzt, um die Vergleichbarkeit herzustellen.

Das Unternehmen konnte in nur 6 Monaten, das Rating auf 2,2 verbessern und liegt somit in der Bewertung weit über dem Branchendurchschnitt.

Folgende Ergebnisse kamen zutage:

Öffnungsrate schädlicher E-Mails

Klickrate auf schädliche Links in E-Mails

Eingabe von Login Credentials auf Phishing-Websites

Öffnungsrate schädlicher Anhänge versch. Dateiformate