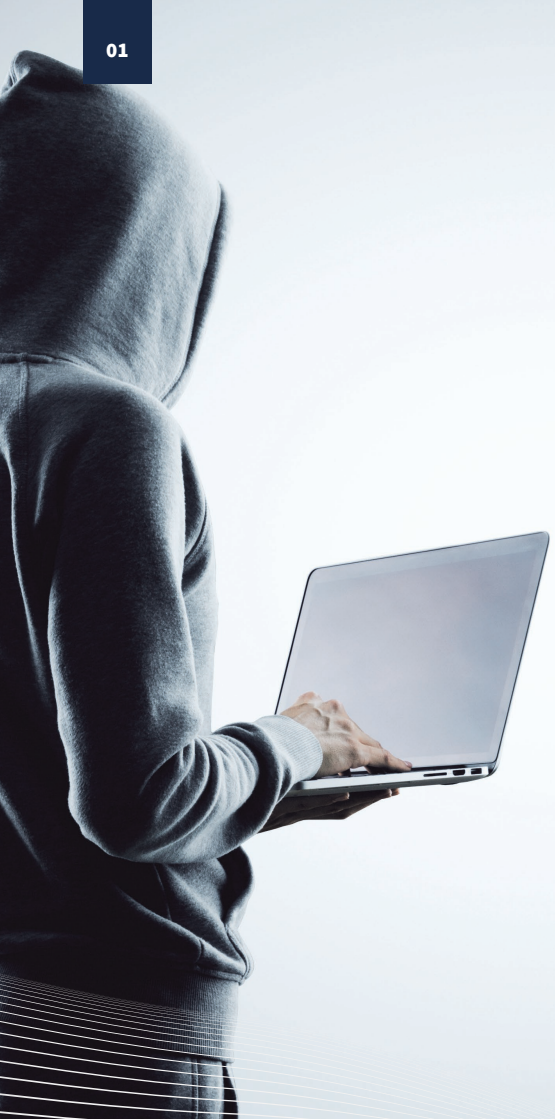
Increase YourSkills

CYBER SECURITY

Case Study 2023

Inhalt



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 bereits 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 Nutzungsverhaltens mit E-Mails geführt haben.

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

48%

deutscher Unternehmen zahlen Lösegeld nach Ransomware-Angriff*

** Hiscox - Cyber Readiness Report 2022*

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.

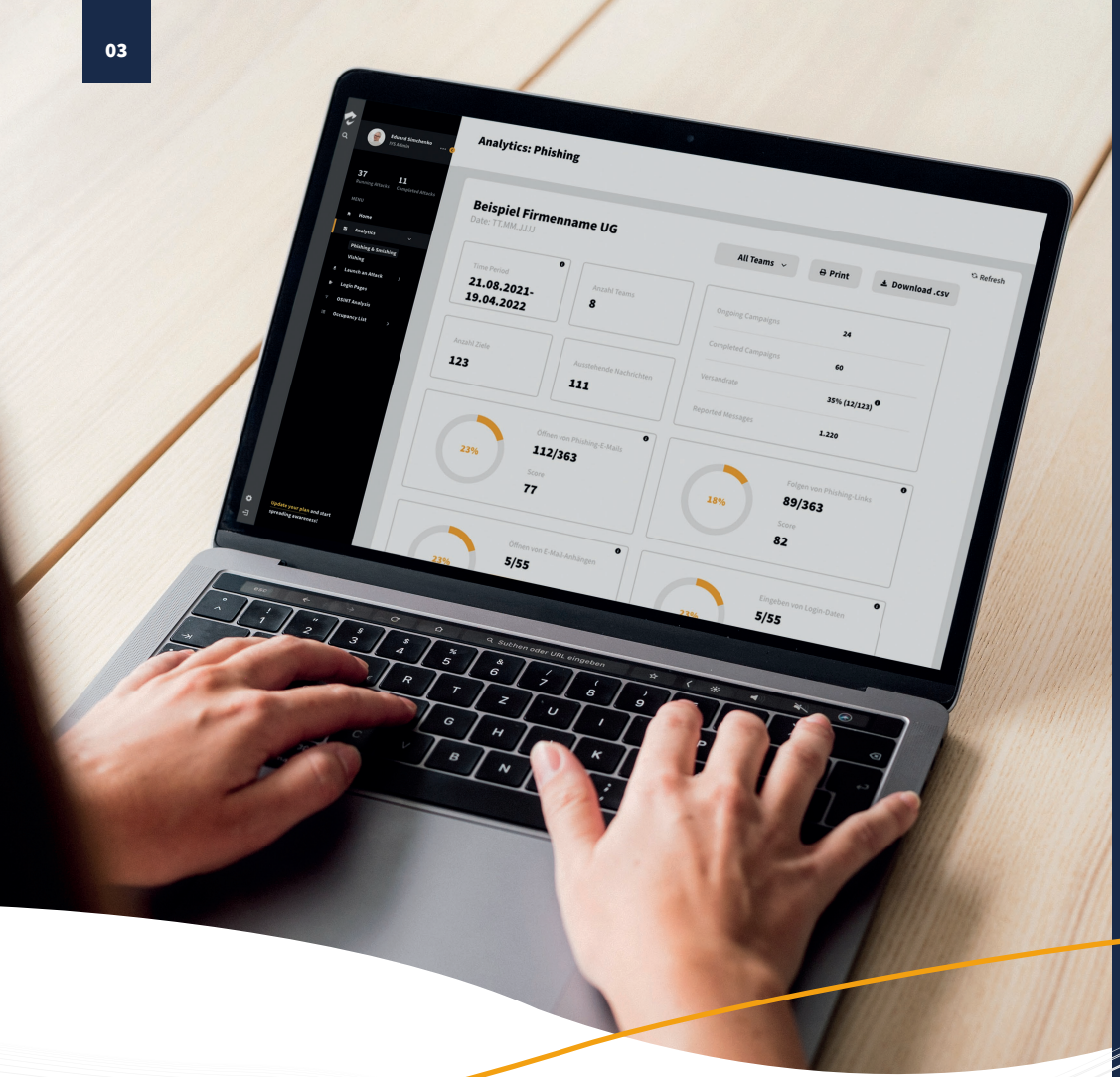
Eine weitere E-Mail, augenscheinlich von der Finanzabteilung, simulierte eine mögliche, aber recht unwahrscheinliche Arbeitsanweisung: Alle personenbezogenen Daten sollten im Rahmen einer Adressprüfung via E-Mail der zuständigen Abteilung zugesandt werden.

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

69%

aller Spam-E-Mails in 2022 waren Cyberangriffe wie z. B. Phishing-E-Mails und E-Mail-Erpressungen.*

** BSI – Die Lage der IT-Sicherheit in Deutschland 2022*



Zusammenfassung

Mit dem Phishing-Attack-Simulator (PAS) wurde bei der anonymisierten Firmenkundschaft (GmbH) ein Phishing-Erst-Audit durchgeführt, 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 verschiedener Dateiformate*

Cybersicherheit: Der Weg vom Wissen zum Handeln ist weit

Die Welt hat sich durch die Pandemie verändert, aber die Skrupellosigkeit von Cyberkriminellen bleibt unverändert. Daher bleibt der Schutz vor Cyberbedrohungen eine anspruchsvolle Aufgabe.

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

34.000

E-Mails mit Schadprogrammen wurden monatlich durchschnittlich in deutschen Regierungsnetzen abgefangen.*

** BSI – Die Lage der IT-Sicherheit in Deutschland 2022*

Warum?

Der Human Factor Report von 2022 zeigt, dass mehr als 9/10 Cyberangriffen die Schwachstelle Mensch nutzen um in IT-Systeme einzudringen [1].

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 [2].

[1] vgl. https://www.proofpoint.com/sites/default/files/threat-reports/pfpt-de-tr-human-factor-report.pdf

[2] vgl. https://www.pwc.de/de/cyber-security/cyberangriffe-gegen-unternehmen-in-deutschland.pdf

> *Die Herausforderungen im Cyberraum bleiben hoch und werden weiter rasant zunehmen.**

** Dr. Gerhard Schabhüser, Vizepräsident des Bundesamts für Sicherheit in der Informationstechnik: BSI – Die Lage der IT-Sicherheit in Deutschland 2022*

>80%

aller Unternehmen werden pro Monat mithilfe eines kompromittierten Lieferdienstkontos angegriffen.*

** Human Factor Report 2022*

Phishing-Erst-Audit

Zur Evaluierung der Schadensrisiken wurde ein Erst-Audit bei der Kundschaft durchgeführt. Dafür hat die IYS Full-Servie-Awareness Plattform folgende Schritte eingeleitet:

- *Erstellung von 3 individuellen Phishing-E-Mails mithilfe unserer OSINT-Engine*
- *Übersendung von 12 Phishing-E-Mails pro Teilnehmer:in*
- *Erstellung eines Managementreports*

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 verschiedener Dateiformate

Das Risikolevel wurde somit mit der Ratingklasse C bewertet (mäßig). Der genaue Score bemisst sich mit dem Index 3,0 (siehe Scorebeschreibung). Auch wenn dies erschreckende Werte sind, ist es doch der Branchendurchschnitt, was aufzeigt, wie vulnerabel das Unternehmen ist.

Eine Klickrate von 49% auf schädliche Links aller Teilnehmenden gibt Anlass zu vier Fragen:

1. **Warum haben so viele Personen auf den Link 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?**

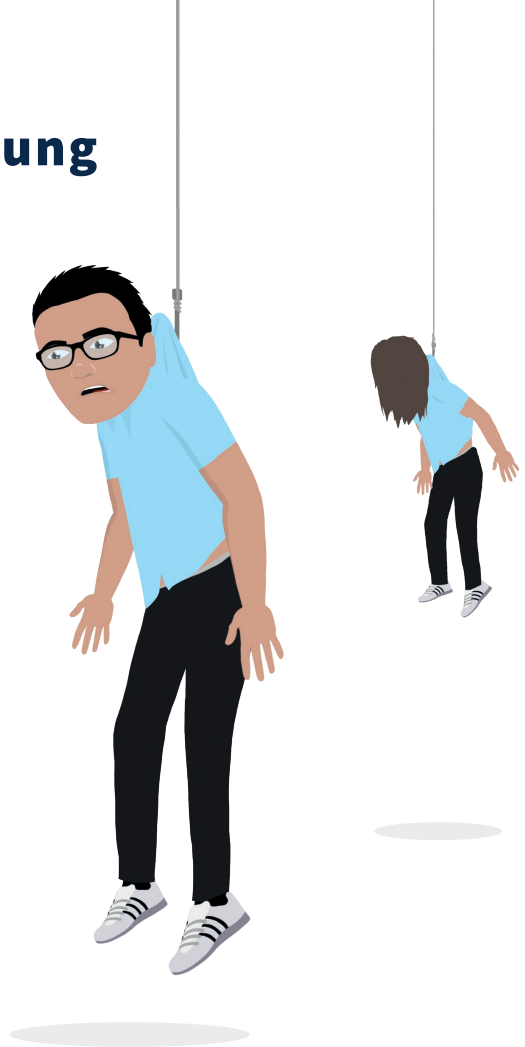
Scorebeschreibung

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

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 Online-Kursen für alle Angestellten**
2. **Spezialschulung und Webinare für alle Angestellten und Abteilungen mit Ratings von 2,5 – 4,8**
3. **Phishing-Kampagnen verschiedener Schwierigkeitsgrade im 3-Monats-Rhythmus und anschließende Nachbesprechung der Angriffsszenarien**
4. **Newsletter mit aktuellen Angriffsszenarien**
5. **Meldebutton für erkannte Phishing-E-Mails**
6. **Nachkontrolle nach 6 Monaten mithilfe einer weiteren Evaluierungskampagne**



> *Das Unternehmen konnte in nur 6 Monaten das Rating auf 1,4 verbessern und liegt somit in der Bewertung weit über dem Branchendurchschnitt.*

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.

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 verschiedener Dateiformate

SO ERREICHEN SIE UNS:

Katharinenstraße 21, 04109 Leipzig

+49 341 249 116 71

www.**increaseyourskills**.com

info@increaseyourskills.com

CYBERSECURITY™
MADE IN EUROPE

Initiated by ECSO. Issued by eurobits e.V.

STARTEN SIE DURCH
– GEMEINSAM MIT UNS!