Increase YourSkills

CYBER SECURITY

Case Study 2023

Content

1 Introduction
4 Summary
5 Why?
7 Phishing Initial Audit
9 Recommended Actions
10 Result
11 Contact

Introduction

As early as 2000, security expert Bruce Schneier noted that after the exploitation of vulnerabilities in hardware and software, the IT world was already in the midst of the third ‘semantic’ wave of network attacks: attacks on people who use hardware and software. These are worse than physical or syntactic attacks because, as Schneier says, they “directly target the human/computer interface, the most insecure interface […] and any attempt to solve the problem must deal with people, not technology.“

This case study shows that awareness-raising measures in the context of a phishing simulation have led to a significant change in the way people use email. In this case, with an anonymised corporate client (GmbH), the phishing training for the employees, the staff representatives, two data protection officers and the IT department took place in two mailings.

48%

of German companies pay a ransom in response to a ransomware attack*

** Hiscox - Cyber Readiness Report 2022*

Among other things, three spear phishing emails were sent out in the phishing training mailing. One of these emails, supposedly originating from the management, would have attempted to install malware on the computer of the persons concerned by means of a drive-by exploit.

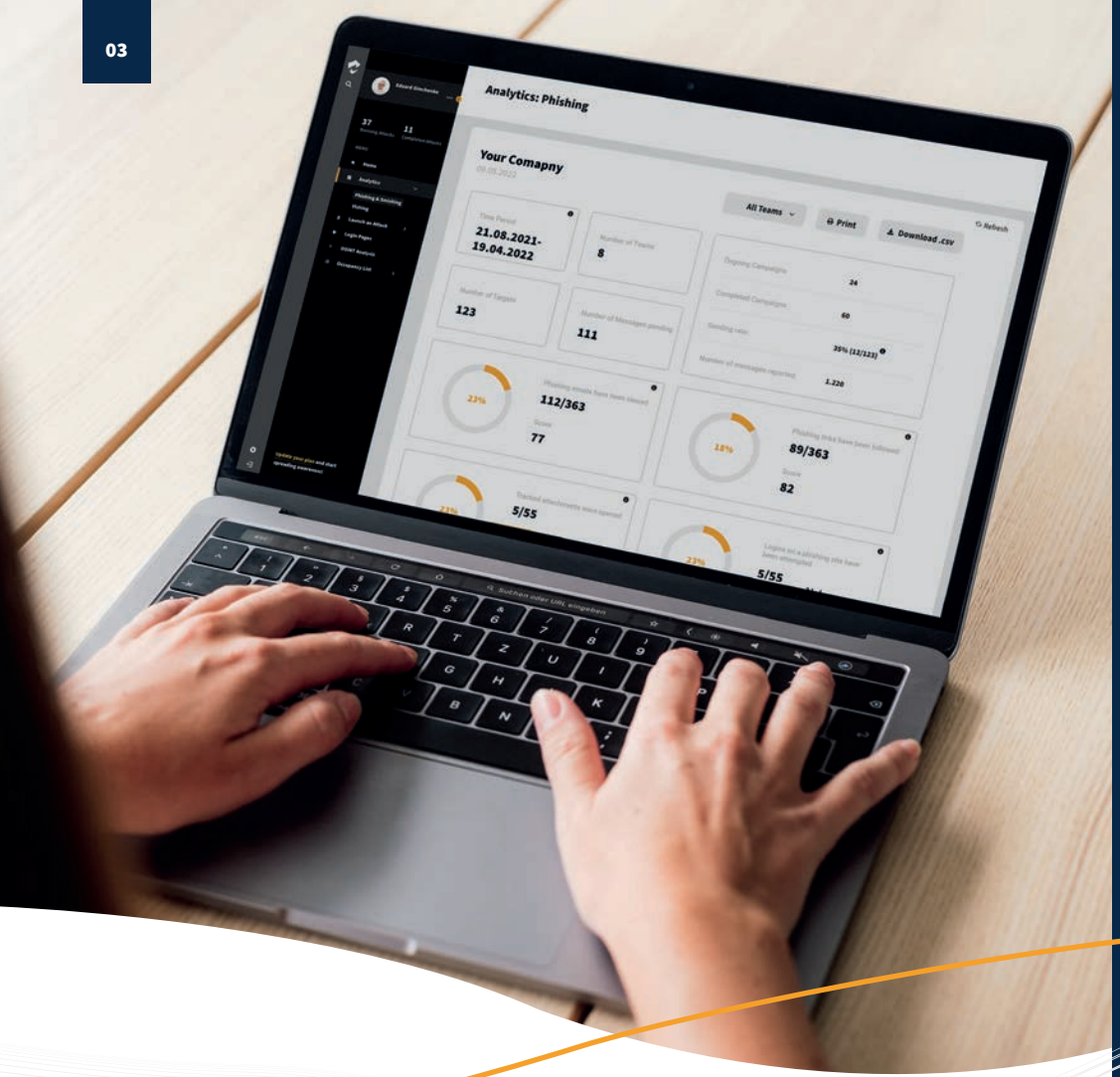
Another email, supposedly from the finance department, simulated a possible but rather improbable work instruction: all personal data should be sent to the responsible department via email as part of address verification.

> *“Cyberattackers do not abide by rules, ethical norms or cultural traditions.”*

69%

of all spam emails in 2022 were cyberattacks such as phishing emails and mail extortion.*

**The State of IT Security in Germany in 2022*



Summary

The client utilised the Phishing Attack Simulator (PAS) to conduct a phishing initial audit to check employees' resilience to social engineering attacks. Individual attack scenarios were created and tested in a spear phishing campaign with the help of Open Source Intelligence (OSINT) mechanisms.

The aim was to measure the following metrics in order to issue an individual security score for the company:

- *The opening rate of malicious emails*
- *The click rate of malicious links in emails*
- *The input of login credentials on phishing websites*
- *The opening rate of malicious attachments (using various file formats)*

Cybersecurity: The Path from Knowledge to Action is Long

The pandemic has changed the world. However, one thing that has remained the same is the unscrupulous behaviour of cybercriminals. As a result, protection from cyberthreats continues to be a challenging task.

> *"This epochal shift is a journey, and like any journey, the road is paved with risks and threats."*

34,000

mails with malware were intercepted on average every month in German government networks.*

**The State of IT Security in Germany in 2022*

Why?

The 2022 Human Factor Report shows that more than 9/10 cyberattacks use human vulnerability as their primary method to penetrate IT systems1.

This confirms that security awareness is the most important building block in developing a meaningful information security structure and the biggest driver for reducing damage scenarios.

Furthermore, a representative survey with the support of PwC shows that the most significant financial loss from cyberattacks can be attributed to phishing[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

> *"The challenges posed in cyberspace remain high and will continue to grow rapidly."**

** Dr. Gerhard Schabhüser, Vice President of the Federal Office for Information Security: BSI – The State of IT Security in Germany in 2022*

>80%

of businesses are attacked by a compromised supplier account in any given month.*

** Human Factor Report 2022*

Phishing Initial Audit

In order to evaluate the risks of potential damage, an initial audit of the company was conducted, for which the IYS Full-Service Awareness Platform carried out the following actions:

- *Creation of 3 customised phishing scenarios using our OSINT engine*
- *Sending of 12 phishing emails per participant*
- *Issuing of a management report*

The following results came to light:

Opening rate of malicious emails

Click rate of malicious links in emails

Input of login credentials on phishing websites

Opening rate of malicious attachments (using various file formats)

The risk level was thus assessed to be a class C-rating (moderate). The exact score is measured with the index of 3.0 (see score description). Even though these are alarming values, they represent the industry average and demonstrate how vulnerable the company is.

A click rate of 39% of malicious links for all participants raises four questions:

1. **Why did so many people click on the linkin the email?**
2. **Why didn‘t more recipients click on the link in the email?**
3. **How do the people concerned feel about the results of the campaign?**
4. **What do the users think of this unfamiliar awareness measure?**

Score Description

Cybersecurity-Index	Score	Rating Class	Risik Profile
1,0 – 1,4	100 – 91	**A**	Excellent
1,5 – 1,9	90 – 81	**A**	Very low
2,0 – 2,4	80 – 71	**B**	Low
2,5 – 2,9	70 – 61	**B**	Medium
3,0 – 3,4	60 – 51	**C**	Moderate
3,5 – 3,9	50 – 35	**C**	Increased
4,0 – 4,3	34 – 25	**D**	High
4,4 – 4,9	24 – 15	**D**	Very high
5,0 – 5,0	14 – 0	**D**	Extremely high
6,0 – 6,0	–	**E**	Unrated

Recommended Actions

In order to sustainably improve the company's security score and reduce the risk potential, we have made the following recommendations:

1. **Basic awareness training in the form of online courses for all employees**
2. **Special training and webinars for all employees and departments with ratings of 2.5 – 4.8**
3. **Phishing campaigns of various levels of difficulty every 3 months and subsequent debriefing of the attack scenarios**
4. **Newsletter with current attack scenarios**
5. **Reporting button for detected phishing attacks**
6. **Follow-up after 6 months with the help of another evaluation campaign**

> *"The company was able to improve its rating to 1.4 in only 6 months and is thus far above the industry average."*

Result

After 6 months, another phishing campaign with the same parameters was sent to the company. Similar levels of difficulty of the attack scenarios were used to establish comparability.

The following results came to light:

Opening rate of malicious emails

Click rate of malicious links in emails

Input of login credentials on phishing websites

Opening rate of malicious attachments (using various file formats)

HOW TO REACH US:

24 Old Queen Street, London, SW1H 9HP

+44 20 4586 8499

www.**increaseyourskills**.com

info@increaseyourskills.com

CYBERSECURITY™
MADE IN EUROPE

Initiated by ECSO. Issued by eurobits e.V.

JOIN US AND GET STARTED