Cyber Security Awareness

Was ist PHISHING und worauf muss ich achten?

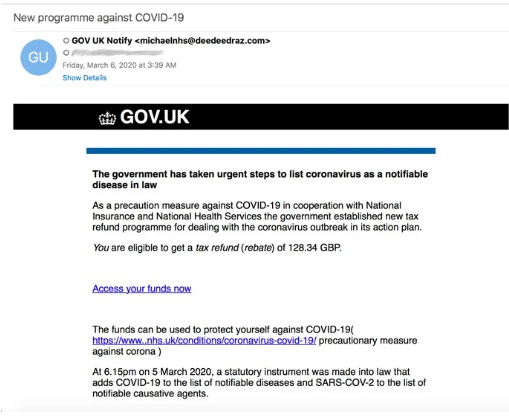
Phishing ist eine Cyberangriffsform, bei der der Angreifer Nachrichten an eine Person, ein Unternehmen oder einer ganzen Organisation verschickt, mit dem Ziel, sensible Informationen oder Daten vom Empfänger zu entlocken oder den Empfänger zum Download von einem Schadcode zu verführen, um so den jeweiligen Arbeitgeber zu schaden. Die Informationen, welche der Angreifer versucht zu entlocken sind personenbezogene Daten, Passwörter, Login- Daten oder Transaktionsnummern. Beim Phishing erschleichen sich die Betrüger das Vertrauen der Empfänger, in dem sie irreführende Behauptungen aufstellen oder ein Szenario inszenieren, welches eine bestimmte Reaktion provozieren soll. Meistens geben sich diese Betrüger als vertrauenswürdige Instanz aus, wie z.B. eine Bank, um so die Opfer zu ködern und diese zu der gewünschten Handlung zu bewegen.

Die beliebteste Form des Phishings sind Phishing- E- Mails. Dabei handelt es sich um gefälschte E- Mails, mit denen versucht wichtige Daten vom Empfänger zu stehlen. Dabei verwenden Angreifer eine E- Mail- Adresse, welche dem Anschein nach von einem vertrauenswürdigen Absender stammen könnte. In der E- Mail wird meistens aufgefordert auf einen Link zu klicken oder seine Angaben zu bestätigen oder zu aktualisieren. Wird dem nachgegangen wird der Empfänger auf eine gefälschte Website weitergeleitet, welche dann die sensiblen Daten abgreift.

Welche Punkte für welche Berufsgruppe zu beachten sind

Personal der Gesundheitsberufe

Ein Bild, das Text enthält.

Automatisch generierte BeschreibungDie Angriffsform des Phishings ist vor allem im Gesundheitsbereich anzutreffen. Vor allem die Zeit der COVID- 19 Pandemie wurden von Angreifern ausgenutzt, um sensible Daten abzufangen. Hier sind zwei Beispiele, die ich zum Thema gefunden habe:

Betrügerische E- Mail, welche sich   
als die britische Regierung ausgibt

Identität der WHO wird hier   
vorgetäuscht

Quelle zu den Bildern: <https://tehtris.com/de/blog/die-welt-des-gesundheitswesens-im-angesicht-von-cybergriffen>

Vor allem im Gesundheitsbereich bringen Cyberangriffe ein hohes Risiko mit sich, da sich um sensible personenbezogene Daten handelt, welche Angreifer versuchen zu entlocken, und daher könnte auch die Sicherheit und/oder Gesundheit eines Patienten involviert sein. Aus diesem Grund ist es sehr wichtig, dass das Personal Phishing- E- Mails oder Websites erkennen können. Diese Punkte muss das Personal im Gesundheitsbereich beachten, um Phishing zu erkennen:

* Überprüfung der Absender- Adresse: Da häufig sich Angreifer als vertrauensvolle Instanzen oder Unternehmen ausgeben, sehen die E- Mail- Adressen zu dem Original sehr ähnlich, aber dennoch gibt es kleine Unterschiede. Aus diesem Grund sollte man unbedingt die Absender- Adresse überprüfen.
* Überprüfung des Betreffs: Sollte der Betreff merkwürdig rüberkommen, dann ist Vorsicht geboten und es sollte einem bewusst sein, dass es sich möglicherweise, um eine Phishing- E- Mail handelt.
* Überprüfung der Anrede: Es ist üblich, dass in Phishing- E- Mails die Empfänger nicht persönlich angesprochen werden. Vor allem wenn eine E- Mail von einem Unternehmen stammen soll und die Anrede „ Sehr geehrte Damen und Herren“ ist, kann dies ein Anzeichen für Phishing sein. Jedoch muss in dem Fall auch nach weiteren Anzeichen Ausschau gehalten werden.
* Überprüfung der Formatierung: Phishing- Mails weisen oft eine schlechte Rechtschreibung oder Syntax auf. Auch Reste von HTML- Behlen wie <b> </b> oder <p> deuten auf Phishing. Zudem ist auch ein uneinheitliches Layout oder ein Wechsel der Schriftart ein Zeichen.
* Überprüfung, ob man zur Angabe von persönlichen Daten ausgefordert wird: Phishing- Mails sind dafür bekannt, dass die Empfänger aufgefordert werden persönliche Daten zu bestätigen. Einige dieser E- Mails enthalten auch Bedrohungen wie „Wenn Sie Ihre Daten nicht bestätigen, wird Ihr Konto gesperrt“. Dies geschieht auch in Kombination mit Fristsetzungen. Die Forderungen können vertrauliche Daten, wie PIN, TAN, Passwort, Adresse oder auch ein Geburtsdatum sein. Es ist wichtig sich im Bewusstsein zu rufen, dass echte Unternehmen nicht nach solchen Daten in einer E-Mail fragen.
* Überprüfung von Links auf Websites: Phishing- Mails könne auch mit Links auch auf Websites verweisen. Diese Links sehen dem Original sehr ähnlich. Daher sollte man, überprüfen, ob diese Links merkwürdige Zahlen- und Buchstaben- Kombinationen enthalten. Wird auf die Website geklickt, so könnte ein Virus unbewusst heruntergeladen werden.
* Überprüfung der Anhänge: Häufig enthalten Phishing- Mails Anhänge, welche meistens keine ordentlichen Namen haben, sondern nur Zeichenfolge. Aussehen können sie wie ein Bild oder PDF- Datei. Beim Herunterladen wird man entweder auf eine gefälschte Website weitergeleitet oder es wird ein Computervirus gedownloadet. Der Anhang einer Phishing- Mail darf nicht geöffnet oder heruntergeladen werden!
* Phishing- Mails betroffenen Unternehmen melden: Gibt es die Vermutung, dass eine gefälschte E- Mail von einem bekannten Unternehmen erhalten worden ist, sollte dieses Unternehmen über dessen in Kenntnis gesetzt werden. So kann einerseits sichergestellt werden, ob die E- Mail tatsächlich vom Unternehmen stammt und andererseits weiß das Unternehmen, dass in seinem Namen gefälschte E- Mails verschickt werden.
* In der Gesundheitsorganisation bekanntmachen: Damit nicht andere Mitarbeiter auf dem Phishing- Angriff reinfallen, muss der Vorfall in der Organisation schnellstmöglich bekannt gemacht werden. Am besten ist es eine E- Mail mit einem Screenshot von der Phishing- Mail an die gesamte Organisation zu verschicken. Man kann den Vorfall auch zuerst beim Vorgesetzten bekanntgeben und dieser kümmert sich dann um die Bekanntgabe.

Die oben genannten Punkte sind auch vom Personal der Verwaltung, der Haus- und Betriebstechnik sowie vom Personal der Medizintechnik zu beachten.

Was ist SMISCHING und worauf muss ich achten!

Genau wie Phishing handelt sich auch beim Smishing um eine Cyberangriffsform. Smishing setzt sich aus den Worten „SMS“ und „Phishing“ zusammen. Bei dieser Cyberangriffsattacke werden gefälschte Textnachrichten verschickt mit dem gleichen Ziel wie beim Phishing- die Angreifer möchten sensible persönliche Daten entlocken. Smishing- Attacken sind stark im Kommen, da viel mehr Leute skeptisch gegenüber E- Mails sind als SMS. Von Phishing haben die meisten gehört und selber schon Erfahrung damit gehabt und aus diesem Grund sind viele vorsichtig gegenüber verdächtigen E- Mails, jedoch schienen die meisten Menschen unvorsichtiger gegenüber SMS zu sein.

Smishing- SMS enthalten einen für den Empfänger schädlichen Inhalt. In erster Linie versuchen Angreifen mit dieser Form der Cyberattacke Bankverbindungen, Passwörter oder andere sensible Daten vom Opfer zu entlocken. Um dies zu erreichen wird manchmal sogar eine schädliche Software auf dem Gerät des Opfers installiert. Social Engineering\* wird häufig in Kombination mit Smishing eingesetzt. Angreifer sind zudem in der Lage persönliche Informationen, wie z.B. Name und Adresse, welche sie aus öffentlichen Online- Tools bekommen haben, einzusetzen. So kann der Smisher den Namen und Standort des Empfängers verwenden, um diesen direkt anzusprechen. Durch diese Details ist die Nachricht aussagekräftiger. In der SMS ist dann ein Link enthalten, welcher auf Phishing- Seiten für Anmeldeinformationen weiterleitet oder zu einer Malware ( =Überbegriff für verschiede Arten von schädlichen Programmen) führt.

\*Social Engineering: Social Engineering befasst sich mit Manipulation und wird häufig von Cyberkriminelle benützt. Angreifer verwenden dabei Informationen aus sozialen Netzwerken und versuchen die menschliche Natur für ihre Zwecke auszunutzen. Dabei setzten die Angreife auf Gefühle wie Angst, Gier, Empathie und versuchen so den Denkprozessen der Empfänger zu manipulieren.

Welche Punkte für welche Berufsgruppe zu beachten sind

* Überprüfung des Absenders: Genau wie beim Phishing versuchen Angreifer das Vertrauen der Opfer zu gewinnen indem sie die Identität von vertrauenswürdigen Instanzen, Unternehmen oder Organisationen annehmen. Erscheint eine SMS als merkwürdig, sollte man bei der entsprechenden Organisation oder Unternehmen nachfragen. Zudem sollte bewusst sein, dass vertrauenswürdige Instanzen, Organisationen oder Unternehmen niemals eine SMS senden würde, in der man aufgefordert wird, seine Daten anzugeben. Aus diesem Grund sollte man zweimal den Namen des Absenders überprüfen.
* Überprüfung des Inhalts: Beinhaltet die SMS beispielsweise die Bekanntgabe über ein Wettbewerb an dem Sie angeblich gewonnen haben, dann handelt es sich höchstwahrscheinlich um eine Smishing- Attacke. Das selbe Konzept kann auch mit einer Bestellungsinformation erscheinen. Wichtig hierbei ist nicht auf den Link zu klicken, die Organisation in der Sie arbeiten schnellstmöglich zu informieren und anschließend die Nachricht zu löschen. Es könnte hilfreich sein davor ein Screenshot zu machen und diesen bei der Bekanntgabe der Organisation mit bsw. einer E- Mail im Anhang mitzuverschicken. Der Screenshot kann auch eine Absicherung sein, falls eine weitere Smishing- Attacke folgt. In dem Fall kann man die SMS mit dem Screenshot vergleichen und so nach Muster Ausschau halte.

Ein weiterer Punkt auf dem man achten muss ist, ob man aufgefordert wird, eine App herunterzuladen. Denn dabei könnte es sich um eine Malware handeln.

* Überprüfung, ob nach persönlichen Informationen gefragt wird: Angreifer können sich sogar als Personen aus dem direkten Umfeld ausgeben um an Informationen zu kommen. Falls Sie aufgefordert werden von jemanden, welcher sich als eine Person aus Ihrem Umfeld auszugeben versucht, Informationen anzugeben, dann ist es klüger erstmals die Identität des Absenders zu überprüfen, indem Kontakt zu der entsprechenden Person aus Ihrem Umfeld aufgenommen wird.

Die oben genannten Punkte sind von allen Berufsgruppen (Personal des Gesundheitswesens, Personal der Verwaltung, Personal Haus- und Betriebstechnik und Personal der Medizintechnik) zu beachten.

Die beste Möglichkeit sich als Unternehmen oder Organisation vor Phishing- und Smishing- Attacken zu schützen ist, die Angestellten zum Thema Cybersicherheit schulen zu lassen. So können sie über die Merkmale aufgeklärt werden und ihnen kann auch bewusst gemacht werden, welche Risiken solche Attacken darstellen.

Quellen:

* <https://www.heise.de/tipps-tricks/Phishing-Mails-erkennen-und-richtig-handeln-3974927.html#anchor_2>
* <https://de.norton.com/blog/online-scams/what-is-phishing>
* <https://www.proofpoint.com/de/threat-reference/phishing>
* <https://www.avira.com/de/blog/so-erkennen-sie-smishing-nachrichten>
* <https://cyber-samurai.net/wissen/glossar/smishing/#phishing-smishing-vishing>
* <https://www.proofpoint.com/de/threat-reference/smishing>