Fragen und Antworten zur Phishing-Kampagne an der Universität Bielefeld

1. Was umfasst die Phishing-Kampagne und wer führt sie durch?

Die Phishing-Kampagne richtet sich an alle Beschäftigten der Universität Bielefeld. Ziel ist es, diese in den Bereichen Phishing und Informationssicherheit weiterzubilden. Unter dem Kunstwort Phishing versteht man Versuche, über gefälschte E-Mails, Webseiten oder andere Formen der Kommunikation die digitale Identität (z. B. Passwörter) der Betroffenen zu stehlen und zum eigenen wirtschaftlichen Vorteil zu missbrauchen.
Im Rahmen der Phishing-Kampagne versenden wir – die SoSafe GmbH aus Köln – im Auftrag der Universität an alle Beschäftigten in unregelmäßigen Abständen simulierte Phishing-Mails. Ziel dieser Simulation ist es, dass Sie "direkt am Objekt" lernen können, wie Phishing funktioniert und woran Sie es erkennen können. Zu diesem Zweck bieten wir darüber hinaus eine umfangreiche Lernumgebung (E-Learning) an: Anhand von interaktiven Lernmodulen, kurzen Videos, Beispielen aus dem Arbeitsalltag und kurzen Quizfragen können Sie die wichtigsten Regeln und Hinweise für den sicheren Umgang mit E-Mails, Computern, Smartphones und Daten lernen und vertiefen.
Behandelt werden z. B. Themen wie Passwortnutzung, Schadsoftware oder Datenmissbrauch. Die Universität erhält keine individuellen Daten über die Phishing-Simulation, sondern lediglich eine vollkommen anonyme Auswertung.

2. Warum wird die Simulation durchgeführt?

Die Phishing-Simulation wird durchgeführt, weil z. B. allein in Deutschland jährlich ein Schaden von 5,6 Mrd. Euro durch Wirtschaftsspionage und Cyberkriminalität entsteht. Solche Angriffe beginnen überwiegend mit einer Phishing-Mail. Bei gezielten Phishing-Angriffen klicken teilweise die Hälfte der Empfänger/innen auf enthaltene Phishing-Links oder öffnen gefährliche Dateianhänge. Durch dieses Verhalten wird den Angreifern/innen ermöglicht z. B. Zugang zu sensiblen dienstlichen Daten oder privaten Informationen zu erlangen. Um solche Angriffe zu verhindern, ist es daher wichtig, alle Beschäftigten für die Risiken und den richtigen Umgang mit Phishing-Mails zu sensibilisieren und zu schulen.

3. Welchen Vorteil bietet die Simulation für mich?

Die Simulation hilft Ihnen nicht nur schädliche Phishing-Mails im beruflichen Umfeld zu erkennen und damit sich und die Universität vor potenziell großem Schaden zu schützen. Sie können das erworbene Wissen auch in Ihrem privaten Kontext nut-

zen, um das Risiko von Cyber-Angriffen für sich und Ihre Familie zu verringern. Denn häufig werden die gezeigten Taktiken auch für Phishing-Angriffe auf Privatpersonen verwendet.

4. Welche Daten werden verarbeitet?

In Abstimmung mit der Universitätsleitung, den Personalräten und der Datenschutzbeauftragten der Universität erhalten wir von der Universität eine Liste mit den E-Mail-Adressdaten aller Beschäftigten. Diese Liste beinhaltet die korrekte Anrede, den Vornamen und Nachnamen, die E-Mail-Adresse, sowie eine Zuordnung zu einer größeren Gruppe (Fakultät bzw. Einrichtung). Diese Daten werden von uns benötigt, um die Phishing-Simulation durchzuführen. Die Universität erhält eine aggregierte und anonyme Auswertung über die Ergebnisse der Phishing-Kampagne. Diese Auswertung lässt keinen Rückschluss auf das Verhalten einzelner Personen zu. Sämtliche Daten werden von uns ausschließlich im Rahmen der bestehenden vertraglichen Vereinbarungen zur auftragsbezogenen Verarbeitung personenbezogener Daten mit der Universität verarbeitet. Im Zuge dessen treffen wir umfangreiche Maßnahmen, um sämtliche Daten angemessen zu schützen.

5. Sind die Phishing-Mails von SoSafe in irgendeiner Weise gefährlich?

Nein, die Mails sind nicht gefährlich, es handelt sich dabei nur um eine Simulation. Zu keiner Zeit sind Ihre persönlichen/dienstlichen Daten oder Ihre Endgeräte in Gefahr. Wenn Sie auf einen enthaltenen Link in einer unserer Phishing-Mails klicken, gelangen Sie auf eine Lernseite im Internet. Dort erhalten Sie nähere Informationen zu der Simulation und vor allem konkrete Hinweise, woran Sie bei dieser konkreten Mail hätten erkennen können, dass es sich um einen Phishing-Versuch handelt.

6. Ich habe auf eine der Phishing-Mails per Mail geantwortet. Werden meine Antworten an SoSafe weitergeleitet?

Ja, diese Antwortmails werden von unseren Servern angenommen. Dort werden sie jedoch sofort vollständig anonymisiert. Sie sind also nicht einer Person zuzuordnen. Es wird lediglich automatisiert ausgewertet, ob eine Antwort erfolgt ist und ob es sich um eine technische Antwort (automatisch von Ihrem Mail-Server generiert), eine automatische Abwesenheitsnotiz oder um eine tatsächliche Antwortmail gehandelt hat. Die Universität erhält eine Kennzahl, die wiedergibt, auf wie viele der Phishing-Mails geantwortet wurde. Sie erhält aber keinen Einblick in den Inhalt der Antworten.

7. Was passiert, wenn ich aus Versehen meine Passwortdaten preisgegeben habe?

Einige unserer Phishing-Mails führen Sie auf eine speziell präparierte Webseite, wo z. B. Ihr Passwort abgefragt wird. Egal was Sie dort in die Formularfelder eingeben, diese Daten werden nicht von uns gespeichert. Es wird von unserem Server lediglich

registriert, dass Daten eingegeben wurden. Im Rahmen der Auswertung der Phishing-Simulation erhält die Universität von uns eine Information, bei wie vielen solcher Eingabemasken etwas eingegeben wurde. Auch hier ist jedoch nicht nachvollziehbar, welche Beschäftigten Daten eingegeben haben. Ein Rückschluss auf das Verhalten einzelner Personen ist technisch ausgeschlossen.

8. Was mache ich, wenn mir eine E-Mail verdächtig vorkommt?

Informieren bzw. kontaktieren Sie ihre EDV-Betreuung bzw. den Service Desk des BITS (servicedesk@uni-bielefeld.de oder -6000). Dort werden Sie über das weitere Vorgehen informiert.

9. Stört mich die Trainingsmaßnahme bei meiner Arbeit?

Echte Phishing-Mail-Angriffe können Sie jederzeit treffen – auch bzw. gerade während der Arbeitszeit. Jedes Jahr entstehen hohe finanzielle Schäden für Unternehmen, den öffentlichen Dienst und Privatpersonen durch Phishing und Betrug im Internet. Unsere Phishing-Simulation ist so aufgebaut, dass Sie während der täglichen Arbeit keine zeitaufwändigen Störungen erleben, aber dennoch eine effektive Trainingsmaßnahme für den Umgang mit Phishing erfahren. Zusätzlich bieten wir mit unserer E-Learning-Plattform die Möglichkeit, dass Sie Ihr Wissen zu Themen rund um IT-Sicherheit in kurzen Lernmodulen vertiefen können. Mit diesem Wissen schützen Sie sich selbst und die Universität vor Phishing-Angriffen aus dem Internet.

10. Ich habe eine inhaltliche Frage zu einem Thema aus den Infotexten auf den Lernseiten oder dem SoSafe E-Learning. An wen kann ich mich wenden?

Wenden Sie sich bei Fragen, die den Einsatz von IT in der Universität betreffen, bitte zunächst an Ihre EDV-Betreuung bzw. den Service Desk des BITS (servicedesk@uni-bielefeld.de oder -6000). Bei Fragen zu unseren Phishing-Mails oder unserem E-Learning-Angebot können Sie sich auch gerne an unseren Support (support@sosafe.de) wenden.

11. Werden meine Antworten aus dem Quiz-Teil der E-Learning-Module an den Arbeitgeber zurückgemeldet?

Wenn Sie das Schulungsangebot (E-Learning) über unsere Webplattform verwenden, absolvieren Sie am Ende jedes Lernmoduls ein kurzes Quiz, welches immer vier Fragen umfasst. Ihre individuellen Antworten in diesem Quiz werden nicht an die Universität zurückgemeldet. Diese erhält lediglich Informationen darüber, wie viele Personen sich auf der E-Learning-Webplattform registriert haben und wie viele Module bereits abgeschlossen und bestanden wurden. Die Universität sieht also nur, wie der Fortschritt aller Beschäftigten insgesamt ist.

12. Erhalte ich einen Nachweis über meine Lernerfolge?

Ja, als registrierte/r Benutzer/in auf unserer E-Learning-Plattform können Sie sich Ihr persönliches Zertifikat ausstellen lassen. Damit können Sie festhalten, dass Sie die Lernmodule absolviert und die Wissensabfragen bestanden haben.

13. Wo erhalte ich weitere Informationen zum Thema Informationssicherheit?

Vertieft werden die Themen rund um Informationssicherheit in unserer E-Learning-Plattform aufgegriffen. Der Zugang zu der E-Learning-Plattform wird Ihnen von der Universität zur Verfügung gestellt.

Weitere Informationen finden Sie auf der Webseite des Informationssicherheitsbeauftragten: https://www.uni-bielefeld.de/informationssicherheit. Herr Sundermeyer steht Ihnen für Fragen gerne zur Verfügung (informationssicherheit@uni-bielefeld.de oder -3032).

Stand: 18. November 2019