phishing.42

Phishing-Agriffe

Cyberkriminelle zielen ihre Attacken nicht ausschließlich digital auf die IT-Infrastruktur von Unternehmen, sondern versuchen auch über die Mitarbeiter an Informationen und Zugänge zu kommen oder diese zur unbeabsichtigten Mitwirkung bei der Ausführung von Schadcode zu gewinnen. Diese Art von Angriffen wird als Social-Engineering bezeichnet und stellt die derzeit häufigste Ursache für erfolgreiche Einbrüche in IT-Infrastrukturen dar.
Die Bedrohung, die von diesen Angriffen ausgeht, stuft das BSI im Bericht „Die Lage der IT-Sicherheit in Deutschland 2019“ weiterhin als relevante Bedrohung ein.

Ziel

Im Rahmen der Dienstleistung phishing.42 wird ein simulierter Social-Engineering-Angriff über E-Mail auf alle oder ausgewählte Mitarbeiter eines Unternehmens durchgeführt. Ziel ist die Sensibilisierung der Mitarbeiter zu den Themen E-Mails mit schadhaftem Link (Drive-by-Download) bzw. schadhaftem Inhalt (Malware) und Phishing zu prüfen. Viele unserer Kunden nutzen die Kampagne auch im Rahmen einer Sensibilisierung zum Thema Informations-sicherheit.

Die Leistung gliedert sich in folgende Schritte:

Übergabe der E-Mail Adressen

Der Auftraggeber übergibt die E-Mail-Adressen der Zielpersonen. Oft erfolgt hierbei auch eine Zuordnung der E-Mail Adressen zu Organi-sationseinheiten des Auftraggebers.

Aufbau von gefälschten Webseiten

Im Rechenzentrum der plan42 werden gefälschte Webseiten aufgebaut. Hierbei handelt es sich, ahängig vom gewählten Szenario, um Seiten zum Download von Gutscheinen, Informationsdienste und Login-Seiten für Intra- oder Extranet-Seiten.

E-Mail Versand

Den Zielpersonen für diesen Test wird ein Anschreiben per E-Mail geschickt, in dem sie, abhängig vom Szenario, z. B. über die Möglichkeit zum Herunterladen von Gut-scheinen auf einer Webseite informiert oder zur Eingabe von Login-Daten aufgefordert werden.
Die Schwierigkeit der Erkennung dieser E-Mails als Fälschung, wird in Abstimmung mit dem Auftraggeber festgelegt.
Hierbei kann es sich um eine professionelle, schwer zu erkennende Phishing E-Mail mit gefälschtem Absender oder auch um E-Mails mit mehr oder weniger versteckten Hinweisen auf eine Fälschung handeln.

Auswertung und Berichterstellung

In jeder E-Mail an die jeweiligen Zielpersonen ist ein individueller HTTP-Link integriert. Hiermit kann zugeordnet werden, welche Personen die Links anklicken bzw. Daten auf den Phishing-Seiten eingeben.
Die Auswertung dieser Informationen kann komplett anonym, personalisiert oder auch individuell z. B. auf Ebene von Organisationsein-heiten des Auftraggebers erfolgen.
Wir setzen strenge Anforderungen im Bereich der technischen und organisatorischen Maß-nahmen zum Schutz der uns übergebenen Daten um.

Nach Beendigung des Auftrags werden alle personenbezogenen Informationen datenschutz-konform gelöscht.

Szenarien

Im Standard Angebot sind zwei Angriffs-szenarien enthalten. Diese werden typischer-weise mit einem Zeitabstand von 4-8 Wochen durchgeführt.