Simulierter (Spear-)Phishing und USB-Drop Angriff

Gemäss ENISA Threat Landscape zählen Phishing-Scams zu den Top Threats der letzten Jahre. Während der Covid-19 Pandemie ist die Anzahl der Phishing-Scams ebenfalls drastisch gestiegen. Die Tendenz ist weiterhin steigend.

Des Weiteren nutzen Cyberkriminelle die natürliche Neugier von Mitarbeitern/Innen durch die Platzierung von präparierten USB-Speichermedien aus, um sich Zugang zu Systemen zu verschaffen. Diese Art von Angriff wird auch als USB-Drop-Attack bezeichnet.

Mitarbeitende, unabhängig von Sektor und Position, sehen sich ständig dieser steigenden Sicherheitsbedrohungen ausgesetzt. Seit Jahren werden gezielt menschliche Schwachstellen durch Cyberkriminelle ausgenützt, um schützenswerte Daten– und Informationen zu entwenden, oder die Basis für weiterführende Angriffe gegen die Organisation zu legen.

Protect7 bietet die Möglichkeit die Awareness Ihrer Mitarbeitenden, unabhängig der Position, durch einen simulierten (Spear-)Phishing und/oder USB-Drop Angriff zu überprüfen.

Methode

Bei einem (Spear-)Phishing Angriff wird den potentiellen Opfern ein realistisches Szenario vorgespielt, um sie absichtlich zu täuschen.

Gut funktionierende Szenarien werden bei Phishing-Versuchen in der Regel durch eine E-Mail von einem gefälschten, aber dem Empfänger bekannten Absender (von einem Geschäftspartner, internem Mitarbeiter) oder zu einem bekannten bevorstehenden Event mit dem Ziel versendet, dass die Opfer auf einen Link in der Mail klicken und/oder auf der erreichten Webseite entsprechende sensitive Daten eingeben.

Bei einem USB-Drop Angriff werden von uns präparierte USB-Sticks im und um das Firmengelände platziert. Sie werden mit dem Ziel platziert, dass neugierige Opfer einerseits den USB-Stick in ein Gerät einstecken und andererseits eine Datei auf dem USB-Stick öffnen (je nach Szenario). Vorzugsweise befinden sich auf dem USB-Stick präparierte Dokumente mit konstant interessanten Themen, zum Beispiel „Lohnlisten" oder ähnliches.

Hauptziel

Das Hauptziel der Überprüfung besteht darin, herauszufinden ob Ihre Mitarbeitenden über genügend Security-Awareness verfügen und Angriffe wie diese erkennen bzw. entsprechend korrekt reagieren.

Sie erhalten dadurch eine Übersicht über die allgemeine Security-Awareness Ihrer Mitarbeitenden und können entsprechende Massnahmen frühzeitig erkennen und einleiten.

Sie erhalten

- Management Summary
- Technischer Report
- Empfehlungen für Verbesserungen
- Präsentation der Resultate
- Reduktion der Ungewissheit

Ihr Vorteil

- Übersicht über die Security-Awareness Ihrer Mitarbeitenden
- Frühzeitige Einleitung von Gegenmassnahmen
- Erster Schritt zur Erhöhung der Sicherheit im gesamten Unternehmen

Preis

- Der Preis ist abhängig von der Anzahl benötigter USB-Sticks und Unternehmensgrösse (Anzahl zu testende Mitarbeitende)
- Gerne unterbreiten wir Ihnen ein individuelles Angebot

SICHERHEITSANALYSEN